# Altell NEO

## Руководство пользователя

Версия документа 1.3

АльтЭль

Санкт-Петербург

2011

# Краткое содержание

# Содержание

# 1. ВВЕДЕНИЕ

В этом руководстве даны указания по использованию основных функций системы Altell NEO. 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.
- Публикации Altell NEO.

## 1.1. 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.

## 1.2. Структура руководства

Данное руководство может быть полезным, если необходимо найти следующие сведения:

- Краткий справочник по командам.

  В этом разделе можно быстро найти нужную команду.
- Краткий список примеров.

  В этом разделе можно быстро найти примеры для использования или изучения.

  Руководство состоит из следующих разделов и приложений:

*Таблица 1 - Структура руководства*

| Раздел | Описание | Страница |
|---|---|---|
| Раздел 1. Использование интерфейса командной строки | В этом разделе представлен обзор интерфейса командной строки Altell NEO, являющегося основным интерфейсом пользователя для системы Altell NEO. | 37 |
| Раздел 2. Управление системой | В этом разделе описаны функции системы Altell NEO для основных задач управления системой, таких как установка сведений об узле, работа с кэшем ARP и установка системных даты и времени. | 41 |
| Раздел 3. Управление пользователями | В этом разделе описана настройка пользователей и аутентификация пользователей. | 90 |
| Раздел 4. Учет трафика | В этом разделе описана настройка учета трафика с помощью системы Altell NEO. | 164 |
| Раздел 5. Регистрация | В этом разделе описан механизм регистрации (записи в журнал) событий в системе Altell NEO. | 189 |
| Перечень сокращений | | 2116 |

## 1.3. Условные обозначения

В руководстве используются информационные абзацы и соглашения о стиле текста.

### 1.3.1. 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.*

### 1.3.2. Соглашения о стиле текста

В данном документе используются следующие соглашения о стиле текста:

| | |
|---|---|
| `Моноширинный` | Примеры, вывод в командной строке и представление узлов конфигурации. |
| **`полужирный моноширинный`** | Пользовательский ввод: текст, вводимый пользователем в командной строке. |
| **полужирный** | Команды, ключевые слова и имена файлов, приведённые в тексте.<br>Объекты в интерфейсе пользователя, такие как вкладки, кнопки, экраны и панели. |
| *курсив* | Аргумент или переменная, вместо которой пользователь должен ввести значение. |

| | |
|---|---|
| <клавиша> | Клавиша на клавиатуре, такая как <Enter>. Сочетания клавиш обозначаются знаком "плюс" (“+”), например <Ctrl>+c. |
| [ *арг1* \| *арг2* ] | Перечисление вариантов составления синтаксиса. Пример: [enable \| disable]. |
| *число1–числоN* | Диапазон чисел, включая границы. Пример: 1–65535, что значит от 1 до 65535 включительно. |
| *арг1..аргN* | Диапазон строковых значений, в которые входят последовательные числа. Пример: eth0..eth3, что означает eth0, eth1, eth2 или eth3. |
| *арг*[ *арг*...] *арг*[,*арг*...] | Значение, которое может дополнительно представлять список элементов (через пробел в первом случае и через запятую во втором). |

# 2. ИСПОЛЬЗОВАНИЕ ИНТЕРФЕЙСА КОМАНДНОЙ СТРОКИ

В этом разделе представлен обзор интерфейса командной строки Altell NEO, являющегося основным интерфейсом пользователя для системы Altell NEO.

В этом разделе рассматриваются следующие вопросы:

- Возможности интерфейса командной строки.
- Основные команды интерфейса командной строки.

## 2.1. Возможности интерфейса командной строки

В этом разделе рассматриваются следующие вопросы:

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

### 2.1.1. Доступ к интерфейсу командной строки

Для доступа к интерфейсу командной строки следует войти в систему Altell NEO либо непосредственно через порт консоли, либо удаленно при помощи сеанса SSH.

- С консоли системы.
- Удаленно, при помощи SSH.

При подключении через последовательный порт (RS232) используются следующие параметры:

- Скорость: 115200 бит/сек;
- Без контроля четности (No parity);
- 8 бит данных (8 data bits);
- 1 стоповый бит (1 stop bit).

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

Когда выдача сообщения запуска системы прекратится, появится запрос на вход в систему:

```
neo login:
```

Войдите в систему, используя идентификатор пользователя и пароль определенной учетной записи пользователя. По умолчанию в системе есть одна предварительно определенная учетная запись пользователя: **admin**. У этого пользователя есть полномочия уровня администратора, что позволяет выполнять все команды Altell NEO и операционной системы. При автозавершении команд и в справке по интерфейсу командной строки отображаются только команды neo.

Идентификатор пользователя: **admin**

Пароль по умолчанию: **admin**

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

### 2.1.2. Интерфейс командной строки и интерпретатор команд системы Altell NEO

В интерфейсе командной строки системы имеются команды двух типов:

- Специфичные команды для эксплуатации и настройки системы Altell NEO.
- Команды, предоставляемые интерпретатором команд операционной системы, в котором работает интерфейс командной строки Altell NEO.

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

## 2.1.3. Уровни полномочий пользователя

Altell NEO поддерживает две роли пользователей:

- Уровень администратора.
- Уровень оператора.

В этом разделе рассматриваются следующие вопросы:

- Роль “Администратор”.
- Роль “Оператор”.

### *2.1.3.1. Роль “Администратор”*

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

Пользователь по умолчанию **admin** является административным пользователем.

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

```
admin@neo# set system login user имя_пользователя level admin
admin@neo# set system login user имя_пользователя authentication
plaintext-password пароль
admin@neo# commit
```

где *имя_пользователя* - это идентификатор создаваемой учетной записи, а пароль - это пароль, назначаемый этому пользователю.

Хотя команды интерпретатора команд операционной системы доступны административному пользователю всегда, они не отображаются при использовании этими пользователями автозавершения 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 Altell NEO будет очень сложно.

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

#### *2.1.3.2. Роль "Оператор"*

Пользователям-операторам предоставлены доступ только на чтение конфигурации и возможность выполнения эксплуатационных команд Altell NEO. 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 Altell NEO (при помощи команды **exit**). Пользователи-операторы 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 команды конвейера, такие как **more**, 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 используется следующая команда:

```
admin@neo# set system login user имя_пользователя level operator
admin@neo# set system login user имя_пользователя authentication
plaintext-password пароль
admin@neo# commit
```

где *имя_пользователя* - это идентификатор создаваемой учетной записи, а *пароль* - это пароль, назначаемый этому пользователю.

Команды интерпретатора команд операционной системы недоступны пользователям-операторам, соответственно, список команд, выдаваемых автозавершением команд пользователям уровня оператора, ограничен командами Altell NEO.

### 2.1.4. Режимы интерфейса

В интерфейсе командной строки Altell NEO имеются два режима: эксплуатационный режим и режим настройки.

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

В режиме настройки обеспечивается доступ к командам для создания конфигурации, ее изменения, удаления, фиксации изменений и отображения сведений о конфигурации, а также к командам 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.

### 2.1.5. Запросы для ввода команд

Запрос для ввода команд показывает пользователю, где он находится в интерфейсе командной строки, под какой учетной записью пользователя он вошел в систему и каково имя узла системы, на который он вошел.

В таблице 2 приведены некоторые примеры запросов на ввод команд и их значения.

*Таблица 2 - Запросы на ввод команд*

| Вид запроса | Смысл запроса |
|---|---|
| `admin@R1:~$` | Пользователь: **admin**<br>Имя узла: R1<br>Режим интерфейса: эксплуатационный режим |
| `admin@R1#` | Пользователь: **admin**<br>Имя узла: R1<br>Режим интерфейса: режим настройки |

### 2.1.6. Использование специальных символов в командах

Интерфейс командной строки Altell NEO основан на интерпретаторе команд bash проекта GNU. Вводя команду 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

*запрос>* **show interfaces ethernet**

В этом примере символы пробела разделяют командную строку на три компоненты: “show,” “interfaces” и “ethernet.”

Если нужно ввести строку, в которой имеется литеральный символ, 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@neo# set firewall name TEST description "external inbound"
```

В этом примере пробел внутри строки “external inbound” заключен в кавычки и потому 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@neo# show interfaces | match eth
```

В этом примере символ конвейера указывает интерпретатору команд выполнить команду **show interfaces** и затем обработать ее вывод с помощью команды **match eth**; в результате будут отображены только строки, содержащие строку “eth”. 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 (“#”).

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

Обратите внимание, что в строку в кавычках можно включить литеральный знак кавычки, поставив перед ним обратную косую черту следующим образом:

"some \"quotes\" within quotes"

Конечно, если нужна литеральная обратная косая черта, правила становятся более сложными. В качестве общего правила постарайтесь избегать использования кавычек и обратных косых черт в качестве литеральных значений в конфигурации.

### 2.1.7. Автозавершение команд

Для того чтобы система автоматически завершала синтаксис команды, следует ввести в запросе на ввод командной строки любой из следующих элементов:

*Таблица 3 - Справочные клавиши интерфейса командной строки*

| Нажатая клавиша: | Результат: |
|---|---|
| <Tab> | Автозавершение команды.<br>- Если команда однозначна, система автоматически создает следующую лексему в синтаксисе.<br>- Если возможен более чем один вариант автозавершения, система отображает список возможных последующих лексем.<br>(Обратите внимание, что пробел после команды или ключевого слова считается за лексему.)<br>При втором нажатии клавиши <Tab> отображается справка интерфейса командной строки для текущего списка лексем. |

| Нажатая клавиша: | Результат: |
|---|---|
| ? | При нажатии на клавишу с вопросительным знаком (“?”) также выполняется автозавершение команды. Для ввода литерального вопросительного знака вначале следует ввести <Ctrl>+v, потом вопросительный знак. |
| <Tab> <Alt>-? | Отображаются все доступные команды Altell NEO и предоставляется возможность автозавершения команды. |

В следующем примере осуществляется поиск всех доступных команд.

```
admin@R1:~$ <Tab>
```

В следующем примере запрашивается завершение команды для набранной строки **sho**

. В этом примере завершение команды однозначно.

```
admin@R1~$ sho<Tab>
admin@R1~$ show
```

В следующем примере запрашивается завершение команды для набранной строки **s**. В этом случае ввод может быть завершен более чем одним способом, и система выдает все допустимые варианты завершения.

```
admin@R1~$:s<Tab>
set         show        shutdown
```

Обратите внимание. что ни клавиша <Tab>, ни сочетание клавиш<Alt>+? не обеспечивают функцию справки по командам, если заключены в кавычки. При использовании внутри кавычек клавиша <Tab> создает символ табуляции, а сочетание клавиш <Alt>+? создает вопросительный знак (“?”).

### 2.1.8. Журнал команд

Интерпретатор команд системы Altell NEO поддерживает журнал команд, где во внутреннем буфере хранятся выполненные команды, которые можно выполнить повторно или исправить.

В таблице 4 показаны наиболее важные сочетания клавиш для работы с журналом команд.

*Таблица 4 - Сочетания клавиш для работы с журналом команд*

| Сочетание | Функция |
|---|---|
| <Стрелка_вверх><br><Control>-p | Переход к предыдущей команде. |
| <Стрелка_вниз><br><Control>-n | Переход к следующей команде. |

### 2.1.9. Правка команд

Интерпретатор команд системы Altell NEO поддерживает правку команд в стиле emacs. В таблице 5 приведены наиболее важные сочетания клавиш для правки.

*Таблица 5 - Сочетания клавиш для правки в командной строке*

| Сочетание | Функция |
|---|---|
| <Стрелка_влево><br><Control>-b | Перемещение назад в командной строке. |
| <Стрелка_вправо><br><Control>-f | Перемещение вперед в командной строке. |
| <Control>-a | Перемещение в начало командной строки. |
| <Control>-e | Перемещение в конец командной строки. |
| <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 вырезки. |
| <Control>-k | Удаление текста от курсора до конца строки с копированием удаленного текста в буфер вырезки. |
| <Control>-y | Вставка текста из буфера вырезки в командную строку от положения курсора. |

### 2.1.10. Отображение длинного вывода

Если отображаемые сведения слишком длинны и не помещаются на экране, на экране в месте разрыва вывода появляется отметка “More”.

В таблице 6 показаны сочетания клавиш для управления отображением сведений на экране “More”.

*Таблица 6 - Варианты отображения на экране "More"*

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

### 2.1.11. Фильтрация вывода команд

В системе Altell NEO 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 7 показаны команды конвейера, реализованные в системе Altell NEO.

*Таблица 7 - 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. |

### 2.1.12. Работа с конфигурацией

В этом разделе рассматриваются следующие вопросы:

- Вход в режим настройки и выход из него.
- Иерархия конфигурации.
- Просмотр конфигурации.
- Добавление в конфигурацию или изменение конфигурации.
- Клонирование узла конфигурации.
- Переименование узлов конфигурации.
- Удаление конфигурации.
- Фиксация изменений в конфигурации.
- Отмена изменений в конфигурации.
- Сохранение конфигурации.
- Загрузка сохраненной конфигурации.
- Начальная загрузка из сохраненной конфигурации.

#### 2.1.12.1. Вход в режим настройки и выход из него

Для входа в режим настройки служит команда **configure** в эксплуатационном режиме.

Вход в режим настройки:

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

При входе в режим настройки вид запроса на ввод команд изменяется; вот вид запроса в эксплуатационном режиме:

*пользователь*@*узел*:~$

а вот в режиме настройки:

*пользователь*@*узел*:#

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

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

#### 2.1.12.2. Иерархия конфигурации

В Altell NEO используется иерархическая система команд. Для того чтобы изменить некоторый параметр системы, необходимо задать значение для соответствующего атрибута. Конфигурация Altell NEO 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.

У *узла* конфигурации всегда есть закрытая пара фигурных скобок, содержимое которой может быть пусто, как в следующем примере:

```
ethernet eth4 {
        }
```

или непусто, как в следующем примере:

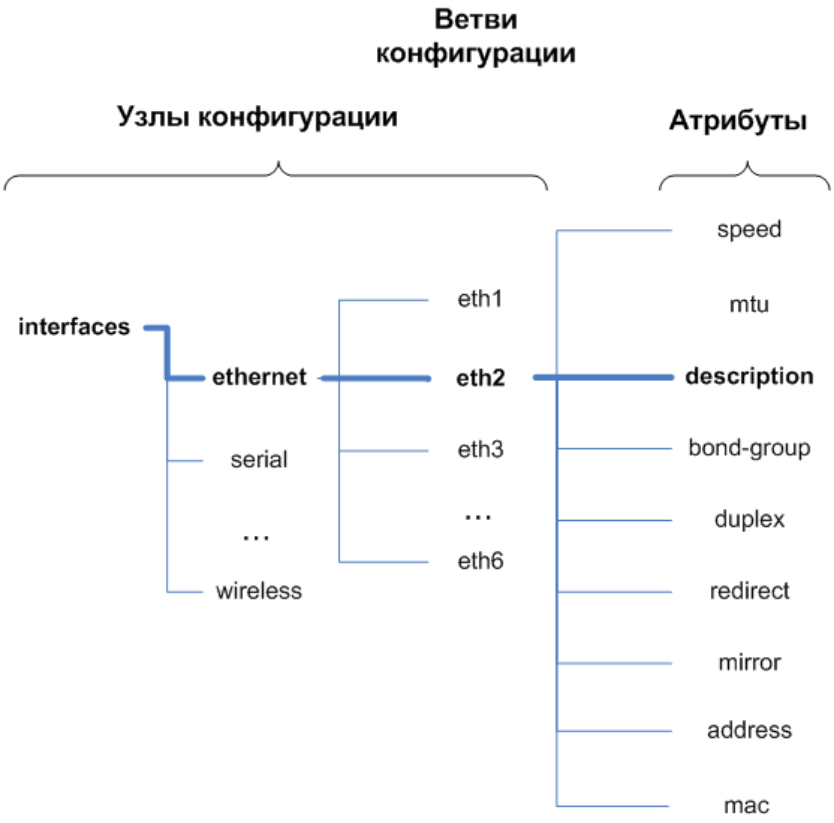
```
ssh {
        cipher gost89
        hostkey-algo ssh-gost2001
    }
```

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

```
address 192.168.1.1/24
```

Узлы конфигурации и атрибуты формируют ветви конфигурации, как показано на рис. 1.

*Рисунок 1 - Иерархия конфигурации*




Местоположение в конфигурации можно определить по запросу [edit ], зависящему от контекста. В квадратных скобках указывается текущий уровень иерархии в конфигурации.

На верхнем уровне иерархии запрос [edit] отображается следующим образом:

```
[edit]
```

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

```
[edit interfaces ethernet]
```

*Рисунок 2 - Переходы между уровнями иерархии конфигурации*


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).

Например, для того чтобы находясь на верхнем уровне иерархии указать адрес для интерфейса Ethernet eth2, необходимо ввести следующую команду:

```
admin@neo# set interfaces ethernet eth2 address 192.168.1.1/24
```

В том случае если установлен текущий уровень иерархии [edit interfaces ethernet eth2], для установки адреса необходимо ввести команду:

```
admin@neo# set address 192.168.1.1/24
```

В таблице 8 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. |

| Команда | Результат |
|---|---|
| `top` | Переход к вершине дерева конфигурации. |
| `up` | Перемещение на один узел вверх в дереве конфигурации. |

Команда **edit** позволяет переходить на интересующую пользователя часть иерархии и выполнять команды относительно местоположения. Это позволяет сократить набор в командной строке при необходимости работы на 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, там где это допускается, следует вводить их с использованием последовательности команд. Например, для того чтобы назначить несколько адресов интерфейсу Ethernet eth4:

```
admin@neo# set interfaces ethernet eth4 address 10.10.10.10/4
admin@neo# set interfaces ethernet eth4 address 10.10.20.1/4
```

Такие параметры, допускающие многократный ввод и сохранение разных значений, названы "множественными", так как в конфигурации Altell NEO они будут созданы как однотипные узлы на одном уровне иерархии, различающиеся только своими значениями.

```
admin@neo# show interfaces ethernet
...
   eth4 {
       address 10.10.10.10/4
       address 10.10.20.1/4
   }
```

### *2.1.12.3. Просмотр конфигурации*

Команда **show** в режиме настройки используется для отображения конфигурации. Можно ограничить отображение конкретным узлом, указав путь к узлу.

В приведенном ниже примере отображается конфигурация для всех настроенных интерфейсов.

```
user@host# show interfaces
     ethernet eth0 {
```

```
        address 10.1.0.62/24
    }
    ethernet eth1 {
        address 172.16.234.23/25
        vrrp {
            virtual-address 172.16.99.99
            vrrp-group 20
        }
    }
    loopback lo {
    }
}
```

В приведенном ниже примере отображается конфигурация только для интерфейса Ethernet eth0.

```
admin@R1# show interfaces ethernet eth0
 address 10.1.0.62/24
```

Если отображаемые сведения не помещаются на один экран, отображение приостанавливается по выдаче одного экрана. В этом случае:

- Для отображения следующей строки нажмите <Enter>.
- Для отображения следующего экрана нажмите <пробел>.
- Для прерывания отображения и возврата к запросу на ввод команд нажмите q.

### *2.1.12.4. Добавление в конфигурацию или изменение конфигурации*

Добавление новой конфигурации выполняется с помощью создания узла конфигурации командой **set** в режиме настройки. Изменение существующей конфигурации выполняется с помощью команды **set** в режиме настройки, как в приведенном ниже примере:

```
admin@R1# set interfaces ethernet eth2 address 192.168.1.100/24
[edit]
admin@R1#
```

Затем для просмотра изменений можно использовать команду **show**:

```
admin@R1# show interfaces ethernet eth2
+address 192.168.1.100/24
```

```
[edit]
admin@R1#
```

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**.

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

При первой загрузке системы дерево конфигурации практически пусто, за исключением нескольких автоматически настроенных узлов. Для любой функциональности, которую нужно настроить в системе, необходимо создать узел. Когда узел создается, к нему применяются все значения по умолчанию для его атрибутов.

#### *2.1.12.5. 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.

Для клонирования узла конфигурации перейдите в точку иерархии конфигурации сразу над узлом, который надо скопировать. Затем для изменения идентификатора можно использовать команду **copy**. На странице 67 приведен пример.

#### *2.1.12.6. 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 если идентификатор множественного узла неправилен, его можно изменить с помощью команды **rename**.

Для переименования узла конфигурации перейдите в точку иерархии конфигурации сразу над узлом, который надо переименовать. Затем воспользуйтесь командой **rename** для

изменения идентификатора. Пример приведен на стр. 78.

#### *2.1.12.7. Удаление конфигурации*

Для удаления атрибута или целого узла в конфигурации служит команда **delete**, как в приведенном ниже примере:

```
admin@R1# delete interfaces ethernet eth2 address 192.168.1.100/24
[edit]
```

Затем для просмотра изменений можно использовать команду **show**:

```
admin@R1# show interfaces ethernet eth2
 -address 192.168.1.100/24
 [edit]
```

Обратите внимание на знак “-” перед удаленным узлом/атрибутом. 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; их нельзя удалить. Некоторые узлы конфигурации являются обязательными, но имеют значения по умолчанию; при удалении одного из таких узлов будет восстановлено значение по умолчанию.

#### *2.1.12.8. Фиксация изменений в конфигурации*

В Altell NEO изменения в конфигурации не вступают в силу до тех пор, пока они не зафиксированы с помощью команды **commit**.

```
admin@R1# commit
[edit]
```

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:

```
admin@R1# show interfaces ethernet eth2
 -address 192.168.1.100/24
[edit]
admin@R1# commit
[edit]
```

```
admin@R1# show interfaces ethernet eth2
[edit]
```

#### 2.1.12.9. Отмена изменений в конфигурации

Выйти из режима настройки при наличии незафиксированных изменений невозможно; необходимо либо зафиксировать изменения, либо отказаться от них. Если фиксировать изменения не нужно, можно отменить их с помощью команды **exit discard**.

```
admin@R1# exit
Cannot exit: configuration modified.
Use 'exit discard' to discard the changes and exit.
[edit]
admin@R1# exit discard
admin@R1:~$
```

#### 2.1.12.10. 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**.

```
admin@R1# save
Saving configuration to '/etc/config/config.boot'... Done [edit]
admin@R1#
```

Можно сохранить конфигурацию в другом месте, указав другое имя файла.

```
admin@R1# save testconfig
Saving configuration to '/etc/config/testconfig'... Done [edit]
admin@R1#
```

Кроме того, можно сохранить файл конфигурации по пути местоположения, отличающемуся от стандартного каталога **/etc/config**, указав другой путь. Можно сохранить на жесткий диск, карту CF или накопитель для USB, включив идентификатор накопителя в путь.

Обратите внимание, что команда **save** записывает только зафиксированные изменения. При попытке записи незафиксированных изменений система выдаст предупреждение о том, что она сохраняет только зафиксированные изменения.

В таблице 9 приведен синтаксис способов указания файла для различных обстоятельств.

*Таблица 9 - 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 конфигурации **/etc/config**. |
| Сервер TFTP | Используется следующий синтаксис для имя_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 имя_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 пользователя и пароля. |
| Сервер HTTP | 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. |

Перед тем, как конфигурацию можно будет сохранить на флэш-накопитель, последний следует проинициализировать командой **flash init** в эксплуатационном режиме.

### *2.1.12.11. 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**.

```
admin@R1# load testconfig
Loading config file /etc/config/testconfig... Done
[edit]
admin@R1#
```

Загруженная конфигурация автоматически фиксируется и становится активной

конфигурацией.

#### *2.1.12.12. Начальная загрузка из сохраненной конфигурации*

Если нужно, чтобы файл был прочитан автоматически при следующем запуске системы, его необходимо сохранить с именем **config.boot** в стандартном каталоге конфигурации. По умолчанию каталогом конфигурации является **/etc/config**.

### 2.1.13. Выполнение эксплуатационной команды из режима настройки

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

```
admin@R1# run show system processes summary
20:45:46 up 1 day, 10:16, 3 users, load average: 0.00, 0.00, 0.00
[edit]
admin@R1#
```

### 2.1.14. 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@R1:~$ show configuration
 interfaces {
     ethernet eth0 {
          address 192.168.1.77/24
     }
     ethernet eth1 {
     }
     loopback lo {
     }
}
service {
     ssh {
     }
}
```

```
system {
     gateway-address 192.168.1.254
     host-name R1
     login {
          user admin {
               authentication {
               encrypted-password ****************
```

## 2.2. Основные команды интерфейса командной строки

В этом разделе приведены следующие команды.

*Таблица 10 - Основные команды интерфейса командной строки*

| 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. |
| 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. |
| `flash init` | Форматирование флэш-накопителя и подготовка его для записи файла конфигурации. |
| `show arp` | Отображение кэша ARP системы. См. стр. 114 в разделе 3. Управление системой . |
| `show configuration` | Отображение конфигурации системы из эксплуатационного режима. |

### 2.2.1. 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**

Эта 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** (см. стр. 71).

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

*Пример 2.1 - Фиксация изменений в конфигурации*

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

```
[edit]
```

### 2.2.2. configure

Вход в режим настройки.

**Синтаксис**

**configure**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта 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 2.2 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 2.2 - Вход в режим настройки*

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

### 2.2.3. 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, **name RULE-SET-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, **name RULE-SET-1**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется, чтобы создать копию, или клон, подузла конфигурации. Допустимо копирование только тех узлов, которые расположены на текущем редактируемом уровне конфигурации. Текущий уровень конфигурации отображается в квадратных скобках перед строкой-приглашением ко вводу команд, например, [edit firewall].

Чтобы упростить переход 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 (“+”); эта пометка исчезает после фиксации изменения в конфигурации.

**Примеры**

В примере 2.3 показано копирование правила межсетевого экрана.

*Пример 2.3 - Клонирование подузлов конфигурации*

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

### 2.2.4. 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**

Эта 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 (“-”); эта пометка исчезает после фиксации изменения в конфигурации.

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

**Примеры**

В примере 2.4 выполняется удаление сервера DNS из конфигурации системы.

*Пример 2.4 - Удаление конфигурации*

```
admin@neo# show system name-server <Tab>
10.0.0.30 10.0.0.31 10.0.0.32
[edit]
admin@neo# delete system name-server 10.0.0.32
[edit]
admin@neo# show system name-server <Tab>
10.0.0.30 10.0.0.31
```

```
[edit]
```

### 2.2.5. 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**

Эта команда используется для отмены всех незафиксированных изменений в конфигурации.

**Примеры**

В примере 2.5 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 2.5 - Отмена изменений в конфигурации*

```
admin@neo# show interfaces ethernet eth2
-address 192.168.1.100/24
+address 192.168.1.101/24
[edit]
admin@neo# discard
Changes have been discarded
[edit]
```

```
admin@neo# show interfaces ethernet eth2
address 192.168.1.100/24
[edit]
```

### 2.2.6. 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**

Эта 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** (см. стр. 84) и фиксируются с помощью команды **commit** (см. стр. 64).

**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 2.6 - Переходы в дереве конфигурации*

```
[edit]
admin@neo# edit system login
[edit system login]
admin@neo# show user
mike {
    authentication {
        encrypted-password
$1$hccJixQo$V6sL5hDl6CUmVZvaH1vTf0
        plaintext-password ""
    }
}
user admin {
    authentication {
        encrypted-password $1$$Ht7gBYnxI1xCdO/JOnodh.
    }
}
[edit system login]
```

## 2.2.7. 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 этой команды на подузле в дереве конфигурации происходит переход к вершине дерева конфигурации.

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

## 2.2.8. 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

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

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

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

Конфигурацию можно загрузить с жесткого диска (включая флэш-диск или накопитель для порта USB), с сервера TFTP, с сервера FTP, с сервера SCP или с сервера HTTP. Обратите внимание, что нельзя загрузить пустой файл конфигурации; в файле конфигурации должен иметься по крайней мере один узел конфигурации. Кроме того, если будет загружен недопустимый файл конфигурации, то будет выдано сообщение об ошибке.

Каталогом конфигурации по умолчанию является **/etc/config**.

В приведенной ниже таблице показан синтаксис указания файла для различных местоположений файла.

*Таблица 11 - Способы указания местоположения для файла конфигурации*

| 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*:<br>ftp://*пользователь*:*пароль*@*узел*/*файл_конфигурации*<br>где *пользователь* это имя пользователя на узле, *пароль* это пароль, связанный с именем пользователя, *узел* это имя узла или IP-адрес сервера FTP, а *файл_конфигурации* это файл конфигурации, включая путь. Если *пользователь* и *пароль* не указаны, будет выдан запрос на их ввод. |
| Сервер SCP | Используется следующий синтаксис для *имя_файла*: |

| | |
|---|---|
| | scp://*пользователь@узел/файл_конфигурации*<br>где *пользователь* это имя пользователя на узле, *узел* это имя узла или IP-адрес сервера SCP, а *файл_конфигурации* это файл конфигурации, включая путь. После того как узел будет добавлен в список известных узлов, может быть использован следующий синтаксис:<br>scp://*пользователь:пароль@узел/файл_конфигурации*,<br>где *пароль* это пароль, ассоциированный с пользователем. Если *пользователь* и *пароль* не указаны, будет выдан запрос на их ввод. |
| Сервер HTTP | Используется следующий синтаксис для *имя_файл*а:<br>http://*узел/файл_конфигурации*,<br>где *узел* это имя узла или IP-адрес сервера HTTP, а *файл_конфигурации* это файл конфигурации, включая путь. |
| Сервер TFTP | Используется следующий синтаксис для имя_файла:<br>tftp://*узел/файл_конфигурации*<br>где *узел* это имя узла или IP-адрес сервера TFTP, а *файл_конфигурации* это файл конфигурации, включая путь относительно корневого каталога TFTP. |

**Примеры**

В примере 2.7 файл конфигурации `testconfig` загружается из каталога конфигурации по умолчанию.

*Пример 2.7 - Загрузка сохраненной конфигурации из файла*

```
admin@neo# load testconfig
Loading config file /etc/config/testconfig... Done
[edit]
admin@neo#
```

## 2.2.9. 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**

Эта 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. Конфигурацию можно загрузить с жесткого диска (включая флэш-диск или накопитель для порта USB), с сервера TFTP, с сервера FTP, с сервера SCP или с сервера HTTP. Обратите внимание, что нельзя загрузить пустой файл конфигурации; в файле конфигурации должен иметься по крайней мере один узел конфигурации.

Каталогом конфигурации по умолчанию является **/etc/config**.

В приведенной ниже таблице показан синтаксис указания файла для различных местоположений файла.

*Таблица 12 - Способы указания местоположения для файла конфигурации*

| Местоположение | Способ указания |
|---|---|
| Абсолютный путь | Используется стандартный способ указания файла в UNIX. |
| Относительный | Указывается имя файла с путем относительно каталога |

| Местоположение | Способ указания |
|---|---|
| путь | конфигурации по умолчанию. |
| Сервер FTP | Используется следующий синтаксис для *имя_файла*: ftp://*пользователь*:*пароль@узел*/*файл_конфигурации* где *пользователь* это имя пользователя на узле, *пароль* это пароль, связанный с именем пользователя, *узел* это имя узла или IP-адрес сервера FTP, а *файл_конфигурации* это файл конфигурации, включая путь. Если *пользователь* и *пароль* не указаны, будет выдан запрос на их ввод. |
| 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. После того как узел будет добавлен в список известных узлов, может быть использован следующий синтаксис: scp://*пользователь:пароль@узел*/*файл_конфигурации*, где *пароль* это пароль, ассоциированный с пользователем. Если *пользователь* и *пароль* не указаны, будет выдан запрос на их ввод. |
| Сервер HTTP | Используется следующий синтаксис для имя_файла: http://*узел*/*файл_конфигурации*, где *узел* это имя узла или IP-адрес сервера HTTP, а *файл_конфигурации* это файл конфигурации, включая путь. |
| 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. |

**Примеры**

В примере 2.8 файл конфигурации testconfig загружается из каталога конфигурации по умолчанию и сливается с текущей конфигурацией.

*Пример 2.8 - Слияние с конфигурацией, считанной из файла*

```
admin@neo# merge testconfig
Loading config file /etc/config/testconfig... Done
[edit]
admin@neo#
```

## 2.2.10. rename

Изменение идентификатора именованного узла конфигурации.

**Синтаксис**

**rename** *старое_имя_узла_настр* **to** *новое_имя_узла_настр*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

Отсутствует.

**Параметры**

*старое_имя_узла_настр*

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

*новое_имя_узла_настр*

Новый идентификатор для узла конфигурации. Формат представляет собой последовательность разделенных пробелами лексем, представляющих имя параметра конфигурации и значение этого параметра; например, **name RULE-SET-1**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется в сочетании для переименования (то есть, для замены идентификатора) узла конфигурации, такого как набор правил межсетевого экрана.

Допустимо переименование только тех узлов, которые расположены на

текущем редактируемом уровне конфигурации. Текущий уровень конфигурации отображается в квадратных скобках перед строкой-приглашением ко вводу команд, например, [edit firewall].

Чтобы упростить переход на нужный уровень конфигурации, следует использовать команду **edit**. Команда **edit** используется для перехода к нужному месту в иерархии конфигурации, после чего переименовывается нужный подузел.

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

**Примеры**

В примере 2.9 переименовывается правило 10 в правило 12 в наборе правил межсетевого экрана RULE-SET -1.

*Пример 2.9 - Переименование узла конфигурации*

```
admin@neo# show firewall
name RULE-SET-1 {
   rule 10 {
      action accept
   }
}
[edit]
admin@neo# edit firewall name RULE-SET-1
[edit firewall name RULE-SET-1]
admin@neo# rename rule 10 to rule 12
[edit firewall name RULE-SET-1]
admin@neo# show
 -rule 10 {
 -
action accept
 -}
```

```
 +rule 12 {
 +   action accept
 +}
[edit firewall name RULE-SET-1]
admin@neo# commit
[edit firewall name RULE-SET-1]
admin@neo# show
 rule 12 {
     action accept
 }
[edit firewall name RULE-SET-1]
admin@neo# top
[edit]
```

### 2.2.11. 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**

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

**Примеры**

В примере 2.10 из режима настройки выполняется команда **show date**

(эксплуатационная).

*Пример 2.10 - Выполнение эксплуатационной команды из режима настройки*

```
admin@neo# run show date
 Sun Dec 16 23:34:06 GMT 2007
[edit]
admin@neo#
```

## 2.2.12. save

Сохранение работающей конфигурации в файл.

**Синтаксис**

**save** *имя_файла*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

Отсутствует.

**Параметры**

*имя_файла*

Имя файла для сохранения сведений, включая путь к файлу.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта 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** (см. стр. 74). Неабсолютный путь интерпретируется как относительный от каталога конфигурации по умолчанию, которым является **/etc/config**.

В приведенной ниже таблице показан синтаксис указания файла для различных местоположений файла.

*Таблица 13 - Способы указания местоположения для файла конфигурации*

| 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:пароль@узел/файл_конфигурации* где *пользователь* это имя пользователя на узле, *пароль* это пароль, связанный с именем пользователя, *узел* это имя узла или IP-адрес сервера FTP, а *файл_конфигурации* это файл конфигурации, включая путь. Если *пользователь* и *пароль* не указаны, будет выдан запрос на их ввод. |
| 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. После того как узел будет добавлен в список известных узлов, может быть использован следующий синтаксис: scp://*пользователь:пароль@узел*/*файл_конфигурации*, где *пароль* это пароль, ассоциированный с пользователем. Если *пользователь* и *пароль* не указаны, будет выдан запрос на их ввод. |
| 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. |

При перезаписи файла конфигурации система создает один файл резервной копии с именем *имя_файла~*. Например, если при сохранении перезаписывается файл **my-config.boot**, система переименовывает предыдущий файл в **my-config.boot~**.

Обратите внимание, что с помощью команды **save** можно записать только зафиксированные изменения. Если сделать изменения в конфигурации и

попытаться сохранить конфигурацию, система выдаст предупреждение о том, что есть незафиксированные изменения, и затем сохранит только зафиксированные изменения.

**Примеры**

В примере 2.11 выполняется сохранение работающей конфигурацией в файл **my-config** в каталоге конфигураций по умолчанию, выход из режима настройки и отображение набора файлов, хранящегося в каталоге конфигураций.

*Пример 2.11 - Сохранение конфигурации в файл*

```
admin@neo# save
 Saving configuration to '/etc/config/config.boot'...
 Done
[edit]
admin@neo# exit
admin@neo:/$ show files /etc/config
-rw-r-r-    1 root     root         1.2K Oct 20 15:28
config.boot
-rw-rw-r-    1 admin    vyattacf      947 Oct 20 15:20
config.boot.2161
-rw-rw-r-    1 admin    vyattacf      947 Oct 20 15:28
config.boot.2963
-rw-rw-r-    1 root     vyattacf      947 Oct 20 15:09
testconfig
admin@neo:~$
```

В примере 2.12 выполняется сохранение текущей работающей конфигурации в файл **my-config** в корневом каталоге сервера TFTP по адресу 10.1.0.35.

*Пример 2.12 - Сохранение конфигурации в файл на сервере TFTP*

```
admin@neo# save tftp://10.1.0.35/my-config
Saving configuration to 'tftp://10.1.0.35/my-config'...
Done
[edit]
```

```
admin@neo#
```

### 2.2.13. set

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

**Синтаксис**

Синтаксис для создания нового узла конфигурации следующий:

**set** *узел-настр* [*идентификатор*]

Синтаксис для установки атрибута внутри узла конфигурации следующий:

**set** *узел-настр* [*идентификатор*] *атрибут* [*значение*]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

Отсутствует.

**Параметры**

*узел-настр*

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**

Эта команда используется для добавления элемента конфигурации к текущей конфигурации — например, для включения протокола маршрутизации или определения интерфейса.

Кроме того, эту 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** (см. стр. 64).

После добавления узла конфигурации его можно изменять с помощью команды **set** (см. стр. 84) или удалить с помощью команды **delete** (см. стр. 68).

**Примеры**

В примере 2.13 выполняются добавление узла конфигурации для интерфейса Ethernet и фиксация изменений.

*Пример 2.13 - Добавление узла конфигурации*

```
admin@neo# set interfaces ethernet eth1 address
192.150.187.108/24
[edit]
admin@neo# commit
[edit]
```

## 2.2.14. show

Отображение сведений о конфигурации в режиме настройки.

**Синтаксис**

**show** [**-all**] *узел-настр*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

Отсутствует.

**Параметры**

*узел-настр*

Узел конфигурации, который нужно просмотреть (включая путь). Узел должен существовать, а созданный узел должен быть зафиксирован.

Указание узла интерпретируется относительно текущего положения пользователя в дереве конфигурации.

**–all**

Включение сведений по умолчанию в отображение.

**Значение по умолчанию**

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

При использовании без параметра **–all** сведения по умолчанию не отображаются.

**Указания по использованию**

Эта команда используется для отображения настроенного состояния системы в режиме настройки.

Команда отображает указанный узел конфигурации и все подузлы. Указание узла интерпретируется относительно текущего местоположения пользователя в дереве конфигурации.

Если параметр **–all** не используется, сведения по умолчанию не включается в вывод команды.

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

**Примеры**

В примере 2.14 показан узел **service**, отображенный при помощи команды **show** в режиме настройки.

*Пример 2.14 - Отображение сведений о конфигурации*

```
admin@neo# show service
dhcp-server {
}
dns {
}
```

```
ssh {
}
telnet {
}
[edit]
admin@neo#
```

## 2.2.15. show configuration

Отображение конфигурации системы из эксплуатационного режима.

**Синтаксис**

**show configuration** [**all** | **files**]

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**all**

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

**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**

Эта 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 2.15 показано отображение конфигурации из эксплуатационного режима. (Для краткости показан только первый экран сведений.)

*Пример 2.15 - Отображение сведений о конфигурации в эксплуатационном режиме*

```
admin@neo:~$ show configuration
interfaces {
     ethernet eth0 {
          address 192.168.1.77/24
     }
     ethernet eth1 {
     }
     loopback lo {
     }
}
service {
     ssh {
     }
}
system {
     gateway-address 192.168.1.254
     host-name neo
     login {
          user admin {
               authentication {
                    encrypted-password ****************
:
```

### 2.2.16. top

Перемещение на верхний уровень иерархии конфигурации.

**Синтаксис**

```
top
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

Отсутствует.

**Параметры**

Отсутствуют.

**Указания по использованию**

Эта команда используется для быстрого перехода на верхний уровень режима настройки.

**Примеры**

В примере 2.16 показан переход вниз по нескольким узлам дерева конфигурации, после чего использование команды **top** для перехода непосредственно к вершине дерева. В данном примере обратите внимание на то, как в строке **[edit]** отображается текущее положение в дереве конфигурации.

*Пример 2.16 - Переход к вершине дерева конфигурации*

```
admin@neo# edit protocols rip interface eth0
[edit protocols/rip/interface/eth0]
admin@neo# top
[edit]
admin@neo#
```

## 2.2.17. up

Перемещение на уровень вверх в дереве конфигурации.

**Синтаксис**

**up**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

Отсутствует.

**Параметры**

Отсутствует.

**Указания по использованию**

Эта команда используется для перехода на один уровень вверх в режиме

настройки.

**Примеры**

В примере 2.17 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 2.17 - Переход на уровень вверх в дереве конфигурации*

```
admin@neo# edit protocols rip interface eth0
[edit protocols/rip/interface/eth0]
admin@neo# up
[edit protocols/rip/interface]
admin@neo# up
[edit protocols/rip/]
```

# 3. УПРАВЛЕНИЕ СИСТЕМОЙ

В этом разделе описаны функции системы Altell NEO 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.

## 3.1. Основная настройка системы

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

- Настройка сведений об узле.
- Настройка DNS.
- Настройка даты и времени.
- Наблюдение за сведениями о системе.

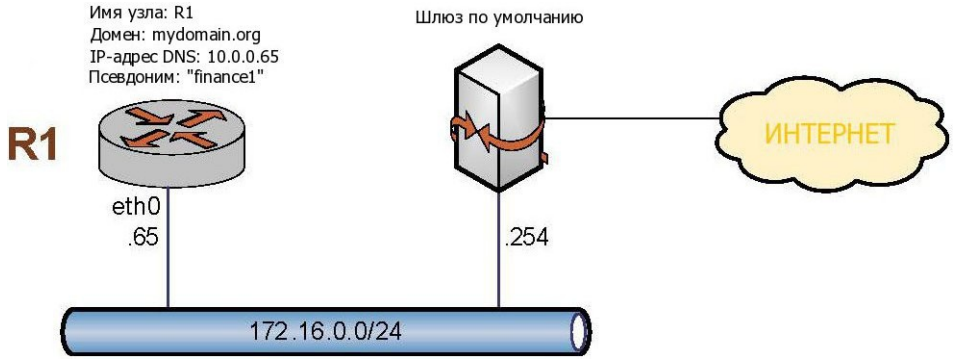
### 3.1.1. Настройка сведений об узле

В этом разделе рассматриваются следующие вопросы:

- Имя узла.
- Домен.
- IP-адрес.
- Шлюз по умолчанию.
- Псевдонимы.

В этом разделе представлены эталонные настройки для сведений об узле системы. Используемая эталонная настройка показана на рис. 3.

*Рисунок 3 - Сведения об узле*




В этом разделе есть следующие примеры:

- Пример 3.1 Установка имени узла системы.
- Пример 3.2 Установка домена системы.
- Пример 3.3 Сопоставление IP-адреса системы с ее именем узла.
- Пример 3.4 Установка шлюза по умолчанию.
- Пример 3.5 Создание псевдонима для системы.

#### *3.1.1.1. Имя узла*

Имя системы Altell NEO устанавливается с помощью команды **system host-name**. В имя системы могут входить буквы, цифры и дефисы (“-”).

В примере 3.1 показана установка имени узла системы в R1. Для установки имени узла системы нужно выполнить следующие действия в режиме настройки:

*Пример 3.1 - Установка имени узла системы*

| Действие | Команда |
|---|---|
| Установка имени узла системы. | admin@neo# **set system host-name R1** [edit] |
| Фиксация изменения. | admin@neo# **commit** [edit] |
| Вид запроса на ввод команд изменяется, отражая изменение | admin@R1# |
| Отображение настройки. | admin@R1# **show system host-name** host-name R1 [edit] |

#### *3.1.1.2. Домен*

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

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

В примере 3.2 домен системы устанавливается на **mydomain.com**. Для установки домена системы нужно выполнить следующие действия в режиме настройки:

*Пример 3.2 - Установка домена системы*

| Действие | Команда |
|---|---|
| Установка имени домена. | admin@R1# **set system domain-name mydomain.com** [edit] |
| Фиксация изменения. | admin@R1# **commit** [edit] |

| | |
|---|---|
| Отображение настройки. | admin@R1# **show system domain-name**<br>domain-name mydomain.com<br>[edit] |

### *3.1.1.3. IP-адрес*

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 10.0.0.65. Это адрес, настроенный для интерфейса-заглушки в эталонной топологии, используемой в данном руководстве.

В примере 3.3 создается статическое сопоставление между именем узла R1 и IP-адресом 10.0.0.65. Это IP-адрес, который сервер DNS будет использовать для разрешения запросов DNS к **R1.mydomain.com**.

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

*Пример 3.3 - Сопоставление IP-адреса системы с ее именем узла*

| Действие | Команда |
|---|---|
| Сопоставление имени узла R1 с IP-адресом 10.0.0.65. | admin@R1# **set system static-host-mapping host-name R1 inet 10.0.0.65**<br>[edit] |
| Фиксация изменения. | admin@R1# **commit**<br>[edit] |
| Отображение настройки. | admin@R1# **show system static-host-mapping** |

```
host-name R1 {
        inet 10.0.0.65
}
[edit]
```

#### 3.1.1.4. Шлюз по умолчанию

В примере 3.4 в качестве шлюза по умолчанию для системы указывается 172.16.0.254. Для указания шлюза по умолчанию нужно выполнить следующие действия в режиме настройки:

*Пример 3.4 - Установка шлюза по умолчанию*

| Действие | Команда |
|---|---|
| Указание шлюза по умолчанию. | admin@R1# **set system gateway-address 172.16.0.254** [edit] |
| Фиксация изменения. | admin@R1# **commit**<br>[edit] |
| Отображение настройки. | admin@R1# **show system gateway-address**<br>gateway-address 172.16.0.254<br>[edit] |

#### 3.1.1.5. Псевдонимы

Для системы можно определить один или несколько псевдонимов путем сопоставления IP-адреса системы с более чем одним именем узла. В примере 3.5 выполняется создание псевдонима **finance1** для системы. Для создания псевдонима для системы нужно выполнить следующие действия в режиме настройки:

*Пример 3.5 - Создание псевдонима для системы*

| Действие | Команда |
|---|---|
| Определение псевдонима. | admin@R1# **set system static-host-mapping host-name R1 alias** |

| | |
|---|---|
| | **finance1**<br>[edit] |
| Фиксация изменения. | admin@R1# **commit**<br>[edit] |
| Отображение настройки. | admin@R1# **show system static-host-mapping**<br>host-name R1 {<br>alias finance1<br>inet 10.0.0.65<br>}<br>[edit] |

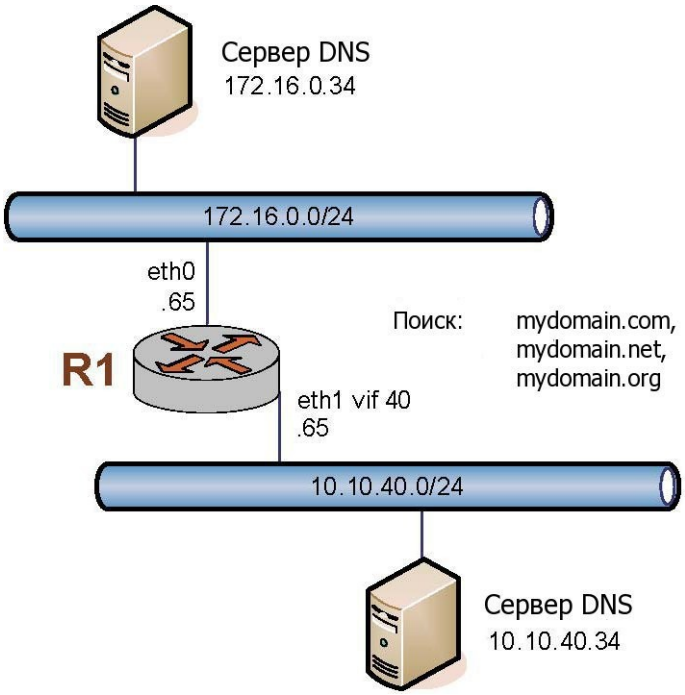
### 3.1.2. Настройка DNS

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 рис. 4.

*Рисунок 4 - Настройка DNS*




В этом разделе есть следующие примеры:

- Пример 3.6 Указание серверов имен DNS.
- Пример 3.7 Установка порядка поиска для автозавершения домена.

### *3.1.2.1. Серверы имен DNS*

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

В примере 3.6 указывается два сервера DNS для системы: один с адресом 172.16.0.34, другой с адресом 10.10.40.34.

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

*Пример 3.6 - Указание серверов имен DNS*

| Действие | Команда |
|---|---|
| Указание первого сервера DNS. | `admin@R1# set system name-server 172.16.0.34`<br>`[edit]` |

| | |
|---|---|
| Указание второго сервера DNS. | admin@R1# **set system name-server 10.10.40.34** [edit] |
| Фиксация изменения. | admin@R1# **commit**<br>[edit] |
| Отображение настройки. | admin@R1# **show system name-server**<br>name-server 172.16.0.34<br>name-server 10.10.40.34<br>[edit] |

#### *3.1.2.2. 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 domain-search**.

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

Для команды **system 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 3.7 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 3.7 - Установка порядка поиска для автозавершения домена*

| Действие | Команда |
|---|---|
| Указание первого имени домена. | admin@R1# **set system domain-search domain mydomain.com**<br>[edit] |

| | |
|---|---|
| Указание второго имени домена. | admin@R1# **set system domain-search domain mydomain.net**<br>[edit] |
| Указание третьего имени домена. | admin@R1# **set system domain-search domain mydomain.org**<br>[edit] |
| Фиксация изменения. | admin@R1# **commit**<br>[edit] |
| Отображение настройки. | admin@R1# **show system domain-search**<br> domain mydomain.com<br> domain mydomain.net<br> domain mydomain.org<br>[edit] |

### 3.1.3. Настройка даты и времени

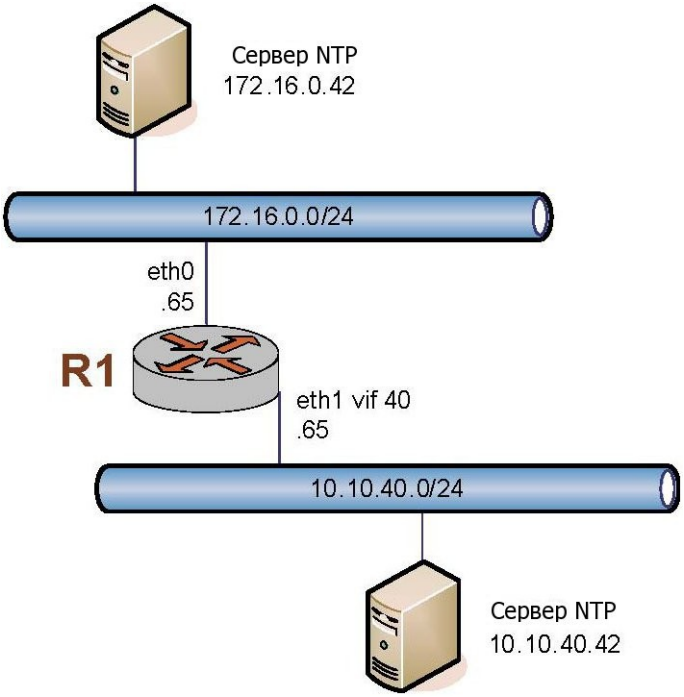
В этом разделе рассматриваются следующие вопросы:

- Установка даты.
- Синхронизация с сервером NTP вручную.
- Установка часового пояса.
- Использование NTP для автоматический синхронизации.

Дату и время можно либо установить вручную, либо получить с помощью автоматической или ручной синхронизации системы с одним или несколькими серверами протокола NTP (сетевого времени). Часовой пояс должен быть установлен вручную либо как разница с гринвичским временем (UTC), либо как номер поддерживаемого буквального часового поиска.

В этом разделе представлены эталонное настройки для сопровождения сведений о дате и времени. Используемая эталонная настройка показана на рис. 5.

*Рисунок 5 - Установка даты и времени*




В этом разделе есть следующие примеры:

- Пример 3.8 Установка даты и времени вручную.
- Пример 3.9 Синхронизация системы с сервером NTP вручную.
- Пример 3.10 Установка часового пояса как региона/местоположения.
- Пример 3.11 Использование NTP для автоматической синхронизации.

### *3.1.3.1. Установка даты*

В примере 3.8 выполняется установка даты вручную на 13:15 ровно 24 апреля 2007 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 нужно выполнить следующие действия в эксплуатационном режиме:

*Пример 3.8 - Установка даты и времени вручную*

| Действие | Команда |
|---|---|
| Указание даты. Используется формат | `admin@R1:~$` **`set date 2007.04.24-`** |

| | |
|---|---|
| *ГГГГ.ММ.ДД-чч:мм* | **13:15**<br>Tue Apr 24 13:15:00 MSD 2007<br>admin@R1:~$ |

### *3.1.3.2. Синхронизация с сервером NTP вручную*

В примере 3.9 вручную выполняется синхронизация часов системы с сервером NTP по адресу 172.16.0.42.

Следует обратить внимание, что это всего лишь выполнение одноразовой синхронизации. Постоянная связь с сервером NTP не устанавливается. Сведения об установке автоматический синхронизации приведены в разделе “Использование NTP для автоматический синхронизации ” на стр. 101.

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

*Пример 3.9 - Синхронизация системы с сервером NTP вручную*

| Действие | Команда |
|---|---|
| Указание местоположения севера NTP. | admin@R1:~$ **set date ntp 172.16.0.42**<br>Tue Apr 24 13:15:00 UTC 2007<br>admin@R1:~$ |

### *3.1.3.3. Установка часового пояса*

Часовой пояс необходимо настроить при помощи команды **system time-zone**. Для этого нужно указать регион/местоположение, которые наилучшим образом соответствуют местоположению машины. Например, если указать **US/Pacific**, будет установлен тихоокеанский часовой пояс США. 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.

В примере 3.10 выполняется установка часового пояса на тихоокеанский (США). Для установки часового пояса нужно выполнить следующие действия в режиме настройки:

*Пример 3.10 - Установка часового пояса как региона/местоположения*

| Действие | Команда |
|---|---|
| Установка часового пояса. | admin@R1# **set system time-zone US/Pacific**<br>[edit]<br>admin@R1# |
| Фиксация сведений. | admin@R1# **commit** [edit] |
| Отображение настройки. | admin@R1# **show system time-zone**<br>time-zone US/Pacific<br>[edit] |

#### *3.1.3.4. Использование NTP для автоматический синхронизации*

Для использования протокола NTP для автоматической синхронизации необходимо создать связи с серверами NTP. Для создания связи с сервером NTP используется команда **system ntp-server** с указанием IP-адреса сервера.

В примере 3.11 выполняется настройка двух серверов NTP: одного по адресу 172.16.0.42, другого по адресу 10.10.40.42.

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

*Пример 3.11 - Использование NTP для автоматической синхронизации*

| Действие | Команда |
|---|---|
| Указание сервера по адресу 172.16.0.42. | admin@R1# **set system ntp-server 172.16.0.42**<br>[edit] |
| Указание сервера по адресу 10.10.40.42. | admin@R1# **set system ntp-server 10.10.40.42**<br>[edit] |
| Фиксация сведений. | admin@R1# **commit**<br>[edit] |

Отображение настройки. (Вывод сокращен.)

```
admin@R1# show system
host-name R1
domain-search {
     domain mydomain.com
        domain mydomain.net
     domain mydomain.org
}
name-server 172.16.0.34
name-server 10.10.40.34
time-zone US/Pacific
ntp-server 172.16.0.42
ntp-server 10.10.40.42
[edit]
```

## 3.2. Наблюдение за сведениями о системе

В этом разделе рассматриваются следующие вопросы:

- Отображение сведений об узле.
- Отображение даты и времени.

В этом разделе есть следующие примеры:

- Пример 3.12 Отображение имени узла системы.
- Пример 3.13 Отображение даты и времени системы.

### 3.2.1. Отображение сведений об узле

Для просмотра настроенного имени узла используется команда **show host name** в эксплуатационном режиме, как показано в примере 3.12:

*Пример 3.12 - Отображение имени узла системы*

```
admin@R1:~$ show host name
R1
admin@R1:~$
```

### 3.2.2. Отображение даты и времени

Для просмотра времени в соответствии с системными часами используется команда **show host date** в эксплуатационном режиме, как показано в примере 3.13:

*Пример 3.13 - Отображение даты и времени системы*

```
admin@R1:~$ show host date
Tue Apr 24 22:23:07 GMT+8 2007
admin@R1:~$
```

## 3.3. Команды управления системой

В этом разделе представлены следующие команды.

*Таблица 14 - Команды управления системой*

| Команды настройки | |
|---|---|
| system domain-name <домен> | Установка домена системы. |
| system domain-search domain <домен> | Определение набора доменов для автозавершения домена. |
| system gateway-address <адрес> | Указание шлюза по умолчанию для системы. |
| system host-name <имя> | Установка имени узла для системы. |
| system name-server <адрес> | Указание серверов имен DNS, доступных системе. |
| system ntp-server <имя> | Указание серверов NTP для использования при синхронизации системных часов. |
| system options reboot-on-panic <значение> | Установка поведения системы при неисправимой ошибке. |
| system static-host-mapping host-name <имя> | Определение статического сопоставления между именем узла и IP-адресом. |
| system time-zone <пояс> | Установка часового пояса для локальных системных часов. |
| system ip arp table-size <размер> | Указание максимального количества записей, которые хранятся в кэше ARP. |

| | |
|---|---|
| `system ipv6 neighbor table-size <размер>` | Указание максимального количества записей, которые хранятся в таблице соседей IPv6. |
| Настройка параметров подключения к серверу LDAP | |
| `system ldap-server` | Настройка параметров подключения к серверу LDAP. |
| `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>` | Установить корневой объект базы поиска групп LDAP. |
| `system ldap-server host <узел>` | Указание IP-адреса или символьного имени сервера 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 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 <ethx>` | Очистка кэша ARP системы для указанного |

| | |
|---|---|
| | интерфейса. |
| `clear connnection-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 флэш-накопителя и подготовка его к записи файла настройки. |
| `reboot` | Перезагрузка системы. |
| `set date` | Установка даты и времени системы непосредственно или указание сервера NTP, с которого их следует принять. |
| `show arp` | Отображение кэша ARP системы. |
| `show date` | Отображение даты и времени системы. |
| `show files` | 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 ntp` | Отображение состояния настроенных серверов NTP. |
| `show reboot` | Отображение даты и времени следующей запланированной перезагрузки. |
| `show system boot-messages` | Отображение сообщений при загрузке, созданных |

| | |
|---|---|
| | ядром. |
| `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 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 версии системного программного обеспечения. |
| `terminal` | Контроль за поведением системного терминала. |

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

| Сходные команды, описанные в других местах | |
|---|---|
| `system login` | Команды управления пользователями описаны в разделе 4. Управление пользователями . |
| `system syslog` | Команды системной регистрации описаны в разделе 5. Регистрация . |

### 3.3.1. clear arp address <ipv4-адрес>

Очистка кэша ARP системы для указанного IP-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.

### 3.3.2. clear arp interface <ethx>

Очистка кэша ARP системы для указанного интерфейса.

**Синтаксис**

**clear arp interface** *eth0..eth23*

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*eth0..eth23*

Очистка всего кэша ARP для указанного интерфейса Ethernet. Диапазон значений от **eth0** до **eth23**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для удаления элементов ARP, связанных с интерфейсом Ethernet, из кэша ARP.

### 3.3.3. clear connnection-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.

### 3.3.4. 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.

### 3.3.5. clear interfaces counters

Очистка счетчиков интерфейсов для всех интерфейсов.

**Синтаксис**

```
clear interfaces counters
```

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для очистки счетчиков для всех интерфейсов всех типов, в том числе ADSL, мостов, Ethernet, заглушек, многоканальных, последовательных интерфейсов и туннелей. Просмотреть значения счетчиков можно при помощи команды **show interfaces counters**.

## 3.3.6. 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 Altell NEO. 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** (см. стр. 80).

**Примеры**

В примере 3.14 выполняется подготовка флэш-накопителя для записи файла настройки и запись работающей настройки в файл **/media/hdd/config/config.boot**.

*Пример 3.14 - Инициализация флэш-накопителя для записи файлов настройки*

```
admin@neo:~$ flash init

This will erase all data on /dev/sdb1.

Your configuration was saved in:
/media/hdd/config/config.boot

admin@neo:~$
```

### 3.3.7. reboot

Перезагрузка системы.

**Синтаксис**

**reboot** [**at** *время* | **cancel**]

**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:

*чч:мм*

*ДД.ММ.ГГГГ*

*“чч:мм ДД.ММ.ГГГГ”*

**midnight**

**noon**

**“now** + *x единицы*”

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.

**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. Команду могут выполнять только пользователи с полномочиями административного уровня.

**Примеры**

В примере 3.15 выполняется перезагрузка системы.

*Пример 3.15 - Перезагрузка системы*

```
admin@R1:~$ reboot
Приступить к перезагрузке? [подтвердите (y/n)]y


Broadcast message from root (ttyS0) (Wed Oct 20 13:44:28
2010):


The system is going down for reboot NOW!
```

В примере 3.16 выполняется перезагрузка системы в указанный день.

*Пример 3.16 - Перезагрузка системы в указанный день*

```
admin@R1:~$ reboot at 21.10.2010
Планируется перезагрузка на Thu Oct 21 00:00:00 2010
Запланировать перезагрузку? [подтвердите (y/n)]y
Запланирована перезагрузка на Thu Oct 21 00:00:00 2010
```

В том случае если указывается момент времени меньше текущего без указания даты, перезагрузка системы планируется в указанный момент времени следующего дня. В примере 3.17 выполняется перезагрузка системы в указанное время следующего дня.

*Пример 3.17 - Перезагрузка системы в указанное время следующего дня*

```
admin@neo:~$ show date
Thu Feb 24 15:56:03 MSK 2011
admin@neo:~$ reboot at '15:55'
Планируется перезагрузка на Fri Feb 25 15:55:00 2011
Запланировать перезагрузку? [подтвердите (y/n)]y
Запланирована перезагрузка на Fri Feb 25 15:55:00 2011
```

В примере 3.18 выполняется отмена перезагрузки, поставленной в расписание.

*Пример 3.18 - Отмена перезагрузки, поставленной в расписание*

```
admin@R1:~$ reboot cancel
Перезагрузка отменена
admin@R1:~$
```

### 3.3.8. set date

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

**Синтаксис**

**set date** {*дата_и_время* | **ntp** *сервер_ntp*}

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*дата_и_время*

Установка даты и времени непосредственно в одном из следующих форматов:

*ММ.ДД-чч:мм*

*ММ.ДД-чч:мм:сс*

*ГГГГ.ММ.ДД-чч:мм*

*ГГГГ.ММ.ДД-чч:мм:сс*

Обратите внимание, что в поле часов (*чч*) используется 24-часовая запись (например, 3:00 пополудни будет представлено числом 15 в поле часов).

*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 западноевропейское (гринвичское) время. Часовой пояс устанавливается с помощью команды **system time-zone** <*часовой_пояс*> (см. стр. 151).

**Примеры**

В примере 3.19 выполняется установка даты и времени системы на 10:55 пополудни 15 мая 2008 г. (принимается, что часовой пояс установлен на тихоокеанское побережье США, летнее время включено).

*Пример 3.19 - Установка даты и времени непосредственно*

```
admin@R1:~$ set date 2008.05.15-22:55
Thu May 15 22:55:00 PDT 2008
admin@R1:~$
```

В примере 3.20 выполняется установка даты и времени системы с использованием сервера NTP.

*Пример 3.20 - Установка даты и времени при помощи сервера NTP*

```
admin@R1:~$ set date ntp 69.59.150.135
15 May 23:00:00 ntpdate[7038]: step time server
69.59.150.135
offset 425.819267 sec
```

```
admin@R1:~$
```

### 3.3.9. show arp

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 15 показаны возможные состояния ARP.

*Таблица 15 - Состояния ARP*

| Состояние | 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 |

| Состояние | Описание |
|---|---|
| | 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 3.21 показан кэш ARP системы R1.

*Пример 3.21 - Отображение кэша ARP*

```
admin@R1:~$ show arp
Address      HWtype HWaddress         Flags Mask Iface
172.16.215.1 ether  00:12:D9:74:BE:91 C          eth0
10.1.0.1     ether  00:04:23:09:0F:79 C          eth0
admin@R1:~$
```

## 3.3.10. show date

Отображение даты и времени системы.

**Синтаксис**

**show date** [**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 3.22 показаны дата и время системы на R1.

*Пример 3.22 - Отображение даты и времени системы*

```
admin@R1:~$ show date
Tue May 20 17:27:07 PDT 2008
admin@R1:~$
```

## 3.3.11. show files

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.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для отображения сведений о файлах в указанном каталоге.

**Примеры**

В примере 3.23 показаны сведения о файлах в каталоге **/etc/config** в системе R1.

*Пример 3.23 - Отображение сведений о файлах*

```
admin@R1:~$ show files /etc/config/
total 8.0K
-rw-rw-- 1 root vyattacf  777 May 20 10:13 config.boot
-rw-r--- 1 root root      712 May 20 10:13
config.boot.2008-05-20-1713.pre-migration
admin@R1:~$
```

### 3.3.12. show hardware cpu

Отображение сведений о процессоре системы.

**Синтаксис**

```
show hardware cpu [summary]
```

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**summary**

Показать центральные процессоры в системе.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для просмотра сведений о процессоре или процессорах в аппаратной платформе системы.

**Примеры**

В примере 3.24 выводятся сведения о ЦП в системе R1.

*Пример 3.24 - Вывод сведений о ЦП*

```
admin@R1:~$ show hardware cpu
processor     : 0
vendor_id     : GenuineIntel
cpu family    : 6
model         : 15
model name    : Intel(R) Xeon(R) CPU     E5310  @ 1.60GHz
```

```
stepping        : 8
cpu MHz         : 1595.101
cache size      : 4096 KB
fdiv_bug        : no
hlt_bug         : no
f00f_bug        : no
coma_bug        : no
fpu             : yes
fpu_exception   : yes
cpuid level     : 10
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 nx constant_tsc up arch_perfmon pebs bts pni
ds_cpl ssse3 dca
bogomips        : 3213.51
clflush size    : 64
power management:
```

### 3.3.13. 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. Интерфейс DMI обеспечивает стандартную платформу для управления ресурсами машины.

**Примеры**

В примере 3.25 выводятся сведения об интерфейсе DMI в системе R1.

*Пример 3.25 - Вывод сведений об интерфейсе DMI*

```
admin@R1:~$ show hardware dmi
bios_date: 11/13/2008
bios_vendor: InventecESC
bios_version: BIOS Version: 2.03
board_asset_tag: No Asset Tag
board_name: MLB1218
board_vendor: InventecESC
board_version: A03
chassis_asset_tag: No Asset Tag
chassis_type: 23
chassis_vendor: InventecESC
chassis_version: PVT
product_name: Seabream
product_version: PVT
sys_vendor: InventecESC
admin@R1:~$
```

## 3.3.14. 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 3.26 выводятся сведения о памяти в системе R1.

*Пример 3.26 - Вывод сведений о памяти*

```
admin@R1:~$ show hardware mem
MemTotal:     515972 kB
MemFree:      341468 kB
Buffers:      28772 kB
Cached:       116712 kB
SwapCached:   0 kB
Active:       35912 kB
Inactive:     117272 kB
HighTotal:    0 kB
HighFree:     0 kB
LowTotal:     515972 kB
LowFree:      341468 kB
SwapTotal:    0 kB
SwapFree:     0 kB
Dirty:        0 kB
Writeback:    0 kB
AnonPages:    7700 kB
Mapped:       4048 kB
Slab:         14644 kB
SReclaimable: 9440 kB
SUnreclaim:   5204 kB
PageTables:   288 kB
NFS_Unstable: 0 kB
```

```
Bounce:        0 kB
CommitLimit:   257984 kB
Committed_AS: 21636 kB
VmallocTotal: 507896 kB
VmallocUsed:   3896 kB
VmallocChunk: 503932 kB
admin@R1:~$
```

### 3.3.15. 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 3.27 выводятся сведения о шине PCI в системе R1.

*Пример 3.27 - Вывод сведений о шине PCI*

```
admin@R1:~$ show hardware pci
00:00.0 Host bridge: Intel Corporation 440BX/ZX/DX -
82443BX/ZX/DX Host bridge (rev 01)
00:01.0 PCI bridge: Intel Corporation 440BX/ZX/DX
82443BX/ZX/DX AGP bridge (rev 01)
00:07.0 ISA bridge: Intel Corporation 82371AB/EB/MB PIIX4
```

```
ISA (rev 08)

00:07.1 IDE interface: Intel Corporation 82371AB/EB/MB
PIIX4 IDE (rev 01)

00:07.3 Bridge: Intel Corporation 82371AB/EB/MB PIIX4
ACPI (rev

08)00:0f.0 VGA compatible controller: VMware Inc Abstract
SVGA II Adapter

00:10.0 SCSI storage controller: LSI Logic / Symbios
Logic 53c1030 PCI-X Fusion-MPT Dual Ultra320 SCSI (rev
01)

00:11.0 Ethernet controller: Advanced Micro Devices [AMD]
79c970 [PCnet32 LANCE] (rev 10)

admin@R1:~$
```

### 3.3.16. 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 3.28 выводится журнал выполнения команд в системе R1.

*Пример 3.28 - Отображение журнала команд*

```
admin@R1:~$ show history
 1 2009-08-05T22:01:33+0000 configure
 2 2009-08-05T22:02:03+0000 commit
 3 2009-08-05T22:02:09+0000 exit
 4 2009-08-05T22:02:09+0000 exit
 5 2009-08-05T22:02:12+0000 exit
 6 2009-08-05T22:11:51+0000 show version
 7 2009-08-05T22:11:55+0000 configure
 8 2009-08-05T22:01:33+0000 configure
 9 2009-08-05T22:02:03+0000 commit
10 2009-08-05T22:02:09+0000 exit
11 2009-08-05T22:02:09+0000 exit
12 2009-08-05T22:02:12+0000 exit
13 2009-08-05T22:11:51+0000 show version
14 2009-08-05T22:11:55+0000 configure
15 2009-08-05T22:11:59+0000 show
16 2009-08-05T22:12:27+0000 show
17 2009-08-05T22:13:01+0000 set interfaces ethernet eth0
address 192.168.1.72/24
18 2009-08-05T22:13:12+0000 set service ssh
19 2009-08-05T22:13:33+0000 set system name-server
192.168.1.254
20 2009-08-05T22:13:45+0000 set system gateway-address
192.168.1.254
21 2009-08-05T22:13:58+0000 commit
22 2009-08-06T05:14:15+0000 show
```

### 3.3.17. show host

Отображение сведений об узлах, достижимых для системы.

**Синтаксис**

**show host** {**lookup** *имя_узла* | **lookup** *ipv4-адрес* | **name** | **date** | **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.

**date**

Вывод даты и времени в соответствии с системными часами.

**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 3.29 выводятся сведения об узле для R2.

*Пример 3.29 - Поиск узлов в сети*

```
admin@R1:~$ show host lookup R2
R2.altell.ru     A     10.1.0.3
admin@R1:~$
```

В примере 3.30 выводится имя, настроенное для R1.

*Пример 3.30 - Вывод имен узлов в сети*

```
admin@R1:~$ show host name
R1
admin@R1:~$
```

В примере 3.31 выводятся дата и время в соответствии с часами системы.

*Пример 3.31 - Вывод даты и времени системы*

```
admin@R1:~$ show host date
Mon Jan 21 17:28:47 PST 2008
admin@R1:~$
```

В примере 3.32 выводятся сведения об операционной системе.

*Пример 3.32 - Вывод сведений об операционной системе*

```
admin@R1:~$ show host os
Linux neo 2.6.35.6-rsbac #1 i586 GNU/Linux
admin@R1:~$
```

### 3.3.18. show interfaces

Отображение сведений о системных интерфейсах.

**Синтаксис**

**show interfaces** [**counters** | **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.

**detail**

Отображение подробных сведений обо всех интерфейсах, доступных в системе.

**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).

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 3.33 выведен первый экран результата работы команды **show interfaces system enabled.**

*Пример 3.33 - Отображение сведений об интерфейсах*

```
admin@R1:~$ show interfaces system enabled

eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
pfifo_fast qlen 100

    link/ether 00:30:48:82:e2:0c brd ff:ff:ff:ff:ff:ff

    inet 10.1.0.54/24 brd 10.1.0.255 scope global eth0

    inet6 fe80::230:48ff:fe82:e20c/64 scope link
valid_lft forever preferred_lft forever

RX: bytes  packets errors dropped overrun mcast
```

```
    348646 4144    0      0       0       0

TX: bytes  packets errors dropped carrier collisions

    168294 1594    0      0       0       0

eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
pfifo_fast qlen 10

    link/ether 00:30:48:82:e2:0d brd ff:ff:ff:ff:ff:ff

    inet 172.16.215.2/24 brd 172.16.215.255 scope global
eth1

    inet6 fe80::230:48ff:fe82:e20d/64 scope link
valid_lft forever preferred_lft forever

RX: bytes  packets errors dropped overrun mcast

    1384   11      0      0       0       0

TX: bytes  packets errors dropped carrier collisions

    1990   18      0      0       0       0

eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
qdisclines 1-23
```

### 3.3.19. show ntp

Отображение состояния настроенных серверов NTP.

**Синтаксис**

**show ntp** {*узел* | *ipv4-адрес* | **0.ru.pool.ntp.org**}

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*узел*

Вывод состояния подключения к серверу NTP с указанным именем узла.

*ipv4-адрес*

Вывод состояния подключения к серверу NTP с указанным именем ipv4-адресом.

**0.ru.pool.ntp.org**

Вывод состояния подключения к серверу NTP по умолчанию.

**Значение по умолчанию**

Отсутствует.

**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 частота опросов сервера системой с обновлением часов NTP. Звёздочка (*) после IP-адреса сервера NTP означает успешную синхронизацию с данным сервером NTP.

Подключения к серверам NTP настраиваются при помощи команды **system ntp-server** <*имя*> (см. стр. 147).

**Примеры**

В примере 3.34 выводится настроенный сервер NTP (в данном случае 69.59.150.135).

*Пример 3.34 - Вывод настроенных серверов NTP*

```
admin@R1:~$ show ntp

remote         local        st poll reach delay   offset
disp

==============================================================
==============

=69.59.150.135 192.168.1.92 3  64   1     0.04057
-0.281460

0.96825

admin@R1:~$
```

В примере 3.35 выводится сервер NTP с IP-адресом 69.59.150.135.

*Пример 3.35 - Вывод сведений о конкретном сервере NTP*

```
admin@R1:~$ show ntp 69.59.150.135

server 69.59.150.135, stratum 3, offset 46.614524, delay
0.0320722

Jan 12:20:36 ntpdate[10192]: step time server
69.59.150.135

offset 46.614524 sec

admin@R1:~$
```

## 3.3.20. 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.

**Примеры**

В примере 3.36 выводятся дата и время следующей запланированной перезагрузки.

*Пример 3.36 - Вывод следующей запланированной перезагрузки*

```
admin@R1:~$ show reboot
Запланирована перезагрузка на Thu Oct 21 10:00:00 2010
admin@R1:~$
```

В примере 3.37 выводится пустой список запланированных перезагрузок.

*Пример 3.37 - Вывод пустого списка запланированных перезагрузок*

```
admin@R1:~$ show reboot
Не обнаружено запланированных перезагрузок
admin@R1:~$
```

## 3.3.21. show system boot-messages

Отображение сообщений при загрузке, созданных ядром.

**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 3.38 выведен первый экран результатов работы команды **show system boot-messages**.

*Пример 3.38 - Отображение сообщений при загрузке*

```
admin@R1:~$ show system boot-messages

[    0.000000] Linux version 2.6.35.6-rsbac (@) (gcc
version 4.4.4 (GCC) ) #1

[    0.000000] BIOS-provided physical RAM map:

[    0.000000]  BIOS-e820: 0000000000000000 -
000000000009e800 (usable)

[    0.000000]  BIOS-e820: 000000000009e800 -
00000000000a0000 (reserved)

[    0.000000]  BIOS-e820: 00000000000f0000 -
0000000000100000 (reserved)

[    0.000000]  BIOS-e820: 0000000000100000 -
000000000f7b0000 (usable)

[    0.000000]  BIOS-e820: 000000000f7b0000 -
000000000f7b3000 (ACPI NVS)

[    0.000000]  BIOS-e820: 000000000f7b3000 -
000000000f7c0000 (ACPI data)

[    0.000000]  BIOS-e820: 00000000ffff0000 -
0000000100000000 (reserved)

[    0.000000] Notice: NX (Execute Disable) protection
missing in CPU or disabl

ed in BIOS!
```

```
[    0.000000] DMI 2.2 present.

[    0.000000] Phoenix BIOS detected: BIOS may corrupt
low RAM, working around

it.

[    0.000000] e820 update range: 0000000000000000 -
0000000000010000 (usable)

==> (reserved)

[    0.000000] e820 update range: 0000000000000000 -
0000000000001000 (usable)

==> (reserved)

[    0.000000] e820 remove range: 00000000000a0000 -
0000000000100000 (usable)

[    0.000000] last_pfn = 0xf7b0 max_arch_pfn = 0x100000

[    0.000000] initial memory mapped : 0 - 00800000

[    0.000000] init_memory_mapping: 0000000000000000-
000000000f7b0000

[    0.000000]  0000000000 - 0000400000 page 4k
```

### 3.3.22. show system connections

Отображение активных сетевых подключений в системе.

**Синтаксис**

**show system connections**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для вывода списка сетевых подключений, активных в сети в настоящее время.

**Примеры**

В примере 3.39 выведен первый экран результатов работы команды **show**

**system connections**.

*Пример 3.39 - Отображение активных подключений*

```
admin@R1:~$ show system connections
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address   Foreign Address
State
tcp   0      0      0.0.0.0:179     0.0.0.0:*
LISTEN
tcp   0      0      0.0.0.0:22      0.0.0.0:*
LISTEN
tcp   0      0      192.168.1.77:22 192.168.1.102:2449
ESTABLISHED
tcp6  0      0      :::2606         :::*
LISTEN
tcp6  0      0      :::80           :::*
LISTEN
tcp6  0      0      :::179          :::*
LISTEN
tcp6  0      0      :::22           :::*
LISTEN
udp   0      0      192.168.1.77:123 0.0.0.0:*
udp   0      0      127.0.0.1:123   0.0.0.0:*
udp   0      0      0.0.0.0:123     0.0.0.0:*
udp6  0      0      fe80::20c:29ff:fe68:123 :::*
udp6  0      0      ::1:123         :::*
udp6  0      0      :::123          :::*
raw6  0      0      :::58           :::* 7
raw6  0      0      :::89           :::* 7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags   Type   State     I-Node Path
unix  12     [ ]     DGRAM            10203  /dev/log
unix  2      [ ACC ] STREAM LISTENING 10657
```

### 3.3.23. 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 3.40 выведен первый экран результатов работы команды **show system kernel-messages**.

*Пример 3.40 - Отображение сообщений из ядра*

```
admin@R1:~$ show system kernel-messages
Linux version 2.6.35.6-rsbac (@) (gcc version 4.4.4 (GCC)
)
BIOS-e820: 0000000000000000 - 000000000009f800 (usable)
BIOS-e820: 000000000009f800 - 00000000000a0000 (reserved)
BIOS-e820: 00000000000f0000 - 0000000000100000 (reserved)
BIOS-e820: 0000000000100000 - 000000000fee0000 (usable)
BIOS-e820: 000000000fee0000 - 000000000fee3000 (ACPI NVS)
BIOS-e820: 000000000fee3000 - 000000000fef0000 (ACPI
data)
BIOS-e820: 000000000fef0000 - 000000000ff00000 (reserved)
BIOS-e820: 00000000fec00000 - 0000000100000000
(reserved)0MB HIGHMEM available.
254MB LOWMEM available.
found SMP MP-table at 000f5a20
```

```
On node 0 totalpages: 65248
  DMA zone: 4096 pages, LIFO batch:0
  DMA32 zone: 0 pages, LIFO batch:0
  Normal zone: 61152 pages, LIFO batch:15
HighMem zone: 0 pages, LIFO batch:0
DMI 2.3 present.
Intel MultiProcessor Specification v1.4
    Virtual Wire compatibility mode.
OEM ID: OEM00000 Product ID: PROD00000000 APIC at:
0xFEE00000
:
```

### 3.3.24. show system memory

Отображение использования памяти системой.

**Синтаксис**

**show system memory** [**quagga**]

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**quagga**

Отображение использования памяти подсистемой Quagga.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для вывода количества памяти, используемой в данный момент системой, и количества свободной памяти.

**Примеры**

В примере 3.41 выводятся сведения об использовании памяти в системе R1.

*Пример 3.41 - Отображение сведений об использовании памяти*

```
admin@R1:~$ show system memory
        total   used   free shared buffers cached
```

```
Mem:   515484 286708 228776      0   48224 197228
Swap:       0      0      0
Total: 515484 286708 228776
admin@R1:~$
```

## 3.3.25. 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 3.42 выведен первый экран результатов работы команды **show system processes**.

*Пример 3.42 - Отображение сведений о процессах*

```
admin@R1:~$ show system processes
PID TTY      STAT     TIME     COMMAND
    1 ?      S        0:01     init [2]
    2 ?      SN       0:00     [ksoftirqd/0]
    3 ?      S<       0:00     [events/0]
    4 ?      S<       0:00     [khelper]
    5 ?      S<       0:00     [kthread]
    7 ?      S<       0:00     [kblockd/0]
```

```
   10 ?        S<      0:00    [khubd]
   68 ?        S       0:00    [pdflush]
   69 ?        S       0:00    [pdflush]
   71 ?        S<      0:00    [aio/0]
   70 ?        S       0:00    [kswapd0]
  656 ?        S<      0:00    [kseriod]
 1481 ?        S<      0:00    [ata/0]
 1484 ?        S<      0:00    [scsi_eh_0]
 1486 ?        S<      0:00    [scsi_eh_1]
 1723 ?        S       0:05    [kjournald]
 1877 ?        S<s     0:00    udevd -daemon
 2548 ?        S<      0:00    [kpsmoused]
 3141 ?        Rs      0:00    /sbin/syslogd
 3147 ?        Ss      0:00    /sbin/klogd -x
 3190 ?        Ss      0:00    /usr/sbin/cron
:
```

### 3.3.26. 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 3.43 выведены результаты работы команды **show system routing-daemons**.

*Пример 3.43 - Отображение списка активных служб маршрутизации*

```
admin@R1:~$ show system routing-daemons
zebra ripd ripngd ospfd ospf6d bgpd
```

## 3.3.27. 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 3.44 выводятся сведения об использовании места файловой системой на R1.

*Пример 3.44 - Отображение сведений о файловой системе и накопителях*

```
admin@R1:~$ show system storage
Filesystem    Size Used Avail Use% Mounted on
/dev/sda2     3.5G    241.9M      3.1G   7% /
none          64.0K     52.0K     12.0K  81% /dev
tmpfs         64.0K     52.0K     12.0K  81% /dev
tmpfs         121.0M         0    121.0M   0% /dev/shm
tmpfs         121.0M    136.0K    120.8M   0%
```

```
/var/volatile
admin@R1:~$
```

## 3.3.28. 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 3.45 выводятся сведения об использовании системы для R1.

*Пример 3.45 - Отображение сведений об использовании системы и пользователях*

```
admin@R1:~$ show system uptime
20:45:59 up 3:04, 2 users, load average: 0.00, 0.00, 0.00
admin@R1:~$
```

## 3.3.29. 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 3.46 выводятся сведения об устройствах, подключенных к системе R1 по шине USB.

*Пример 3.46 - Отображение сведений о периферийных устройствах на шине USB*

```
admin@R1:~$ show system usb
Bus 001 Device 002: ID 0d49:7212 Maxtor
Bus 001 Device 001: ID 1d6b:0001 Linux Foundation 1.1
root hub
admin@R1:~$
```

## 3.3.30. show tech-support

Консолидированный отчет по сведениям о системе.

**Синтаксис**

**show tech-support** [**save** [*имя_файла*]]

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**save**

Сохранение сведений о поддержке в файл в каталоге **/etc/config/support**. Имя файла имеет формат *имя_узла*.**tech-support**.*отметка_времени*, где *имя_узла* это имя узла, настроенное для данной машины, а *отметка_времени* это время сохранения файла в формате *ГГГГ-ММ-ДД-ччммсс*.

Для ограничения числа выходных файлов до 10 используется механизм циклического замещения, то есть при создании одиннадцатого файла наиболее старый файл удаляется.

*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 Altell NEO при подаче заявки.

**Примеры**

В примере 3.47 выводится первый экран технического отчета.

*Пример 3.47 - Отображение консолидированных сведений о системе*

```
admin@R1:~$ show tech-support

--------
Show Tech-Support
--------

--------
CONFIGURATION
--------

--------
NEO version
```

```
--------
Altell NEO 1.5, revision 00:00:00:00:00:00


--------
Configuration File
--------
  interfaces {
      ethernet eth0 {
          address 192.168.200.1/24
          duplex auto
          speed auto
      }
      ethernet eth1 {
          address dhcp
          duplex auto
          speed auto
```

### 3.3.31. show version

Отображение сведений о версии системного программного обеспечения.

**Синтаксис**

**show version [ quagga ]**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

quagga

Отображение версии кода **quagga**, используемого в системе.

**Примеры**

В примере 3.48 показан образец вывода команды **show version** без параметра.

*Пример 3.48 - Отображение сведений о версии*

```
admin@neo:~$ show version
```

```
Altell NEO 1.5, revision 00:00:00:00:00:00
admin@neo:~$
```

В примере 3.49 показан образец вывода команды **show version quagga**.

*Пример 3.49 - Отображение сведений о версии кода quagga*

```
admin@neo:~$ show version quagga
Quagga 0.99.17 ().
Copyright 1996-2005 Kunihiro Ishiguro, et al.
admin@neo:~$
```

### 3.3.32. system domain-name <домен>

Установка домена системы.

**Синтаксис**

**set system domain-name** *домен*

**delete system domain-name**

**show system domain-name**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
    domain-name текст
}
```

**Параметры**

*домен*

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

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для установки домена системы.

Обратите внимание, что **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.

### 3.3.33. system domain-search domain <домен>

Определение набора доменов для автозавершения домена.

#### Синтаксис

**set system domain-search domain** *домен*

**delete system domain-search domain** *домен*

**show system domain-search domain**

#### Режим интерфейса

Режим настройки.

#### Ветвь конфигурации

```
system {
     domain-search {
          domain текст
     }
}
```

#### 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, altell.ru. Разрешены буквы, цифры, дефисы (“-”) и одна точка (“.”).

Можно указать до 6 доменов, создав до 6 множественных 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.

Обратите внимание, что **domain-name** и **domain-search** не могут быть настроены одновременно - они являются взаимоисключающими.

Форма **set** этой команды используется для добавлению 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.

## 3.3.34. system gateway-address <адрес>

Указание шлюза по умолчанию для системы.

**Синтаксис**

**set system gateway-address** *ipv4-адрес*

**delete system gateway-address**

**show system gateway-address**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
        gateway-address ipv4-адрес
}
```

**Параметры**

*ipv4-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.

## 3.3.35. 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 текст
}
```

**Параметры**

*имя*

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

Значение по умолчанию “neo”. При удалении имени узла или при попытке удаления узла конфигурации **system** имя узла возвращается к значению по умолчанию.

**Значение по умолчанию**

По умолчанию имя узла предварительно настроено как “neo”. 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 (“neo”).

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

## 3.3.36. system name-server <адрес>

Указание серверов имен DNS, доступных для системы.

**Синтаксис**

**set system name-server** *адрес*

**delete system name-server** *адрес*

**show system name-server**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
```

```
        name-server ipv4-адрес {
        }
    }
```

**Параметры**

*ipv4-адрес*

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

Можно указать несколько серверов имен DNS, создав несколько экземпляров узла конфигурации **name-server**.

**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.

## 3.3.37. system ntp-server <имя>

Указание серверов NTP для использования при синхронизации системных часов.

**Синтаксис**

**set system ntp-server** *сервер*

**delete system ntp-server** *сервер*

**show system ntp-server**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
```

```
            ntp-server [ipv4-адрес|текст] {
        }
    }
```

**Параметры**

*сервер*

Множественный узел. IP-адрес или имя узла сервера NTP. Система автоматически получит дату и время системы с указанного сервера (или 4серверов).

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

**Значение по умолчанию**

По умолчанию система использует сервер NTP по адресу **0.ru.pool.ntp.org**.

**Указания по использованию**

Эта команда используется для указания серверов NTP для данной системы.

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

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

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

## 3.3.38. system options reboot-on-panic <значение>

Установка поведения системы в случае неисправимой ошибки.

**Синтаксис**

**set system options reboot-on-panic** *значение*

**delete system options reboot-on-panic**

**show system options reboot-on-panic**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
```

```
            options {
                reboot-on-panic [true|false]
        }
    }
```

**Параметры**

*значение*

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**

Значение по умолчанию **true**.

**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.

## 3.3.39. 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 текст {
                inet ipv4-адрес
                alias текст {
                }
            }
        }
}
```

**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 интерфейса, статически сопоставляемого с именем узла.

*псевдоним*

Необязательный. Множественный узел. Псевдоним для интерфейса. 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. Обратите внимание, что **set** нельзя использовать для изменения имени узла. Для замены имени узла следует удалить элемент сопоставления и создать новый с правильным именем узла.

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

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

## 3.3.40. system time-zone <пояс>

Установка часового пояса для локальных часов системы.

**Синтаксис**

```
set system time-zone пояс
delete system time-zone
show system time-zone
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
        time-zone текст
}
```

**Параметры**

*пояс*

Строка, обозначающая часовой пояс.

Ее формат *регион/местоположение*. Например, US/Pacific. 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. 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 часового пояса в первый раз или для изменения установленного часового пояса.

Форма **delete** этой команды используется для удаления установленного часового пояса. В результате восстанавливается часовой пояс по умолчанию (Europe/Moscow).

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

## 3.3.41. 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 [1024|2048|4096|8192|16384]
        }
}
```

**Параметры**

*размер*

Максимальное количество записей, которые хранятся в кэше ARP. Допустимые значения: 1024, 204, 4096, 8192, 16384.

**Значение по умолчанию**

Значение по умолчанию 1024.

**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.

## 3.3.42. 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 ipv6 neighbor table-size**

**show ipv6 neighbor table-size**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
```

```
        ipv6{
            neighbor {
                table-size [1024|2048|4096|8192|16384]
        }
    }
```

**Параметры**

*размер*

Максимальное количество записей, которые хранятся в в таблице соседей IPv6. Допустимые значения: 1024, 204, 4096, 8192, 16384.

**Значение по умолчанию**

Значение по умолчанию 1024.

**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.

## 3.3.43. 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 текст
    }
}
```

**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.

## 3.3.44. 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 текст
        }
}
```

**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.

## 3.3.45. system ldap-server host <узел>

Указать IP-адрес или символьное имя 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 текст
        }
}
```

**Параметры**

*узел*

Обязательный. IPv4-адрес или символьное имя сервера LDAP, к которому будет осуществляться подключение.

**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.

## 3.3.46. system ldap-server nettimeout <время>

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

**Синтаксис**

**set system ldap-server** *время*

**delete system ldap-server**

**show system ldap-server**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
        ldap-server
```

```
            nettimeout целоебеззнака32
    }
```

**Параметры**

*время*

Максимальный интервал времени ожидания, в секундах, для всех сетевых взаимодействий с сервером LDAP.

**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.

## 3.3.47. 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 текст
        }
}
```

**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.

## 3.3.48. 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 целоебеззнака32разр
        }
}
```

**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.

## 3.3.49. 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 целоебеззнака32разр
    }
}
```

**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.

## 3.3.50. system ldap-server tls <режим>

Использовать режим TLS для подключения к серверу LDAP.

**Синтаксис**

```
set system ldap-server tls [enable|disable]
delete system ldap-server
show system ldap-server
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
        ldap-server
        tls [enable|disable]
}
```

**Параметры**

*режим*

Режим 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 TLS.

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

LDAPS. При этом согласование протокола SSL/TLS выполняется до того, как происходит обмен трафика LDAP.

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.

## 3.3.51. 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**

**show system ldap-server**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
        ldap-server {
            userbasedn текст
        }
}
```

**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.

## 3.3.52. terminal

Контроль за поведением системного терминала.

**Синтаксис**

**terminal {key query-help {enable|disable} | length** *длина* **| pager [***просмотр_стран***] | width** *ширина***}**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**key query-help**

Установка возможности использования вопросительного знака для получения справки. Варианты - **enable** и **disable.** Вариант по умолчанию **enable**.

*длина*

Установка длины экрана терминала в строках.

*просмотр_стран*

Программа, используемая для постраничного просмотра на терминале. Если программа не указана, используется программа по умолчанию (less).

*ширина*

Установка ширины экрана терминала на данное число колонок.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта программа используется для установки поведения терминала.

# 4. УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

В этом разделе описана настройка пользователей и аутентификация пользователей. В этом разделе рассматриваются следующие вопросы:

- Настройка управления пользователями.
- Команды управления пользователями.

## 4.1. 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.

### 4.1.1. Обзор управления пользователями

Системой Altell NEO поддерживается следующее:

- Управление учетными записями пользователей, основанное на ролях, через локальную базу данных (аутентификация при входе в систему).
- Доступ по SSH с использованием общих открытых ключей для аутентификации.

#### *4.1.1.1. 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**.

Можно изменить информацию учетной записи пользователя, используя низкоуровневые команды операционной системы, но изменения, сделанные таким образом, не сохраняются при перезагрузках. Для внесения постоянных изменений в учетные сведения пользователей следует использовать интерфейс командной строки Altell NEO.

Следует обратить внимание, что в системе Altell NEO команда Linux **passwd** может быть использована только пользователями с административными полномочиями.

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.

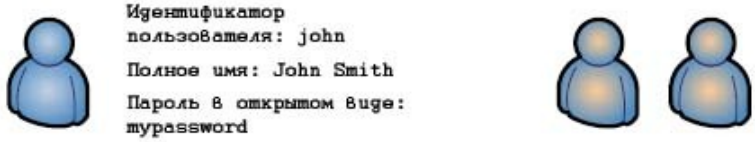
#### *4.1.1.2. Доступ по SSH с помощью общих открытых ключей*

Удаленный доступ к операционной системе Altell NEO, как правило, устанавливается через SSH. SSH позволяет обеспечить защищенный сеанс, однако использовании SSH существует одна потенциальная проблема, которая заключается в том, что если для проверки подлинности используется пароль, 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** (см. стр. 171). Кроме того, в настройке системы Altell NEO 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.

### 4.1.2. 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 рис. 6.

*Рисунок 6 - Учетная запись пользователя для входа в систему*



В этом разделе имеется следующий пример:

- Пример 4.1 Создание пользовательской учетной записи для входа в систему.

В примере 4.1 выполняется создание пользовательской учетной записи для **John Smith**. John имеет пользовательский идентификатор **john** и будет использовать пароль **mypassword**. Следует обратить внимание, что после фиксации настройки при ее выводе будет отображаться только зашифрованная версия пароля.

> ***ПРИМЕЧАНИЕ*** *Пользовательская информация может быть изменена из командной строки UNIX (при наличии достаточных полномочий). Однако любые изменения, внесенные в учетные записи или аутентификацию пользователей маршрутизатора Altell NEO через командную строку UNIX, будут перезаписаны при следующей фиксации настройки маршрутизатора под управлением Altell NEO из интерфейса командной строки.*

Для создания учетной записи пользователя, предназначенной для входа в систему, выполните следующие действие в режиме настройки:

*Пример 4.1 - Создание учетной записи пользователя для входа в систему*

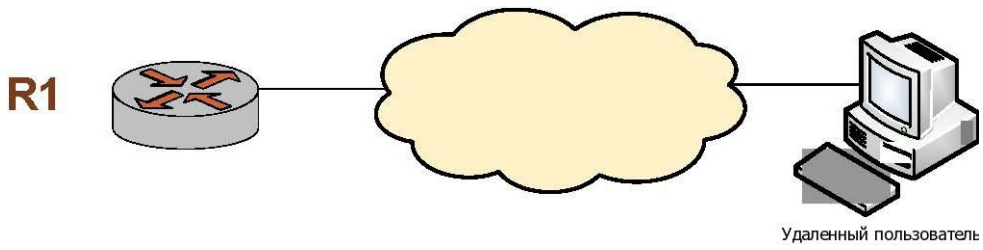
| Действие | Команда |
|---|---|
| Создание узла конфигурации **user**, указание идентификатора пользователя и его полного имени. | admin@R1# **set system login user john full-name "John Smith"**<br>[edit] |
| Указание пароля пользователя открытым текстом. | admin@R1# **set system login user john authentication plaintext-password mypassword**<br>[edit] |
| Фиксация изменения. После фиксации пароля он может быть отображен только в зашифрованной форме как значение атрибута **encrypted-password**. | admin@R1# **commit**<br>[edit] |
| Отображение содержимого узла конфигурации **system login**. | admin@R1# **show system login**<br>user admin { |

| Действие | Команда |
| --- | --- |
| | authentication {<br>encrypted-password $1$<br>$ZbzUPUD24iyfRwCKIT16q0<br>}<br>}<br>user john {<br>authentication<br>encrypted-password $1$<br>$Ht7gBYnxI1xCdO/JOnodh.<br>plaintext-password ""<br>}<br>full-name "John Smith"<br>} |

### 4.1.3. 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 Altell NEO 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 **assh-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 4.2 - 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**. | admin@R1# **loadkey john scp://j2@xyz.abc.com/home/j2/.ssh/xxx.pub**<br>Enter host password for user 'j2':<br>################################<br>## 100.0% Done<br>[edit] |
| Фиксация изменения. | admin@R1# **commit**<br>[edit] |
| 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. | admin@R1# **set service ssh disable-password-authentication**<br>[edit] |
| Фиксация изменения. | admin@R1# **commit**<br>[edit] |
| Отображение изменения. | admin@R1# **show service ssh**<br>disable-password-authentication |

```
[edit]
```

Сохранение настройки для сохранения состояния изменений после перезагрузки.

```
admin@R1# save
Saving configuration to
'/etc/config/config.boot'...
Done
[edit]
```

Отображение изменения.

```
admin@R1# show system login
     user admin {
          authentication {
               encrypted-password
$1$$ZbzUPUD24iyfRwCKIT16q0
     }
}
user john {
     authentication
          encrypted-password $1$
$Ht7gBYnxI1xCdO/JOnodh.
          plaintext-password ""
          public-keys
j2@xyz.abc.com {
               key
AAAAB3NzaC1yc2EAAAABIwAAAIEAqaCtQ
r8hr6iUEvvQD3hGyryR5k+/UjFRFrHbqH
NhjxdlYviXveVXoZrKAKHtANRp5
E+j4WZMbSd4oYt9P9lFevyZv3xmdZE+uk
uPlQBBAUnL29k1FtJ+G7I5tXGun9VR07J
zUpEb8/KP1U4ajYClc3HxpOLpu5AU5u7j
vKu/wA0=
               type ssh-rsa
          }
     }
```

```
            full-name "John Smith"
        }
```

## 4.2. Команды управления пользователями

Команды управления пользователями приведены в таблице 16.

*Таблица 16 - 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 <заставка>` | Указание заставки для отображения после входа в систему. |
| `system login banner pre-login <заставка>` | Указание заставки для отображения перед входом в систему. |
| `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> full-name <имя>` | Запись полного имени пользователя. |
| `system login user <пользователь> group <группа>` | Внесение пользователя в группу. |
| `system login user` | Указание домашнего каталога для пользователя. |

| | |
|---|---|
| `<пользователь> home-directory <каталог>` | |
| `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 users` | Вывод списка пользователей, в настоящее время вошедших в систему. |

### 4.2.1. 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 Altell NEO.

*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 **assh-keygen** и имеют имена с расширением .**pub**. В них содержатся тип аутентификации (например, **ssh-gost2001**), строка значения ключа и идентификатор пользователя удаленной системы (например, **vasya@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 на стр. 179). 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 17 - Способы указания местоположения для файла общего открытого ключа*

| Местоположение | Способ указания |
|---|---|
| Путь в локальной системе | Может быть указан абсолютный или относительный путь. Используется стандартный способ указания файла в UNIX. |
| Сервер FTP | Используется следующий синтаксис для параметра *имя_файла*: **ftp**://*пользователь:пароль@узел/файл_ключа* где *пользователь* это имя пользователя на узле, *пароль* это пароль, связанный с именем пользователя, *узел* это имя узла или IP-адрес сервера FTP, а *файл_ключа* это файл ключа, включая путь. Если *пользователь* и *пароль* не указаны, будет выдан запрос на их ввод. |
| 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 |

| Местоположение | Способ указания |
|---|---|
| | путь. После того как узел будет добавлен в список известных узлов, может быть использован следующий синтаксис: scp://*пользователь:пароль@узел/файл_конфигурации*, где *пароль* это пароль, ассоциированный с пользователем. Если *пользователь* и *пароль* не указаны, будет выдан запрос на их ввод. |
| 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. |

### 4.2.2. system login

Создание узла конфигурации для управления пользователями и проверки их подлинности.

**Синтаксис**

```
set system login
delete system login
show 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 **delete** этой команды используется для восстановления сведений по умолчанию о пользователях и аутентификации пользователей.

Форма **show** этой команды используется для просмотра сведений о пользователях, а также об аутентификации пользователей.

### 4.2.3. system login banner post-login <заставка>

Указание заставки для отображения после входа в систему.

**Синтаксис**

**set system login banner post-login** *заставка*

**delete system login banner post-login**

**show system login banner post-login**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
    login {
        banner {
            post-login текст
        }
    }
```

```
}
```

**Параметры**

*заставка*

Заставка для отображения после ввода пользователем допустимого пароля при входе 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 заставки для отображения после входа в систему.

Форма **delete** этой команды используется для возврата к заставке по умолчанию после входа в систему.

Форма **show** этой команды используется для просмотра настройки заставки для отображения после входа в систему.

### 4.2.4. system login banner pre-login <заставка>

Указание заставки для отображения перед входом в систему.

**Синтаксис**

**set system login banner pre-login** *заставка*

**delete system login banner pre-login**

**show system login banner pre-login**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
    login {
        banner {
            pre-login текст
```

```
            }
        }
    }
```

**Параметры**

*заставка*

Заставка для отображения при входе в систему перед вводом пользователем имени. 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.

Форма **set** этой команды используется для указания заставки для отображения перед входом в систему.

Форма **delete** этой команды используется для возврата к заставке по умолчанию после входа в систему.

Форма **show** этой команды используется для просмотра настройки заставки для отображения перед входом в систему.

### 4.2.5. 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 текст {
                }
            }
        }
```

**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.

Следует обратить внимание на то, что хотя сведения о пользователе и аутентификации могут быть изменены с помощью интерпретатора команд операционной системы, система перезапишет эти изменения при следующей фиксации настройки в интерпретаторе команд Altell NEO. Если нужно сделать сохраняющиеся изменения в сведениях о пользователях или об аутентификации, следует использовать команды интерфейса командной строки Altell NEO.

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 используемую пользователем в текущий момент учетную запись он удалить не может.

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

### 4.2.6. 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 текст {
            authentication {
                encrypted-password текст
                plaintext-password текст
            }
        }
    }
}
```

**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 “$”, он должен быть заключен в одинарные кавычки, например, '564$jhgJ4'.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для установки пароля для проверки подлинности пользователя. Пароли автоматически шифруются системой при помощи шифра MD5. Зашифрованная версия сохраняется внутри системы и используется при необходимости. При отображении выводится зашифрованное значение. Открытый пароль выводится в виде двойных кавычек в настройке.

Требования к паролям:

- Пароль не должен основываться на словарном слове.
- Пароль должен содержать как минимум 8 символов.
- Пароль должен содержать хотя бы одну цифру.
- Пароль должен содержать хотя бы одну заглавную букву.
- Пароль должен содержать хотя бы одну строчную букву.

Поведение системы при регистрации пользователя:

- После каждой из первых трех ошибок происходит задержка на 3 секунды.
- После трех подряд ошибок происходит блокировка на 10 минут.

При блокировке пользователь может пытаться зарегистрироваться, но даже при вводе правильного пароля попытка будет не успешной.

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.

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

## 4.2.7. 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 текст {
               authentication {
                    public-keys текст {
                         key текст
                         type [ssh-gost2001 | ssh-dss |
ssh-rsa]
                    }
               }
          }
     }
}
```

**Параметры**

*пользователь*

Идентификатор пользователя.

ид_ключа

Идентификатор ключа. Обычно он имеет вид *пользователь@узел* и создается при использовании команды **assh-keygen** для создания пары открытого и закрытого ключей.

*значение_ключа*

Строка общего открытого ключа.

*тип_ключа*

Тип используемой проверки подлинности. Этот параметр должен быть указан обязательно. Поддерживаются следующие значения:

**ssh-gost2001:** использовать аутентификацию по алгоритму ГОСТ Р 34.10-2001.

**ssh-dss:** использовать аутентификацию на основе стандарта DSS.

**ssh-rsa:** использовать аутентификацию по алгоритму RSA.

**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. Все изменения, сделанные пользователем напрямую в этом файле, будут потеряны.

Рекомендуется не изменять эти параметры непосредственно с помощью формы **set** данной команды, а использовать команду **loadkey** (см. стр. 171). Эта команда заполнит аргументы **key-id**, **key-value**, **key-options** и **key-type** для указанного пользователя по файлу открытого ключа, созданному командой Linux **assh-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. Процедура отключения проверки подлинности по паролю для SSH описана в разделе 20.2.3. service ssh disable-password-authentication .

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.

### 4.2.8. 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 текст {
               full-name текст
          }
     }
}
```

**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.

### 4.2.9. 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 текст {
               group текст
          }
     }
}
```

**Параметры**

*пользователь*

Идентификатор пользователя.

*группа*

Строка, представляющая группу, 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.

### 4.2.10. system login user <пользователь> home-directory <каталог>

Указание домашнего каталога для пользователя.

**Синтаксис**

**set system login user user home-directory** *каталог*

**delete system login user user home-directory**

**show system login user user home-directory**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
     login {
          user текст {
               home-directory текст
          }
     }
}
```

**Параметры**

*пользователь*

Идентификатор пользователя.

*каталог*

Строка, представляющая домашний каталог пользователя, например /home/admin.

**Значение по умолчанию**

Домашний каталог /**home**/<*пользователь*>.

**Указания по использованию**

Эта команда используется для указания домашнего каталога пользователя.

Форма **set** этой команды используется для указания домашнего каталога пользователя.

Форма **delete** этой команды используется для восстановления домашнего каталога по умолчанию для пользователя.

Форма **show** этой команды используется для просмотра домашнего каталога пользователя.

## 4.2.11. 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 текст {
               level [admin | operator]
          }
     }
}
```

**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 Altell NEO или в нижележащей операционной системе.

**operator**: Назначение пользователю ограниченных полномочий. Пользователь может выполнять эксплуатационные команды в интерфейсе командной строки Altell NEO, а также ограниченные формы команд **ping** и **traceroute**. 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 Altell NEO командам и ко всем командам операционной системы. Доступ к командам операционной системы является прямым: пользователю не надо выходить в другой режим интерпретатора команд перед выполнением этих команд. Хотя у административных пользователей есть возможность выполнить любую команду, реализованную в системе, в автозавершении команд и в справке интерфейса командной строки отображаются только команды Altell NEO.

**Пользователь-оператор**. Пользователи, которым назначена роль оператора, имеют доступ к набору эксплуатационных команд Altell NEO, но не имеют доступа к командам настройки. Кроме того, у них есть ограниченный доступ к командам операционной системы. В настоящее время для пользователей с ролью оператора в автозавершении команд и в справке интерфейса командной строки отображаются все команды Altell NEO.

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.

## 4.2.12. show system login users

Отображение учетных сведений о пользователях.

**Синтаксис**

```
show system login users [all|locked|other|neo]
```

**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.

**neo**

Отображение сведений об учетных записях Altell NEO.

**Значение по умолчанию**

Отображение сведений об учетных записях Altell NEO.

**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 4.3 выводятся сведения об учетных записях пользователей Altell NEO на R1.

*Пример 4.3 - Отображение сведений об учетных записях пользователей*

```
admin@R1:~$ show system login users
Username Type   Tty   From          Last login
dave     neo                        never logged in
```

```
test     neo    pts/0 192.168.1.10  Wed Mar 3 04:49:02
2010  admin@R1:~$
```

### 4.2.13. 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 4.4 выводятся сведения о пользователях, в настоящий момент вошедших в систему R1.

*Пример 4.4 - Отображение сведений о пользователях, вошедших в систему в данный момент*

```
admin@R1:~$ show users
USER       TTY      IDLE      TIME            HOST
admin      pts/0    00:00     Oct 20 16:00:57
192.168.200.2
admin@R1:~$
```

# 5. РЕГИСТРАЦИЯ

В этом разделе описан механизм регистрации (записи в журнал) событий в Altell NEO. Рассматриваются следующие вопросы:

- Настройка регистрации.
- Команды регистрации.

## 5.1. Настройка регистрации

В этом разделе рассматриваются следующие вопросы:

- Обзор регистрации.
- Пример настройки регистрации.
- Включение и отключение регистрации для конкретных функций.

### 5.1.1. Обзор регистрации

Важные события в системе записываются в сообщения журнала (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 системы Altell NEO используется процесс UNIX **syslog-ng**. Настройка регистрации, выполненная из интерфейса командной строки системы, сохраняется в файле **/etc/syslog-ng/neo.conf**.

По умолчанию локальная регистрация включена, а сообщения сохраняются в базе данных **/var/log/system.db**.

#### *5.1.1.1. Типы источников сообщений при регистрации*

Altell NEO поддерживает стандартные типы источников сообщений системного журнала. Они перечислены ниже. Кроме того, можно избирательно включить регистрацию для конкретных компонентов маршрутизации. Эти сведения приведены в разделе “Включение и отключение регистрации для конкретных функций ” на стр. 193.

*Таблица 18 - Типы источников сообщений для системного журнала*

| Тип источника сообщений | Описание |
|---|---|
| auth | Проверка подлинности и авторизация |
| authpriv | Несистемная авторизация |
| cron | Служба cron |
| daemon | Системные службы |
| kern | Ядро |
| lpr | Буфер построчного принтера |
| mail | Подсистема электронной почты |
| mark | Отметка времени |
| news | Подсистема USENET |
| protocols | Протоколы маршрутизации (идентичен local7) |
| security | Подсистема безопасности |
| syslog | Системная регистрация |
| user | Прикладные процессы |
| uucp | Подсистема UUCP |
| local0 | Локальный тип источника сообщений 0 |
| local1 | Локальный тип источника сообщений 1 |
| local2 | Локальный тип источника сообщений 2 |
| local3 | Локальный тип источника сообщений 3 |
| local4 | Локальный тип источника сообщений 4 |
| local5 | Локальный тип источника сообщений 5 |
| local6 | Локальный тип источника сообщений 6 |
| all | Все типы источников сообщений, исключая “mark” |

#### *5.1.1.2. Файлы журналов для регистрации*

При включенной регистрации сообщения системного журнала всегда записываются в базу данных **system.db** в каталоге **/var/log** локальной файловой системы. Кроме того, системные журналы можно отправить на консоль или на сервер, на котором работает служебная программа **syslogd** (то есть на сервер системного журнала).

- Для направления сообщений системного журнала на консоль используется команда **system syslog console**.
- Для направления сообщений системного журнала на удаленный компьютер, на котором работает служебная программа **syslogd**, используется команда **system syslog host**.

#### *5.1.1.3. Местоположение и экспорт журнала*

Сообщения записываются в файл журнала **system.db** в каталоге **/var/log** файловой системы Altell NEO. 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%.

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.

#### *5.1.1.4. 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 Altell NEO, связываются с одними из перечисленных ниже уровней серьезности.

*Таблица 19 - 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, — 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. |
| **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.*

### 5.1.2. Пример настройки регистрации

В примере 5.1 выполняется настройка записи сообщений журнала связанных с ядром уровня **info** и более высоких на удалённой машине.

Для этого нужно выполнить следующие действия в режиме настройки:

*Пример 5.1 - Настройка записи журнала на удалённой машине и запись событий, связанных с ядром, имеющих уровень серьезности "info" и выше*

| Действие | Команда |
|---|---|
| Настройка записи событий, связанных с ядром и имеющих уровень серьёзности «info» и выше на удалённой машине 192.168.102.37 | admin@R1# **set system syslog host 192.168.102.37 facility kern level info**<br>[edit] |
| Фиксация настройки. | admin@R1# **commit**<br>[edit]<br>admin@R1# |

### 5.1.3. Включение и отключение регистрации для конкретных функций

В некоторых модулях маршрутизатора Altell NEO — например BGP, OSPF и IPSec VPN — создаются характерные для модуля сообщения, которые можно включить и выключить внутри узла конфигурации для данного модуля. При включении регистрации для модуля системы сообщения журнала отправляются в те же места назначения, которые настроены для системного журнала.

## 5.2. Команды регистрации

В этом разделе представлены следующие команды.

*Таблица 20 - Команды регистрации*

| 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 allow-log-delete` | Настройка допустимости удаления не экспортированных сообщений журнала. |
| `system syslog global facility <источник> level <уровень>` | Указание типов сообщений, которые будут отправляться в главный файл журнала системы. |
| `system syslog host <имя_узла> facility <источник> level <уровень>` | Указание типов сообщений, которые будут отправляться на удаленный сервер системного журнала. |
| Эксплуатационные команды | |
| `clear log` | Очистка системного журнала. |
| `dump log all` | Экспорт всего системного журнала |
| `dump log date` | Экспорт системного журнала за определённую дату/время |
| `dump log from-date` | Экспорт системного журнала за диапазон времени |
| `dump log to-date` | Экспорт системного журнала до определённой даты. |
| `show log` | Отображение системного журнала |
| `show log authorization` | Отображение журнала авторизации |
| `show log date` | Отображение системного журнала за определённую дату/время |
| `show log from-date` | Отображение системного журнала за диапазон времени |
| `show log program` | Отображение сообщений в журнале определённой программы |
| `show log programs` | Отображение списка программ, записывавших сообщения в системный журнал |

| | |
|---|---|
| `show log tail` | Отображение последних записей системного журнала |
| `show log to-date` | Отображение записей системного журнала от самых старых до определённой даты |

### 5.2.1. clear log

Очистка системного журнала

**Синтаксис**

**`clear log`**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Указания по использованию**

Эта команда используется для очистки системного журнала.

По умолчанию удаляются все экспортированные записи системного журнала. Если система настроена так, что допускается удаление не экспортированных сообщений журнала, будут удалены все записи журнала.

Очистка системного журнала не приводит к остановке регистрации событий системой.

Команда доступна только пользователям с привилегиями администратора.

### 5.2.2. dump log all

Экспорт всего системного журнала.

**Синтаксис**

**`dump log all [to`** *`имя_файла`*`]`

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**`to`** *`имя_файла`*

Имя файла, в который будут записаны сообщения журнала.

**Указания по использованию**

Эта команда используется для экспорта всех сообщений системного журнала. По умолчанию производится экспорт на подключенный флэш-носитель, в файл «`syslog.csv`» корневого каталога носителя. При указании параметра «`to`» производится экспорт 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.

*Таблица 21 - Способы указания местоположения для экспорта файла журнала*

| 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:пароль@узел/файл_ключа* где *пользователь* это имя пользователя на узле, *пароль* это пароль, связанный с именем пользователя, *узел* это имя узла или IP-адрес сервера FTP, а *файл_ключа* это файл ключа, включая путь. Если *пользователь* и *пароль* не указаны, будет выдан запрос на их ввод. |
| 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. После того как узел будет добавлен в список известных узлов, может быть использован следующий синтаксис: scp://*пользователь:пароль@узел/файл_конфигурации*, где *пароль* это пароль, ассоциированный с пользователем. Если *пользователь* и *пароль* не указаны, |

| Местоположение | Способ указания |
|---|---|
| | будет выдан запрос на их ввод. |
| 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. |

### 5.2.3. dump log date

Экспорт системного журнала за определённую дату/время.

#### Синтаксис

**dump log date** *дата* **[to** *имя_файла***]**

#### Режим интерфейса

Эксплуатационный режим.

#### Параметры

**date** *дата*

Дата/время экспортируемых сообщений журнала в формате «ГГГГ.ММ.ДД [чч[:мм[:сс]]]».

**to** *имя_файла*

Имя файла, в который будут записаны сообщения журнала.

#### Указания по использованию

Эта команда используется для экспорта сообщений системного журнала определённой даты. По умолчанию производится экспорт на подключенный флэш-носитель, в файл «`syslog.csv`» корневого каталога носителя. При указании параметра «**to**» производится экспорт файла по указанному адресу, который может быть локальным или находиться на сервере TFTP, FTP или SCP.

Формат путей параметра «**to**» описан в таблице «Таблица 21 - Способы указания местоположения для экспорта файла журнала».

### 5.2.4. dump log from-date

Экспорт системного журнала за диапазон времени.

**Синтаксис**

**dump log from-date** *дата1* **[to-date** *дата2***] [to** *имя_файла***]**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**from-date** *дата1*

Начальная дата экспортируемых сообщений журнала в формате «ГГГГ.ММ.ДД [чч[:мм[:сс]]]».

**to-date** *дата2*

Конечная дата экспортируемых сообщений журнала в формате «ГГГГ.ММ.ДД [чч[:мм[:сс]]]».

**to** *имя_файла*

Имя файла, в который будут записаны сообщения журнала.

**Указания по использованию**

Эта команда используется для экспорта сообщений системного журнала определённого диапазона времени. По умолчанию производится экспорт на подключенный флэш-носитель, в файл «syslog.csv» корневого каталога носителя.

Экспорт производится начиная от даты указанной параметром **from-date**. Если параметр **to-date** не задан, то экспорт производится по текущую дату, если задан, то до даты указанной в параметре **to-date**.

При указании параметра «**to**» производится экспорт файла по указанному адресу, который может быть локальным или находиться на сервере TFTP, FTP или SCP.

Формат путей параметра «**to**» описан в таблице «Таблица 21 - Способы указания местоположения для экспорта файла журнала».

## 5.2.5. dump log to-date

Экспорт системного журнала до определённой даты.

**Синтаксис**

**dump log to-date** *дата* **[to** *имя_файла***]**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**to-date** *дата*

Конечная дата экспортируемых сообщений журнала в формате «ГГГГ.ММ.ДД [чч[:мм[:сс]]]».

**to** *имя_файла*

Имя файла, в который будут записаны сообщения журнала.

**Указания по использованию**

Эта команда используется для экспорта сообщений системного журнала до определённой даты. По умолчанию производится экспорт на подключенный флэш-носитель, в файл «syslog.csv» корневого каталога носителя.

Экспорт производится от самой последней записи журнала до даты, указанной в параметре **to-date**.

При указании параметра «**to**» производится экспорт файла по указанному адресу, который может быть локальным или находиться на сервере TFTP, FTP или SCP.

Формат путей параметра «**to**» описан в таблице «Таблица 21 - Способы указания местоположения для экспорта файла журнала».

### 5.2.6. show log

Отображение системного журнала

**Синтаксис**

**show log**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Указания по использованию**

Эта команда используется для вывода системного журнала.

## 5.2.7. show log authorization

Отображение журнала авторизации

**Синтаксис**

**show log authorization**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Указания по использованию**

Эта команда используется для отображения сообщений, относящихся к авторизации из системного журнала. Фактически, выводимые сообщения записаны в едином системном журнале, команда лишь проводит выборку сообщений относящихся к объекту «**auth**».

## 5.2.8. show log date

Отображение системного журнала за определённую дату/время.

**Синтаксис**

**show log date** *дата*

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**date** *дата*

Дата отображаемых сообщений журнала в формате «ГГГГ.ММ.ДД [чч[:мм[:сс]]]».

**Указания по использованию**

Эта команда используется для вывода сообщений системного журнала за определённую дату.

Отображаются сообщения с датой, указанной в параметре `date`. В качестве даты можно задать только время, в этом случае будет производиться выборка за текущий день по указанному времени.

## 5.2.9. show log from-date

Отображение системного журнала за диапазон времени.

**Синтаксис**

**show log from-date** *дата1* **[to-date** *дата2***]**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**from-date** *дата1*

Начальная дата отображаемых сообщений журнала в формате «ГГГГ.ММ.ДД [чч[:мм[:сс]]]».

**to-date** *дата2*

Конечная дата отображаемых сообщений журнала в формате «ГГГГ.ММ.ДД [чч[:мм[:сс]]]».

**Указания по использованию**

Эта команда используется для вывода сообщений системного журнала за определённый диапазон времени.

Отображаются сообщения начиная от даты указанной параметром **from-date**. Если параметр **to-date** не задан, то отображаются сообщения по текущую дату, если задан, то до даты указанной в параметре **to-date**.

В качестве даты можно задать только время, в этом случае будет производиться выборка за текущий день по указанному времени.

## 5.2.10. show log program

Отображение сообщений в журнале определённой программы.

**Синтаксис**

**show log program** *программа*

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**program** *программа*

Имя программы, для которой производится выборка сообщений.

**Указания по использованию**

Эта команда используется для вывода сообщений системного журнала, оставленных определённой программой.

Отображаются сообщения программы, указанной в параметре **program**.

## 5.2.11. show log programs

Отображение списка программ, записывавших сообщения в системный журнал.

**Синтаксис**

```
show log programs
```

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Указания по использованию**

Эта команда используется для вывода списка программ, сообщения которых хранятся в системном журнале.

## 5.2.12. show log tail

Отображение последних записей системного журнала.

**Синтаксис**

**show log tail** [*число_строк*]

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*число_строк*

Число отображаемых строк.

**Указания по использованию**

Эта команда используется для отображения последних строк системного журнала.

При использовании команды без параметров отображаются последние десять строк. Если указан параметр *число_строк*, отображаются последние *число_строк* строк сообщений.

### 5.2.13. show log to-date

Отображение записей системного журнала от самых старых до определённой даты.

**Синтаксис**

**show log to-date** *дата*

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**to-date** *дата*

Конечная дата отображаемых сообщений журнала в формате «ГГГГ.ММ.ДД [чч[:мм[:сс]]]».

**Указания по использованию**

Эта команда используется для отображения сообщений системного журнала до определённой даты. Отображаются сообщения от самой старой записи журнала до даты, указанной в параметре `to-date`.

### 5.2.14. 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 **syslog** 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.

Сообщения журналов, созданные системой Altell NEO, связываются с одним из уровней серьёзности перечисленных в таблице уровней серьёзности.

Altell NEO поддерживает стандартные типы источников сообщений системного журнала перечисленные в таблице источников сообщений системного журнала (Таблица 18 - Типы источников сообщений для системного журнала).

Форма **set** этой команды используется для создания настройки системного журнала.

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

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

## 5.2.15. 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 текст {
                    level текст
                }
            }
        }
}
```

**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**

Отсутствует.

**Указания по использованию**

Эта команда используется для указания типов сообщений, которые будут отправляться на консоль.

Форма **set** этой команды используется для указания типов сообщений, которые будут отправляться на консоль.

Форма **delete** этой команды используется для восстановления настройки сообщений для консоли по умолчанию.

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

## 5.2.16. system syslog global allow-log-delete

Настройка допустимости удаления не экспортированных сообщений журнала.

**Синтаксис**

**set system syslog global allow-log-delete**

**delete system syslog global allow-log-delete**

**show system syslog global allow-log-delete**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
    syslog {
        global {
            allow-log-delete {
            }
        }
    }
}
```

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Выключено.

**Указания по использованию**

Эта команда используется для указания допустимости удаления не экспортированных сообщений журнала. В выключенном состоянии система не позволяет удалять сообщения журнала до тех пор, пока они не будут экспортированы. Во включенном допускается удаление не экспортированных записей как в ручном, так и в автоматическом режиме.

Форма **set** этой команды используется для указания допустимости удаления не экспортированных сообщений журнала.

Форма **delete** этой команды используется для запрещения удаления не экспортированных сообщений журнала.

Форма **show** этой команды используется для просмотра настройки допустимости удаления не экспортированных сообщений журнала.

## 5.2.17. system syslog global facility <источник> level <уровень>

Указание типов сообщений, которые будут отправляться в главный 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 текст {
                    level текст
               }
          }
     }
}
```

**Параметры**

*источник*

Множественный узел. Типы сообщений, которые будут отправляться в главный системный журнал. Поддерживаемые типы источников сообщений приведены в таблице типов источников сообщений (см. стр. 172).

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 сообщений (см. стр. 190).

**Значение по умолчанию**

Для всех источников регистрируются важные события, а для сообщений об авторизации — все события.

**Указания по использованию**

Эта команда используется для указания типов сообщений, которые будут отправляться в главный системный журнал.

Форма **set** этой команды используется для указания типов сообщений, которые будут отправляться в главный системный журнал.

Форма **delete** этой команды используется для удаления настройки типов сообщений, отправляемых в главный системный журнал.

Форма **show** этой команды используется для просмотра настройки для сообщений, отправляемых в главный системный журнал.

## 5.2.18. 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 file** *имя_узла* **facility** [*источник* [**level**]]

**show system syslog file** *имя_узла* **facility** [*источник* [**level**]]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
    syslog {
        host текст {
```

```
                facility текст {
                    level текст
                }
            }
        }
}
```

**Параметры**

*имя_узла*

Множественный узел. Имя узла, куда отправляются указанные сообщения журнала. На узле должен работать протокол **syslog**. В качестве *имя_узла* может быть указан IP-адрес или имя узла. В составе имен файлов 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 на узел. Поддерживаемые типы источников сообщений журнала приведены в таблице типов источников сообщений (см. стр. 172).

Можно отправлять на узел сообщения из нескольких типов источников, создав несколько узлов конфигурации **facility** в узле конфигурации **host**.

*уровень*

Наименьший уровень серьезности 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 (см. стр. 190).

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для указания типов сообщений, которые будут отправляться в 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 восстановления настройки по умолчанию для сообщений, отправляемых на удаленный сервер системного журнала.

Форма **show** этой команды используется для просмотра настройки для сообщений, отправляемых на удаленный сервер системного журнала.

# 6. НАСТРОЙКА ИНТЕРФЕЙСОВ

## 6.1. Управляющий интерфейс

В данном разделе описаны следующие команды.

*Таблица 22 - Команды настройки управляющего интерфейса Altell NEO*

| Команды настройки | |
|---|---|
| `interfaces management <состояние>` | Включение/выключение управляющего интерфейса Altell NEO. |

### 6.1.1. interfaces management <*состояние*>

Включение/выключение управляющего интерфейса Altell NEO.

**Синтаксис**

**`set interfaces management`** ***`состояние`***

***`delete interfaces management`***

***`show interfaces management`***

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    management [true|false]
}
```

**Параметры**

*`состояние`*

Указание включения/выключения управляющего интерфейса Altell NEO. Поддерживаемые значения:

**true**: Включение управляющего интерфейса.

**false**: Выключение управляющего интерфейса.

**Значение по умолчанию**

По умолчанию принято значение **true**, управляющий интерфейс включён.

**Указания по использованию**

***ПРЕДУПРЕЖДЕНИЕ*** *Опасный параметр! При ошибке в*

*конфигурации возможна потеря сетевого доступа к системе.*

*Изменение данного параметра влечёт за собой автоматическое сохранение конфигурации во время фиксации и перезагрузку системы.*

Команда используется для включения и выключения управляющего интерфейса Altell NEO. По умолчанию, один из интерфейсов NEO 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 NEO 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 NEO для работы в обслуживаемых сетях, данная команда позволяет отключить такое поведение управляющего интерфейса.

При переключении из состояния **true** в **false** происходит переименование интерфейса **ethm** в **eth0** и прописывание всех настроенных на нём служб в конфигурацию NEO. После перезагрузки интерфейсом **eth0** можно будет пользоваться так же, как и любым другим.

При обратном переключении происходит обратное переименование (из **eth0** в **ethm**) и на интерфейсе **ethm**, после перезагрузки, восстанавливаются штатные для него службы DHCP, SSH и HTTPS.

Форма **set** данной команды используется для включения управляющего интерфейса.

Форма **delete** данной команды используется для восстановления значения, принятого по умолчанию.

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

## 6.2. Настройка интерфейсов Ethernet

В данном разделе описаны следующие команды.

*Таблица 23 - Команды настройки интерфейсов Ethernet*

| Команды настройки | |
|---|---|
| `interfaces ethernet <ethx>` | Определение интерфейса Ethernet. |
| `interfaces 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-link-detect` | Отключение определения изменения состояния физического канала для интерфейса Ethernet. |
| `interfaces ethernet <ethx> duplex <режим_дуплекса>` | Установка режима дуплекса для интерфейса Ethernet. |
| `interfaces ethernet <ethx> ip enable-proxy-arp` | Включение режима проксирования ARP для интерфейса Ethernet. |
| `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 counters` | Очистка статистических счетчиков для интерфейса Ethernet. |
| `show interfaces ethernet` | Вывод сведений и статистических данных для интерфейсов Ethernet. |
| `show interfaces ethernet detail` | Вывод подробных сведений для интерфейсов Ethernet. |
| `show interfaces ethernet <ethx> brief` | Вывод кратких сведений о состоянии для интерфейса Ethernet. |

| | |
|---|---|
| `show interfaces ethernet <ethx> capture` | Вывод сведений о сетевом трафике, записанном на интерфейсе Ethernet. |
| `show interfaces ethernet <ethx> identify` | Включение светодиодного индикатора на интерфейсе Ethernet для его определения. |
| `show interfaces ethernet <ethx> physical` | Вывод сведений о физическом уровне для интерфейса Ethernet. |
| `show interfaces ethernet <ethx> queue` | Вывод сведений об очередях для интерфейса Ethernet. |
| `show interfaces ethernet <ethx> statistics` | Отображение аппаратной статистики для адаптеров Ethernet. |

### 6.2.1. clear interfaces ethernet 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 **eth23** 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**.

### 6.2.2. 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 eth0..eth23 {
    }
}
```

**Параметры**

*ethx*

Множественный узел. Идентификатор для определяемого интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23** в зависимости от реально имеющихся в системе интерфейсов Ethernet.

Количество созданных узлов конфигурации интерфейсов Ethernet совпадает с количеством физических сетевых интерфейсов Ethernet, определенных в системе.

**Значение по умолчанию**

При запуске системы для всех существующих в системе физических интерфейсов Ethernet создаются узлы настройки.

**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. Однако поскольку при запуске системы узлы настройки для всех физических интерфейсов создаются автоматически, форму **set** данной команды может потребоваться использовать только для создания интерфейса Ethernet, узел конфигурации которого удален вручную.

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.

### 6.2.3. interfaces ethernet <ethx> address

Назначение IP-адреса и префикса сети интерфейсу Ethernet.

**Синтаксис**

**set interfaces ethernet *ethx* address** {*ipv4-адрес* | *ipv6-адрес* | **dhcp**}

**delete interfaces ethernet *ethx* address** {*ipv4-адрес* | *ipv6-адрес* | **dhcp**}

**show interfaces ethernet** *ethx* **address**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    ethernet eth0..eth23 {
        address [ipv4-адрес|ipv6-адрес|dhcp]
    }
}
```

**Параметры**

*ethx*

Множественный узел. Идентификатор определяемого интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**.

*ipv4-адрес*

IPv4-адрес для данного интерфейса Ethernet. Для указания адреса используется формат *ip-адрес/префикс* (например, 192.168.1.77/24). Назначить интерфейсу несколько IP-адресов можно, создав соответствующее количество узлов конфигурации **address.**

*ipv6-адрес*

IPv6-адрес для данного интерфейса Ethernet. Для указания адреса используется формат *ipv6-адрес/префикс* (например, 2001:db8:1234::/48). Назначить интерфейсу несколько IPv6-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*> (см. стр. 224), которая имеет более высокий приоритет. Если после истечения срока аренды значение MTU явно не указывается, оно устанавливается равным 1500.

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.

## 6.2.4. 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 eth0..eth23 {
        description текст
    }
}
```

**Параметры**

*ethx*

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

Значение должно лежать в диапазоне от **eth0** до **eth23**.

*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.

## 6.2.5. 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 eth0..eth23 {
        disable
    }
}
```

**Параметры**

*ethx*

Множественный узел. Идентификатор определяемого интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23.**

**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.

## 6.2.6. interfaces ethernet <ethx> disable-link-detect

Отключение определения изменения состояния физического канала для интерфейса Ethernet.

**Синтаксис**

**set interfaces ethernet** *ethx* **disable-link-detect**

**delete interfaces ethernet** *ethx* **disable-link-detect**

**show interfaces ethernet** *ethx*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    ethernet eth0..eth23 {
```

```
            disable-link-detect
        }
    }
```

**Параметры**

*ethx*

Множественный узел. Идентификатор определяемого интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**.

**Значение по умолчанию**

Определение изменения состояния физического канала на интерфейсе включено.

**Указания по использованию**

Эта команда используется для отмены определения изменения состояния физического канала на интерфейсе Ethernet (например, когда сетевой кабель не подключен).

Форма **set** данной команды используется для отключения определения изменения состояния физического канала.

Форма **delete** данной команды используется для включения определения изменения состояния физического канала.

Форма **show** данной команды используется для просмотра настройки интерфейса Ethernet.

## 6.2.7. 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 eth0..eth23 {
```

```
            duplex [auto|half|full]
        }
    }
```

**Параметры**

*ethx*

Множественный узел. Идентификатор определяемого интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**.

*режим_дуплекса*

Режим дуплекса интерфейса. Поддерживаемые значения:

**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.

> ***ПРИМЕЧАНИЕ*** *Не всё оборудование поддерживает возможность явного указания режима дуплекса. Если используется оборудование, не поддерживающее такую установку, 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.

### 6.2.8. interfaces ethernet <ethx> ip enable-proxy-arp

Включение режима проксирования ARP для интерфейса Ethernet.

**Синтаксис**

**set interfaces ethernet** *ethx* **ip enable-proxy-arp**

**delete interfaces ethernet** *ethx* **ip enable-proxy-arp**

**show interfaces ethernet** *ethx* **ip**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    ethernet eth0..eth23 {
        ip {
            enable-proxy-arp
        }
    }
}
```

**Параметры**

*ethx*

Множественный узел. Идентификатор определяемого интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**.

**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.

## 6.2.9. 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 eth0..eth23 {
        mac mac-адрес
    }
}
```

**Параметры**

*ethx*

Множественный узел. Идентификатор определяемого интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**.

*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.

## 6.2.10. 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 eth0..eth23 {
        mtu целоебеззнака32разр
    }
}
```

**Параметры**

*ethx*

Множественный узел. Идентификатор определяемого интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**.

*mtu*

Установка значения MTU (в октетах) для интерфейса Ethernet в целом, включая все логические интерфейсы, настроенные на нем. Значение должно лежать в диапазоне от 68 до 9000.

**Значение по умолчанию**

Если значение явно не указано, фрагментация не выполняется.

**Указания по использованию**

Команда позволяет установить значение MTU (максимальный размер передаваемого блока данных) для интерфейса Ethernet. Установленное значение также применяется ко всем виртуальным интерфейсам, связанным с данным интерфейсом Ethernet.

Значение MTU интерфейса, являющегося частью интерфейса агрегированных каналов Ethernet, не может быть изменено.

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, а отправителю будет направлено соответствующее сообщение ICMP “Packet too big” с указанием того, что отправленный пакет имел слишком большой размер.

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.

## 6.2.11. 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 eth0..eth23 {
        speed [auto|10|100|1000]
    }
}
```

**Параметры**

*ethx*

Множественный узел. Идентификатор определяемого интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**.

*скорость*

Устанавливаемая скорость интерфейса Ethernet. Поддерживаемые значения:

**auto**: Скорость интерфейса будет автоматически согласована маршрутизатором с интерфейсом на другом конце подключения.

**10**: 10 Мб/с.

**100**: 100 Мб/с.

**1000**: 1000 Мб/с.

**Значение по умолчанию**

Значение скорости для канала Ethernet устанавливается автоматически.

**Указания по использованию**

Команда используется для установки скорости интерфейса Ethernet.

> ***ПРИМЕЧАНИЕ*** *Оборудование может не поддерживать возможность явной установки скорости передачи. Если используется оборудование, не поддерживающее такую установку, 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.

## 6.2.12. show interfaces ethernet

Вывод сведений и статистических данных для интерфейсов Ethernet.

**Синтаксис**

**show interfaces ethernet** [*ethx*]

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*ethx*

Отображение сведений для указанного интерфейса Ethernet.

**Значение по умолчанию**

Отображение сведений для всех интерфейсов Ethernet.

**Указания по использованию**

Команда используется для просмотра состояния работоспособности интерфейса Ethernet.

**Примеры**

В примере 6.1 выводятся сведения для всех интерфейсов Ethernet.

*Пример 6.1 - Вывод сведений для всех интерфейсов Ethernet*

```
admin@neo:~$ show interfaces ethernet
Interface IP Address   State      Link Description
eth0      -            admin down down
eth1      -            up         up
eth2      10.1.0.66/24 up         up
eth3      -            up         down
```

В примере 6.2 выводятся сведения для интерфейса **eth2**.

*Пример 6.2 - Вывод сведений для одного интерфейса Ethernet*

```
admin@neo:~$ show interfaces ethernet eth2
eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
pfifo_fast qlen 1000
     link/ether 00:13:46:e7:f8:87 brd ff:ff:ff:ff:ff:ff
     inet 10.1.0.66/24 brd 10.1.0.255 scope global eth2
     inet6 fe80::211:46ff:fee7:f687/64 scope link
     valid_lft forever preferred_lft forever
RX: bytes packets errors dropped overrun mcast
   533348    3572      0       0       0     0
TX: bytes packets errors dropped carrier collisions
```

```
    54412     541       0       0       0          0
```

## 6.2.13. show interfaces ethernet detail

Вывод подробных сведений для интерфейсов Ethernet.

**Синтаксис**

**show interfaces ethernet detail**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Команда используется для вывода детализированной статистики, а также сведений о настройке интерфейсов Ethernet.

**Примеры**

В примере 6.3 показано первое окно вывода для команды **show interfaces ethernet detail**.

*Пример 6.3 - Вывод подробных сведений для интерфейса Ethernet*

```
admin@neo:~$ show interfaces ethernet detail
eth0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
     link/ether 00:40:63:e2:e4:00 brd ff:ff:ff:ff:ff:ff
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
eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
pfifo_fast qlen 1000
     link/ether 00:40:63:e2:e3:dd brd ff:ff:ff:ff:ff:ff
     inet6 fe80::240:63ff:fee2:e3dd/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
      468       6      0       0       0          0
eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
pfifo_fast qlen 1000
     link/ether 00:13:46:e7:f8:87 brd ff:ff:ff:ff:ff:ff
     inet 10.1.0.66/24 brd 10.1.0.255 scope global eth2
     inet6 fe80::211:46ff:fee7:f687/64 scope link
        valid_lft forever preferred_lft forever
lines 1-23
```

### 6.2.14. show interfaces ethernet <ethx> brief

Вывод кратких сведений о состоянии для интерфейса Ethernet.

**Синтаксис**

**show interfaces ethernet** *ethx* **brief**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*ethx*

Идентификатор интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23** в зависимости от реально имеющихся в системе интерфейсов Ethernet.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Команда используется для отображения состояния интерфейса Ethernet.

**Примеры**

В примере 6.4 представлен вывод кратких сведений о состоянии для интерфейса eth2.

*Пример 6.4 -Вывод кратких сведений о состоянии интерфейса Ethernet*

```
admin@neo:~$ show interfaces ethernet eth2 brief
```

```
Interface IP Address   State Link Description
eth2      10.1.0.66/24 up    up
```

### 6.2.15. show interfaces ethernet <ethx> capture

Отображение сведений о сетевом трафике, записанном на интерфейсе Ethernet.

**Синтаксис**

**show interfaces ethernet** *ethx* **capture [not port** *порт* **| port** *порт***]**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*ethx*

Идентификатор интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23** в зависимости от реально имеющихся в системе интерфейсов Ethernet.

**not port** *порт*

Вывод сетевого трафика, записанного на всех портах, кроме указанного.

**port** *порт*

Вывод сетевого трафика, записанного на указанном порту.

**Значение по умолчанию**

Выводится весь сетевой трафик, записанный на всех портах на указанном интерфейсе.

**Указания по использованию**

Команда используется для вывода сетевого трафика, записанного на указанном интерфейсе. Для того чтобы остановить вывод, следует ввести <Ctrl>+C.

**Примеры**

В примере 6.5 представлен вывод сетевого трафика, записанного на интерфейсе eth0.

*Пример 6.5 - Отображение записанного сетевого трафика*

```
admin@neo:~$ show interfaces ethernet eth0 capture
```

```
Capturing traffic on eth0 …

0.000000 fe80::ad08:8661:4d:b925 -> ff02::c SSDP M-SEARCH
* HTTP/1.1

0.000067 fe80::69ca:5c11:bcf6:29da -> ff02::c SSDP M-
SEARCH * HTTP/1.1

2.608804 fe80::8941:71ef:b55d:e348 -> ff02::1:2 DHCPv6
Solicit

3.010862 fe80::ad08:8661:4d:b925 -> ff02::c SSDP M-SEARCH
* HTTP/1.1

3.010901 fe80::69ca:5c11:bcf6:29da -> ff02::c SSDP M-
SEARCH * HTTP/1.1

4.568357 192.168.1.254 -> 238.255.255.251 SSDP NOTIFY *
HTTP/1.1

4.568372 192.168.1.254 -> 238.255.255.251 SSDP NOTIFY *
HTTP/1.1
```

...

### 6.2.16. show interfaces ethernet <ethx> identify

Включение светодиодного индикатора на интерфейсе Ethernet для его определения.

**Синтаксис**

**show interfaces ethernet** *ethx* **identify**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*ethx*

Идентификатор интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23** в зависимости от реально имеющихся в системе интерфейсов Ethernet.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Команда используется для поиска физического порта Ethernet, который связан с интерфейсом *ethx* в системе.

**Примеры**

В примере 6.6 приведен вывод для команды **show interfaces ethernet** *ethx*

**identify**.

*Пример 6.6 - Идентификация интерфейса Ethernet по миганию светодиода*

```
admin@neo:~$ show interfaces ethernet eth2 identify
Interface eth2 should be blinking now.
Press Enter to stop...
```

## 6.2.17. show interfaces ethernet <ethx> physical

Вывод сведений о физическом уровне для интерфейса Ethernet.

**Синтаксис**

**show interfaces ethernet** *ethx* **physical**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*ethx*

Идентификатор интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23** в зависимости от реально имеющихся в системе интерфейсов Ethernet.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Команда используется для вывода сведений о физическом уровне для интерфейса Ethernet.

**Примеры**

В примере 6.7 приведен вывод для команды **show interfaces ethernet** *ethx* **physical**.

*Пример 6.7 - Вывод сведений о физическом уровне для интерфейса Ethernet*

```
admin@neo:~$ show interfaces ethernet eth0 physical
Settings for eth0:
   Current message level: 0x00000007 (7)
   Link detected: yes
driver: pcnet32
```

```
version: 1.35
firmware-version:
bus-info: 0000:02:00.0
admin@neo:~$
```

## 6.2.18. show interfaces ethernet <ethx> queue

Вывод сведений об очередях для интерфейса Ethernet.

**Синтаксис**

**show interfaces ethernet** *ethx* **queue [class | filter]**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*ethx*

Идентификатор интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23** в зависимости от реально имеющихся в системе интерфейсов Ethernet.

**class**

Отображение классов очередей для указанного интерфейса.

**filter**

Отображение фильтров очередей для указанного интерфейса.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет вывести сведения об очередях для интерфейса Ethernet.

**Примеры**

В примере 6.8 приведен вывод сведений об очередях для интерфейса eth0.

*Пример 6.8 - Вывод сведений об очередях для интерфейса Ethernet*

```
admin@neo:~$ show interfaces ethernet eth0 queue
qdisc pfifo_fast 0: root bands 3 priomap 1 2 2 2 1 2 0 0
1 1 1 1 1 1 1 1
 Sent 810323 bytes 6016 pkt (dropped 0, overlimits 0
```

```
requeues 0)
 rate 0bit 0pps backlog 0b 0p requeues 0
```

### 6.2.19. show interfaces ethernet <ethx> statistics

Отображение аппаратной статистики для адаптеров Ethernet.

**Синтаксис**

**show interfaces ethernet** *ethx* **statistics**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*ethx*

Идентификатор интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23** в зависимости от реально имеющихся в системе интерфейсов Ethernet.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Команда позволяет отобразить статистику Ethernet для указанного интерфейса.

**Примеры**

В примере 6.9 приведен вывод статистики Ethernet для интерфейса eth3.

*Пример 6.9 - Вывод статистики Ethernet*

```
admin@neo:~$ show interfaces ethernet eth3 statistics

NIC statistics: tx_ok: 1111 rx_ok: 1467 tx_err: 0 rx_err:
4 rx_fifo: 0 frame_align: 0tx_ok_1col: 0 tx_ok_mcol: 0
rx_ok_phys: 1376rx_ok_bcast: 1 rx_ok_mcast: 0 tx_abort: 0
tx_underrun: 0 rx_frags: 0

admin@neo:~$
```

## 6.3. Настройка интерфейса заглушки

В данном разделе представлены следующие команды.

| Команды настройки |
|---|

| | |
|---|---|
| `interfaces loopback lo` | Определение интерфейса заглушки. |
| `interfaces loopback lo address` | 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. |
| `show interfaces loopback detail` | Отображение подробных сведений и статистических данных для интерфейса заглушки. |
| `show interfaces loopback lo brief` | Отображение кратких сведений о состоянии для интерфейса заглушки. |

## 6.3.1. 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**.

## 6.3.2. 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**

При запуске системы узел конфигурации создается автоматически.

**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.

Интерфейс заглушки обладает следующими преимуществами:

- Так как интерфейс заглушки всегда включен, сеанс маршрутизации (например, сеанс BGP) может быть продолжен даже в том случае, если произойдет сбой выходного интерфейса.

- Можно упростить сбор управляющих сведений, указав интерфейс заглушки в качестве интерфейса для отправки и приема управляющих сведений, таких как журналы и ловушки SNMP.

- Интерфейс заглушки может быть использован для усиления безопасности посредством фильтрации при помощи правил контроля доступа, в которых

локальный интерфейс указан в качестве единственно допустимого места назначения.

- При использовании OSPF можно представить интерфейс заглушки в качестве интерфейсного маршрута в сеть, не зависящего от того, включены ли физические интерфейсы. Это повышает надежность, так как увеличивается вероятность того, что маршрутизируемый трафик будет получен и затем перенаправлен.
- При использовании BGP на независимых устройствах к интерфейсу заглушки можно настроить параллельные пути. Это обеспечивает лучшее распределение нагрузки.

Форма **set** данной команды используется для создания интерфейса заглушки. Так как при запуске системы автоматически создаются узлы настройки для всех интерфейсов заглушки, форма **set** данной команды может потребоваться только в том случае, если узел конфигурации интерфейса заглушки был удален вручную.

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.

### 6.3.3. interfaces loopback lo address

Назначение интерфейсу заглушки IP-адреса и префикса сети.

**Синтаксис**

**set interfaces loopback lo address {***ipv4-адрес* **|** *ipv6-адрес***}**

**delete interfaces loopback lo address {***ipv4-адрес* **|** *ipv6-адрес***}**

**show interfaces loopback lo address**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
```

```
        loopback lo {
            address [ipv4-адрес|ipv6-адрес]
        }
}
```

**Параметры**

*ipv4-адрес*

IPv4 -адрес и префикс сети для указанного интерфейса. Для указания адреса используется формат *ip-адрес/префикс* (например, 127.0.0.1/8).

Чтобы назначить интерфейсу заглушки несколько IP-адресов, следует создать соответствующее количество узлов конфигурации **address.**

*ipv6-адрес*

IPv6-адрес, а также префикс сети для указанного интерфейса. Для указания адреса используется формат *ipv6-адрес/префикс* (например, 2001:db8:1234::/48).

Чтобы назначить интерфейсу заглушки несколько IPv6-адресов, следует создать соответствующее количество узлов конфигурации **address**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

При запуске система автоматически создает интерфейс заглушки с именем **lo**. Для этого интерфейса необходимо назначить IP-адрес. 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 следует сопоставить с адресом интерфейса заглушки, а не физического интерфейса.

- При настройке OSPF и iBGP в качестве идентификатора маршрутизатора следует установить адрес интерфейса заглушки.

> ***ПРИМЕЧАНИЕ*** *по умолчанию таблица маршрутизации содержит подключенные маршруты для интерфейсов* ***lo****:*

*127.0.0.1/8 (IPv4) и ::1/128 (IPv6).*

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.

### 6.3.4. 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 текст
    }
}
```

**Параметры**

*описание*

Текстовое 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.

### 6.3.5. show interfaces loopback

Вывод сведений об интерфейсе заглушки.

**Синтаксис**

```
show interfaces loopback [lo]
```

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**lo**

Вывод подробных сведений о настройке и статистических данных для интерфейса заглушки.

**Значение по умолчанию**

Вывод кратких сведений о состоянии интерфейса заглушки.

**Указания по использованию**

Команда используется для отображения состояния интерфейса заглушки.

**Примеры**

В примере 6.10 приведен вывод сведений для интерфейса заглушки.

*Пример 6.10 - Вывод сведений об интерфейсе заглушки*

```
admin@neo:~$ show interfaces loopback
Interface IP Address  State Link Description
lo        127.0.0.1/8 up    up
```

В примере 6.11 приведен вывод подробных сведений для интерфейса заглушки.

*Пример 6.11 - Вывод подробных сведений для интерфейса заглушки*

```
admin@neo:~$ show interfaces loopback lo
lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
     link/loopback 00:00:00:00:00:00 brd
00:00:00:00:00:00
```

```
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       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
        0       0      0       0       0          0
```

### 6.3.6. show interfaces loopback detail

Вывод подробных сведений и статистических данных для интерфейса заглушки.

**Синтаксис**

**`show interfaces loopback detail`**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Команда используется для вывода подробных сведений, а также данных статистики для интерфейса заглушки.

**Примеры**

В примере 6.12 приведен вывод подробной статистики для интерфейса заглушки.

*Пример 6.12 - Вывод статистики для интерфейса заглушки*

```
admin@neo:~$ show interfaces loopback detail
lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd
00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
```

```
        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
        0       0      0       0       0          0
```

### 6.3.7. show interfaces loopback lo brief

Вывод кратких сведений о состоянии для интерфейса заглушки.

**Синтаксис**

**show interfaces loopback lo brief**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Команда используется для вывода сведений о состоянии интерфейса заглушки.

**Примеры**

В примере 6.13 приведен вывод кратких сведений для интерфейса заглушки.

*Пример 6.13 - Вывод кратких сведений для интерфейса заглушки*

```
admin@neo:~$ show interfaces loopback lo brief
Interface IP Address  State Link Description
lo        127.0.0.1/8 up    up
```

## 6.4. Настройка виртуальных интерфейсов

В данном разделе представлены следующие команды.

| Команды настройки | |
|---|---|
| Виртуальные интерфейсы на интерфейсах Ethernet | |
| `interfaces ethernet <ethx>` | 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> disable-link-detect` | Отключение определения изменений состояния физического канала для виртуального интерфейса 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> disable-link-detect` | Отключение определения изменений состояния физического канала для виртуального интерфейса агрегированных каналов Ethernet. |
| Эксплуатационные команды | |
| `show interfaces bonding <bondx> vif` | Отображение сведений о виртуальном интерфейсе агрегированных каналов Ethernet. |

| | |
|---|---|
| `show interfaces bonding <bondx> vif <идентификатор_vlan> brief` | Отображение кратких сведений о состоянии для виртуального интерфейса агрегированных каналов Ethernet. |
| `show interfaces bonding <bondx> vif <идентификатор_vlan> queue` | Отображение сведений об очередях для виртуального интерфейса. |
| `show interfaces ethernet <ethx> vif <идентификатор_vlan>` | Отображение сведений о виртуальном интерфейсе Ethernet. |
| `show interfaces ethernet <ethx> vif <идентификатор_vlan> brief` | Отображение кратких сведений о состоянии для виртуального интерфейса Ethernet. |
| `show interfaces ethernet <ethx> vif <идентификатор_vlan> queue` | Отображение сведений об очередях для виртуального интерфейса. |

### 6.4.1. 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 bond0..bond99 {
        vif 0-4094 {
        }
```

```
        }
    }
```

**Параметры**

*bondx*

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 0 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 агрегированных каналов Ethernet.

Виртуальные интерфейсы, созданные для интерфейсов агрегированных каналов Ethernet, принимают 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 и всей его настройки.

Форма **show** данной команды используется для просмотра настройки виртуального интерфейса.

### 6.4.2. 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 {***ipv4-адрес* **|** *ipv6-адрес* **| dhcp}**

**delete interfaces bonding** *bondx* **vif** *идентификатор_vlan* **address {***ipv4-адрес* **|** *ipv6-адрес* **| dhcp}**

**show interfaces bonding** *bondx* **vif** *идентификатор_vlan* **address**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    bonding bond0..bond99 {
        vif 0-4094 {
            address [ipv4-адрес|ipv6-адрес|dhcp]
        }
    }
}
```

**Параметры**

*bondx*

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 0 до 4094.

*ipv4-адрес*

IPv4-адрес и префикс сети для указанного виртуального интерфейса. Для указания адреса используется формат *ip-адрес/префикс* (например, 192.168.1.77/24). Чтобы назначить виртуальному интерфейсу несколько IP-адресов, следует создать соответствующее количество узлов конфигурации **address**.

*ipv6-адрес*

IPv6-адрес и префикс сети для указанного виртуального интерфейса. Для указания адреса используется формат *ipv6-адрес/префикс* (например,

2001:db8:1234::/48). Чтобы назначить виртуальному интерфейсу несколько IPv6-адресов, следует создать 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.

### 6.4.3. 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 bond0..bond99 {
        vif 0-4094 {
            description текст
```

```
            }
        }
    }
```

**Параметры**

*bondx*

Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от **bond0** до **bond99**.

*идентификатор_vlan*

Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 0 до 4094.

*описание*

Текстовое 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.

Форма **delete** данной команды используется для удаления текстового описания виртуального интерфейса.

Форма **show** данной команды используется для отображения настройки текстового описания виртуального интерфейса.

### 6.4.4. interfaces bonding <bondx> vif <идентификатор_vlan> disable

Отключение виртуального интерфейса 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 bond0..bond99 {
        vif 0-4094 {
            disable
        }
    }
}
```

**Параметры**

*bondx*

Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от **bond0** до **bond99**.

*идентификатор_vlan*

Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 0 до 4094.

**Значение по умолчанию**

Виртуальный интерфейс включен.

**Указания по использованию**

Команда используется для отключения виртуального интерфейса 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.

### 6.4.5. interfaces bonding <bondx> vif <идентификатор_vlan> disable-link-detect

Отключение определения изменений состояния физического канала для виртуального интерфейса агрегированных каналов Ethernet.

**Синтаксис**

**set interfaces bonding** *bondx* **vif** *идентификатор_vlan* **disable-link-detect**

**delete interfaces bonding** *bondx* **vif** *идентификатор_vlan* **disable-link-detect**

**show interfaces bonding** *bondx* **vif** *идентификатор_vlan*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    bonding bond0..bond99 {
        vif 0-4094 {
            disable-link-detect
        }
    }
}
```

**Параметры**

*bondx*

Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от **bond0** до **bond99**.

*идентификатор_vlan*

Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 0 до 4094.

**Значение по умолчанию**

По умолчанию режим **disable-link-detect** не установлен.

**Указания по использованию**

Команда используется для того, чтобы указать виртуальному интерфейсу агрегированных каналов Ethernet не определять изменения состояния нижележащего физического канала (например, когда сетевой кабель не подключен).

Форма **set** данной команды используется для отключения определение изменений состояния физического канала.

Форма **delete** данной команды используется для включения определения изменений состояния физического канала.

Форма **show** данной команды используется для того, чтобы просмотреть

настройку виртуального интерфейса агрегированных каналов Ethernet.

### 6.4.6. 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 eth0..eth23 {
        vif 0-4094 {
        }
    }
}
```

**Параметры**

*ethx*

Множественный узел. Идентификатор определяемого интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**.

*идентификатор_vlan*

Множественный узел. Идентификатор VLAN для виртуального интерфейса, используемый с системой тегов VLAN стандарта 802.1Q. Значение должно лежать в диапазоне от 0 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.

## 6.4.7. 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 {ipv4-адрес | ipv6-адрес | dhcp}

delete interfaces ethernet ethx vif идентификатор_vlan
address {ipv4-адрес | ipv6-адрес | dhcp}

show interfaces ethernet ethx vif идентификатор_vlan
address
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    ethernet eth0..eth23 {
        vif 0-4094 {
            address [ipv4-адрес|ipv6-адрес|dhcp]
        }
    }
}
```

**Параметры**

*ethx*

Множественный узел. Идентификатор определяемого интерфейса Ethernet.

Значение должно лежать в диапазоне от **eth0** до **eth23**.

*идентификатор_vlan*

Множественный узел. Идентификатор VLAN для виртуального интерфейса.

Значение должно лежать в диапазоне от 0 до 4094.

*ipv4-адрес*

IPv4-адрес и префикс сети для указанного виртуального интерфейса. Для указания адреса используется формат *ip-адрес/префикс* (например, 192.168.1.77/24). Чтобы назначить виртуальному интерфейсу несколько IP-адресов, следует создать соответствующее количество узлов конфигурации **address**.

*ipv6-адрес*

IPv6-адрес и префикс сети для указанного виртуального интерфейса. Для указания адреса используется формат *ipv6-адрес/префикс* (например, 2001:db8:1234::/48). Чтобы назначить виртуальному интерфейсу несколько IPv6-адресов, следует создать 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 используется для удаления IP-адреса для указанного виртуального интерфейса.

Форма **show** данной команды используется для отображения настройки IP-адреса указанного виртуального интерфейса.

### 6.4.8. 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 eth0..eth23 {
        vif 0-4094 {
            description: текст
        }
    }
}
```

**Параметры**

*ethx*

Множественный узел. Идентификатор определяемого интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**.

*идентификатор_vlan*

Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 0 до 4094.

*описание*

Текстовое описание виртуального интерфейса.

**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.

### 6.4.9. interfaces ethernet <ethx> vif <идентификатор_vlan> disable

Отключение виртуального интерфейса 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 eth0..eth23 {
          vif 0-4094 {
               disable
          }
     }
}
```

**Параметры**

*ethx*

Множественный узел. Идентификатор определяемого интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**.

*идентификатор_vlan*

Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 0 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.

## 6.4.10. interfaces ethernet <ethx> vif <идентификатор_vlan> disable-link-detect

Отключение определения изменений состояния физического канала для виртуального интерфейса Ethernet.

**Синтаксис**

**set interfaces ethernet** *ethx* **vif** *идентификатор_vlan* **disable-link-detect**

**delete interfaces ethernet** *ethx* **vif** *идентификатор_vlan* **disable-link-detect**

**show interfaces ethernet** *ethx* **vif** *идентификатор_vlan*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    ethernet eth0..eth23 {
        vif 0-4094 {
            disable-link-detect
        }
    }
}
```

**Параметры**

*ethx*

Множественный узел. Идентификатор определяемого интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**.

*идентификатор_vlan*

Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 0 до 4094.

**Значение по умолчанию**

По умолчанию режим **disable-link-detect** не установлен.

**Указания по использованию**

Команда позволяет отключить определение изменения состояния физического канала (например, когда сетевой кабель не подключен) для интерфейса Ethernet.

Форма **set** данной команды используется для отключения определение изменений состояния физического канала.

Форма **delete** данной команды используется для включения определения изменений состояния физического канала.

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

## 6.4.11. show interfaces bonding <bondx> vif <идентификатор_vlan>

Вывод сведений о виртуальном интерфейсе агрегированных каналов Ethernet.

**Синтаксис**

**show interfaces bonding** *bondx* **vif** *идентификатор_vlan*

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*bondx*

Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от **bond0** до **bond99**.

*идентификатор_vlan*

Вывод сведений для указанного виртуального интерфейса.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Команда позволяет просмотреть состояние управления и работоспособности виртуального интерфейса агрегированных каналов Ethernet.

**Примеры**

В примере 6.14 приведен вывод сведений для виртуального интерфейса vif 9, созданного на основе интерфейса агрегированных каналов bond0.

*Пример 6.14 - Вывод сведений для виртуального интерфейса агрегированных каналов*

```
admin@neo:~$ show interfaces bonding bond0 vif 9
bond0.9@bond0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
qdisc noqueue
     link/ether 00:0c:29:da:3a:3d brd ff:ff:ff:ff:ff:ff
     inet6 fe80::20c:29ff:feda:3a3d/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
     2914      13      0       0       0          0
admin@neo:~$
```

## 6.4.12. show interfaces bonding <bondx> vif <идентификатор_vlan> brief

Отображение кратких сведений о состоянии для виртуального интерфейса агрегированных каналов Ethernet.

**Синтаксис**

**show interfaces bonding** *bondx* **vif** *идентификатор_vlan* **brief**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*bondx*

Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от **bond0** до **bond99**.

*идентификатор_vlan*

Вывод сведений для указанного виртуального интерфейса.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Команда используется для отображения состояния виртуального интерфейса.

**Примеры**

В примере 6.15 приведен вывод кратких сведений о состоянии для интерфейса bond2.6.

*Пример 6.15 - Вывод кратких сведений о состоянии для виртуального интерфейса*

```
admin@neo:~$ show interfaces bonding bond2 vif 6 brief
Interface IP Address    State    Link Description
bond2.6   10.2.6.66/24  up       up
```

## 6.4.13. show interfaces bonding <bondx> vif <идентификатор_vlan> queue

Вывод сведений об очередях для виртуального интерфейса.

**Синтаксис**

**show interfaces bonding** *bondx* **vif** *идентификатор_vlan* **queue [class | filter]**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*bondx*

Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от **bond0** до **bond99**.

*идентификатор_vlan*

Вывод сведений для указанного виртуального интерфейса.

**class**

Отображение классов очередей для указанного интерфейса.

**filter**

Отображение фильтров очередей для указанного интерфейса.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Команда используется для вывода сведений об очередях для виртуального

интерфейса.

**Примеры**

В примере 6.16 приведен вывод информации об очередях для интерфейса bond0.6.

*Пример 6.16 - Вывод сведений об очередях для виртуального интерфейса*

```
admin@neo:~$ show interfaces bonding bond0 vif 6 queue
qdisc pfifo_fast 0: root bands 3 priomap 1 2 2 2 1 2 0 0
1 1 1 1 1 1 1 1
 Sent 380009 bytes 5177 pkt (dropped 0, overlimits 0
requeues 0)
 rate 0bit 0pps backlog 0b 0p requeues 0
```

## 6.4.14. show interfaces ethernet <ethx> vif <идентификатор_vlan>

Вывод сведений о виртуальном интерфейсе Ethernet.

**Синтаксис**

**show interfaces ethernet** *ethx* **vif** *идентификатор_vlan*

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*ethx*

Идентификатор определяемого интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**.

*идентификатор_vlan*

Вывод сведений для указанного виртуального интерфейса.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Команда используется для отображения состояния управления и работоспособности виртуального интерфейса Ethernet.

**Примеры**

В примере 6.17 приведен вывод сведений для виртуального интерфейса vif 11, настроенного на интерфейсе eth0.

*Пример 6.17 - Вывод сведений для виртуального интерфейса Ethernet*

```
admin@neo:~$ show interfaces ethernet eth0 vif 11
eth0.11@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
qdisc noqueue
     link/ether 00:0c:29:da:3a:3d brd ff:ff:ff:ff:ff:ff
     inet6 fe80::20c:29ff:feda:3a3d/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
     2914      13      0       0       0          0
admin@neo:~$
```

## 6.4.15. show interfaces ethernet <ethx> vif <идентификатор_vlan> brief

Вывод кратких сведений о состоянии для виртуального интерфейса Ethernet.

**Синтаксис**

**show interfaces ethernet** *ethx* **vif** *идентификатор_vlan* **brief**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*ethx*

Идентификатор интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23** в зависимости от реально имеющихся в системе интерфейсов Ethernet.

*идентификатор_vlan*

Вывод сведений для указанного виртуального интерфейса.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Команда используется для отображения состояния виртуального интерфейса.

**Примеры**

В примере 6.18 приведен вывод кратких сведений о состоянии для интерфейса eth2.6.

*Пример 6.18 - Вывод кратких сведений о состоянии для виртуального интерфейса*

```
admin@neo:~$ show interfaces ethernet eth2 vif 6 brief
Interface IP Address     State   Link Description
eth2.6    10.1.6.66/24   up      up
```

## 6.4.16. show interfaces ethernet <ethx> vif <идентификатор_vlan> queue

Вывод сведений об очередях для виртуального интерфейса.

**Синтаксис**

```
show interfaces ethernet ethx vif идентификатор_vlan
queue [class | filter]
```

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*ethx*

Идентификатор интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23** в зависимости от реально имеющихся в системе интерфейсов Ethernet.

*идентификатор_vlan*

Вывод сведений для указанного виртуального интерфейса.

**class**

Отображение классов очередей для указанного интерфейса.

**filter**

Отображение фильтров очередей для указанного интерфейса.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Команда используется для вывода сведений об очередях для виртуального интерфейса.

**Примеры**

В примере 6.19 приведен вывод сведений для интерфейса eth0.6.

*Пример 6.19 - Вывод сведений об очередях для виртуального интерфейса*

```
admin@neo:~$ show interfaces ethernet eth0 vif 6 queue
qdisc pfifo_fast 0: root bands 3 priomap 1 2 2 2 1 2 0 0
1 1 1 1 1 1 1 1
 Sent 380009 bytes 5177 pkt (dropped 0, overlimits 0
requeues 0)
 rate 0bit 0pps backlog 0b 0p requeues 0
```

## 6.5. Настройка мостов

В данном разделе представлены следующие команды.

*Таблица 24 - Команды настройки мостов*

| Команды настройки | |
|---|---|
| Мостовые группы | |
| `interfaces bridge <brx>` | Определение мостовой группы. |
| `interfaces bridge <brx> address <адрес>` | 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> disable-link-detect` | Отключение определения изменений состояния физического канала для мостовой группы. |
| `interfaces bridge <brx> forwarding-delay <время_задержки>` | Установка времени задержки пересылки, в течение которого мостовая группа продолжает прослушивание после изменения топологии. |
| `interfaces bridge <brx>` | 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 <идентификатор_группы>` | 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 пути для интерфейса Ethernet, входящего в состав мостовой группы. |
| Виртуальные интерфейсы Ethernet | |
| `interfaces ethernet <ethx> vif <идентификатор_vlan> bridge-group bridge <идентификатор_группы>` | 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 пути для виртуального интерфейса Ethernet, входящего в состав мостовой группы. |
| Туннельные интерфейсы | |

| | |
|---|---|
| `interfaces tunnel <tunx> bridge-group bridge <идентификатор_группы>` | 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 bridge-group priority <приоритет>` | Установка приоритета пути для туннельного интерфейса GRE, входящего в состав мостовой группы. |
| Интерфейсы агрегированных каналов Ethernet | |
| `interfaces bonding <bondx> bridge-group bridge <идентификатор_группы>` | 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 пути для интерфейса агрегированных каналов Ethernet, входящего в состав мостовой группы. |
| Виртуальные интерфейсы агрегированных каналов Ethernet | |
| `interfaces bonding <bondx> vif <идентификатор_vlan> bridge-group bridge <идентификатор_группы>` | 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` | Установка приоритета пути 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. |

## 6.5.1. clear interfaces bridge counters

Очистка статистической информации для интерфейса моста.

**Синтаксис**

**clear interfaces bridge [***интерфейс***] counters**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*интерфейс*

Идентификатор интерфейса, для которого требуется очистить счетчики. В качестве интерфейса может быть указан интерфейс Ethernet, интерфейс агрегированных каналов Ethernet или виртуальный интерфейс Ethernet (идентификатор виртуального интерфейса указывается в формате **eth***x*.**vif***y*).

**Значение по умолчанию**

Статистические счетчики очищаются для интерфейсов всех мостов.

**Указания по использованию**

Команда используется для очистки статистических счетчиков для интерфейсов мостов. Если интерфейс Ethernet явно не указан, статистические счетчики очищаются для всех интерфейсов мостов. Просмотреть значения счетчиков можно при помощи команды **show interfaces counters**.

## 6.5.2. interfaces bonding <bondx> bridge-group bridge <идентификатор_группы>

Включение интерфейса агрегированных каналов Ethernet в состав мостовой группы.

**Синтаксис**

**set interfaces bonding** *bondx* **bridge-group bridge** *идентификатор_группы*

**delete interfaces bonding** *bondx* **bridge-group bridge**

**show interfaces bonding** *bondx* **bridge-group bridge**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    bonding bond0..bond99 {
        bridge-group {
            bridge br0..br999
        }
    }
}
```

**Параметры**

*bondx*

Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от **bond0** до **bond99**.

*идентификатор_группы*

Идентификатор мостовой группы, в состав которой требуется включить интерфейс. Поддерживаются идентификаторы 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.

### 6.5.3. 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 bond0..bond99 {
        bridge-group {
            cost [0-2147483647]
        }
    }
}
```

**Параметры**

*bondx*

Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от **bond0** до **bond99**.

*стоимость*

Стоимость пути для интерфейса, входящего в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 2147483647. Значение по умолчанию равно 19.

**Значение по умолчанию**

Значение стоимости пути равно 19.

**Указания по использованию**

Команда позволяет установить стоимость 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.

### 6.5.4. interfaces bonding <bondx> bridge-group priority <приоритет>

Установка приоритета пути 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 bond0..bond99 {
        bridge-group {
            priority [0-255]
        }
    }
}
```

**Параметры**

*bondx*

Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от **bond0** до **bond99**.

*приоритет*

Приоритет пути для интерфейса, входящего в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 255. Значение по умолчанию равно 128.

**Значение по умолчанию**

Приоритет равен 128.

**Указания по использованию**

Команда используется для назначения приоритета пути 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.

### 6.5.5. interfaces bonding <bondx> vif <идентификатор_vlan> bridge-group bridge <идентификатор_группы>

Включение виртуального интерфейса агрегированных каналов Ethernet в состав мостовой группы.

**Синтаксис**

**set interfaces bonding** *bondx* **vif** *идентификатор_vlan* **bridge-group bridge** *идентификатор_группы*

**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 bond0..bond99 {
        vif 0-4094 {
            bridge-group {
                bridge br0..br999
```

```
                    }
                }
            }
        }
```

**Параметры**

*bondx*

Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от **bond0** до **bond99**.

*идентификатор_vlan*

Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 0 до 4094.

*идентификатор_группы*

Идентификатор мостовой группы, в состав которой требуется включить интерфейс. Поддерживаются идентификаторы 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.

### 6.5.6. 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 bond0..bond99 {
        vif 0-4094 {
            bridge-group {
                cost [0-2147483647]
            }
        }
    }
}
```

**Параметры**

*bondx*

Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от **bond0** до **bond99**.

*идентификатор_vlan*

Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 0 до 4094.

*стоимость*

Стоимость пути для интерфейса, входящего в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 2147483647. Значение по умолчанию равно 19.

**Значение по умолчанию**

Значение стоимости пути равно 19.

**Указания по использованию**

Команда позволяет установить стоимость пути для виртуального 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.

### 6.5.7. interfaces bonding <bondx> vif <идентификатор_vlan> bridge-group priority <приоритет>

Установка приоритета пути 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 bond0..bond99 {
        vif 0-4094 {
            bridge-group {
                priority [0-255]
            }
        }
    }
```

}

**Параметры**

*bondx*

Идентификатор интерфейса агрегированных каналов Ethernet. Поддерживаются значения в диапазоне от **bond0** до **bond99**.

*идентификатор_vlan*

Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 0 до 4094.

*приоритет*

Приоритет пути для интерфейса, входящего в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 255. Значение по умолчанию равно 128.

**Значение по умолчанию**

Приоритет равен 128.

**Указания по использованию**

Команда позволяет назначить приоритет пути 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.

## 6.5.8. interfaces tunnel <tunx> bridge-group bridge <идентификатор_группы>

Включение туннельного интерфейса GRE в состав мостовой группы.

**Синтаксис**

**set interfaces tunnel** *tunx* **bridge-group bridge** *идентификатор_группы*

**delete interfaces tunnel** *tunx* **bridge-group bridge**

**show interfaces tunnel** *tunx* **bridge-group bridge**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    tunnel tun0..tun999 {
        bridge-group {
            bridge br0..br999
        }
    }
}
```

**Параметры**

*tunx*

Идентификатор туннельного интерфейса GRE. Поддерживаются значения в диапазоне от **tun0** до **tun999**.

*идентификатор_группы*

Идентификатор мостовой группы, в состав которой требуется включить интерфейс. Поддерживаются идентификаторы в диапазоне от **br0** до **br999**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Команда используется для включения туннельного интерфейса GRE в состав мостовой группы.

> *В состав сетевого моста могут быть включены только туннели GRE специального типа, созданные с использованием параметра **gre-bridge** команды **interfaces tunnel <tunx> encapsulation**. 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.

### 6.5.9. 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 tun0..tun999 {
          bridge-group {
               cost [1-65535]
          }
     }
}
```

**Параметры**

*tunx*

Идентификатор туннельного интерфейса GRE. Поддерживаются значения в диапазоне от **tun0** до **tun999**.

*стоимость*

Стоимость пути для интерфейса, входящего в состав мостовой группы. Значение должно лежать в диапазоне от 1 до 65535. Значение по умолчанию равно 19.

**Значение по умолчанию**

Значение стоимости пути равно 19.

**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.

### 6.5.10. interfaces tunnel <tunx> bridge-group bridge-group priority <приоритет>

Установка приоритета пути 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 tun0..tun999 {
        bridge-group {
            priority [1-255]
        }
    }
}
```

**Параметры**

*tunx*

Идентификатор туннельного интерфейса GRE. Поддерживаются значения в диапазоне от **tun0** до **tun999**.

*приоритет*

Приоритет пути для интерфейса, входящего в состав мостовой группы. Значение должно лежать в диапазоне от 1 до 255. Значение по умолчанию равно 128.

**Значение по умолчанию**

Приоритет равен 128.

**Указания по использованию**

Команда позволяет назначить приоритет пути 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.

## 6.5.11. 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 br0..br999 {
    }
}
```

**Параметры**

*brx*

Множественный узел. Идентификатор мостовой группы. Поддерживаются идентификаторы 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.

## 6.5.12. interfaces bridge <brx> address <адрес>

Назначение адреса мостовой группе.

**Синтаксис**

```
set interfaces bridge brx address адрес
delete interfaces bridge brx address адрес
show interfaces bridge brx address
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    bridge br0..br999 {
        address текст
    }
}
```

**Параметры**

*brx*

Идентификатор мостовой группы. Поддерживаются идентификаторы в диапазоне от **br0** до **br999.**

*адрес*

Множественный узел. IP-адрес и префикс сети для указанного интерфейса. Адрес должен быть указан либо в форме *ip-адрес/префикс*, либо **dhcp.** Если указано значение **dhcp,** IP-адрес и префикс сети будут получены с использованием протокола DHCP.

Чтобы назначить мостовой группе несколько IP-адресов, следует создать соответствующее количество узлов конфигурации **address** .

**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.

## 6.5.13. 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 br0..br999 {
        aging целоебеззнака32разр
    }
```

}

**Параметры**

*brx*

Идентификатор мостовой группы. Поддерживаются идентификаторы в диапазоне от **br0** до **br999.**

*время_хранения*

Интервал времени хранения, по истечении которого MAC-адрес удаляется из таблицы пересылки. Значение должно лежать в диапазоне от 1 до 4294967295. Значение по умолчанию 300.

**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.

## 6.5.14. 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 br0..br999 {
        description текст
    }
}
```

**Параметры**

*brx*

Идентификатор мостовой группы. Поддерживаются идентификаторы в диапазоне от **br0** до **br999.**

*описание*

Текстовое 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.

## 6.5.15. 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 br0..br999 {
        disable
    }
}
```

**Параметры**

*brx*

Идентификатор мостовой группы. Поддерживаются идентификаторы в диапазоне от **br0** до **br999**.

**disable**

Отключение моста на данной мостовой группы.

**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 значения, принятого по умолчанию для данной мостовой группы.

Форма **show** данной команды используется для просмотра настройки мостовой группы.

## 6.5.16. interfaces bridge <brx> disable-link-detect

Отключение определения изменений состояния физического канала для мостовой группы.

**Синтаксис**

**set interfaces bridge** *brx* **disable-link-detect**

**delete interfaces bridge** *brx* **disable-link-detect**

**show interfaces bridge** *brx*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    bridge br0..br999 {
        disable-link-detect
    }
}
```

**Параметры**

*brx*

Идентификатор мостовой группы. Поддерживаются идентификаторы в диапазоне от **br0** до **br999.**

**Значение по умолчанию**

На интерфейсе включено определение изменения состояния физического канала.

**Указания по использованию**

Команда используется для отключения определения изменения состояния канала для мостовой группы (например, когда сетевой кабель не подключен).

Форма **set** данной команды используется для отключения определение изменений состояния физического канала.

Форма **delete** данной команды используется для включения определения изменений состояния физического канала.

Форма **show** данной команды используется для просмотра настройки мостовой группы.

## 6.5.17. 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 br0..br999 {
        forwarding-delay целоебеззнака32разр
    }
}
```

**Параметры**

*brx*

Идентификатор мостовой группы. Поддерживаются идентификаторы в диапазоне от **br0** до **br999.**

*время_задержки*

Интервал времени, в секундах, в течение которого мост находится в состоянии прослушивания сведений о топологии связующего дерева после изменения топологии. Значение должно лежать в диапазоне от 1 до 4294967295. Значение по умолчанию равно 15.

**Значение по умолчанию**

Перед переходом в режим пересылки мост находится в состоянии прослушивания в течение 15 секунд.

**Указания по использованию**

Команда используется для установки интервала времени, в течение которого мост находится в состоянии прослушивания после изменения топологии.

После изменения топологии сети сетевой мост 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 мост 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.

## 6.5.18. 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 br0..br999 {
        hello-time целоебеззнака32разр
    }
}
```

**Параметры**

*brx*

Идентификатор мостовой группы. Поддерживаются идентификаторы в диапазоне от **br0** до **br999.**

*интервал*

Интервал времени, в секундах, через который данный сетевой мост будет передавать пакеты "hello". Значение должно лежать в диапазоне от 1 до 4294967295. Значение по умолчанию равно 2.

**Значение по умолчанию**

Значение по умолчанию равно 2.

**Указания по использованию**

Команда используется для установки интервала времени, через который сетевой мост 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 мостом, который 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".

### 6.5.19. 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 br0..br999 {
        max-age целоебеззнака32разр
    }
}
```

**Параметры**

*brx*

Идентификатор мостовой группы. Поддерживаются идентификаторы в диапазоне от **br0** до **br999.**

*интервал*

Интервал, в течение которого мостовая группа ожидает получения пакета

"hello" перед перевычислением топологии связующего дерева. Значение должно лежать в диапазоне от 1 до 4294967295. Значение по умолчанию равно 20.

**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".

## 6.5.20. 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 br0..br999 {
        priority целоебеззнака32разр
    }
```

}

**Параметры**

*brx*

Идентификатор мостовой группы. Поддерживаются идентификаторы в диапазоне от **br0** до **br999.**

*приоритет*

Приоритет пересылки сетевого моста в рамках связующего дерева. Чем меньше установленное значение, тем больший приоритет имеет сетевой мост. По умолчанию установлено значение 0, определяющее наивысший приоритет.

**Значение по умолчанию**

Значение по умолчанию равно 0.

**Указания по использованию**

Команда используется для установки приоритета пересылки данного моста 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.

## 6.5.21. 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 br0..br999 {
        stp [true|false]
    }
}
```

**Параметры**

*brx*

Идентификатор мостовой группы. Поддерживаются идентификаторы в диапазоне от **br0** до **br999.**

*состояние*

Позволяет включить или отключить протокол STP для указанного моста. Поддерживаемые значения:

**true**: Включение протокола STP для данного моста.

**false**: Выключение протокола STP для данного моста.

По умолчанию принято значение **false**.

**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 данного интерфейса.

Форма **delete** данной команды используется для восстановления значения, принятого по умолчанию.

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

## 6.5.22. interfaces ethernet <ethx> bridge-group bridge <идентификатор_группы>

Включение интерфейса Ethernet в состав мостовой группы.

**Синтаксис**

**set interfaces ethernet** *ethx* **bridge-group bridge** *идентификатор_группы*

**delete interfaces ethernet** *ethx* **bridge-group bridge**

**show interfaces ethernet** *ethx* **bridge-group bridge**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    ethernet eth0..eth23 {
        bridge-group {
            bridge br0..br999
        }
    }
}
```

**Параметры**

*ethx*

Интерфейс Ethernet, который требуется включить в состав мостовой группы. Поддерживаются значения в диапазоне от **eth0** до **eth23**. Интерфейс должен быть заранее определен.

*идентификатор_группы*

Идентификатор мостовой группы, в состав которой требуется включить интерфейс. Поддерживаются идентификаторы 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.

## 6.5.23. 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 eth0..eth23 {
          bridge-group {
               cost [0-2147483647]
          }
     }
}
```

**Параметры**

*ethx*

Интерфейс Ethernet, который требуется включить в состав мостовой группы. Поддерживаются значения в диапазоне от **eth0** до **eth23.** Интерфейс должен быть заранее определен.

*стоимость*

Стоимость пути для интерфейса, входящего в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 2147483647. Значение по

умолчанию равно 19.

**Значение по умолчанию**

Значение стоимости пути равно 19.

**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.

## 6.5.24. interfaces ethernet <ethx> bridge-group priority <приоритет>

Установка приоритета пути 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 eth0..eth23 {
        bridge-group {
            priority [0-255]
        }
    }
}
```

**Параметры**

*ethx*

Интерфейс Ethernet, который требуется включить в состав мостовой группы. Поддерживаются значения в диапазоне от **eth0** до **eth23.** Интерфейс должен быть заранее определен.

*приоритет*

Приоритет пути для интерфейса, входящего в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 255. Значение по умолчанию равно 128.

**Значение по умолчанию**

Приоритет равен 128.

**Указания по использованию**

Команда позволяет установить приоритет пути для интерфейса Ethernet.

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.

## 6.5.25. interfaces ethernet <ethx> vif <идентификатор_vlan> bridge-group bridge <идентификатор_группы>

Включение виртуального интерфейса в состав мостовой группы.

**Синтаксис**

**set interfaces ethernet** *ethx* **vif** *идентификатор_vlan* **bridge-group bridge** *идентификатор_группы*

**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 eth0..eth23 {
```

```
                vif 0-4095 {
                     bridge-group {
                          bridge br0..br999
                     }
                }
           }
      }
```

**Параметры**

*ethx*

Интерфейс Ethernet, на базе которого создан виртуальный интерфейс. Поддерживаются значения в диапазоне от **eth0** до **eth23.** Интерфейс должен быть заранее определен.

*идентификатор_vlan*

Идентификатор виртуального интерфейса, который требуется включить в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 4095. Виртуальный интерфейс должен быть заранее определен.

*идентификатор_группы*

Идентификатор мостовой группы, в состав которой требуется включить интерфейс. Поддерживаются идентификаторы 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.

### 6.5.26. 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 eth0..eth23 {
        vif 0-4095 {
            bridge-group {
                cost [0-2147483647]
            }
        }
    }
}
```

**Параметры**

*ethx*

Интерфейс Ethernet, на базе которого создан виртуальный интерфейс. Поддерживаются значения в диапазоне от **eth0** до **eth23.** Интерфейс должен быть заранее определен.

*идентификатор_vlan*

Идентификатор виртуального интерфейса, который требуется включить в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 4095.

*стоимость*

Стоимость виртуального интерфейса, входящего в состав сетевого моста. Значение должно лежать в диапазоне от 0 до 2147483647. Значение по умолчанию равно 19.

**Значение по умолчанию**

Значение стоимости пути равно 19.

**Указания по использованию**

Команда позволяет установить стоимость пути для виртуального интерфейса Ethernet, входящего в состав мостовой группы.

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.

## 6.5.27. interfaces ethernet <ethx> vif <идентификатор_vlan> bridge-group priority <приоритет>

Установка приоритета пути 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 eth0..eth23 {
        vif 0-4095 {
            bridge-group {
                priority 0-255
```

```
                    }
                }
            }
        }
```

**Параметры**

*ethx*

Интерфейс Ethernet, на базе которого создан виртуальный интерфейс. Поддерживаются значения в диапазоне от **eth0** до **eth23**. Интерфейс должен быть заранее определен.

*идентификатор_vlan*

Идентификатор виртуального интерфейса, который требуется включить в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 4095.

*приоритет*

Приоритет виртуального интерфейса, входящего в состав мостовой группы. Значение должно лежать в диапазоне от 0 до 255. Значение по умолчанию равно 128.

**Значение по умолчанию**

Приоритет равен 128.

**Указания по использованию**

Команда позволяет установить приоритет пути 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.

## 6.5.28. show bridge

Вывод сведений об активных мостовых группах.

**Синтаксис**

**show bridge [***мостовая_группа* **[macs | spanning-tree]]**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*мостовая_группа*

Отображение сведений для указанной мостовой группы, значение должно лежать в диапазоне от **br0** до **br999.**

**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.

## 6.5.29. show interfaces bridge

Вывод сведений об интерфейсе сетевого моста.

**Синтаксис**

**show interfaces bridge [***мостовая_группа* **[brief] | detail]**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*мостовая_группа*

Отображение сведений для указанной мостовой группы, значение должно лежать в диапазоне от **br0** до **br999.**

**brief**

Вывод кратких сведений для указанной мостовой группы.

**detail**

Вывод подробных сведений об интерфейсе моста.

**Указания по использованию**

Команда используется для вывода сведений о настроенных интерфейсах мостов.

При использовании команды без параметров отображаются сведения обо всех активных интерфейсах мостов. Если указан идентификатор мостовой группы, сведения отображаются только для указанной мостовой группы.

## 6.6. Настройка беспроводных интерфейсов

Интерфейс беспроводной локальной сети (WLAN) обеспечивает поддержку спецификации беспроводной сети 802.11 (часть называемой Wi-Fi) при помощи совместимого оборудования. При наличии поддержки со стороны оборудования подсистема беспроводной сети Altell NEO может обеспечивать поддержку нескольких интерфейсов на одно физическое устройство.

Режим работы беспроводного интерфейса - это беспроводная точка доступа (или просто "точка доступа").

В данном разделе приведены следующие команды:

*Таблица 25 - Команды настройки беспроводных интерфейсов*

| Команды настройки | |
|---|---|
| `interfaces wireless <wlanx>` | Определение беспроводного интерфейса. |
| `interfaces wireless <wlanx> address` | Установка IP-адреса и префикса подсети для беспроводного интерфейса. |
| `interfaces wireless <wlanx> channel <канал>` | Установка канала для использования беспроводным интерфейсом. |
| `interfaces wireless <wlanx> country <страна>` | Установка страны, в которой развертывается беспроводной интерфейс. |
| `interfaces wireless <wlanx> description <описание>` | Ввод описания для беспроводного интерфейса. |
| `interfaces wireless <wlanx> disable-broadcast-ssid` | Установка режима без вещания имени сети (SSID) для беспроводного интерфейса. |

| | |
|---|---|
| `interfaces wireless <wlanx> disable-link-detect` | Отключение определения изменения состояния физического канала для беспроводного интерфейса. |
| `interfaces wireless <wlanx> mac <mac-адрес>` | Установка MAC-адреса для беспроводного интерфейса. |
| `interfaces wireless <wlanx> mode <режим>` | Установка режима 802.11 для беспроводного интерфейса. |
| `interfaces wireless <wlanx> physical-device <устройство>` | Связывание физического устройства с беспроводным интерфейсом. |
| `interfaces wireless <wlanx> security wpa` | Установка шифра для шифрования WPA. |
| `interfaces wireless <wlanx> ssid <имя_сети>` | Ввод имени сети (SSID) для беспроводного интерфейса. |
| `interfaces wireless <wlanx> type <тип>` | Указание типа беспроводного устройства для беспроводного интерфейса. |
| Эксплуатационные команды | |
| `show interfaces wireless` | Отображение состояния и статистики для беспроводных интерфейсов. |
| `show interfaces wireless <wlanx>` | Отображение состояния и статистики для беспроводного интерфейса. |
| `show interfaces wireless <wlanx> brief` | Отображение краткой сводки состояния для беспроводного интерфейса. |
| `show interfaces wireless <wlanx> capture` | Перехват и отображение трафика на беспроводном интерфейсе. |
| `show interfaces wireless <wlanx> queue` | Отображение сведений об очередях для беспроводного интерфейса. |
| `show interfaces wireless <wlanx> scan` | Поиск доступных беспроводных сетей. |
| `show interfaces wireless <wlanx> stations` | Отображение сведений о рабочих станциях, подключенных по радио к беспроводному интерфейсу. |

## 6.6.1. Настройка беспроводной точки доступа

В примере, приводимом в данном разделе, выполняется создание беспроводной точки доступа. Точка доступа имеет следующие характеристики:

- IP-адрес 192.168.40.1/24;
- Имя сети (**ssid**) “Testsec”;
- Ключевая фраза WPA “12345678”;
- Используется протокол 802.11n;
- Работа происходит на канале 1.

В этом примере используется физическое устройство по умолчанию (**phy0**) и автоматически создается MAC-адрес.

> ***ПРИМЕЧАНИЕ*** *При настройке нескольких интерфейсов в режиме беспроводной точки доступа необходимо указать уникальные IP-адреса, каналы, имена сетей (SSID) и MAC-адреса.*

Для создания беспроводной точки доступа нужно выполнить следующие действия:

*Пример 6.20 - Настройка точки доступа*

| Действие | Команда |
|---|---|
| Создание беспроводного интерфейса и указание его типа как беспроводной точки доступа. | `admin@R1# set interfaces wireless wlan0 type access-point [edit]` |
| Указание IP-адреса. | `admin@R1# set interfaces wireless wlan0 address 192.168.40.1/24 [edit]` |
| Указание имени сети. | `admin@R1# set interfaces wireless wlan0 ssid Testsec [edit]` |
| Указание кодовой фразы WPA. | `admin@R1# set wireless wlan0 security wpa interfaces passphrase “12345678”` |

```
[edit]
```

Указание режима 802.11.

```
admin@R1# set interfaces wireless
wlan0 mode n
[edit]
```

Указание канала.

```
admin@R1# set interfaces wireless
wlan0 channel 1
[edit]
```

Фиксация изменений.

```
admin@R1# commit
[edit]
```

Отображение настройки.

```
admin@R1# show interfaces
wireless
wireless wlan0 {
     address 192.168.40.1/24
channel 1 mode n security {
          wpa {
               passphrase "Test
phrase"
          }
     }
ssid Test type access-point
}
[edit]
```

### 6.6.2. interfaces wireless <wlanx>

Определение беспроводного интерфейса.

**Синтаксис**

**set interfaces wireless** *wlanx*

**delete interfaces wireless** *wlanx*

**show interfaces wireless** *wlanx*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    wireless wlan0..wlan999
        { }
}
```

**Параметры**

*wlanx*

Обязательный. Множественный узел. Идентификатор беспроводного интерфейса. Значение должно лежать в диапазоне от **wlan0** до **wlan999**.

Можно определить несколько беспроводных интерфейсов, создав несколько узлов конфигурации wireless.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для настройки беспроводного интерфейса. Можно определить несколько беспроводных интерфейсов, создав несколько узлов конфигурации **wireless**.

> ***ПРИМЕЧАНИЕ*** *Создание нескольких узлов конфигурации wireless на одном и том же физическом устройстве поддерживается для некоторых сочетаний драйверов и оборудования.*

Следует заметить, что для изменения имени беспроводного интерфейса нельзя использовать команду **set**. Для изменения имени беспроводного интерфейса необходимо удалить старый узел конфигурации **wireless** и создать новый.

Форма **set** этой команды используется для создания беспроводного интерфейса. После создания интерфейса его состояние можно просмотреть с помощью команды **show interfaces wireless**.

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

беспроводного интерфейса.

Форма **show** используется для просмотра настройки беспроводного интерфейса.

### 6.6.3. interfaces wireless <wlanx> address

Установка IP-адреса и префикса подсети для беспроводного интерфейса.

**Синтаксис**

```
set interfaces wireless wlanx address {ipv4-адрес | ipv6-адрес | dhcp}
delete interfaces wireless wlanx address {ipv4-адрес | ipv6-адрес | dhcp}
show interfaces wireless wlanx address
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    wireless wlan0..wlan999 {
        address [ipv4-адрес|ipv6-адрес|dhcp]
    }
}
```

**Параметры**

*wlanx*

Идентификатор беспроводного интерфейса. Значение должно лежать в диапазоне от **wlan0** до **wlan999**.

*ipv4-адрес*

Множественный узел. IPv4-адрес для данного интерфейса. Используется формат ip-адрес/префикс (например, 192.168.1.77/24). Можно определить несколько IP-адресов для одного интерфейса, создав соответствующее количество узлов конфигурации address.

*ipv6-адрес*

Множественный узел. IPv6-адрес для данного интерфейса. Для указания адреса используется формат ipv6-адрес/префикс (например,

2001:db8:1234::/48). Можно определить несколько IPv6-адресов для одного интерфейса, создав соответствующее количество узлов конфигурации **address**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для установки IP-адреса и префикса подсети для беспроводного интерфейса.

Форма **set** этой команды используется для установки IP-адреса и префикса подсети. Для назначения интерфейсу нескольких IP-адресов следует создать соответствующее количество узлов конфигурации address.

Форма **delete** этой команды используется для удаления настройки IP-адреса.

Форма **show** этой команды используется для просмотра настройки IP-адреса.

### 6.6.4. interfaces wireless <wlanx> channel <канал>

Установка канала для использования беспроводным интерфейсом.

**Синтаксис**

```
set interfaces wireless wlanx channel канал
delete interfaces wireless wlanx channel канал
show interfaces wireless wlanx channel
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    wireless wlan0..wlan999 {
        channel целоебеззнака32разр
    }
}
```

**Параметры**

*wlanx*

Идентификатор беспроводного интерфейса. Значение должно лежать в диапазоне от **wlan0** до **wlan999**.

*канал*

Канал, который должен использоваться интерфейсом. Значение должно лежать в диапазоне от 1 до 14. По умолчанию канал выбирается оборудованием.

**Значение по умолчанию**

Канал выбирается беспроводным оборудованием.

**Указания по использованию**

Эта команда используется для установки канала для беспроводного интерфейса. Для интерфейсов, у которых для параметра **type** установлено значение **access-point**, канал необходимо установить явно с помощью данной команды.

Форма **set** этой команды используется для установки канала.

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

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

### 6.6.5. interfaces wireless <wlanx> country <страна>

Установка страны, в которой развертывается беспроводной интерфейс.

**Синтаксис**

```
set interfaces wireless wlanx country страна
delete interfaces wireless wlanx country страна
show interfaces wireless wlanx country
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    wireless wlan0..wlan999 {
        country текст
    }
}
```

**Параметры**

*wlanx*

Идентификатор беспроводного интерфейса. Значение должно лежать в

диапазоне от **wlan0** до **wlan999**.

*страна*

Обозначение страны, в которой развертывается беспроводной интерфейс. Значение является двухбуквенным кодом страны по стандарту ISO с номером 639. Примеры: US, EU, JP). Значением по умолчанию является RU.

**Значение по умолчанию**

По умолчанию код страны RU.

**Указания по использованию**

Эта команда используется для установки страны, в которой развертывается беспроводной интерфейс. Это позволяет контролировать использование частот и выходной мощности на основе нормативных требований для указанной страны.

Форма **set** этой команды используется для установки страны.

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

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

### 6.6.6. interfaces wireless <wlanx> description <описание>

Ввод описания для беспроводного интерфейса.

**Синтаксис**

**set interfaces wireless** *wlanx* **description** *описание*

**delete interfaces wireless** *wlanx* **description**

**show interfaces wireless** *wlanx* **description**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    wireless wlan0..wlan999 {
        description текст
    }
}
```

**Параметры**

*wlanx*

Идентификатор беспроводного интерфейса. Значение должно лежать в диапазоне от **wlan0** до **wlan999**.

*описание*

Мнемоническое имя или описание беспроводного интерфейса.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для установки описания для беспроводного интерфейса.

Форма **set** этой команды используется для ввода описания.

Форма **delete** этой команды используется для удаления этого описания.

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

## 6.6.7. interfaces wireless <wlanx> disable-broadcast-ssid

Установка режима без вещания имени сети (SSID) для беспроводного интерфейса.

**Синтаксис**

**set interfaces wireless** *wlanx* **disable-broadcast-ssid**

**delete interfaces wireless** *wlanx* **disable-broadcast-ssid**

**show interfaces wireless** *wlanx* **disable-broadcast-ssid**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    wireless wlan0..wlan999 {
        disable-broadcast-ssid
    }
}
```

**Параметры**

*wlanx*

Идентификатор беспроводного интерфейса. Значение должно лежать в диапазоне от **wlan0** до **wlan999**.

**Значение по умолчанию**

Имя сети (SSID) вещается.

**Указания по использованию**

Эта команда используется для отключения вещания имени сети (SSID) беспроводным интерфейсом. Отключение передачи имени сети обычно используется для сокрытия беспроводной точки доступа.

> ***ПРИМЕЧАНИЕ*** *Этот параметр допустим только в случае, когда интерфейс настроен как беспроводная точка доступа (то есть значение type есть access-point).*

Форма **set** этой команды используется для отключения вещания имени сети.

Форма **delete** этой команды используется для включения вещания имени сети.

Форма **show** этой команды используется, чтобы увидеть, включено вещание имени сети или нет.

## 6.6.8. interfaces wireless <wlanx> disable-link-detect

Отключение определения изменения состояния физического канала для беспроводного интерфейса.

**Синтаксис**

```
set interfaces wireless wlanx disable-link-detect
delete interfaces wireless wlanx disable-link-detect
show interfaces wireless wlanx
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    wireless wlan0..wlan999 {
        disable-link-detect
    }
}
```

**Параметры**

*wlanx*

Идентификатор беспроводного интерфейса. Значение должно лежать в диапазоне от **wlan0** до **wlan999**.

**Значение по умолчанию**

Интерфейс, на котором определяются изменения состояния физического канала.

**Указания по использованию**

Эта команда используется для отмены определения изменения физического состояния на беспроводном канале.

***ПРИМЕЧАНИЕ*** *Этот параметр допустим только в случае, когда интерфейс настроен как беспроводная точка доступа.*

Форма **set** этой команды используется для отключения определения изменений физического состояния.

Форма **delete** этой команды используется для включения определения изменений физического состояния.

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

## 6.6.9. interfaces wireless <wlanx> mac <mac-адрес>

Установка MAC-адреса для беспроводного интерфейса.

**Синтаксис**

**set interfaces wireless** *wlanx* **mac** *mac-адрес*

**delete interfaces wireless** *wlanx* **mac**

**show interfaces wireless** *wlanx* **mac**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    wireless wlan0..wlan999 {
        mac mac-адрес
```

```
        }
    }
```

**Параметры**

*wlanx*

Идентификатор беспроводного интерфейса. Значение должно лежать в диапазоне от **wlan0** до **wlan999**.

*mac-адрес*

MAC-адрес для беспроводного интерфейса. Формат адреса - шесть 8-битовых шестнадцатеричных чисел, разделенных двоеточиями, например, 00:0a:59:9a:f2:ba.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для установки MAC-адреса для беспроводного интерфейса. В режиме точки доступа каждый беспроводной интерфейс должен иметь уникальный MAC-адрес.

Формат **set** этой команды используется для указания MAC-адреса.

Форма **delete** этой команды используется для удаления MAC-адреса.

Форма **show** этой команды используется для просмотра настройки MAC-адреса.

## 6.6.10. interfaces wireless <wlanx> mode <режим>

Установка режима 802.11 для беспроводного интерфейса.

**Синтаксис**

**set interfaces wireless** *wlanx* **mode** *режим*

**delete interfaces wireless** *wlanx* **mode**

**show interfaces wireless** *wlanx* **mode**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    wireless wlan0..wlan999 {
```

```
            mode [a|b|g|n]
        }
    }
```

**Параметры**

*wlanx*

Идентификатор беспроводного интерфейса. Значение должно лежать в диапазоне от **wlan0** до **wlan999**.

*режим*

Буква, означающая режим 802.11, который должен использоваться беспроводным интерфейсом.

Поддерживаются следующие значения:

**a**: Работа в соответствии с поправкой IEEE 802.11a-1999 к спецификации 802.11 (54 Мбит/с по полосе 5 ГГц).

**b**: Работа в соответствии с поправкой IEEE 802.11b-1999 к спецификации 802.11 (11 Мбит/с по полосе 2,4 ГГц).

**g**: Работа в соответствии со спецификацией IEEE 802.11g-2003 (54 Мбит/с по полосе 2,4 ГГц).

**n**: Работа в соответствии со спецификацией IEEE 802.11n-2009 (до 600 Мбит/с с четырьмя пространственными потоками по каналам шириной 40 МГц).

**Значение по умолчанию**

Интерфейс работает в соответствии со спецификацией IEEE 802.11g-2003.

**Указания по использованию**

Эта команда используется для установки режима 802.11 для беспроводного интерфейса. Стандарт IEEE 802.11 выдержал несколько редакций и дополнений, называемых 802.11a, 802.11b и т.д.

> ***ПРИМЕЧАНИЕ*** *Этот параметр допустим только в случае, когда интерфейс настроен как беспроводная точка доступа (то есть значение type есть access-point).*

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

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

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

### 6.6.11. interfaces wireless <wlanx> physical-device <устройство>

Связывание физического устройства с беспроводным интерфейсом.

**Синтаксис**

**set interfaces wireless** *wlanx* **physical-device** *устройство*

**delete interfaces wireless** *wlanx* **physical-device**

**show interfaces wireless** *wlanx* **physical-device**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    wireless wlan0..wlan999 {
        physical-device текст
    }
}
```

**Параметры**

*wlanx*

Идентификатор беспроводного интерфейса. Значение должно лежать в диапазоне от wlan0 до wlan999.

*устройство*

Идентификатор, представляющий физическое устройство, которое следует связать с беспроводным интерфейсом. Значение должно лежать в диапазоне от **phy0** до **phy9**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для указания физического устройства, связанного с беспроводным интерфейсом.

Это значение является необязательным для первого беспроводного интерфейса на устройстве, но необходимо, если имеется более одного физического устройства.

Форма **set** этой команды используется для указания физического устройства, связанного с беспроводным интерфейсом.

Форма **delete** этой команды используется для удаления описания физического устройства.

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

## 6.6.12. interfaces wireless <wlanx> security wpa

Установка шифра для шифрования WPA.

**Синтаксис**

**set interfaces wireless** *wlanx* **security wpa** [**cipher** *шифр* | **mode** *режим* | **passphrase** *кодовая_фраза* | **x509-cert** *имя_сертификата*]

**delete interfaces wireless** *wlanx* **security wpa** [**cipher** | **mode** | **passphrase** | **x509-cert**]

**show interfaces wireless** *wlanx* **security wpa** [**cipher** | **mode** | **passphrase** | **x509-cert**]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    wireless wlan0..wlan999 {
        security {
            wpa {
                cipher текст
                mode текст
                passphrase текст
            }
        }
    }
}
```

**Параметры**

*wlanx*

Идентификатор беспроводного интерфейса. Значение должно лежать в диапазоне от **wlan0** до **wlan999**.

*шифр*

Алгоритм шифрования, который должен использоваться для вещательных и многоадресных кадров в режиме WPA. Следует обратить внимание, что значение типа шифрования, указанное здесь, используется только в том случае, если используется режим WPA, но не WPA2; в режиме WPA2 всегда используется шифрование CCMP. Поддерживаются следующие значения:

**CCMP**: использует AES в режиме счетчика с CBC-MAC, в соответствии со спецификациями RFC 3610 и IEEE 802.11i/D7.0.

**TKIP**: не поддерживается. По умолчанию CCMP.

*режим*

Режим WPA, требуемый для беспроводного интерфейса. Поддерживаются следующие значения:

**wpa**: требуется режим WPA в соответствии со спецификацией IEEE 802.11i/D3.

**wpa2**: требуется WPA2, то есть полная спецификация IEEE 802.11i/RSN.

**both**: допускаются и WPA, и WPA2. Значением по умолчанию является **both**.

*кодовая_фраза*

Строка, которая должна использоваться в качестве общей кодовой фразы WPA для беспроводного интерфейса. Кодовая фраза должна содержать от 8 до 63 печатаемых символов. Кодовая фраза, содержащая пробелы, должна быть заключена в кавычки.

*имя_сертификата*

Строка, которая должна содержать имя действенного X.509 сертификата с открытым ключом ГОСТ Р 34.10-2001. При задании сертификата автоматически включается использование EAP-TLS метода IEEE 802.1x авторизации. Сертификат должен быть создан или импортирован ранее в систему управления ключами, узел **pki**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для включения безопасности WPA на беспроводном интерфейсе и для указания параметров WPA.

Следует обратить внимание, что при включенном WPA интерфейс может либо пользоваться кодовой фразой в качестве ключа шифрования (при помощи параметра **passphrase**).

***ПРИМЕЧАНИЕ*** *Используется только WPA.*

Форма **set** этой команды используется для включения шифрования WPA и установки параметров WPA.

Форма **delete** этой команды используется для отключения шифрования WPA и удаления настройки WPA.

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

## 6.6.13. interfaces wireless <wlanx> ssid <имя_сети>

Ввод имени сети (SSID) для беспроводного интерфейса.

**Синтаксис**

**set interfaces wireless** *wlanx* **ssid** *имя_сети*

**delete interfaces wireless** *wlanx* **ssid**

**show interfaces wireless** *wlanx* **ssid**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    wireless wlan0..wlan999 {
        ssid текст
    }
}
```

**Параметры**

*wlanx*

Идентификатор беспроводного интерфейса. Значение должно лежать в диапазоне от wlan0 до wlan999.

*имя_сети*

Имя сети (SSID) для беспроводного интерфейса. Имя сети, содержащее пробелы, должно быть заключено в кавычки.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для указания имени сети (SSID) для беспроводного интерфейса. Этот маркет необходим для идентификации беспроводной сети; установка этого параметра обязательна. Число имен сетей, которые можно установить на интерфейсе, зависит от используемого оборудования.

Форма **set** этой команды используется для ввода имени сети.

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

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

## 6.6.14. interfaces wireless <wlanx> type <тип>

Указание типа беспроводного устройства для беспроводного интерфейса.

**Синтаксис**

**set interfaces wireless** *wlanx* **type** *тип*

**delete interfaces wireless** *wlanx* **type**

**show interfaces wireless** *wlanx* **type**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    wireless wlan0..wlan999 {
        type [access-point | monitor | station] } }
```

**Параметры**

*wlanx*

Идентификатор беспроводного интерфейса. Значение должно лежать в диапазоне от wlan0 до wlan999.

*тип*

Тип беспрводного устройства для данного беспроводного интерфейса. Поддерживаются следующие значения:

**access-point**: беспроводной интерфейс обеспечивает беспроводной доступ к сети для клиентов.

**monitor**: беспроводной интерфейс осуществляет пассивное наблюдение за беспроводным трафиком.

**station**: беспроводной интерфейс работает в качестве клиента беспроводной сети.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для указания типа беспроводного устройства для беспроводного интерфейса. Установка этого параметра обязательна. Для интерфейсов, настроенных как **access-point**, доступен только режим моста.

Формат **set** этой команды используется для указания типа устройства для беспроводного интерфейса.

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

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

## 6.6.15. show interfaces wireless

Отображение состояния и статистики для беспроводных интерфейсов.

**Синтаксис**

```
show interfaces wireless [detail | info]
```

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**detail**

Отображение подробных сведений о состоянии и статистики для всех беспроводных интерфейсов.

**info**

Отображение сведений о всех беспроводных интерфейсах, присущих только беспроводным сетям.

**Значение по умолчанию**

Отображаются сведения для всех беспроводных интерфейсах.

**Указания по использованию**

Эта команда используется для просмотра состояния работоспособности беспроводных интерфейсов.

**Примеры**

В примере 6.21 приведен вывод сведений для всех беспроводных интерфейсов.

*Пример 6.21 - Отображение сведений о беспроводных интерфейсах*

```
admin@neo:~$ show interfaces wireless
Interface IP Address      State Link Description
wlan0     192.168.40.1/24 up    up
```

В примере 6.22 приведен вывод подробных сведений для всех беспроводных интерфейсов.

*Пример 6.22 - Отображение подробных сведений о беспроводных интерфейсах*

```
admin@neo:~$ show interfaces wireless detail
wlan0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc
pfifo_fast state DOWN0link/ether 00:21:91:d1:18:ca brd
ff:ff:ff:ff:ff:ff
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
```

В примере 6.23 приведен вывод характерных для беспроводной связи сведений для всех беспроводных интерфейсов.

*Пример 6.23 - Отображение характерных для беспроводной связи сведений для всех беспроводных интерфейсов*

```
admin@neo:~$ show interfaces wireless info
Interface    Type              SSID
Channel
wlan0        managed           -                    ?
```

```
admin@neo:~$
```

### 6.6.16. show interfaces wireless <wlanx>

Отображение состояния и статистики для беспроводного интерфейса.

**Синтаксис**

**show interfaces wireless** *wlanx*

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*wlanx*

Идентификатор беспроводного интерфейса. Значение должно лежать в диапазоне от **wlan0** до **wlan999**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для просмотра состояния и статистики для указанного беспроводного интерфейса.

**Примеры**

В примере 6.24 приведен вывод состояния и статистики для интерфейса wlan0.

*Пример 6.24 - Отображение состояния и статистики для конкретного беспроводного интерфейса*

```
admin@neo:~$ show interfaces wireless wlan0

wlan0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc
pfifo_fast state DOWN0link/ether 00:21:91:d1:18:ca brd
ff:ff:ff:ff:ff:ff

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
```

### 6.6.17. show interfaces wireless <wlanx> brief

Отображение краткой сводки состояния для беспроводного интерфейса.

**Синтаксис**

**show interfaces wireless** *wlanx* **brief**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*wlanx*

Идентификатор беспроводного интерфейса. Значение должно лежать в диапазоне от **wlan0** до **wlan999**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для отображения кратких сведений о состоянии и статистики для указанного беспроводного интерфейса.

**Примеры**

В примере 6.25 приведен вывод кратких сведений о состоянии для интерфейса **wlan0**.

*Пример 6.25 - Отображение сводки состояния для беспроводного интерфейса*

```
admin@neo:~$ show interfaces wireless wlan0 brief

Interface IP Address State Link Description wlan0
192.168.40.1/24 up up
```

## 6.6.18. show interfaces wireless <wlanx> capture

Перехват и отображение трафика на беспроводном интерфейсе.

**Синтаксис**

**show interfaces wireless** *wlanx* **capture**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*wlanx*

Идентификатор беспроводного интерфейса. Значение должно лежать в диапазоне от **wlan0** до **wlan999**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для перехвата трафика на указанном беспроводном интерфейсе. Для того чтобы остановить вывод, нажмите

<Ctrl>+c.

**Примеры**

В примере 6.26 приведены перехваченные данные на интерфейсе **wlan0**.

*Пример 6.26 - Отображение перехваченных данных*

```
admin@neo:~$ show interfaces wireless wlan0 capture

Capturing traffic on wlan0 ... 0.000000
fe80::ad08:8661:4d:b925 -> ff02::c SSDP M-SEARCH *
HTTP/1.1 0.000067 fe80::69ca:5c11:bcf6:29da -> ff02::c
SSDP M-SEARCH * HTTP/1.1 2.608804
fe80::8941:71ef:b55d:e348 -> ff02::1:2 DHCPv6 Solicit
3.010862 fe80::ad08:8661:4d:b925 -> ff02::c SSDP M-SEARCH
* HTTP/1.1 3.010901 fe80::69ca:5c11:bcf6:29da -> ff02::c
SSDP M-SEARCH * HTTP/1.1 4.568357 192.168.1.254 ->
238.255.255.251 SSDP NOTIFY * HTTP/1.1 4.568372
192.168.1.254 -> 238.255.255.251 SSDP NOTIFY * HTTP/1.1
```

## 6.6.19. show interfaces wireless <wlanx> queue

Отображение сведений об очередях для беспроводного интерфейса.

**Синтаксис**

**show interfaces wireless** *wlanx* **queue** [**class** | **filter**]

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*wlanx*

Идентификатор беспроводного интерфейса. Значение должно лежать в диапазоне от **wlan0** до **wlan999**.

*class*

Отображение классов очередей для указанного интерфейса.

*filter*

Отображение фильтров очередей для указанного интерфейса.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для просмотра сведений об очередях для беспроводного интерфейса.

**Примеры**

В примере 6.27 приведен вывод сведений об очередях для интерфейса wlan0.

*Пример 6.27 - Отображение сведений об очередях для беспроводного интерфейса*

```
admin@neo:~$ show interfaces wireless wlan0 queue

qdisc pfifo_fast 0: root bands 3 priomap 1 2 2 2 1 2 0 0
1 1 1 1 1 1 1 1 Sent 810323 bytes 6016 pkt (dropped 0,
overlimits 0 requeues 0) rate 0bit 0pps backlog 0b 0p
requeues 0
```

## 6.6.20. show interfaces wireless <wlanx> scan

Поиск доступных беспроводных сетей.

**Синтаксис**

**show interfaces wireless** *wlanx* **scan** [**detail**]

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*wlanx*

Идентификатор беспроводного интерфейса. Значение должно лежать в диапазоне от **wlan0** до **wlan999**.

*detail*

Отображение подробных сведений о поиске для указанного беспроводного интерфейса.

**Значение по умолчанию**

Отображение списка беспроводных сетей в радиусе действия указанного беспроводного интерфейса.

**Указания по использованию**

Эта команда используется для просмотра сведений о беспроводных сетях в радиусе действия указанного беспроводного интерфейса. Эта команда используется на беспроводном интерфейсе, настроенном в качестве рабочей станции.

***ПРИМЕЧАНИЕ*** *Не всё беспроводное оборудование и не все его драйверы поддерживают поиск. Для получения подробных сведений следует ознакомиться с документацией по*

*беспроводному оборудованию и его драйверам.*

**Примеры**

В примере 6.28 приведен вывод сведений о поиске для интерфейса **wlan0**.

*Пример 6.28 - Отображение сведений о поиске для конкретного беспроводного интерфейса*

```
admin@neo:~$ show interfaces wireless wlan0 scan
Access-point SSID Chan Signal (dbm) 00:22:3f:b5:68:d6
Moore 1 -77
00:40:10:10:00:03 Jbridge2 11 -67 00:13:46:42:ff:fe
BubbaNet 10 -89
```

В примере 6.29 приведен вывод подробных сведений о поиске для интерфейса wlan0.

*Пример 6.29 - Отображение подробных сведений о поиске для конкретного беспроводного интерфейса*

```
admin@neo:~$ show interfaces wireless wlan0 scan detail
BSS 00:22:3f:b5:68:d6 (on wlan0)
TSF: 13932293222787 usec (161d, 06:04:53)
freq: 2412
beacon interval: 100
capability: ESS Privacy ShortSlotTime (0x0411)
signal: -84.00 dBm
SSID: Moore
Supported rates: 1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0
DS Paramater set: channel 1
ERP: Barker_Preamble_Mode
Extended supported rates: 6.0 9.0 12.0 48.0
WPS: * Version: 1.0
*
Manufacturer: NETGEAR, Inc.
*
Model: WGR614v8
```

```
*
Device name: WGR614v8 (Wireless AP)
* Config methods: Label, PBC WPA: * Version: 1
*
Group cipher: TKIP
*
Pairwise ciphers: TKIP
*
Authentication suites: PSK
*
Capabilities: 16-PTKSA-RC (0x000c)
WMM: parameter: 01 80 00 03 a4 00 00 27 a4 00 00 42 43 5e
00 62 32 2f 00
```

### 6.6.21. show interfaces wireless <wlanx> stations

Отображение сведений о рабочих станциях, подключенных по радио к беспроводному интерфейсу.

**Синтаксис**

**show interfaces wireless** *wlanx* **stations**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*wlanx*

Идентификатор беспроводного интерфейса. Значение должно лежать в диапазоне от **wlan0** до **wlan999**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для отображения сведений о рабочих станциях, подключенных к беспроводному интерфейсу. Эта команда используется на беспроводном интерфейсе, настроенном в качестве точки доступа.

**Примеры**

В примере 6.30 показан вывод данных о рабочих станциях на интерфейсе wlan0.

*Пример 6.30 - Отображение данных о рабочих станциях*

```
admin@neo:~$ show interfaces wireless wlan0 stations

Station Signal RX: bytes packets TX: bytes
packets00:1d:e0:30:26:3f -45 59074 1409 75714 631
```

# 6.7. Агрегирование каналов Ethernet

В данном разделе описаны способы агрегирования каналов Ethernet в более крупный виртуальный канал. В данном разделе рассматриваются следующие вопросы:

- Настройка агрегирования каналов Ethernet.
- Команды агрегирования каналов Ethernet.

## 6.7.1. Настройка агрегирования каналов Ethernet

В этом разделе рассматриваются следующие вопросы:

- Обзор агрегирования каналов Ethernet.
- Пример настройки агрегирования каналов Ethernet.

### *6.7.1.1. 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.

Многие реализации агрегирования каналов Ethernet были нестандартными. Чтобы способствовать повышению уровня стандартизации в этой области рынка, 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. Протокол LACP 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.

В агрегированный канал можно включать виртуальные частные сети (VLAN); однако

группировка нескольких виртуальных частных сетей в агрегированную магистраль не рекомендуется. Так как целью агрегирования является улучшение доступности и пропускной способности, агрегированный канал должен базироваться на реальных физических каналах.

#### *6.7.1.2. 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 агрегата — то есть указывается созданный интерфейс агрегирования.

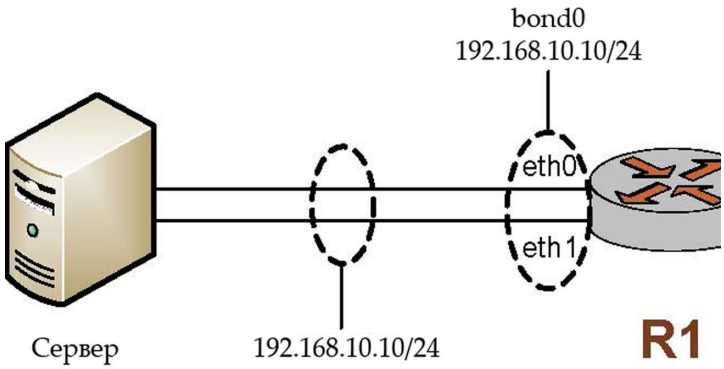
На рисунке 8 показана простая схема агрегирования каналов Ethernet, в которой агрегированный канал Ethernet состоит из двух физических каналов Ethernet. В этом примере:

- Группа агрегирования **bond0** создается при помощи режима агрегирования по умолчанию (802.3ad).
- Интерфейсы **eth0** и **eth1** являются физическими каналами. Они оба добавляются к агрегированному интерфейсу **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 6.31 - Создание группы агрегирования из двух интерфейсов Ethernet*

| Действие | Команда |
|---|---|
| Создание группы агрегирования bond0. | `admin@R1# set interfaces bonding bond0`<br>`[edit]` |
| Установка IP-адреса для группы агрегирования. | `admin@R1# set interfaces bonding bond0 address 192.168.10.10/24`<br>`[edit]` |
| Установка режима агрегирования для группы агрегирования. | `admin@R1# set interfaces bonding bond0 mode 802.3ad`<br>`[edit]` |
| Добавление eth0 ко группе агрегирования bond0. | `admin@R1# set interfaces ethernet eth0 bond-group bond0`<br>`[edit]` |
| Добавление eth1 ко группе | `admin@R1# set interfaces ethernet` |

| | |
|---|---|
| агрегирования bond0. | **eth1 bond-group bond0**<br>[edit] |
| Фиксация изменения. | admin@R1# **commit**<br>[edit] |
| Отображение настройки группы агрегирования. | admin@R1# **show interfaces bonding bond0**<br>**address 192.168.10.10/24 mode 802.3ad**<br>[edit] |
| Отображение настройки eth0. | admin@R1# **show interfaces ethernet eth0**<br>**bond-group bond0**<br>[edit] |
| Отображение настройки eth1. | admin@R1# **show interfaces ethernet eth1**<br>**bond-group bond0**<br>[edit] |

### 6.7.2. Пример настройки агрегирования каналов Ethernet с VLAN

Если интерфейс агрегирования уже собран, становится возможным создать VLAN внутри него. В приведенном ниже примере к предыдущему примеру 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 6.32 - Добавление VLAN к существующему интерфейсу агрегирования*

| Действие | Команда |
|---|---|
| Добавление настройки виртуального интерфейса ко группе агрегирования. | admin@R1# **set interfaces bonding bond0 vif 192 address** |

| | |
|---|---|
| | **10.192.248.225/24**<br>[edit] |
| Фиксация изменения. | admin@R1# **commit**<br>[edit] |
| Отображение новой настройки группы агрегирования. | admin@R1# **show interfaces bonding bond0**<br>address 192.168.10.10/24<br>mode 802.3ad<br>vif 192 {<br>address 10.192.248.225/24 }<br>[edit] |

### 6.7.3. Команды агрегирования каналов Ethernet

В данном разделе приведены следующие команды.

*Таблица 26 - Команды агрегирования каналов Ethernet*

| 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> disable-link-detect | Отключение определения изменения состояния физического канала для группы агрегирования интерфейсов Ethernet. |
| interfaces bonding <bondx> mac <mac-адрес> | Установка MAC-адреса группы агрегирования интерфейсов Ethernet. |

| | |
|---|---|
| `interfaces bonding <bondx> mode` | 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. |
| Группа агрегирования | |
| `interfaces ethernet <ethx> bond-group <bondx>` | Добавление интерфейса Ethernet в группу агрегирования. |
| Эксплуатационные команды | |
| `show interfaces bonding` | Вывод сведений о группе агрегирования интерфейсов Ethernet. |

### 6.7.4. interfaces bonding <bondx>

Определение интерфейса агрегирования каналов Ethernet (группы агрегирования).

**Синтаксис**

**set interfaces bonding** *bondx*

**delete interfaces bonding** *bondx*

**show interfaces bonding** *bondx*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    bonding bond0..bond99
    {}
}
```

**Параметры**

*bondx*

Множественный узел. Идентификатор определяемой группы агрегирования. 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 группы агрегирования каналов Ethernet.

Форма **delete** данной команды используется для удаления всей настройки для группы агрегирования каналов Ethernet.

Форма **show** данной команды используется для просмотра настройки группы агрегирования каналов Ethernet.

## 6.7.5. interfaces bonding <bondx> address

Назначение сетевого адреса группе агрегирования интерфейсов Ethernet.

**Синтаксис**

**set interfaces bonding** *bondx* **address** {*подсеть_ipv4* | *подсеть_ipv6* | **dhcp**}

**delete interfaces bonding** *bondx* **address** {*подсеть_ipv4* | *подсеть_ipv6* | **dhcp**}

**show interfaces bonding** *bondx* **address**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    bonding bond0..bond99 {
        address [подсеть_ipv4|подсеть_ipv6|dhcp]
```

```
        }
    }
```

**Параметры**

*bondx*

Множественный узел. Идентификатор группы агрегирования. Поддерживаются значения в диапазоне от **bond0** до **bond99**.

*подсеть_ipv4*

Адрес подсети IPv4 для данного интерфейса. Используется формат ip-адрес/префикс (например, 192.168.1.77/24). Назначить интерфейсу несколько адресов подсетей IPv4 можно, создав соответствующее количество узлов конфигурации **address**.

*подсеть_ipv6*

Адрес подсети IPv6 для данного интерфейса. Для указания адреса используется формат ipv6-адрес/префикс (например, 2001:db8:1234::/48). Назначить интерфейсу несколько адресов подсетей IPv6 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**

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. 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.

### 6.7.6. interfaces bonding <bondx> description <описание>

Ввод описания для группы агрегирования интерфейсов 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 bond0..bond99 {
        description текст
    }
}
```

**Параметры**

*bondx*

Идентификатор группы агрегирования. Поддерживаются значения в диапазоне от **bond0** до **bond99**.

*описание*

Краткое 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 группы агрегирования.

Форма **delete** этой команды используется для удаления этого описания.

Форма **show** этой команды используется для просмотра этого описания.

### 6.7.7. interfaces bonding <bondx> disable

Отключение группы агрегирования интерфейсов 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 bond0..bond99 {
        disable
    }
}
```

**Параметры**

*bondx*

Идентификатор группы агрегирования. 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.

Форма **delete** этой команды используется для включения интерфейса.

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

### 6.7.8. interfaces bonding <bondx> disable-link-detect

Отключение определения изменения состояния физического канала для группы агрегирования интерфейсов Ethernet.

**Синтаксис**

**set interfaces bonding** *bondx* **disable-link-detect**

**delete interfaces bonding** *bondx* **disable-link-detect**

**show interfaces bonding** *bondx*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    bonding bond0..bond99 {
        disable-link-detect
    }
}
```

**Параметры**

*bondx*

Идентификатор группы агрегирования. Поддерживаются значения в диапазоне от **bond0** до **bond99**.

**Значение по умолчанию**

Интерфейс, на котором определяются изменения состояния физического канала.

**Указания по использованию**

Команда используется для того, чтобы указать группе агрегирования каналов Ethernet не определять изменение состояния нижележащего физического канала (например, когда сетевой кабель не подключен).

Форма **set** этой команды используется для отключения определения изменений состояния физического канала.

Форма **delete** данной команды используется для включения определения изменений состояния физического канала.

Форма **show** данной команды используется для просмотра настройки группы агрегирования каналов Ethernet.

## 6.7.9. interfaces bonding <bondx> mac <mac-адрес>

Установка MAC-адреса группы агрегирования интерфейсов 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 bond0..bond23 {
        mac mac-адрес
    }
}
```

**Параметры**

*bondx*

Идентификатор группы агрегирования. Поддерживаются значения в диапазоне от **bond0** до **bond99**.

*mac-адрес*

MAC-адрес для группы агрегирования интерфейсов 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 группу агрегирования.

**Указания по использованию**

Эта команда используется для установки MAC-адреса группы агрегирования.

Форма **set** этой команды используется для установки MAC-адреса группы агрегирования.

Форма **delete** этой команды используется для удаления настроенного MAC-адреса для группы агрегирования.

Форма **show** этой команды используется для просмотра настройки MAC-

адреса для группы агрегирования.

## 6.7.10. interfaces bonding <bondx> mode

Установка режимов агрегирования для группы агрегирования интерфейсов Ethernet.

**Синтаксис**

```
set interfaces bonding bondx mode {802.3ad | active-backup | adaptive-load-balance | round-robin | transmit-load-balance | xor-hash | broadcast}

delete interfaces bonding bondx mode

show interfaces bonding bondx mode
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    bonding bond0..bond23 {
        mode текст
    }
}
```

**Параметры**

*bondx*

Идентификатор группы агрегирования. Поддерживаются значения в диапазоне от **bond0** до **bond99**.

**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 в группе агрегирования(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 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 группы агрегирования каналов Ethernet.

Форма **set** этой команды используется для установки режима агрегирования группы агрегирования.

Форма **delete** этой команды используется для восстановления режима агрегирования по умолчанию для группы агрегирования.

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

## 6.7.11. interfaces bonding <bondx> mtu <mtu>

Ввод значения MTU для группы агрегирования интерфейсов 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 bond0..bond99 {
        mtu целоебеззнака32разр }}
```

**Параметры**

*bondx*

Идентификатор группы агрегирования. Поддерживаются значения в

диапазоне от **bond0** до **bond99**.

*mtu*

Установка значения MTU (в октетах) для интерфейса Ethernet в целом, включая все логические интерфейсы, настроенные на нем. Значение должно лежать в диапазоне от 1 до 1500.

**Значение по умолчанию**

Используется значение MTU первого канала Ethernet, добавленного к группе.

**Указания по использованию**

Эта команда используется для установки параметра MTU (максимальная длина передаваемого блока) для группы агрегирования каналов Ethernet. Это значение применяется также ко всем виртуальным интерфейсам, определенным для интерфейса агрегирования.

Следует заметить, в результате изменения параметра MTU для агрегата изменяются параметры MTU всех интерфейсов Ethernet в агрегате. Кроме того, явное изменение параметра MTU для каналов Ethernet в агрегате (путем настройки отдельных каналов) не допускается.

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, а отправителю будет направлено соответствующее сообщение ICMP “Packet too big” с указанием того, что отправленный пакет имел слишком большой размер.

Форма **set** этой команды используется для установки параметра MTU группы агрегирования.

Форма **delete** этой команды используется для восстановления значения MTU по умолчанию и отключения фрагментации.

Форма **show** этой команды используется для просмотра настройки MTU для группы агрегирования.

## 6.7.12. interfaces bonding <bondx> primary <ethx>

Установка одного из каналов Ethernet в группе агрегирования в качестве первичного канала.

**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 bond0..bond99 {
        primary ethx
    }
}
```

**Параметры**

*bondx*

Идентификатор группы агрегирования. Поддерживаются значения в диапазоне от **bond0** до **bond99**.

*ethx*

Идентификатор первичного интерфейса Ethernet в группе агрегирования. Поддерживаются значения в диапазоне от **eth0** до **eth23**.

**Значение по умолчанию**

Первичный канал отсутствует.

**Указания по использованию**

Эта команда используется для указания первичного интерфейса Ethernet в интерфейсе агрегирования каналов Ethernet.

Этот вариант возможен, лишь если используется режим агрегирования "активный-резервный".

Если используется режим агрегирования "активный-резервный" и интерфейс помечен как первичный, то он всегда остается единственным активным членом интерфейса агрегирования до тех пор, пока он доступен. Альтернативные интерфейсы используются только тогда, когда первичный выходит из оперативного режима.

Такой вариант полезен, когда один из интерфейсов агрегата 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.

## 6.7.13. interfaces ethernet <ethx> bond-group <bondx>

Добавление интерфейса Ethernet в группу агрегирования.

**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 eth0..eth23 {
        bond-group bond0..bond99
    }
}
```

**Параметры**

*ethx*

Множественный узел. Идентификатор определяемого интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**.

*bondx*

Идентификатор группы агрегирования. Поддерживаются значения в диапазоне от **bond0** до **bond99**.

**Значение по умолчанию**

Отсутствуют.

**Указания по использованию**

Эта команда используется для добавления интерфейса Ethernet в группу агрегирования каналов Ethernet.

Интерфейс Ethernet может быть членом только одной группы агрегирования каналов Ethernet, а группа агрегирования должна быть предварительно определена 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.

## 6.7.14. show interfaces bonding

Вывод сведений о группе агрегирования интерфейсов Ethernet.

**Синтаксис**

```
show interfaces bonding [detail | slaves]
```

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**detail**

Отображение подробных сведений для интерфейса агрегирования.

**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 6.33 приведен вывод для команды **show interfaces bonding**.

*Пример 6.33 - Отображение сведений об интерфейсах агрегирования*

```
admin@neo:~$ show interfaces bonding
Interface IP Address State Link Description
bond3 10.192.136.2/29 up up
bond3.128 10.192.128.2/24 up up
```

В примере 6.34 приведен вывод команды **show interfaces bonding slaves**.

*Пример 6.34 - Отображение сведений о составляющих интерфейсах агрегата*

```
admin@neo:~$ show interfaces bonding slaves
Interface Mode State Link Slaves
bond0 802.3ad up up eth2 eth3
bond1 802.3ad up down eth1
```

## 6.8. 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:

- Настройка интерфейса псевдо-Ethernet.
- Команды для интерфейсов псевдо-Ethernet.

### 6.8.1. Настройка интерфейса псевдо-Ethernet

В этом разделе рассматриваются следующие вопросы:

- Обзор интерфейсов псевдо-Ethernet.
- Примеры настройки интерфейса псевдо-Ethernet.

## 6.8.2. Обзор интерфейсов псевдо-Ethernet

Под интерфейсом псевдо-Ethernet подразумевается создание нескольких виртуальных устройств Ethernet 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>** (см. стр. 357). 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.

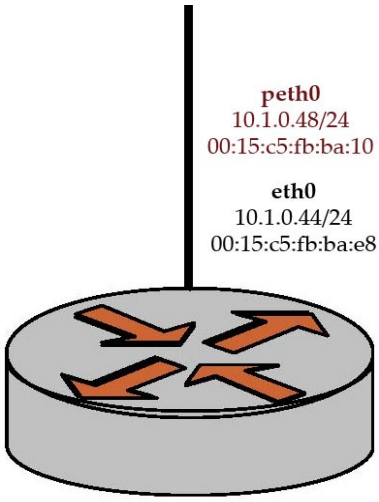
#### *6.8.2.1. Примеры настройки интерфейса псевдо-Ethernet*

На рисунке 9 приведен простой пример использования интерфейса псевдо-Ethernet. В этом примере:

- Интерфейсу Ethernet **eth0** назначен IP-адрес 10.1.0.44/24, а также он имеет MAC-адрес 00:15:c5:fb:ba:e8.
- Интерфейс псевдо-Ethernet **peth0** связан с физическим интерфейсом **eth0**. Для него назначен IP-адрес 10.1.0.48/24, а также MAC-адрес 00:15:c5:fb:ba:10.

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 10.1.0.48/32.

*Рисунок 9 - Создание интерфейса псевдо-Ethernet*




Для настройки данной схемы нужно выполнить следующие действия в режиме настройки.

*Пример 6.35 - Создание интерфейса псевдо-Ethernet*

| Действие | Команда |
|---|---|
| Создание интерфейса псевдо-Ethernet и назначение ему адреса. | admin@neo# **set interfaces pseudo-ethernet peth0 address 10.1.1.1/24**<br>[edit] |
| Создание описания для интерфейса. | admin@neo# **set interfaces pseudo-ethernet peth0 description "Sample virtual Ethernet interface"**<br>[edit] |
| Привязка интерфейса псевдо-Ethernet к физическому порту Ethernet. | admin@neo# **set interfaces pseudo-ethernet peth0 link eth0**<br>[edit] |
| Назначение MAC-адреса для интерфейса псевдо-Ethernet | admin@neo# **set interfaces pseudo-ethernet peth0 mac 00:15:c5:fb:ba:10**<br>[edit] |
| Фиксация изменений. | admin@neo# **commit**<br>[edit] |
| Вывод настройки интерфейса псевдо-Ethernet | admin@neo# **show interfaces pseudo-ethernet peth0**<br>address 10.1.1.1/24<br>description "Sample virtual Ethernet interface"  link eth0<br>mac 00:15:c5:fb:ba:10<br>[edit] |

### 6.8.3. Команды для интерфейсов псевдо-Ethernet

В данном разделе приведены следующие команды.

*Таблица 27 - 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> disable-link-detect` | Отключение определения изменения состояния физического канала для интерфейса псевдо-Ethernet . |
| `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. |
| Эксплуатационные команды | |
| При работе с интерфейсами псевдо-Ethernet могут быть использованы все эксплуатационные команды, предназначенные для работы с интерфейсами Ethernet. Данные команды приведены в разделе “6.2. Настройка интерфейсов Ethernet ”. | |

Все возможности доступные для работы с интерфейсами Ethernet также доступны для работы с интерфейсами псевдо-Ethernet. В следующих разделах представлены команды,

которые позволяют использовать другие компоненты системы для работы с интерфейсами Ethernet.

### 6.8.4. 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 peth0..pethx
    {}
}
```

**Параметры**

*pethx*

Множественный узел. Идентификатор определяемого интерфейса псевдо-Ethernet; например **eth0**.

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**.

После определения интерфейса псевдо-Ethernet, ему можно назначить MAC-

адрес при помощи команды **interfaces pseudo-ethernet <pethx> mac <mac-addr>** (см. стр. 358) 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.

### 6.8.5. interfaces pseudo-ethernet <pethx> address

Назначение IP-адреса и префикса сети для интерфейса псевдо-Ethernet.

**Синтаксис**

```
set interfaces ethernet pethx address {ipv4-адрес | ipv6-адрес | dhcp}

delete interfaces ethernet pethx address { ipv4-адрес | ipv6-адрес | dhcp}

show interfaces ethernet pethx address
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    pseudo-ethernet peth0..pethx {
        address [ipv4-адрес|ipv6-адрес|dhcp]
    }
}
```

**Параметры**

`pethx`

Множественный узел. Идентификатор определяемого интерфейса псевдо-Ethernet; например, **peth0**.

`ipv4`

IPv4-адрес для данного интерфейса. Для указания адреса используется следующий формат *ip-адрес/префикс* (например, 192.168.1.77/24). Можно

определить несколько IP-адресов для одного интерфейса псевдо-Ethernet, создав соответствующее количество узлов конфигурации **address**.

`ipv6`

IPv6-адрес для данного интерфейса. Для указания адреса используется следующий формат *ipv6-адрес/префикс* (например, 2001:db8:1234::/48). Можно определить несколько IPv6-адресов для одного интерфейса псевдо-Ethernet, создав соответствующее количество узлов конфигурации **address**.

`dhcp`

Параметр определяет интерфейс 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. Можно назначить более одного IP-адреса для интерфейса, создав 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.

## 6.8.6. 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 peth0..pethx {
        description текст
    }
}
```

**Параметры**

*pethx*

Множественный узел. Идентификатор определяемого интерфейса псевдо-Ethernet; например, **peth0**.

*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.

## 6.8.7. 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 peth0..pethx {
    disable
}
}
```

**Параметры**

*pethx*

Множественный узел. Идентификатор определяемого интерфейса псевдо-Ethernet; например, **peth0**.

**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.

## 6.8.8. interfaces pseudo-ethernet <pethx> disable-link-detect

Отключение определения изменения состояния физического канала для интерфейса псевдо-Ethernet.

**Синтаксис**

**set interfaces pseudo-ethernet** *pethx* **disable-link-detect**

**delete interfaces pseudo-ethernet** *pethx* **disable-link-detect**

**show interfaces pseudo-ethernet** *pethx*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    pseudo-ethernet peth0..pethx {
        disable-link-detect
```

```
        }
    }
```

**Параметры**

*pethx*

Множественный узел. Идентификатор определяемого интерфейса псевдо-Ethernet; например, **peth0**.

**Значение по умолчанию**

Интерфейс, на котором определяются изменения состояния физического канала.

**Указания по использованию**

Данная команда позволяет отключить определение изменения состояния физического канала для интерфейса псевдо-Ethernet (например, когда сетевой кабель не подключен).

Форма **set** данной команды используется для отключения определения изменения состояния физического канала.

Форма **delete** данной команды используется для включения определения изменения состояния физического канала.

Форма **show** данной команды используется для отображения настройки интерфейса псевдо-Ethernet.

## 6.8.9. 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 peth0..pethx {
```

```
            link eth0..eth23
        }
    }
```

**Параметры**

*pethx*

Множественный узел. Идентификатор определяемого интерфейса псевдо-Ethernet; например, **peth0**.

*link*

Обязательный. Физический интерфейс Ethernet, связанный с интерфейсом псевдо-Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23** в зависимости от реально имеющихся в системе интерфейсов Ethernet. Числовые значения в идентификаторах виртуального и реального интерфейсов **peth***x* и **eth***x* могут не совпадать (то есть 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.

## 6.8.10. 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 peth0..pethx {
        mac mac-адрес
    }
}
```

**Параметры**

*pethx*

Множественный узел. Идентификатор определяемого интерфейса псевдо-Ethernet; например, **peth0**.

*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.

## 6.9. PPPoE

В данном разделе приведены команды для настройки подключений PPPoE.

| Режим настройки | |
|---|---|
| interfaces ethernet <ethx> pppoe <номер> | Включение или отключение модуля PPPoE на указанном интерфейсе Ethernet. |
| interfaces ethernet <ethx> pppoe <номер> access-concentrator <имя> | Данная команда позволяет указать имя сервера доступа для подключения. |
| interfaces ethernet <ethx> pppoe <номер> connect-on-demand | Создание подключения PPPoE по запросу. |
| interfaces ethernet <ethx> pppoe <номер> default-route <параметры> | Включение или отключение автоматического добавления маршрута по умолчанию при установлении соединения PPPoE. |
| interfaces ethernet <ethx> pppoe <номер> idle-timeout <таймаут> | 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 <параметры> | 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 для всех интерфейсов PPPoE. |
| show interfaces pppoe <интерфейс> | Вывод сведений для указанного интерфейса PPPoE. |
| show interfaces pppoe <интерфейс> capture | Вывод сетевого трафика, записанного на указанном интерфейсе PPPoE. |
| show interfaces pppoe <интерфейс> log | Вывод сведений журнала регистрации для указанного интерфейса PPPoE. |
| show interfaces pppoe <интерфейс> queue | Вывод сведений об очередях для указанного интерфейса PPPoE. |

### 6.9.1. interfaces ethernet <ethx> pppoe <номер>

Включение или отключение модуля PPPoE на указанном интерфейсе Ethernet.

**Синтаксис**

```
set interfaces ethernet ethx pppoe номер
delete interfaces ethernet ethx pppoe номер
show interfaces ethernet ethx pppoe номер
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    ethernet ethx {
```

```
            pppoe 0-15 {
            }
        }
    }
```

**Параметры**

*ethx*

Обязательный. Имя указанного интерфейса Ethernet. Значение должно лежать в диапазоне от **eth1** до **eth23**.

*номер*

Обязательный. Номер устройства PPPoE. Этот номер должен быть уникален. Интерфейс PPPoE будет иметь имя **pppoe***X*, 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.

## 6.9.2. 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 0-15 {
            access-concentrator текст
        }
    }
}
```

**Параметры**

*ethx*

Обязательный. Имя указанного интерфейса Ethernet. Значение должно лежать в диапазоне от **eth1** до **eth23**.

*номер*

Обязательный. Номер устройства PPPoE. Этот номер должен быть уникален. Интерфейс PPPoE будет иметь имя **pppoe***X*, где X — номер устройства PPPoE (например, pppoe7). 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 .

### 6.9.3. interfaces ethernet <ethx> pppoe <номер> connect-on-demand

Создание подключения PPPoE по запросу.

**Синтаксис**

**set interfaces ethernet** *ethx* **pppoe** *номер* **connect-on-demand**

**delete interfaces ethernet** *ethx* **pppoe** *номер* **connect-on-demand**

**show interfaces ethernet** *ethx* **pppoe** *номер* **connect-on-demand**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    ethernet ethx {
        pppoe 0-15 {
```

```
                    connect-on-demand
                }
            }
        }
```

**Параметры**

*ethx*

Обязательный. Имя указанного интерфейса Ethernet. Значение должно лежать в диапазоне от **eth1** до **eth23**.

*номер*

Обязательный. Номер устройства PPPoE. Этот номер должен быть уникален. Интерфейс PPPoE будет иметь имя **pppoe***X*, где *X* — номер устройства PPPoE (например, pppoe7). Значение должно лежать в диапазоне от 0 до 15.

**Значение по умолчанию**

Подключение по запросу не используется.

**Указания по использованию**

При использовании данной команды установка подключений PPPoE будет осуществляться автоматически только тогда, когда будет отправляться трафик.

В том случае если подключение по запросу не используется, подключения PPPoE создаются при загрузке и остаются включенными. Если соединение по какой-либо причине разрывается, оно сразу устанавливается заново. 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 этой команды 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. Для установки периода простоя используется команда interfaces ethernet <ethx> pppoe <номер> idle-timeout <таймаут> .

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.

### 6.9.4. interfaces ethernet <ethx> pppoe <номер> default-route <параметры>

Включение или отключение автоматического добавления маршрута по умолчанию при установлении соединения PPPoE.

**Синтаксис**

**set interfaces ethernet** *ethx* **pppoe** *номер* **default-route** *параметры*

**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 0-15 {
            default-route [auto|none]
        }
    }
}
```

**Параметры**

*ethx*

Обязательный. Имя указанного интерфейса Ethernet. Значение должно лежать в диапазоне от **eth1** до **eth23**.

*номер*

Обязательный. Номер устройства PPPoE. Этот номер должен быть уникален. Интерфейс PPPoE будет иметь имя **pppoe***X*, где *X* — номер устройства PPPoE (например, pppoe7). Значение должно лежать в диапазоне от 0 до 15.

*параметры*

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.

## 6.9.5. interfaces ethernet <ethx> pppoe <номер> idle-timeout <таймаут>

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 0-15 {
               idle-timeout целое32разрядн
          }
     }
}
```

**Параметры**

*ethx*

Обязательный. Имя указанного интерфейса Ethernet. Значение должно лежать в диапазоне от **eth1** до **eth23**.

*номер*

Обязательный. Номер устройства PPPoE. Этот номер должен быть уникален. Интерфейс PPPoE будет иметь имя **pppoe***X*, где *X* — номер устройства PPPoE (например, pppoe7). Значение должно лежать в диапазоне от 0 до 15.

*таймаут*

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 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.

### 6.9.6. 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 0-15 {
            local-address ipv4-адрес
        }
    }
```

```
}
```

**Параметры**

*ethx*

Обязательный. Имя указанного интерфейса Ethernet. Значение должно лежать в диапазоне от **eth1** до **eth23**.

*номер*

Обязательный. Номер устройства PPPoE. Этот номер должен быть уникален. Интерфейс PPPoE будет иметь имя **pppoe***X*, где *X* — номер устройства PPPoE (например, pppoe7). Значение должно лежать в диапазоне от 0 до 15.

*ipv4-адрес*

IP-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.

## 6.9.7. 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 0-15 {
               mtu 68-1492
          }
     }
}
```

**Параметры**

*ethx*

Обязательный. Имя указанного интерфейса Ethernet. Значение должно лежать в диапазоне от **eth1** до **eth23**.

*номер*

Обязательный. Номер устройства PPPoE. Этот номер должен быть уникален. Интерфейс PPPoE будет иметь имя **pppoe***X*, где *X* — номер устройства PPPoE (например, pppoe7). 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.

### 6.9.8. interfaces ethernet <ethx> pppoe <номер> name-server <параметры>

Данная команда позволяет указать требуется ли получение адресов серверов DNS от удаленного узла соединения PPPoE.

**Синтаксис**

**set interfaces ethernet** *ethx* **pppoe** *номер* **name-server** *параметры*

**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 0-15 {
            name-server [auto|none]
        }
    }
}
```

**Параметры**

*ethx*

Обязательный. Имя указанного интерфейса Ethernet. Значение должно лежать в диапазоне от **eth1** до **eth23**.

*номер*

Обязательный. Номер устройства PPPoE. Этот номер должен быть уникален. Интерфейс PPPoE будет иметь имя **pppoe***X*, где *X* — номер устройства PPPoE (например, pppoe7). Значение должно лежать в диапазоне от 0 до 15.

*параметры*

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 установлено значение **auto**.

**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.

## 6.9.9. 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 0-15 {
            password текст
        }
```

```
        }
    }
```

**Параметры**

*ethx*

Обязательный. Имя указанного интерфейса Ethernet. Значение должно лежать в диапазоне от **eth1** до **eth23**.

*номер*

Обязательный. Номер устройства PPPoE. Этот номер должен быть уникален. Интерфейс PPPoE будет иметь имя **pppoe***X*, где *X* — номер устройства PPPoE (например, pppoe7). 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.

## 6.9.10. 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 0-15 {
            remote-address ipv4-адрес
        }
    }
}
```

**Параметры**

*ethx*

Обязательный. Имя указанного интерфейса Ethernet. Значение должно лежать в диапазоне от **eth1** до **eth23**.

*номер*

Обязательный. Номер устройства PPPoE. Этот номер должен быть уникален. Интерфейс PPPoE будет иметь имя **pppoe***X*, где *X* — номер устройства PPPoE (например, pppoe7). 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.

## 6.9.11. 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 0-15 {
               service-name текст
          }
     }
}
```

**Параметры**

*ethx*

Обязательный. Имя указанного интерфейса Ethernet. Значение должно лежать в диапазоне от **eth1** до **eth23**.

*номер*

Обязательный. Номер устройства PPPoE. Этот номер должен быть уникален. Интерфейс PPPoE будет иметь имя **pppoe***X*, где X — номер устройства PPPoE (например, pppoe7). 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.

## 6.9.12. 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 0-15 {
            user-id текст
        }
    }
}
```

**Параметры**

*ethx*

Обязательный. Имя указанного интерфейса Ethernet. Значение должно лежать в диапазоне от **eth1** до **eth23**.

*номер*

Обязательный. Номер устройства PPPoE. Этот номер должен быть уникален. Интерфейс PPPoE будет иметь имя **pppoe***X*, где *X* — номер устройства PPPoE (например, pppoe7). 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.

## 6.9.13. show interfaces pppoe

Вывод сведений для всех интерфейсов PPPoE.

**Синтаксис**

```
show interfaces pppoe
```

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Вывод сведений для всех интерфейсов

**Указания по использованию**

Эта команда позволяет вывести сведения обо всех настроенных интерфейсах PPPoE.

## 6.9.14. show interfaces pppoe <интерфейс>

Вывод сведений для указанного интерфейса PPPoE.

**Синтаксис**

**show interfaces pppoe** *интерфейс*

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*интерфейс*

Обязательный. Имя интерфейса PPPoE, для которого требуется вывести сведения, например, **pppoe7**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда позволяет вывести сведения для указанного интерфейса PPPoE.

**Примеры**

*Пример 6.36 - Вывод сведений для интерфейса pppoe1*

```
admin@neo:~$ show interfaces pppoe pppoe1

pppoe1: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu
1492 qdisc pfifo_fast state UNKNOWN qlen 3

    link/ppp

    inet 192.168.33.2 peer 10.0.0.1/32 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
```

## 6.9.15. show interfaces pppoe <интерфейс> capture

Вывод сетевого трафика, записанного на указанном интерфейсе PPPoE.

**Синтаксис**

**show interfaces pppoe** *интерфейс* **capture** [**not port** *порт* | **port** *порт*]

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*интерфейс*

Обязательный. Имя интерфейса PPPoE, для которого требуется вывести сведения, например, **pppoe7**.

**not port** *порт*

Вывести сетевой трафик для всех портов кроме указанного.

**port** *порт*

Вывести трафик для указанного порта.

**Значение по умолчанию**

Выводится трафик для всех сетевых портов, записанный на указанном интерфейсе PPPoE.

**Указания по использованию**

Эта команда используется для вывода сетевого трафика на указанном интерфейсе PPPoE.

## 6.9.16. show interfaces pppoe <интерфейс> log

Вывод сведений журнала регистрации для указанного интерфейса PPPoE.

**Синтаксис**

**show interfaces pppoe** *интерфейс* **log** [**tail**]

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*интерфейс*

Обязательный. Имя интерфейса PPPoE, для которого требуется вывести сведения, например, **pppoe7**.

**tail**

Вывод регистрационных сообщений в режиме реального времени по мере их поступления. Для того чтобы остановить вывод, нажмите <Ctrl + C>.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для вывода данных регистрации для указанного интерфейса PPPoE.

## 6.9.17. show interfaces pppoe <интерфейс> queue

Вывод сведений об очередях для указанного интерфейса PPPoE.

**Синтаксис**

**show interfaces pppoe** *интерфейс* **queue**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*интерфейс*

Обязательный. Имя интерфейса PPPoE, для которого требуется вывести сведения, например, **pppoe7**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для вывода данных об очередях для указанного интерфейса PPPoE.

# 7. ТУННЕЛИРОВАНИЕ IP

## 7.1. 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 Altell NEO поддерживаются три наиболее часто используемых механизма туннелирования:

- Туннели на основе протокола GRE (Generic Routing Encapsulation) могут быть использованы для транспортировки не-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 (см. стр. 402).
- 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 экранирования, 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.

## 7.2. 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 не-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 не-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. В том случае если 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.

## 7.3. 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 (см. стр. 402). 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 6.5. Настройка мостов на стр. 263.

## 7.4. 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 доставка трафика такого вида может быть использовано туннелирование на базе GRE.

Также 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.

## 7.5. 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 (см. стр. 402).

## 7.6. 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 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 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 17.1.8. Защита туннеля GRE с использованием IPSec на стр. 1167.

## 7.7. 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.

### 7.7.1. Перед началом настройки

В этом наборе примеров предполагается использование двух систем Altell NEO с именами узлов neo1 и neo2.

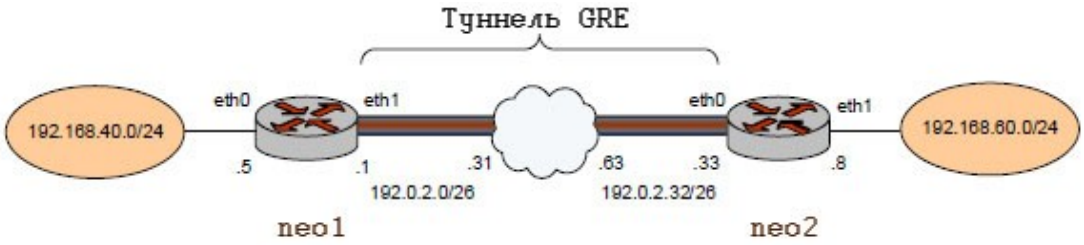
- Все интерфейсы Ethernet, используемые в настройке туннеля, должны быть заранее настроены. В этом примере используется интерфейс eth1 на узле neo1 и интерфейс eth0 на узле neo2.

### 7.7.2. Настройка базового туннеля GRE

В данном разделе приведены примеры настройки базового туннеля GRE между системами Altell NEO с именами neo1 и neo2. Сначала настраивается узел neo1, затем узел neo2.

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 10.

*Рисунок 10 - Настройка базового туннеля GRE*




### *7.7.2.1. Настройка узла neo1*

В примере 7.1 настраивается туннель GRE от узла neo1 к узлу neo2 через ГВС. В данном примере приведено создание туннельного интерфейса и оконечной точки туннеля на узле neo1.

- Туннельному интерфейсу tun0 на узле neo1 назначается IP-адрес 10.20.20.1 из сети 10.20.20.0/24.
- В качестве адреса локальной оконечной точки туннеля (**local-ip**) в этом примере используется адрес 192.0.2.1, назначенный интерфейсу **eth1**.
- В качестве IP-адреса удаленного оконечного узла туннеля (**remote-ip**) используется адрес 192.0.2.33 на узле neo2.

В примере 7.1 приведено создание туннельного интерфейса и оконечного узла туннеля на узле neo1. Для этого необходимо выполнить следующие действия на узле neo1 в режиме настройки.

*Пример 7.1 - Создание оконечного узла базового туннеля GRE на узле neo1*

| Действие | Команда |
|---|---|
| Создание туннельного интерфейса и назначение ему IP-адреса. | `admin@neo1# set interfaces tunnel tun0 address 10.20.20.1/24`<br>`[edit]` |
| Указание IP-адреса источника для данного туннеля. | `admin@neo1# set interfaces tunnel tun0 local-ip 192.0.2.1`<br>`[edit]` |

| | |
|---|---|
| Указание IP-адреса удаленного оконечного узла туннеля. | admin@neo1# **set interfaces tunnel tun0 remote-ip 192.0.2.33**<br>[edit] |
| Указание режима инкапсуляции для туннеля. | admin@neo1# **set interfaces tunnel tun0 encapsulation gre**<br>[edit] |
| Указание краткого текстового описания для туннеля. | admin@neo1# **set interfaces tunnel tun0 description "GRE tunnel to neo2"**<br>[edit] |
| Фиксация настройки. | admin@neo1# **commit**<br>[edit] |
| Вывод настройки. | admin@neo1# **show interfaces tunnel tun0**<br>address 10.20.20.1/24<br>description "Tunnel to neo2"<br>encapsulation gre<br>local-ip 192.0.2.1<br>remote-ip 192.0.2.33<br>[edit] |
| Добавление статического интерфейсного маршрута к сети 192.168.60.0/24 через туннель. | admin@neo1# **set protocols static interface-route 192.168.60.0/24 next-hop-interface tun0**<br>[edit] |
| Фиксация настройки. | admin@neo1# **commit**<br>[edit] |

#### *7.7.2.2. Настройка узла neo2*

В этом разделе приведена настройка оконечного узла туннеля на узле neo2.

- Туннельному интерфейсу tun0 на узле neo2 назначается IP-адрес 10.20.20.2 из сети

10.20.20.0/24.

- В качестве адреса источника для оконечной точки туннеля (**local-ip**) в этом примере используется адрес 192.0.2.33.
- В качестве IP-адреса удаленного оконечного узла туннеля (**remote-ip**) используется адрес 192.0.2.1 на узле neo1.
- Создается статический маршрут для обеспечения доступа к удаленной локальной сети через созданный туннель.

В примере 7.2 приведено создание оконечного узла туннеля на узле neo2. Для этого необходимо выполнить следующие действия на узле neo2 в режиме настройки.

*Пример 7.2 - Создание оконечного узла базового туннеля GRE на узле neo2*

| Действие | Команда |
|---|---|
| Создание туннельного интерфейса и назначение ему IP-адреса. | admin@neo2# **set interfaces tunnel tun0 address 10.20.20.2/24**<br>[edit] |
| Указание IP-адреса источника для данного туннеля. | admin@neo2# **set interfaces tunnel tun0 local-ip 192.0.2.33**<br>[edit] |
| Указание IP-адреса удаленного оконечного узла туннеля. | admin@neo2# **set interfaces tunnel tun0 remote-ip 192.0.2.1**<br>[edit] |
| Указание режима инкапсуляции для туннеля. | admin@neo2# **set interfaces tunnel tun0 encapsulation gre**<br>[edit] |
| Указание краткого текстового описания для туннеля. | admin@neo2# **set interfaces tunnel tun0 description "GRE tunnel to neo1"**<br>[edit] |
| Фиксация настройки. | admin@neo2# **commit**<br>[edit] |

| | |
|---|---|
| Вывод настройки. | admin@neo2# **show interfaces tunnel tun0**<br>address 10.20.20.2/24<br>description "Tunnel to neo1"<br>encapsulation gre<br>local-ip 192.0.2.33<br>remote-ip 192.0.2.1<br>[edit] |
| Добавление статического интерфейсного маршрута к сети 192.168.40.0/24 через туннель. | admin@neo2# **set protocols static interface-route 192.168.40.0/24 next-hop-interface tun0**<br>[edit] |
| Фиксация настройки. | admin@neo2# **commit**<br>[edit] |

## 7.7.3. 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 набор правил межсетевого экрана.

### *7.7.3.1. Настройка узла neo1*

В примере 7.3 приведены дополнительные параметры настройки для оконечного узла neo1 , созданного в примере 7.1:

- Ключ 101088 обеспечивает механизм парольной защиты. Это значение должно быть одинаковым на всех оконечных узлах.
- 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 два набора правил межсетевого экрана:
  - 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 7.3 предполагается создание нового туннеля с параметрами из примера 7.1, ниже приведены только отличающиеся параметры.

Для настройки оконечной точки туннеля GRE, необходимо выполнить следующие шаги на узле neo1 в режиме настройки.

*Пример 7.3 - Добавление значений в настройку оконечного узла туннеля GRE на узле neo1*

| Действие | Команда |
|---|---|
| Указание ключа аутентификации. | admin@neo1# **set interfaces tunnel tun0 key 101088**<br>[edit] |
| Установка TTL. | admin@neo1# **set interfaces tunnel tun0 ttl 220**<br>[edit] |
| Установка DSCP. | admin@neo1# **set interfaces tunnel tun0 dscp 55**<br>[edit] |
| Установка MTU. | admin@neo1# **set interfaces tunnel tun0 mtu 1460**<br>[edit] |
| Применение правил межсетевого экрана к входящим пакетам. | admin@neo1# **set interfaces tunnel tun0 firewall in name tun0-fw-in**<br>[edit] |
| Применение правил межсетевого экрана к исходящим пакетам. | admin@neo1# **set interfaces tunnel tun0 firewall out name tun0-fw-out** |

```
[edit]
```

Фиксация настройки.

```
admin@neo1# commit
[edit]
```

Вывод настройки.

```
admin@neo1# show interfaces
tunnel tun0
address 10.20.20.1/24
description “Tunnel to neo2”
dscp 55
encapsulation gre
firewall
   in {
      name tun0-fw-in
   }
   out {
      name tun0-fw-out
   }
}
key 101088
local-ip 192.0.2.1
remote-ip 192.0.2.33
mtu 1460
ttl 220
[edit]
```

#### *7.7.3.2. Настройка узла neo2*

В примере 7.4 приведены дополнительные параметры настройки для оконечного узла туннеля в системе neo2, созданного в примере 7.2:

- Ключ 101088 обеспечивает механизм парольной защиты. Значение должно совпадать с ключом, настроенным на узле neo1.
- Значение TTL установлено равным 220, значение поля DSCP установлено равным 55, а значение MTU установлено равным 1460.

- К туннельному интерфейсу применяются два набора правил межсетевого экрана:
  - 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 7.4 предполагается создание нового туннеля с параметрами из примера 7.2, ниже приведены только отличающиеся параметры.

Для этого необходимо выполнить следующие действия на узле neo2 в режиме настройки.

*Пример 7.4 - Добавление значений в настройку оконечного узла туннеля GRE на узле neo2*

| Действие | Команда |
|---|---|
| Указание ключа аутентификации. | admin@neo2# **set interfaces tunnel tun0 key 101088**<br>[edit] |
| Установка TTL. | admin@neo2# **set interfaces tunnel tun0 ttl 220**<br>[edit] |
| Установка DSCP. | admin@neo2# **set interfaces tunnel tun0 dscp 55**<br>[edit] |
| Установка MTU. | admin@neo2# **set interfaces tunnel tun0 mtu 1460**<br>[edit] |
| Применение правил межсетевого экрана к входящим пакетам. | admin@neo2# **set interfaces tunnel tun0 firewall in name tun0-fw-in**<br>[edit] |
| Применение правил межсетевого экрана | admin@neo2# **set interfaces tunnel** |

к исходящим пакетам.

```
tun0 firewall out name tun0-fw-out
[edit]
```

Фиксация настройки.

```
admin@neo2# commit
[edit]
```

Вывод настройки.

```
admin@neo2# show interfaces
tunnel tun0
address 10.20.20.2/24
description "Tunnel to neo1"
dscp 55
encapsulation gre
firewall {
    in {
        name tun0-fw-in
    }
    out {
        name tun0-fw-out
    }
}
key 101088
local-ip 10.10.1.2
mtu 1460
remote-ip 10.10.1.1
ttl 220
```

## 7.8. 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> encapsulation (см. стр. 402). 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 6.5. Настройка мостов на стр. 263.

## 7.9. Команды 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. |

## 7.9.1. 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 **tun23**.

**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**.

## 7.9.2. 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..tun23 {
    }
}
```

**Параметры**

*tunx*

Обязательный. Идентификатор определяемого туннельного интерфейса. Значение должно лежать в диапазоне от **tun0** до **tun23**.

**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.

## 7.9.3. 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 tun0..tun23 {
```

```
            address ipv4-адрес
        }
    }
```

**Параметры**

*tunx*

Обязательный. Множественный узел. Имя определяемого туннельного интерфейса. Значение должно лежать в диапазоне от **tun0** до **tun23**.

*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.

## 7.9.4. 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 tun0..tun23 {
        description текст
    }
}
```

**Параметры**

*tunx*

Обязательный. Имя определяемого туннельного интерфейса. Значение должно лежать в диапазоне от **tun0** до **tun23**.

*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.

## 7.9.5. 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 tun0..tun23 {
        disable
    }
}
```

**Параметры**

*tunx*

Обязательный. Имя определяемого туннельного интерфейса. Значение должно лежать в диапазоне от **tun0** до **tun23**.

**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.

## 7.9.6. 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 tun0..tun23 {
        dscp текст
    }
}
```

**Параметры**

*tunx*

Обязательный. Имя определяемого туннельного интерфейса. Значение должно лежать в диапазоне от **tun0** до **tun23**.

*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.

## 7.9.7. 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 tun0..tun23 {
        encapsulation [gre|gre-bridge|ipip|sit]
    }
}
```

**Параметры**

*tunx*

Обязательный. Имя определяемого туннельного интерфейса. Значение должно лежать в диапазоне от **tun0** до **tun9**.

**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 не-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 6.5. Настройка мостов на стр. 263.

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 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.

## 7.9.8. 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 tun0..tun23 {
        key 0-999999
    }
}
```

**Параметры**

*tunx*

Обязательный. Имя определяемого туннельного интерфейса. Значение должно лежать в диапазоне от **tun0** до **tun23**.

*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.

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.

## 7.9.9. 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 tun0..tun23 {
        local-ip ipv4-адрес
    }
}
```

**Параметры**

*tunx*

Обязательный. Имя определяемого туннельного интерфейса. Значение должно лежать в диапазоне от **tun0** до **tun23**.

*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.

## 7.9.10. 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 tun0..tun23 {
        mtu 64-8024
    }
}
```

**Параметры**

*tunx*

Обязательный. Имя определяемого туннельного интерфейса. Значение должно лежать в диапазоне от **tun0** до **tun23**.

*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.

## 7.9.11. 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 tun0..tun23 {
        multicast [enable|disable]
    }
```

}

**Параметры**

*tunx*

Обязательный. Имя определяемого туннельного интерфейса. Значение должно лежать в диапазоне от **tun0** до **tun23**.

*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.

## 7.9.12. 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 tun0..tun23 {
          remote-ip ipv4-адрес
     }
}
```

**Параметры**

*tunx*

Обязательный. Имя определяемого туннельного интерфейса. Значение должно лежать в диапазоне от **tun0** до **tun23**.

*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.

## 7.9.13. 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 tun0..tun23 {
          ttl 0-255
     }
}
```

**Параметры**

*tunx*

Обязательный. Имя определяемого туннельного интерфейса. Значение должно лежать в диапазоне от **tun0** до **tun23**.

*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.

## 7.9.14. 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 tun23.

**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 7.5 приведен вывод сведений о состоянии туннельного интерфейса tun0, использующего протокол GRE.

*Пример 7.5 - "show interfaces tunnel": Отображение настройки туннеля*

```
admin@neo:~$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
```

# 8. СТАТИЧЕСКАЯ МАРШРУТИЗАЦИЯ

## 8.1. Пересылка и маршрутизация

В этом разделе описаны эксплуатационные команды для пересылки и базовой маршрутизации.

В данном разделе приведены следующие команды:

*Таблица 28 - Команды пересылки и маршрутизации*

| Эксплуатационные команды | |
|---|---|
| `clear ip prefix-list` | Очистка статистики или состояния для списка префиксов. |
| `clear ip route cache` | Очистка кэша маршрутизации ядра. |
| `show ip forwarding` | Отображение состояния пересылки пакетов IP. |
| `show ip route` | Отображение маршрутов, содержащихся в таблице маршрутизации и таблице пересылки. |
| `show ip route <префикс_подсети_ipv4> longer-prefixes` | Отображение префиксов длины большей, чем длина указанного префикса. |
| `show ip route cache` | Отображение кэша маршрутизации ядра. |
| `show ip route connected` | Отображение маршрутов, подключенных напрямую. |
| `show ip route forward` | Отображение маршрутов, которые содержатся в таблице пересылки (Forwarding Information Base, FIB). |
| `show ip route kernel` | Отображение маршрутов ядра. |
| `show ip route static` | Отображение статических маршрутов. |
| `show ip route summary` | Отображение кратких сведений о маршрутах. |
| `show ip route supernets-only` | Отображение маршрутов вышестоящих сетей. |
| `show tableshow table` | Отображение таблицы маршрутизации системы. |

### 8.1.1. clear ip prefix-list

Очистка статистики или состояния для списка префиксов.

**Синтаксис**

**clear ip 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 сети.

**Значение по умолчанию**

Статистика очищается для всех списков префиксов.

**Указания по использованию**

Команда позволяет очистить статистические данные или состояния для списка префиксов.

### 8.1.2. clear ip route cache

Очистка кэша маршрутизации ядра.

**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.

### 8.1.3. show ip forwarding

Отображение состояния пересылки пакетов IP.

**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 8.1 приведен вывод сведений о состоянии пересылки пакетов IP.

*Пример 8.1 - Отображение состояния пересылки пакетов IP*

```
admin@neo:~$ show ip forwarding
 IP forwarding is on
admin@neo:~$
```

### 8.1.4. show ip route

Отображение маршрутов, содержащихся в таблице маршрутизации и таблице пересылки.

**Синтаксис**

**show ip route** [*ipv4-адрес* | *префикс_подсети_ipv4*]

**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.

**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, RIB).

Маршруты из таблицы пересылки также могут быть выведены посредством команды **show ip route forward** (см. стр. 420).

**Примеры**

В примере 8.2 приведен образец вывода маршрутов из таблицы маршрутизации и таблицы пересылки.

*Пример 8.2 - Отображение маршрутов из таблицы маршрутизации и таблицы пересылки*

```
admin@neo:~$ show ip route

Codes: K - kernel route, C - connected, S - static, R -
RIP, O - OSPF, I - ISIS, B - BGP, > - selected route, * -
FIB route

S>* 0.0.0.0/0 [1/0] via 10.1.0.1, eth0

O 10.1.0.0/24 [110/10] is directly connected, eth0,
05:35:15

C>* 10.1.0.0/24 is directly connected, eth0

O>* 10.192.32.0/24 [110/20] via 10.1.0.45, eth0, 05:35:15

O>* 10.192.128.0/24 [110/11] via 10.1.0.66, eth0,
05:35:15

O>* 10.192.128.1/32 [110/11] via 10.1.0.66, eth0,
05:35:15

O>* 10.192.129.0/24 [110/11] via 10.1.0.66, eth0,
05:35:15

O>* 10.192.130.0/24 [110/11] via 10.1.0.66, eth0,
05:35:15

O>* 10.192.131.0/24 [110/11] via 10.1.0.66, eth0,
05:35:15
```

```
C>* 127.0.0.0/8 is directly connected, lo
O>* 172.16.0.0/24 [110/11] via 10.1.0.4, eth0, 05:35:15
O>* 172.16.1.0/24 [110/11] via 10.1.0.4, eth0, 05:35:15
O>* 172.16.2.0/24 [110/11] via 10.1.0.4, eth0, 05:35:15
O>* 172.16.3.0/24 [110/11] via 10.1.0.4, eth0, 05:35:15
O>* 172.16.4.0/24 [110/11] via 10.1.0.4, eth0, 05:35:15
O>* 172.16.5.0/24 [110/11] via 10.1.0.4, eth0, 05:35:15
O>* 172.16.6.0/24 [110/11] via 10.1.0.4, eth0, 05:35:15
O>* 172.16.7.0/24 [110/11] via 10.1.0.4, eth0, 05:35:15
O>* 172.16.8.0/24 [110/11] via 10.1.0.4, eth0, 05:35:15
O>* 172.16.9.0/24 [110/11] via 10.1.0.4, eth0, 05:35:15
C>* 172.16.234.0/25 is directly connected, eth1
S>* 192.94.202.0/24 [1/0] via 172.16.234.27, eth1
admin@neo:~$
```

В примере 8.3 приведен способ вывода маршрута к адресу 10.192.128.1.

*Пример 8.3 - Отображение сведений о маршрутизации, касающихся указанного адреса*

```
admin@neo:~$ show ip route 10.192.128.1
Routing entry for 10.192.128.1/32
  Known via "ospf", distance 110, metric 11, best
  Last update 09:47:07 ago
  * 10.1.0.66, via eth0
admin@neo:~$
```

### 8.1.5. show ip route <префикс_подсети_ipv4> longer-prefixes

Отображение префиксов длины большей, чем длина указанного префикса.

**Синтаксис**

**show ip route** *префикс_подсети_ipv4* **longer-prefixes**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*префикс_подсети_ipv4*

Обязательный. Отображение префиксов длины большей, чем длина указанного префикса.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Команда используется для вывода всех префиксов большей длины, чем длина указанного IP-адреса или префикса.

**Примеры**

В примере 8.4 приведен вывод префиксов, имеющих длину больше, чем у префикса 10.192.128.0/24.

*Пример 8.4 - Отображение маршрутов, имеющих сетевой префикс длиннее указанного*

```
admin@neo:~$ show ip route 10.192.128.0/24 longer-
prefixes

Codes: K - kernel route, C - connected, S - static, R -
RIP, O - OSPF, I - ISIS, B - BGP, > - selected route, * -
FIB route

O>* 10.192.128.0/24 [110/11] via 10.1.0.66, eth0,
09:36:20

O>* 10.192.128.1/32 [110/11] via 10.1.0.66, eth0,
09:36:20

admin@neo:~$
```

## 8.1.6. show ip route cache

Отображение кэша маршрутизации ядра.

**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. До того, как может быть выполнена маршрутизация по алгоритму ECMP (Equal-Cost-Multi-Path), необходимо иметь несколько путей с равной стоимостью.

**Примеры**

В примере 8.5 приведен вывод списка маршрутов из кэша маршрутизации ядра.

*Пример 8.5 - Вывод списка маршрутов из кэша маршрутизации ядра*

```
admin@neo:~$ show ip route cache
local 10.1.0.62 from 10.1.0.1 dev lo src 10.1.0.62
    cache <local,src-direct> users 1 age 42sec iif eth0
multicast 224.0.0.5 from 10.1.0.45 dev lo src 10.1.0.62
    cache <local,mc> users 1 used 8 age 5sec iif eth0
local 10.1.0.62 from 69.59.150.131 dev lo src 10.1.0.62
    cache <local> users 1 used 3 age 47sec iif eth0
10.1.0.1 from 10.1.0.62 dev eth0
    cache users 1 age 42sec mtu 1500 advmss 1460 hoplimit
64
10.0.0.30 from 10.1.0.62 tos lowdelay via 10.1.0.1 dev
eth0
    cache users 2 age 0sec mtu 1500 advmss 1460 hoplimit
64
multicast 224.0.0.5 from 10.1.0.56 dev lo src 10.1.0.62
    cache <local,mc> users 1 used 8 age 8sec iif eth0
multicast 224.0.0.5 from 10.1.0.66 dev lo src 10.1.0.62
    cache <local,mc> users 1 used 8 age 0sec iif eth0
multicast 224.0.0.6 dev eth0 src 10.1.0.62
    cache <mc> users 1 age 21sec mtu 1500 advmss 1460
```

```
hoplimit 64

multicast 224.0.0.5 from 10.1.0.4 dev lo src 10.1.0.62

    cache <local,mc> users 1 used 9 age 1sec iif eth0

69.59.150.131 via 10.1.0.1 dev eth0 src 10.1.0.62

    cache users 1 age 47sec mtu 1500 advmss 1460 hoplimit
64

multicast 224.0.0.5 dev eth0 src 10.1.0.62

    cache <local,mc> users 1 used 8 age 5sec mtu 1500
advmss 1460 hoplimit 64

69.59.150.131 from 10.1.0.62 via 10.1.0.1 dev eth0

    cache users 1 used 1 age 47sec mtu 1500 advmss 1460
hoplimit 64

local 10.1.0.62 from 10.0.0.30 tos lowdelay dev lo src
10.1.0.62

    cache <local> users 1 used 1 age 0sec iif eth0

admin@neo:~$
```

В примере 8.6 приведен способ вывода сведений о маршруте 10.1.0.62 из кэша маршрутизации ядра.

*Пример 8.6 - Отображение конкретного маршрута из кэша маршрутизации ядра*

```
admin@neo:~$ show ip route cache 10.1.0.62

local 10.1.0.62 from 10.1.0.1 dev lo src 10.1.0.62

    cache <local,src-direct> users 1 used 3 age 9sec iif
eth0

local 10.1.0.62 from 69.59.150.131 dev lo src 10.1.0.62

    cache <local> users 1 used 7 age 102sec iif eth0

local 10.1.0.62 from 10.0.0.30 tos lowdelay dev lo src
10.1.0.62

    cache <local> users 1 used 33 iif eth0

admin@neo:~$
```

### 8.1.7. show ip route connected

Отображение маршрутов, подключенных напрямую.

**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 Altell NEO.

**Примеры**

В примере 8.7 приведен вывод маршрутов, подключенных напрямую.

*Пример 8.7 - Отображение маршрутов, подключенных напрямую*

```
admin@neo:~$ show ip route connected

Codes: K - kernel route, C - connected, S - static, R -
RIP, O - OSPF, I - ISIS, B - BGP, > - selected route, * -
FIB route

C>* 10.1.0.0/24 is directly connected, eth0

C>* 127.0.0.0/8 is directly connected, lo

C>* 172.16.234.0/25 is directly connected, eth1

admin@neo:~$
```

## 8.1.8. show ip route forward

Отображение маршрутов, которые содержатся в таблице пересылки (Forwarding Information Base, FIB).

**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 8.8 показано, как отобразить маршруты, записанные в таблице пересылки.

*Пример 8.8 - Отображение маршрутов из таблицы пересылки*

```
admin@neo:~$ show ip route forward
default via 10.1.0.1 dev eth0 proto zebra
10.1.0.0/24 dev eth0 proto kernel scope link src
10.1.0.62
10.192.32.0/24 via 10.1.0.45 dev eth0 proto zebra metric
20
10.192.128.0/24 via 10.1.0.66 dev eth0 proto zebra metric
11
10.192.128.1 via 10.1.0.66 dev eth0 proto zebra metric 11
10.192.129.0/24 via 10.1.0.66 dev eth0 proto zebra metric
11
10.192.130.0/24 via 10.1.0.66 dev eth0 proto zebra metric
11
10.192.131.0/24 via 10.1.0.66 dev eth0 proto zebra metric
11
172.16.0.0/24 via 10.1.0.4 dev eth0 proto zebra metric 11
172.16.1.0/24 via 10.1.0.4 dev eth0 proto zebra metric 11
172.16.2.0/24 via 10.1.0.4 dev eth0 proto zebra metric 11
172.16.3.0/24 via 10.1.0.4 dev eth0 proto zebra metric 11
172.16.4.0/24 via 10.1.0.4 dev eth0 proto zebra metric 11
```

```
172.16.5.0/24 via 10.1.0.4 dev eth0 proto zebra metric 11

172.16.6.0/24 via 10.1.0.4 dev eth0 proto zebra metric 11

172.16.7.0/24 via 10.1.0.4 dev eth0 proto zebra metric 11

172.16.8.0/24 via 10.1.0.4 dev eth0 proto zebra metric 11

172.16.9.0/24 via 10.1.0.4 dev eth0 proto zebra metric 11

172.16.234.0/25 dev eth1 proto kernel scope link src
172.16.234.23

192.94.202.0/24 via 172.16.234.27 dev eth1 proto zebra

admin@neo:~$
```

В примере 8.9 показано, как отобразить сведения о маршруте 10.1.0.0/24 из таблицы пересылки.

*Пример 8.9 - Отображение сведений о маршруте из таблицы пересылки*

```
admin@neo:~$ show ip route forward 10.1.0.0/24

10.1.0.0/24 dev eth0 proto kernel scope link src
10.1.0.62

admin@neo:~$
```

### 8.1.9. show ip route kernel

Отображение маршрутов ядра.

**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 10.172.24.0 netmask 255.255.255.0 gw
```

```
10.1.0.1
```

**Примеры**

В примере 8.10 показано, как отобразить маршруты ядра.

*Пример 8.10 - Отображение маршрутов ядра*

```
admin@neo:~$ show ip route kernel

Codes: K - kernel route, C - connected, S - static, R -
RIP, O - OSPF, I - ISIS, B - BGP, > - selected route, * -
FIB route

K>* 10.172.24.0/24 via 10.1.0.1, eth0

admin@neo:~$
```

## 8.1.10. show ip route static

Отображение статических маршрутов.

**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 8.11 показано, как вывести список статических маршрутов.

*Пример 8.11 - Отображение списка статических маршрутов*

```
admin@neo:~$ show ip route static

Codes: K - kernel route, C - connected, S - static, R -
RIP, O - OSPF, I - ISIS, B - BGP, > - selected route, * -
FIB route

S>* 0.0.0.0/0 [1/0] via 10.1.0.1, eth0
```

```
S>* 192.94.202.0/24 [1/0] via 172.16.234.27, eth1
admin@neo:~$
```

### 8.1.11. show ip route summary

Отображение кратких сведений о маршрутах.

**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 8.12 показано, как вывести сводную информацию о маршрутах.

*Пример 8.12 - Отображение сводной информации о маршрутах*

```
admin@neo:~$ show ip route summary
Route Source   Routes    FIB
connected      4         4
static         2         2
ospf           1         0
ebgp           0         0
ibgp           289016    289011
---
Totals         289023    289017
[edit]
```

### 8.1.12. show ip route supernets-only

Отображение маршрутов вышестоящих сетей.

**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 8.13 показано, как вывести список маршрутов вышестоящих сетей.

*Пример 8.13 - Отображение маршрутов вышестоящих сетей*

```
admin@neo:~$ show ip route supernets-only

Codes: K - kernel route, C - connected, S - static, R -
RIP, O - OSPF, I - ISIS, B - BGP, > - selected route, * -
FIB route

S>* 0.0.0.0/0 [1/0] via 10.1.0.1, eth0
```

### 8.1.13. show table

Отображение таблицы маршрутизации системы.

**Синтаксис**

**show table**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для отображения таблицы маршрутизации Altell NEO.

**Примеры**

В примере 8.14 показано, как вывести таблицу маршрутизации.

*Пример 8.14 - Отображение таблицы маршрутизации*

```
admin@neo:~$ show table
table 0
```

## 8.2. Настройка статических маршрутов

В этом разделе рассматриваются следующие вопросы:

- Обзор статических маршрутов.
- Настройка статических маршрутов.
- Плавающие статические маршруты.

### 8.2.1. 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 Altell NEO. Однако, если канал терпит сбой, маршрутизатор удалит из таблицы маршрутизации маршруты, в том числе статические, в которых этот интерфейс использовался для достижения следующего транзитного участка.

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.

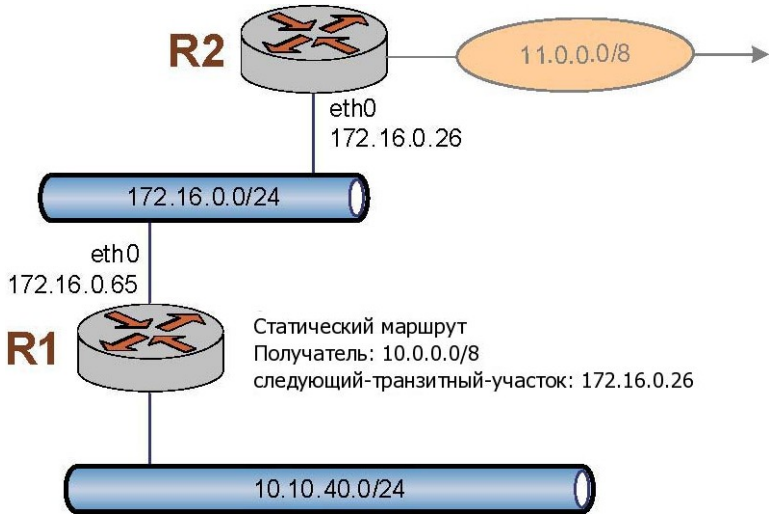
Все маршруты, которые маршрутизатор получает из настройки или от протоколов динамической маршрутизации, хранятся в таблице маршрутизации (RIB).

Одноадресные маршруты непосредственно используются для определения таблицы пересылки, используемой для пересылки пакетов одноадресной передачи.

### 8.2.2. Настройка статических маршрутов

В этом примере представлены образцы настроек для основных статических маршрутов. После выполнения всех действий система будет настроена в соответствии с рис. 11. В этом примере создается статический маршрут, фактически указывающий, что “все пакеты, адресованные в сеть 11.0.0.0/8, следует переслать на адрес 172.16.0.26”.

*Рисунок 11 - Статические маршруты*




В этом разделе имеются следующие примеры:

- Пример 8.15 Создание статического маршрута.

В примере 8.15 выполняется создание статического маршрута к сети 11.0.0.0/8, направляемого через узел 172.16.0.26. Для создания статического маршрута необходимо выполнить следующую последовательность команд в режиме настройки:

*Пример 8.15 - Создание статического маршрута*

| Действие | Команда |
|---|---|
| Создание статического маршрута к R2. | admin@R1# **set protocols static route 11.0.0.0/8 next-hop 172.16.0.26**<br>[edit] |
| Фиксация настройки. | admin@R1# **commit**<br>[edit] |

### 8.2.3. 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.

## 8.3. Средства наблюдения за сведениями о статических маршрутах

В этом разделе рассматриваются следующие вопросы:

- Эксплуатационные команды статической маршрутизации.
- Вывод статических маршрутов в таблице маршрутизации.

### 8.3.1. Эксплуатационные команды статической маршрутизации

Следующие эксплуатационные команды используются для отображения сведений о статических маршрутах.

| Эксплуатационные команды | |
|---|---|
| `show ip route` | Вывод сведений о маршрутах, которые содержатся в таблице маршрутизации. |

В этом разделе представлены следующие примеры:

- Пример 8.16 Просмотр статических маршрутов в таблице маршрутизации.

### 8.3.2. Вывод статических маршрутов в таблице маршрутизации

Для отображения сведений о маршруте используется команда **show ip route**. Для того чтобы просмотреть только статические маршруты, используется команда **show ip route static**, как показано в примере 8.16.

*Пример 8.16 - Просмотр статических маршрутов в таблице маршрутизации*

```
admin@R1:~$ show ip route static
 Codes: K - kernel route, C - connected, S - static, R - RIP, O -
OSPF, I - ISIS, B - BGP, > - selected route, * - FIB route
S>* 0.0.0.0/0 [1/0] via 10.1.0.1, eth0
S>* 10.7.0.48/28 [1/0] via 10.6.0.57, eth1
admin@R1:~$
```

## 8.4. Команды статической маршрутизации

В данном разделе приведены следующие команды:

*Таблица 29 - Команды настройки статической маршрутизации*

| Команды настройки | |
|---|---|
| `protocols static interface-route <подсеть> next-hop-interface <ethx>` | Установка интерфейса следующего транзитного участка для статического маршрута, основанного на интерфейсе. |
| `protocols static route <подсеть> blackhole` | Настройка статического маршрута в "черную дыру". |

| | |
|---|---|
| `protocols static route <подсеть> next-hop <адрес>` | Установка следующего транзитного участка статического маршрута. |

## 8.4.1. protocols static interface-route <подсеть> next-hop-interface <ethx>

Установка интерфейса следующего транзитного участка для статического маршрута, основанного на интерфейсе.

**Синтаксис**

**set protocols static interface-route** *подсеть* **next-hop-interface** *ethx* **[disable | distance** *расстояние***]**

**delete protocols static interface-route** *подсеть* **next-hop-interface** *ethx* **[disable | distance]**

**show protocols static interface-route** *подсеть* **next-hop-interface** *ethx* **[disable | distance]**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
     static {
          interface-route подсеть_ipv4 {
               next-hop-interface eth0..eth23 {
                    disable distance 1-255
               }
          }
     }
}
```

**Параметры**

*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.**

*ethx*

Обязательный. Интерфейс Ethernet следующего транзитного участка.

**disable**

Отключение статического маршрута на основе интерфейса.

*расстояние*

Необязательный. Установка расстояния следующего транзитного участка 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.

Форма **set** данной команды позволяет указать интерфейс следующего транзитного участка для данного маршрута.

Форма **delete** данной команды позволяет удалить интерфейс следующего транзитного участка.

Форма **show** позволяет просмотреть интерфейс следующего транзитного участка для данного маршрута.

## 8.4.2. protocols static route <подсеть> blackhole

Настройка статического маршрута в "черную дыру".

**Синтаксис**

**set protocols static route** *подсеть* **blackhole** [**distance** *расстояние*]

**delete protocols static route** *подсеть* **blackhole** [**distance**]

**show protocols static route** *подсеть* **blackhole** [**distance**]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

protocols {

```
        static {
            route подсеть_ipv4 {
                blackhole {
                    distance 1-255
                }
            }
        }
    }
```

**Параметры**

*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".

### 8.4.3. protocols static route <подсеть> next-hop <адрес>

Установка следующего транзитного участка статического маршрута.

**Синтаксис**

**set protocols static route** *подсеть* **next-hop** *адрес* [**disable** | **distance** *расстояние* ]

**delete protocols static route** *подсеть* **next-hop** *адрес* **[disable | distance]**

**show protocols static route** *подсеть* **next-hop** *адрес* **[disable | distance]**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
     static {
          route префикс_подсети_ipv4 {
               next-hop ipv4-адрес {
                    disable distance 1-255
               }
          }
     }
}
```

**Параметры**

*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**.

*адрес*

Обязательный. Адрес маршрутизатора следующего транзитного участка.

**disable**

Отключение статического маршрута.

*расстояние*

Необязательный. Установка расстояния следующего транзитного участка 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 участок для данного маршрута.

Форма **delete** данной команды позволяет удалить следующий транзитный участок для статического маршрута.

Форма **show** данной команды позволяет вывести настройку следующего транзитного участка для статического маршрута.

# 9. НАСТРОЙКА RIP

В этом разделе даны указания по настройке протокола RIP на системе Altell NEO.

Рассматриваются следующие вопросы:

- Обзор RIP.
- Поддерживаемые стандарты.
- Настройка RIP.

## 9.1. 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 участков до получателя. Максимальное число транзитных участков — 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.

## 9.2. Поддерживаемые стандарты

Реализация протокола RIP соответствует следующим стандартам:

- RFC 1058: Routing Information Protocol.
- RFC 2453: RIP Version 2.

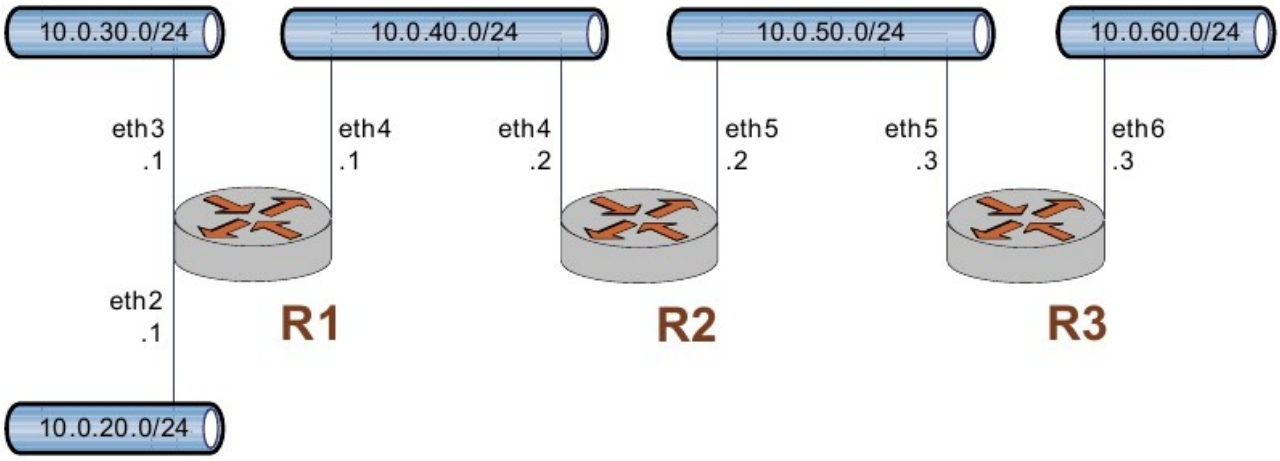
## 9.3. Настройка RIP

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 рис. 12.

*Рисунок 12 - Эталонная схема настройки RIP*




### 9.3.1. Основная настройка RIP

В данном разделе выполняется настройка протокола RIP на маршрутизаторах, обозначенных на эталонной схеме как R1, R2 и R3. Эти маршрутизаторы объявляют свои маршруты в сетях 10.0.40.0/24 и 10.0.50.0/24.

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 9.1 - Основная настройка RIP*

| Маршрутизатор | Действие | Команда (команды) |
|---|---|---|
| R1 | Объявление для сети 10.0.40.0/24. | `admin@R1# set protocols rip network 10.0.40.0/24`<br>`[edit]` |
| R1 | Перераспределение непосредственно подключенных маршрутов на RIP. | `admin@R1# set protocols rip redistribute connected`<br>`[edit]` |

| | | |
|---|---|---|
| R1 | Фиксация настройки. | admin@R1# **commit**<br>[edit] |
| R1 | Отображение настройки. | admin@R1# **show protocols**<br>rip {<br>network 10.0.40.0/24<br>redistribute {<br>connected {<br>}<br>}<br>}<br>[edit] |
| R2 | Объявление для сети 10.0.40.0/24. | admin@R2# **set protocols rip network 10.0.40.0/24**<br>[edit] |
| R2 | Объявление для сети 10.0.50.0/24. | admin@R2# **set protocols rip network 10.0.50.0/24**<br>[edit] |
| R2 | Перераспределение непосредственно подключенных маршрутов на RIP. | admin@R2# **set protocols rip redistribute connected**<br>[edit] |
| R2 | Фиксация настройки. | admin@R2# **commit**<br>[edit] |
| R2 | Отображение настройки. | admin@R2# **show protocols**<br>rip {<br>network 10.0.40.0/24<br>network 10.0.50.0/24<br>redistribute {<br>connected { |

```
            }
        }
    }
    [edit]
```

| | | |
|---|---|---|
| R3 | Объявление для сети 10.0.50.0/24. | `admin@R3# set protocols rip network 10.0.50.0/24`<br>`[edit]` |
| R3 | Перераспределение непосредственно подключенных маршрутов на RIP. | `admin@R3# set protocols rip redistribute connected`<br>`[edit]` |
| R3 | Фиксация настройки. | `admin@R3# commit`<br>`[edit]` |
| R3 | Отображение настройки. | `admin@R3# show protocols`<br>`rip {`<br>`  network 10.0.50.0/24`<br>`  redistribute {`<br>`  connected {`<br>`  }`<br>`  }`<br>`}`<br>`[edit]` |

## 9.3.2. Проверка настройки RIP

Для проверки настройки RIP можно использовать следующие команды эксплуатационного режима.

### *9.3.2.1. R3: show ip route*

В примере 9.2 приведен образец вывода команды **show ip route** для маршрутизатора R3.

*Пример 9.2 - Проверка RIP на R3: ”show ip route”*

```
admin@R3:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O -
OSPF, I - ISIS, B - BGP, > - selected route, * - FIB route
R>* 10.0.20.0/24 [120/3] via 10.0.50.2, eth5, 00:20:16
R>* 10.0.30.0/24 [120/3] via 10.0.50.2, eth5, 00:34:04
R>* 10.0.40.0/24 [120/2] via 10.0.50.2, eth5, 02:15:26
C>* 10.0.50.0/24 is directly connected, eth5
C>* 10.0.60.0/24 is directly connected, eth6
C>* 127.0.0.0/8 is directly connected, lo
admin@R3:~$
```

Из вывода видно, что маршруты к 10.0.20.0/24, 10.0.30.0/24 и 10.0.40.0/24 получены по RIP и что пакеты к этим сетям будут пересылаться наружу через интерфейс eth5 на 10.0.50.2. Сети 10.0.50.0/24 и 10.0.60.0/24 подключены непосредственно.

#### *9.3.2.2. R3: show ip rip*

В результате выполнения команды **show ip rip** для R3 отображаются аналогичные сведения, но в другом формате, что представлено в примере 9.3.

*Пример 9.3 - Проверка RIP на R3: “show ip rip”*

```
admin@R3:~$ 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) 10.0.20.0/24   10.0.50.2 3    10.0.50.2 0    00:23
R(n) 10.0.30.0/24   10.0.50.2 3    10.0.50.2 0    00:23
R(n) 10.0.40.0/24   10.0.50.2 2    10.0.50.2 0    00:23
C(i) 10.0.50.0/24   0.0.0.0   1    self 0
C(r) 10.0.60.0/24   0.0.0.0   1 self (connected:1)     0
```

Из вывода видно, что сети 10.0.20.0/24, 10.0.30.0/24 и 10.0.40.0/24 получены по RIP и что пакеты к этим сетям будут направлены на 10.0.50.2. Сети 10.0.50.0/24 и 10.0.60.0/24 подключены непосредственно.

#### *9.3.2.3. R3: ping 10.0.20.1*

При помощи команды **ping** с маршрутизатора R3 можно убедиться, что узлы в удаленных сетях достижимы. В данном случае проверяется достижимость IP-адреса маршрутизатора R1. Результат показан в примере 9.4.

*Пример 9.4 - Проверка RIP на R3: "ping 10.0.20.1"*

```
admin@R3:~$ ping 10.0.20.1
PING 10.0.20.1 (10.0.20.1) 56(84) bytes of data.
64 bytes from 10.0.20.1: icmp_seq=1 ttl=63 time=7.39 ms
64 bytes from 10.0.20.1: icmp_seq=2 ttl=63 time=1.56 ms
64 bytes from 10.0.20.1: icmp_seq=3 ttl=63 time=1.49 ms
^C
-- 10.0.20.1 ping statistics --
3 packets transmitted, 3 received, 0% packet loss, time 2002ms rtt
min/avg/max/mdev = 1.497/3.482/7.390/2.763 ms
```

Тем самым получено подтверждение работоспособности настройки RIP и достижимости уделенной сети.

## 9.4. Команды настройки на уровне маршрутизатора

В данном разделе описаны команды для настройки протокола RIP на уровне маршрутизатора.

В данном разделе описаны следующие команды.

| Команды настройки | |
|---|---|
| `protocols rip default-distance <расстояние>` | Установка административного расстояния 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 <ethx>` | Включение протокола RIP на интерфейсе. |
| `protocols rip neighbor <ipv4-адрес>` | Определение маршрутизатора, соседнего по RIP. |
| `protocols rip network <подсеть_ipv4>` | Указание подсети для протокола RIP. |
| `protocols rip network-distance <подсеть_ipv4>` | Указание административного расстояния до подсети RIP. |
| `protocols rip passive-interface <ethx>` | Установка пассивного режима для указанного интерфейса. |
| `protocols rip route <подсеть_ipv4>` | Указание статического маршрута RIP. |
| `protocols rip timers garbage-collection <секунды>` | Установка таймеров для сборки мусора RIP. |
| `protocols rip timers timeout <секунды>` | Установка интервала для времени неактивности RIP. |
| `protocols rip timers update <секунды>` | Установка таймера для обновления таблицы маршрутизации RIP. |
| `Эксплуатационные команды` | |
| `debug rip events` | Включение или отключение вывода отладочных сообщений, относящихся к событиям RIP. |
| `debug rip packet` | Включение или отключение вывода отладочных сообщений, относящихся ко всем типам пакетов RIP. |

| | |
|---|---|
| `debug rip zebra` | Включение или отключение вывода отладочных сообщений для процесса Zebra, работающего с протоколом RIP. |
| `show debugging rip` | Отображение флагов отладки протокола RIP. |
| `show ip route rip` | Отображение всех маршрутов RIP по IP. |
| `show ip rip` | Отображение сведений о протоколе RIP. |

### 9.4.1. debug rip events

Включение или отключение вывода отладочных сообщений, относящихся к событиям RIP.

**Синтаксис**

**debug rip events**

**no debug rip events**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для включения вывода сообщений уровня трассировки, относящихся к событиям протокола RIP.

Форма **no** этой команды используется для отключения вывода отладочных сообщений для событий RIP.

### 9.4.2. debug rip packet

Включение или отключение вывода отладочных сообщений, относящихся ко всем типам пакетов RIP.

**Синтаксис**

**debug rip packet** [**recv** [**detail**] | **send** [**detail**]]

**no debug rip packet** [**recv** | **send** ]

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**recv**

Необязательный. Вывод отладочных данных для всех принятых пакетов.

**recv detail**

Необязательный. Вывод подробных отладочных данных для всех принятых пакетов.

**send**

Необязательный. Вывод отладочных данных для всех отправленных пакетов.

**send detail**

Необязательный. Вывод подробных отладочных данных для всех отправленных пакетов.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для включения вывода сообщений уровня трассировки, относящихся ко всем типам пакетов протокола RIP.

Форма **no** этой команды используется для отключения вывода отладочных сообщений, относящихся ко всем типам пакетов протокола RIP.

### 9.4.3. debug rip zebra

Включение или отключение вывода отладочных сообщений для процесса Zebra, работающего с протоколом RIP.

**Синтаксис**

**debug rip zebra**

**no debug rip 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 трассировки, относящихся к процессу Zebra, работающему с протоколом RIP.

Форма **no** этой команды используется для отключения вывода отладочных сообщений, относящихся к процессу Zebra, работающему с протоколом RIP.

### 9.4.4. protocols rip default-distance <расстояние>

Установка административного расстояния для RIP.

**Синтаксис**

**set protocols rip default-distance** *расстояние*

**delete protocols rip default-distance**

**show protocols rip default-distance**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
          rip {
               default-distance 1-255
          }
}
```

**Параметры**

*расстояние*

Обязательный. Установка административного расстояния по умолчанию для протокола RIP. Значение должно лежать в диапазоне от 1 до 255. Значение по умолчанию равно 120.

**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.

### 9.4.5. 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 originate
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
        rip {
            default-information {
                originate
            }
        }
}
```

**Параметры**

Отсутствуют.

**Значение по умолчанию**

По умолчанию система не создает внешний маршрут по умолчанию 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.

### 9.4.6. 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 1-16
          }
}
```

**Параметры**

*метрика*

Обязательный. Метрика будет назначена внешним маршрутам, импортированным в RIP для перераспределения. Значение должно лежать в диапазоне от 1 до 16. Значение по умолчанию равно 1.

**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.

## 9.4.7. protocols rip interface <ethx>

Включение протокола RIP на интерфейсе.

**Синтаксис**

```
set protocols rip interface ethx
delete protocols rip interface ethx
show protocols rip interface ethx
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
        rip {
            interface eth0..eth23
        }
}
```

**Параметры**

*ethx*

Обязательный. Множественный узел. Имя определенного интерфейса Ethernet.

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.

### 9.4.8. protocols rip neighbor <ipv4-адрес>

Определение маршрутизатора, соседнего по RIP.

**Синтаксис**

```
set protocols rip neighbor ipv4-адрес
delete protocols rip neighbor ipv4-адрес
show protocols rip neighbor
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
        rip {
            neighbor ipv4-адрес
        }
}
```

**Параметры**

*ipv4-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.

### 9.4.9. protocols rip network <подсеть_ipv4>

Указание подсети для протокола RIP.

**Синтаксис**

**set protocols rip network** *подсеть_ipv4*

**delete protocols rip network** *подсеть_ipv4*

**show protocols rip network**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
        rip {
            network подсеть_ipv4
        }
}
```

**Параметры**

*подсеть_ipv4*

Обязательный. Множественный узел. Адрес подсети RIP в формате подсети IP.

Можно определить более одной подсети 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.

### 9.4.10. protocols rip network-distance <подсеть_ipv4>

Указание административного расстояния до подсети RIP.

**Синтаксис**

**set protocols rip network-distance** *подсеть_ipv4* {**access-**

**list** *имя_списка* | **distance** *расстояние*}

**delete protocols rip network-distance** *подсеть_ipv4* [**access-list** *имя_списка* | **distance** *расстояние*]

**show protocols rip network-distance** *подсеть_ipv4* [**access-list** | **distance**]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
        rip {
            network-distance подсеть_ipv4 {
                access-list текст
                distance 1-255
            }
        }
}
```

**Параметры**

*подсеть_ipv4*

Обязательный. Адрес в формате подсети IP, определяющий подсеть.

*имя_списка*

Имя списка доступа, применяемого к указанной подсети.

*расстояние*

Административное расстояние, применяемое к указанной подсети. Значение должно лежать в диапазоне от 1 до 255. Значение по умолчанию равно 120.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Форма **set** этой команды используется для установки административного расстояния до подсети RIP или для применения списка доступа к подсети RIP.

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 **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.

## 9.4.11. protocols rip passive-interface <ethx>

Установка пассивного режима для указанного интерфейса.

**Синтаксис**

```
set protocols rip passive-interface ethx
delete protocols rip passive-interface ethx
show protocols rip passive-interface
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
        rip {
            passive-interface eth0..eth23
        }
}
```

**Параметры**

*ethx*

Обязательный. Множественный узел. Имя настроенного интерфейса Ethernet, 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.

## 9.4.12. protocols rip route <подсеть_ipv4>

Указание статического маршрута RIP.

**Синтаксис**

**set protocols rip route** *подсеть_ipv4*

**delete protocols rip route** *подсеть_ipv4*

**show protocols rip route**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
          rip {
               route подсеть_ipv4
          }
}
```

**Параметры**

*подсеть_ipv4*

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.

## 9.4.13. protocols rip timers garbage-collection <секунды>

Установка таймеров для сборки мусора RIP.

**Синтаксис**

**set protocols rip timers garbage-collection** *секунды*

**delete protocols rip timers garbage-collection** [*секунды*]

**show protocols rip timers garbage-collection**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
          rip {
               timers {
                    garbage-collection 5-2147483647
               }
          }
}
```

**Параметры**

*секунды*

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.

## 9.4.14. protocols rip timers timeout <секунды>

Установка интервала для времени неактивности RIP.

**Синтаксис**

```
set protocols rip timers timeout секунды
delete protocols rip timers timeout [секунды]
show protocols rip timers timeout
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
          rip {
               timers {
                    timeout 5-2147483647
               }
          }
}
```

**Параметры**

*секунды*

Обязательный. Интервал неактивности RIP в секундах. Значение должно лежать в диапазоне от 5 до 2147483647. Значение по умолчанию равно 180.

**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.

## 9.4.15. protocols rip timers update <секунды>

Установка таймера для обновления таблицы маршрутизации RIP.

**Синтаксис**

**set protocols rip timers update** *секунды*

**delete protocols rip timers update [***секунды***]**

**show protocols rip timers update**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
          rip {
               timers {
                    update 5-2147483647
               }
          }
}
```

**Параметры**

*секунды*

Обязательный. Интервал. с которым происходит обновление таблиц маршрутизации RIP. Значение должно лежать в диапазоне от 5 до 2147483647. Значение по умолчанию равно 30.

**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.

## 9.4.16. show debugging rip

Отображение флагов отладки протокола RIP.

**Синтаксис**

```
show debug rip
```

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для вывода режима отладки RIP.

## 9.4.17. 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 9.5 приведен образец вывода всех маршрутов RIP из таблицы RIB.

*Пример 9.5 - "show ip route rip": отображение маршрутов*

```
admin@neo:~$ show ip route rip
Codes: K - kernel route, C - connected, S - static, R - RIP, O -
OSPF,
I - ISIS, B - BGP, > - selected route, * - FIB route
```

## 9.4.18. 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 9.6 приведен образец вывода сведений о протоколе RIP.

*Пример 9.6 - "show ip rip": отображение сведений RIP*

```
admin@neo:~$   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
C(i) 192.168.1.0/24 0.0.0.0   1 self    0
```

```
admin@neo:~$
```

## 9.5. Команды перераспределения маршрутов

В этом разделе описаны команды перераспределения маршрутов с других протоколов маршрутизации на RIP.

| Команды настройки | |
|---|---|
| `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. |
| Эксплуатационные команды | |
| Отсутствуют | |

### 9.5.1. 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 1-16
                    route-map текст
                }
            }
        }
}
```

**Параметры**

*метрика*

Метрика маршрутизации для применения к маршрутам BGP, импортируемым в таблицы маршрутизации RIP. Значение должно лежать в диапазоне от 1 до 16. Значение по умолчанию равно 1.

*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.

## 9.5.2. 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 1-16
                         route-map текст
                    }
               }
          }
}
```

**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. Значение по умолчанию равно 1.

*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.

## 9.5.3. 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 1-16
                        route-map текст
                    }
                }
            }
        }
```

**Параметры**

*метрика*

Необязательный. Метрика маршрутизации для применения к маршрутам ядра, импортируемым в таблицы маршрутизации RIP. Значение должно лежать в диапазоне от 1 до 16. Значение по умолчанию равно 1.

*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.

## 9.5.4. 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 1-16
                         route-map текст
                    }
               }
          }
}
```

**Параметры**

*метрика*

Необязательный. Метрика маршрутизации для применения к маршрутам OSPF, импортируемым в таблицы маршрутизации RIP. Значение должно лежать в диапазоне от 1 до 16. Значение по умолчанию равно 1.

*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.

### 9.5.5. 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 1-16
                         route-map текст
                    }
               }
          }
}
```

**Параметры**

*метрика*

Необязательный. Метрика маршрутизации для применения к статическим маршрутам, импортируемым в таблицы маршрутизации RIP. Значение должно лежать в диапазоне от 1 до 16. Значение по умолчанию равно 1.

*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.

## 9.6. Команды фильтрации маршрутов RIP

В данном разделе описаны команды фильтрации маршрутов RIP. Рассматриваются следующие команды:

| Команды настройки | |
|---|---|
| `protocols rip distribute-list access-list` | Применение списка доступа к фильтрации входящих или исходящих пакетов RIP. |
| `protocols rip distribute-list interface <ethx> access-list` | Применение списка доступа к конкретному интерфейсу для фильтрации входящих или исходящих пакетов RIP. |

| | |
|---|---|
| `protocols rip distribute-list interface <ethx> 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. |

Эксплуатационные команды

Отсутствуют.

### 9.6.1. 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_для_входящих* | **out** *список_для_исходящих*}

**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 целоебеззнака32разр
                         out целоебеззнака32разр
                    }
               }
          }
}
```

**Параметры**

*список_для_входящих*

Идентификатор определенного списка доступа. Указанный список доступа будет применен к фильтрации входящих пакетов RIP.

*список_для_исходящих*

Идентификатор определенного списка доступа. Указанный список доступа будет применен к фильтрации исходящих 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.

## 9.6.2. protocols rip distribute-list interface <ethx> access-list

Применение списка доступа к конкретному интерфейсу для фильтрации входящих или исходящих пакетов RIP.

**Синтаксис**

**set protocols rip distribute-list interface** *ethx* **access-list** {**in** *список_для_входящих* | **out** *список_для_исходящих*]

**delete protocols rip distribute-list interface** *ethx* **access-list** {**in** | **out**}

**show protocols rip distribute-list interface** *ethx* **access-list** {**in** | **out**}

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
        rip {
            distribute-list {
                interface eth0..eth23
                access-list {
```

```
                                    in целоебеззнака32разр
                                    out целоебеззнака32разр
                                    }
                                }
                            }
                        }
                }
```

**Параметры**

*ethx*

Обязательный. Интерфейс, на котором будет выполняться фильтрация пакетов.

*список_для_входящих*

Идентификатор определенного списка доступа. Указанный список доступа будет применен к фильтрации входящих пакетов RIP на указанном интерфейсе.

*список_для_исходящих*

Идентификатор определенного списка доступа. Указанный список доступа будет применен к фильтрации исходящих 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.

### 9.6.3. protocols rip distribute-list interface <ethx> prefix-list

Применение списка префиксов к конкретному интерфейсу для фильтрации входящих

или исходящих пакетов RIP.

**Синтаксис**

**set protocols rip distribute-list interface** *ethx* **prefix-list** {**in** *список_для_входящих* | **out** *список_для_исходящих*}

**delete protocols rip distribute-list interface** *ethx* **prefix-list** {**in** | **out**}

**show protocols rip distribute-list interface** *ethx* **prefix-list** {**in** | **out**}

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
          rip {
               distribute-list {
                    interface eth0..eth23
                    prefix-list {
                         in текст
                         out текст
                         }
                    }
               }
          }
}
```

**Параметры**

*ethx*

Обязательный. Интерфейс, к которому будет применен фильтр по списку префиксов.

*список_для_входящих*

Идентификатор определенного списка префиксов. Указанный список префиксов будет применен к фильтрации входящих пакетов RIP на указанном интерфейсе.

*список_для_исходящих*

Идентификатор определенного списка префиксов. Указанный список префиксов будет применен к фильтрации исходящих 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.

## 9.6.4. 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_для_входящих* | **out** *список_для_исходящих*}

**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 текст
                         out текст
                    }
```

```
                    }
                }
            }
```

**Параметры**

*список_для_входящих*

Идентификатор определенного списка префиксов. Указанный список префиксов будет применен к фильтрации входящих пакетов RIP.

*список_для_исходящих*

Идентификатор определенного списка префиксов. Указанный список префиксов будет применен к фильтрации исходящих 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.

## 9.7. Команды RIP для интерфейсов

В данном разделе описаны команды настройки RIP на различных интерфейсах. Рассматриваются следующие команды:

| Команды настройки | |
|---|---|
| `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

Отсутствуют.

## 9.7.1. 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 текст {
        ip {
            rip
        }
}
```

**Параметры**

*интерфейс*

Обязательный. Тип интерфейса. Подробное описание ключевых слов и аргументов приведено в Приложении 3 на стр. 2105.

**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.

### 9.7.2. interfaces <интерфейс> ip rip authentication

Указание аутентификации RIP на интерфейсе.

**Синтаксис**

**set interfaces** *интерфейс* **ip rip authentication** [**md5** *ключ_md5* **password** *пароль_md5* | **plaintext-password** *пароль*]

**delete interfaces** *интерфейс* **ip rip authentication** [**md5** *ключ_md5* **password** | **plaintext-password**]

**show interfaces** *интерфейс* **ip rip authentication** [**md5** *ключ_md5* **password** | **plaintext-password**]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces текст {
          ip {
               rip {
                    authentication {
                         md5 целоебеззнака32разр {
     password текст
                         }
                         plaintext-password текст
                    }
               }
          }
}
```

**Параметры**

*интерфейс*

Обязательный. Тип интерфейса. Подробное описание ключевых слов и аргументов приведено в Приложении 3 на стр. 2105.

*ключ_md5*

Необязательный. Идентификатор ключа аутентификации. Он должен быть одинаковым на отправляющей и принимающей системах. Значение должно

лежать в диапазоне от 1 до 255.

*пароль_md5*

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 хэш-кода из содержимого пакета и пароля RIP. Вычисленное значение хэш-кода и ключ MD5 включаются в состав передаваемого пакета, и принимающая система (настроенная с тем же самым паролем) вычисляет свой хэш-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.

### 9.7.3. 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 текст {
          ip {
               rip {
                    split-horizon {
                         disable
                         poison-reverse
                    }
               }
          }
}
```

**Параметры**

*интерфейс*

Обязательный. Тип интерфейса. Подробное описание ключевых слов и аргументов приведено в Приложении 3 на стр. 2105.

**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 участков 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.

# 10. НАСТРОЙКА OSPF

В данном разделе даны указания по настройке протокола OSPF на системе Altell NEO.

Рассматриваются следующие вопросы:

- Обзор OSPF.
- Поддерживаемые стандарты.
- Настройка OSPF.

## 10.1. 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.

## 10.2. Поддерживаемые стандарты

Реализация протокола OSPF соответствует следующем у стандарту:

- RFC 2328: OSPF Version 2.

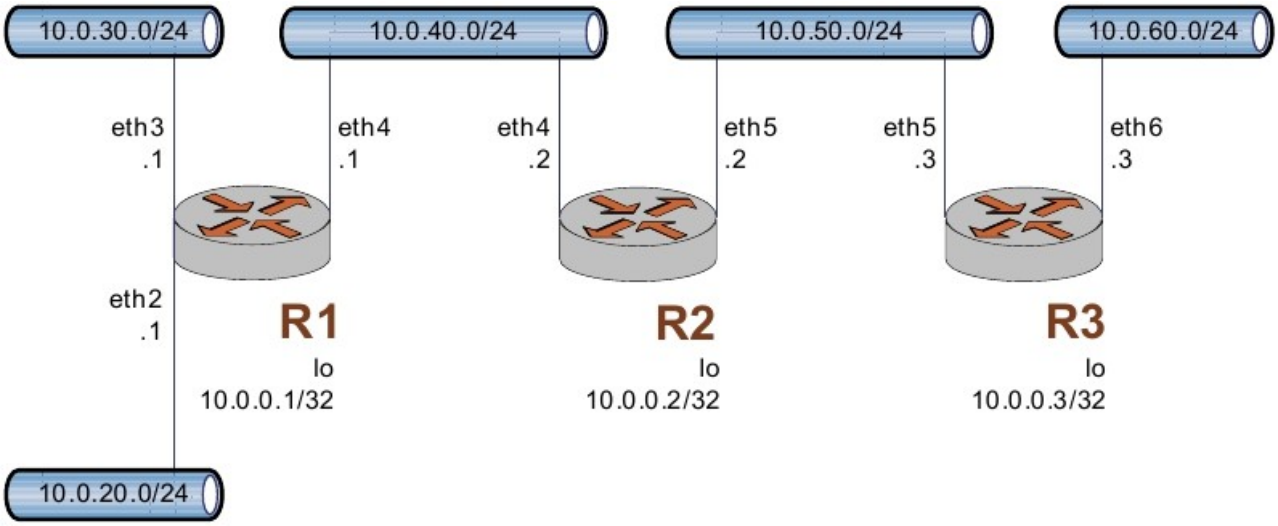
## 10.3. Настройка OSPF

В этом разделе рассматриваются следующие вопросы:

- Основная настройка OSPF.
- Проверка настройки OSPF.

В данном разделе описан пример настройки для протокола OSPF. Пример настройки основан на эталонной схеме, приведенной на рис. 13.

*Рисунок 13 - Эталонная схема настройки OSPF*




### 10.3.1. Основная настройка OSPF

В данном разделе выполняется настройка протокола OSPF на маршрутизаторах, обозначенных на эталонной схеме как R1, R2 и R3. Это маршрутизаторы объявляют свои маршруты в сетях 10.0.40.0/24 и 10.0.50.0/24.

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 10.1 - Основная настройка OSPF*

| Маршрутизатор | Действие | Команда (команды) |
|---|---|---|
| R1 | Установка адреса интерфейса заглушки в качестве идентификатора маршрутизатора в OSPF. | admin@R1# **set protocols ospf parameters router-id 10.0.0.1**<br>[edit] |
| R1 | Объявление в сети 10.0.40.0/24. | admin@R1# **set protocols ospf area 0.0.0.0 network 10.0.40.0/24**<br>[edit] |
| R1 | Перераспределение непосредственно подключенных маршрутов на OSPF | admin@R1# **set protocols ospf redistribute connected**<br>[edit] |
| R1 | Фиксация настройки. | admin@R1# **commit**<br>[edit] |
| R1 | Отображение настройки. | admin@R1# **show protocols**<br>ospf {<br>area 0.0.0.0 {<br>network 10.0.40.0/24<br>}<br>parameters {<br>router-id 10.0.0.1<br>}<br>redistribute {<br>connected {<br>}<br>} |

| | | |
|---|---|---|
| | | }<br>[edit] |
| R2 | Установка адреса интерфейса заглушки в качестве идентификатора маршрутизатора в OSPF. | admin@R2# **set protocols ospf parameters router-id 10.0.0.2**<br>[edit] |
| R2 | Объявление в сети 10.0.40.0/24. | admin@R2# **set protocols ospf area 0.0.0.0 network 10.0.40.0/24**<br>[edit] |
| R2 | Объявление для сети 10.0.50.0/24. | admin@R2# **set protocols ospf area 0.0.0.0 network 10.0.50.0/24**<br>[edit] |
| R2 | Перераспределение непосредственно подключенных маршрутов на OSPF | admin@R2# **set protocols ospf redistribute connected**<br>[edit] |
| R2 | Фиксация настройки. | admin@R2# **commit**<br>[edit] |
| R2 | Отображение настройки. | admin@R2# **show protocols**<br>ospf {<br>area 0.0.0.0 {<br>network 10.0.40.0/24<br>network 10.0.50.0/24<br>}<br>parameters { |

```
                router-id 10.0.0.2
            }
            redistribute {
                connected {
                }
            }
        }
        [edit]
```

| | | |
|---|---|---|
| R3 | Установка адреса интерфейса заглушки в качестве идентификатора маршрутизатора в OSPF. | admin@R3# **set protocols ospf parameters router-id 10.0.0.3**<br>[edit] |
| R3 | Объявление для сети 10.0.50.0/24. | admin@R3# **set protocols ospf area 0.0.0.0 network 10.0.50.0/24**<br>[edit] |
| R3 | Перераспределение непосредственно подключенных маршрутов на OSPF | admin@R3# **set protocols ospf redistribute connected**<br>[edit] |
| R3 | Фиксация настройки. | admin@R3# **commit**<br>[edit] |
| R3 | Отображение настройки. | admin@R3# **show protocols**<br>ospf {<br>area 0.0.0.0 {<br>network 10.0.50.0/24<br>}<br>parameters {<br>router-id 10.0.0.3 |

```
        }
        redistribute {
            connected {
            }
        }
    }
    [edit]
```

## 10.3.2. Проверка настройки OSPF

Для проверки настройки OSPF можно использовать следующие команды эксплуатационного режима.

### *10.3.2.1. R3: show ip route*

В примере 10.2 приведен вывод для команды **show ip route** для маршрутизатора R3.

*Пример 10.2 - Проверка OSPF на R3: "show ip route"*

```
admin@R3:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O -
OSPF, I - ISIS, B - BGP, > - selected route, * - FIB route

O>* 10.0.0.1/32 [110/20] via 10.0.50.2, eth5, 00:04:21
O>* 10.0.0.2/32 [110/20] via 10.0.50.2, eth5, 00:03:31
C>* 10.0.0.3/32 is directly connected, lo
O>* 10.0.20.0/24 [110/20] via 10.0.50.2, eth5, 03:06:06
O>* 10.0.30.0/24 [110/20] via 10.0.50.2, eth5, 03:07:39
O>* 10.0.40.0/24 [110/20] via 10.0.50.2, eth5, 03:07:40
O    10.0.50.0/24 [110/10] is directly connected, eth5, 03:07:45
C>* 10.0.50.0/24 is directly connected, eth5
C>* 10.0.60.0/24 is directly connected, eth6
C>* 127.0.0.0/8 is directly connected, lo
```

Из вывода видно, что маршруты к 10.0.0.1/32, 10.0.0.2/32, 10.0.20.0/24, 10.0.30.0/24 и 10.0.40.0/24 получены по OSPF (и являются выбранными маршрутами). Кроме того, пакеты к

этим сетям будут пересылаться наружу через eth5 на 10.0.50.2. 10.0.0.3/32, 10.0.50.0/24 и 10.0.60.0/24 подключены напрямую к R3. Непосредственно подключенные маршруты выбираются раньше любых обнаруженных с помощью OSPF (т.е. 10.0.50.0/24).

#### *10.3.2.2. R3: ping 10.0.20.1*

При помощи команды **ping** с маршрутизатора R3 можно убедиться, что узлы в удаленных сетях достижимы. В примере 10.3 проверяется достижимость IP-адреса R1.

*Пример 10.3 - Проверка OSPF на R3: "ping 10.0.20.1"*

```
admin@R3:~$ ping 10.0.20.1
PING 10.0.20.1 (10.0.20.1) 56(84) bytes of data.
64 bytes from 10.0.20.1: icmp_seq=1 ttl=63 time=5.75 ms
64 bytes from 10.0.20.1: icmp_seq=2 ttl=63 time=1.74 ms
64 bytes from 10.0.20.1: icmp_seq=3 ttl=63 time=1.40 ms
^C
-- 10.0.20.1 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.

## 10.4. Команды настройки OSPF на уровне маршрутизатора

В данном разделе описаны команды для настройки протокола OSPF на уровне маршрутизатора. Рассматриваются следующие команды:

| 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` | 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 <значение>` | 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 | |
| `debug ospf event` | Включение или отключение вывода отладочных сообщений, относящихся к событиям OSPF. |
| `debug ospf ism` | Включение или отключение вывода отладочных сообщений, относящихся к ISM в OSPF. |
| `debug ospf lsa` | Включение или отключение вывода отладочных сообщений, относящихся к объявлениям состояния канала (LSA) в OSPF. |
| `debug ospf nsm` | Включение или отключение вывода отладочных сообщений, относящихся к NSM в OSPF. |

| | |
|---|---|
| `debug ospf nssa` | Включение и отключение вывода отладочных сообщений, относящихся к малотупиковым областям (not-so-stubby areas, NSSA) в OSPF. |
| `debug ospf packet all` | Включение или отключение вывода отладочных сообщений, относящихся ко всем типам пакетов OSPF. |
| `debug ospf packet dd` | Включение или отключение вывода отладочных сообщений, относящихся к пакетам описания базы данных (DD) протокола OSPF. |
| `debug ospf packet hello` | Включение или отключение вывода отладочных сообщений, относящихся к пакетам приветствия протокола OSPF. |
| `debug ospf packet ls-ack` | Включение или отключение вывода отладочных сообщений, относящихся к пакетам уведомления о состоянии канала (LS Ack) протокола OSPF. |
| `debug ospf packet ls-request` | Включение или отключение вывода отладочных сообщений, относящихся к пакетам запроса состояния канала (LSR) протокола OSPF. |
| `debug ospf packet ls-update` | Включение или отключение вывода отладочных сообщений для пакетов обновления информации о состоянии канала (LSU) протокола OSPF. |
| `debug ospf zebra` | Включение или отключение вывода отладочных сообщений для процесса Zebra, работающего с протоколом OSPF. |

| | |
|---|---|
| `show debugging ospf` | 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. |

### 10.4.1. debug ospf event

Включение или отключение вывода отладочных сообщений, относящихся к событиям OSPF.

**Синтаксис**

**`debug ospf event`**

**`no debug ospf event`**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для включения вывода сообщений уровня трассировки, относящихся к событиям OSPF.

Форма **no** этой команды используется для отключения вывода отладочных сообщений для событий OSPF.

## 10.4.2. debug ospf ism

Включение или отключение вывода отладочных сообщений, относящихся к ISM в OSPF.

**Синтаксис**

**debug ospf ism** [**events** | **status** | **timers**]

**no debug ospf 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 трассировки, относящихся к событиям ISM в OSPF.

Форма **no** этой команды используется для отключения вывода отладочных сообщений ISM в OSPF.

## 10.4.3. debug ospf lsa

Включение или отключение вывода отладочных сообщений, относящихся к объявлениям состояния канала (LSA) в OSPF.

**Синтаксис**

**debug ospf lsa** [**flooding** | **generate** | **install** | **refresh**]

**no debug ospf 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 трассировки, относящихся к объявлениям состояния каналов в OSPF.

Форма **no** этой команды используется для отключения вывода отладочных сообщений, относящихся к объявлениям состояния каналов в OSPF.

## 10.4.4. debug ospf nsm

Включение или отключение вывода отладочных сообщений, относящихся к NSM в OSPF.

**Синтаксис**

**debug ospf nsm** [**events** | **status** | **timers**]

**no debug ospf 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 трассировки, относящихся к событиям NSM в OSPF.

Форма **no** этой команды используется для отключения вывода отладочных сообщений NSM в OSPF.

## 10.4.5. debug ospf nssa

Включение и отключение вывода отладочных сообщений, относящихся к малотупиковым областям (not-so-stubby areas, NSSA) в OSPF.

**Синтаксис**

**debug ospf nssa**

**no debug ospf nssa**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для включения вывода сообщений уровня трассировки, относящихся к малотупиковым областям (NSSA) в OSPF.

Форма **no** этой команды используется для отключения вывода отладочных сообщений, относящихся к малотупиковым областям (NSSA) в OSPF.

## 10.4.6. debug ospf packet all

Включение или отключение вывода отладочных сообщений, относящихся ко всем типам пакетов OSPF.

**Синтаксис**

**debug ospf packet all** [**detail** | **recv** [**detail**] | **send** [**detail**]]

**no debug ospf packet all** [**detail** | **recv** [**detail**] | **send** [**detail**]]

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**detail**

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.

**detail**

Необязательный. Вывод подробных отладочных сообщений для полученных пакетов OSPF всех типов.

**send**

Необязательный. Вывод отладочных сообщений для всех переданных пакетов OSPF.

**detail**

Необязательный. Вывод подробных отладочных сообщений для всех переданных пакетов OSPF.

**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 трассировки, относящихся ко всем типам пакетов OSPF, приходящих на маршрутизатор и уходящих с него.

Форма **no** этой команды используется для отключения вывода отладочных сообщений, относящихся ко всем типам пакетов OSPF.

## 10.4.7. debug ospf packet dd

Включение или отключение вывода отладочных сообщений, относящихся к пакетам описания базы данных (DD) протокола OSPF.

**Синтаксис**

**debug ospf packet dd** [**detail** | **recv** [**detail**] | **send** [**detail**]]

**no debug ospf packet dd** [**detail** | **recv** [**detail**] | **send** [**detail**]]

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**detail**

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.

**detail**

Необязательный. Вывод подробных 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 для переданных пакетов DD протокола OSPF.

**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 трассировки, 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 **no** этой команды используется для отключения вывода отладочных сообщений, относящихся к пакетам DD протокола OSPF.

## 10.4.8. debug ospf packet hello

Включение или отключение вывода отладочных сообщений, относящихся к пакетам приветствия протокола OSPF.

**Синтаксис**

**debug ospf packet hello** [**detail** | **recv** [**detail**] | **send** [**detail**]]

**no debug ospf packet hello** [**detail** | **recv** [**detail**] | **send** [**detail**]]

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**detail**

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.

**detail**

Необязательный. Вывод подробных 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 для переданных пакетов приветствия протокола OSPF.

**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 трассировки, 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 **no** этой команды используется для отключения вывода отладочных сообщений, относящихся к пакетам приветствия протокола OSPF.

## 10.4.9. debug ospf packet ls-ack

Включение или отключение вывода отладочных сообщений, относящихся к пакетам уведомления о состоянии канала (LS Ack) протокола OSPF.

**Синтаксис**

```
debug ospf packet ls-ack [detail | recv [detail] | send
[detail]]
```

```
no debug ospf packet ls-ack [detail | recv [detail] |
send [detail]]
```

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**detail**

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.

**detail**

Необязательный. Вывод подробных 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 для переданных пакетов LS Ack протокола OSPF.

**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 трассировки, 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 **no** этой команды используется для отключения вывода отладочных сообщений, относящихся к пакетам LS Ack протокола OSPF.

## 10.4.10. debug ospf packet ls-request

Включение или отключение вывода отладочных сообщений, относящихся к пакетам запроса состояния канала (LSR) протокола OSPF.

**Синтаксис**

**debug ospf packet ls-request** [**detail** | **recv** [**detail**] | **send** [**detail**]]

**no debug ospf packet ls-request** [**detail** | **recv** [**detail**] | **send** [**detail**]]

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**detail**

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.

**detail**

Необязательный. Вывод подробных 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 для переданных пакетов LSR протокола OSPF.

**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 трассировки, 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 **no** этой команды используется для отключения вывода отладочных сообщений, относящихся к пакетам LSR протокола OSPF.

## 10.4.11. debug ospf packet ls-update

Включение или отключение вывода отладочных сообщений для пакетов обновления информации о состоянии канала (LSU) протокола OSPF.

**Синтаксис**

```
debug ospf packet ls-update [detail | recv [detail] |
send [detail]]

no debug ospf packet ls-update [detail | recv [detail] |
send [detail]]
```

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**detail**

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.

**detail**

Необязательный. Вывод подробных 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 для переданных

пакетов LSU протокола OSPF.

**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 трассировки, относящихся к пакетам обновления информации о состоянии канала (LSR) протокола OSPF. В пакетах LSU соседу по OSPF передаются любые запрошенные обновления для LSA.

Форма **no** этой команды используется для отключения вывода отладочных сообщений, относящихся к пакетам LSU протокола OSPF.

## 10.4.12. debug ospf zebra

Включение или отключение вывода отладочных сообщений для процесса Zebra, работающего с протоколом OSPF.

**Синтаксис**

**debug ospf zebra** [**interface** | **redistribute**]

**no debug ospf 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

трассировки, относящихся к процессу Zebra, работающему с протоколом OSPF.

Форма **no** этой команды используется для отключения вывода отладочных сообщений, относящихся к процессу Zebra, работающему с протоколом OSPF.

## 10.4.13. 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 на 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.

## 10.4.14. 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 целоебеззнака32разр {
                export текст
            }
        }
}
```

**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.

## 10.4.15. 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 1-4294967
               }
          }
}
```

**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.

## 10.4.16. 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 0-16777214
                         metric-type 1-2
                         route-map текст
                    }
               }
          }
}
```

**Параметры**

**always**

Необязательный. Маршрут по умолчанию объявляется всегда.

**metric** *метрика*

Необязательный. Метрика, применяемая к маршруту по умолчанию. Значение должно лежать в диапазоне от 0 до 16777214. Значение по умолчанию равно 1.

**metric-type** *тип*

Необязательный. Тип метрики внешнего маршрута, связываемый с объявлением состояния канала (LSA) по умолчанию типа 5. Поддерживаются следующие значения:

1: Внешний маршрут типа 1.

2: Внешний маршрут типа 2.

Значение по умолчанию равно 2.

**route-map** *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.

## 10.4.17. 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 0-16777214
          }
}
```

**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.

## 10.4.18. protocols ospf distance

Установка административного расстояния OSPF по типу маршрута.

**Синтаксис**

**set protocols ospf distance** {**global** *расст_для_всех* | **ospf** [**external** *расст_для_внешних* | **inter-area** *расст_для_межобл* | **intra-area** *расст_для_внутриобл*]}

**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 1-255
                ospf {
```

```
                                external 1-255
                                inter-area 1-255
                                intra-area 1-255
                            }
                        }
                    }
                }
```

**Параметры**

*расст_для_всех*

Административное расстояние, устанавливаемое для всех маршрутов. Значение должно лежать в диапазоне от 1 до 255.

*расст_для_внешних*

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.

*расст_для_межобл*

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.

расст_для_внутриобл

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 120.

**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.

## 10.4.19. 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.

## 10.4.20. 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_объявления_при_закрытии* | **on-startup** *время_объявления_при_запуске*]

**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 5-86400
                            on-startup 5-86400
                        }
                    }
                }
            }
```

**Параметры**

**administrative**

Необязательный. Объявление максимальной метрики в течение неопределенного периода.

**on-shutdown** *время_объявления_при_закрытии*

Объявление максимальной метрики при закрытии процесса OSPF. Аргумент *время_объявления_при_закрытии* 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_объявления_при_запуске*

Объявление максимальной метрики при запуске или перезагрузке процесса OSPF. Аргумент *время_объявления_при_запуске* 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.

## 10.4.21. 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.

## 10.4.22. 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 1-65535
                priority 0-255
            }
        }
}
```

**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.

## 10.4.23. 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 [cisco|ibm|shortcut|
standard]
                    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 в соответствии с описанием в документе draft-ietf-ospf-shortcut-abr-02.txt;

**standard**: выделение маршрутизатора как стандартного ABR.

Значение по умолчанию равно **standard**.

**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:

1. Используется IP-адрес интерфейса заглушки.
2. Используется наибольший из IP-адресов интерфейсов маршрутизатора.
3. 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.

## 10.4.24. 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 eth0..eth23 {}
          }
}
```

**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.

## 10.4.25. 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 1-16
                         metric-type 1-2
                         route-map текст
                    }
               }
          }
}
```

**Параметры**

**metric** *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.

**metric-type** *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.

**route-map** *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.

## 10.4.26. 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 1-16
                        metric-type 1-2
                        route-map текст
                    }
                }
            }
        }
```

**Параметры**

**metric** *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.

**metric-type** *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.

**route-map** *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.

## 10.4.27. 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 1-16
                         metric-type 1-2
                         route-map текст
                    }
               }
          }
}
```

**Параметры**

**metric** *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.

**metric-type** *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.

**route-map** *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.

## 10.4.28. 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 1-16
                    metric-type 1-2
                    route-map текст
                }
            }
        }
}
```

**Параметры**

**metric** *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.

**metric-type** *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.

**route-map** *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.

## 10.4.29. 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 1-16
                         metric-type 1-2
                         route-map текст
                    }
               }
          }
}
```

**Параметры**

**metric** *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.

**metric-type** *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.

**route-map** *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.

## 10.4.30. protocols ospf refresh timers <значение>

Установка значений для таймеров обновления OSPF.

**Синтаксис**

**set protocols ospf refresh timers** *значение*

**delete protocols ospf refresh timers**

**show protocols ospf refresh timers**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
          ospf {
               refresh {
                    timers 10-1800
               }
          }
}
```

**Параметры**

*значение*

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.

## 10.4.31. protocols ospf timers throttle spf

Включение или отключение задержки вычислений SPF в OSPF.

**Синтаксис**

**set protocols ospf timers throttle spf** [**delay** *задержка* | **initial-holdtime** *начальный_интервал* | **max-holdtime** *максимальный_интервал*]

**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 0-600000

     initial-holdtime 0-600000

     max-holdtime 0-600000
                         }
                    }
               }
          }
}
```

**Параметры**

**delay** *задержка*

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** *начальный_интервал*

Необязательный. Начальный интервал (в мс) между последовательными расчетами SPF. Значение должно лежать в диапазоне от 0 до 600000.

**max-holdtime** *максимальный_интервал*

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.

## 10.4.32. show debugging ospf

Отображение флагов отладки протокола OSPF.

**Синтаксис**

```
show debugging ospf
```

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствует.

**Значение по умолчанию**

Отсутствуют

**Указания по использованию**

Эта команда используется для вывода режима отладки OSPF.

## 10.4.33. 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.

**Примеры**

В примере 10.4 приведен образец вывода сведений OSPF.

*Пример 10.4 - "show ip ospf": отображение сведений о настройке OSPF*

```
admin@neo:~$ show ip ospf
OSPF Routing Process, Router ID: 10.100.10.1
Supports only single TOS (TOS0) routes
This implementation conforms to RFC2328
RFC1583Compatibility flag is disabled
OpaqueCapability flag is disabled
Initial SPF scheduling delay 200 millisec(s)
Minimum hold time between consecutive SPFs 1000
millisec(s)
Maximum hold time between consecutive SPFs 10000
```

```
millisec(s)
Hold time multiplier is currently 1
SPF algorithm last executed 1w2d01h ago
SPF timer is inactive
Refresh timer 10 secs
Number of external LSA 1. Checksum Sum 0x000083e4
Number of opaque AS LSA 0. Checksum Sum 0x00000000
Number of areas attached to this router: 1
Area ID: 10.1.0.0
Shortcutting mode: Default, S-bit consensus: no
Number of interfaces in this area: Total: 1, Active: 1
Number of fully adjacent neighbors in this area: 2
Area has no authentication
Number of full virtual adjacencies going through this
area: 0
SPF algorithm executed 3 times
Number of LSA 4
Number of router LSA 3. Checksum Sum 0x0000ccad
Number of network LSA 1. Checksum Sum 0x00000df2
Number of summary LSA 0. Checksum Sum 0x00000000
Number of ASBR summary LSA 0. Checksum Sum 0x00000000
Number of NSSA LSA 0. Checksum Sum 0x00000000
Number of opaque link LSA 0. Checksum Sum 0x00000000
Number of opaque area LSA 0. Checksum Sum 0x00000000
admin@neo:~$
```

### 10.4.34. 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.

**Примеры**

В примере 10.5 приведен образец вывода сведений о граничных маршрутизаторах OSPF.

*Пример 10.5 - "show ip ospf border-router": отображение сведений о граничных маршрутизаторах OSPF*

```
admin@neo:~$ show ip ospf border-routers
============ OSPF router routing table =============
R    10.1.0.58 [10] area: 10.1.0.0, ASBR
via 10.1.0.58, eth2
```

## 10.4.35. show ip ospf database

Отображение сведений о базе данных OSPF.

**Синтаксис**

**show ip ospf database** [**max-age** | **self-originate** | {**asbr-summary** | **external** | **network** | **nssa-external** | **opaque-area** | **opaque-as** | **opaque-link** | **router** | **summary**} [**adv-router** *ipv4-адрес* | *ipv4-адрес* [**adv-router** *ipv4-адрес* | **self-originate**]]]

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**max-age**

Отображение базы данных максимального возраста OSPF.

**self-originate**

Отображение базы данных маршрутов OSPF, созданных локальным маршрутизатором.

**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.

**adv-router** *ipv4-адрес*

Необязательный. Отображение базы данных OSPF для данного адреса указанного объявляемого маршрутизатора.

*ipv4-адрес*

Необязательный. Отображение базы данных OSPF для данного адреса.

**self-originate**

Необязательный. Отображение базы данных маршрутов OSPF для данного адреса, созданных локальным маршрутизатором.

**Значение по умолчанию**

Отсутствует.

#### Указания по использованию

Эта команда используется для отображения сведений базы данных OSPF.

#### Примеры

В примере 10.6 приведен образец вывода общих сведений базы данных OSPF.

*Пример 10.6 - "show ip ospf database": отображение общих сведений базы данных OSPF*

```
admin@neo:~$ show ip ospf database

OSPF Router with ID (10.100.10.1)

Router Link States (Area 10.1.0.0)

Link ID   ADV Router     Age
     Seq# CkSum     Link count

10.1.0.33 10.1.0.33 123  0x800003e5
     0x791f    1

10.1.0.58 10.1.0.58 123  0x80000562
     0x4e7e    1

10.100.10.1    10.100.10.1
     117  0x800001b6     0xfe13
     1

Net Link States (Area 10.1.0.0)

Link ID   ADV Router     Age
     Seq# CkSum

10.1.0.58 10.1.0.58 123 0x800003df 0x0bf3

AS External Link States

Link ID   ADV Router     Age
     Seq# CkSum     Route

76.0.0.0  10.1.0.58 1850 0x800000b3 0x83e4 E2

76.0.0.0/8 [0x0]
```

## 10.4.36. 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.

**Примеры**

В примере 10.7 приведен образец вывода сведений OSPF по всем интерфейсам.

*Пример 10.7 - "show ip ospf interface": отображение сведений о настройке и состоянии OSPF*

```
admin@neo:~$ show ip ospf interface

eth0 is down

ifindex 3, MTU 1500 bytes, BW 0 Kbit
<UP,BROADCAST,MULTICAST> OSPF not enabled on this
interface

eth1 is down

ifindex 4, MTU 1500 bytes, BW 0 Kbit
<UP,BROADCAST,MULTICAST> OSPF not enabled on this
interface

eth1_rename is down

ifindex 0, MTU 1500 bytes, BW 0 Kbit
<BROADCAST,MULTICAST> OSPF not enabled on this interface

eth2 is up

ifindex 5, MTU 1500 bytes, BW 0 Kbit

<UP,BROADCAST,RUNNING,MULTICAST>

Internet Address 10.1.0.62/24, Broadcast 10.1.0.255,
Area

10.1.0.0

MTU mismatch detection:enabled

Router ID 10.100.10.1, Network Type BROADCAST, Cost: 10

Transmit Delay is 1 sec, State DROther, Priority 1
```

```
Designated Router (ID) 10.1.0.58, Interface Address
10.1.0.58

Backup Designated Router (ID) 10.1.0.33, Interface
Address

10.1.0.33

Multicast group memberships: OSPFAllRouters

Timer intervals configured, Hello 10s, Dead 40s, Wait
40s, Retransmit 5

Hello due in 0.721s

Neighbor Count is 2, Adjacent neighbor count is 2
eth2_rename is down

ifindex 0, MTU 1500 bytes, BW 0 Kbit
<BROADCAST,MULTICAST>

OSPF not enabled on this interface eth3 is down

ifindex 2, MTU 1500 bytes, BW 0 Kbit
<BROADCAST,MULTICAST>

OSPF not enabled on this interface lo is up

ifindex 1, MTU 16436 bytes, BW 0 Kbit
<UP,LOOPBACK,RUNNING>

OSPF not enabled on this interface
```

## 10.4.37. 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.

**Примеры**

В примере 10.8 приведен образец вывода сведений о соседях по OSPF для всех соседей.

*Пример 10.8 - "show ip ospf neighbor": отображение сведений о соседях по OSPF*

```
admin@neo:~$ show ip ospf neighbor
Neighbor ID Pri State    Dead Time Address
Interface RXmtL RqstL DBsmL
10.1.0.33 1 Full/Backup       33.842s 10.1.0.33 eth2:10.1.0.62
     0    0    0
10.1.0.58 1 Full/DR           38.581s 10.1.0.58 eth2:10.1.0.62
     0    0    0
```

## 10.4.38. 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.

**Примеры**

В примере 10.9 приведен образец вывода сведений о маршрутах OSPF.

*Пример 10.9 - "show ip ospf route": отображение сведений о маршрутах OSPF*

```
admin@neo:~$ show ip ospf route

============ OSPF network routing table ============ N
     10.1.0.0/24    [10] area: 10.1.0.0

directly attached to eth2

============ OSPF router routing table ============= R
     10.1.0.58 [10] area: 10.1.0.0, ASBR

via 10.1.0.58, eth2

============ OSPF external routing table =========== N
E2 76.0.0.0/8  [10/20] tag: 0

via 10.1.0.7, eth2
```

## 10.4.39. 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.

**Примеры**

В примере 10.10 приведен вывод всех маршрутов OSPF на IP.

*Пример 10.10 - "show ip route ospf": отображение маршрутов*

```
admin@neo:~$ show ip route ospf

Codes: K - kernel route, C - connected, S - static, R -
RIP, O - OSPF,

I - ISIS, B - BGP, > - selected route, * - FIB route

O    10.1.0.0/24 [110/10] is directly connected, eth2,
01w2d21h O>* 76.0.0.0/8 [110/20] via 10.1.0.7, eth2,
4d12h48m
```

## 10.5. Команды для областей OSPF

В данном разделе описаны команды для настройки областей OSPF.

Рассматриваются следующие команды:

| Команды настройки | |
|---|---|
| `protocols ospf area <идентификатор_области>` | Определение области OSPF. |
| `protocols ospf area <идентификатор_области> area-type normal` | Выделение области OSPF в качестве нормальной области. |
| `protocols ospf area <идентификатор_области> area-type nssa` | Выделение области OSPF в качестве малотупиковой области (NSSA). |
| `protocols ospf area <идентификатор области> area-type stub` | Выделение области OSPF в качестве тупиковой области. |
| `protocols ospf area <идентификатор_области> authentication` | Указание типа аутентификации для области OSPF. |
| `protocols ospf area <идентификатор_области> network <подсеть_ipv4>` | Указание адреса подсети для области OSPF. |

| | |
|---|---|
| `protocols ospf area <идентификатор_области> range <подсеть_ipv4>` | Создание граничным маршрутизатором области (ABR) сводки маршрутов, соответствующих диапазону префиксов. |
| `protocols ospf area <идентификатор_области> shortcut <режим>` | Установка режима срезки OSPF на граничном маршрутизаторе области (ABR). |
| `protocols ospf area <идентификатор_области> virtual-link <ipv4-адрес> authentication` | Указание характеристик аутентификации для виртуального канала. |
| `protocols ospf area <идентификатор_области> virtual-link <ipv4-адрес> dead-interval <интервал>` | Указание мертвого интервала для виртуального канала. |
| `protocols ospf area <идентификатор_области> virtual-link <ipv4-адрес> hello-interval <интервал>` | Установка интервала между пакетами приветствия OSPF на виртуальном канале. |
| `protocols ospf area <идентификатор_области> virtual-link <ipv4-адрес> retransmit-interval <интервал>` | Указание интервала повторной передачи для виртуального канала. |
| `protocols ospf area <идентификатор_области> virtual-link <ipv4-адрес> transmit-delay <задержка>` | Указание задержки передачи для виртуального канала. |

Эксплуатационные команды

Отсутствуют.

### 10.5.1. protocols ospf area <идентификатор_области>

Определение области OSPF.

**Синтаксис**

**set protocols ospf area** *идентификатор_области*

**delete protocols ospf area** *идентификатор_области*

**show protocols ospf area** *идентификатор_области*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
        ospf {
            area текст
        }
}
```

**Параметры**

*идентификатор_области*

Обязательный. Идентификатор области OSPF. В качестве идентификатора может быть указан IP-адрес или десятичное число.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для определения области внутри автономной системы (AS) OSPF.

Форма **set** этой команды используется для создания области OSPF или определения ее характеристик.

Форма **delete** этой команды используется для удаления области OSPF.

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

### 10.5.2. protocols ospf area <идентификатор_области> area-type normal

Выделение области OSPF в качестве нормальной области.

**Синтаксис**

**set protocols ospf area** *идентификатор_области* **area-type normal**

**delete protocols ospf area** *идентификатор_области* **area-type**

**show protocols ospf area** *идентификатор_области* **area-type**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
          ospf {
               area текст {
                    area-type {
                         normal
                    }
               }
          }
}
```

**Параметры**

*идентификатор_области*

Обязательный. Идентификатор настраиваемой области OSPF. В качестве идентификатора может быть указан IP-адрес или десятичное число.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для выделения области OSPF как нормальной области.

Нормальная область - это область, не являющаяся ни тупиковой, ни малотупиковой. В нормальных областях объявляются все внешние маршруты.

Форма **set** этой команды используется для установки нормального типа для области OSPF.

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

области.

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

### 10.5.3. protocols ospf area <идентификатор_области> area-type nssa

Выделение области OSPF в качестве малотупиковой области (NSSA).

**Синтаксис**

**set protocols ospf area** *идентификатор_области* **area-type nssa** [**default-cost** *стоимость* | **no-summary** | **translate** {**always** | **candidate** | **never**}]

**delete protocols ospf area** *идентификатор_области* **area-type nssa** [**default-cost** | **no-summary** | **translate**]

**show protocols ospf area** *идентификатор_области* **area-type nssa** [**default-cost** | **translate**]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
          ospf {
               area текст {
                    area-type {
                         nssa {

    default-cost: 0-16777215

    no-summary

    translate {

         always

         candidate

         never
```

```
        }
                                }
                            }
                        }
                    }
            }
```

**Параметры**

*идентификатор_области*

Обязательный. Идентификатор настраиваемой области OSPF. В качестве идентификатора может быть указан IP-адрес или десятичное число.

*стоимость*

Необязательный. Административная стоимость, или метрика, применяемая к маршруту по умолчанию в этой области. Значение должно лежать в диапазоне от 0 до 6777215.

**no-summary**

Необязательный. Предотвращение создание сводок маршрутов внутри области.

**translate**

Необязательный. Директива граничному маршрутизатору области NSSA, в каких ситуациях переводить LSA типа 7 во внешние для AS LSA типа 5.

**always**

Перевод LSA типа 7 во внешние для AS LSA типа 5 выполняется всегда.

**candidate**

Преобразуются только LSA типа 7 от возможного граничного маршрутизатора NSSA.

**never**

Перевод LSA типа 7 во внешние для AS LSA типа 5 не выполняется.

**Значение по умолчанию**

По умолчанию в области создаются маршруты-сводки и преобразуются только LSA типа 7 от возможного граничного маршрутизатора NSSA.

**Указания по использованию**

Эта команда используется для выделения области OSPF в качестве малотупиковой области.

Внешние для AS LSA типа 5 в тупиковых областях не разрешены, но LSA типа 7 могут быть переведены в LSA типа 5 граничным маршрутизатором области NSSA и таким образом могут проходить через NSSA. Маршруты между областями не разрешены.

Форма **set** этой команды используется для установки малотупикового типа области OSPF.

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

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

### 10.5.4. protocols ospf area <идентификатор области> area-type stub

Выделение области OSPF в качестве тупиковой области.

**Синтаксис**

**set protocols ospf area** *идентификатор_области* **area-type stub** [**default-cost** *стоимость* | **no-summary**]

**delete protocols ospf area** *идентификатор_области* **area-type stub** [**default-cost** | **no-summary**]

**show protocols ospf area** *идентификатор_области* **area-type stub** [**default-cost**]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
          ospf {
               area текст {
                    area-type {
                         stub {

    default-cost 0-16777215
```

```
        no-summary
                                }
                            }
                        }
                    }
            }
```

**Параметры**

*идентификатор_области*

Обязательный. Идентификатор настраиваемой области OSPF. В качестве идентификатора может быть указан IP-адрес или десятичное число.

*стоимость*

Необязательный. Административная стоимость, или метрика, применяемая к маршруту по умолчанию в этой области. Значение должно лежать в диапазоне от 0 до 6777215.

**no-summary**

Необязательный. Предотвращение создание сводок маршрутов внутри области.

**Значение по умолчанию**

По умолчании в области создаются маршруты-сводки.

**Указания по использованию**

Эта команда используется для выделения данной области OSPF в качестве тупиковой. В тупиковой области внешние для AS LSA типа 5 не разрешены.

Форма **set** этой команды используется для установки тупикового типа области OSPF.

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

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

## 10.5.5. protocols ospf area <идентификатор_области> authentication

Указание типа аутентификации для области OSPF.

**Синтаксис**

**set protocols ospf area** *идентификатор_области* **authentication** *тип*

**delete protocols ospf area** *идентификатор_области* **authentication**

**show protocols ospf area** *идентификатор_области* **authentication**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
          ospf {
               area текст {
                    authentication текст
               }
          }
}
```

**Параметры**

*идентификатор_области*

Обязательный. Идентификатор настраиваемой области OSPF. В качестве идентификатора может быть указан IP-адрес или десятичное число.

*тип*

Тип используемой аутентификации. Поддерживаются следующие значения:

**md5**: Через сеть пересылается значение хэш-кода, вычисленное из пароля в пакете OSPF и пароля при помощи алгоритма md5.

**plaintext-password**: Пароли пересылаются по сети открытым текстом.

**Значение по умолчанию**

По умолчанию используется простая аутентификация (открытым текстом).

**Указания по использованию**

Эта команда используется для установки типа аутентификации в области OSPF.

При простой аутентификации пароли пересылаются через сеть открытым текстом. При аутентификации MD5 в системе используется алгоритм

Message Digest 5 (MD5) для вычисления значения хэш-кода из содержимого пакета и пароля OSPF. Вычисленное значение хэш-кода и ключ MD5 включаются в состав передаваемого пакета, и принимающая система (настроенная с тем же самым паролем) вычисляет свой хэш-код, который должен соответствовать передаваемому.

Форма **set** этой команды используется для установки типа аутентификации.

Форма **delete** этой команды используется для удаления типа аутентификации.

Форма **show** этой команды используется для отображения типа аутентификации.

### 10.5.6. protocols ospf area <идентификатор_области> network <подсеть_ipv4>

Указание адреса подсети для области OSPF.

**Синтаксис**

**set protocols ospf area** *идентификатор_области* **network** *подсеть_ipv4*

**delete protocols ospf area** *идентификатор_области* **network** *подсеть_ipv4*

**show protocols ospf area** *идентификатор_области* **network**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
        ospf {
            area текст {
                network подсеть_ipv4
            }
        }
}
```

**Параметры**

*идентификатор_области*

Обязательный. Идентификатор настраиваемой области OSPF. В качестве идентификатора может быть указан IP-адрес или десятичное число.

*подсеть_ipv4*

Обязательный. Множественный узел. Подсеть, используемая в качестве области OSPF. Используется формат *IP-адрес/префикс*.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда предназначена для указания подсети, используемой в качестве области OSPF.

Форма **set** этой команды используется для указания подсети области.

Форма **delete** этой команды используется для удаления настройки подсети области OSPF.

Форма **show** этой команды используется для отображения настройки подсети области OSPF.

## 10.5.7. protocols ospf area <идентификатор_области> range <подсеть_ipv4>

Создание граничным маршрутизатором области (ABR) сводки маршрутов, соответствующих диапазону префиксов.

**Синтаксис**

**set protocols ospf area** *идентификатор_области* **range** *подсеть_ipv4* [**cost** *стоимость* | **not-advertise** | **substitute** *подсеть_ipv4*]

**delete protocols ospf area** *идентификатор_области* **range** [*подсеть_ipv4* [**cost** | **not-advertise** | **substitute**]]

**show protocols ospf area** *идентификатор_области* **range** [*подсеть_ipv4* [**cost** | **substitute**]]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
        ospf {
            area текст {
```

```
                    area-type {
                        range {
    cost 0-16777215
    not-advertise
    substitute подсеть_ipv4
                        }
                    }
                }
            }
}
```

**Параметры**

*идентификатор_области*

Обязательный. Идентификатор настраиваемой области OSPF. В качестве идентификатора может быть указан IP-адрес или десятичное число.

*подсеть_ipv4*

Обязательный. Диапазон для получения сводки, выраженный в виде подсети IPv4 в формате *ip-адрес/префикс.*

*стоимость*

Необязательный. Административная стоимость, или метрика, применяемая к маршрутам в данном диапазоне. Значение должно лежать в диапазоне от 0 до 16777215.

**not-advertise**

Необязательный. Директива маршрутизатору не объявлять маршруты в данном диапазоне.

**substitute** *подсеть_ipv4*

Необязательный. Директива маршрутизатору объявлять маршруты в данном диапазоне, как будто у них префикс совпадает с указанным. Используется формат *ip-адрес/префикс*.

**Значение по умолчанию**

По умолчанию маршруты объявляются, а подстановка для маршрутов не выполняется.

**Указания по использованию**

Эта команда используется для выдачи маршрутизатору директивы получать сводку маршрутов, соответствующих диапазону префиксов. Команда может использоваться только на граничном маршрутизаторе области (ABR).

Форма **set** этой команды используется для установки диапазона областей.

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

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

## 10.5.8. protocols ospf area <идентификатор_области> shortcut <режим>

Установка режима срезки OSPF на граничном маршрутизаторе области (ABR).

**Синтаксис**

**set protocols ospf area** *идентификатор_области* **shortcut** *режим*

**delete protocols ospf area** *идентификатор_области* **shortcut**

**show protocols ospf area** *идентификатор_области* **shortcut**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
          ospf {
               area текст {
                    shortcut текст
               }
          }
}
```

**Параметры**

*идентификатор_области*

Обязательный. Идентификатор настраиваемой области OSPF. В качестве

идентификатора может быть указан IP-адрес или десятичное число.

*режим*

Обязательный. Режим срезки. Поддерживаются следующие значения:

**default**: Если у ABR есть активное подключение к магистрали, область не используется для срезки, и ABR не устанавливает бит срезки (бит S) в LSA маршрутизатора, направленном для области. Если у ABR нет подключения к магистрали, область всегда используется для срезки, и ABR устанавливает бит S в LSA маршрутизатора, направленном для области.

**disable**: ABR не использует данную область для срезания и не устанавливает бит S в LSA маршрутизатора, направленном для области.

**enable**: Если у ABR есть активное подключение к магистрали, то ABR устанавливает бит S в LSA маршрутизатора, и область используется для срезания при условии, что все другие ABR, видимые через данную область, также выставляют бит S. Если у ABR нет подключения к магистрали, то ABR независимо ни от чего использует данную область для срезания и устанавливает бит S в LSA маршрутизатора, направленном для области.

**Значение по умолчанию**

По умолчанию используется режим **default**.

**Указания по использованию**

Эта команда используется для установки режима срезки для граничного маршрутизатора области OSPF в соответствии со стандартом, описанным в документе draft-ietf-ospf-shortcut-abr-02.txt. Данная команда может использоваться только на ABR.

Форма **set** этой команды используется для установки режима срезки на ABR.

Форма **delete** этой команды используется для удаления настройки срезки на ABR.

Форма **show** этой команды используется для отображения настройки срезки на ABR.

### 10.5.9. protocols ospf area <идентификатор_области> virtual-link <ipv4-адрес> authentication

Указание характеристик аутентификации для виртуального канала.

**Синтаксис**

**set protocols ospf area** *идентификатор_области* **virtual-link** *ipv4-адрес* **authentication** [**md5 key-id** *ид_ключа* **md5-key** *ключ_md5* | **plaintext-password** *пароль*]

**delete protocols ospf area** *идентификатор_области* **virtual-link** *ipv4-адрес* **authentication** [**md5 key-id** *ид_ключа* **md5-key** | **plaintext-password**]

**show protocols ospf area** *идентификатор_области* **virtual-link** *ipv4-адрес* **authentication** [**md5 key-id** *ид_ключа* **md5-key** | **plaintext-password**]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
          ospf {
               area текст {
                    virtual-link ipv4-адрес {
                         authentication {
     md5 {
          key-id 1-255 {
               md5-key текст
          }
     }
     plaintext-password текст
                         }
                    }
               }
          }
}
```

**Параметры**

*идентификатор_области*

Обязательный. Идентификатор настраиваемой области OSPF. В качестве идентификатора может быть указан IP-адрес или десятичное число.

*ipv4-адрес*

Обязательный. Областной идентификатор виртуального канала, выраженный в форме IPv4-адреса.

**key-id** *ид_ключа*

Необязательный. Идентификатор ключа аутентификации. Он должен быть одинаковым на отправляющей и принимающей системах. Значение должно лежать в диапазоне от 1 до 255.

**md5-key** *ключ_md5*

Необязательный. Ключ MD5, используемый в качестве входных данных для алгоритма хэширования MD5. Он должен быть одинаковым на отправляющей и принимающей системах.

**plaintext-password** *пароль*

Необязательный. Пароль, используемый в простой аутентификации (открытыми текстом). Он должен быть не длиннее восьми символов и одинаковым на отправляющей и принимающей системах.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для установки аутентификации на виртуальном канале.

При простой аутентификации пароли пересылаются через сеть открытым текстом. При аутентификации MD5 в системе используется алгоритм Message Digest 5 (MD5) для вычисления значения хэш-кода из содержимого пакета и пароля OSPF. Вычисленное значение хэш-кода и ключ MD5 включаются в состав передаваемого пакета, и принимающая система (настроенная с тем же самым паролем) вычисляет свой хэш-код, который должен соответствовать передаваемому.

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

Форма **delete** этой команды используется для удаления настройки аутентификации на виртуальном канале.

Форма **show** этой команды используется для отображения сведений о настройке аутентификации на виртуальном канале.

## 10.5.10. protocols ospf area <идентификатор_области> virtual-link <ipv4-адрес> dead-interval <интервал>

Указание мертвого интервала для виртуального канала.

**Синтаксис**

**set protocols ospf area** *идентификатор_области* **virtual-link** *ipv4-адрес* **dead-interval** *интервал*

**delete protocols ospf area** *идентификатор_области* **virtual-link** *ipv4-адрес* **dead-interval**

**show protocols ospf area** *идентификатор_области* **virtual-link** *ipv4-адрес* **dead-interval**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
          ospf {
               area текст {
                    virtual-link ipv4-адрес {
                         dead-interval 1-65535
                    }
               }
          }
}
```

**Параметры**

*идентификатор_области*

Обязательный. Идентификатор настраиваемой области OSPF. В качестве идентификатора может быть указан IP-адрес или десятичное число.

*ipv4-адрес*

Обязательный. Областной идентификатор виртуального канала, выраженный в форме IPv4-адреса.

*интервал*

Время в секундах, которое виртуальный канал должен ожидать для обнаружения пакетов приветствия от соседних маршрутизаторов до объявления соседа неработоспособным. Значение должно лежать в диапазоне от 1 до 65535. По умолчанию выбирается четырехкратная величина интервала приветствия.

**Значение по умолчанию**

Мертвый интервал вчетверо дольше интервала приветствия.

**Указания по использованию**

Команда используется для указания интервала, в течение которого виртуальный канал ожидает получения пакетов приветствия от своего соседа.

Если в течение мертвого интервала интерфейс не получает пакета приветствия от соседа, то статус соседа изменяется на неработоспособный, а всё соответствующее состояние очищается.

Мертвый интервал должен быть одинаковым на всех маршрутизаторах, предназначенных для установления двунаправленной связи в сети. Если его величина на двух маршрутизаторах не согласована, их смежность не будет установлена, и каждый из них не будет учитывать связи, устанавливаемые на другом.

Форма **set** этой команды используется для указания мертвого интервала.

Форма **delete** этой команды используется для восстановления длительности мертвого интервала по умолчанию.

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

## 10.5.11. protocols ospf area <идентификатор_области> virtual-link <ipv4-адрес> hello-interval <интервал>

Установка интервала между пакетами приветствия OSPF на виртуальном канале.

**Синтаксис**

**set protocols ospf area** *идентификатор_области* **virtual-link** *ipv4-адрес* **hello-interval** *интервал*

**delete protocols ospf area** *идентификатор_области* **virtual-link** *ipv4-адрес* **hello-interval**

**show protocols ospf area** *идентификатор_области* **virtual-link** *ipv4-адрес* **hello-interval**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
          ospf {
               area текст {
                    virtual-link ipv4-адрес {
                         hello-interval 1-65535
                    }
               }
          }
}
```

**Параметры**

*идентификатор_области*

Обязательный. Идентификатор настраиваемой области OSPF. В качестве идентификатора может быть указан IP-адрес или десятичное число.

*ipv4-адрес*

Обязательный. Областной идентификатор виртуального канала, выраженный в форме IPv4-адреса.

*интервал*

Обязательный. Интервал (в секундах) между пакетами приветствия. Это значение должно быть одинаковым на всех узлах системы. Значение должно лежать в диапазоне от 1 до 65535. Значение по умолчанию равно 10.

**Значение по умолчанию**

Пакеты приветствия отправляются каждые 10 секунд.

**Указания по использованию**

Эта команда используется для установки интервала, с которым на виртуальном канале отправляются пакеты приветствия OSPF.

Пакет приветствия - это пакет OSPF, используемый для обнаружения соседей в той же подсети (непосредственно подключенных маршрутизаторов) и поддержания взаимоотношений с ними. Чем больше интервал между пакетами приветствия, тем меньше служебный трафик между маршрутизаторами, но тем дольше происходит обнаружение изменений в топологии.

Интервал приветствия должен быть одинаковым на всех маршрутизаторах, предназначенных для установления двунаправленной связи в сети. Если его величина на двух маршрутизаторах не согласована, их смежность не будет установлена, и каждый из них не будет учитывать связи, устанавливаемые на другом.

Форма **set** этой команды используется для установки интервала приветствия.

Форма **delete** этой команды используется для восстановления интервала приветствия по умолчанию.

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

## 10.5.12. protocols ospf area <идентификатор_области> virtual-link <ipv4-адрес> retransmit-interval <интервал>

Указание интервала повторной передачи для виртуального канала.

**Синтаксис**

```
set protocols ospf area идентификатор_области virtual-
link ipv4-адрес retransmit-interval интервал

delete protocols ospf area идентификатор_области virtual-
link ipv4-адрес retransmit-interval

show protocols ospf area идентификатор_области virtual-
link ipv4-адрес retransmit-interval
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
```

```
                ospf {
                     area текст {
                          virtual-link ipv4-адрес {
                               retransmit-interval 1-65535
                          }
                     }
                }
          }
```

**Параметры**

*идентификатор_области*

Обязательный. Идентификатор настраиваемой области OSPF. В качестве идентификатора может быть указан IP-адрес или десятичное число.

*ipv4-адрес*

Обязательный. Областной идентификатор виртуального канала, выраженный в форме IPv4-адреса.

*интервал*

Обязательный. Интервал (в секундах) между повторными передачами неподтвержденных объявлений состояния канала. Это значение должно быть одинаковым на всех узлах системы. Значение должно лежать в диапазоне от 1 до 65535. Значение по умолчанию равно 5.

**Значение по умолчанию**

Неподтвержденные LSA передаются повторно с 5-секундным интервалом.

**Указания по использованию**

Команда используется для установки интервала повторной передачи для виртуального канала. Данный параметр представляет число секунд до повторной передачи неподтвержденного объявления состояния канала.

Когда маршрутизатор с OSPF отправляет LSA соседу, сосед подтверждает получение пакетом подтверждения состояния канала (link-state acknowledgement, LS Ack). Если происходит сбой при приеме локальным маршрутизатором ожидаемого пакета LS Ack, маршрутизатор повторно передает LSA с интервалом, указанным данной командой. Это значение

должно быть одинаковым на всех узлах системы.

Форма **set** этой команды используется для установки значения по умолчанию для интервала повторной передачи.

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

Форма **show** этой команды используется для отображения настройки интервала повторной передачи.

## 10.5.13. protocols ospf area <идентификатор_области> virtual-link <ipv4-адрес> transmit-delay <задержка>

Указание задержки передачи для виртуального канала.

**Синтаксис**

**set protocols ospf area** *идентификатор_области* **virtual-link** *ipv4-адрес* **transmit-delay** *задержка*

**delete protocols ospf area** *идентификатор_области* **virtual-link** *ipv4-адрес* **transmit-delay**

**show protocols ospf area** *идентификатор_области* **virtual-link** *ipv4-адрес* **transmit-delay**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
          ospf {
               area текст {
                    virtual-link ipv4-адрес {
                         transmit-delay 1-65535
                    }
               }
          }
}
```

**Параметры**

*идентификатор_области*

Обязательный. Идентификатор настраиваемой области OSPF. В качестве

идентификатора может быть указан IP-адрес или десятичное число.

*ipv4-адрес*

Обязательный. Областной идентификатор виртуального канала, выраженный в форме IPv4-адреса.

*задержка*

Обязательный. Задержка (в секундах) между последовательными передачами состояния канала. Это значение должно быть одинаковым на всех узлах системы. Значение должно лежать в диапазоне от 1 до 65535. Значение по умолчанию равно 1.

**Значение по умолчанию**

Передача состояния канала происходит с одно секундным интервалом.

**Указания по использованию**

Команда используется для установки задержки передачи на виртуальном канале в области. Устанавливаемое значение является примерным временем, необходимым для отправки пакета обновления состояния канала (LSU).

Этот таймер используется для согласования запаздывания передачи и распространения в подсети, особенно в низкоскоростных подсетях, где запаздывания могут быть значительными. Для учета таких изменений маршрутизатор увеличивает на единицу возраст объявлений состояний каналов в пакетах LSU.

В указанное время входят как время передачи, так и запаздывание при распространении через сеть. Перед передачей LSA к возрасту пакета LSA добавляется задержка передачи. Возраст LSA используется сетью для расстановки LSA в правильном порядке, чтобы можно было определить, какие из конкурирующих LSA являются более свежими и достоверными.

LSA нумеруются в последовательности, но номера последовательности конечны и потому не могут использоваться как единственное средство определения наиболее свежего LSA. Потому OSPF отслеживает ещё и возраст LSA. Каждый раз при передаче LSA на другой маршрутизатор к возрасту LSA добавляется задержка передачи. Возраст пакета вместе с его номером в последовательности помогает маршрутизатору-получателю определить, какая версия полученного LSA является более свежей и потому

должна использоваться.

Форма **set** этой команды используется для установки задержки передачи.

Форма **delete** этой команды используется для восстановления задержки передачи по умолчанию.

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

## 10.5.14. show debugging ospf

Отображение флагов отладки протокола OSPF.

**Синтаксис**

```
show debugging ospf
```

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для вывода режима отладки OSPF.

## 10.5.15. 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.

**Примеры**

В примере 10.11 приведен образец вывода сведений OSPF.

*Пример 10.11 - "show ip ospf": отображение сведений о настройке OSPF*

```
admin@neo:~$ show ip ospf
OSPF Routing Process, Router ID: 10.100.10.1
Supports only single TOS (TOS0) routes
This implementation conforms to RFC2328
RFC1583Compatibility flag is disabled
OpaqueCapability flag is disabled
Initial SPF scheduling delay 200 millisec(s)
Minimum hold time between consecutive SPFs 1000
millisec(s)
Maximum hold time between consecutive SPFs 10000
millisec(s)
Hold time multiplier is currently 1
SPF algorithm last executed 1w2d01h ago
SPF timer is inactive
Refresh timer 10 secs
Number of external LSA 1. Checksum Sum 0x000083e4
Number of opaque AS LSA 0. Checksum Sum 0x00000000
Number of areas attached to this router: 1
Area ID: 10.1.0.0
Shortcutting mode: Default, S-bit consensus: no
Number of interfaces in this area: Total: 1, Active: 1
Number of fully adjacent neighbors in this area: 2
Area has no authentication
Number of full virtual adjacencies going through this
area: 0
SPF algorithm executed 3 times
Number of LSA 4
Number of router LSA 3. Checksum Sum 0x0000ccad
```

```
Number of network LSA 1. Checksum Sum 0x00000df2
Number of summary LSA 0. Checksum Sum 0x00000000
Number of ASBR summary LSA 0. Checksum Sum 0x00000000
Number of NSSA LSA 0. Checksum Sum 0x00000000
Number of opaque link LSA 0. Checksum Sum 0x00000000
Number of opaque area LSA 0. Checksum Sum 0x00000000
```

## 10.5.16. 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.

**Примеры**

В примере 10.12 приведен образец вывода сведений о граничных маршрутизаторах OSPF.

*Пример 10.12 - "show ip ospf border-router": отображение сведений о граничных маршрутизаторах OSPF*

```
admin@neo:~$ show ip ospf border-routers
============ OSPF router routing table ============= R
     10.1.0.58 [10] area: 10.1.0.0, ASBR
via 10.1.0.58, eth2
```

## 10.5.17. show ip ospf database

Отображение сведений о базе данных OSPF.

**Синтаксис**

**show ip ospf database** [**max-age** | **self-originate** | {**asbr-summary** | **external** | **network** | **nssa-external** | **opaque-area** | **opaque-as** | **opaque-link** | **router** | **summary**} [**adv-router** *ipv4-адрес* | *ipv4-адрес* [**adv-router** *ipv4-адрес* | **self-originate**]]]

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**max-age**

Отображение базы данных максимального возраста OSPF.

**self-originate**

Отображение базы данных маршрутов OSPF, созданных локальным маршрутизатором.

**asbr-summary**

Отображение базы данных сводок граничных маршрутизаторов автономных систем (Autonomous System Border Router, ASBR) OSPF.

*расст_для_внешних*

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.

**adv-router** *ipv4-адрес*

Необязательный. Отображение базы данных OSPF для данного адреса указанного объявляемого маршрутизатора.

*ipv4-адрес*

Необязательный. Отображение базы данных OSPF для данного адреса.

**self-originate**

Необязательный. Отображение базы данных маршрутов OSPF для данного адреса, созданных локальным маршрутизатором.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для отображения сведений базы данных OSPF.

**Примеры**

В примере 10.13 приведен образец вывода общих сведений базы данных OSPF.

*Пример 10.13 - "show ip ospf database": отображение общих сведений базы данных OSPF*

```
admin@neo:~$ show ip ospf database

OSPF Router with ID (10.100.10.1)

Router Link States (Area 10.1.0.0)

Link ID   ADV Router     Age
     Seq# CkSum     Link count

10.1.0.33 10.1.0.33 123  0x800003e5
     0x791f    1

10.1.0.58 10.1.0.58 123  0x80000562
     0x4e7e    1

10.100.10.1    10.100.10.1
     117  0x800001b6     0xfe13
     1

Net Link States (Area 10.1.0.0)

Link ID   ADV Router     Age
     Seq# CkSum
```

```
10.1.0.58 10.1.0.58 123 0x800003df 0x0bf3

AS External Link States

Link ID   ADV Router     Age
     Seq# CkSum     Route

76.0.0.0  10.1.0.58 1850 0x800000b3 0x83e4 E2

76.0.0.0/8 [0x0]
```

## 10.5.18. 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.

**Примеры**

В примере 10.14 приведен образец вывода сведений OSPF по всем интерфейсам.

*Пример 10.14 - "show ip ospf interface": отображение сведений о настройке и состоянии OSPF*

```
admin@neo:~$ show ip ospf interface

eth0 is down

ifindex 3, MTU 1500 bytes, BW 0 Kbit
<UP,BROADCAST,MULTICAST> OSPF not enabled on this
interface

eth1 is down

ifindex 4, MTU 1500 bytes, BW 0 Kbit
```

```
<UP,BROADCAST,MULTICAST> OSPF not enabled on this
interface

eth1_rename is down

ifindex 0, MTU 1500 bytes, BW 0 Kbit
<BROADCAST,MULTICAST> OSPF not enabled on this interface

eth2 is up

ifindex 5, MTU 1500 bytes, BW 0 Kbit

<UP,BROADCAST,RUNNING,MULTICAST>

Internet Address 10.1.0.62/24, Broadcast 10.1.0.255,
Area 10.1.0.0

MTU mismatch detection:enabled

Router ID 10.100.10.1, Network Type BROADCAST, Cost: 10

Transmit Delay is 1 sec, State DROther, Priority 1

Designated Router (ID) 10.1.0.58, Interface Address
10.1.0.58

Backup Designated Router (ID) 10.1.0.33, Interface
Address 10.1.0.33

Multicast group memberships: OSPFAllRouters

Timer intervals configured, Hello 10s, Dead 40s, Wait
40s, Retransmit 5

Hello due in 0.721s

Neighbor Count is 2, Adjacent neighbor count is 2
eth2_rename is down

ifindex 0, MTU 1500 bytes, BW 0 Kbit
<BROADCAST,MULTICAST>

OSPF not enabled on this interface eth3 is down

ifindex 2, MTU 1500 bytes, BW 0 Kbit
<BROADCAST,MULTICAST>

OSPF not enabled on this interface lo is up

ifindex 1, MTU 16436 bytes, BW 0 Kbit
<UP,LOOPBACK,RUNNING>

OSPF not enabled on this interface
```

## 10.5.19. 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.

**Примеры**

В примере 10.15 приведен образец вывода сведений о соседях по OSPF для всех соседей.

*Пример 10.15 - "show ip ospf neighbor": отображение сведений о соседях по OSPF*

```
admin@neo:~$ show ip ospf neighbor

Neighbor ID Pri State    Dead Time Address
     Interface RXmtL RqstL DBsmL

10.1.0.33 1 Full/Backup
     33.842s 10.1.0.33 eth2:10.1.0.62
```

```
          0    0    0

10.1.0.58 1 Full/DR
     38.581s 10.1.0.58 eth2:10.1.0.62
          0    0    0
```

## 10.5.20. 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.

**Примеры**

В примере 10.16 приведен образец вывода сведений о маршрутах OSPF.

*Пример 10.16 - "show ip ospf route": отображение сведений о маршрутах OSPF*

```
admin@neo:~$ show ip ospf route

============ OSPF network routing table ============ N
     10.1.0.0/24    [10] area: 10.1.0.0

directly attached to eth2

============ OSPF router routing table ============= R
     10.1.0.58 [10] area: 10.1.0.0, ASBR

via 10.1.0.58, eth2

============ OSPF external routing table =========== N
E2 76.0.0.0/8  [10/20] tag: 0

via 10.1.0.7, eth2
```

### 10.5.21. 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.

**Примеры**

В примере 10.17 приведен вывод всех маршрутов OSPF на IP.

*Пример 10.17 - "show ip route ospf": отображение маршрутов*

```
admin@neo:~$ show ip route ospf

Codes: K - kernel route, C - connected, S - static, R -
RIP, O - OSPF, I - ISIS, B - BGP, > - selected route, *
- FIB route

O    10.1.0.0/24 [110/10] is directly connected, eth2,
01w2d21h O>* 76.0.0.0/8 [110/20] via 10.1.0.7, eth2,
4d12h48m
```

## 10.6. Команды OSPF для интерфейсов

В данном разделе описаны команды настройки OSPF на различных интерфейсах.

Рассматриваются следующие команды:

| Команды настройки | |
|---|---|
| `interfaces <интерфейс> ip ospf` | Включение OSPF на указанном интерфейсе. |
| `interfaces <интерфейс> ip ospf authentication` | Указание метода аутентификации для OSPF на интерфейсе. |

| | |
|---|---|
| `interfaces <интерфейс> ip ospf bandwidth <проп_спос>` | Указание пропускной способности интерфейса для вычисления стоимости OSPF. |
| `interfaces <интерфейс> ip ospf cost <стоимость>` | Установка стоимости маршрутизации для OSPF на интерфейсе. |
| `interfaces <интерфейс> ip ospf dead-interval <интервал>` | Установка мертвого интервала OSPF на интерфейсе. |
| `interfaces <интерфейс> ip ospf hello-interval <интервал>` | Установка интервала между пакетами приветствия OSPF на интерфейсе. |
| `interfaces <интерфейс> ip ospf mtu-ignore` | Отключение определения несоответствия MTU на интерфейсе. |
| `interfaces <интерфейс> ip ospf network <тип>` | Указание типа подсети OSPF на интерфейсе. |
| `interfaces <интерфейс> ip ospf priority <приоритет>` | Установка приоритета OSPF на интерфейсе. |
| `interfaces <интерфейс> ip ospf retransmit-interval <интервал>` | Установка интервала повторной передачи OSPF на интерфейсе. |
| `interfaces <интерфейс> ip ospf transmit-delay <задержка>` | Указание задержки передачи OSPF на интерфейсе. |

Эксплуатационные команды

Отсутствует.

### 10.6.1. interfaces <интерфейс> ip ospf

Включение OSPF на указанном интерфейсе.

**Синтаксис**

**set interfaces** *интерфейс* **ip ospf**

**delete interfaces** *интерфейс* **ip ospf**

**show interfaces** *интерфейс* **ip ospf**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces текст {
        ip {
            ospf {
            }
        }
}
```

**Параметры**

*интерфейс*

Обязательный. Тип интерфейса. Подробное описание ключевых слов и аргументов приведено в таблице в Приложении 3 на стр. 2105.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для включения протокола маршрутизации OSPF на интерфейсе.

Форма **set** этой команды используется для включения OSPF на интерфейсе.

Форма **delete** этой команды используется для удаления всей настройки OSPF и отключения OSPF на указанном интерфейсе.

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

## 10.6.2. interfaces <интерфейс> ip ospf authentication

Указание метода аутентификации для OSPF на интерфейсе.

**Синтаксис**

**set interfaces** *интерфейс* **ip ospf authentication** [**md5 key-id** *ид_ключа* **md5-key** *ключ_md5* | **plaintext-password** *пароль*]

**delete interfaces** *интерфейс* **ip ospf authentication** [**md5 key-id** *ид_ключа* **md5-key** | **plaintext-password**]

**show interfaces** *интерфейс* **ip ospf authentication** [**md5 key-id** *ид_ключа* **md5-key** | **plaintext-password**]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces текст {
          ip {
               ospf {
                    authentication {
                         md5 {

     key-id 1-255 {

          md5-key текст

     }
                         }
                         plaintext-password текст
                    }
               }
          }
}
```

**Параметры**

*интерфейс*

Обязательный. Тип интерфейса. Подробное описание ключевых слов и аргументов приведено в таблице в Приложении 3 на стр. 2105.

*ид_ключа*

Необязательный. Ключ, используемый для идентификации ключа MD5. Он должен быть одинаковым на отправляющей и принимающей системах. Значение должно лежать в диапазоне от 1 до 255.

*ключ_md5*

Необязательный. Паролеподобный ключ MD5, состоящий не более чем из 16

алфавитно-цифровых символов и используемый в качестве входных данных для алгоритма хэширования MD5. Чем длиннее ключ, тем выше безопасность. Он должен быть одинаковым на отправляющей и принимающей системах.

*пароль*

Необязательный. Пароль, используемый в простой аутентификации (открытыми текстом). Он должен быть не длиннее восьми символов и одинаковым на отправляющей и принимающей системах.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Команда используется для указания метода аутентификации, применяемого протоколом OSPF на интерфейсе. Эта аутентификация независима от аутентификации, настроенной в области OSPF.

При простой аутентификации пароли пересылаются через сеть открытым текстом. При аутентификации MD5 в системе используется алгоритм Message Digest 5 (MD5) для вычисления значения хэш-кода из содержимого пакета и пароля OSPF. Вычисленное значение хэш-кода и ключ MD5 включаются в состав передаваемого пакета, и принимающая система (настроенная с тем же самым паролем) вычисляет свой хэш-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 смежность не будет установлена, и каждый из них не будет учитывать связи, устанавливаемые на другом.

Форма **set** этой команды используется для установки аутентификации на интерфейсе.

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

Форма **show** этой команды используется для отображения сведений о настройке аутентификации.

### 10.6.3. interfaces <интерфейс> ip ospf bandwidth <проп_спос>

Указание пропускной способности интерфейса для вычисления стоимости OSPF.

**Синтаксис**

**set interfaces** *интерфейс* **ip ospf bandwidth** *проп_спос*

**delete interfaces** *интерфейс* **ip ospf bandwidth**

**show interfaces** *интерфейс* **ip ospf bandwidth**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces текст {
        ip {
            ospf {
                bandwidth целоебеззнака32разр
            }
        }
}
```

**Параметры**

*интерфейс*

Обязательный. Тип интерфейса. Подробное описание ключевых слов и аргументов приведено в таблице в Приложении 3 на стр. 2105.

*проп_спос*

Пропускная способность интерфейсов Ethernet в килобитах/с. Значение должно лежать в диапазоне от 1 до 10000000.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Команда используется для указания пропускной способности интерфейса в целях расчета стоимости OSPF.

Форма **set** этой команды используется для указания пропускной способности интерфейса.

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

пропускной способности.

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

## 10.6.4. interfaces <интерфейс> ip ospf cost <стоимость>

Установка стоимости маршрутизации для OSPF на интерфейсе.

**Синтаксис**

**set interfaces** *интерфейс* **ip ospf cost** *стоимость*

**delete interfaces** *интерфейс* **ip ospf cost**

**show interfaces** *интерфейс* **ip ospf cost**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces текст {
          ip {
               ospf {
                    cost целоебеззнака32разр
               }
          }
}
```

**Параметры**

*интерфейс*

Обязательный. Тип интерфейса. Подробное описание ключевых слов и аргументов приведено в таблице в Приложении 3 на стр. 2105.

*стоимость*

Метрика состояния канала (стоимость OSPF), объявляемая в LSA в качестве стоимости отправки пакетов по интерфейсу. Значение должно лежать в диапазоне от 1 до 65535.

**Значение по умолчанию**

Подробные сведения об умолчаниях для стоимости OSPF приведены ниже в пункте "Указания по использованию".

**Указания по использованию**

Команда используется для переопределения вручную стоимости OSPF по умолчанию, вычисленной системой на интерфейсе. На интерфейсе можно назначить только одну стоимость.

По умолчанию метрика, связанная с каналом, вычисляется по следующей формуле:

```
стоимость = 108 / пропускная_способность
```

Стоимость достижения любого места назначения есть сумма стоимостей отдельных транзитных участков. Стоимости всегда округляются до ближайшего целого. Стоимости, меньшие 1, округляются до 1.

В таблице 30 приведены стоимости OSPF для некоторых распространенных типов линий связи.

*Таблица 30 - Стоимости OSPF для распространенных типов линий связи*

| Тип линии связи | Стоимость OSPF |
|---|---|
| 56 Кбит/с | 1785 |
| 64 Кбит/с | 1562 |
| 128 Кбит/с | 781 |
| 256 Кбит/с | 390 |
| 512 Кбит/с | 195 |
| 768 Кбит/с | 130 |
| T1 (1,544 Мбит/с) | 64 |
| E1 (2,048 Мбит/с) | 48 |
| 4 Мбит/с по Token Ring | 6 |
| 10 Мбит/с по Ethernet | 10 |
| 16 Мбит/с по Token Ring | 6 |
| T3 (44,736 Мбит/с) | 2 |
| 100 и более Мбит/с | 1 |

Из чисел, приведенных в таблице 30, видно, что OSPF не дает возможности различить интерфейсы быстрее 100 Мбит/с, например интерфейсы быстрого Ethernet (100 Мбит/с) и гигабитного Ethernet (1000 Мбит/с). Если необходимо различить интерфейсы от 100 Мбит/с и быстрее, необходимо вручную назначить стоимость для них с помощью данной команды.

Форма **set** этой команды используется для указания стоимости OSPF на

интерфейсе.

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

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

## 10.6.5. interfaces <интерфейс> ip ospf dead-interval <интервал>

Установка мертвого интервала OSPF на интерфейсе.

**Синтаксис**

**set interfaces** *интерфейс* **ip ospf dead-interval** *интервал*

**delete interfaces** *интерфейс* **ip ospf dead-interval**

**show interfaces** *интерфейс* **ip ospf dead-interval**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces текст {
          ip {
               ospf {
                    dead-interval целоебеззнака32разр
               }
          }
}
```

**Параметры**

*интерфейс*

Обязательный. Тип интерфейса. Подробное описание ключевых слов и аргументов приведено в таблице в Приложении 3 на стр. 2105.

*интервал*

Время в секундах, которое данный интерфейс должен ожидать для обнаружения пакетов приветствия от соседних маршрутизаторов до объявления соседа неработоспособным. Значение должно лежать в диапазоне от 1 до 65535. По умолчанию выбирается четырехкратная

величина интервала приветствия.

**Значение по умолчанию**

Мертвый интервал вчетверо дольше интервала приветствия.

**Указания по использованию**

Команда используется для указания интервала, в течение которого интерфейс ожидает получения пакетов приветствия от своего соседа.

Если в течение мертвого интервала интерфейс не получает пакета приветствия от соседа, то статус соседа изменяется на неработоспособный, а всё соответствующее состояние очищается.

Мертвый интервал должен быть одинаковым на всех маршрутизаторах, предназначенных для установления двунаправленной связи в сети. Если его величина на двух маршрутизаторах не согласована, их смежность не будет установлена, и каждый из них не будет учитывать связи, устанавливаемые на другом.

Форма **set** этой команды используется для указания мертвого интервала.

Форма **delete** этой команды используется для восстановления длительности мертвого интервала по умолчанию.

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

## 10.6.6. interfaces <интерфейс> ip ospf hello-interval <интервал>

Установка интервала между пакетами приветствия OSPF на интерфейсе.

**Синтаксис**

**set interfaces** *интерфейс* **ip ospf hello-interval** *интервал*

**delete interfaces** *интерфейс* **ip ospf hello-interval**

**show interfaces** *интерфейс* **ip ospf hello-interval**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces текст {
        ip {
            ospf {
```

```
                    hello-interval целоебеззнака32разр
                }
            }
        }
```

**Параметры**

*интерфейс*

Обязательный. Тип интерфейса. Подробное описание ключевых слов и аргументов приведено в таблице в Приложении 3 на стр. 2105.

*интервал*

Обязательный. Интервал (в секундах) между пакетами приветствия. Это значение должно быть одинаковым на всех узлах системы. Значение должно лежать в диапазоне от 1 до 65535. Значение по умолчанию равно 10.

**Значение по умолчанию**

Пакеты приветствия отправляются каждые 10 секунд.

**Указания по использованию**

Эта команда используется для установки интервала, с которым на интерфейсе отправляются пакеты приветствия OSPF.

Пакет приветствия - это пакет OSPF, используемый для обнаружения соседей в той же подсети (непосредственно подключенных маршрутизаторов) и поддержания взаимоотношений с ними. Чем больше интервал между пакетами приветствия, тем меньше служебный трафик между маршрутизаторами, но тем дольше происходит обнаружение изменений в топологии.

Интервал приветствия должен быть одинаковым на всех маршрутизаторах, предназначенных для установления двунаправленной связи в сети. Если его величина на двух маршрутизаторах не согласована, их смежность не будет установлена, и каждый из них не будет учитывать связи, устанавливаемые на другом.

Форма **set** этой команды используется для установки интервала приветствия.

Форма **delete** этой команды используется для восстановления интервала приветствия по умолчанию.

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

интервала приветствия.

## 10.6.7. interfaces <интерфейс> ip ospf mtu-ignore

Отключение определения несоответствия MTU на интерфейсе.

**Синтаксис**

**set interfaces** *интерфейс* **ip ospf mtu-ignore**

**delete interfaces** *интерфейс* **ip ospf mtu-ignore**

**show interfaces** *интерфейс* **ip ospf**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces текст {
        ip {
            ospf {
                mtu-ignore
            }
        }
}
```

**Параметры**

*интерфейс*

Обязательный. Тип интерфейса. Подробное описание ключевых слов и аргументов приведено в таблице в Приложении 3 на стр. 2105.

**Значение по умолчанию**

Определение несоответствия MTU включено по умолчанию.

**Указания по использованию**

Команда используется для отключения определения несоответствия MTU на интерфейсе OSPF.

OSPF отправляет значение MTU интерфейса в пакете описания базы данных. Если значения MTU у соседей по OSPF не соответствуют друг другу, смежность по OSPF не может быть сформирована. Функция определения несоответствия MTU определяет несоответствия MTU и сообщает о них в форме отладочного сообщения.

Возможность определения несоответствия MTU является важным средством поиска и устранения неполадок. Если определение несоответствия MTU не включено, то несоответствие MTU можно определить только проверкой настройки обоих интерфейсов.

Бывают развертывания сетей, в которых несоответствия MTU не только неустранимы, но даже являются частью нормального развертывания. Только в таких случаях определение несоответствия MTU следует отключать для формирования нормальной смежности по OSPF.

Форма **set** этой команды используется для отключения определения несоответствия MTU.

Форма **delete** этой команды используется для повторного включения определения несоответствия MTU.

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

## 10.6.8. interfaces <интерфейс> ip ospf network <тип>

Указание типа подсети OSPF на интерфейсе.

**Синтаксис**

```
set interfaces интерфейс ip ospf network тип
delete interfaces интерфейс ip ospf network
show interfaces интерфейс ip ospf network
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces текст {
        ip {
            ospf {
                network текст
            }
        }
}
```

**Параметры**

*интерфейс*

Обязательный. Тип интерфейса. Подробное описание ключевых слов и аргументов приведено в таблице в Приложении 3 на стр. 2105.

*тип*

Тип подсети для данного интерфейса. Поддерживаются следующие значения:

**broadcast**: интерфейс поддерживает вещательный режим, например канал ЛВС.

**non-broadcast**: интерфейс не поддерживает вещательный режим.

**point-to-point**: интерфейс поддерживает режим "точка-точка", например интерфейс NBMA.

**point-to-multipoint**: интерфейс поддерживает режим "точка-несколько точек", например интерфейс PPP или логический интерфейс "точка-точка" на Frame Relay.

Значение по умолчанию равно **broadcast**.

#### Значение по умолчанию

Поддерживается вещательный режим.

#### Указания по использованию

Команда используется для настройки и отображения типа подсети на интерфейсе.

Форма **set** этой команды используется для указания типа подсети.

Форма **delete** этой команды используется для удаления типа подсети.

Форма **show** этой команды используется для отображения типа подсети.

## 10.6.9. interfaces <интерфейс> ip ospf priority <приоритет>

Установка приоритета OSPF на интерфейсе.

#### Синтаксис

**set interfaces** *интерфейс* **ip ospf priority** *приоритет*

**delete interfaces** *интерфейс* **ip ospf priority**

**show interfaces** *интерфейс* **ip ospf priority**

#### Режим интерфейса

Режим настройки.

**Ветвь конфигурации**

```
interfaces текст {
        ip {
            ospf {
                priority целоебеззнака32разр
            }
        }
}
```

**Параметры**

*интерфейс*

Обязательный. Тип интерфейса. Подробное описание ключевых слов и аргументов приведено в таблице в Приложении 3 на стр. 2105.

*приоритет*

Приоритет маршрутизатора OSPF на данном интерфейсе. Значение должно лежать в диапазоне от 0 до 255, причем маршрутизатор с приоритетом 0 не может быть выделенным маршрутизатором. Значение по умолчанию равно 1.

**Значение по умолчанию**

Интерфейс OSPF имеет приоритет 1.

**Указания по использованию**

Команда используется для установки приоритета на интерфейсе в вещательной подсети, к которой подключен интерфейс. Приоритет определяет, какие маршрутизаторы выбираются выделенными маршрутизаторами (Designated Router, DR) и резервными выделенными маршрутизаторами (Backup Designated Router, BDR) области.

DR и BDR используются для сокращения объема избыточного трафика OSPF в вещательных сетях путем сокращения числа смежных маршрутизаторов, которым маршрутизатор должен рассылать свои сведения о топологии. В вещательных сетях (наподобие Ethernet) каждый маршрутизатор устанавливает отношение смежности с одним DR и одним BDR, а не с каждым маршрутизатором в его области. Затем DR и BDR рассылают эти сведения всем другим маршрутизаторам в данном сегменте

сети.

Приоритет может лежать в диапазоне от 0 до 255. Маршрутизатор с самым высоким приоритетом выбирается в качестве DR, а со следующим по величине - в качестве BDR. Чем больше число, тем выше приоритет.

Маршрутизаторы с приоритетом 0 не подлежат выбору в качестве выделенных.

Форма **set** этой команды используется для указания приоритета OSPF.

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

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

## 10.6.10. interfaces <интерфейс> ip ospf retransmit-interval <интервал>

Установка интервала повторной передачи OSPF на интерфейсе.

**Синтаксис**

**set interfaces** *интерфейс* **ip ospf retransmit-interval** *интервал*

**delete interfaces** *интерфейс* **ip ospf retransmit-interval**

**show interfaces** *интерфейс* **ip ospf retransmit-interval**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces текст {
          ip {
               ospf {
                    retransmit-interval
целоебеззнака32разр
               }
          }
}
```

**Параметры**

*интерфейс*

Обязательный. Тип интерфейса. Подробное описание ключевых слов и аргументов приведено в таблице в Приложении 3 на стр. 2105.

*интервал*

Время (в секундах) ожидания подтверждения, после которого система повторяет передачу LSA своим соседям. Значение должно лежать в диапазоне от 3 до 65535. Значение по умолчанию равно 5.

**Значение по умолчанию**

Неподтвержденные LSA передаются повторно с 5-секундным интервалом.

**Указания по использованию**

Команда используется для указания времени, в течение которого интерфейс должен ожидать подтверждения обновления состояния канала перед повторной отправкой обновления.

Пакет обновления состояния канала является частью обмена базами данных топологи между маршрутизаторами. При отправке пакета начального описания базы данных (DD) в нем содержатся только заголовки LSA. Если принимающий маршрутизатор определяет, что ему нужен некий фрагмент топологии OSPF, он отправляет пакет запроса состояния канала для запроса полного пакета LSA у отправляющего маршрутизатора.

После отправки пакета обновления отправляющий маршрутизатор ожидает подтверждения (явного или неявного) от отправляющего маршрутизатора. При явном подтверждении принимающий маршрутизатор отправляет пакет подтверждения состояния канала (LS-Ack) маршрутизатору, отправившему обновление. При неявном подтверждении маршрутизатор, отправивший обновление, принимает LSA со сведениями об обновлении от получающего маршрутизатора.

Если за время интервала повторной передачи не приходит ни явного, ни неявного подтверждения, отправляющий маршрутизатор повторит передачу пакета обновления состояния канала.

Если интервал слишком велик, сеть стабилизируется медленно. Если интервал слишком мал, происходят ненужные повторные передачи.

Форма **set** этой команды используется для установки интервала повторной передачи OSPF на интерфейсе.

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

Форма **show** этой команды используется для отображения настройки интервала повторной передачи.

## 10.6.11. interfaces <интерфейс> ip ospf transmit-delay <задержка>

Указание задержки передачи OSPF на интерфейсе.

**Синтаксис**

**set interfaces** *интерфейс* **ip ospf transmit-delay** *задержка*

**delete interfaces** *интерфейс* **ip ospf transmit-delay**

**show interfaces** *интерфейс* **ip ospf transmit-delay**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces текст {
          ip {
               ospf {
                    transmit-delay целоебеззнака32разр
               }
          }
}
```

**Параметры**

*интерфейс*

Обязательный. Тип интерфейса. Подробное описание ключевых слов и аргументов приведено в таблице в Приложении 3 на стр. 2105.

*задержка*

Обязательный. Задержка (в секундах) между последовательными передачами состояния канала. Это значение должно быть одинаковым на всех узлах системы. Значение должно лежать в диапазоне от 1 до 65535. Значение по умолчанию равно 1.

**Значение по умолчанию**

Передача состояния канала происходит с одно секундным интервалом.

**Указания по использованию**

Команда используется для установки задержки передачи на интерфейсе. Устанавливаемое значение является примерным временем, необходимым для отправки пакета обновления состояния канала (LSU).

Этот таймер используется для согласования запаздывания передачи и распространения в подсети, особенно в низкоскоростных подсетях, где запаздывания могут быть значительными. Для учета таких изменений маршрутизатор увеличивает на единицу возраст объявлений состояний каналов в пакетах LSU.

В указанное время входят как время передачи, так и запаздывание при распространении через сеть. Перед передачей LSA к возрасту пакета LSA добавляется задержка передачи. Возраст LSA используется сетью для расстановки LSA в правильном порядке, чтобы можно было определить, какие из конкурирующих LSA являются более свежими и достоверными.

LSA нумеруются в последовательности, но номера последовательности конечны и потому не могут использоваться как единственное средство определения наиболее свежего LSA. Потому OSPF отслеживает ещё и возраст LSA. Каждый раз при передаче LSA на другой маршрутизатор к возрасту LSA добавляется задержка передачи. Возраст пакета вместе с его номером в последовательности помогает маршрутизатору-получателю определить, какая версия полученного LSA является более свежей и потому должна использоваться.

Форма **set** этой команды используется для установки задержки передачи.

Форма **delete** этой команды используется для восстановления задержки передачи по умолчанию.

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

# 11. ПОЛИТИКИ МАРШРУТИЗАЦИИ

Политика маршрутизации — 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 Altell NEO политики маршрутизации 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 Altell NEO, 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 Altell NEO, 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.

## 11.1. 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.

### 11.1.1. Фильтрация маршрутов с помощью списков доступа

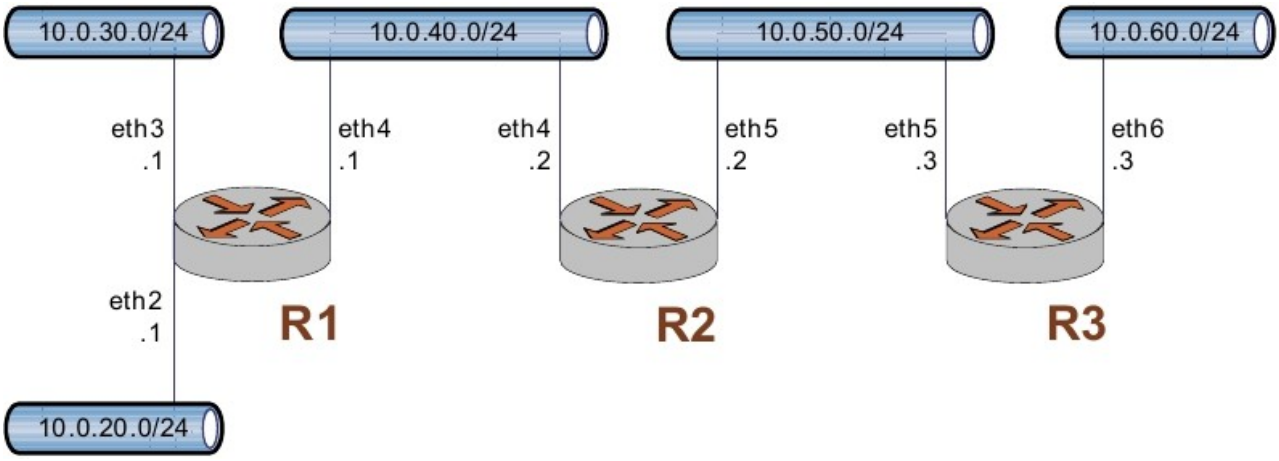
В этом разделе рассматриваются следующие вопросы:

- 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. 14.

*Рисунок 14 - Эталонная схема настройки RIP*




### *11.1.1.1. Основная настройка RIP*

В данном примере предполагается, что интерфейсы маршрутизатора уже настроены; настройка протокола RIP на каждом из маршрутизаторов приведена ниже.

*Пример 11.1 - Основная настройка RIP*

| Маршрутизатор | Действие | Команда (команды) |
|---|---|---|
| R1 | Отображение настройки. | admin@R1# **show protocols**<br>rip {<br>network 10.0.40.0/24<br>redistribute {<br>connected {<br>}<br>}<br>}<br>[edit] |
| R2 | Отображение настройки. | admin@R2# **show protocols**<br>rip {<br>network 10.0.40.0/24<br>network 10.0.50.0/24<br>redistribute { |

```
                    connected {
                    }
               }
          }
          [edit]
```

R3 Отображение настройки.

```
admin@R3# show protocols
rip {
     network 10.0.50.0/24
     redistribute {
          connected {
          }
     }
}
[edit]
```

#### *11.1.1.2. Проверка настройки RIP*

Для проверки настройки RIP можно использовать следующие команды эксплуатационного режима.

##### 11.1.1.2.1. R3: show ip routes

В примере 11.2 приведен вывод для команды **show ip route** для маршрутизатора R3.

*Пример 11.2 - Проверка RIP на R3: "show ip route"*

```
admin@R3:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O -
OSPF, I - ISIS, B - BGP, > - selected route, * - FIB route

R>* 10.0.20.0/24 [120/3] via 10.0.50.2, eth5, 00:20:16
R>* 10.0.30.0/24 [120/3] via 10.0.50.2, eth5, 00:34:04
R>* 10.0.40.0/24 [120/2] via 10.0.50.2, eth5, 02:15:26
C>* 10.0.50.0/24 is directly connected, eth5
C>* 10.0.60.0/24 is directly connected, eth6
```

```
C>* 127.0.0.0/8 is directly connected, lo
```

Из вывода видно, что маршруты к 10.0.20.0/24, 10.0.30.0/24 и 10.0.40.0/24 получены по RIP и что пакеты к этим сетям будут пересылаться наружу через eth5 на 10.0.50.2. Сети 10.0.50.0/24 и 10.0.60.0/24 подключены напрямую.

#### 11.1.1.2.2. R3: show ip rip

В результате выполнения команды **show ip rip** для R3 отображаются аналогичные сведения, но в другом формате, что представлено в примере 11.3.

*Пример 11.3 - Проверка RIP на R3: "show ip rip"*

```
admin@R3:~$ 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) 10.0.20.0/24   10.0.50.2 3    10.0.50.2 0    00:23
R(n) 10.0.30.0/24   10.0.50.2 3    10.0.50.2 0    00:23
R(n) 10.0.40.0/24   10.0.50.2 2    10.0.50.2 0    00:23
C(i) 10.0.50.0/24   0.0.0.0   1    self 0
C(r) 10.0.60.0/24   0.0.0.0   1 self (connected:1)     0
```

Из вывода видно, что сети 10.0.20.0/24, 10.0.30.0/24 и 10.0.40.0/24 получены по RIP и что пакеты к этим сетям будут направлены на 10.0.50.2. Сети 10.0.50.0/24 и 10.0.60.0/24 подключены напрямую.

### *11.1.1.3. Создание политики фильтрации маршрутов*

В этом разделе с помощью списков доступа выполняется настройка политики фильтрации маршрутов на R2 для отклонения входящих маршрутов от 10.0.20.0/24.

*Пример 11.4 - Настройка фильтрации маршрутов*

| Маршрутизатор | Действие | Команда (команды) |
|---|---|---|

| | | |
|---|---|---|
| R2 | Создание списка доступа и правила для отклонения указанных маршрутов. | admin@R2# **set policy access-list 100 rule 10 action deny**<br>[edit] |
| R2 | Соответствие любому получателю. | admin@R2# **set policy access-list 100 rule 10 destination any**<br>[edit] |
| R2 | Соответствие отправителю 10.0.20.0. | admin@R2# **set policy access-list 100 rule 10 source network 10.0.20.0**<br>[edit] |
| R2 | Указание маски сети в дополнительном коде. | admin@R2# **set policy access-list 100 rule 10 source inverse-mask 0.0.0.255**<br>[edit] |
| R2 | Создание правила для разрешения всех остальных маршрутов. | admin@R2# **set policy access-list 100 rule 20 action permit**<br>[edit] |
| R2 | Соответствие любому получателю. | admin@R2# **set policy access-list 100 rule 20 destination any**<br>[edit] |
| R2 | Соответствие любому отправителю. | admin@R2# **set policy access-list 100 rule 20 source any**<br>[edit] |
| R2 | Фиксация изменений. | admin@R2# **commit**<br>[edit] |
| R2 | Отображение настройки. | admin@R2# **show policy** |

```
access-list 100 {
     rule 10 {
          action deny
          destination {
               any
          }
          source {
               inverse-mask
0.0.0.255
               network
10.0.20.0
          }
     }
     rule 20 {
          action permit
          destination {
               any
          }
          source {
               any
          }
     }
}
[edit]
```

#### *11.1.1.4. Применение политики фильтрации маршрутов*

В этом разделе политика фильтрации маршрутов применяется ко входящим объявлениям RIP на R2.

*Пример 11.5 - Применение политики фильтрации маршрутов*

| Маршрутизатор | Действие | Команда (команды) |
|---|---|---|

| | | |
|---|---|---|
| R2 | Использование списка доступа, созданного в предыдущем примере, для фильтрации входящих объявлений о маршрутах. | admin@R2# **set protocols rip distribute-list access-list in 100**<br>[edit] |
| R2 | Фиксация настройки. | admin@R2# **commit**<br>[edit] |
| R2 | Отображение настройки. | admin@R2# **show protocols**<br>rip {<br>distribute-list {<br>access-list {<br>in 100<br>}<br>}<br>network 10.0.40.0/24<br>network 10.0.50.0/24<br>redistribute {<br>connected {<br>}<br>}<br>}<br>[edit] |

#### *11.1.1.5. Проверка настройки политики фильтрации маршрутов*

Для проверки настройки политики фильтрации маршрутов можно использовать следующие команды эксплуатационного режима.

##### 11.1.1.5.1. R3: show ip route

В примере 11.6 приведен вывод для команды **show ip route** для маршрутизатора R3.

*Пример 11.6 - Проверка изменений политики маршрутизации на R3: "show ip route"*

```
admin@R3:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O -
OSPF, I - ISIS, B - BGP, > - selected route, * - FIB route

R>* 10.0.30.0/24 [120/3] via 10.0.50.2, eth5, 00:45:21
R>* 10.0.40.0/24 [120/2] via 10.0.50.2, eth5, 00:45:21
C>* 10.0.50.0/24 is directly connected, eth5
C>* 10.0.60.0/24 is directly connected, eth6
C>* 127.0.0.0/8 is directly connected, lo
```

Из вывода видно, что маршруты к 10.0.30.0/24 и 10.0.40.0/24 получены по RIP и что пакеты к этим сетям будут пересылаться наружу через eth5 на 10.0.50.2. Сети 10.0.50.0/24 и 10.0.60.0/24 подключены напрямую. Обратите внимание, что маршрута к 10.0.20.0/24 нет, так как он был отфильтрован политикой маршрутизации.

#### 11.1.1.5.2. R3: show ip rip

В результате выполнения команды **show ip rip** для R3 отображаются аналогичные сведения, но в другом формате, что представлено в примере 11.7.

*Пример 11.7 - Проверка изменений политики маршрутизации на R3: "show ip rip"*

```
admin@R3:~$ 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) 10.0.30.0/24    10.0.50.2      3    10.0.50.2 0    00:22:00
R(n) 10.0.40.0/24    10.0.50.2      2    10.0.50.2 0    00:22:00
C(i) 10.0.50.0/24    0.0.0.0        1         self 0
C(i) 10.0.60.0/24    0.0.0.0   1    self 0
```

Из вывода видно, что сети 10.0.30.0/24 и 10.0.40.0/24 получены по RIP и что пакеты к этим сетям будут направлены на 10.0.50.2. Сети 10.0.50.0/24 и 10.0.60.0/24 подключены

напрямую. Отсутствует маршрут к 10.0.20.0/24.

## 11.1.2. Фильтрация входящих маршрутов с помощью списков префиксов

В данном разделе рассматриваются следующие вопросы:

- Настройка списка префиксов.
- Проверка входного фильтра.

### *11.1.2.1. Настройка списка префиксов*

Обычным требованием к настройкам BGP является фильтрация входящих объявлений маршрутов от равноправного узла BGP. В системе Altell NEO фильтрация такого рода выполняется при помощи политик маршрутизации, которые затем применяются к процессу BGP в качестве политик “импорта”. В данном примере для выполнения фильтрации применяются списки префиксов в сочетании с картами маршрутов.

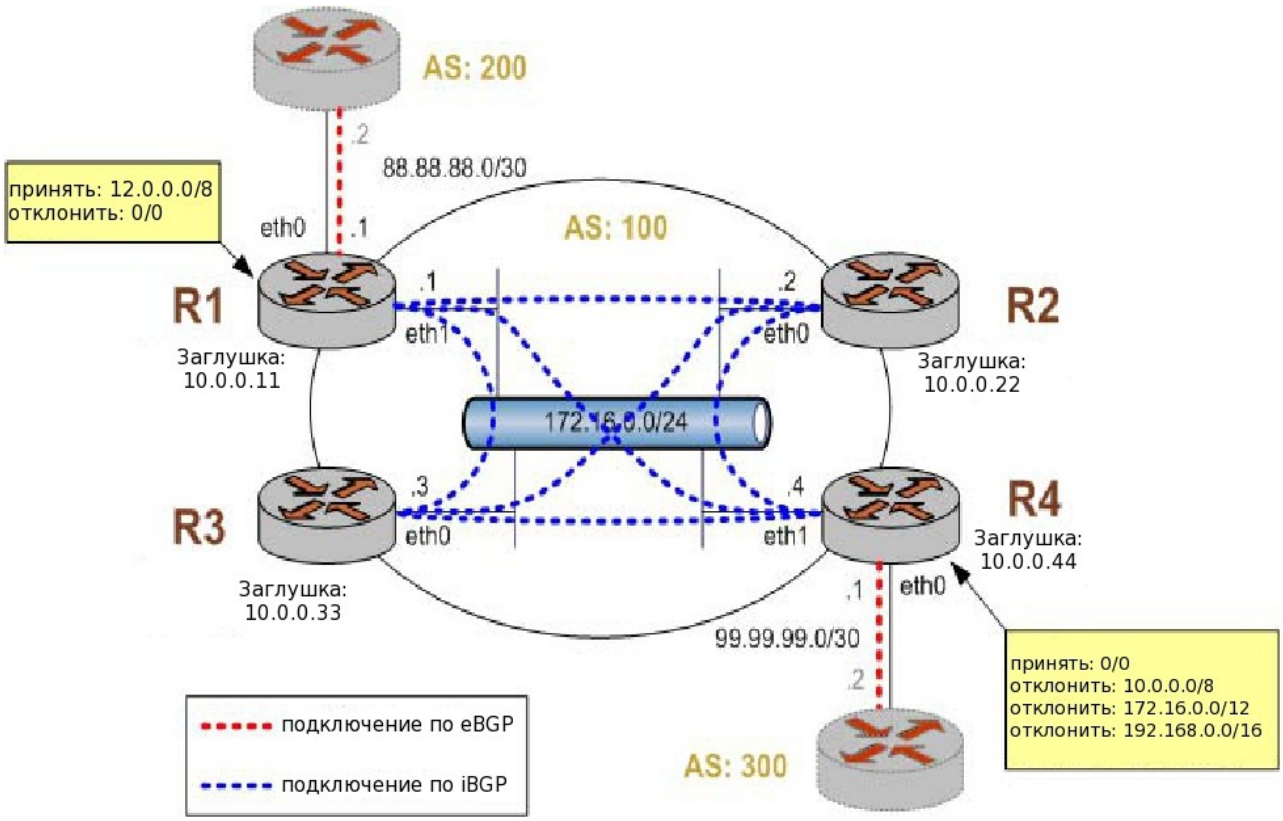
В примере 11.8 создаются следующие политики фильтрации на входе:

- R1 должен принимать только сеть 12.0.0.0/8 от его равноправного узла eBGP и отклонять всё остальное.
- R4 должен разрешать все маршруты Интернета, но отклонять все сети RFC 1918 от его равноправного узла eBGP.

Такая политика импорта показана на рис. 15.

*Принимается, что маршрутизаторы в AS100 настроены для iBGP и eBGP как изображено, а также что маршрутизаторы в AS200 и AS300 настроены соответственно как равноправные узлы eBGP.*

*Рисунок 15 - Фильтрация входящих маршрутов*




Для создания фильтра входящих маршрутов следует выполнить следующие действия в режиме настройки:

*Пример 11.8 - Создание политики импорта*

| Маршрутизатор | Действие | Команда (команды) |
|---|---|---|
| R1 | Создание списка префиксов, которые следует разрешить. В данном случае такой префикс только один - 12.0.0.0/8. | `admin@R1#` **`set policy prefix-list ALLOW-PREFIXES rule 1 action permit`**<br>`[edit]`<br>`admin@R1#` **`set policy prefix-list ALLOW-PREFIXES rule 1 prefix 12.0.0.0/8`**<br>`[edit]` |

| | | |
|---|---|---|
| R1 | Создание правила карты маршрутов для разрешения всех префиксов из списка. | admin@R1# **set policy route-map eBGP-IMPORT rule 10 action permit**<br>[edit]<br>admin@R1# **set policy route-map eBGP-IMPORT rule 10 match ip address prefix-list ALLOW-PREFIXES**<br>[edit] |
| R1 | Создание правила карты маршрутов для отклонения всех остальных префиксов. | admin@R1# **set policy route-map eBGP-IMPORT rule 20 action deny**<br>[edit] |
| R1 | Назначение созданной политики карты маршрутов политикой карты маршрутов импорта для AS 200. | admin@R1# **set protocols bgp 100 neighbor 88.88.88.2 route-map import eBGP-IMPORT**<br>[edit] |
| R1 | Фиксация настройки. | admin@R1# **commit**<br>[edit] |
| R1 | Сброс сеанса BGP с равноправным узлом для включения новых политик. | admin@R1# **run clear ip bgp 88.88.88.2**<br>[edit] |
| R1 | Отображение настройки политики. | admin@R1# **show policy**<br>prefix-list ALLOW-PREFIXES {<br>rule 1 {<br>action permit<br>prefix 12.0.0.0/8<br>}<br>}<br>route-map eBGP-IMPORT { |

```
        rule 10 {
            action permit
            match {
                ip {
                    address {

        prefix-list ALLOW-
PREFIXES
                    }
                }
            }
        }
        rule 20 {
            action deny
        }
}
[edit]
admin@R1#
```

R1 — Отображение настройки BGP для соседа eBGP с адресом 88.88.88.2.

```
admin@R1# show protocols bgp
100 neighbor 88.88.88.2
remote-as 200
route-map {
    import eBGP-IMPORT
}
[edit]
admin@R1#
```

R4 — Создание правила, которому будет соответствовать любой префикс от 10.0.0.0/8 до 32.

```
admin@R4# set policy prefix-
list RFC1918PREFIXES rule 1
action permit
[edit]
admin@R4# set policy prefix-
```

| | | |
|---|---|---|
| | | **list RFC1918PREFIXES rule 1 le 32**<br>[edit]<br>admin@R4# **set policy prefix-list RFC1918PREFIXES rule 1 prefix 10.0.0.0/8**<br>[edit] |
| R4 | Создание правила, которому будет соответствовать любой префикс от 172.16.0.0/12 до 32. | admin@R4# **set policy prefix-list RFC1918PREFIXES rule 2 action permit**<br>[edit]<br>admin@R4# **set policy prefix-list RFC1918PREFIXES rule 2 le 32**<br>[edit]<br>admin@R4# **set policy prefix-list RFC1918PREFIXES rule 2 prefix 172.16.0.0/12**<br>[edit] |
| R4 | Создание правила, которому будет соответствовать любой префикс от 192.168.0.0/16 до 32. | admin@R4# **set policy prefix-list RFC1918PREFIXES rule 3 action permit**<br>[edit]<br>admin@R4# **set policy prefix-list RFC1918PREFIXES rule 3 le 32**<br>[edit]<br>admin@R4# **set policy prefix-list RFC1918PREFIXES rule 3 prefix 192.168.0.0/16**<br>[edit] |

| | | |
|---|---|---|
| R4 | Создание правила карты маршрутов для отклонения всех префиксов из списка. | admin@R4# **set policy route-map eBGP-IMPORT rule 10 action deny**<br>[edit]<br>admin@R4# **set policy route-map eBGP-IMPORT rule 10 match ip address prefix-list RFC1918PREFIXES**<br>[edit] |
| R4 | Создание правила карты маршрутов для разрешения всех остальных префиксов. | admin@R4# **set policy route-map eBGP-IMPORT rule 20 action permit**<br>[edit] |
| R4 | Назначение созданной политики карты маршрутов политикой карты маршрутов импорта для AS 300. | admin@R4# **set protocols bgp 100 neighbor 99.99.99.2 route-map import eBGP-IMPORT**<br>[edit] |
| R4 | Фиксация настройки. | admin@R4# **commit**<br>[edit] |
| R4 | Сброс сеанса BGP с равноправным узлом для включения новых политик. | admin@R1# **run clear ip bgp 99.99.99.2**<br>[edit] |
| R4 | Отображение настройки политики. | admin@R4# **show policy**<br>prefix-list RFC1918PREFIXES {<br>rule 1 {<br>action permit le 32<br>prefix 10.0.0.0/8<br>}<br>rule 2 {<br>action permit le 32 |

```
          prefix
172.16.0.0/12
     }
     rule 3 {
          action permit le 32
          prefix
192.168.0.0/16
     }
}
route-map eBGP-IMPORT {
     rule 10 {
          action deny
          match {
               ip {
                    address {

     prefix-list
RFC1918PREFIXES
                    }
               }
          }
     }
     rule 20 {
          action permit
     }
}
[edit]
admin@R4#
```

| | | |
|---|---|---|
| R4 | Отображение настройки BGP для соседа eBGP с адресом 99.99.99.2. | admin@R4# **show protocols bgp 100 neighbor 99.99.99.2**<br>remote-as 300 |

```
route-map {
     import eBGP-IMPORT
} [edit]
admin@R4#
```

#### *11.1.2.2. Проверка входного фильтра*

Для проверки настройки входного фильтра можно использовать следующие команды.

##### 11.1.2.2.1. R1: show ip bgp

В примере 11.9 приведена таблица BGP маршрутизатора R1 перед применением фильтра импорта.

*Пример 11.9 - Входящие маршруты BGP на R1 до фильтрации при импорте*

```
admin@R1:~$ show ip bgp
BGP table version is 0, local router ID is 10.0.0.11
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

Network   Next Hop  Metric LocPrf Weight Path
*> 2.0.0.0/24       88.88.88.2     0         0    200  i
*> 2.1.0.0/24       88.88.88.2     0         0    200  i
*> 2.2.0.0/24       88.88.88.2     0         0    200  i
*>i3.0.0.0/24       99.99.99.2     0    100  0    300  i
*>i3.1.0.0/24       99.99.99.2     0    100  0    300  i
*>i3.2.0.0/24       99.99.99.2     0    100  0    300  i
*> 12.0.0.0         88.88.88.2     0         0    200  i
*>i13.0.0.0/24      99.99.99.2     0    100  0    300  i
*> 88.88.88.0/30    88.88.88.2     0         0    200  i
*>i99.99.99.0/30    99.99.99.2     0    100  0    300  i
*> 172.16.0.0/24    0.0.0.0        1         32768     i
```

```
* i  10.0.0.44 1    100  0         i
*>i172.16.128.0/24  99.99.99.2     0    100  0    300  i
*>i192.168.2.0      99.99.99.2     0    100  0    300  i

Total number of prefixes 13
```

#### 11.1.2.2.2. R1: show ip bgp

В примере 11.10 приведена таблица BGP маршрутизатора R1 после применения фильтра импорта.

*Пример 11.10 - Входящие маршруты BGP на R1 после фильтрации при импорте*

```
admin@R1:~$ show ip bgp

BGP table version is 0, local router ID is 10.0.0.11
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

Network   Next Hop  Metric LocPrf Weight Path
*>i3.0.0.0/24       99.99.99.2     0    100  0    300  i
*>i3.1.0.0/24       99.99.99.2     0    100  0    300  i
*>i3.2.0.0/24       99.99.99.2     0    100  0    300  i
*> 12.0.0.0         88.88.88.2     0         0    200  i
*>i13.0.0.0/24      99.99.99.2     0    100  0    300  i
*>i99.99.99.0/30    99.99.99.2     0    100  0    300  i
*> 172.16.0.0/24    0.0.0.0   1         32768     i
* i  10.0.0.44 1    100  0    i
*>i172.16.128.0/24  99.99.99.2     0    100  0    300  i
*>i192.168.2.0      99.99.99.2     0    100  0    300  i
Total number of prefixes 9
```

Следует обратить внимание, что в таблице остался только элемент 12.0.0.0 от 88.88.88.2.

#### 11.1.2.2.3. R4: show ip bgp

В примере 11.11 приведена таблица BGP маршрутизатора R4 перед применением фильтра импорта.

*Пример 11.11 - Входящие маршруты BGP на R4 до фильтрации при импорте*

```
admin@R4:~$ show ip bgp
BGP table version is 0, local router ID is 10.0.0.44
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

Network   Next Hop  Metric LocPrf Weight Path
*> 3.0.0.0/24       99.99.99.2     0         0    300  i
*> 3.1.0.0/24       99.99.99.2     0         0    300  i
*> 3.2.0.0/24       99.99.99.2     0         0    300  i
*>i12.0.0.0         88.88.88.2     0    100  0    200  i
*> 13.0.0.0/24      99.99.99.2     0         0    300  i
*> 99.99.99.0/30    99.99.99.2     0         0    300  i
* i172.16.0.0/24    10.0.0.11 1    100  0    i
*>   0.0.0.0   1         32768     i
*> 172.16.128.0/24  99.99.99.2     0         0    300  i
*> 192.168.2.0 99.99.99.2     0         0    300  i

Total number of prefixes 9
```

#### 11.1.2.2.4. R4: show ip bgp

Ниже приведена таблица BGP маршрутизатора R4 после применения фильтра импорта.

*Пример 11.12 - Входящие маршруты BGP на R4 после фильтрации при импорте*

```
admin@R4:~$ show ip bgp
BGP table version is 0, local router ID is 10.0.0.44
Status codes: s suppressed, d damped, h history, * valid, > best,
```

```
i - internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

Network   Next Hop  Metric LocPrf Weight Path
*> 3.0.0.0/24  99.99.99.2     0         0    300  i
*> 3.1.0.0/24  99.99.99.2     0         0    300  i
*> 3.2.0.0/24  99.99.99.2     0         0    300  i
*>i12.0.0.0    88.88.88.2     0    100  0    200  i
*> 13.0.0.0/24 99.99.99.2     0         0    300  i
*> 99.99.99.0/30    99.99.99.2     0         0    300  i
* i172.16.0.0/24    10.0.0.11 1    100  0    i
*>   0.0.0.0   1         32768     i

Total number of prefixes 7
```

## 11.1.3. Фильтрация исходящих маршрутов с помощью списков путей автономных систем

В этом разделе рассматриваются следующие вопросы:

- Настройка AS-path-list.
- Проверка исходящего фильтра.

### *11.1.3.1. Настройка AS-path-list*

Ещё одно обычное требование к настройке BGP — фильтрация исходящих префиксов. В системе Altell NEO фильтрация такого рода выполняется при помощи политик маршрутизации, которые затем применяются к процессу BGP в качестве политик “экспорта”.

В примере, приведенном в данном разделе, предполагается, что системе AS100 не нужно быть транзитной автономной системой для AS 200 или AS 300, что означает следующее:

- Маршруты eBGP от равноправного узла eBGP маршрутизатора R1 (AS 200) не следует отправлять на равноправный узел eBGP маршрутизатора R4.
- Маршруты с равноправного узла eBGP маршрутизатора R4 (AS 300) не следует отправлять на равноправный узел eBGP маршрутизатора R1.

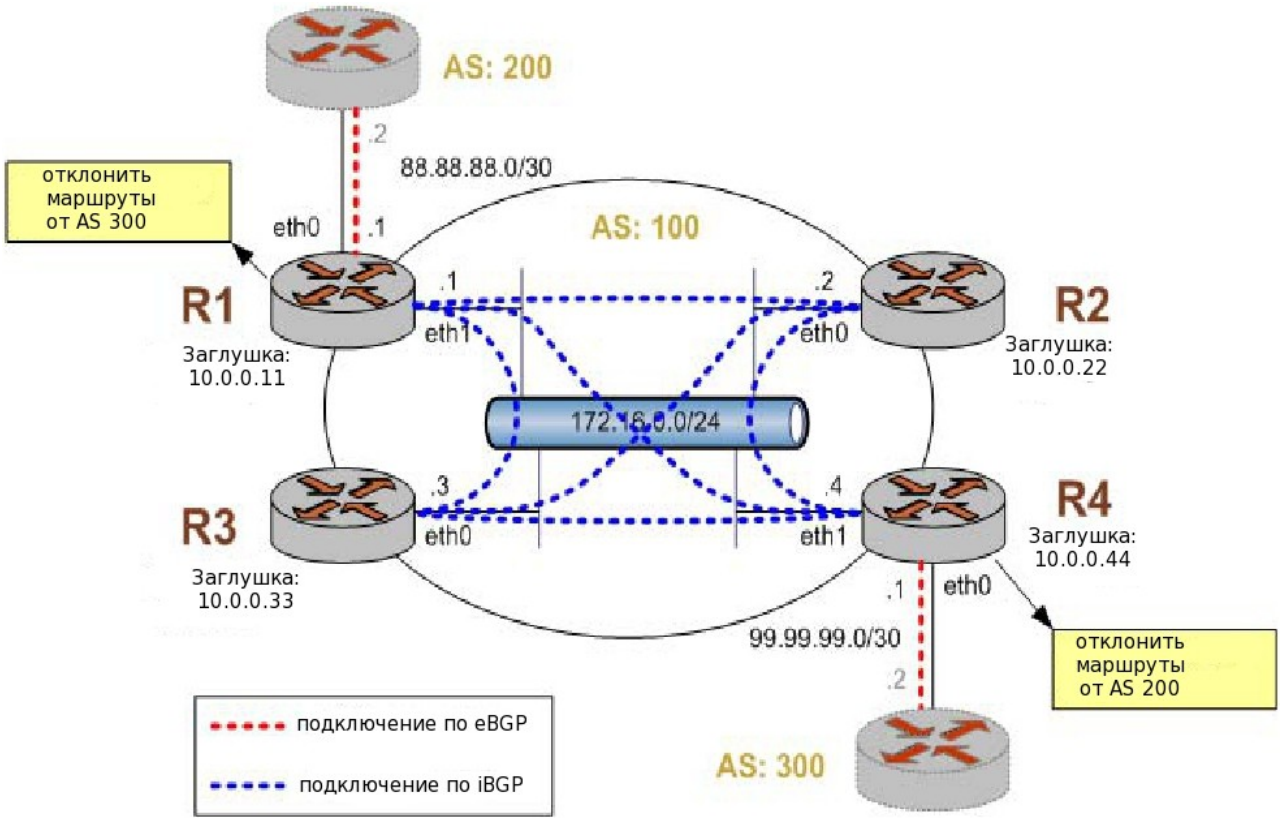
Если бы такая фильтрация *не была реализована*, то AS 300 мог бы отправлять трафик, предназначенный для AS 200, на маршрутизатор R4, и указанный трафик передавался бы через сеть AS 100.

Есть несколько способов реализации такой политики маршрутизации: два наиболее распространенных заключаются в фильтрации на основе префиксов сети или на основе пути автономной системы. В данном примере существующая политика экспорта BGP обновляется с добавлением дополнительных ограничений, которые не дадут AS 100 возможности выступать в качестве транзитной сети для AS 200 и AS 300.

Описанная политика экспорта показана на рисунке 16.

Принимается, что маршрутизаторы в AS100 настроены для iBGP и eBGP как изображено и что маршрутизаторы в AS200 и AS300 настроены соответственно как равноправные узлы eBGP.

*Рисунок 16 - Фильтрация исходящих маршрутов*




Для создания такой политики экспорта следует выполнить следующие действия в режиме настройки:

*Пример 11.13 - Создание политики экспорта*

| Маршрутизатор | Действие | Команда (команды) |
|---|---|---|
| R1 | Создание списка путей AS, которые следует отклонить. В данном случае такой только один - AS300. | admin@R1# **set policy as-path-list AS300 rule 1 action permit**<br>[edit]<br>admin@R1# **set policy as-path-list AS300 rule 1 regex 300**<br>[edit] |
| R1 | Создание правила карты маршрутов для отклонения всех путей AS из списка. | admin@R1# **set policy route-map eBGP-EXPORT rule 10 action deny**<br>[edit]<br>admin@R1# **set policy route-map eBGP-EXPORT rule 10 match as-path AS300**<br>[edit] |
| R1 | Создание правила карты маршрутов для разрешения всех остальных префиксов. | admin@R1# **set policy route-map eBGP-EXPORT rule 20 action permit**<br>[edit] |
| R1 | Назначение созданной политики карты маршрутов политикой карты маршрутов экспорта для AS 200. | admin@R1# **set protocols bgp 100 neighbor 88.88.88.2 route-map export eBGP-EXPORT**<br>[edit] |
| R1 | Фиксация настройки. | admin@R1# **commit**<br>[edit] |
| R1 | Сброс сеанса BGP с | admin@R1# **run clear ip bgp** |

| | | |
|---|---|---|
| | равноправным узлом для включения новых политик. | **88.88.88.2**<br>[edit] |
| R1 | Отображение настроек политик. | admin@R1# **show policy as-path-list AS300**<br>rule 1 {<br>action permit<br>regex 300<br>}<br>[edit]<br>admin@R1# **show policy route-map eBGP-EXPORT**<br>rule 10 {<br>action deny<br>match {<br>as-path AS300}<br>}<br>}<br>rule 20 {<br>action permit<br>}<br>[edit] |
| R1 | Отображение настройки BGP для соседа eBGP с адресом 88.88.88.2. | admin@R1# **show protocols bgp 100 neighbor 88.88.88.2**<br>remote-as 200<br>route-map {<br>export eBGP-EXPORT<br>import eBGP-IMPORT<br>}<br>[edit] |
| R4 | Создание списка путей AS, которые следует отклонить. В | admin@R4# **set policy as-path-list AS200 rule 1 action** |

| | | |
|---|---|---|
| | данном случае такая AS только одна - AS200. | **permit**<br>[edit]<br>admin@R4# **set policy as-path-list AS200 rule 1 regex 200**<br>[edit] |
| R4 | Создание правила карты маршрутов для отклонения всех путей AS из списка. | admin@R4# **set policy route-map eBGP-EXPORT rule 10 action deny**<br>[edit]<br>admin@R4# **set policy route-map eBGP-EXPORT rule 10 match as-path AS200**<br>[edit] |
| R4 | Создание правила карты маршрутов для разрешения всех остальных префиксов. | admin@R4# **set policy route-map eBGP-EXPORT rule 20 action permit**<br>[edit] |
| R4 | Назначение созданной политики карты маршрутов политикой карты маршрутов экспорта для AS 300. | admin@R4# **set protocols bgp 100 neighbor 99.99.99.2 route-map export eBGP-EXPORT**<br>[edit] |
| R4 | Фиксация настройки. | admin@R4# **commit**<br>[edit] |
| R4 | Сброс сеанса BGP с равноправным узлом для включения новых политик. | admin@R4# **run clear ip bgp 99.99.99.2**<br>[edit] |
| R4 | Отображение настроек политик. | admin@R4# **show policy as-path-list AS200**<br>rule 1 { |

```
        action permit
        regex 200
}
[edit]
admin@R4# show policy route-
map eBGP-EXPORT
rule 10 {
        action deny
        match {
                as-path AS200}
        }
}
rule 20 {
        action permit
}
[edit]
admin@R4#
```

R4 — Отображение настройки BGP для соседа eBGP с адресом 99.99.99.2.

```
admin@R4# show protocols bgp
100 neighbor 99.99.99.2
remote-as 300 route-map {
        export eBGP-EXPORT
        import eBGP-IMPORT
}
[edit]
admin@R4#
```

#### *11.1.3.2. Проверка исходящего фильтра*

Для проверки настройки исходящего фильтра можно использовать следующие команды.

##### 11.1.3.2.1. AS 200: show ip bgp

В примере 11.14 приведена таблица BGP системы AS 200 *до* применения фильтра

экспорта.

*Пример 11.14 - Исходящие маршруты BGP на AS 200 до фильтрации при экспорте*

```
admin@AS200:~$ show ip bgp
BGP table version is 0, local router ID is 10.0.11.11
Status codes: s suppressed, d damped, h history, * valid, >
best, i - internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network   Next Hop  Metric    LocPrf    Weight    Path
*>   2.0.0.0/24     0.0.0.0   0         32768     i
*>   2.1.0.0/24     0.0.0.0   0         32768     i
*>   2.2.0.0/24     0.0.0.0   0         32768     i
*>   3.0.0.0/24     88.88.88.1              0    100  300  i
*>   3.1.0.0/24     88.88.88.1              0    100  300  i
*>   3.2.0.0/24     88.88.88.1              0    100  300  i
*>   12.0.0.0  0.0.0.0   0         32768     i
*>   13.0.0.0/24    88.88.88.1              0    100  300  i
*>   88.88.88.0/30  0.0.0.0   0         32768     i
*>   99.99.99.0/30  88.88.88.1              0    100  300  i
*>   172.16.0.0/24  88.88.88.1     1        0    100  i

Total number of prefixes 11
```

#### 11.1.3.2.2. AS 200: show ip bgp

В примере 11.15 приведена таблица BGP системы AS 200 *после* применения фильтра экспорта.

*Пример 11.15 - Исходящие маршруты BGP на AS 200 после фильтрации при экспорте*

```
admin@AS200:~$ show ip bgp
BGP table version is 0, local router ID is 10.0.11.11
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal, r RIB-failure, S Stale, R Removed
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network   Next Hop  Metric    LocPrf    Weight    Path
*>   2.0.0.0/24     0.0.0.0   0         32768     i
*>   2.1.0.0/24     0.0.0.0   0         32768     i
*>   2.2.0.0/24     0.0.0.0   0         32768     i
*>   12.0.0.0  0.0.0.0   0         32768     i
*>   88.88.88.0/30  0.0.0.0   0         32768     i
*>   172.16.0.0/24  88.88.88.1     1         0    100 i

Total number of prefixes 6
```

## 11.2. Команды политик маршрутизации

В данном разделе описаны команды политик маршрутизации системы Altell NEO.

| 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` | 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 списка доступа. |
| `policy access-list <номер_списка> rule <номер_правила> destination` | Определение критерия соответствия для правила списка доступа на основе получателя. |
| `policy access-list <номер_списка> rule <номер_правила> source` | Определение критериев соответствия для правила списка доступа на основе отправителя. |
| Списки доступа IPv6 | |
| `policy access-list6 <номер_списка>` | Определение списка доступа IPv6. |
| `policy access-list6 <номер_списка> description <описание>` | Ввод краткого описания для списка доступа IPv6. |
| `policy access-list6 <номер_списка> rule <номер_правила>` | Создание правила для списка доступа IPv6. |
| `policy access-list6 <номер_списка> rule <номер_правила> action` | Указание действия, которое должно быть выполнено для пакетов, соответствующих правилу списка доступа IPv6. |
| `policy access-list6 <номер_списка> rule <номер_правила> description <описание>` | Ввод краткого описания для правила списка доступа IPv6. |

| | |
|---|---|
| `policy access-list6 <номер_списка> rule <номер_правила> destination` | Определение критерия соответствия в правиле списка доступа IPv6 на основе получателя. |
| `policy access-list6 <номер_списка> rule <номер_правила> source` | 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` | 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 <рег_выр>` | 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` | 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 <рег_выр>` | 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 | 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` | 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 для 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` | Указание действия, которое должно быть выполнено для пакетов, соответствующих правилу карты маршрутов. |
| `policy route-map <имя_карты> rule <номер_правила> call <цель>` | Вызов другой карты маршрутов. |
| `policy route-map <имя_карты> rule <номер_правила> continue <номер_цели>` | 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 <ethx>` | Определение условия соответствия для карты маршрутов на основе интерфейса первого транзитного участка. |
| `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 участка. |
| `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 участка. |
| `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` | Определение условия соответствия для карты маршрутов на основе способа получения маршрута. |
| `policy route-map <имя_карты> rule <номер_правила> match peer <ipv4-адрес>` | 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. |

| | |
|---|---|
| `policy 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 участка 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` | 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 | |
| `show ip access-list` | Отображение всех списков доступа IP. |
| `show ip as-path-access-list` | Отображение всех списков доступа по путям AS. |
| `show ip community-list` | Отображение всех списков сообществ IP. |
| `show ip extcommunity-list` | Отображение всех расширенных списков сообществ IP. |
| `show ip prefix-list` | Отображение списков префиксов IP. |
| `show ip protocol` | Отображение карт маршрутов IP по протоколам. |
| `show route-map` | Отображение сведений карты маршрутов. |

### 11.2.1. 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 целоебеззнака32разр {}
}
```

**Параметры**

*номер_списка*

Множественный узел. Численный идентификатор списка доступа. Номера списков доступа могут принимать следующие значения:

- от 1 до 99: стандартный список доступа IP;
- от 100 до 199: расширенный список доступа IP;
- от 1300 от 1999: стандартный список доступа IP (расширенный диапазон);
- от 2000 до 2699: расширенный список доступа IP (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.

## 11.2.2. 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 целоебеззнака32разр {
        description текст
    }
}
```

**Параметры**

*номер_списка*

Номер определенного 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.

### 11.2.3. 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 целоебеззнака32разр {
        rule целоебеззнака32разр {}
    }
}
```

**Параметры**

*номер_списка*

Номер определенного списка доступа.

*номер_правила*

Множественный узел. Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 4294967295. Можно определить несколько правил, создав несколько узлов конфигурации **rule**.

**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.

## 11.2.4. policy access-list <номер_списка> rule <номер_правила> action

Указание действия, которое должно быть выполнено для пакетов, соответствующих правилу списка доступа.

**Синтаксис**

**set policy access-list** *номер_списка* **rule** *номер_правила* **action** {**deny** | **permit**}

**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 целоебеззнака32разр {
        rule целоебеззнака32разр {
            action {
                deny
                permit
            }
        }
    }
}
```

**Параметры**

*номер_списка*

Номер определенного списка доступа.

*номер_правила*

Номер определенного правила списка 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, пересылаются.

**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.

### 11.2.5. policy access-list <номер_списка> rule <номер_правила> description <описание>

Ввод краткого описания правила списка 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 целоебеззнака32разр {
        rule целоебеззнака32разр {
            description текст
        }
    }
}
```

**Параметры**

*номер_списка*

Номер определенного списка доступа.

*номер_правила*

Номер определенного правила списка доступа.

*описание*

Краткое текстовое описание для 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.

## 11.2.6. policy access-list <номер_списка> rule <номер_правила> destination

Определение критерия соответствия в правиле списка доступа на основе получателя.

**Синтаксис**

**set policy access-list** *номер_списка* **rule** *номер_правила* **destination** {**any** | **host** *ipv4-адрес* | **inverse-mask** *ipv4-адрес* | **network** *подсеть_ipv4*}

**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 целоебеззнака32разр {
        rule целоебеззнака32разр {
            destination {
                any
                host ipv4-адрес
                inverse-mask ipv4-адрес
                network подсеть_ipv4
            }
```

```
            }
        }
    }
```

**Параметры**

*номер_списка*

Номер определенного списка доступа.

*номер_правила*

Номер определенного списка доступа.

**any**

Соответствие для пакетов, предназначенных любому получателю. В команде обязательно должен присутствовать ровно один параметр из списка any, host, inverse-mask и network.

**host** *ipv4-адрес*

Соответствие для пакетов, предназначенных указанному узлу IPv4. В команде обязательно должен присутствовать ровно один параметр из списка **any**, **host**, **inverse-mask** и **network**.

**inverse-mask** *ipv4-адрес*

Соответствие для пакетов, предназначенных для подсети, указанной маской. В команде обязательно должен присутствовать ровно один параметр из списка **any**, **host**, **inverse-mask** и **network**.

**network** *подсеть_ipv4*

Соответствие для пакетов, предназначенных указанной подсети. Используется формат *ip-адрес/префикс*. В команде обязательно должен присутствовать ровно один параметр из списка **any**, **host**, **inverse-mask** и **network**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

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. Если не указано

никаких критериев соответствия, то фильтрация пакетов по получателю происходить не будет; это значит, что разрешены пакеты для всех получателей.

Форма **show** этой команды используется для отображения параметров настройки фильтрации пакетов по получателю с помощью правил списка доступа.

### 11.2.7. policy access-list <номер_списка> rule <номер_правила> source

Определение критериев соответствия в правиле списка доступа на основе отправителя.

**Синтаксис**

**set policy access-list** *номер_списка* **rule** *номер_правила* **source** {**any** | **host** *ipv4-адрес* | **inverse-mask** *ipv4-адрес* | **network** *подсеть_ipv4*}

**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 целоебеззнака32разр {
        rule целоебеззнака32разр {
            source {
                any
                host ipv4-адрес
                inverse-mask ipv4-адрес
                network подсеть_ipv4
            }
        }
    }
}
```

**Параметры**

*номер_списка*

Номер определенного списка доступа.

*номер_правила*

Номер определенного правила списка доступа.

**any**

Соответствие для пакетов, приходящих от любого отправителя. В команде обязательно должен присутствовать ровно один параметр из списка **any**, **host**, **inverse-mask** и **network**.

**host** *ipv4-адрес*

Соответствие для пакетов, приходящих от указанного узла IPv4. В команде обязательно должен присутствовать ровно один параметр из списка **any**, **host**, **inverse-mask** и **network**.

**inverse-mask** *ipv4-адрес*

Соответствие для пакетов, приходящих от подсети, указанной маской. В команде обязательно должен присутствовать ровно один параметр из списка **any**, **host**, **inverse-mask** и **network**.

**network** *подсеть_ipv4*

Соответствие для пакетов, приходящих от указанной подсети. Используется формат *ip-адрес/префикс*. В команде обязательно должен присутствовать ровно один параметр из списка **any**, **host**, **inverse-mask** и **network**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

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. Если не указано никаких критериев соответствия, то фильтрация пакетов по получателю происходить не будет; это значит, что разрешены пакеты ото всех отправителей.

Форма **show** этой команды используется для отображения параметров

настройки фильтрации пакетов по отправителю с помощью правил списка доступа.

### 11.2.8. policy access-list6 <номер_списка>

Определение списка доступа IPv6.

**Синтаксис**

**set policy access-list6** *номер_списка*

**delete policy access-list6** *номер_списка*

**show policy access-list6** *номер_списка*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
policy {
    access-list6 целоебеззнака32разр {}
}
```

**Параметры**

*номер_списка*

Множественный узел. Численный идентификатор списка доступа IPv6. Номера списков доступа могут принимать следующие значения:

- от 1 до 99: стандартный список доступа IP;
- от 100 до 199: расширенный список доступа IP;
- от 1300 от 1999: стандартный список доступа IP (расширенный диапазон);
- от 2000 до 2699: расширенный список доступа IP (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.

### 11.2.9. policy access-list6 <номер_списка> description <описание>

Ввод краткого описания списка доступа IPv6.

**Синтаксис**

**set policy access-list6** *номер_списка* **description** *описание*

**delete policy access-list6** *номер_списка* **description**

**show policy access-list6** *номер_списка* **description**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
policy {
    access-list6 целоебеззнака32разр {
        description текст
    }
}
```

**Параметры**

*номер_списка*

Номер определенного списка доступа IPv6.

*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.

### 11.2.10. policy access-list6 <номер_списка> rule <номер_правила>

Создание правила списка доступа IPv6.

**Синтаксис**

**set policy access-list6** *номер_списка* **rule** *номер_правила*

**delete policy access-list6** *номер_списка* **rule** *номер_правила*

**show policy access-list6** *номер_списка* **rule** *номер_правила*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
policy {
    access-list6 целоебеззнака32разр {
        rule целоебеззнака32разр {}
    }
}
```

**Параметры**

**номер_списка**

Номер определенного списка доступа IPv6.

**номер_правила**

Множественный узел. Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 65535. Можно определить несколько правил, создав несколько узлов конфигурации **rule**.

**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.

## 11.2.11. policy access-list6 <номер_списка> rule <номер_правила> action

Указание действия, которое должно быть выполнено для пакетов, соответствующих правилу списка доступа IPv6.

**Синтаксис**

**set policy access-list6** *номер_списка* **rule** *номер_правила* **action** {**deny** | **permit**}

**delete policy access-list6** *номер_списка* **rule** *номер_правила* **action**

**show policy access-list6** *номер_списка* **rule** *номер_правила* **action**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
policy {
    access-list6 целоебеззнака32разр {
        rule целоебеззнака32разр {
            action {
                deny
                permit
            }
        }
    }
}
```

**Параметры**

*номер_списка*

Номер определенного списка доступа IPv6.

*номер_правила*

Номер определенного правила списка 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, пересылаются.

**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.

## 11.2.12. policy access-list6 <номер_списка> rule <номер_правила> description <описание>

Ввод краткого описания правила списка доступа IPv6.

**Синтаксис**

**set policy access-list6** *номер_списка* **rule** *номер_правила* **description** *описание*

**delete policy access-list6** *номер_списка* **rule** *номер_правила* **description**

**show policy access-list6** *номер_списка* **rule** *номер_правила* **description**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
policy {
    access-list6 целоебеззнака32разр {
        rule целоебеззнака32разр {
            description текст
        }
    }
}
```

**Параметры**

*номер_списка*

Номер определенного списка доступа IPv6.

*номер_правила*

Номер определенного правила списка доступа.

*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.

## 11.2.13. policy access-list6 <номер_списка> rule <номер_правила> destination

Определение критерия соответствия в правиле списка доступа IPv6 на основе получателя.

**Синтаксис**

**set policy access-list6** *номер_списка* **rule** *номер_правила* **destination** {**any** | **host** ipv6-адрес | **inverse-mask** *ipv6-адрес* | **network** *подсеть_ipv6*}

**delete policy access-list6** *номер_списка* **rule** *номер_правила* **destination**

**show policy access-list6** *номер_списка* **rule** *номер_правила* **destination**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
policy {
    access-list6 целоебеззнака32разр {
```

```
                rule целоебеззнака32разр {
                     destination {
                          any
                          host ipv6-адрес
                          inverse-mask ipv6-адрес
                          network подсеть_ipv6
                     }
                }
           }
      }
```

**Параметры**

*номер_списка*

Номер определенного списка доступа IPv6.

*номер_правила*

Номер определенного списка доступа IPv6.

**any**

Соответствие для пакетов, предназначенных любому получателю. В команде обязательно должен присутствовать ровно один параметр из списка **any**, **host**, **inverse-mask** и **network**.

**host** *ipv6-адрес*

Соответствие для пакетов, предназначенных указанному узлу IPv6. В команде обязательно должен присутствовать ровно один параметр из списка **any**, **host**, **inverse-mask** и **network**.

**inverse-mask** *ipv6-адрес*

Соответствие для пакетов, предназначенных для подсети, указанной маской. В команде обязательно должен присутствовать ровно один параметр из списка **any**, **host**, **inverse-mask** и **network**.

**network** *подсеть_ipv6*

Соответствие для пакетов, предназначенных указанной подсети. Используется формат *ipv6-адрес/префикс*. В команде обязательно должен присутствовать ровно один параметр из списка **any**, **host**, **inverse-mask** и

**network**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

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. Если не указано никаких критериев соответствия, то фильтрация пакетов по получателю происходить не будет; это значит, что разрешены пакеты для всех получателей.

Форма **show** этой команды используется для отображения параметров настройки фильтрации пакетов по получателю с помощью правил списка доступа.

## 11.2.14. policy access-list6 <номер_списка> rule <номер_правила> source

Определение критериев соответствия в правиле списка доступа IPv6 на основе отправителя.

**Синтаксис**

**set policy access-list6** *номер_списка* **rule** *номер_правила* **source** {**any** | **exact-match** | **network** *подсеть_ipv6*}

**delete policy access-list6** *номер_списка* **rule** *номер_правила* **source**

**show policy access-list6** *номер_списка* **rule** *номер_правила* **source**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
policy {
    access-list6 целоебеззнака32разр {
        rule целоебеззнака32разр {
            source {
                any
```

```
                    exact-match
                    network подсеть_ipv6
                }
            }
        }
    }
```

**Параметры**

*номер_списка*

Номер определенного списка доступа IPv6.

*номер_правила*

Номер определенного правила списка доступа IPv6.

**any**

Соответствие для пакетов, приходящих от любого отправителя. В команде обязательно должен присутствовать ровно один параметр из списка **any**, **exact-match** и **network**.

**exact-match**

Соответствие для пакетов, приходящих от одного из префиксов подсетей. В команде обязательно должен присутствовать ровно один параметр из списка **any**, **exact-match** и **network**.

**network** *подсеть_ipv6*

Соответствие для пакетов, приходящих от указанной подсети. Используется формат *ipv6-адрес/префикс*. В команде обязательно должен присутствовать ровно один параметр из списка **any**, **exact-match** и **network**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

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. Если не указано никаких критериев соответствия, то фильтрация пакетов по получателю

происходить не будет; это значит, что разрешены пакеты ото всех отправителей.

Форма **show** этой команды используется для отображения параметров настройки фильтрации пакетов по отправителю с помощью правил списка доступа.

### 11.2.15. 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.

## 11.2.16. 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**

Имя определенного 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.

## 11.2.17. 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 целоебеззнака32разр {}
    }
}
```

**Параметры**

*имя_списка*

Имя определенного списка путей AS.

*номер_правила*

Множественный узел. Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 4294967295. Можно определить несколько правил, создав несколько узлов конфигурации **rule**.

**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.

## 11.2.18. policy as-path-list <имя_списка> rule <номер_правила> action

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** {**deny** | **permit**}

**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 целоебеззнака32разр {
            action {
                deny
                permit
            }
        }
    }
}
```

**Параметры**

*имя_списка*

Имя определенного списка путей AS.

*номер_правила*

Номер определенного правила списка путей AS.

**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, пересылаются.

**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 выполняется маршрутизация по получателю, то есть пакеты отправляются по обычным каналам пересылки.

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.

## 11.2.19. 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 целоебеззнака32разр {
            description текст
        }
    }
```

```
}
```

**Параметры**

*имя_списка*

Имя определенного списка путей AS.

*номер_правила*

Номер определенного правила списка путей AS.

*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.

## 11.2.20. policy as-path-list <имя_списка> rule <номер_правила> regex <рег_выр>

Определение критериев соответствия в правиле списка путей AS на основе регулярного выражения.

**Синтаксис**

**set policy as-path-list** *имя_списка* **rule** *номер_правила* **regex** *рег_выр*

**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 целоебеззнака32разр {
                regex текст
            }
        }
    }
```

**Параметры**

*имя_списка*

Имя определенного списка путей AS.

*номер_правила*

Номер определенного правила списка путей AS.

*рег_выр*

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**

Форма **set** этой команды используется для определения критериев соответствия, которые будут использоваться при определении политики пересылки на основе путей AS.

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** (см. стр. 645), соответствующие пакеты либо разрешаются, либо отклоняются.

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.

## 11.2.21. 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 целоебеззнака32разр {}
}
```

**Параметры**

*номер_списка*

Множественный узел. Численный идентификатор списка сообщества. Можно создать несколько списков сообщества, создав несколько узлов конфигурации **policy community-list**.

**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.

## 11.2.22. 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 целоебеззнака32разр {
        description текст
    }
}
```

**Параметры**

*номер_списка*

Номер определенного 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.

## 11.2.23. 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 целоебеззнака32разр {
        rule целоебеззнака32разр {}
    }
}
```

**Параметры**

*номер_списка*

Номер определенного списка сообщества.

*номер_правила*

Множественный узел. Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 4294967295. Можно определить несколько правил, создав несколько узлов конфигурации **rule**.

**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.

## 11.2.24. policy community-list <номер_списка> rule <номер_правила> action

Указание действия, которое должно быть выполнено над пакетами, соответствующими правилу списка сообщества.

**Синтаксис**

```
set policy community-list номер_списка rule
номер_правила action {deny | permit}

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 целоебеззнака32разр {
        rule целоебеззнака32разр {
            action {
                deny
                permit
            }
        }
    }
}
```

**Параметры**

*номер_списка*

Номер определенного списка сообщества.

*номер_правила*

Номер определенного правила списка сообщества.

**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, пересылаются.

**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 выполняется маршрутизация по получателю, то есть пакеты отправляются по обычным каналам пересылки.

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.

### 11.2.25. 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 целоебеззнака32разр {
        rule целоебеззнака32разр {
            description текст
        }
    }
}
```

**Параметры**

*номер_списка*

Номер определенного списка сообщества.

*номер_правила*

Номер определенного правила списка сообщества.

*описание*

Краткое текстовое описание правила 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.

## 11.2.26. policy community-list <номер_списка> rule <номер_правила> regex <рег_выр>

Определение критериев соответствия правила списка путей сообщества на основе регулярного выражения.

**Синтаксис**

**set policy community-list** *номер_списка* **rule** *номер_правила* **regex** *рег_выр*

**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 целоебеззнака32разр {
        rule целоебеззнака32разр {
            regex текст
        }
    }
```

}

**Параметры**

*номер_списка*

Номер определенного списка сообщества.

*номер_правила*

Номер определенного правила списка сообщества.

*рег_выр*

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**

Форма **set** этой команды используется для определения критериев соответствия, которые будут использоваться при определении политики пересылки на основе сообщества BGP.

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** (см. стр. 645), соответствующие пакеты либо разрешаются, либо отклоняются.

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.

## 11.2.27. 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 текст {}
}
```

**Параметры**

*имя_списка*

Множественный узел. Текстовый идентификатор для списка префиксов. Можно создать несколько списков префиксов, создав несколько узлов конфигурации **policy prefix-list**.

**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.

## 11.2.28. 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 текст {
            description текст
        }
    }
```

**Параметры**

*имя_списка*

Имя определенного 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.

## 11.2.29. 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 текст {
        rule целоебеззнака32разр {}
    }
}
```

**Параметры**

*имя_списка*

Имя определенного списка префиксов.

*номер_правила*

Множественный узел. Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 4294967295. Можно определить несколько правил, создав несколько узлов конфигурации **rule**.

**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.

## 11.2.30. policy prefix-list <имя_списка> rule <номер_правила> action

Указание действия, которое должно быть выполнено над пакетами, соответствующими правилу списка префиксов.

**Синтаксис**

**set policy prefix-list** *имя_списка* **rule** *номер_правила* **action** {**deny** | **permit**}

**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 текст {
        rule целоебеззнака32разр {
```

```
                    action {
                        deny
                        permit
                    }
                }
            }
```

**Параметры**

*имя_списка*

Имя определенного списка префиксов.

*номер_правила*

Номер определенного правила списка префиксов.

**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, пересылаются.

**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 выполняется маршрутизация по получателю, то есть пакеты отправляются по обычным каналам пересылки.

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.

### 11.2.31. 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 текст {
        rule целоебеззнака32разр {
            description текст
        }
    }
}
```

**Параметры**

*имя_списка*

Имя определенного списка префиксов.

*номер_правила*

Номер определенного правила списка префиксов.

*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.

## 11.2.32. 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 текст {
        rule целоебеззнака32разр {
            ge 0-32
        }
    }
}
```

**Параметры**

*имя_списка*

Имя определенного списка префиксов.

*номер_правила*

Номер определенного правила списка префиксов.

*значение*

Число, представляющее префикс подсети. Данному правилу будут соответствовать префиксы подсетей, большие указанного числа или равные

ему. Значение должно лежать в диапазоне от 0 до 32.

**Значение по умолчанию**

Если префикс не указан, считается, что все префиксы подсетей соответствуют правилу.

**Указания по использованию**

Форма **set** этой команды используется для указания префикса подсети при определении политики маршрутизации. 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.

В правиле списка префиксов может быть указано ровно одно сравнение (**ge**, **le** или **prefix**).

Форма **delete** этой команды используется для удаления указанного префикса "**ge**". Если префикс не указан, считается, что все префиксы подсетей соответствуют правилу.

Форма **show** этой команды используется для отображения значения, указанного как префикс "**ge**".

## 11.2.33. 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 текст {
```

```
            rule целоебеззнака32разр {
                le 0-32
            }
        }
    }
```

**Параметры**

*имя_списка*

Имя определенного списка префиксов.

*номер_правила*

Номер определенного правила списка префиксов.

*значение*

Число, представляющее префикс подсети. Данному правилу будут соответствовать префиксы подсетей, меньшие указанного числа или равные ему. Значение должно лежать в диапазоне от 0 до 32.

**Значение по умолчанию**

Если префикс не указан, считается, что все префиксы подсетей соответствуют правилу.

**Указания по использованию**

Форма **set** этой команды используется для указания префикса подсети при определении политики маршрутизации. 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.

В правиле списка префиксов может быть указано ровно одно сравнение (**ge**, **le** или **prefix**).

Форма **delete** этой команды используется для удаления указанного префикса “**le**”. Если префикс не указан, считается, что все префиксы подсетей соответствуют правилу.

Форма **show** этой команды используется для отображения значения, указанного как префикс “**le**”.

### 11.2.34. 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 текст {
        rule целоебеззнака32разр {
            prefix подсеть_ipv4
        }
    }
}
```

**Параметры**

*имя_списка*

Имя определенного списка префиксов.

*номер_правила*

Номер определенного правила списка префиксов.

*подсеть_ipv4*

Подсеть IPv4. Данному правилу будут соответствовать подсети, в точности совпадающие с данной подсетью. Используется формат *ip-адрес/префикс*.

**Значение по умолчанию**

Если подсеть не указана, считается, что все подсети соответствуют правилу.

**Указания по использованию**

Форма **set** этой команды используется для указания подсети при

определении политики маршрутизации. 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.

В правиле списка префиксов может быть указано ровно одно сравнение (**ge**, **le** или **prefix**).

Форма **delete** этой команды используется для удаления указанного префикса "**ge**". Если префикс не указан, считается, что все префиксы подсетей соответствуют правилу.

Форма **show** этой команды используется для отображения значения, указанного как префикс "**ge**".

## 11.2.35. 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 текст {}
}
```

**Параметры**

*имя_списка*

Множественный узел. Текстовый идентификатор для списка префиксов IPv6. Можно создать несколько списков префиксов IPv6, создав несколько узлов конфигурации **policy prefix-list6**.

**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.

## 11.2.36. 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 текст {
        description текст
    }
}
```

**Параметры**

*имя_списка*

Имя определенного 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.

## 11.2.37. 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 текст {
        rule целоебеззнака32разр {}
    }
}
```

**Параметры**

*имя_списка*

Имя определенного списка префиксов IPv6.

*номер_правила*

Множественный узел. Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 4294967295. Можно определить несколько правил, создав несколько узлов конфигурации **rule**.

**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.

## 11.2.38. policy prefix-list6 <имя_списка> rule <номер_правила> action

Указание действия, которое должно быть выполнено над пакетами, соответствующими правилу списка префиксов IPv6.

**Синтаксис**

**set policy prefix-list6** *имя_списка* **rule** *номер_правила* **action** {**deny** | **permit**}

**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 текст {
        rule целоебеззнака32разр {
            action {
                deny
                permit
            }
        }
    }
}
```

**Параметры**

*имя_списка*

Имя определенного списка префиксов IPv6.

*номер_правила*

Номер определенного правила списка префиксов IPv6.

**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, пересылаются.

**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 выполняется маршрутизация по получателю, то есть пакеты отправляются по обычным каналам пересылки.

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.

## 11.2.39. 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 текст {
            rule целоебеззнака32разр {
                description текст
            }
        }
    }
```

**Параметры**

*имя_списка*

Имя определенного списка префиксов IPv6.

*номер_правила*

Номер определенного правила списка префиксов IPv6.

*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.

## 11.2.40. 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-list6 текст {
        rule целоебеззнака32разр {
            ge 0-128
        }
    }
}
```

**Параметры**

*имя_списка*

Имя определенного списка префиксов IPv6.

*номер_правила*

Номер определенного правила списка префиксов IPv6.

*значение*

Число, представляющее префикс подсети. Данному правилу будут соответствовать префиксы подсетей, большие указанного числа или равные ему. Значение должно лежать в диапазоне от 0 до 128.

**Значение по умолчанию**

Если префикс не указан, считается, что все префиксы подсетей соответствуют правилу.

**Указания по использованию**

Форма **set** этой команды используется для указания префикса подсети при определении политики маршрутизации. 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.

В правиле списка префиксов может быть указано ровно одно сравнение (**ge**, **le** или **prefix**).

Форма **delete** этой команды используется для удаления указанного префикса

"**ge**". Если префикс не указан, считается, что все префиксы подсетей соответствуют правилу.

Форма **show** этой команды используется для отображения значения, указанного как префикс "**ge**".

## 11.2.41. 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-list6 текст {
        rule целоебеззнака32разр {
            le 0-128
        }
    }
}
```

**Параметры**

*имя_списка*

Имя определенного списка префиксов IPv6.

*номер_правила*

Номер определенного правила списка префиксов IPv6.

*значение*

Число, представляющее префикс подсети. Данному правилу будут

соответствовать префиксы подсетей, меньшие указанного числа или равные ему. Значение должно лежать в диапазоне от 0 до 128.

**Значение по умолчанию**

Если префикс не указан, считается, что все префиксы подсетей соответствуют правилу.

**Указания по использованию**

Форма **set** этой команды используется для указания префикса подсети при определении политики маршрутизации. 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.

В правиле списка префиксов может быть указано ровно одно сравнение (**ge**, **le** или **prefix**).

Форма **delete** этой команды используется для удаления указанного префикса "**le**". Если префикс не указан, считается, что все префиксы подсетей соответствуют правилу.

Форма **show** этой команды используется для отображения значения, указанного как префикс "**le**".

## 11.2.42. 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-list6 текст {
          rule целоебеззнака32разр {
               prefix подсеть_ipv6
          }
     }
}
```

**Параметры**

*имя_списка*

Имя определенного списка префиксов.

*номер_правила*

Номер определенного правила списка префиксов.

*подсеть_ipv6*

Подсеть IPv6. Данному правилу будут соответствовать подсети, в точности совпадающие с данной подсетью. Используется формат *ipv6-адрес/префикс* (то есть <x:x:x:x:x:x:x:x>/<0-128>).

**Значение по умолчанию**

Если подсеть не указана, считается, что все подсети соответствуют правилу.

**Указания по использованию**

Форма **set** этой команды используется для указания подсети при определении политики маршрутизации. 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.

В правиле списка префиксов может быть указано ровно одно сравнение (**ge**, **le** или **prefix**).

Форма **delete** этой команды используется для удаления указанного префикса “**ge**”. Если префикс не указан, считается, что все префиксы подсетей соответствуют правилу.

Форма **show** этой команды используется для отображения значения, указанного как префикс “**ge**”.

## 11.2.43. 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 текст {}
}
```

**Параметры**

*имя_карты*

Множественный узел. Текстовый идентификатор карты маршрутов. Можно создать несколько карт маршрутов, создав несколько узлов конфигурации **policy route-map**.

**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.

## 11.2.44. 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 текст {
        description текст
    }
}
```

**Параметры**

*имя_карты*

Имя определенной 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.

## 11.2.45. 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 текст {
        rule целоебеззнака32разр {}
    }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Множественный узел. Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 4294967295. Можно определить несколько правил, создав несколько узлов конфигурации **rule**.

**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.

## 11.2.46. policy route-map <имя_карты> rule <номер_правила> action

Указание действия, которое должно быть выполнено над пакетами, соответствующими правилу карты маршрутов.

**Синтаксис**

**set policy route-map** *имя_карты* **rule** *номер_правила* **action** {**deny** | **permit**}

**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 текст {
        rule целоебеззнака32разр {
            action {
                deny
                permit
            }
        }
    }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

**deny**

Пакеты, соответствующие данному правилу, игнорируются без каких-либо действий и сообщений.

**permit**

Пакеты, соответствующие данному правилу, пересылаются.

**Значение по умолчанию**

Маршруты отклоняются.

**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 выполняется

маршрутизация по получателю, то есть пакеты отправляются по обычным каналам пересылки.

Действием по умолчанию карты маршрутов является **deny**; то есть если нет элементов, удовлетворяющих критериям соответствия, то маршрут отклоняется. Для изменения такого поведения нужно указать пустое правило **permit** в качестве последнего элемента в карте маршрутов.

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.

## 11.2.47. policy route-map <имя_карты> rule <номер_правила> call <цель>

Вызов другой карты маршрутов.

**Синтаксис**

**set policy route-map** *имя_карты* **rule** *номер_правила* **call** *цель*

**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 текст {
        rule целоебеззнака32разр {
            call текст
        }
    }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

*цель*

Идентификатор вызываемой карты маршрутов.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Форма **set** этой команды используется для вызова другой карты маршрутов.

Новая карта маршрутов вызывается после того, как все действия **set**, указанные в карте 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 правило отклоняется независимо от любых дальнейших политик проверки соответствия или выхода.

Форма **delete** этой команды используется для удаления данного оператора из карты маршрутов.

Форма **show** этой команды используется для отображения параметров настройки правила карты маршрутов.

## 11.2.48. policy route-map <имя_карты> rule <номер_правила> continue <номер_цели>

Вызов другого правила в текущей карте маршрутов.

**Синтаксис**

**set policy route-map** *имя_карты* **rule** *номер_правила* **continue** *номер_цели*

**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 текст {
    rule целоебеззнака32разр {
        continue целоебеззнака32разр
    }
}
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

*номер_цели*

Идентификатор вызываемого правила карты маршрутов.

**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 карте 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.

## 11.2.49. 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_правила* **rule** *номер_правила* **description**

**show policy route-map** *имя_карты* **rule** *номер_правила* **description**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
policy {
    route-map текст {
        rule целоебеззнака32разр {
            description текст
        }
    }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

*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.

## 11.2.50. 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 текст {
        rule целоебеззнака32разр {
            match {
                as-path текст
            }
        }
    }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

*имя_списка*

Пути AS в маршруте проверяются на соответствие путям, разрешенным в указанном данным параметром списке 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**

Форма **set** этой команды используется для определения условия

соответствия, основанного на списке путей AS, в политике карты маршрутов Пакеты проверяются по тому, соответствуют ли пути AS, перечисленные в маршруте, пути AS, определенному с помощью этой команды. В зависимости от действия, определенного в правиле при помощи команды **policy route-map <имя_карты> rule <номер_правила> action** (см. стр. 678), соответствующие пакеты либо разрешаются, либо отклоняются. На основе сведений о передаче, указанных операторами **set** в правиле карты маршрутов, разрешенные пакеты передаются к своим различным получателям.

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 **delete** этой команды используется для удаления условия соответствия по пути AS.

Форма **show** этой команды используется для отображения настройки условия соответствия по пути AS.

## 11.2.51. 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-matc**h}

**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 текст {
    rule целоебеззнака32разр {
        match {
            community {
                community-list
целоебеззнака32разр
                exact-match
            }
        }
    }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

**community-list** *номер_списка*

Сообщества BGP в маршруте проверяются на соответствие сообществам, разрешенным в указанном данным параметром списке сообществ BGP. Политика сообществ BGP к этому моменту должна быть уже определена. Обязательно должен быть указан либо параметр **community-list**, либо параметр **exact-match**.

**exact-match**

Сообщества BGP должны соответствовать в точности. Обязательно должен быть указан либо параметр **community-list**, либо параметр **exact-match**.

**Значение по умолчанию**

Если ни одно условие соответствия по спискам сообщества не определено, фильтрация пакетов по сообществам BGP не выполняется.

**Указания по использованию**

Форма **set** этой команды используется для определения условия соответствия, основанного на сообществах BGP, в политике карты

маршрутов.

Пакеты проверяются по тому, соответствуют ли сообщества BGP, перечисленные в маршруте, сообществам, определенным с помощью этой команды. В зависимости от действия, определенного в правиле при помощи команды **policy route-map <имя_карты> rule <номер_правила> action** (см. стр. 678), соответствующие пакеты либо разрешаются, либо отклоняются. На основе сведений о передаче, указанных операторами **set** в правиле карты маршрутов, разрешенные пакеты передаются своим различным получателям.

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 **delete** этой команды используется для удаления условия соответствия по сообществу BGP.

Форма **show** этой команды используется для отображения настройки условия соответствия по сообществу BGP.

## 11.2.52. policy route-map <имя_карты> rule <номер_правила> match interface <ethx>

Определение условия соответствия в карте маршрутов на основе интерфейса первого транзитного участка.

**Синтаксис**

**set policy route-map** *имя_карты* **rule** *номер_правила* **match interface** *ethx*

**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 текст {
     rule целоебеззнака32разр {
          match {
               interface текст
          }
     }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

*ethx*

Проверяется соответствие интерфейса первого транзитного участка, указанного в маршруте, определенному данным параметром имени интерфейса.

**Значение по умолчанию**

Если ни одно условие соответствия по интерфейсам не определено, фильтрация пакетов по интерфейсу не выполняется.

**Указания по использованию**

Форма **set** этой команды используется для определения условия соответствия, основанного на интерфейсе первого транзитного участка, в политике карты маршрутов.

Пакеты проверяются по тому, соответствует ли интерфейс первого транзитного участка маршрута интерфейсу, определенному с помощью этой команды. В зависимости от действия, определенного в правиле при помощи команды **policy route-map <имя_карты> rule <номер_правила> action** (см. стр. 678), соответствующие пакеты либо разрешаются, либо отклоняются. На основе сведений о передаче, указанных операторами **set** в правиле карты маршрутов, разрешенные пакеты передаются к своим

различным получателям.

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 **delete** этой команды используется для удаления условия соответствия по интерфейсу.

Форма **show** этой команды используется для отображения настройки условия соответствия по интерфейсу.

## 11.2.53. 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 текст {
        rule целоебеззнака32разр {
            match {
                ip address {
                    access-list целоебеззнака32разр
                    prefix-list текст
                }
            }
```

```
                }
            }
        }
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

**access-list** *номер_списка*

IP-адрес отправителя или получателя маршрута проверяется на соответствие IP-адресам, разрешенным указанным списком доступа. Список доступа к моменту выдачи команды должен быть уже определен. Обязательно должен быть указан либо параметр **access-list**, либо параметр **prefix-list**.

**prefix-list** *имя_списка*

Подсеть отправителя или получателя маршрута проверяется на соответствие подсетям, разрешенным указанным списком префиксов. Список префиксов к моменту выдачи команды должен быть уже 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**

Форма **set** этой команды используется для определения условия соответствия, основанного на IP-адресе, в политике карты маршрутов.

Пакеты проверяются по тому, соответствует ли IP-адрес отправителя или получателя маршрута адресу, содержащемуся в указанном списке доступа или списке префиксов. В зависимости от действия, определенного в правиле при помощи команды **policy route-map <имя_карты> rule <номер_правила> action** (см. стр. 678), соответствующие пакеты либо разрешаются, либо отклоняются. На основе сведений о передаче, указанных операторами **set** в правиле карты маршрутов, разрешенные пакеты передаются своим различным получателям.

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 **delete** этой команды используется для удаления условия соответствия по IP-адресу.

Форма **show** этой команды используется для отображения настройки условия соответствия по IP-адресу.

## 11.2.54. policy route-map <имя_карты> rule <номер_правила> match ip nexthop

Определение условия соответствия в карте маршрутов на основе адреса следующего транзитного участка.

**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 текст {
        rule целоебеззнака32разр {
            match {
                ip {
                    nexthop {

access-list целоебеззнака32разр

prefix-list текст
```

```
                                    }
                                }
                            }
                        }
                    }
                }
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

**access-list** *номер_списка*

IP-адрес следующего транзитного участка в маршруте проверяется на соответствие IP-адресам, разрешенным указанным списком доступа. Список доступа к данному моменту должен быть уже определен. Обязательно должен быть указан либо параметр **access-list**, либо параметр **prefix-list**.

**prefix-list** *имя_списка*

IP-адрес следующего транзитного участка в маршруте проверяется на соответствие IP-адресам, разрешенным указанным списком префиксов. Список префиксов к данному моменту должен быть уже определен. Обязательно должен быть указан либо параметр **access-list**, либо параметр **prefix-list**.

**Значение по умолчанию**

Если ни одно условие соответствия по следующему транзитному участку не определено, фильтрация пакетов по следующему транзитному участку не выполняется.

**Указания по использованию**

Форма **set** этой команды используется для определения условия соответствия, основанного на IP-адресе следующего транзитного участка, в политике карты маршрутов.

Пакеты проверяются по тому, соответствует ли IP-адрес следующего транзитного участка маршрута адресу, содержащемуся в указанном списке

доступа или списке префиксов. В зависимости от действия, определенного в правиле при помощи команды **policy route-map <имя_карты> rule <номер_правила> action** (см. стр. 678), соответствующие пакеты либо разрешаются, либо отклоняются. На основе сведений о передаче, указанных операторами **set** в правиле карты маршрутов, разрешенные пакеты передаются своим различным получателям.

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 **delete** этой команды используется для удаления условия соответствия по IP-адресу следующего транзитного участка.

Форма **show** этой команды используется для отображения настройки условия соответствия по IP-адресу следующего транзитного участка.

## 11.2.55. 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 текст {
        rule целоебеззнака32разр {
```

```
                match {
                    ip {
                        route-source {

        access-list целоебеззнака32разр

        prefix-list текст
                            }
                    }
                }
            }
        }
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

**access-list** *номер_списка*

Считается найденным соответствие для маршрутов, объявляемых с адресов, содержащихся в указанном списке доступа. Список доступа к моменту выдачи команды должен быть уже определен. Обязательно должен быть указан либо параметр **access-list**, либо параметр **prefix-list**.

**prefix-list** *имя_списка*

Считается найденным соответствие для маршрутов, объявляемых с адресов, содержащихся в указанном списке префиксов. Список префиксов к моменту выдачи команды должен быть уже 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**

Форма **set** этой команды используется для определения условия соответствия, основанного на адресе, с которого объявляются маршруты (адресе отправителя маршрутов), в политике карты маршрутов.

Пакеты проверяются по тому, соответствует ли адрес отправителя маршрута адресу, содержащемуся в указанном списке доступа или списке префиксов. В зависимости от действия, определенного в правиле при помощи команды **policy route-map <имя_карты> rule <номер_правила> action** (см. стр. 678), соответствующие пакеты либо разрешаются, либо отклоняются. На основе сведений о передаче, указанных операторами **set** в правиле карты маршрутов, разрешенные пакеты передаются своим различным получателям.

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 **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.

## 11.2.56. 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 текст {
          rule целоебеззнака32разр {
               match {
                    ipv6 {
                         address {

     access-list6 целоебеззнака32разр

     prefix-list6 текст
                         }
                    }
               }
          }
     }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

**access-list6** *номер_списка*

IP-адрес отправителя или получателя маршрута проверяется на соответствие IP-адресам, разрешенным указанным списком доступа. Список доступа к моменту выдачи команды должен быть уже определен. Обязательно должен быть указан либо параметр **access-list6**, либо параметр **prefix-list6**.

**prefix-list6** *имя_списка*

Подсеть отправителя или получателя маршрута проверяется на соответствие подсетям, разрешенным указанным списком префиксов. Список префиксов к моменту выдачи команды должен быть уже 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**

Форма **set** этой команды используется для определения условия соответствия, основанного на IPv6-адресе, в политике карты маршрутов.

Пакеты проверяются по тому, соответствует ли IPv6-адрес отправителя или получателя маршрута адресу, содержащемуся в указанном списке доступа или списке префиксов. В зависимости от действия, определенного в правиле при помощи команды **policy route-map <имя_карты> rule <номер_карты> action** (см. стр. 678), соответствующие пакеты либо разрешаются, либо отклоняются. На основе сведений о передаче, указанных операторами **set** в правиле карты маршрутов, разрешенные пакеты передаются своим различным получателям.

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 **delete** этой команды используется для удаления условия соответствия по IPv6-адресу.

Форма **show** этой команды используется для отображения настройки условия соответствия по IPv6-адресу.

## 11.2.57. policy route-map <имя_карты> rule <номер_правила> match ipv6 nexthop

Определение условия соответствия в карте маршрутов на основе IPv6-адреса следующего транзитного участка.

**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 текст {
        rule целоебеззнака32разр {
            match {
                ipv6 {
                    nexthop {

    access-list6 целоебеззнака32разр

    prefix-list6 текст
                    }
                }
            }
        }
    }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

**access-list6** *номер_списка*

IPv6-адрес следующего транзитного участка в маршруте проверяется на соответствие IPv6-адресам, разрешенным указанным списком доступа. Список доступа к моменту выдачи команды должен быть уже определен. Обязательно должен быть указан либо параметр **access-list6**, либо параметр **prefix-list6**.

**prefix-list6** *имя_списка*

IPv6-адрес следующего транзитного участка в маршруте проверяется на соответствие IPv6-адресам, разрешенным указанным списком префиксов. Список префиксов к моменту выдачи команды должен быть уже определен. Обязательно должен быть указан либо параметр **access-list6**, либо параметр **prefix-list6**.

**Значение по умолчанию**

Если ни одно условие соответствия по следующему транзитному участку не определено, фильтрация пакетов по следующему транзитному участку не выполняется.

**Указания по использованию**

Форма **set** этой команды используется для определения условия соответствия, основанного на IPv6-адресе следующего транзитного участка, в политике карты маршрутов.

Пакеты проверяются по тому, соответствует ли IPv6-адрес следующего транзитного участка маршрута адресу, содержащемуся в указанном списке доступа или списке префиксов. В зависимости от действия, определенного в правиле при помощи команды **policy route-map <имя_карты> rule <номер_карты> action** (см. стр. 678), соответствующие пакеты либо разрешаются, либо отклоняются. На основе сведений о передаче, указанных операторами **set** в правиле карты маршрутов, разрешенные пакеты передаются своим различным получателям.

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 **delete** этой команды используется для удаления условия соответствия по IPv6-адресу следующего транзитного участка.

Форма **show** этой команды используется для отображения настройки условия соответствия по IPv6-адресу следующего транзитного участка.

## 11.2.58. 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 текст {
        rule целоебеззнака32разр {
            match {
                metric целоебеззнака32разр
            }
        }
    }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

*метрика*

Число, представляющее метрику маршрута; на соответствие этому числу проверяется метрика в маршруте.

**Значение по умолчанию**

Если ни одно условие соответствия по метрике не определено, фильтрация

пакетов по метрике не выполняется.

**Указания по использованию**

Форма **set** этой команды используется для определения условия соответствия, основанного на метрике маршрута, в политике карты маршрутов.

Пакеты проверяются по тому, соответствует ли метрика маршрута метрике, определенной с помощью этой команды. В зависимости от действия, определенного в правиле при помощи команды **policy route-map <имя_карты> rule <номер_правила> action** (см. стр. 678), соответствующие пакеты либо разрешаются, либо отклоняются. На основе сведений о передаче, указанных операторами **set** в правиле карты маршрутов, разрешенные пакеты передаются своим различным получателям.

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 **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.

## 11.2.59. policy route-map <имя_карты> rule <номер_правила> match origin

Определение условия соответствия в карте маршрутов на основе способа получения маршрута.

**Синтаксис**

**set policy route-map** *имя_карты* **rule** *номер_правила* **match origin** {**egp** | **igp** | **incomplete**}

**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 текст {
        rule целоебеззнака32разр {
            match {
                origin {
                    origin-code [egp|igp|incomplete]
                }
            }
        }
    }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

**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**

Форма **set** этой команды используется для определения условия соответствия, основанного на коде BGP способа получения, в политике карты маршрутов.

Пакеты проверяются по тому, соответствует ли код BGP способа получения в маршруте коду, определенному с помощью этой команды. В зависимости от действия, определенного в правиле при помощи команды **policy route-map map-name rule rule-num action** (см. стр. 678), соответствующие пакеты либо разрешаются, либо отклоняются. На основе сведений о передаче, указанных операторами **set** в правиле карты маршрутов, разрешенные пакеты передаются своим различным получателям.

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 **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.

## 11.2.60. policy route-map <имя_карты> rule <номер_правила> match peer <ipv4-адрес>

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*

**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 текст {
        rule целоебеззнака32разр {
            match {
                peer ipv4-адрес
            }
        }
    }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

*ipv4-адрес*

IPv4-адрес. На соответствие этому адресу проверяется адрес равноправного узла в маршруте.

**Значение по умолчанию**

Если ни одно условие соответствия по адресам равноправных узлов не определено, фильтрация пакетов по IP-адресам равноправных узлов не выполняется.

**Указания по использованию**

Форма **set** этой команды используется для определения условия соответствия, основанного на IP-адресе равноправного узла, в политике карты маршрутов.

Пакеты проверяются по тому, соответствует ли адрес равноправного узла в маршруте адресу, определенному с помощью этой команды. В зависимости от действия, определенного в правиле при помощи команды **policy route-map <имя_карты> rule <номер_правила> action** (см. стр. 678), соответствующие пакеты либо разрешаются, либо отклоняются. На основе сведений о передаче, указанных операторами **set** в правиле карты

маршрутов, разрешенные пакеты передаются своим различным получателям.

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 **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.

## 11.2.61. 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 текст {
        rule целоебеззнака32разр {
            match {
                tag целоебеззнака32разр
            }
        }
    }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

*тег*

32-разрядное значение, представляющее тег OSPF. На соответствие этому значению проверяется содержимое 32-разрядного поля внешнего тега LSA (Link-State Advertisement, объявление состояния канала) протокола OSPF в маршруте.

**Значение по умолчанию**

Если ни одно условие соответствия по тегу не определено, фильтрация пакетов по тегу не выполняется.

**Указания по использованию**

Форма **set** этой команды используется для определения условия соответствия, основанного на теге OSPF, в политике карты маршрутов.

Пакеты проверяются по тому, соответствует ли значение 32-разрядного поля внешнего тега LSA протокола OSPF значению, определенному с помощью этой команды. В зависимости от действия, определенного в правиле при помощи команды **policy route-map <имя_карты> rule <номер_правила> action** (см. стр. 678), соответствующие пакеты либо разрешаются, либо отклоняются. На основе сведений о передаче, указанных операторами **set** в правиле карты маршрутов, разрешенные пакеты передаются к своим различным получателям.

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 **delete** этой команды используется для удаления условия соответствия по тегу OSPF.

Форма **show** этой команды используется для отображения настройки условия соответствия по тегу OSPF.

## 11.2.62. 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** {**goto** *номер_правила* | **next**}

**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 текст {
        rule целоебеззнака32разр {
            on-match {
                goto целоебеззнака32разр
            }
        }
    }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

**goto** *номер_правила*

Номер определенного правила карты маршрутов. Когда все соответствия, перечисленные в правиле карты маршрутов, найдены, происходит выход из текущего правила карты маршрутов, вызов правила, указанного данным параметром, и его выполнение. Следует заметить, что переход на предшествующее правило списка маршрутов не разрешается.

**next**

Когда все соответствия, перечисленные в правиле карты маршрутов, найдены, происходит выход из текущего правила карты маршрутов, вызов следующего правила в последовательности и его выполнение.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

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. Когда все условия соответствий, указанные в правиле карты маршрутов, удовлетворены, происходит вызов правила, указанного данной командой, и его выполнение.

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 **delete** этой команды используется для удаления политики выхода.

Форма **show** этой команды используется для отображения настройки политики выхода из карты маршрутов.

## 11.2.63. policy 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 текст {
        rule целоебеззнака32разр {
            set {
                aggregator {
                    as 1-65535
                    ip ipv4-адрес
                }
            }
        }
    }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

**as** *номер_as*

Изменение номера автономной системы агрегатора BGP в маршруте на указанное значение. Значение должно лежать в диапазоне от 1 до 65535.

**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.

## 11.2.64. 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 текст {
          rule целоебеззнака32разр {
               set {
                    as-path-prepend текст
               }
          }
     }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

*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.

## 11.2.65. 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 текст {
        rule целоебеззнака32разр {
            set {
                atomic-aggregate
            }
        }
    }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

**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.

## 11.2.66. 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** *имя_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 текст {
        rule целоебеззнака32разр {
            set {
                comm-list {
```

```
                                comm-list текст
                                delete
                            }
                        }
                    }
                }
            }
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

**comm-list** *имя_списка*

Удаление сообществ, перечисленных в указанном списке сообществ, из списка сообществ маршрута. Список сообществ к моменту выдачи команды должен быть уже определен.

**delete**

Удаление всего списка сообществ маршрута.

**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.

## 11.2.67. 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 текст {
        rule целоебеззнака32разр {
            set {
                community текст
            }
        }
    }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

**additive**

Добавление указанного сообщества к существующим сообществам в пути. Если указано ключевое слово **additive**, необходимо использовать двойные кавычки.

*сообщество*

Сообщество BGP. Поддерживаются значения в виде номера сообщества в

формате *aa:nn* или названия известных сообществ BGP **local-AS**, **no-export**, **no-advertise** и **internet**.

**none**

Удаление атрибута сообществ из информации 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.

## 11.2.68. policy route-map <имя_карты> rule <номер_правила> set ip-next-hop <ipv4-адрес>

Изменение получателя следующего транзитного участка 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 текст {
        rule целоебеззнака32разр {
            set {
```

```
                    ip-next-hop ipv4-адрес
                }
            }
        }
    }
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

**ip-next-hop** *ipv4-адрес*

IPv4-адрес следующего транзитного участка.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Форма **set** этой команды используется для изменения получателя следующего транзитного участка для пакетов, проходящих через карту маршрутов. Когда все условия соответствий, указанные в правиле карты маршрутов, удовлетворены, происходит изменение следующего транзитного участка 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.

## 11.2.69. 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 текст {
        rule целоебеззнака32разр {
            set {
                local-preference целоебеззнака32разр
            }
        }
    }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

**local-pref**

Новое значение для атрибута пути локального предпочтения BGP.

**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.

## 11.2.70. 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 текст {
        rule целоебеззнака32разр {
            set {
                metric текст
            }
        }
    }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

*метрика*

Число, представляющее новую метрику, которая должна быть использована в маршруте.

**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.

## 11.2.71. 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 текст {
        rule целоебеззнака32разр {
            set {
                metric-type [type-1|type-2]
            }
        }
    }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

**type-1**

Внешняя метрика OSPF типа 1. В этой метрике при вычислении стоимости доступа ко внешней сети используются как внешние, так и внутренние стоимости.

**type-2**

Внешняя метрика OSPF типа 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 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.

## 11.2.72. policy route-map <имя_карты> rule <номер_правила> set origin

Изменение кода BGP способа получения маршрута.

**Синтаксис**

**set policy route-map** *имя_карты* **rule** *номер_правила* **set origin** {*номер_as* | **egp** | **igp** | **incomplete**}

**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 текст {
     rule целоебеззнака32разр {
          set {
               origin [egp|igp|incomplete]
          }
     }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

*номер_as*

Номер автономной системы. Значение должно лежать в диапазоне от 1 до 65535.

**egp**

Установка значения **egp** (Exterior Gateway Protocol) для кода способа получения BGP.

**igp**

Установка значения **igp** (Interior Gateway Protocol) для кода способа получения BGP.

**incomplete**

Установка значения **incomplete** для кода способа получения BGP.

**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.

### 11.2.73. 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 текст {
        rule целоебеззнака32разр {
            set {
                originator-id ipv4-адрес
            }
        }
    }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

*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.

## 11.2.74. 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**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
policy {
    route-map текст {
        rule целоебеззнака32разр {
            set {
                tag целоебеззнака32разр
```

```
                    }
                }
            }
        }
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

номер_правила

Номер определенного правила карты маршрутов.

*тег*

32-разрядное число, представляющее новое значение поля внешнего тега LSA протокола OSPF.

**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.

## 11.2.75. 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 текст {
        rule целоебеззнака32разр {
            set {
                weight целоебеззнака32разр
            }
        }
    }
}
```

**Параметры**

*имя_карты*

Имя определенной карты маршрутов.

*номер_правила*

Номер определенного правила карты маршрутов.

*вес*

Вес BGP для записи в таблицу маршрутизации. Значение должно лежать в диапазоне от 0 до 65535.

**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.

## 11.2.76. show ip access-list

Отображение всех списков доступа IP.

**Синтаксис**

**show ip access-list**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для отображения списков доступа IP.

**Примеры**

В примере 11.6 приведен образец вывода списков доступа IP.

*Пример 11.16 - Вывод списков доступа IP.*

```
admin@neo:~$ show ip access-list
ZEBRA:
Standard IP access list 1
     permit any
RIP:
Standard IP access list 1
     permit any
OSPF:
Standard IP access list 1
     permit any
BGP:
Standard IP access list 1
     permit any
```

## 11.2.77. show ip as-path-access-list

Отображение всех списков доступа по путям AS.

**Синтаксис**

**show ip as-path-access-list**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для отображения списков доступа по путям AS.

**Примеры**

В примере 11.17 приведен образец вывода списков доступа по путям AS.

*Пример 11.17 - Вывод списков доступа по путям AS*

```
admin@neo:~$ show ip as-path-access-list
AS path access list IN
     permit 50:1
```

## 11.2.78. show ip community-list

Отображение всех списков сообществ IP.

**Синтаксис**

**show ip community-list**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для отображения списков сообществ.

**Примеры**

В примере 11.18 приведен образец вывода списков сообществ.

*Пример 11.18 - Вывод списков сообществ*

```
admin@neo:~$ show ip community-list
```

```
Community (expanded) access list 101
     permit AB*
```

## 11.2.79. show ip extcommunity-list

Отображение всех расширенных списков сообществ IP.

**Синтаксис**

**show ip extcommunity-list**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для отображения расширенных списков сообществ IP.

**Примеры**

В примере 11.19 приведен образец вывода расширенных списков сообществ IP.

*Пример 11.19 - Вывод расширенных списков сообществ IP*

```
admin@neo:~$ show ip extcommunity-list
Community (expanded) access list 101
     permit AB*
```

## 11.2.80. show ip prefix-list

Отображение списков префиксов IP.

**Синтаксис**

**show ip prefix-list** [**detail** | **summary** | **list-name** [**seq** *номер_последовательности* | *подсеть_ipv4* [**first-match** | **longer**]]]

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**detail**

Отображение подробных сведений для всех списков префиксов IP.

**summary**

Отображение сводки сведений для всех списков префиксов IP. имя_списка

Отображение сведений об именованном списке префиксов IP.

**seq-num**

Отображение указанной последовательности из именованного списка префиксов IP.

*подсеть_ipv4*

Отображение префикса выбора именованного списка префиксов IP.

**first-match**

Отображение первого соответствия префиксу выбора из именованного списка префиксов IP.

**longer**

Отображение более длинного соответствия префиксу выбора из именованного списка префиксов IP.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для отображения списков префиксов.

**Примеры**

В примере 11.20 приведен образец вывода списков префиксов.

*Пример 11.20 - Вывод списков префиксов*

```
admin@neo:~$ show ip prefix-list
ZEBRA: ip prefix-list ABC: 1 entries
     seq 1 permit 192.168.2.0/24 ge 25
RIP: ip prefix-list ABC: 1 entries
     seq 1 permit 192.168.2.0/24 ge 25
OSPF: ip prefix-list ABC: 1 entries
     seq 1 permit 192.168.2.0/24 ge 25
BGP: ip prefix-list ABC: 1 entries
```

```
seq 1 permit 192.168.2.0/24 ge 25
```

## 11.2.81. 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 IP по протоколам.

**Примеры**

В примере 11.21 приведен образец вывода карт маршрутов IP по протоколам.

*Пример 11.21 - Вывод карт маршрутов IP по протоколам*

```
admin@neo:~$ show ip protocol
Protocol  : route-map
------------
system    : none
kernel    : none
connected : none
static    : none
rip       : none
ripng     : none
ospf      : none
ospf6     : none
isis      : none
bgp       : none
hsls      : none
```

```
any        : none
```

## 11.2.82. show route-map

Отображение сведений карты маршрутов.

**Синтаксис**

**show route-map** [**map-name**]

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для отображения сведений карты маршрутов.

**Примеры**

В примере 11.22 приведен образец вывода сведений карты маршрутов.

*Пример 11.22 - Вывод сведений карты маршрутов*

```
admin@neo:~$ show route-map
ZEBRA:
route-map MAP1, permit, sequence 1
  Match clauses:
  Set clauses:
  Call clause:
  Action:
     Exit routemap
RIP:
route-map MAP1, permit, sequence 1
  Match clauses:
     interface eth0
  Set clauses:
  Call clause:
  Action:
     Exit routemap
```

```
OSPF:
route-map MAP1, permit, sequence 1
  Match clauses:
     interface eth0
  Set clauses:
  Call clause:
  Action:
     Exit routemap
BGP:
route-map MAP1, permit, sequence 1
  Match clauses:
  Set clauses:
  Call clause:
  Action:
     Exit routemap
```

# 12. МАРШРУТИЗАЦИЯ МНОГОАДРЕСНЫХ ПЕРЕДАЧ

## 12.1. Многоадресные передачи

### 12.1.1. Понятие многоадресной передачи

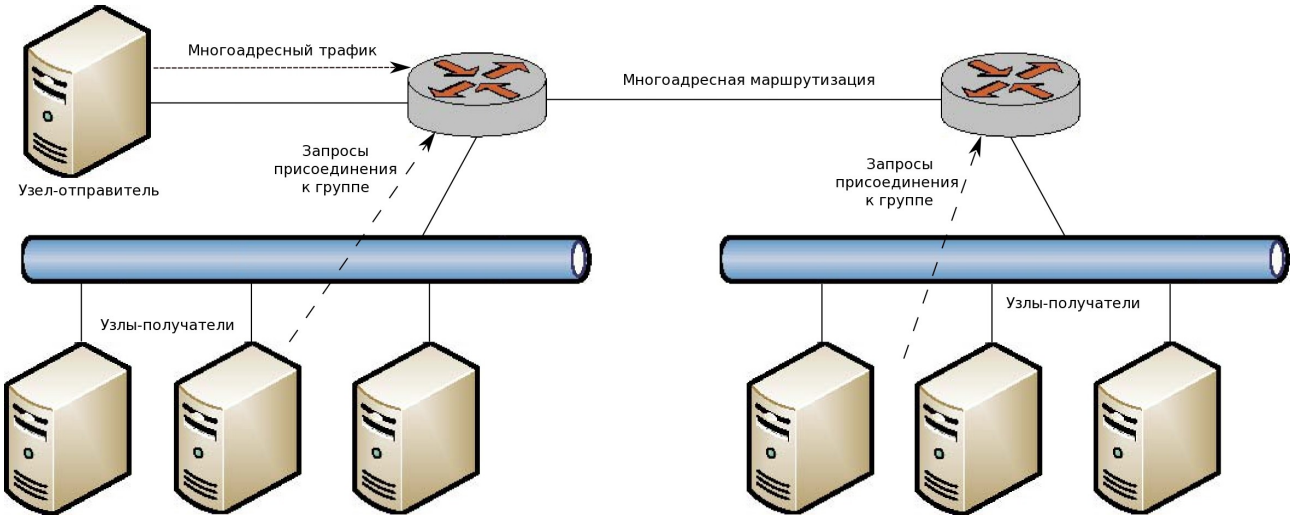
При одноадресной передаче сетевой трафик передается в единственную точку назначения. Если сетевой трафик необходимо передать в группу точек назначения, то используется многоадресная передача. Многоадресный трафик может быть принят только членами группы точек назначения, прослушивающими многоадресный 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 17 - Интрасеть с поддержкой многоадресной передач*




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.

### 12.1.2. 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.

## 12.2. Протокол DVMRP и его настройка

Маршрутизация многоадресных передач IP в Altell NEO 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 (см. раздел 12.1. ), 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.

### 12.2.1. 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.

## 12.2.2. 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@neo# set protocols dvmrp
[edit]
admin@neo# commit
[edit]
```

В данном случае система Altell NEO 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.

## 12.2.3. Настройка многоадресных передач на сетевых интерфейсах

Помимо конфигурации по умолчанию, в системе можно установить параметры маршрутизации многоадресных передач на каждый интерфейс, поддерживающий многоадресную передачу.

### *12.2.3.1. 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:

```
admin@neo# set protocols dvmrp interface eth0 disable
[edit]
```

#### *12.2.3.2. 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.

**ВНИМАНИЕ:** Система не обрабатывает интерфейсы с метрикой больше 31. Общая рекомендация заключается в том, чтобы метрика была настолько мала, насколько это возможно.

Значение метрики по умолчанию равно 1 (см. раздел 12.4. ).

Пример настройки:

```
admin@neo# set protocols dvmrp interface eth1 metric 2
[edit]
```

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 (см. раздел 12.4. ).

Пример настройки:

```
admin@neo# set protocols dvmrp interface eth1 threshold 10
[edit]
```

### 12.2.4. 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:

```
admin@neo# set protocols dvmrp tunnel mtun0 local 192.168.1.77
[edit]
admin@neo# set protocols dvmrp tunnel mtun0 remote 192.168.2.99
[edit]
```

Или

```
admin@neo# set protocols dvmrp tunnel mtun0 local 10.0.0.1
[edit]
admin@neo# set protocols dvmrp tunnel mtun0 remote myhost.mydomain
[edit]
```

### 12.2.5. 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:

```
admin@neo# set protocols dvmrp alias LOCAL_ONE 239.0.0.0/16
[edit]
admin@neo# set protocols dvmrp alias LOCAL_TWO 239.1.1.0/16
[edit]
```

Впоследствии псевдонимы LOCAL_ONE и LOCAL_TWO можно использовать для ограничения областей видимости:

```
admin@neo# set protocols dvmrp interface eth1 bound LOCAL_ONE
[edit]
admin@neo# set protocols dvmrp interface eth1 bound LOCAL_TWO
[edit]
admin@neo# set protocols dvmrp tunnel mtun0 LOCAL_TWO
[edit]
```

Это значит, что сеть LOCAL_ONE видима только через интерфейс **eth1**, а сеть LOCAL_TWO видима через интерфейс **eth1** и туннель **mtun0**. Дейтаграммы с адресов LOCAL_ONE и LOCAL_TWO не будут перенаправляться на другие интерфейсы.

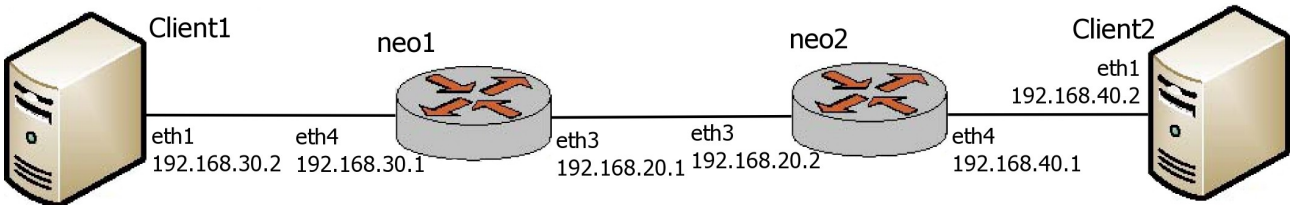
## 12.3. Примеры

### 12.3.1. 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 18 - Простейший пример настройки маршрутизации многоадресных передач*




На маршрутизаторах **neo1** и **neo2** настроен протокол DVMRP. Клиентские компьютеры **Client1** и **Client2** видят друг друга за счёт статической маршрутизации между маршрутизаторами **neo1** и **neo2**. Горизонтальные линии на схеме соответствуют многоадресной передаче.

Ниже представлена последовательность команд для настройки протокола DVMRP в данной сети.

*Пример 12.1 - Простейший пример настройки многоадресной маршрутизации*

| Действие | Команда |
|---|---|
| IP-адрес на интерфейсе eth3 маршрутизатора neo1. | `admin@neo1# set interfaces ethernet eth3 address 192.168.20.1/24`<br>`[edit]` |
| IP-адрес на интерфейсе eth4 маршрутизатора neo1. | `admin@neo1# set interfaces ethernet eth4 address 192.168.30.1/24`<br>`[edit]` |
| Включение поддержки DVMRP на neo1. | `admin@neo1# set protocols dvmrp`<br>`[edit]` |
| Установка порога DVMRP на интерфейсе eth3 на neo1. | `admin@neo1# set protocols dvmrp interface eth3 threshold 5`<br>`[edit]` |
| Установка порога DVMRP на | `admin@neo1# set protocols dvmrp` |

интерфейсе eth4 на neo1.

```
interface eth4 threshold 5
[edit]
```

Установка статического маршрута до neo2 для одноадресных передач на neo1.

```
admin@neo1# set protocols static
route 192.168.40.0/24 next-hop
192.168.20.2
[edit]
```

Установка статического маршрута до neo2 для многоадресных передач на neo1.

```
admin@neo1# set protocols static
route 224.0.0.0/4 next-hop
192.168.20.2
[edit]
```

Фиксация изменений.

```
admin@neo1# commit
[edit]
```

Вывод настройки интерфейсов на neo1.

```
admin@neo1# show interfaces
interfaces {
     ethernet eth3 {
          address 192.168.20.1/24
     }
     ethernet eth4 {
          address 192.168.30.1/24
     }
          management true
}
[edit]
```

Вывод настройки протоколов на neo1.

```
admin@neo1# show protocols
protocols {
     dvmrp {
          interface eth3 {
               threshold 5
          }
          interface eth4 {
```

```
                    threshold 5
               }
          }
          static {
               route 192.168.40.0/24 {
                    next-hop
192.168.20.2 {
                    }
               }
               route 224.0.0.0/4 {
                    next-hop
192.168.20.2 {
                    }
               }
          }
}
[edit]
```

IP-адрес на интерфейсе eth3 маршрутизатора neo2.

```
admin@neo2# set interfaces
ethernet eth3 address
192.168.40.1/24
[edit]
```

IP-адрес на интерфейсе eth4 маршрутизатора neo2.

```
admin@neo2# set interfaces
ethernet eth4 address
192.168.20.2/24
[edit]
```

Включение поддержки DVMRP на neo2.

```
admin@neo2# set protocols dvmrp
[edit]
```

Установка порога DVMRP на интерфейсе eth3 на neo2.

```
admin@neo2# set protocols dvmrp
interface eth3 threshold 5
[edit]
```

Установка порога DVMRP на интерфейсе eth4 на neo2.

```
admin@neo2# set protocols dvmrp
interface eth4 threshold 5
[edit]
```

Установка статического маршрута до neo1 для одноадресных передач на neo2.

```
admin@neo2# set protocols static
route 192.168.30.0/24 next-hop
192.168.20.1
[edit]
```

Установка статического маршрута до neo1 для многоадресных передач на neo2.

```
admin@neo2# set protocols static
route 224.0.0.0/4 next-hop
192.168.20.1
[edit]
```

Фиксация изменений.

```
admin@neo2# commit
[edit]
```

Вывод настройки интерфейсов на neo2.

```
admin@neo2# show interfaces
interfaces {
     ethernet eth3 {
          address 192.168.40.1/24
     }
     ethernet eth4 {
          address 192.168.20.2/24
     }
     management true
}
[edit]
```

Вывод настройки протоколов на neo2.

```
admin@neo2# show protocols
protocols {
     dvmrp {
          interface eth3 {
               threshold 5
          }
```

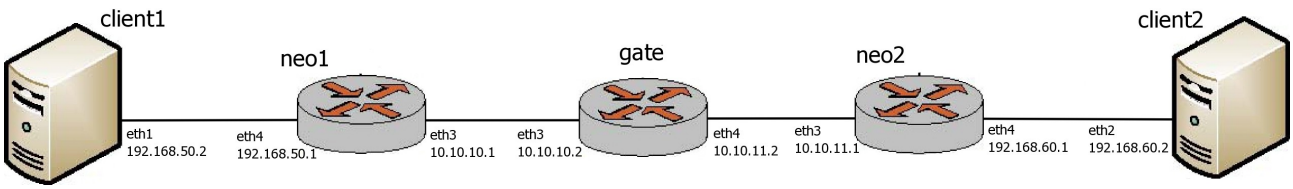
```
                interface eth4 {
                    threshold 5
                }
            }
            static {
                route 192.168.30.0/24 {
                    next-hop
        192.168.20.1 {
                    }
                }
                route 224.0.0.0/4 {
                    next-hop
        192.168.20.1 {
                    }
                }
            }
        }
        [edit]
```

### 12.3.2. 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 19 - Пример настройки протокола DVMRP с использованием туннелей*



В примере описана ситуация, когда 2 маршрутизатора (**neo1** и **neo2**) связаны туннелем DVMRP через промежуточный маршрутизатор (**gate**), который не поддерживает многоадресную передачу.

- Шлюз по умолчанию на neo1: 10.10.10.2.
- Шлюз по умолчанию на neo2: 10.10.11.2.
- **client1**: настольный компьютер со шлюзом по умолчанию 192.168.50.1.
- **client2**: настольный компьютер со шлюзом по умолчанию 192.168.60.1.
- На маршрутизаторе **gate**, через который связаны **neo1** и **neo2**, многоадресная передача не поддерживается.

Порядок выполнения команд, данный в примере, существенен: к моменту настройки туннеля его удаленный конец должен быть достижим.

*Пример 12.2 - Пример настройки протокола DVMRP с использованием туннелей*

| Действие | Команда |
|---|---|
| IP-адрес на интерфейсе eth3 маршрутизатора neo1. | admin@neo1# **set interfaces ethernet eth3 address 10.10.10.1/24** [edit] |
| IP-адрес на интерфейсе eth4 маршрутизатора neo1. | admin@neo1# **set interfaces ethernet eth4 address 192.168.50.1/24** [edit]IP-адрес на интерфейсе eth3 маршрутизатора neo1 |
| Включение поддержки DVMRP на neo1. | admin@neo1# **set protocols dvmrp** [edit] |
| Установка порога DVMRP на интерфейсе eth3 на neo1. | admin@neo1# **set protocols dvmrp interface eth3 threshold 5** [edit] |
| Установка порога DVMRP на интерфейсе eth4 на neo1. | admin@neo1# **set protocols dvmrp interface eth4 threshold 5** |

| | |
|---|---|
| | [edit] |
| Фиксация изменений. | admin@neo1# **commit**<br>[edit] |
| IP-адрес на интерфейсе eth3 маршрутизатора neo2 | admin@neo2# **set interfaces ethernet eth3 address 10.10.11.1/24**<br>[edit] |
| IP-адрес на интерфейсе eth4 маршрутизатора neo2. | admin@neo2# **set interfaces ethernet eth4 address 192.168.60.1/24**<br>[edit] |
| Включение поддержки DVMRP на neo2. | admin@neo2# **set protocols dvmrp**<br>[edit] |
| Установка порога DVMRP на интерфейсе eth3 на neo2. | admin@neo2# **set protocols dvmrp interface eth3 threshold 5**<br>[edit] |
| Установка порога DVMRP на интерфейсе eth2 на neo2. | admin@neo2# **set protocols dvmrp interface eth4 threshold 5**<br>[edit] |
| Фиксация изменений. | admin@neo2# **commit**<br>[edit] |
| Включение туннеля DVMRP на neo1. | admin@neo1# **set protocols dvmrp tunnel mtun0**<br>[edit] |
| Установка локального конца туннеля DVMRP на neo1. | admin@neo1# **set protocols dvmrp tunnel mtun0 local 10.10.10.1**<br>[edit] |
| Установка удаленного конца туннеля | admin@neo1# **set protocols dvmrp** |

| | |
|---|---|
| DVMRP на neo1. | **tunnel mtun0 remote 10.10.11.1**<br>[edit] |
| Установка порога DVMRP по умолчанию для туннеля на neo1. | admin@neo1# **set protocols dvmrp tunnel mtun0 threshold**<br>[edit] |
| Установка статического маршрута до gate на neo1. | admin@neo1# **set protocols static route 0.0.0.0/0 next-hop 10.10.10.2**<br>[edit] |
| Фиксация изменений. | admin@neo1# **commit**<br>[edit] |
| Включение туннеля DVMRP на neo2. | admin@neo2# **set protocols dvmrp tunnel mtun0**<br>[edit] |
| Установка локального конца туннеля DVMRP на neo2. | admin@neo2# **set protocols dvmrp tunnel mtun0 local 10.10.11.1**<br>[edit] |
| Установка удаленного конца туннеля DVMRP на neo2. | admin@neo2# **set protocols dvmrp tunnel mtun0 remote 10.10.10.1**<br>[edit] |
| Установка порога DVMRP по умолчанию для туннеля на neo2. | admin@neo2# **set protocols dvmrp tunnel mtun0 threshold**<br>[edit] |
| Установка статического маршрута до gate на neo2. | admin@neo2# **set protocols static route 0.0.0.0/0 next-hop 10.10.11.2**<br>[edit] |
| Фиксация изменений. | admin@neo2# **commit** |

```
[edit]
```

Вывод настройки интерфейсов на neo1.

```
admin@neo1# show interfaces
interfaces {
     ethernet eth3 {
          address 10.10.10.1/24
     }
     ethernet eth4 {
          address 192.168.50.1/24
     }
}
[edit]
```

Вывод настройки протоколов на neo1.

```
admin@neo1# show protocols
protocols {
     dvmrp {
          interface eth3 {
               threshold 5
          }
          interface eth4 {
               threshold 5
          }
          tunnel mtun0 {
               local 10.10.10.1
               remote 10.10.11.1
          }
     }
     static {
          route 0.0.0.0/0 {
               next-hop
10.10.10.2 {
               }
          }
```

```
          route 192.168.30.0/24 {
               next-hop
192.168.20.1 {
               }
          }
     }
}
[edit]
```

Вывод настройки интерфейсов на neo2.

```
admin@neo2# show interfaces
interfaces {
     ethernet eth3 {
          address 10.10.11.1/24
     }
     ethernet eth4 {
          address 192.168.60.1/24
     }
}
[edit]
```

Вывод настройки протоколов на neo2.

```
admin@neo2# show protocols
protocols {
     dvmrp {
          interface eth3 {
               threshold 5
          }
          interface eth4 {
               threshold 5
          } в
          tunnel mtun0 {
               local 10.10.11.1
               remote 10.10.10.1
          }
```

```
        }
        static {
            route 0.0.0.0/0 {
                next-hop
10.10.11.2 {
                }
            }
            route 192.168.30.0/24 {
                next-hop
192.168.20.1 {
                }
            }
        }
}
[edit]
```

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 **192.168.50.2/24**, шлюз по умолчанию **192.168.50.1**
- client1: IP-адрес **192.168.60.2/24**, шлюз по умолчанию **192.168.60.1**

## 12.4. 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` | 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 <число>` | Назначение метрики DVMRP для интерфейса. |
| `protocols dvmrp interface <интерфейс> threshold <число>` | 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_IP-адрес_туннеля>` | Указание локального IP-адреса туннеля DVMRP. |
| `protocols dvmrp tunnel <имя_туннеля> metric <метрика>` | Установка метрики для туннеля DVMRP. |
| `protocols dvmrp tunnel <имя_туннеля> remote <IP-адрес>` | Установка IP-адреса удаленного конца туннеля DVMRP. |
| `protocols dvmrp tunnel <имя_туннеля> threshold` | Установка порога (минимального времени жизни дейтаграмм) для туннеля DVMRP. |

| Эксплуатационные команды | |
|---|---|
| `show ip dvmrp` | Отображение статистики и таблиц маршрутизации протокола DVMRP. |

### 12.4.1. 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. 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.

### 12.4.2. 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 текст {
            netmask подсеть_ipv4
        }
    }
}
```

**Параметры**

*псевдоним*

Обязательный для формы **set**. Имя административно ограниченной подсети с многоадресной передачей.

*подсеть_ipv4*

Подсеть, с которой связывается псевдоним. В соответствии с RFC 2365, подсеть должна описываться значением 239.X.X.X/X.

**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.

### 12.4.3. 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 текст
    }
}
```

**Параметры**

*интерфейс*

Обязательный. 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.

### 12.4.4. protocols dvmrp interface <интерфейс> bound

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 текст {
               bound текст
          }
     }
}
```

**Параметры**

*интерфейс*

Обязательный. Имя интерфейса, с которым связывается административно ограниченная подсеть.

*псевдоним*

Обязательный (для формы **set**). 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.

## 12.4.5. 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 текст {
            disable
        }
    }
```

```
}
```

**Параметры**

*интерфейс*

Обязательный. 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.

## 12.4.6. protocols dvmrp interface <интерфейс> metric <число>

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 текст {
```

```
                    metric 1-31
                }
            }
        }
```

**Параметры**

*интерфейс*

Обязательный. Интерфейс, на котором назначается метрика.

*метрика*

Числовое значение метрики, назначаемой интерфейсу. Метрика не должна превосходить 31.

**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.

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.

## 12.4.7. protocols dvmrp interface <интерфейс> threshold <число>

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 текст {
               threshold 1-(2^32-1)
          }
     }
}
```

**Параметры**

*интерфейс*

Обязательный. Интерфейс, на котором назначается метрика.

*порог*

Числовое значение порога, назначаемого интерфейсу.

**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.

## 12.4.8. 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 mtun0-mtun9
    }
}
```

**Параметры**

*имя_туннеля*

Обязательный. Имя создаваемого туннеля.

**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.

## 12.4.9. 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 mtun0-mtun9 {
               bound текст
          }
     }
}
```

**Параметры**

*имя_туннеля*

Обязательный. Имя связываемого туннеля.

*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.

## 12.4.10. protocols dvmrp tunnel <имя_туннеля> local <локальный_IP-адрес_туннеля>

Указание локального IP-адреса туннеля DVMRP.

**Синтаксис**

**set protocols dvmrp tunnel** *имя_туннеля* **local** локальный_IP-адрес_туннеля

**delete protocols dvmrp tunnel** *имя_туннеля* **local**

**show protocols dvmrp tunnel** *имя_туннеля* **local**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
    dvmrp {
        tunnel mtun0-mtun9 {
            local ip-адрес
        }
    }
}
```

**Параметры**

*имя_туннеля*

Обязательный. Имя туннеля, для которого назначается локальный IP-адрес.

*локальный_IP-адрес_туннеля*

IP-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.

## 12.4.11. 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 mtun0-mtun9 {
            metric 1-10
        }
    }
}
```

**Параметры**

*имя_туннеля*

Обязательный. Имя туннеля, для которого назначается метрика.

*метрика*

Числовое значение метрики, назначаемой туннелю, число от 1 до 10 включительно. Метрика маршрута не должна превышать 31.

**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.

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.

## 12.4.12. protocols dvmrp tunnel <имя_туннеля> remote <IP-адрес>

Установка IP-адреса удаленного конца туннеля DVMRP.

**Синтаксис**

**set protocols dvmrp tunnel** *имя_туннеля* **remote** [*удаленный_IP-адрес_туннеля* | *имя_удаленного_узла*]

**delete protocols dvmrp tunnel** *имя_туннеля* **remote**

**show protocols dvmrp tunnel** *имя_туннеля* **remote**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
     dvmrp {
          tunnel mtun0-mtun9 {
               remote [ip-адрес | текст]
          }
     }
}
```

**Параметры**

*имя_туннеля*

Обязательный. Имя туннеля, для которого назначается удаленный IP-адрес.

*локальный_IP-адрес_туннеля*

IP-адрес удаленного конца туннеля DVMRP.

*имя_удаленного_узла*

Имя узла удаленного конца туннеля DVMRP.

**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.

## 12.4.13. protocols dvmrp tunnel <имя_туннеля> threshold <число>

Установка порога (минимального времени жизни дейтаграмм) для туннеля DVMRP.

**Синтаксис**

**set protocols dvmrp tunnel** *имя_туннеля* **threshold** *число*

**delete protocols dvmrp tunnel** *имя_туннеля* **threshold**

**show protocols dvmrp tunnel** *имя_туннеля* **threshold**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
protocols {
    dvmrp {
        tunnel mtun0-mtun9 {
            threshold 1-(2^32-1)
        }
    }
}
```

**Параметры**

*имя_туннеля*

Обязательный. Имя туннеля, для которого назначается порог.

*порог*

Числовое значение порога, назначаемого туннелю.

**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.

## 12.4.14. show ip dvmrp

Отображение статистики и таблиц маршрутизации протокола DVMRP.

**Синтаксис**

**show ip dvmrp**

**Режим интерфейса**

Эксплуатационный режим

**Ветвь конфигурации**

Отсутствует.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует

**Указания по использованию**

Команда используется для отображения статистики и таблиц

маршрутизации протокола DVMRP на данном маршрутизаторе.

# 13. ПРЕОБРАЗОВАНИЕ СЕТЕВЫХ АДРЕСОВ (NAT)

## 13.1. Обзор технологии NAT

В этом разделе описано, как настроить преобразование сетевых адресов (NAT) в системе.

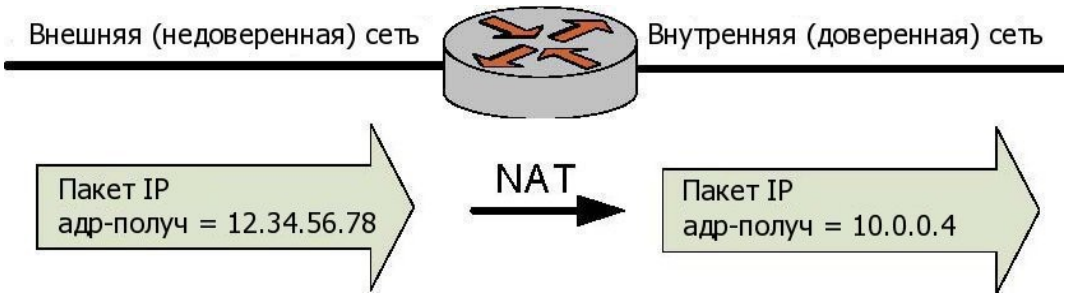
В этом разделе рассматриваются следующие вопросы:

- Краткий обзор технологии NAT.
- Преимущества NAT.
- Виды NAT.
- Взаимодействие между технологией NAT, маршрутизацией, межсетевым экраном и DNS.
- Правила NAT.
- Настройка вида правила NAT.
- Фильтры на основе протокола, адреса отправителя и адреса получателя.
- Преобразование адреса: “внутренние” и “внешние” адреса.
- “Входные” и “Выходные” интерфейсы.

### 13.1.1. 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 20 - 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).

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 со 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.

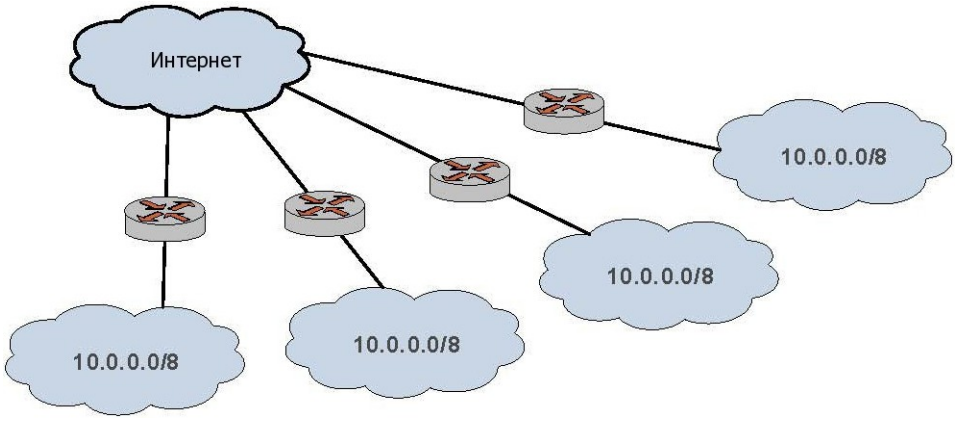
### 13.1.2. Преимущества NAT

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 21.

*Рисунок 21 - Повторное использование адресного пространства*




- NAT позволяет повысить уровень безопасности.

*Рисунок 22 - Совместное использование NAT и межсетевого экрана*

- 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.
- 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.

## 13.1.3. Виды NAT

Существует три основных вида преобразования сетевых адресов (NAT):

- Преобразование сетевого адреса отправителя. Оно также называется SNAT. “Маскировка” - частный случай SNAT.
- Преобразование сетевого адреса получателя. Оно также называется DNAT.
- Двунаправленное преобразование сетевых адресов. Двунаправленное преобразование сетевых адресов является результатом одновременной настройки SNAT и DNAT.

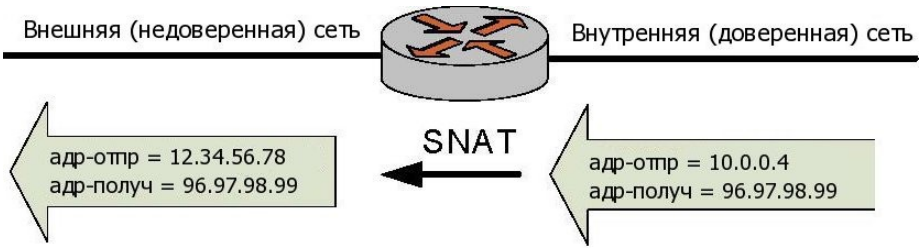
### *13.1.3.1. Преобразование сетевого адреса отправителя (SNAT)*

***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 23. 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 23 - Преобразование сетевого адреса отправителя (SNAT)*

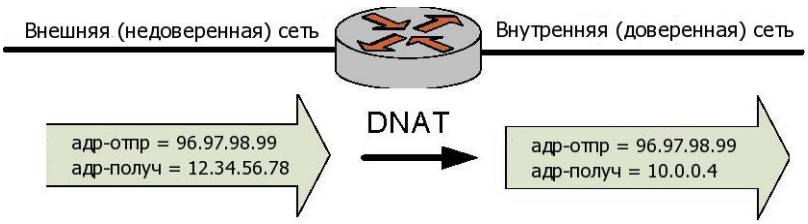



### *13.1.3.2. Преобразование сетевого адреса получателя (DNAT)*

***ПРИМЕЧАНИЕ** DNAT выполняется перед маршрутизацией*

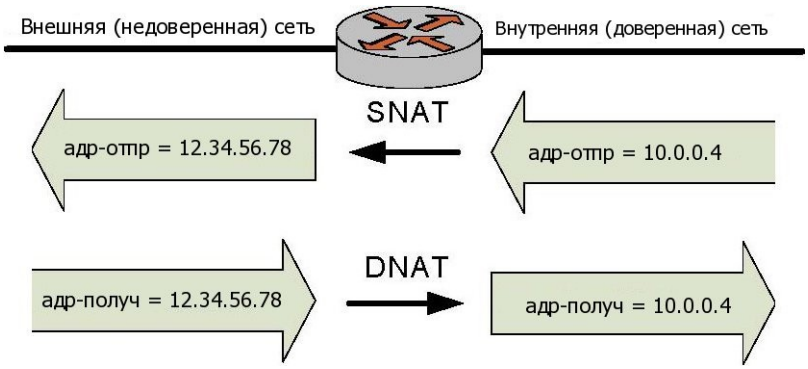
В то время как SNAT изменяет адрес отправителя сетевых пакетов, DNAT изменяет адрес получателя сетевых пакетов при их прохождении через систему. DNAT обычно используется в тех случаях, когда общедоступному узлу требуется инициировать сеанс связи со внутренним (частным) узлом; например, когда подписчик получает доступ к новостному серверу, как представлено на рисунке 24.

*Рисунок 24 - Преобразование сетевых адресов получателя (DNAT)*



#### *13.1.3.3. Двунаправленное преобразование сетевых адресов*

*Рисунок 25 - Двунаправленное преобразование сетевых адресов*




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 25 приведен пример двунаправленного NAT.

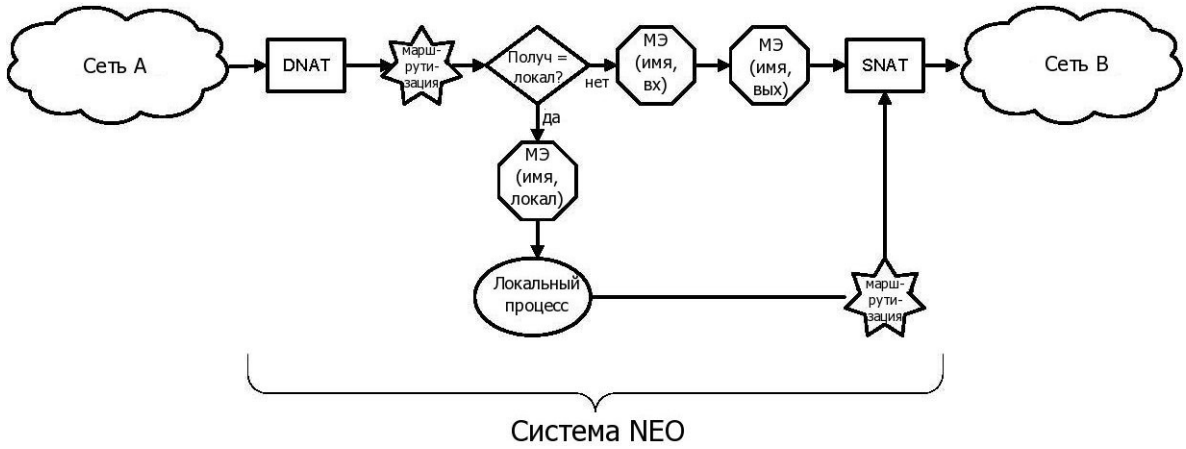
### 13.1.4. Совместное использование NAT, маршрутизации, межсетевого экрана и DNS

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.

На рисунке 26 представлена схема прохождения трафика при использовании NAT, маршрутизации и межсетевого экрана.

*Рисунок 26 - Прохождение трафика через систему Altell NEO*




### *13.1.4.1. Совместное использование NAT и маршрутизации*

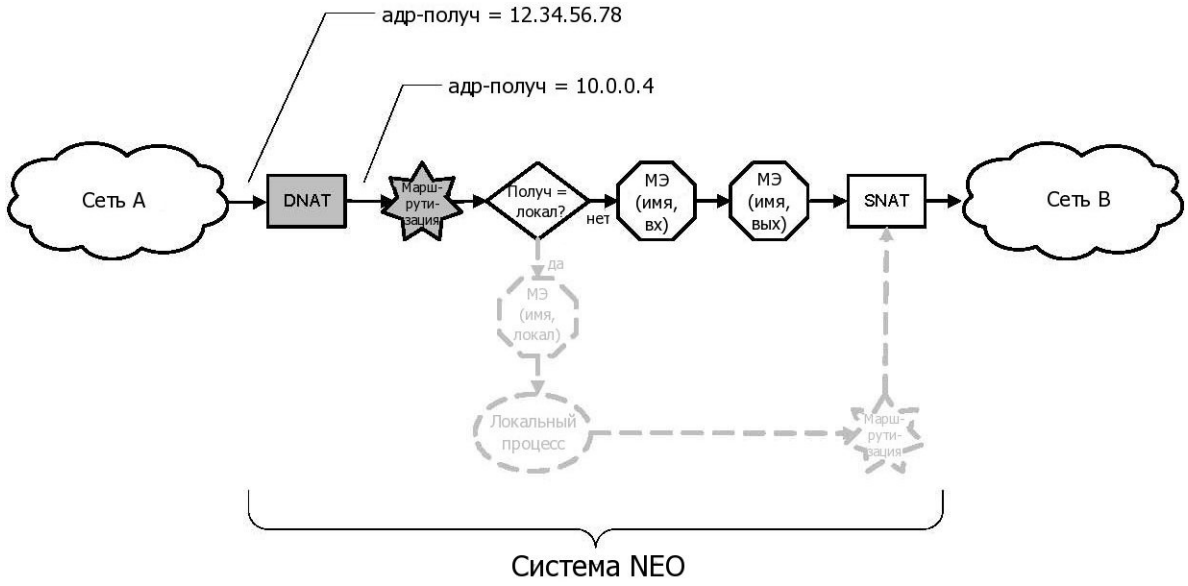
При совместном использовании NAT и маршрутизации необходимо учитывать влияние правил DNAT и SNAT на решения о маршрутизации. Типовые схемы, приведенные в этом разделе, раскрывают данный вопрос.

#### 13.1.4.1.1. Схема 1a: DNAT—Пакеты, проходящие через систему

***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; см. рисунок 27.

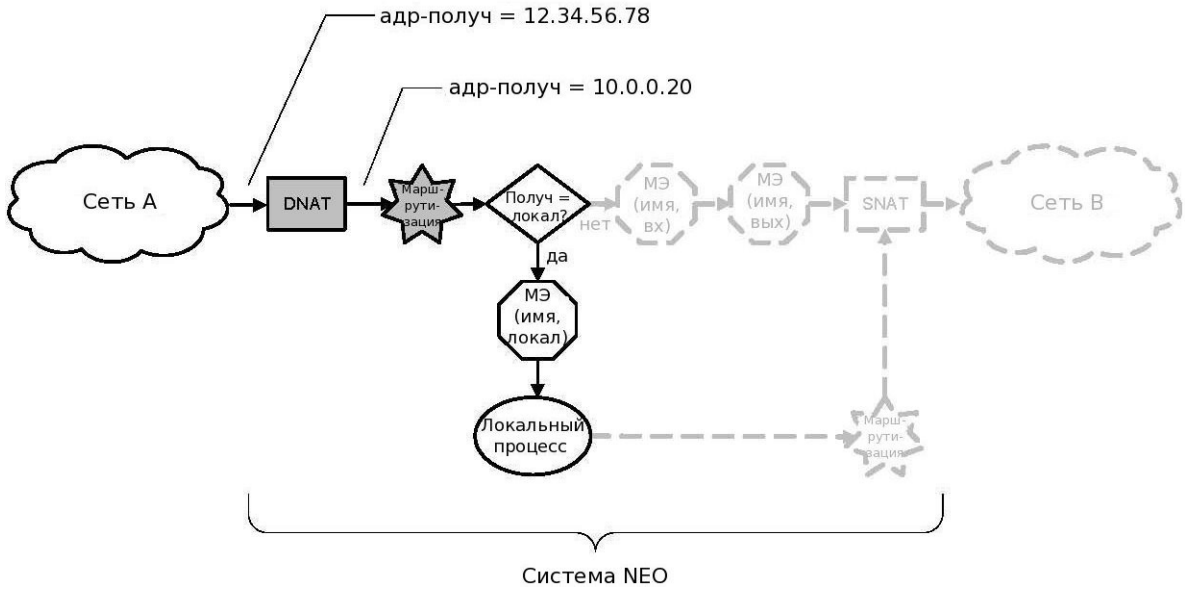
*Рисунок 27 - Решения о маршрутизации при прохождении DNAT*




#### 13.1.4.1.2. Схема 1б: DNAT— Пакеты, предназначенные для системы Altell NEO

Аналогичная ситуация происходит, когда сетевые пакеты предназначаются для локальной системы. В этой схеме пакеты предназначены для одного из локальных процессов системы.

*Рисунок 28 - Решения о маршрутизации при использовании DNAT для пакетов, предназначенных системе Altell NEO*



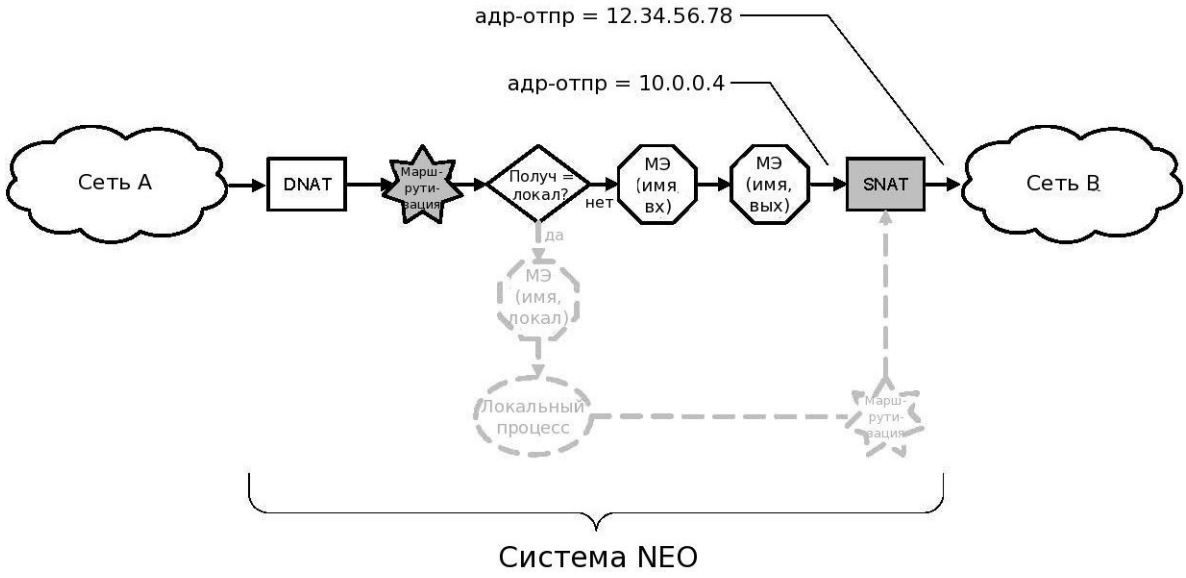

Опять же, так как преобразование DNAT применяется к сетевым пакетам *перед* принятием решения о маршрутизации, принятие решения о маршрутизации осуществляется на основе *измененных* адресов получателя — а *не* первоначальных адресов (рис. 28).

#### 13.1.4.1.3. Схема 2a: SNAT— Пакеты, проходящие через систему Altell NEO

***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; см. рисунок 29.

*Рисунок 29 - Решения о маршрутизации при прохождении SNAT*

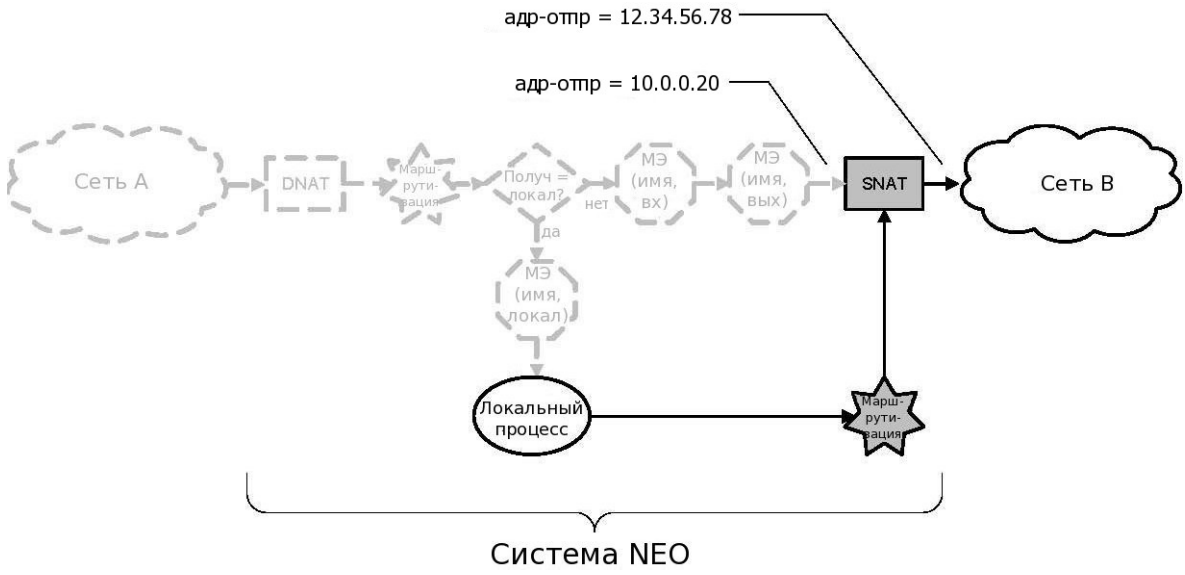



#### 13.1.4.1.4. Схема 2б: SNAT— Пакеты, отправителем которых является Altell NEO

В этой схеме сетевые пакеты отправляются процессом внутри системы Altell NEO.

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; см. рис. 30.

*Рисунок 30 - Решения о маршрутизации при использовании SNAT для пакетов, отправленных системой Altell NEO*




### *13.1.4.2. Совместное использование NAT и межсетевого экранирования*

При совместном использовании NAT и межсетевого экрана важно иметь представление о последовательности обработки сетевого трафика данными службами. В частности, следует иметь в виду, что наборы правил "**name**" межсетевого экрана и наборы правил "**modify**" межсетевого экрана исполняются в различных точках потока сетевого трафика. Типовые схемы, приведенные в этом разделе, раскрывают этот вопрос.

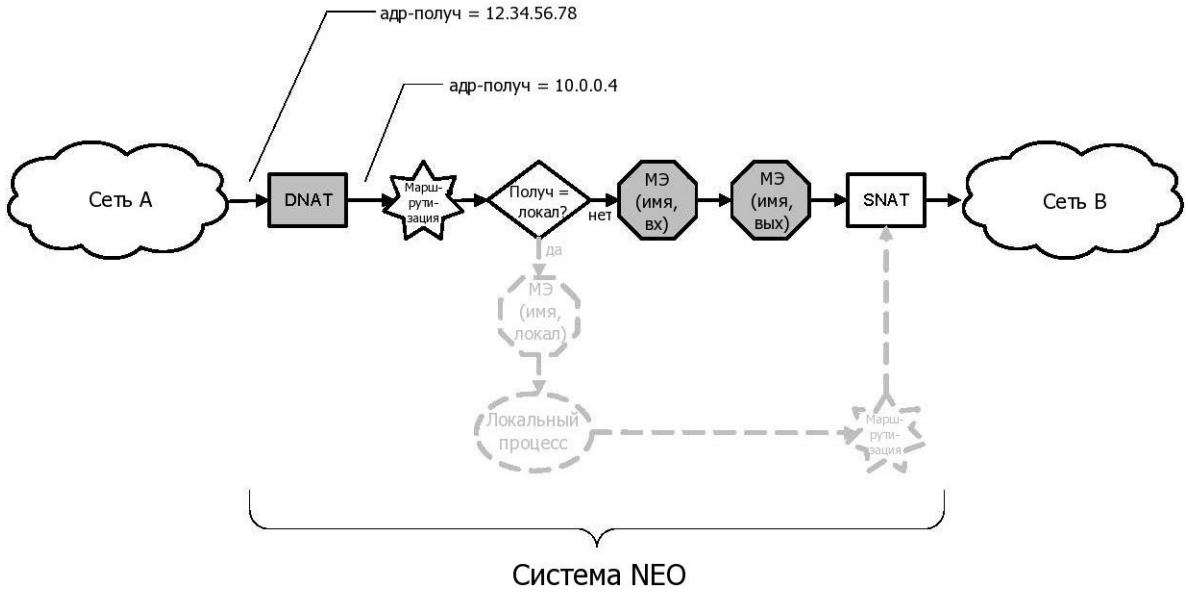
#### 13.1.4.2.1. Схема 1a: DNAT—Пакеты, проходящие через систему Altell NEO

В этой схеме сетевые пакеты отправлены из сети A и проходят через систему Altell NEO.

Для модифицирующих правил межсетевого экрана (наборы правил "**modify**"), применяемых ко входящим сетевым пакетам, полученным на интерфейсе, правила межсетевого экрана применяются *до* осуществления преобразования сетевого адреса получателя (то есть на основе *исходного (первоначального)* адреса получателя). Для наборов правил "**name**" межсетевого экрана, применяемых ко входящим пакетам на интерфейсе, правила межсетевого экрана применяются *после* осуществления преобразования сетевого адреса получателя (то есть на основе *измененного* адреса получателя).

Для правил “**modify**” и правил “**name**” межсетевого экрана, применяемых к исходящим пакетам на интерфейсе, правила межсетевого экрана применяются *после* осуществления преобразования сетевого адреса получателя (то есть, на основе *измененного* адреса получателя); рис. 31.

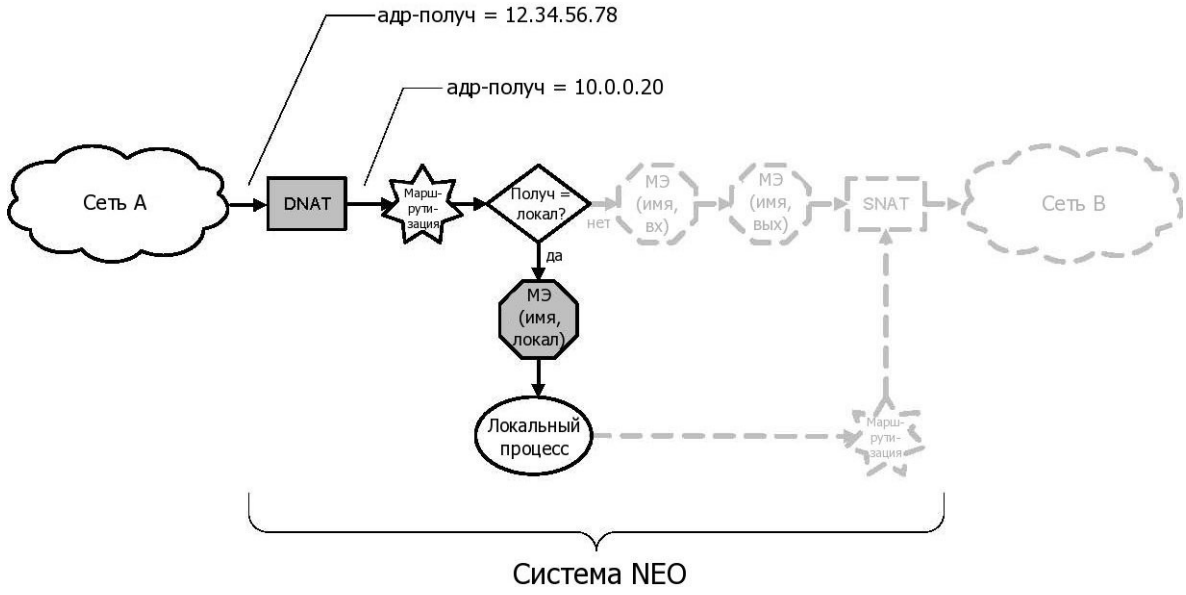
*Рисунок 31 - Решение МЭ при прохождении DNAT*




#### 13.1.4.2.2. Схема 1б: DNAT— Пакеты, предназначенные для системы Altell NEO

В этой схеме пакеты предназначены для одного из процессов в системе Altell NEO. Следует отметить, что наборы правил “**modify**” межсетевого экрана не применяются к пакетам, предназначенным для локальной системы; применяются только правила “**name**”. Когда к пакетам, предназначенным для локальной системы, применяются правила "**name**" межсетевого экрана, они применяются *после* осуществления преобразования сетевого адреса получателя (то есть, на основе *измененного* адреса получателя); рис. 32.

*Рисунок 32 - Решения МЭ при использовании DNAT для пакетов, предназначенных системе Altell NEO*

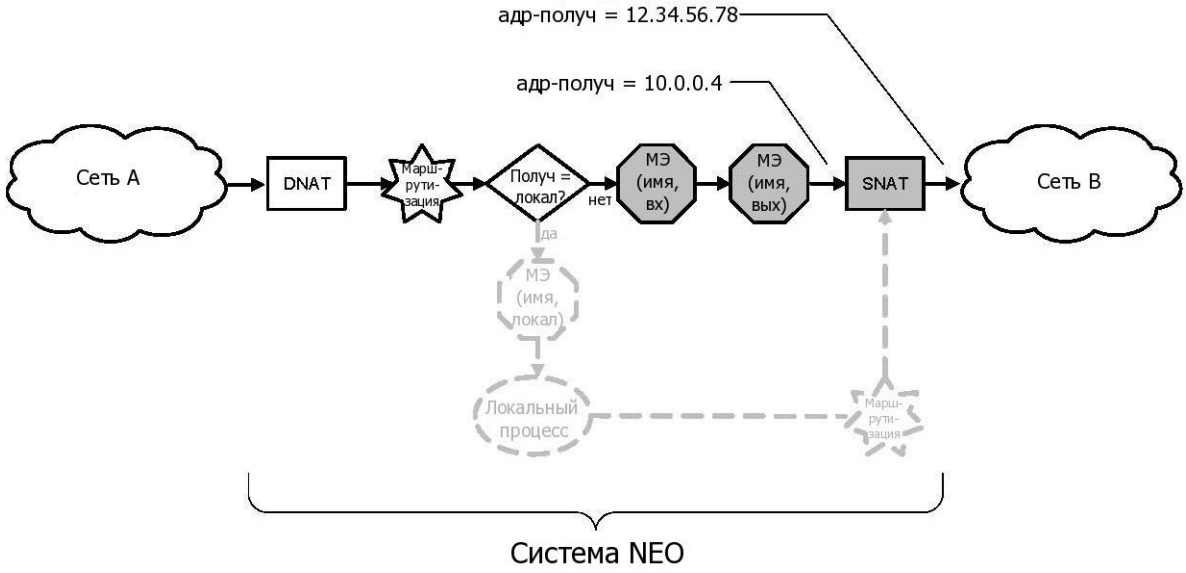



#### 13.1.4.2.3. Схема 2a: SNAT— Пакеты, проходящие через систему

***ПРИМЕЧАНИЕ*** *Правила SNAT осуществляются на основе исходного (первоначального) адреса отправителя.*

Правила межсетевого экрана применяются до осуществления преобразования сетевого адреса отправителя. Это означает, что решения МЭ принимаются на основе *исходного (первоначального)* адреса отправителя — а не измененного адреса отправителя. Такой порядок выполнения справедлив как для правил "**modify**", так и для правил "**name**" межсетевого экрана, как для входящих, так и для исходящих пакетов; см. рис. 33.

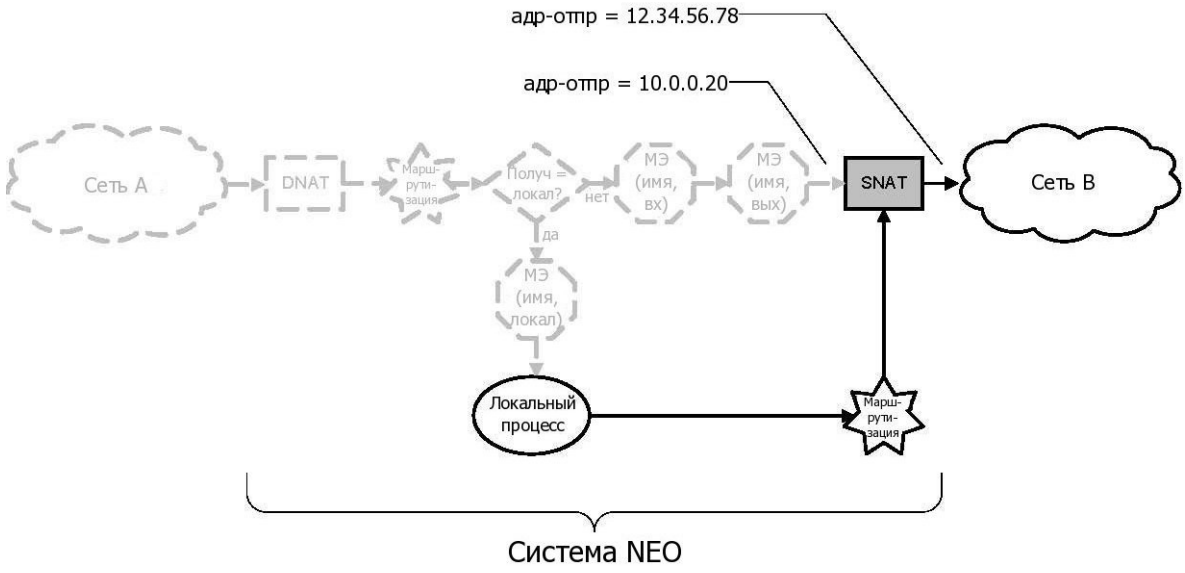
*Рисунок 33 - Решения МЭ при использовании SNAT для пакетов, проходящих через систему Altell NEO*




#### 13.1.4.2.4. Схема 2б: SNAT— Пакеты, отправителем которых является Altell NEO

В данной схеме сетевые пакеты отправляются одним из процессов в системе Altell NEO. Следует отметить, что так как сеанс инициируется внутренним процессом, к исходящим пакетам применяются только правила “**modify**” межсетевого экрана. Они применяются к *исходному (первоначальному)* адресу отправителя, а не *измененному* адресу. Правила “**name**” межсетевого экрана не применяются.

*Рисунок 34 - Решения МЭ при использовании SNAT для пакетов, отправленных системой Altell NEO*




#### *13.1.4.3. Совместное использование NAT и DNS*

Технологии NAT и DNS могут использоваться совместно, в том числе для управления балансировкой нагрузки. Имеются дополнительные коммутаторы балансировки нагрузки, которые функционируют на основе протоколов высших уровней (уровни 4-7). Например, в крупном банке могу использоваться веб-серверы с транзакционной балансировкой нагрузки между ними.

В этих случаях следует выполнять настройку преобразования сетевых адресов с особой осторожностью для получения желаемых результатов. Обсуждение DNS и балансировки нагрузки выходит за рамки этого раздела.

## 13.2. 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.

***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.

Для создания или изменения правила NAT используются команды **set** и узел конфигурации **service nat** с указанием номера, который будет являться идентификатором правила; см. пример 13.1:

*Пример 13.1 - Создание правила NAT*

```
admin@neo#set service nat rule 10
```

## 13.2.1. Настройка вида правила 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 13.2 определяется правило SNAT с номером 10.

*Пример 13.2 - Создание правила преобразования сетевого адреса отправителя (SNAT)*

```
admin@neo#set service nat rule 10 type source
```

## 13.2.2. Фильтры на основе протокола, адреса отправителя и адреса получателя

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**).

### *13.2.2.1. 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 13.3 настраивается применение правила 10 к пакетам протокола TCP. Преобразование сетевых адресов будет осуществляться только для пакетов протокола TCP.

*Пример 13.3 - Фильтрация пакетов на основе протоколов*

```
admin@neo#set service nat rule 10 protocols tcp
```

#### 13.2.2.2. Фильтр на основе адреса 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 13.4 настраивается применение правила 10 только к пакетам, адрес отправителя которых равен 10.0.0.4.

*Пример 13.4 - Фильтрация на основе адреса отправителя*

```
admin@neo#set service nat rule 10 source address 10.0.0.4
```

В примере 13.5 настраивается применение правила 15 к пакетам, адрес отправителя которых принадлежит сети 10.0.0.0/24, а номер сетевого порта отправителя равен 80.

*Пример 13.5 - Фильтрация на основе сети отправителя и номера сетевого порта*

```
admin@neo#set service nat rule 15 source address 10.0.0.0/24
admin@neo#set service nat rule 15 source port 80
```

#### 13.2.2.3. 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 13.6 настраивается применение правила 20 к пакетам, адрес получателя которых равен 12.34.56.78.

*Пример 13.6 - Фильтрация на основе адреса получателя*

```
admin@neo#set service nat rule 20 destination address 12.34.56.78
```

Фильтрация может выполняться не только на основе адреса получателя, но и на основе его номера порта.

### 13.2.3. Преобразование адреса: “внутренние” и “внешние” адреса

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.

#### *13.2.3.1. 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 13.7 настраивается применение правила 20, которое будет подставлять адрес 10.0.0.4 в качестве IP-адреса входящего пакета для пакетов, удовлетворяющих условиям, определенным в правиле.

*Пример 13.7 - Установка внутреннего IP-адреса для настройки DNAT*

```
admin@neo#set service nat rule 20 inside-address address 10.0.0.4
```

В примере 13.8 настраивается применение правила 25, которое будет подставлять адреса от 10.0.0.0 до 10.0.0.3 в качестве диапазона IP-адресов получателя для входящих пакетов, удовлетворяющих условиям правила.

*Пример 13.8 - Установка диапазона внутренних адресов для настройки DNAT*

```
admin@neo#set service nat rule 25 inside-address 10.0.0.0-10.0.0.3
```

#### *13.2.3.2. 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 13.9 настраивается применение правила 10, которое осуществляет подстановку адреса 12.34.56.78 в качестве IP-адреса отправителя для сетевых пакетов, удовлетворяющих условиям правила.

*Пример 13.9 - Установка внешнего адреса для настройки SNAT*

```
admin@neo#set service nat rule 10 outside-address address
12.34.56.78
```

В примере 13.10 настраивается применение правила 15 для подстановки адресов от 12.34.56.64 до 12.34.56.79 в качестве IP-адресов отправителя для исходящих пакетов, удовлетворяющих критерию правила.

*Пример 13.10 - Установка диапазона внешних адресов для настройки SNAT*

```
admin@neo#set service nat rule 15 outside-address 12.34.56.64-
12.34.56.79
```

### 13.2.4. “Входные” и “Выходные” интерфейсы

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 13.11 для правила 20 указывается, что для принятия входящего трафика будет прослушиваться интерфейс eth0.

*Пример 13.11 - Установка входного интерфейса для правила DNAT*

```
admin@neo#set service nat rule 20 inbound-interface eth0
```

В примере 13.12 для правила 10 устанавливается отправка исходящего трафика через интерфейс eth1.

*Пример 13.12 - Установка выходного интерфейса для правила SNAT*

```
admin@neo#set service nat rule 10 outbound-interface eth1
```

## 13.3. 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:

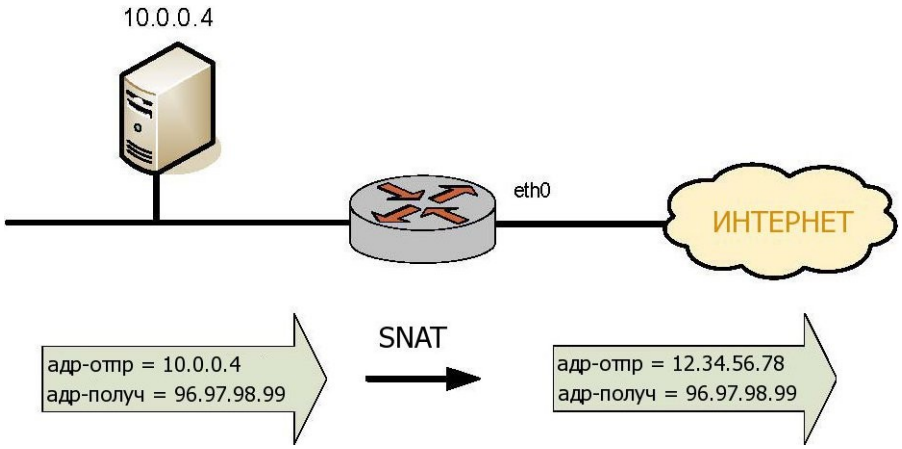
- Преобразование сетевого адреса отправителя (один к одному).
- Преобразование сетевого адреса отправителя (многие к одному).
- Преобразование сетевого адреса отправителя (многие ко многим).
- Преобразование сетевого адреса отправителя (один ко многим).
- Маскировка.
- Преобразование сетевого адреса получателя (один к одному).
- Преобразование сетевого адреса получателя (один ко многим).
- Двунаправленное преобразование сетевых адресов.
- Если подключения инициируются только из сети 10.0.0.0/24, тогда необходимо только правило 10. Если подключения инициируются только из сети 11.22.33.0/24 , тогда необходимо только правило 20.
- "Исключающий" параметр.

### 13.3.1. Преобразование сетевого адреса отправителя (один к одному)

На рисунке 35 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 35 - Настройка SNAT (один к одному)*



Для настройки преобразования сетевых адресов в соответствии с данным рисунком нужно выполнить следующие действия в режиме настройки.

*Пример 13.13 - Настройка SNAT (один к одному)*

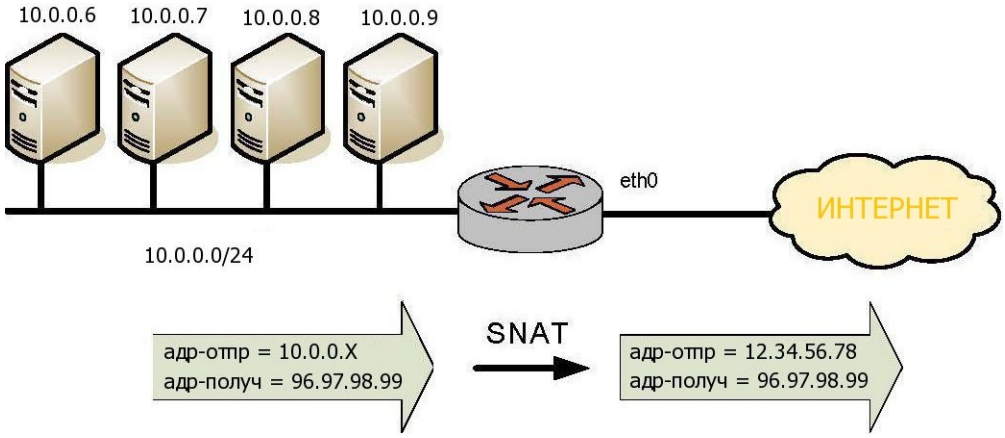
| Действие | Команда |
|---|---|
| Создание правила 10. Правило 10 является правилом преобразования сетевого адреса отправителя (SNAT). | admin@neo# **set service nat rule 10 type source**<br>[edit] |
| Применение правила к сетевым пакетам, отправленным с узла 10.0.0.4. | admin@neo# **set service nat rule 10 source address 10.0.0.4**<br>[edit] |
| Отправка трафика через интерфейс eth0. Адрес 12.34.56.78 используется в качестве адреса отправителя для исходящих сетевых пакетов. Следует учесть, что внешний адрес должен быть одним из адресов, назначенных выходному интерфейсу. | admin@neo# **set service nat rule 10 outbound-interface** eth0<br>[edit]<br>admin@neo# **set service nat rule 10 outside-address address 12.34.56.78**<br>[edit] |
| Фиксация изменения. | admin@neo# **commit**<br>[edit] |
| Вывод настройки. | admin@neo# **show service nat rule 10**<br>outbound-interface eth0<br>outside-address {<br>address 12.34.56.78<br>}<br>source {<br>address 10.0.0.4<br>}<br>type source |

```
[edit]
```

### 13.3.2. Преобразование сетевого адреса отправителя (многие к одному)

На рисунке 36 приведен пример преобразования сетевого адреса отправителя, где несколько различных “внутренних” адресов динамически заменяются на один “внешний” адрес. В этом примере все узлы подсети 10.0.0.0/24 будут использовать один и тот же внешний адрес отправителя.

*Рисунок 36 - Настройка SNAT (многие к одному)*




Для настройки преобразования сетевых адресов в соответствии с данным рисунком нужно выполнить следующие действия в режиме настройки.

*Пример 13.14 - Настройка SNAT (многие к одному)*

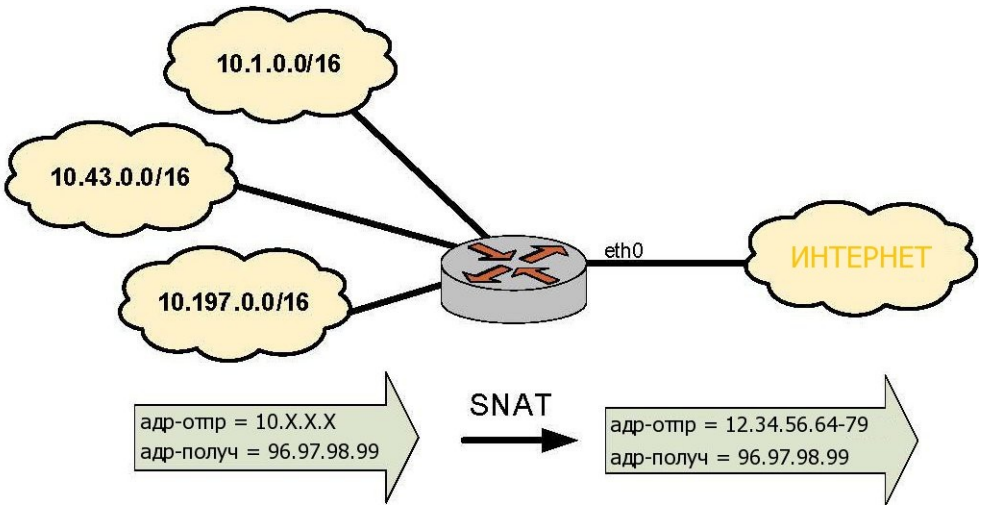
| Действие | Команда |
|---|---|
| Создание правила 10. Правило 10 является правилом преобразования сетевого адреса отправителя (SNAT). | `admin@neo# set service nat rule 10 type source`<br>`[edit]` |
| Применение данного правила к пакетам, которые были отправлены любым узлом сети 10.0.0.0/24. | `admin@neo# set service nat rule 10 source address 10.0.0.0/24`<br>`[edit]` |
| Отправка трафика через интерфейс eth0. Адрес 12.34.56.78 используется в | `admin@neo# set service nat rule 10 outbound-interface eth0` |

| | |
|---|---|
| качестве адреса отправителя для исходящих сетевых пакетов. Следует учесть, что внешний адрес должен быть одним из адресов, определенных на выходном интерфейсе. | [edit]<br>admin@neo# **set service nat rule 10 outside-address address 12.34.56.78**<br>[edit] |
| Фиксация изменения. | admin@neo# **commit**<br>[edit] |
| Вывод настройки. | admin@neo# **show service nat rule 10**<br> outbound-interface eth0<br> outside-address {<br>  address 12.34.56.78 }<br> source {<br>  address 10.0.0.0/24<br> }<br> type source<br>[edit] |

### 13.3.3. Преобразование сетевого адреса отправителя (многие ко многим)

В преобразованиях типа "многие ко многим" набор частных IP-адресов заменяется на набор общедоступных адресов. На рисунке 37 большое пространство частных адресов (/8) преобразуется в несколько внешних адресов (/28 или /30).

*Рисунок 37 - Настройка SNAT (многие ко многим)*




Для настройки преобразования сетевых адресов в соответствии с данным рисунком нужно выполнить следующие действия в режиме настройки.

*Пример 13.15 - Настройка SNAT (многие ко многим)*

| Действие | Команда |
|---|---|
| Создание правила 10. Правило 10 является правилом преобразования сетевого адреса отправителя (SNAT). | `admin@neo# set service nat rule 10 type source`<br>`[edit]` |
| Применение данного правила к пакетам, которые были отправлены любым узлом сети 10.0.0.0/8. | `admin@neo# set service nat rule 10 source address 10.0.0.0/8`<br>`[edit]` |
| Отправка сетевого трафика через интерфейс eth0. Выбор адреса в диапазоне от 12.34.56.64 до 12.34.56.79 в качестве адреса отправителя исходящих пакетов. Следует отметить, что внешние адреса должны быть определены на выходном интерфейсе. | `admin@neo# set service nat rule 10 outbound-interface eth0`<br>`[edit]`<br>`admin@neo# set service nat rule 10 outside-address address 12.34.56.64-12.34.56.79`<br>`[edit]` |

Фиксация изменения.

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

Вывод настройки.

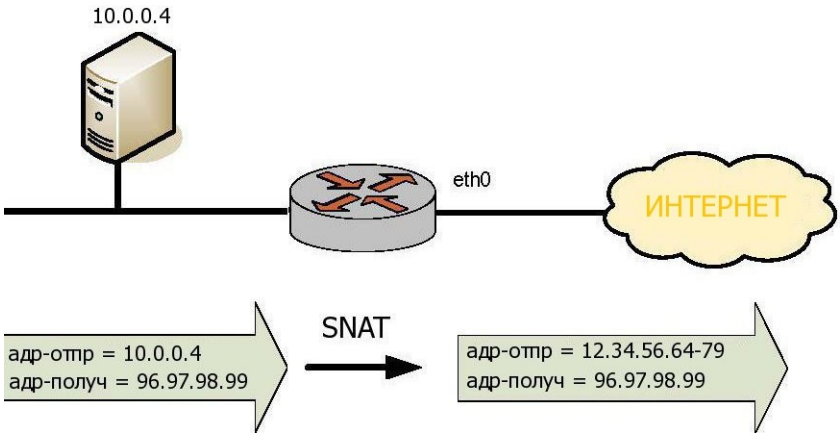
```
admin@neo# show service nat rule
10
 outbound-interface eth0
 outside-address {
     address 12.34.56.64-
12.34.56.79
 }
 source {
     address 10.0.0.0/8
 }
 type source
[edit]
```

### 13.3.4. 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; рис. 38.

Для настройки преобразования сетевых адресов в соответствии с данным рисунком нужно выполнить следующие действия в режиме настройки.

*Рисунок 38 - Настройка SNAT (один ко многим)*




*Пример 13.16 - Преобразование сетевого адреса отправителя (один ко многим)*

| Действие | Команда |
|---|---|
| Создание правила 10. Правило 10 является правилом преобразования сетевого адреса отправителя (SNAT). | admin@neo# **set service nat rule 10 type source**<br>[edit] |
| Применение правила к сетевым пакетам, отправленным с узла 10.0.0.4. | admin@neo# **set service nat rule 10 source address 10.0.0.4**<br>[edit] |
| Отправка сетевого трафика через интерфейс eth0. Выбор адреса в диапазоне от 12.34.56.64 до 12.34.56.79 в качестве адреса отправителя исходящих пакетов. Следует отметить, что внешние адреса должны быть определены на выходном интерфейсе. | admin@neo# **set service nat rule 10 outbound-interface eth0**<br>[edit]<br>admin@neo# **set service nat rule 10 outside-address address 12.34.56.64-12.34.56.79**<br>[edit] |
| Фиксация изменения. | admin@neo# **commit**<br>[edit] |
| Вывод настройки. | admin@neo# **show service nat rule** |

```
10
 outbound-interface eth0
 outside-address {
     address 12.34.56.64-
12.34.56.79
 }
 source {
     address 10.0.0.4
 }
 type source
[edit]
```

### 13.3.5. Маскировка

Маскировка при преобразовании сетевых адресов используется в тех случаях, когда устройствам в локальной сети назначены частные IP-адреса, и данные устройства расположены за маршрутизатором, имеющим внешний интерфейс с назначенным общедоступным IP-адресом. При использовании правил "маскировки" весь сетевой трафик, исходящий из частной сети, "маскируется" таким образом, что для узлов внешней сети сетевые пакеты выглядят так же, как если бы они были отправлены с единственного общедоступного (public) IP-адреса. Этот 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.

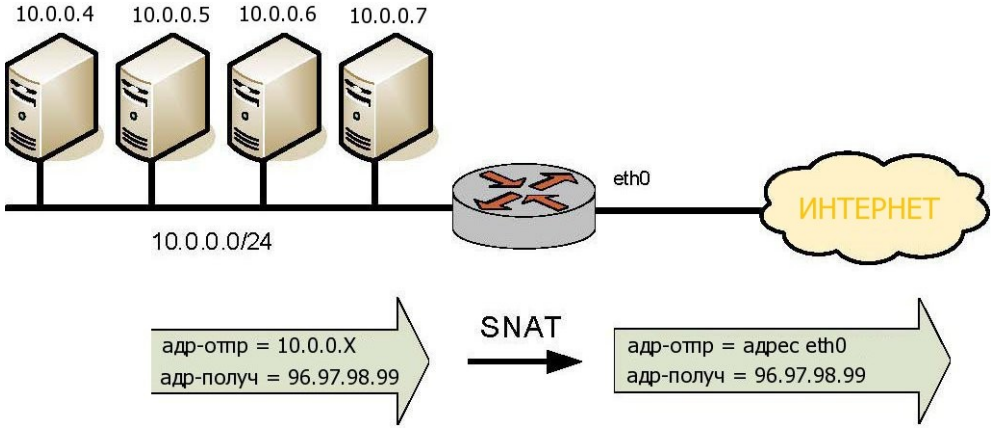
Правила "маскировки" состоят из условий, на основе которых осуществляется проверка соответствия:

- 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 39 приведен пример использования "маскировки".

*Рисунок 39 - Маскировка*




Для настройки преобразования сетевых адресов в соответствии с данным рисунком нужно выполнить следующие действия в режиме настройки.

*Пример 13.17 - Маскировка*

| Действие | Команда |
|---|---|
| Создание правила 10. Правило 10 является правилом преобразования сетевого адреса отправителя (SNAT). | `admin@neo# set service nat rule 10 type masquerade [edit]` |
| Применение данного правила к пакетам, которые были отправлены любым узлом сети 10.0.0.0/24. | `admin@neo# set service nat rule 10 source address 10.0.0.0/24 [edit]` |
| Отправка сетевого трафика через интерфейс eth0. Использование IP- | `admin@neo# set service nat rule 10 outbound-interface eth0` |

| | |
|---|---|
| адреса выходного интерфейса в качестве внешнего адреса. | `[edit]` |
| Фиксация изменения. | `admin@neo# commit`<br>`[edit]` |
| Вывод настройки. | `admin@neo# show service nat rule 10`<br>`  outbound-interface eth0`<br>`  source {`<br>`  address 10.0.0.0/24`<br>`  }`<br>`  type masquerade`<br>`[edit]` |

## 13.3.6. Преобразование сетевого адреса получателя (один к одному)

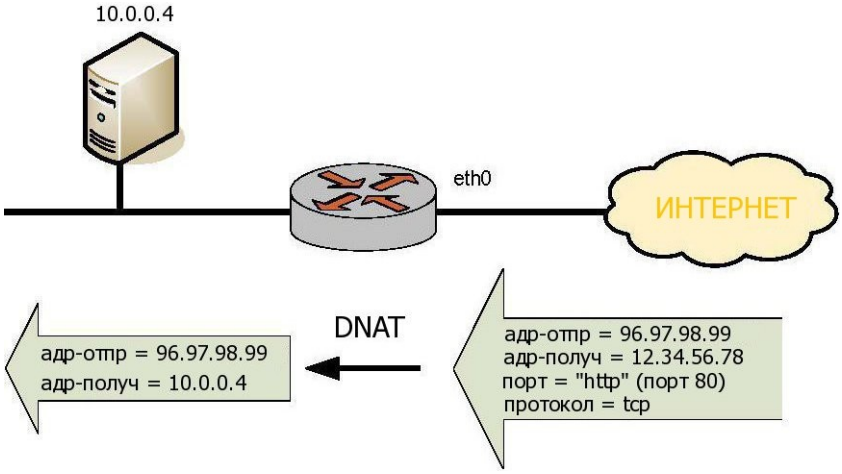
Преобразование сетевого адреса получателя (DNAT) используется только в тех случаях, когда необходимо принимать входящий трафик.

### *13.3.6.1. 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, рис. 40.

Для настройки преобразования сетевых адресов в соответствии с данным рисунком нужно выполнить следующие действия в режиме настройки.

*Рисунок 40 - Настройка DNAT (один к одному)*




*Пример 13.18 - Преобразование сетевого адреса получателя (один к одному)*

| Действие | Команда |
|---|---|
| Создание правила 10. Правило 10 является правилом преобразования сетевого адреса получателя (DNAT). | admin@neo# **set service nat rule 10 type destination**<br>[edit] |
| Применение данного правила ко всем входящим пакетам TCP на интерфейсе eth0 для адреса 12.34.56.78 и порта HTTP. | admin@neo# **set service nat rule 10 inbound-interface eth0**<br>[edit]<br>admin@neo# **set service nat rule 10 destination address 12.34.56.78**<br>[edit]<br>admin@neo# **set service nat rule 10 protocols tcp**<br>[edit]<br>admin@neo# **set service nat rule 10 destination port http**<br>[edit] |
| Пересылка трафика на адрес 10.0.0.4. | admin@neo# **set service nat rule 10 inside-address address 10.0.0.4**<br>[edit] |
| Фиксация изменения. | admin@neo# **commit**<br>[edit] |

Вывод настройки.

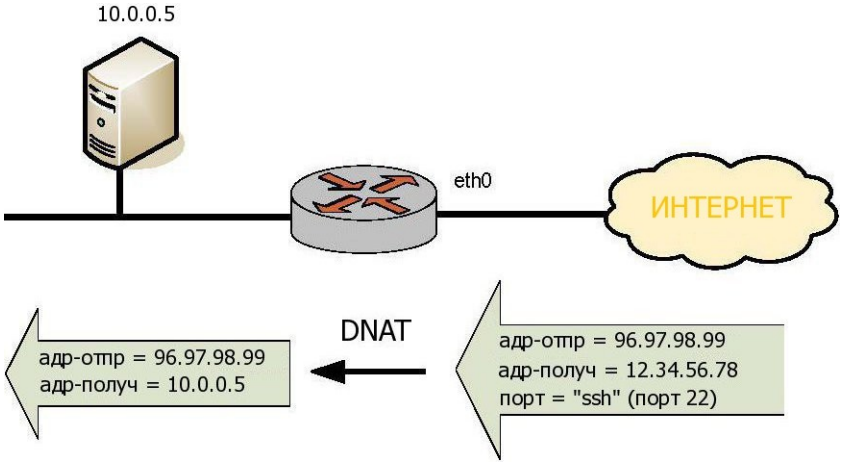
```
admin@neo# show service nat rule 10
destination {
     address 12.34.56.78
     port http
 }
 inbound-interface eth0
 inside-address {
     address 10.0.0.4
 }
 protocols tcp
 type destination
[edit]
```

### 13.3.6.2. 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, рис. 41.

Для настройки преобразования сетевых адресов в соответствии с данным рисунком нужно выполнить следующие действия в режиме настройки.

*Рисунок 41 - Настройка DNAT (один к одному) - фильтрация по имени порта*



*Пример 13.19 - Настройка DNAT (один к одному) - фильтрация по имени порта*

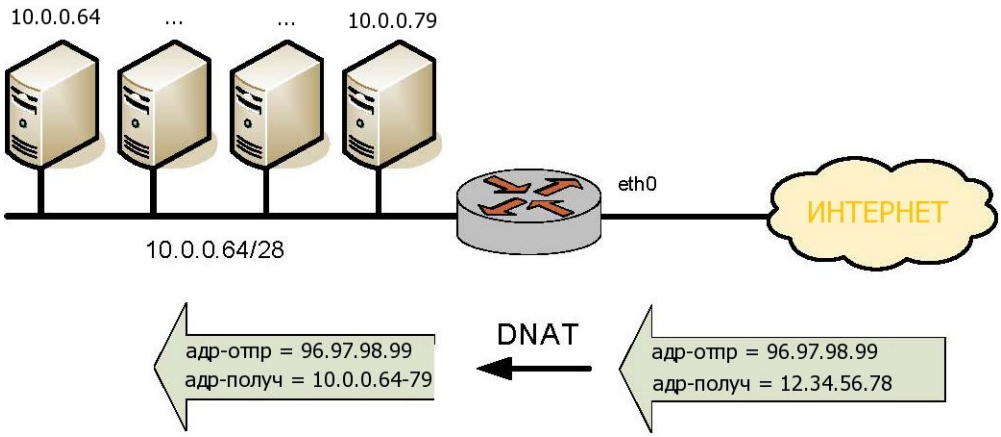
| Действие | Команда |
|---|---|
| Создание правила 10. Правило 10 является правилом преобразования сетевого адреса получателя (DNAT). | admin@neo# **set service nat rule 10 type destination**<br>[edit] |
| Применение данного правила ко всем входящим пакетам на интерфейсе eth0 для адреса 12.34.56.78 и порта SSH. | admin@neo# set **service nat rule 10 inbound-interface eth0**<br>[edit]<br>admin@neo# **set service nat rule 10 protocol tcp**<br>[edit]<br>admin@neo# **set service nat rule 10 destination port ssh**<br>[edit]<br>admin@neo# **set service nat rule 10 destination address 12.34.56.78**<br>[edit] |
| Пересылка трафика на адрес 10.0.0.5. | admin@neo# **set service nat rule 10 inside-address address 10.0.0.5**<br>[edit] |
| Фиксация изменения. | admin@neo# **commit**<br>[edit] |
| Вывод настройки. | admin@neo# show service nat rule 10<br>destination {<br>address 12.34.56.78<br>port ssh<br>} |

```
inbound-interface eth0
inside-address {
address 10.0.0.5
}
protocols tcp
type destination
[edit]
```

### 13.3.7. 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 рис. 42.

*Рисунок 42 - Настройка DNAT (один ко многим)*




Для настройки преобразования сетевых адресов в соответствии с данным рисунком нужно выполнить следующие действия в режиме настройки.

*Пример 13.20 - Настройка DNAT (один ко многим)*

| Действие | Команда |
|---|---|
| Создание правила 10. Правило 10 является правилом преобразования сетевого адреса получателя (DNAT). | `admin@neo# set service nat rule 10 type destination`<br>`[edit]` |
| Применение данного правила на | `admin@neo# set service nat rule` |

| | |
|---|---|
| | **10 inbound-interface eth0**<br>[edit] |
| интерфейсе eth0 для адреса 12.34.56.78. | admin@neo# **set service nat rule 10 destination address 12.34.56.78**<br>[edit] |
| Пересылка трафика на адреса из диапазона от 10.0.0.64 до 10.0.0.79. | admin@neo# **set service nat rule 10 inside-address address 10.0.0.64-10.0.0.79**<br>[edit] |
| Фиксация изменения. | admin@neo# **commit**<br>[edit] |
| Вывод настройки. | admin@neo# **show service nat rule 10**<br>destination {<br>address 12.34.56.78<br>}<br>inbound-interface eth0<br>inside-address {<br>address 10.0.0.64-10.0.0.79<br>}<br>type destination<br>[edit] |

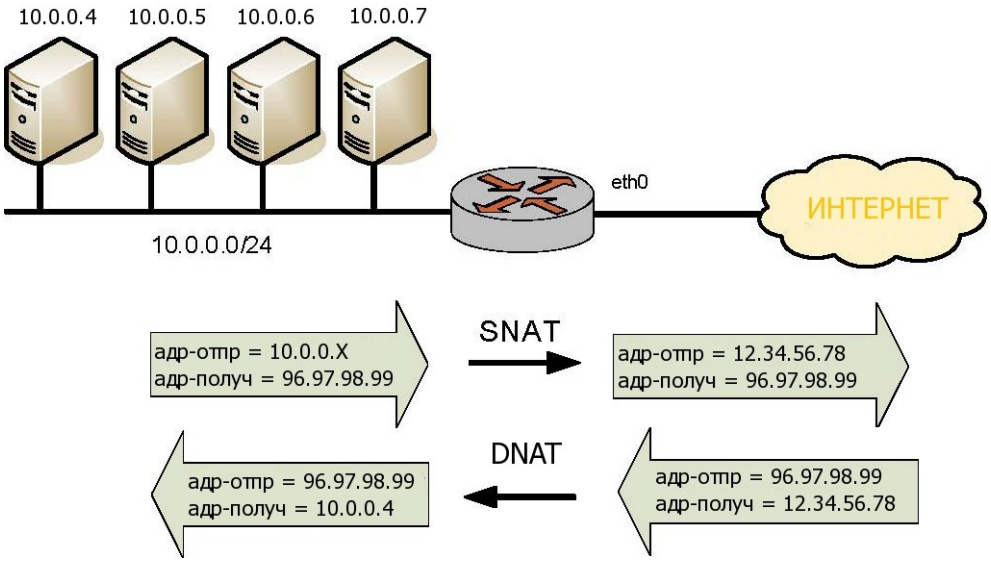
### 13.3.8. Двунаправленное преобразование сетевых адресов

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); рис. 43.

Для настройки преобразования сетевых адресов в соответствии с данным рисунком

нужно выполнить следующие действия в режиме настройки.

*Рисунок 43 - Двунаправленное преобразование сетевых адресов*




*Пример 13.21 - Двунаправленное преобразование сетевых адресов*

| Действие | Команда |
|---|---|
| Создание правила 10. Правило 10 является правилом преобразования сетевого адреса отправителя (SNAT). | admin@neo# **set service nat rule 10 type source**<br>[edit] |
| Применение данного правила к пакетам, отправленным любым узлом сети 10.0.0.0/24. | admin@neo# **set service nat rule 10 source address 10.0.0.0/24**<br>[edit] |
| Отправка трафика через интерфейс eth0. Использование адреса 12.34.56.78 в качестве адреса отправителя для исходящих пакетов. | admin@neo# **set service nat rule 10 outbound-interface eth0**<br>[edit]<br>admin@neo# **set service nat rule 10 outside-address address 12.34.56.78**<br>[edit] |
| Создание правила 20. Правило 20 | admin@neo# **set service nat rule** |

является правилом преобразования сетевого адреса получателя (DNAT).

```
20 type destination
[edit]
```

Применение данного правила на интерфейсе eth0 для адреса 12.34.56.78.

```
admin@neo# set service nat rule
20 inbound-interface eth0
[edit]
admin@neo# set service nat rule
20 destination address
12.34.56.78
[edit]
```

Пересылка трафика на адрес 10.0.0.4.

```
admin@neo# set service nat rule
20 inside-address address
10.0.0.4
[edit]
```

Фиксация изменения.

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

Вывод настройки.

```
admin@neo# show service nat rule
10
 outbound-interface eth0
 outside-address {
     address 12.34.56.78
 }
 source {
     address 10.0.0.0/24
 }
 type source
[edit]
admin@neo# show service nat rule
20
 destination {
     address 12.34.56.78
```

```
}
inbound-interface eth0
inside-address {
    address 10.0.0.4
}
type destination
[edit]
```

### 13.3.9. Сопоставление диапазонов адресов

Возможно сопоставление адресов одной сети с адресами другой сети. Например, можно сопоставить адреса сети 10.0.0.0/24 с адресами сети 11.22.33.0/24, то есть адрес 10.0.0.1 будет сопоставлен с адресом 11.22.33.1, адрес 10.0.0.2 будет сопоставлен с адресом 11.22.33.2 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 13.22 - Сопоставление диапазонов адресов*

| Действие | Команда |
|---|---|
| Создание правила 10. Правило 10 является правилом преобразования сетевого адреса отправителя (SNAT). | admin@neo# **set service nat rule 10 type source**<br>[edit] |
| Применение данного правила к пакетам, отправленным любым узлом сети 10.0.0.0/24. | admin@neo# **set service nat rule 10 source address 10.0.0.0/24**<br>[edit] |
| Отправка трафика через интерфейс eth0. Использование адреса 11.22.33.*x* в качестве адреса отправителя для исходящих пакетов. | admin@neo# **set service nat rule 10 outbound-interface eth0**<br>[edit]<br>admin@neo# **set service nat rule 10 outside-address address** |

```
11.22.33.0/24
[edit]
```

Создание правила 20. Правило 20 является правилом преобразования сетевого адреса отправителя (SNAT).

```
admin@neo# set service nat rule
20 type source
[edit]
```

Применение данного правила к пакетам, отправленным любым узлом сети 11.22.33.0/24.

```
admin@neo# set service nat rule
20 source address 11.22.33.0/24
[edit]
```

Отправка трафика через интерфейс eth1. Использование адреса 10.0.0.*x* в качестве адреса отправителя для исходящих пакетов.

```
admin@neo# set service nat rule
20 outbound-interface eth1
[edit]
admin@neo# set service nat rule
20 outside-address address
10.0.0.0/24
[edit]
```

Фиксация изменения.

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

Вывод настройки.

```
admin@neo# show service nat rule
10
 outbound-interface eth0
 outside-address {
     address 11.22.33.0/24
 }
 source {
     address 10.0.0.0/24
 }
 type source
[edit]
admin@neo# show service nat rule
20
```

```
outbound-interface eth1
outside-address {
    address 10.0.0.0/24
}
source {
    address 11.22.33.0/24
}
type source
[edit]
```

Если подключения инициируются только узлами сети 10.0.0.0/24, тогда требуется только правило 10. Если подключения инициируются только узлами сети 11.22.33.0/24, то требуется только правило 20.

Сопоставление сетей осуществляется аналогично преобразованию сетевых адресов получателя (DNAT).

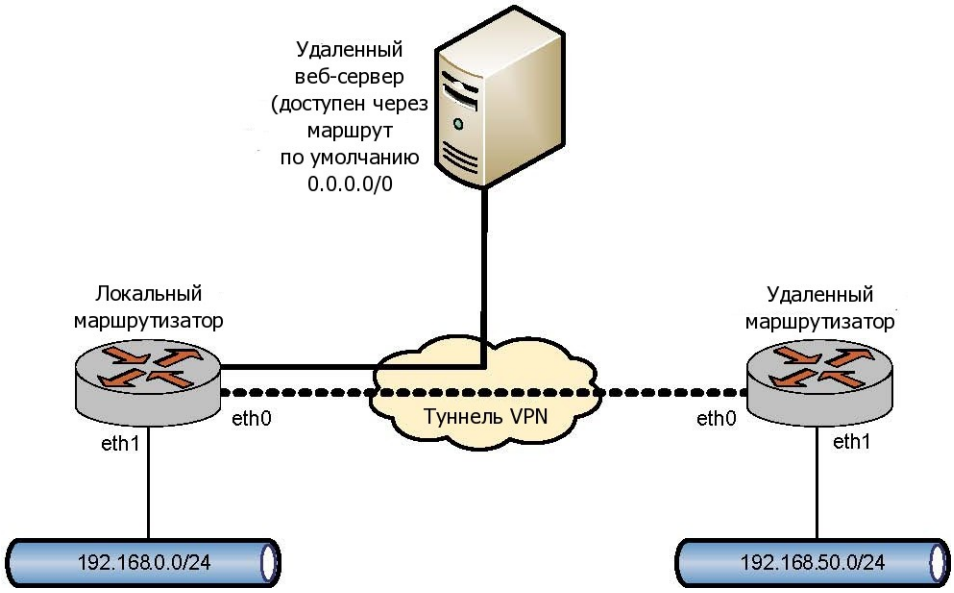
### 13.3.10. Маскировка и VPN

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 [“!”]). Такая схема приведена на рисунке 44.

Для настройки преобразования сетевых адресов в соответствии с данным рисунком нужно выполнить следующие действия в режиме настройки.

*Рисунок 44 - Маскировка и VPN*




*Пример 13.23 - Настройка правил маскировки в обход туннеля VPN*

| Действие | Команда |
|---|---|
| Создание правила 10. Правило 10 является правилом преобразования сетевого адреса отправителя (SNAT). | `admin@neo# set service nat rule 10 type masquerade`<br>`[edit]` |
| Применение данного правила к сетевым пакетам, которые были отправлены любым узлом сети 192.168.0.0/24. | `admin@neo# set service nat rule 10 source address 192.168.0.0/24`<br>`[edit]` |
| Применение данного правила ко всем сетевым пакетам, кроме пакетов, предназначенных сети для сети 192.168.50.0/24. | `admin@neo# set service nat rule 10 destination address ! 192.168.50.0/24`<br>`[edit]` |
| Отправка сетевого трафика через интерфейс eth0. Использование IP-адреса выходного интерфейса в качестве внешнего адреса. | `admin@neo# set service nat rule 10 outbound-interface eth0`<br>`[edit]` |

Фиксация изменения.

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

Вывод настройки.

```
admin@neo# show service nat rule
10
 destination {
     address !192.168.50.0/24
 }
 outbound-interface eth0
 source {
     address 192.168.0.0/24
 }
 type masquerade
[edit]
```

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 13.24.

*Пример 13.24 - Единственное "исключающее правило": корректное поведение*

```
rule 10 {
     destination {
          address !192.168.50.0/24
     }
     outbound-interface eth0
     source {
          address 192.168.0.0/24
     }
     type masquerade
}
```

Это правило создает исключение для сети 192.168.50.0/24, как и требовалось. С другой стороны, рассмотрим набор из двух правил преобразований адресов в примере 13.25.

*Пример 13.25 - Несколько "исключающих правил": поведение, отличное от ожидаемого*

```
rule 10 {
     destination {
          address !192.168.50.0/24
     }
     outbound-interface eth0
     source {
          address 192.168.0.0/24
     }
     type masquerade
}
rule 20 {
     destination {
          address !172.16.50.0/24
     }
     outbound-interface eth0
     source {
          address 192.168.0.0/24
     }
     type masquerade
}
```

В результате выполнения данного набора правил исключение для сетей 192.168.50.0/24 и 172.16.50.0/24 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 192.168.50.0/24, не будет установлено соответствие для правила 10 (которому будут соответствовать пакеты, сеть получателя которых отлична от 192.168.50.0/24). После чего пакет будут проверен на соответствие правилу 20. Для пакета, имеющего сеть получателя 192.168.50.0/24, будет установлено соответствие правилу 20 (так как адрес получателя не лежит в сети 172.16.50.0/24), в результате для пакета будет выполнено преобразование сетевого адреса,

что не является желаемым результатом.

Аналогично, пакет с адресом получателя 172.16.50.0/24 будет соответствовать правилу 10, в результате чего будет осуществлено преобразование адресов.

### 13.3.11. 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 13.26 используется параметр **exclude** для решения задачи, рассмотренной в примере 13.24.

*Пример 13.26 - Единственное исключающее правило: корректное поведение - использование параметра "exclude"*

```
rule 10 {
     destination {
          address 192.168.50.0/24
     }
     exclude outbound-interface eth0
     source {
          address 192.168.0.0/24
     }
     type masquerade
}
rule 20 {
     outbound-interface eth0
     source {
          address 192.168.0.0/24
     }
     type masquerade
}
```

Дополнительное правило (правило 20) требуется для обработки пакетов, для которых не требуется создавать исключения.

В примере 13.27 используется параметр **exclude**, чтобы получить результат, который

не был получен в примере 13.25. В этом примере правило 30 обрабатывает неисключенные пакеты.

*Пример 13.27 - Использование нескольких исключающих правил: корректное поведение - использование параметра "exclude"*

```
rule 10 {
     destination {
          address 192.168.50.0/24
     }
     exclude outbound-interface eth0
     source {
          address 192.168.0.0/24
     }
     type masquerade
}
rule 20 {
     destination {
          address 172.16.50.0/24
     }
     exclude outbound-interface eth0
     source {
          address 192.168.0.0/24
     }
     type masquerade
}
rule 30 {
     outbound-interface eth0
     source {
          address 192.168.0.0/24
     }
     type masquerade
}
```

## 13.4. Команды NAT

В этом разделе приведены команды преобразования сетевых адресов (NAT).

В этом разделе приведены следующие команды:

*Таблица 31 - Команды NAT*

| Команды настройки | |
|---|---|
| `service nat` | Включение преобразования сетевых адресов (NAT). |
| `service nat rule <номер_правила>` | Определение правила преобразования сетевых адресов (NAT). |
| `service nat rule <номер_правила> destination` | Указание адреса получателя и номера порта, которые будут использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT). |
| `service nat rule <номер_правила> disable` | Отключение правила преобразования сетевых адресов (NAT). |
| `service nat rule <номер_правила> exclude` | Создание правила, определяющего исключения для указанных пакетов, при преобразовании сетевых адресов. |
| `service nat rule <номер_правила> inbound-interface <интерфейс>` | Указание входного интерфейса, на котором будет выполняться правило преобразования сетевого адреса получателя (DNAT). |
| `service nat rule <номер_правила> inside-address` | Определение внутреннего адреса для правила, осуществляющего преобразование сетевого адреса получателя. |
| `service nat rule <номер_правила> log <состояние>` | Регистрация для правил преобразования сетевого адреса (NAT), для которых было установлено соответствие. |
| `service nat 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 rule <номер_правила> outside-address` | Определение внешнего адреса для правила преобразования сетевого адреса отправителя (SNAT). |
| `service nat rule <номер_правила> protocol <протокол>` | Указание протоколов, для которых осуществляется преобразование сетевых адресов (NAT). |
| `service nat rule <номер_правила> source` | Указание адреса отправителя и номера порта, по которым будет осуществляться проверка соответствия в правиле преобразования сетевого адреса (NAT). |
| `service nat rule <номер_правила> type <вид>` | Установка вида преобразования для правила преобразования сетевого адреса (NAT). |
| Эксплуатационные команды | |
| `clear nat counters` | Очистка счетчиков для активных правил преобразования сетевых адресов (NAT). |
| `show nat rules` | Отображение настроенных правил преобразования сетевых адресов (NAT). |
| `show nat statistics` | Вывод статистики для службы преобразования сетевых адресов (NAT). |
| `show nat translations` | Вывод активных преобразований сетевых адресов. |

### 13.4.1. clear nat counters

Очистка счетчиков для активных правил преобразования сетевых адресов (NAT).

**Синтаксис**

**clear nat counters [rule** *номер_правила*]

**Режим ввода команды**

Эксплуатационный режим.

**Параметры**

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 1024.

**Значение по умолчанию**

Счетчики сбрасываются для всех правил преобразования сетевых адресов (NAT).

**Указания по использованию**

Команда позволяет сбросить счетчики для правил преобразования сетевых адресов (NAT). По умолчанию счетчики сбрасываются для всех правил. Если указывается номер правила, счетчики сбрасываются только для указанного правила.

## 13.4.2. service nat

Включение преобразования сетевых адресов (NAT).

**Синтаксис**

```
set service nat
delete service nat
show service nat
```

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    nat{
    }
}
```

**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.

### 13.4.3. service nat rule <номер_правила>

Определение правила преобразования сетевых адресов (NAT).

**Синтаксис**

```
set service nat rule номер_правила
delete service nat rule [номер_правила]
show service nat rule [номер_правила]
```

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    nat {
        rule 1-1024 {
        }
    }
}
```

**Параметры**

*номер_правила*

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 1024.

**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.

### 13.4.4. service nat rule <номер_правила> destination

Указание адреса получателя и номера порта, которые будут использоваться для проверки соответствия сетевого пакета правилу преобразования сетевых адресов (NAT).

**Синтаксис**

```
set service nat rule номер_правила destination [address
адрес | port порт ]

delete service nat rule номер_правила destination
[address | port]

show service nat rule номер_правила destination [address
| port]
```

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    nat {
        rule 1-1024 {
            destination {
                address текст
                port текст
            }
        }
    }
```

}

**Параметры**

*номер_правила*

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 1024.

*адрес*

Адрес получателя для проверки соответствия. Допустимые форматы:

*ip-адрес*: IPv4-адрес.

*ip-адрес/префикс*: IPv4-адрес сети, где 0.0.0.0/0 соответствует любой сети.

*ip-адрес–ip-адрес*: Диапазон IPv4-адресов; например, 192.168.1.1–192.168.1.150.

*!ip-адрес*: Любой IPv4-адрес, КРОМЕ указанного.

*!ip-адрес/префикс*: Любой IPv4-адрес сети, КРОМЕ указанного.

*!ip-адрес–ip-адрес*: Любые IP-адреса, КРОМЕ лежащих в указанном диапазоне.

*порт*

Порт получателя для проверки соответствия. Допустимые форматы:

*имя_порта*: Название службы; например, http. Названия различных служб можно указать в файле /etc/services.

*номер_порта*: Номер сетевого порта. Значение должно лежать в диапазоне от 1 до 65535.

*начало-конец*: Диапазон номеров сетевых портов; 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**

Команда позволяет указать получателя, на основе которого будет осуществляться установление 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 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 получателя NAT.

### 13.4.5. service nat rule <номер_правила> disable

Отключение правила преобразования сетевых адресов (NAT).

**Синтаксис**

```
set service nat rule номер_правила disable
delete service nat rule номер_правила disable
show service nat rule номер_правила
```

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    nat {
        rule 1-1024 {
            disable
        }
    }
}
```

**Параметры**

*номер_правила*

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 1024.

**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.

## 13.4.6. service nat rule <номер_правила> exclude

Создание правила, определяющего исключения для указанных пакетов, при преобразовании сетевых адресов.

**Синтаксис**

```
set service nat rule номер_правила exclude
delete service nat rule номер_правила exclude
show service nat rule номер_правила
```

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    nat {
        rule 1-1024 {
            exclude
        }
    }
}
```

**Параметры**

*номер_правила*

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 1024.

**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.

## 13.4.7. service nat rule <номер_правила> inbound-interface <интерфейс>

Указание входного интерфейса, на котором будет выполняться правило преобразования сетевого адреса получателя (DNAT).

**Синтаксис**

**set service nat rule** *номер_правила* **inbound-interface** *интерфейс*

**delete service nat rule** *номер_правила* **inbound-interface**

**show service nat rule** *номер_правила* **inbound-interface**

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    nat {
        rule 1-1024 {
            inbound-interface текст
        }
    }
}
```

**Параметры**

*номер_правила*

Обязательный. Множественный узел. Численный идентификатор правила.

Значение должно лежать в диапазоне от 1 до 1024.

*интерфейс*

Входной интерфейс Ethernet или последовательный интерфейс. Преобразование сетевого адреса получателя (DNAT) будет осуществляться для трафика, принятого на указанном интерфейсе. Можно указать только отдельный виртуальный интерфейс, а не интерфейс в целом. Для этого используется следующий формат *int.vif*. Например, чтобы указать виртуальный интерфейс **vif** 40 на интерфейсе eth0, следует указать **eth0.40**. Также можно указать **eth+**, чтобы указать все интерфейсы Ethernet, или **any**, чтобы указать любой интерфейс.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда используется для указания входного интерфейса Ethernet или последовательного 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.

## 13.4.8. service nat rule <номер_правила> inside-address

Определение внутреннего адреса для правила, осуществляющего преобразование сетевого адреса получателя.

**Синтаксис**

```
set service nat rule номер_правила inside-address
[address адрес | port порт]

delete service nat rule номер_правила inside-address
[address адрес | port порт]

show service nat rule номер_правила inside-address
[address адрес | port порт ]
```

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    nat {
        rule 1-1024 {
            inside-address {
                address текст
                port текст
            }
        }
    }
}
```

**Параметры**

*номер_правила*

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 1024.

*адрес*

Адрес, диапазон адресов, или адрес сети, который используется для преобразования внутреннего адреса. Допустимые форматы:

*ipv4-адрес*: Преобразование к указанному IP-адресу.

*ipv4-адрес–ipv4-адрес*: Преобразование к одному из адресов из указанного пула адресов; например, 192.168.1.1–192.168.1.150.

*сеть_ipv4*: Преобразование к указанной сети. Обычно это используется при применении двунаправленного преобразования адресов одной сети в адреса другой сети.

*порт*

Номер сетевого порта, который будет использоваться для преобразования внутреннего адреса. Допустимые форматы:

*номер_порта*: Преобразование к указанному порту. Значение должно лежать в диапазоне от 1 до 65535.

*начало–конец*: Преобразование к одному из портов из указанного диапазона; например, 1001–1005.

**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.

## 13.4.9. service nat rule <номер_правила> log <состояние>

Регистрация для правил преобразования сетевого адреса (NAT), для которых было установлено соответствие.

**Синтаксис**

```
set service nat rule номер_правила log состояние
```

**delete service nat rule** *номер_правила* **log**

**show service nat rule** *номер_правила* **log**

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
     nat {
          rule 1-1024 {
               log [disable|enable]
          }
     }
}
```

**Параметры**

*номер_правила*

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 1024.

*состояние*

Указание создавать записи журнала для правил преобразования сетевых адресов, для которых было установлено соответствие. Допустимые значения:

**disable***:* Записи журнала для правил, для которых найдено соответствие, не создаются.

**enable**: Записи журнала для правил, для которых найдено соответствие, 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.

## 13.4.10. service nat 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 rule номер_правила outbound-interface
интерфейс

delete service nat rule номер_правила outbound-interface

show service nat rule номер_правила outbound-interface
```

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    nat {
        rule 1-1024 {
            outbound-interface текст
        }
    }
}
```

**Параметры**

*номер_правила*

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 1024.

*интерфейс*

Необязательный для правил преобразования сетевых адресов отправителя (тип **source**); обязательный для правил "маскировки" (тип **masquerade**). Не указывается для правил преобразования сетевого адреса получателя (тип **destination**). Выходной интерфейс или последовательный интерфейс. Преобразование сетевого адреса отправителя (SNAT) или "маскировка" (**masquerade**) будут осуществляться для сетевого трафика, отправляемого через данный интерфейс. Можно указать только отдельный виртуальный интерфейс, а не интерфейс в целом. Для указания виртуального интерфейса используется следующий формат: *int.vif*. Чтобы указать виртуальный интерфейс **vif 40** на интерфейсе **eth0,** следует указать **eth0.40**. Также можно указать **eth+** , чтобы указать все интерфейсы Ethernet, или **any**, чтобы указать любой интерфейс.

**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.

Настройка выходного интерфейса является необязательной для правил преобразования сетевого адреса отправителя (тип **source** ) и обязательной для правил "маскировки" (тип **masquerade**). Не указывается для правил преобразования сетевого адреса получателя (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.

## 13.4.11. service nat rule <номер_правила> outside-address

Определение внешнего адреса для правила преобразования сетевого адреса отправителя (SNAT).

**Синтаксис**

```
set service nat rule номер_правила outside-address
[address адрес | port порт]

delete service nat rule номер_правила outside-address
[address | port]

show service nat rule номер_правила outside-address
[address | port]
```

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    nat {
        rule 1-1024 {
            outside-address {
                address текст
                port текст
            }
        }
    }
}
```

**Параметры**

*номер_правила*

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 1024.

*адрес*

Адрес или диапазон адресов, которые будут использованы для преобразования внешнего адреса. Указанный адрес или адреса должны быть назначены выходному интерфейсу. Допустимые форматы:

*ip-адрес*: Преобразование к указанному IP-адресу.

*ip-адрес–ip-адрес*: Преобразование к одному из IP-адресов из указанного пула IP-адресов; например, 192.168.1.1–192.168.1.150.

*сеть_ipv4*: Преобразование к указанной сети. Обычно это используется при применении двунаправленного преобразования адресов одной сети в адреса другой сети.

*порт*

Сетевой порт, который будет использоваться для преобразования внешнего адреса. Допустимые форматы:

*номер_порта:* Преобразование к указанному порту. Значение должно лежать в диапазоне от 1 до 65535.

*начало–конец*: Преобразование к одному из портов из указанного диапазона; например, 1001–1005.

**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.

## 13.4.12. service nat rule <номер_правила> protocol <протокол>

Указание протоколов, для которых осуществляется преобразование сетевых адресов (NAT).

**Синтаксис**

**set service nat rule** *номер_правила* **protocol** *протокол*

**delete service nat rule** *номер_правила* **protocol**

**show service nat rule** *номер_правила* **protocol**

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    nat {
        rule 1-1024 {
            protocol текст
        }
    }
}
```

**Параметры**

*номер_правила*

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 1024.

*протокол*

Сетевой протокол (протоколы), для которого осуществляется преобразование сетевых адресов. Могут быть использованы любые наименования протоколов или их номера, определенные в файле **/etc/protocols**. Ключевые слова **all** (для всех протоколов) и **tcp_udp** (для протоколов TCP и UDP) также поддерживаются.

При указании перед названием протокола восклицательного знака (“!”) соответствие будет установлено для любого протокола, кроме указанного. Например, при указании **!tcp** соответствие будет установлено для всех протоколов, кроме TCP.

**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.

## 13.4.13. service nat rule <номер_правила> source

Указание адреса отправителя и номера порта, по которым будет осуществляться проверка соответствия в правиле преобразования сетевого адреса (NAT).

**Синтаксис**

```
set service nat rule номер_правила source [address адрес
| port порт]

delete service nat rule номер_правила source [address |
port]

show service nat rule номер_правила source [address |
port]
```

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    nat {
        rule 1-1024 {
            source {
                address текст
                port текст
            }
        }
    }
```

```
}
```

**Параметры**

*номер_правила*

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 1024.

*адрес*

Адрес отправителя для проверки соответствия. Допустимы следующие форматы:

*ip-адрес*: Проверка соответствия указанному адресу.

*ip-адрес/префикс*: Адрес сети, где 0.0.0.0/0 соответствует любой сети.

*ip-адрес–ip-адрес*: Соответствие будет установлено для диапазона IP-адресов; например, 192.168.1.1–192.168.1.150.

*!ip-адрес*: Соответствие будет установлено для всех IP-адресов, кроме указанного.

*!ip-адрес/префикс*: Соответствие будет установлено для всех адресов сети, кроме указанного.

*!ip-адрес–ip-адрес*: Соответствие будет установлено для всех IP-адресов, кроме входящих в указанный диапазон.

*порт*

Порт отправителя для проверки соответствия. 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 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 адреса отправителя для преобразования сетевых адресов.

Форма **delete** данной команды позволяет удалить настройку адреса отправителя для преобразования сетевых адресов.

Форма **show** данной команды используется для отображения настройки адреса отправителя для преобразования сетевых адресов.

## 13.4.14. service nat rule <номер_правила> type <вид>

Установка вида преобразования для правила преобразования сетевого адреса (NAT).

**Синтаксис**

```
set service nat rule номер_правила type вид
delete service nat rule номер_правила type
show service nat rule номер_правила type
```

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    nat {
        rule 1-1024 {
            type [source|destination|masquerade]
        }
    }
}
```

**Параметры**

*номер_правила*

Обязательный. Множественный узел. Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 1024.

*вид*

Указывает, выполняется ли в правиле преобразование адреса отправителя (SNAT) или адреса получателя (DNAT). Следует отметить, что это зависит от направления интерфейса. Поддерживаются следующие значения:

**source**: Данное правило используется для преобразования сетевых адресов отправителя. Обычно правила данного типа применяются к исходящим пакетам.

**destination**: Данное правило используется для преобразования сетевых адресов получателя. Обычно правила данного вида применяются ко входящим пакетам.

**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 (отправителя или получателя).

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.

## 13.4.15. show nat rules

Отображение настроенных правил преобразования сетевых адресов (NAT).

**Синтаксис**

```
show nat 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 13.28 приведен вывод для команды **show nat 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. 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, не изменяя номер сетевого порта, и выполняется в том и только том случае, если порт получателя равен 80 для любого адреса получателя.

- Если перед номером правила указывается символ “X” (например, как для правила 30), правило является исключающим.

*Пример 13.28 - Вывод сведений о правилах NAT*

```
admin@neo:~$ show nat rules
Type Codes: SRC - source, DST - destination, MASQ — masquerade
             X at the front of rule implies rule is excluded
rule type intf translation
-- -- -- ------
10   SRC  eth2 saddr 192.168.74.0/24 to 172.16.139.0/24
   proto-tcp   sport ANY
               when daddr ANY, dport 80

20   DST  eth2 daddr 172.16.139.0/24 to 192.168.74.0/24
   proto-all   dport ANY

X30  MASQ eth0 saddr ANY to 172.16.117.200
   proto-tcp   sport ANY to 80
               when daddr ANY, dport 8080
```

## 13.4.16. show nat statistics

Вывод статистики для службы преобразования сетевых адресов (NAT).

**Синтаксис**

**show nat 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 13.29 приведен вывод для команды **show nat statistics**.

*Пример 13.29 - Вывод сведений о статистике для правил NAT*

```
admin@neo:~$ show nat statistics

Type Codes: SRC - source, DST - destination, MASQ — masquerade

rule count type    IN        OUT

-- --- -- ----- -----

1    6     MASQ     -        eth2

2    6     MASQ     -        eth3
```

## 13.4.17. show nat translations

Вывод активных преобразований сетевых адресов.

**Синтаксис**

**show nat translations [destination [address** *адрес* **| detail | monitor [detail]] | detail | monitor | source [address** *адрес* **| detail | monitor [detail]]]**

**Режим ввода команды**

Эксплуатационный режим.

**Параметры**

**destination**

Вывод сведений о преобразованиях сетевого адреса получателя.

**destination address** *адрес*

Вывод сведений о преобразованиях сетевого адреса получателя адрес.

**destination detail**

Вывод подробных сведений о преобразованиях сетевого адреса получателя (DNAT).

**destination monitor**

Вывод результатов наблюдения за преобразованиями сетевого адреса получателя в режиме реального времени. Чтобы остановить вывод, следует ввести <Ctrl>+C.

**destination monitor detail**

Вывод подробных результатов наблюдения за преобразованиями сетевого адреса получателя в режиме реального времени. Чтобы остановить вывод, следует ввести <Ctrl>+C.

**detail**

Вывод подробных сведений о всех преобразованиях сетевых адресов.

**monitor**

Вывод результатов наблюдения за преобразованиями сетевых адресов в режиме реального времени. Чтобы остановить вывод, следует ввести <Ctrl>+C.

**source**

Вывод сведений о преобразованиях сетевого адреса отправителя.

**source address** *адрес*

Вывод сведений о преобразованиях сетевого адреса отправителя адрес .

**source detail**

Вывод подробных сведений о преобразованиях сетевых адресов отправителя.

**source monitor**

Вывод результатов наблюдения за преобразованиями сетевого адреса отправителя в режиме реального времени. Чтобы остановить вывод, следует ввести <Ctrl>+C.

**source monitor detail**

Вывод подробных результатов наблюдения за преобразованиями сетевого адреса отправителя в режиме реального времени. Чтобы остановить вывод, следует ввести <Ctrl>+C.

**Указания по использованию**

Данная команда позволяет вывести сведения о правилах преобразования сетевых адресов.

**Примеры**

В примере 13.30 приведен образец вывода для команды **show nat translations.**

*Пример 13.30 - Вывод преобразований сетевых адресов*

```
admin@neo:~$ show nat translations
Pre-NAT            Post-NAT          Type  Prot Timeout
15.0.0.16          172.16.117.100    snat  tcp  106
15.0.0.20          172.16.117.101    snat  tcp  431959
15.0.0.16          172.16.117.100    snat  tcp  58
20.0.0.16:23       15.0.0.16:5000    dnat  tcp  431996
admin@neo:~$
```

В примере 13.31 приведен образец вывода для команды **show nat translations detail**.

*Пример 13.31 - Вывод детализированных сведений о преобразованиях сетевых адресов*

```
admin@neo:~$ show nat translations detail
Inside src      Inside dst       Outside src
Outside dst
15.0.0.16:41920 172.16.117.17:22 172.16.117.100:41920
172.16.117.17:22
  tcp: snat: 15.0.0.16 ==> 172.16.117.100 timeout: 103
use: 1 15.0.0.20:55853 172.16.117.17:23
172.16.117.101:55853 172.16.117.17:23
  tcp: snat: 15.0.0.20 ==> 172.16.117.101 timeout: 431956
use: 1 15.0.0.16:46585 172.16.117.17:23
172.16.117.100:46585 172.16.117.17:23
  tcp: snat: 15.0.0.16 ==> 172.16.117.100 timeout: 54
use: 1 172.16.117.17:51391 20.0.0.16:23
```

```
172.16.117.17:51391  15.0.0.16:5000

  tcp: dnat: 20.0.0.16:23 ==> 15.0.0.16:5000 timeout:
431993 use: 1

admin@neo:~$
```

В примере 13.32 приведен образец вывода для команды **show nat translations source address 15.0.0.16**.

*Пример 13.32 - Вывод сведений NAT для адреса отправителя 15.0.0.16*

```
admin@neo:~$ show nat translations source address
15.0.0.16

Inside src      Inside dst       Outside src
Outside dst

15.0.0.16:57634 172.16.117.17:22 172.16.117.100:57634
172.16.117.17:22

  tcp: snat: 15.0.0.16 ==> 172.16.117.100 timeout: 106
use: 1 15.0.0.16:46884 172.16.117.17:23
172.16.117.100:46884 172.16.117.17:23

  tcp: snat: 15.0.0.16 ==> 172.16.117.100 timeout: 115
use: 1

admin@neo:~$
```

В примере 13.33 приведен вывод для команды **show nat translations source monitor**.

*Пример 13.33 - Вывод сведений о преобразованиях сетевых адресов отправителя в режиме реального времени*

admin@neo:~$ **show nat translations source monitor**

Type control-C to quit

| Pre-NAT | Post-NAT | Type | Prot | Timeout | Type |
|---|---|---|---|---|---|
| 15.0.0.16 | 172.16.117.100 | snat | icmp | 30 | new |
| 15.0.0.16 | 172.16.117.100 | snat | icmp | 29 | update |
| 15.0.0.16 | 172.16.117.100 | snat | icmp | | destroy |
| 15.0.0.16 | 172.16.117.100 | snat | icmp | 30 | new |
| 15.0.0.16 | 172.16.117.100 | snat | icmp | 30 | update |
| 15.0.0.16 | 172.16.117.100 | snat | icmp | | destroy |
| 15.0.0.20 | 172.16.117.101 | snat | tcp | | destroy |

admin@neo:~$

В примере 13.34 приведен образец вывода для команды **show nat translations source monitor detail**.

*Пример 13.34 - Вывод подробных результатов наблюдения за преобразованиями сетевого адреса*

```
admin@neo:~$ show nat translations source monitor detail

Type control-C to quit

Inside src      Inside dst    Outside src        Outside
dst

15.0.0.16   172.16.117.17     172.16.117.100
172.16.117.17

  icmp: snat: 15.0.0.16 ==> 172.16.117.100 timeout: 30
type: new

15.0.0.16   172.16.117.17     172.16.117.100
172.16.117.17

  icmp: snat: 15.0.0.16 ==> 172.16.117.100 timeout: 30
type: update

15.0.0.16   172.16.117.17     172.16.117.100
172.16.117.17

  icmp: snat: 15.0.0.16 ==> 172.16.117.100 type: destroy

15.0.0.16   172.16.117.17     172.16.117.100
172.16.117.17

  icmp: snat: 15.0.0.16 ==> 172.16.117.100 timeout: 30
type: new

15.0.0.16   172.16.117.17     172.16.117.100
172.16.117.17

  icmp: snat: 15.0.0.16 ==> 172.16.117.100 timeout: 30
type: update

15.0.0.16   172.16.117.17     172.16.117.100
172.16.117.17

  icmp: snat: 15.0.0.16 ==> 172.16.117.100 type: destroy

admin@neo:~$
```

# 14. НАСТРОЙКА МЕЖСЕТЕВОГО ЭКРАНА

## 14.1. Обзор межсетевого экрана

В этом разделе представлен обзор защитных функций межсетевого экрана в системе Altell NEO.

В этом разделе рассматриваются следующие вопросы:

- Функциональность межсетевого экрана системы Altell NEO.
- Определение экземпляров межсетевого экрана.
- Межсетевой экран с поддержкой состояния и отслеживание подключений.
- Применение экземпляров межсетевого экрана к интерфейсам.
- Взаимодействие между межсетевыми экраном, NAT и маршрутизацией.
- Межсетевой экран на основе зон.
- Межсетевой экран Ipv6.

### 14.1.1. Функциональность межсетевого экрана системы Altell NEO

Функциональность межсетевого экрана предназначена для анализа и фильтрации пакетов IP между сетевыми интерфейсами. Ее наиболее частое применение - это 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 системы Altell NEO 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.**
- Допускающие определение критерии для правил соответствия пакетов, в том числе IP-адрес отправителя, IP-адрес получателя, порт отправителя, порт получателя, протокол IP и тип ICMP.
- Общее определение на основе параметров IP, таких как маршрутизация по отправителю и вещательные пакеты.

В межсетевом экране Altell NEO 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.

### 14.1.2. Определение экземпляров межсетевого экрана

Чтобы использовать функцию межсетевого экрана, следует определить набор правил ("экземпляр") межсетевого экрана и сохранить его с некоторым именем. Экземпляр межсетевого экрана состоит из ряда правил. После чего экземпляр применяется к интерфейсу в качестве фильтра пакетов.

### 14.1.3. Правила межсетевого экрана

В правилах межсетевого экрана указываются условия соответствия для трафика и действия, которые должны быть предприняты, если условия соответствия выполняются. Соответствие трафика может проверяться по ряду характеристик, в том числе по IP-адресу отправителя, IP-адресу получателя, порту отправителя, порту получателя, протоколу IP и типу ICMP.

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).

По умолчанию в любом наборе правил межсетевого экрана есть неявное окончательное действие **reject all** (отвергнуть все); это значит, что трафик, не соответствующий ни одному правилу в наборе правил, отбрасывается со сбросом TCP. Это действие по умолчанию может быть изменено при помощи команды **firewall name** <*имя*> **default-action** <*действие*>.

### 14.1.4. 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.

### 14.1.5. Межсетевой экран с поддержкой состояния и отслеживание подключений

Интерфейс командной строки системы Altell NEO 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 **firewall conntrack-table-size** <*размер*> и **firewall conntrack-tcp-loose** <*состояние*>.

### 14.1.6. Применение экземпляров межсетевого экрана к интерфейсам

Когда экземпляр межсетевого экрана определен, его можно применить к интерфейса, и экземпляр будет работать как пакетный фильтр. Экземпляр межсетевого экрана фильтрует пакеты одним из следующих способов в зависимости от того, что указано при применении экземпляра межсетевого экрана:

- **in** (входящий). Если применить экземпляр с использованием ключевого слова **in**, межсетевой экран будет фильтровать транзитный сетевой трафик, входящий в интерфейс и проходящий через систему Altell NEO. (Сюда не относится сетевой

трафик предназначенный для самого Altell NEO.) С использованием ключевого слова **in** можно применить один пакетный фильтр.

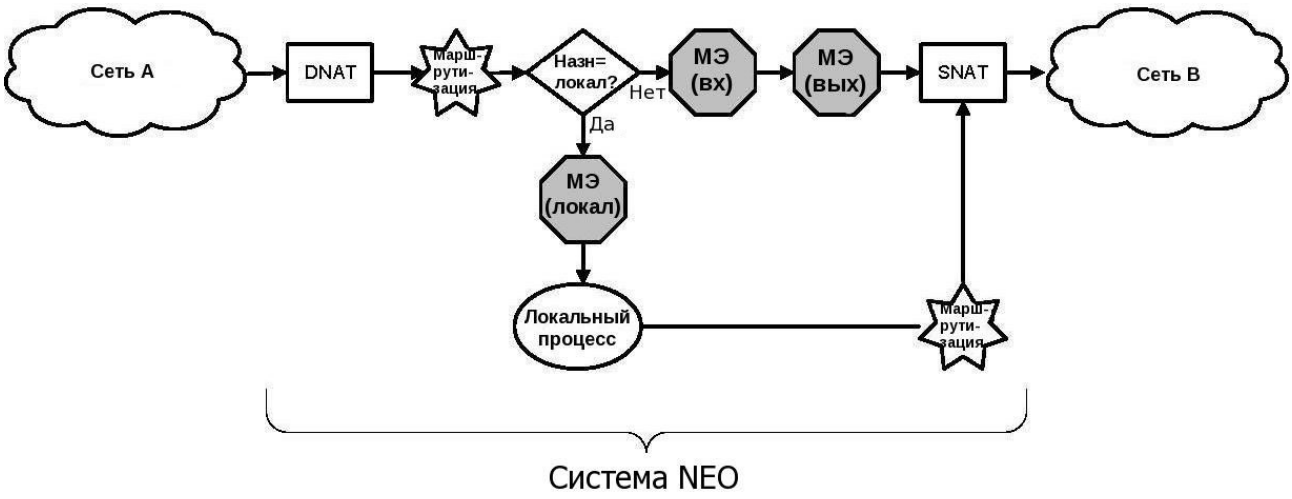
- **out** (исходящий). Если применить экземпляр с использованием ключевого слова **out,** межсетевой экран будет фильтровать транзитный сетевой трафик, покидающий интерфейс. (Сюда не относятся пакеты, исходящие от самого Altell NEO.) С использованием ключевого слова **out** можно применить один пакетный фильтр.
- **local** (локальный). Если применить экземпляр с использованием ключевого слова **local**, межсетевой фильтр будет фильтровать пакеты, предназначенные для системы Altell NEO, входящие на интерфейсе. С использованием ключевого слова **local** можно применить один пакетный фильтр.

К интерфейсу может быть применено всего до трех экземпляров межсетевого фильтра: один экземпляр с указанием ключевого слова **in**, один экземпляр с указанием ключевого слова **out** и один экземпляр с указанием ключевого слова **local**.

### 14.1.7. 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 системе Altell NEO. Если порядок обработки не принимается во внимание, полученные результаты могут отличаться от ожидаемых. На рис. 45 показан поток трафика через межсетевой экран, NAT и службы маршрутизации внутри системы Altell NEO.

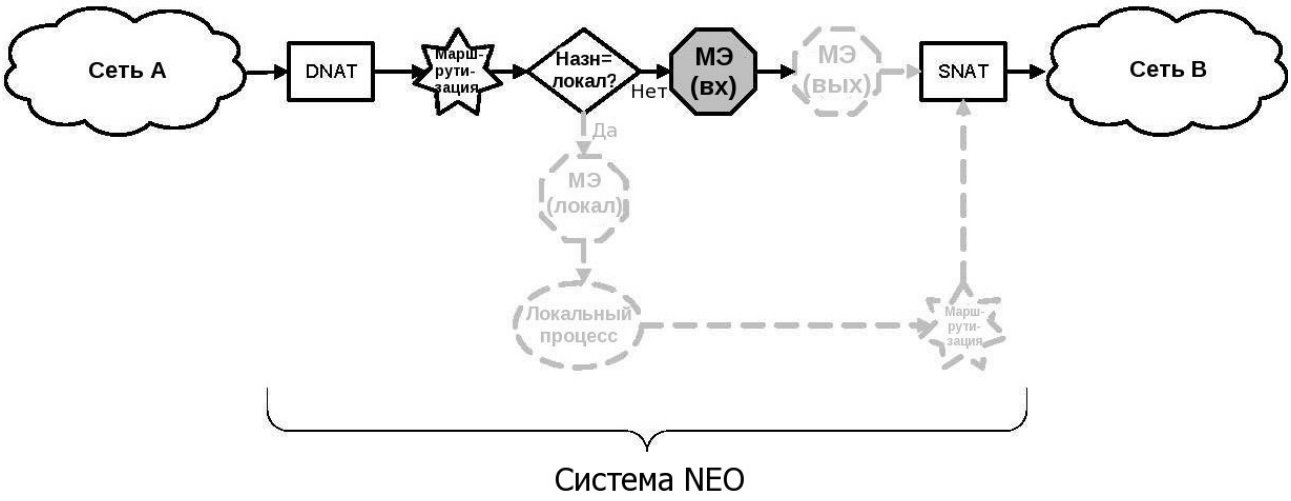
*Рисунок 45 - Прохождение трафика через межсетевой экран, NAT и службу маршрутизации*



**Вариант 1: прохождение транзитного трафика через Altell NEO; фильтрация транзитного трафика, приходящего на интерфейс**

На рисунке 46 показаны взаимосвязи между межсетевым экраном, NAT и маршрутизацией в системе Altell NEO по ходу потока транзитного трафика (проходящего сквозь систему) и экземпляры межсетевого экрана, применённые к трафику, принимаемому (**in**) на интерфейсе.

*Рисунок 46 - Прохождение транзитного трафика, принимаемого на интерфейсе, через систему Altell NEO*

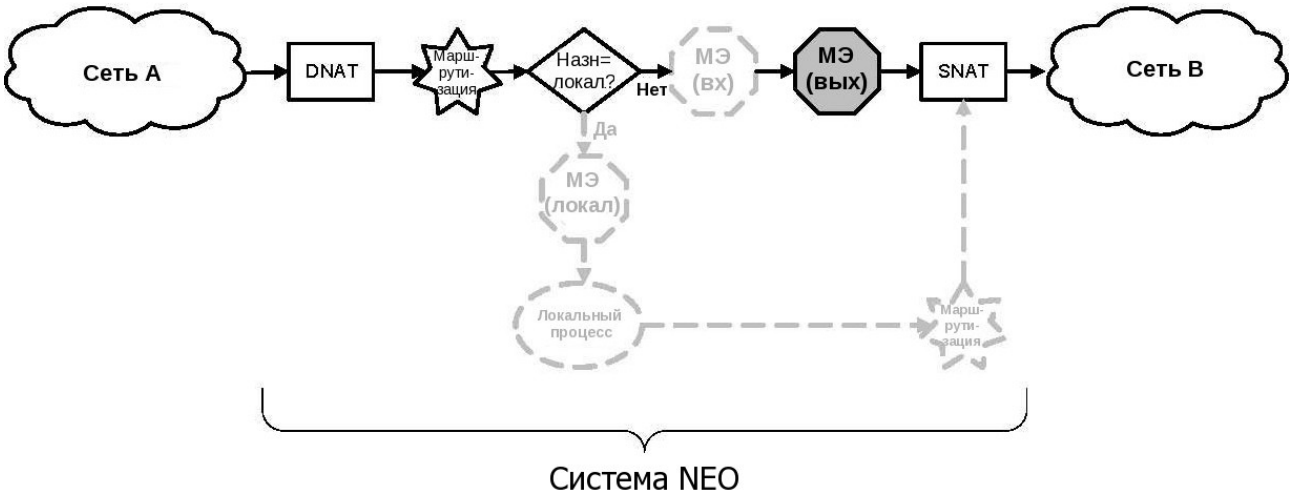



Следует заметить, что соответствие экземплярам межсетевого экрана проверяется после DNAT и решений о маршрутизации, но до SNAT.

**Вариант 2: прохождение транзитного трафика через Altell NEO; фильтрация транзитного трафика, уходящего через интерфейс**

На рисунке 47 показаны взаимосвязи между межсетевым экраном, NAT и маршрутизацией в системе Altell NEO по ходу потока транзитного трафика (проходящего сквозь систему) и экземпляры межсетевого экрана, применённые к трафику, уходящему (**out**) через интерфейс.

*Рисунок 47 - Прохождение транзитного трафика через систему Altell NEO*

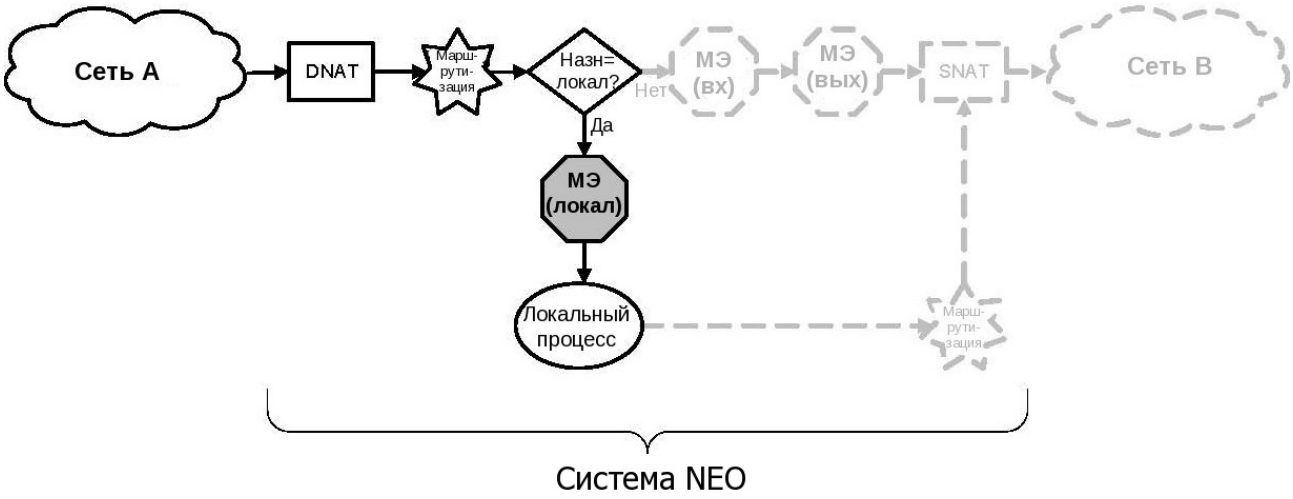



Следует заметить, что соответствие экземплярам межсетевого экрана проверяется после DNAT и решений о маршрутизации, но до SNAT.

**Вариант 3: прохождение трафика, направленного в локальную систему, через Altell NEO; его фильтрация при вхождении на интерфейс**

На рисунке 48 показаны взаимосвязи между межсетевым экраном, NAT и маршрутизацией в системе Altell NEO по ходу потока трафика, приходящего в саму систему Altell NEO и экземпляры межсетевого экрана, применённые к локальному **(local)** трафику на интерфейсе.

*Рисунок 48 - Прохождение трафика, направленного в локальную систему, через Altell NEO*

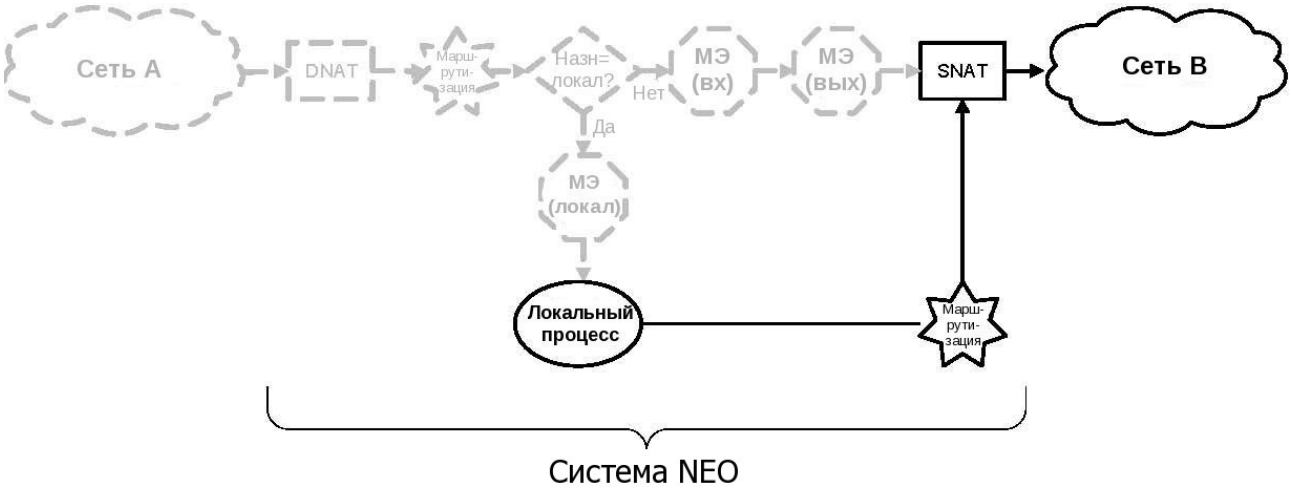



Следует заметить, что соответствие экземплярам межсетевого экрана проверяется после DNAT и маршрутизации. В этом варианте SNAT не выполняется.

**Вариант 4: прохождение трафика, направленного из локальной системы, через Altell NEO**

На рисунке 49 показаны взаимосвязи между межсетевым экраном, NAT и маршрутизацией в системе Altell NEO по ходу потока трафика, исходящего из самой системы Altell NEO.

*Рисунок 49 - Прохождение трафика, направленного из локальной системы, через Altell NEO*




Следует отметить, что к сетевому трафику, исходящему из системы Altell NEO нельзя применить экземпляр межсетевого экрана. В этом варианте DNAT не выполняется.

## 14.1.8. Межсетевой экран на основе зон

Обычные наборы правил межсетевого экрана применяются к каждому интерфейсу в отдельности и работают как пакетные фильтры для интерфейса. В межсетевом экране на основе зон интерфейсы сгруппированы в "зоны безопасности", в которых все входящие в одну зону интерфейсы имеют одинаковый уровень безопасности.

Политики фильтрации трафика применяются к потокам трафика между зонами. Трафик, передаваемый между интерфейсами, лежащими в одной зоне, не фильтруется и передается свободно, так как интерфейсы имеют общий уровень безопасности.

На рис. 50 показан пример реализации межсетевого экрана на основе зон. В этом примере:

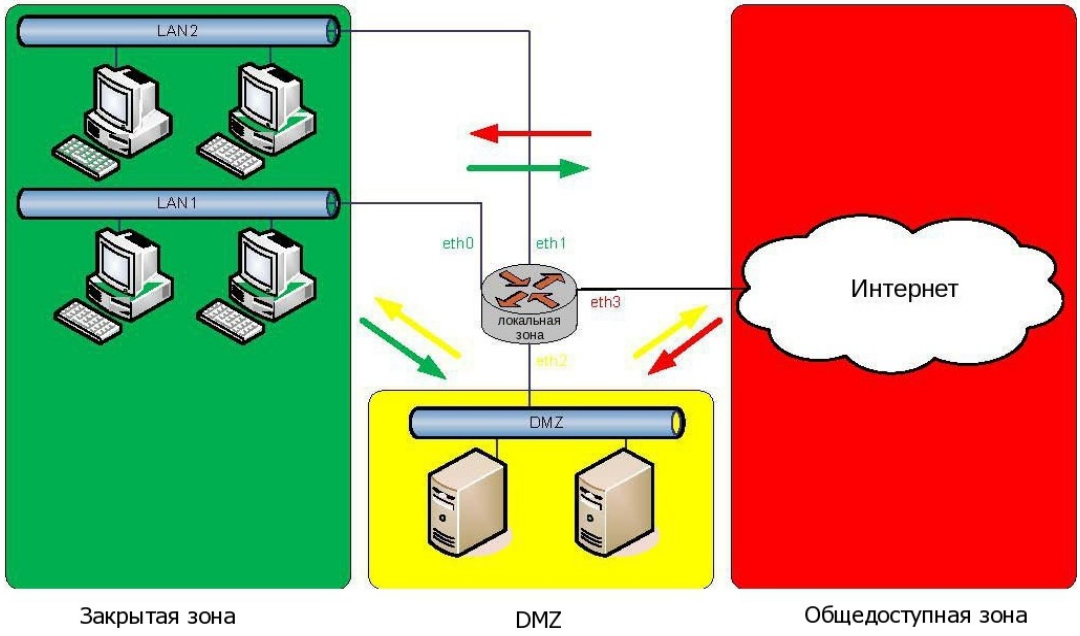
- Имеются три транзитных зоны (то есть точки, где трафик проходит через маршрутизатор): закрытая зона, демилитаризованная зона (DMZ) и общедоступная

зона.

- Интерфейс **eth3** лежит в общедоступной зоне; **eth0** и **eth1** лежат в закрытой зоне; **eth2** лежит в DMZ.
- Стрелки из одной зоны в другую представляют политики фильтрации трафика, применяемые к трафику, передаваемому между зонами.
- Трафик, передаваемый между LAN 1 и LAN 2, остаётся в одной и той же зоне безопасности, так что трафик из LAN1 в LAN2 и обратно передается без фильтрации.

Помимо трех транзитных зон, на рис. 50 есть и четвёртая зона - “локальная зона”

*Рисунок 50 - Межсетевой экран, основанный на политиках зон безопасности*




Локальная зона - это сам маршрутизатор. По умолчанию весь трафик, приходящий на маршрутизатор и исходящий из него, разрешается. Тем не менее, можно настроить политики фильтрации трафика, разрешающие трафик в локальную зону из конкретных зон и подобным же образом из локальной зоны только в конкретные зоны. Если применить политику фильтрации, явно разрешающую трафик, направленный в локальную зону из другой зоны, трафик изо всех остальных зон в локальную зону будет игнорироваться до тех пор, пока не будет явно разрешен политикой фильтрации.

Аналогично, если применить политику фильтрации, явно разрешающую трафик, направленный из локальной зоны в другую зону, трафик во все остальные зоны будет

игнорироваться до тех пор, пока не будет явно разрешен политикой фильтрации.

Следует обратить внимание на следующие дополнительные моменты, касающиеся межсетевых экранов на основе зон.

- Интерфейс может быть связан только с одной зоной.
- К интерфейсу, принадлежащему к зоне, не может быть применён индивидуальный для этого интерфейса набор правил межсетевого экрана, и наоборот.
- Трафик между интерфейсами, не принадлежащими ни к какой зоне, передается без фильтрации, и к этим интерфейсам могут быть применены индивидуальные наборы правил межсетевого экрана.
- По умолчанию весь трафик в зону игнорируется, если он не разрешён явно политикой фильтрации для зоны-отправителя.
- Политики фильтрации являются однонаправленными: они определяются как “пара зон”, определяющая зону, откуда исходит трафик (зона-отправитель) и зону, куда трафик адресован (зона-получатель ).

На рис. 50 можно увидеть следующие однонаправленные политики:

- Из закрытой зоны в DMZ.
- Из общедоступной зоны в DMZ.
- Из закрытой зоны в общедоступную зону.
- Из DMZ в общедоступную зону.
- Из общедоступной зоны в закрытую зону.
- Из DMZ в закрытую зону.

### 14.1.9. Межсетевой экран 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 правила межсетевого экрана IPv4 и правила межсетевого экрана IPv6 полностью независимы. Пакеты IPv4 не проверяются по правилам в наборах правил IPv6, и пакеты IPv6 не проверяются по правилам в наборах правил IPv4. Пакеты каждой версии протокола IP не проверяются по правилам в таблице для другой версии протокола IP; 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 к межсетевым экранам 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.

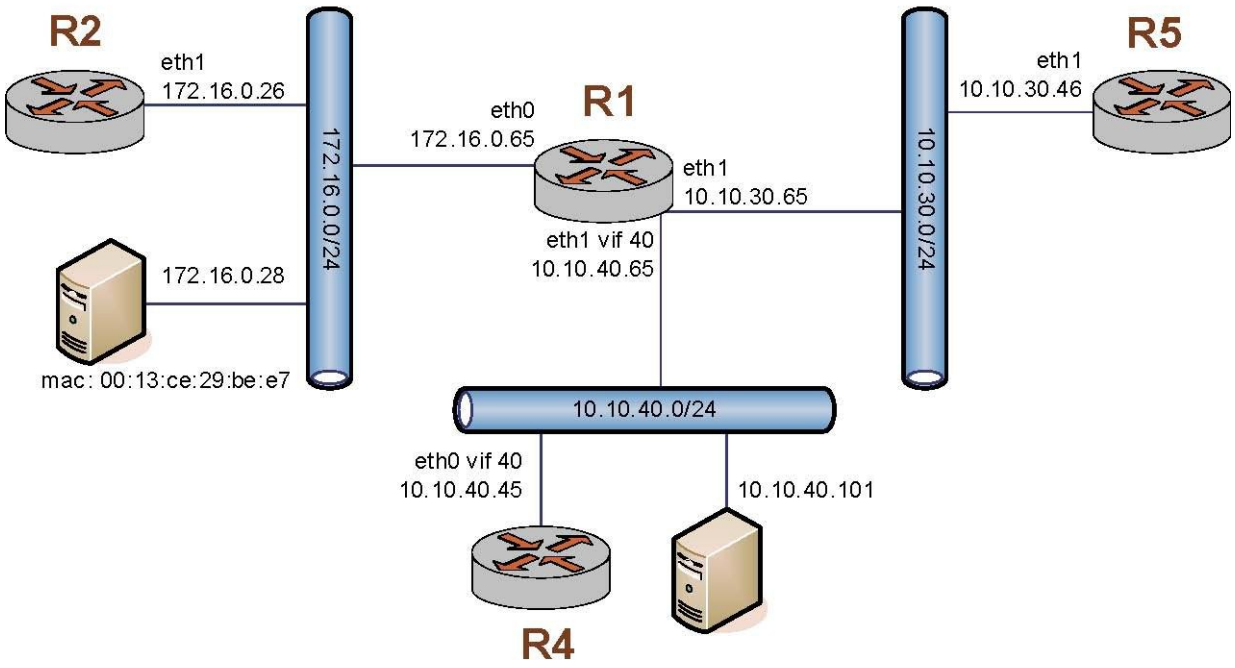
## 14.2. Примеры настройки

В этом разделе рассматриваются следующие вопросы:

- Фильтрация по IP-адресу отправителя.
- Фильтрация по IP-адресам отправителя и получателя.
- Фильтрация по IP-адресу отправителя и протоколу получателя.
- Определение межсетевого фильтра.
- 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.
- Настройка межсетевого экрана на основе зон.

В данном разделе описан пример настройки для межсетевого экрана. После выполнения всех действий на маршрутизаторе R1 будет настроен межсетевой экран, как показано на рис. 51.

*Рисунок 51 - Настройка межсетевого экрана*




В этом разделе есть следующие примеры:

- Пример 14.1 Фильтрация по IP-адресу отправителя.
- Пример 14.2 Фильтрация по IP-адресам отправителя и получателя.
- Пример 14.3 Фильтрация по IP-адресу отправителя и протоколу получателя.
- Пример 14.4 Определение межсетевого фильтра.
- Пример 14.5 Фильтрация по MAC-адресу отправителя.
- Пример 14.6 Исключение адреса.
- Пример 14.7 Активация в течение указанных периодов времени.
- Пример 14.8 Ограничение скорости для конкретных входящих пакетов.
- Пример 14.9 Принятие пакетов с установленными конкретными флагами TCP.
- Пример 14.10 Принятие пакетов ICMP с конкретными именами типов.
- Пример 14.11 Отклонение трафика на основе групп адресов, сетей или портов.
- Пример 14.12 Игнорирование попыток подключения от одного и того же отправителя при превышении указанного порога их числа за данный промежуток времени.

### 14.2.1. Фильтрация по IP-адресу отправителя

В примере 14.1 выполняется определение экземпляра межсетевого экрана, состоящего из одного правила для фильтрации только по IP-адресу отправителя. Это правило будет отклонять пакеты, приходящие с маршрутизатора R2. Затем экземпляр межсетевого экрана применяется ко входящим пакетам на интерфейсе **eth0**.

Для создания экземпляра для фильтрации по IP-адресу отправителя выполните следующие действия в режиме настройки:

*Пример 14.1 - Фильтрация по IP-адресу отправителя*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для межсетевого экрана FWTEST-1 и его правила Rule 1. Это правило отклоняет трафик, соответствующий указанным критериям. | admin@R1# **set firewall name FWTEST-1 rule 1 action reject**<br>[edit] |
| Это правило применяется к трафику, отправителем которого является 176.16.0.26. | admin@R1# **set firewall name FWTEST-1 rule 1 source address 172.16.0.26**<br>[edit] |
| Применение FWTEST-1 ко входящим пакетам на eth0. | admin@R1# **set interfaces ethernet eth0 firewall in name FWTEST-1**<br>[edit] |
| Фиксация настройки. | admin@R1# **commit**<br>[edit] |

### 14.2.2. Фильтрация по IP-адресам отправителя и получателя

В примере 14.2 определяется ещё один экземпляр межсетевого экрана. Он состоит из одного правила для фильтрации на основе IP-адресов как отправителя, так и получателя. Это правило принимает пакеты, исходящие из маршрутизатора R5 через интерфейс **eth1** с адресом 10.10.30.46 и предназначенные адресу 10.10.40.101. Затем экземпляр межсетевого

экрана применяется к пакетам, исходящим из виртуального интерфейса **vif 1** на интерфейсе **eth1**.

Для создания экземпляра для фильтрации по IP-адресу отправителя и получателя выполните следующие действия в режиме настройки:

*Пример 14.2 - Фильтрация по IP-адресам отправителя и получателя*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для межсетевого экрана FWTEST-1 и его правила Rule 1. Это правило указывает принять трафик, соответствующий указанным критериям. | admin@R1# **set firewall name FWTEST-2 rule 1 action accept**<br>[edit] |
| Это правило применяется к трафику, отправителем которого является 10.10.30.46. | admin@R1# **set firewall name FWTEST-2 rule 1 source address 10.10.30.46**<br>[edit] |
| Это правило применяется к трафику, получателем которого является 10.10.40.101. | admin@R1# **set firewall name FWTEST-2 rule 1 destination address 10.10.40.101**<br>[edit] |
| Применение FWTEST-2 к исходящим пакетам на eth1 vif 40. | admin@R1# **set interfaces ethernet eth1 vif 40 firewall out name FWTEST-2**<br>[edit] |
| Фиксация настройки. | admin@R1# **commit**<br>[edit] |

### 14.2.3. Фильтрация по IP-адресу отправителя и протоколу получателя

В примере 14.3 определяется правило межсетевого экрана для фильтрации по IP-

адресу отправителя и протоколу получателя. Это правило разрешает пакеты TCP, исходящие с адреса 10.10.30.46 (это маршрутизатор R5) и предназначенные для порта Telnet на R1. Экземпляр применяется к локальным пакетам (то есть пакетам, предназначенным для данного маршрутизатора R1), приходящим через eth1.

Для создания экземпляра для фильтрации по IP-адресу отправителя и протоколу получателя выполните следующие действия в режиме настройки:

*Пример 14.3 - Фильтрация по IP-адресу отправителя и протоколу получателя*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для межсетевого экрана FWTEST-3 и его правила Rule 1. Это правило принимает трафик, соответствующий указанным критериям. | admin@R1# **set firewall name FWTEST-3 rule 1 action accept**<br>[edit] |
| Это правило применяется к трафику, отправителем которого является 10.10.30.46. | admin@R1# **set firewall name FWTEST-3 rule 1 source address 10.10.30.46**<br>[edit] |
| Это правило применяется к трафику TCP. | admin@R1# **set firewall name FWTEST-3 rule 1 protocol tcp**<br>[edit] |
| Это правило применяется к трафику, предназначенному для службы Telnet. | admin@R1# **set firewall name FWTEST-3 rule 1 destination port telnet**<br>[edit] |
| Применение FWTEST-3 к пакетам, предназначенным для данного маршрутизатора и приходящим на eth1. | admin@R1# **set interfaces ethernet eth1 firewall local name FWTEST-3**<br>[edit] |
| Фиксация настройки. | admin@R1# **commit**<br>[edit] |

### 14.2.4. Определение межсетевого фильтра

В примере 14.4 выполняется создание межсетевого пакетного фильтра, разрешающего пакеты, исходящие из 10.10.40.0/24 и предназначенные для 172.16.0.0/24. Затем экземпляр межсетевого фильтра применяется ко входящим пакетам с виртуального интерфейса vif 40 на интерфейсе eth1.

Для создания межсетевого фильтра выполните следующие действия в режиме настройки:

*Пример 14.4 - Определение межсетевого фильтра*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для межсетевого экрана FWTEST-4 и его правила Rule 1. Это правило принимает трафик, соответствующий указанным критериям. | admin@R1# **set firewall name FWTEST-4 rule 1 action accept**<br>[edit] |
| Это правило применяется к трафику, приходящему из сети 10.10.40.0/24. | admin@R1# **set firewall name FWTEST-4 rule 1 source address 10.10.40.0/2**4<br>[edit] |
| Это правило применяется к трафику, предназначенному для сети 172.16.0.0/24. | admin@R1# **set firewall name FWTEST-4 rule 1 destination address 172.16.0.0/24**<br>[edit] |
| Применение FWTEST-4 к пакетам, предназначенным для данного маршрутизатора и приходящим через виртуальный интерфейс vif 40 на eth1. | admin@R1# **set interfaces ethernet eth1 vif 40 firewall in name FWTEST-4**<br>[edit] |
| Фиксация настройки. | admin@R1# **commit**<br>[edit] |

### 14.2.5. Фильтрация по MAC-адресу отправителя

В примере 14.5 выполняется определение экземпляра межсетевого экрана, состоящего 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. Экземпляр межсетевого экрана применяется ко входящим пакетам на интерфейсе eth0.

Для создания экземпляра для фильтрации по MAC-адресу отправителя выполните следующие действия в режиме настройки:

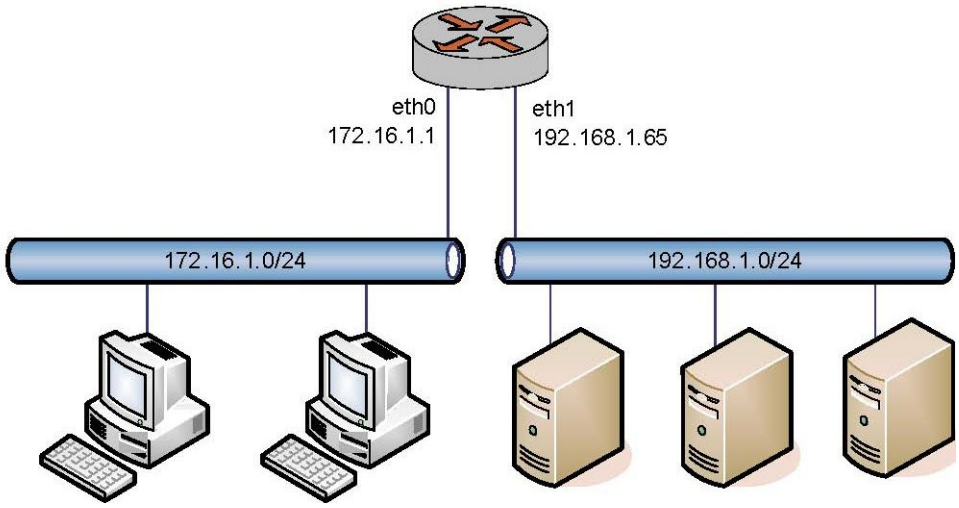
*Пример 14.5 - Фильтрация по MAC-адресу отправителя*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для межсетевого экрана FWTEST-5 и его правила Rule 1. Это правило принимает трафик, соответствующий указанным критериям. | admin@R1# **set firewall name FWTEST-5 rule 1 action accept**<br>[edit] |
| Это правило применяется к трафику, отправителем которого является MAC-адрес 00:13:ce:29:be:e7. | admin@R1# **set firewall name FWTEST-5 rule 1 source mac-address 00:13:ce:29:be:e7**<br>[edit] |
| Применение FWTEST-5 ко входящим пакетам на eth0. | admin@R1# **set interfaces ethernet eth0 firewall in name FWTEST-5**<br>[edit] |
| Фиксация настройки. | admin@R1# **commit**<br>[edit] |

### 14.2.6. Исключение адреса

Правило межсетевого экрана, показанное в примере 14.6, разрешает весь трафик из сети 172.16.1.0/24, за исключением того, который предназначен серверу 192.168.1.100.

*Рисунок 52 - Исключение адреса*




Для создания экземпляра для исключения адреса выполните следующие действия в режиме настройки:

*Пример 14.6 - Исключение адреса*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для межсетевого экрана FWTEST-5 и правила 10. Ввод описания для правила. | admin@R1# **set firewall name NEGATED-EXAMPLE rule 10 description "Allow all traffic from LAN except to server 192.168.1.100"**<br>[edit] |
| Весь трафик, соответствующий правилу, будет принят. | admin@R1# **set firewall name NEGATED-EXAMPLE rule 10 action accept**<br>[edit] |
| Любой трафик из сети 172.16.1.0/24 соответствует правилу. | admin@R1# **set firewall name NEGATED-EXAMPLE rule 10 source address 172.16.1.0/24**<br>[edit] |

Трафик, предназначенный для любого узла назначения, КРОМЕ 192.168.1.100, соответствует правилу. Трафик, не соответствующий правилу, вызывает переход к правилу по умолчанию "**reject all**".

```
admin@R1# set firewall name
NEGATED-EXAMPLE rule 10
destination address !
192.168.1.100
[edit]
```

Применение экземпляра NEGATED-EXAMPLE ко входящим пакетам на eth0.

```
admin@R1# set interfaces ethernet
eth0 firewall in name NEGATED-
EXAMPLE
[edit]
```

Фиксация настройки.

```
admin@R1# commit
[edit]
```

Вывод настройки.

```
admin@R1# show firewall
name NEGATED-EXAMPLE {
     rule 10 {
          action accept
          description "Allow all
traffic from LAN except to server
192.168.1.100"
          destination {
               address !
192.168.1.100
               }
          source {
               address
172.16.1.0/24
          }
     }
}
[edit]
admin@R1# show interfaces
```

```
ethernet eth0
address 172.16.1.1/24
firewall {
     in {
          name NEGATED-EXAMPLE
     }
}
[edit]
```

### 14.2.7. Активация в течение указанных периодов времени

Altell NEO поддерживает фильтрацию с учетом даты и времени. Для правил межсетевого экрана существует возможность указать время, которое будет определять период действия правила.

Правило межсетевого экрана, показанное в примере 14.7, ограничивает время активности правила, настроенного в примере 14.6, интервалом с 9:00 до 17:00 по понедельникам. для добавления ограничения к правилу выполните следующие действия в режиме настройки:

*Пример 14.7 - Активация в течение указанных периодов времени*

| Действие | Команда |
|---|---|
| Установка времени начала действия на 9:00. | admin@R1# **set firewall name NEGATED-EXAMPLE rule 10 time starttime 09:00:00**<br>[edit] |
| Установка времени окончания действия на 17:00. | admin@R1# **set firewall name NEGATED-EXAMPLE rule 10 time stoptime 17:00:00**<br>[edit] |
| Установка дней недели. | admin@R1# **set firewall name NEGATED-EXAMPLE rule 10 time weekdays Mon,Tue,Wed,Thu,Fri** |

```
[edit]
```

Фиксация настройки.

```
admin@R1# commit
[edit]
```

Вывод настройки.

```
admin@R1# show firewall
name NEGATED-EXAMPLE {
     rule 10 {
          action accept
          description "Allow all
traffic from LAN except to server
192.168.1.100"
          destination {
               address !
192.168.1.100
          }
          source {
               address
172.16.1.0/24
          }
          time {
               starttime 09:00:00
               stoptime 17:00:00
               weekdays
Mon,Tue,Wed,Thu,Fri
          }
     }
}
[edit]
admin@R1# show interfaces
ethernet eth0
address 172.16.1.1/24
firewall {
```

```
        in {
            name NEGATED-EXAMPLE
        }
    }
[edit]
```

### 14.2.8. Ограничение скоростей передачи трафика

Для ограничения скорости прохождения входящих пакетов можно использовать правило межсетевого экрана, включающее фильтр TBF (Token Bucket Filter), работающий по алгоритму маркерного ведра. Частота проходящих пакетов ограничивается административно установленным значением, но возможно ее превышение для коротких групп пакетов.

Например, для создания правила, ограничивающего частоту пакетов эхо-запросов ICMP (пингов) до двух в секунду, но дающего возможность кратковременного превышения этой частоты без игнорирования пакетов, выполните следующие действия в режиме настройки:

*Пример 14.8 - Ограничение скорости для конкретных входящих пакетов*

| Действие | Команда |
|---|---|
| Установка ICMP в качестве протокола-образца для проверки совпадения. | admin@R1# **set firewall name RATE-LIMIT rule 20 protocol icmp**<br>[edit] |
| Установка типа ICMP на 8 (эхо-запрос). | admin@R1# **set firewall name RATE-LIMIT rule 20 icmp type 8**<br>[edit] |
| Установка кода ICMP на 0 для типа 8 | admin@R1# **set firewall name RATE-LIMIT rule 20 icmp code 0**<br>[edit] |
| Установка требуемой частоты в 2 пакета в секунду. | admin@R1# **set firewall name RATE-LIMIT rule 20 limit rate 2/second**<br>[edit] |

Установка размера группы в 5 пакетов.

```
admin@R1# set firewall name RATE-
LIMIT rule 20 limit burst 5
[edit]
```

Установка принятия в качестве действия.

```
admin@R1# set firewall name RATE-
LIMIT rule 20 action accept
[edit]
```

Установка описания.

```
admin@R1# set firewall name RATE-
LIMIT rule 20 description “Rate-
limit incoming icmp echo-request
packets to 2/second allowing
short bursts of 5 packets”
[edit]
```

Фиксация настройки.

```
admin@R1# commit
[edit]
```

Вывод настройки.

```
admin@R1# show firewall name
RATE-LIMIT
rule 20 {
     action accept
     description "Rate-limit
incoming icmp
echo-request packets to 2/second
allowing short bursts of 5
packets"
     icmp {
          code 0
          type 8
     }
     limit {
          burst 5
          rate 2/second
```

```
        }
        protocol icmp
}
[edit]
admin@R1#
```

### 14.2.9. Проверка соответствия флагов TCP

Altell NEO 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 14.9 - Принятие пакетов с установленными конкретными флагами TCP*

| Действие | Команда |
|---|---|
| Установка TCP в качестве протокола-образца для проверки совпадения. | admin@R1# **set firewall name TCP-FLAGS rule 30 protocol tcp**<br>[edit] |
| Установка флагов TCP для проверки совпадения. | admin@R1# **set firewall name TCP-FLAGS rule 30 tcp flags SYN,!ACK,!FIN,!RST**<br>[edit] |
| Установка принятия в качестве действия. | admin@R1# **set firewall name TCP-FLAGS rule 30 action accept**<br>[edit] |
| Фиксация настройки. | admin@R1# **commit**<br>[edit] |
| Вывод настройки. | admin@R1# **show firewall name TCP-FLAGS**<br>rule 30 {<br>action accept<br>protocol tcp |

```
        tcp {
            flags SYN,!ACK,!FIN,!
RST
        }
}
[edit]admin@R1#
```

### 14.2.10. Проверка соответствия имен типов ICMP

Пакеты можно фильтровать по именам типов ICMP. Например, для создания правила, разрешающего прохождение только пакетов эхо-запроса ICMP, выполните следующие действия в режиме настройки:

*Пример 14.10 - Принятие пакетов ICMP с конкретными именами типов*

| Действие | Команда |
|---|---|
| Установка ICMP в качестве протокола-образца для проверки совпадения. | admin@R1#**set firewall name ICMP-NAME rule 40 protocol icmp**<br>[edit] |
| Установка типа пакетов ICMP для проверки совпадения. | admin@R1# **set firewall name ICMP-NAME rule 40 icmptype-name echo-request**<br>[edit] |
| Установка принятия в качестве действия. | admin@R1# **set firewall name ICMP-NAME rule 40 action accept**<br>[edit] |
| Фиксация настройки. | admin@R1# **commit**<br>[edit] |
| Вывод настройки. | admin@R1# **show firewall**<br>name ICMP-NAME<br>rule 40 {action accept protocol<br>icmp icmp {type-name echo-request |

```
}}
[edit]
admin@R1#
```

### 14.2.11. Проверка соответствия групп

Можно определить группы адресов, портов и сетей для аналогичной фильтрации. Например, для создания правила, отклоняющего трафик на группу адресов и портов из группы сетей, выполните следующие действия в режиме настройки:

*Пример 14.11 - Отклонение трафика на основе групп адресов, сетей или портов*

| Действие | Команда |
|---|---|
| Добавление диапазона адресов в группу адресов. | admin@R1# **set firewall group address-group SERVERS address 1.1.1.1-1.1.1.5**<br>[edit] |
| Добавление еще одного адреса в группу адресов. | admin@R1# **set firewall group address-group SERVERS address 1.1.1.7**<br>[edit] |
| Добавление сети в группу сетей. | admin@R1# **set firewall group network-group NETWORKS network 10.0.10.0/24**<br>[edit] |
| Добавление порта в группу портов. | admin@R1# **set firewall group port-group PORTS port 22**<br>[edit] |
| Добавление имени порта в группу портов. | admin@R1# **set firewall group port-group PORTS port ftp**<br>[edit] |
| Добавление диапазона портов в группу | admin@R1# **set firewall group** |

| | |
|---|---|
| портов. | **port-group PORTS port 1000-2000**<br>[edit] |
| Фиксация настройки. | admin@R1# **commit**<br>[edit] |
| Вывод настройки. | admin@R1# **show firewall group**<br>group {<br>address-group SERVERS {<br>address 1.1.1.1-1.1.1.5<br>address 1.1.1.7<br>}<br>network-group NETWORKS {<br>network 10.0.10.0/24<br>}<br>port-group PORTS {<br>port 22<br>port ftp<br>port 1000-2000<br>}<br>}<br>[edit]<br>admin@R1# |
| Указание действия отклонения в экземпляре межсетевого экрана. | admin@R1# **set firewall name REJECT-GROUPS rule 10 action reject**<br>[edit] |
| Указание группы адресов получателей в качестве образца для проверки совпадения. | admin@R1# **set firewall name REJECT-GROUPS rule 10 destination group address-group SERVERS**<br>[edit] |
| Указание группы портов получателей в | admin@R1# s**et firewall name** |

качестве образца для проверки совпадения.

```
REJECT-GROUPS rule 10 destination
group port-group PORTS
[edit]
```

Указание группы сетей отправителей в качестве образца для проверки совпадения.

```
admin@R1# set firewall name
REJECT-GROUPS rule 10 source
group network-group NETWORKS
[edit]
```

Фиксация настройки.

```
admin@R1# commit
[edit]
```

Вывод настройки.

```
admin@R1# show firewall name
REJECT-GROUPS
rule 10{
     action reject
     destination {
          group {
               address-group
SERVERS
               port-group PORTS
               }
          }
     source {
          group {
               network-group
NETWORKS
          }
     }
}
[edit]
admin@R1#
```

### 14.2.12. 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 14.12 - Игнорирование попыток подключения от одного и того же отправителя при превышении указанного порога их числа за данный промежуток времени*

| Действие | Команда |
|---|---|
| Проверка пакетов TCP. | admin@R1# **set firewall name STOP-BRUTE rule 10 protocol tcp**<br>[edit] |
| Проверка порта назначение на совпадение с 22 (т.е. ssh). | admin@R1# s**et firewall name STOP-BRUTE rule 10 destination port 22**<br>[edit] |
| Проверка числа попыток подключения. | admin@R1# **set firewall name STOP-BRUTE rule 10 state new enable**<br>[edit] |
| Проверка трехкратного повторения адресов отправителя ... | admin@R1# **set firewall name STOP-BRUTE rule 10 recent count 3**<br>[edit] |
| ... в течение 30 секунд. | admin@R1# **set firewall name STOP-BRUTE rule 10 recent time 30**<br>[edit] |
| Игнорирование пактов, | admin@R1# **set firewall name STOP-** |

удовлетворяющих этим критериям.

```
BRUTE rule 10 action drop
[edit]
```

Фиксация настройки.

```
admin@R1# commit
[edit]
```

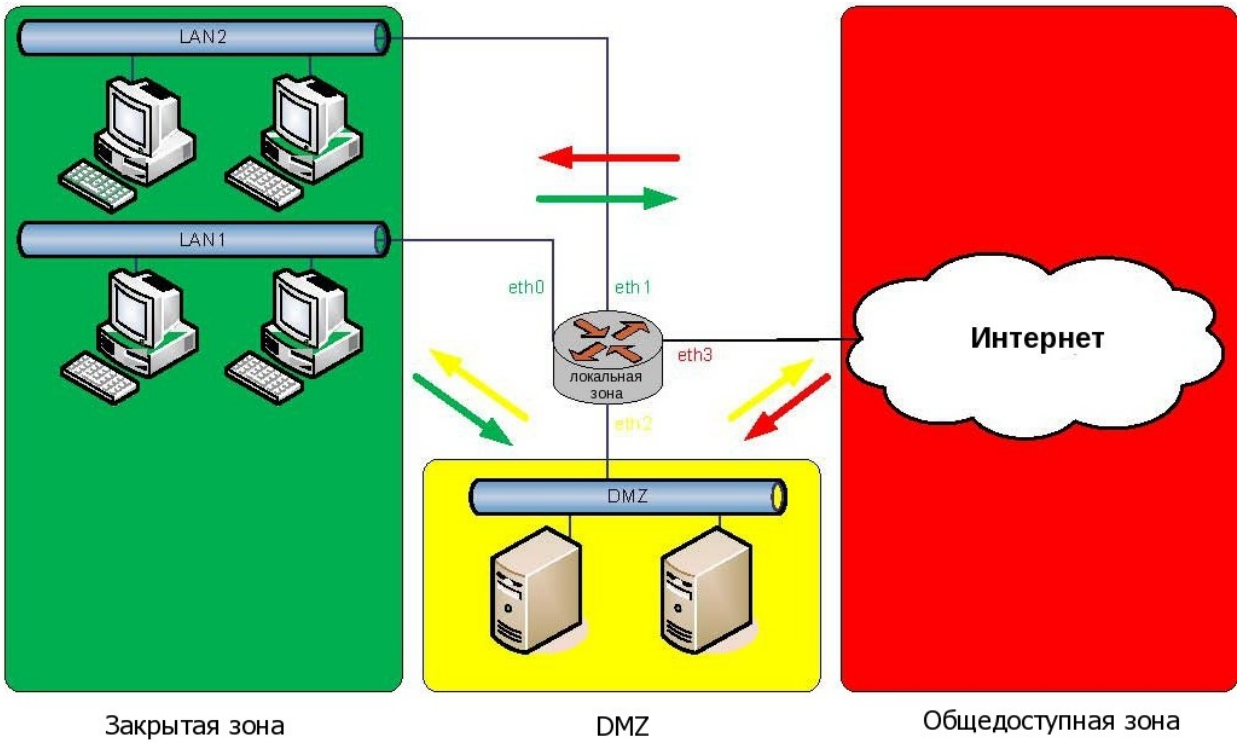
Вывод настройки.

```
admin@R1# show firewall name
STOP-BRUTE
rule 10{
     action drop
     destination {
          port 22
     }
     protocol tcp
     recent {
          count 3
          time 30
     }
     state {
          new enable
     }
}
[edit]
admin@R1#
```

### 14.2.13. Настройка межсетевого экрана на основе зон

Системой Altell NEO поддерживается еще одна модель межсетевого экрана - это модель на основе зон. На рис. 53 показана настройка на основе зон с тремя зонами, определенными пользователем. В приведенных ниже примерах показана настройка для этого рисунка.

*Рисунок 53 - Настройка межсетевого экрана на основе зон безопасности*




### 14.2.14. Фильтрация трафика между транзитными зонами

Для создания политик зон выполните следующие действия в режиме настройки:

*Пример 14.13 - Создание политик зон*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для зоны DMZ и ввод описания для этой зоны. | `admin@R1# set zone-policy zone dmz description "DMZ ZONE"`<br>`[edit]` |
| Добавление интерфейса, содержащегося в зоне. | `admin@R1# set zone-policy zone dmz interface eth2`<br>`[edit]` |
| Создание узла конфигурации для закрытой зоны и ввод описания для этой зоны. | `admin@R1# set zone-policy zone private description "PRIVATE ZONE"` |

```
[edit]
```

Добавление одного из интерфейсов, содержащихся в зоне.

```
admin@R1# set zone-policy zone private interface eth0
[edit]
```

Добавление еще одного интерфейса, содержащегося в зоне.

```
admin@R1# set zone-policy zone private interface eth1
[edit]
```

Создание узла конфигурации для общедоступной зоны и ввод описания для этой зоны.

```
admin@R1# set zone-policy zone public description “PUBLIC ZONE”
[edit]
```

Добавление интерфейса, содержащегося в зоне.

```
admin@R1# set zone-policy zone public interface eth3
[edit]
```

Фиксация настройки.

```
admin@R1# commit
[edit]
```

Вывод настройки.

```
admin@R1# show zone-policy
zone dmz {
     description "DMZ ZONE"
     interface eth2
}
zone private {
     description "PRIVATE ZONE"
     interface eth0
     interface eth1
}
zone public {
     description "PUBLIC ZONE"
     interface eth3
}
```

```
[edit]
```

В данный момент никакой передачи трафика между зонами нет. Весь трафик, передаваемый из одной зоны в другую, будет проигнорирован. Следует заметить, что поскольку интерфейсы **eth0** и **eth1** лежат в одной и той же зоне, передача трафика между ними происходит беспрепятственно. Теперь будут созданы наборы правил межсетевого экрана для разрешения передачи трафика между зонами. В первую очередь создается набор правил для трафика в общедоступную зону.

*Пример 14.14 - Создание набора правил межсетевого экрана для трафика в общедоступную зону*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для набора правил to_public и ввод описания для этого набора. | admin@R1# **set firewall name to_public description "allow all traffic to PUBLIC zone"**<br>[edit] |
| Создание правила для принятия всего трафика, передаваемого в общедоступную зону. | admin@R1# **set firewall name to_public rule 1 action accept**<br>[edit] |
| Фиксация настройки. | admin@R1# **commit**<br>[edit] |
| Вывод настройки межсетевого экрана. | admin@R1# **show firewall name to_public**<br>description "allow all traffic to PUBLIC zone"<br>rule 1 {<br>action accept<br>}<br>[edit] |

Затем создаются наборы правил для трафика в зону DMZ.

*Пример 14.15 - Создание правил межсетевого экрана для трафика в зону DMZ*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для набора правил private_to_dmz и ввод описания для этого набора. | admin@R1# **set firewall name private_to_dmz description "filter traffic from PRIVATE zone to DMZ zone"**<br>[edit] |
| Создание правила для разрешения прохождения трафика, передаваемого из закрытой зоны на определенные порты в зоне DMZ. | admin@R1# **set firewall name private_to_dmz rule 1 action accept**<br>[edit]<br>admin@R1# **set firewall name private_to_dmz rule 1 destination port http,https,ftp,ssh,telnet**<br>[edit]<br>admin@R1# **set firewall name private_to_dmz rule 1 protocol tcp**<br>[edit] |
| Создание правила для разрешения прохождения всего трафика icmp из закрытой зоны в зону DMZ. | admin@R1# **set firewall name private_to_dmz rule 2 action accept**<br>[edit]<br>admin@R1# **set firewall name private_to_dmz rule 2 icmp type-name any**<br>[edit]<br>admin@R1# **set firewall name private_to_dmz rule 2 protocol icmp** |

```
[edit]
```

Фиксация настройки.

```
admin@R1# commit
[edit]
```

Вывод настройки межсетевого экрана.

```
admin@R1# show firewall name
private_to_dmz
description "filter traffic from
PRIVATE zone to DMZ zone"
rule 1 {
     action accept
     destination {
          port
http,https,ftp,ssh,telnet
     }
     protocol tcp
}
rule 2 {
     action accept
     icmp {
          type-name any
     }
     protocol icmp
}
[edit]
```

Создание узла конфигурации для набора правил public_to_dmz и ввод описания для этого набора.

```
admin@R1# set firewall name
public_to_dmz description "filter
traffic from PUBLIC zone to DMZ
zone"
[edit]
```

Создание правила для разрешения прохождения трафика, передаваемого из

```
admin@R1# set firewall name
public_to_dmz rule 1 action
```

| | |
|---|---|
| общедоступной зоны на определенные порты в зоне DMZ. | **accept**<br>[edit]<br>admin@R1# **set firewall name public_to_dmz rule 1 destination port http,https**<br>[edit]<br>admin@R1# **set firewall name public_to_dmz rule 1 protocol tcp**<br>[edit] |
| Создание правила для разрешения прохождения всего трафика icmp из общедоступной зоны в зону DMZ. | admin@R1# **set firewall name public_to_dmz rule 2 action accept**<br>[edit]<br>admin@R1# **set firewall name public_to_dmz rule 2 icmp type-name any**<br>[edit]<br>admin@R1# **set firewall name public_to_dmz rule 2 protocol icmp**<br>[edit] |
| Фиксация настройки. | admin@R1# **commit**<br>[edit] |
| Вывод настройки межсетевого экрана. | admin@R1# **show firewall name public_to_dmz**<br>description "filter traffic from PUBLIC zone to DMZ zone"<br>rule 1 {<br>action accept<br>destination {<br>port http,https |

```
        }
        protocol tcp
    }
    rule 2 {
        action accept
        icmp {
            type-name any
        }
        protocol icmp
    }
    [edit]
```

Теперь создается набор правил для трафика, передаваемого в закрытую зону.

*Пример 14.16 - Создание набора правил межсетевого экрана для трафика, передаваемого в закрытую зону*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для набора правил to_private и ввод описания для этого набора. | admin@R1# **set firewall name to_private description "filter traffic to PRIVATE zone"**<br>[edit] |
| Создание правила для разрешения прохождения в закрытую зону только трафика, исходящего из этой зоны (т.е. ранее установленные сеансы и связанный с ними трафик). | admin@R1# **set firewall name to_private rule 1 action accept**<br>[edit]<br>admin@R1# **set firewall name to_private rule 1 state established enable**<br>[edit]<br>admin@R1# **set firewall name to_private rule 1 state related enable**<br>[edit] |

| | |
|---|---|
| | admin@R1# **set firewall name to_private rule 1 protocol all**<br>[edit] |
| Фиксация настройки. | admin@R1# **commit**<br>[edit] |
| Вывод настройки межсетевого экрана. | admin@R1# **show firewall name to_private**<br>description "filter traffic to PRIVATE zone"<br>rule 1 {<br>action accept<br>protocol all<br>state {<br>established enable<br>related enable<br>}<br>}<br>[edit] |

Теперь эти наборы правил применяются для фильтрации трафика между зонами. Сначала для зоны DMZ.

*Пример 14.17 - Применение наборов правил для зоны DMZ*

| Действие | Команда |
|---|---|
| Применение набора правил private_to_dmz к трафику, передаваемому из закрытой зоны в зону DMZ. | admin@R1# **set zone-policy zone dmz from private firewall name private_to_dmz**<br>[edit] |
| Применение набора правил public_to_dmz к трафику, передаваемому из общедоступной зоны в зону DMZ. | admin@R1# **set zone-policy zone dmz from public firewall name public_to_dmz** |

| | |
|---|---|
| | [edit] |
| Фиксация настройки. | admin@R1# **commit**<br>[edit] |
| Вывод настройки политики для зоны DMZ. | admin@R1# **show zone-policy zone dmz**<br>description "DMZ ZONE"<br>from private {<br>  firewall {<br>  name private_to_dmz<br>  }<br>}<br>from public {<br>  firewall {<br>  name public_to_dmz<br>  }<br>}<br>interface eth2<br>[edit] |

Затем для закрытой зоны.

*Пример 14.18 - Применение наборов правил к закрытой зоне*

| Действие | Команда |
|---|---|
| Применение набора правил to_private к трафику из зоны DMZ в закрытую зону. | admin@R1# **set zone-policy zone private from dmz firewall name to_private**<br>[edit] |
| Применение набора правил to_private к трафику из общедоступной зоны в закрытую зону. | admin@R1# **set zone-policy zone private from public firewall name to_private**<br>[edit] |

| | |
|---|---|
| Фиксация настройки. | admin@R1# **commit**<br>[edit] |
| Вывод настройки политики для закрытой зоны. | admin@R1# **show zone-policy zone private**<br>description "PRIVATE ZONE"<br>from dmz {<br>  firewall {<br>  name to_private<br>  }<br>}<br>from public {<br>  firewall {<br>  name to_private<br>  }<br>}<br>interface eth0<br>interface eth1<br>[edit] |

И, наконец, для общедоступной зоны.

*Пример 14.19 - Применение наборов правил к общедоступной зоне*

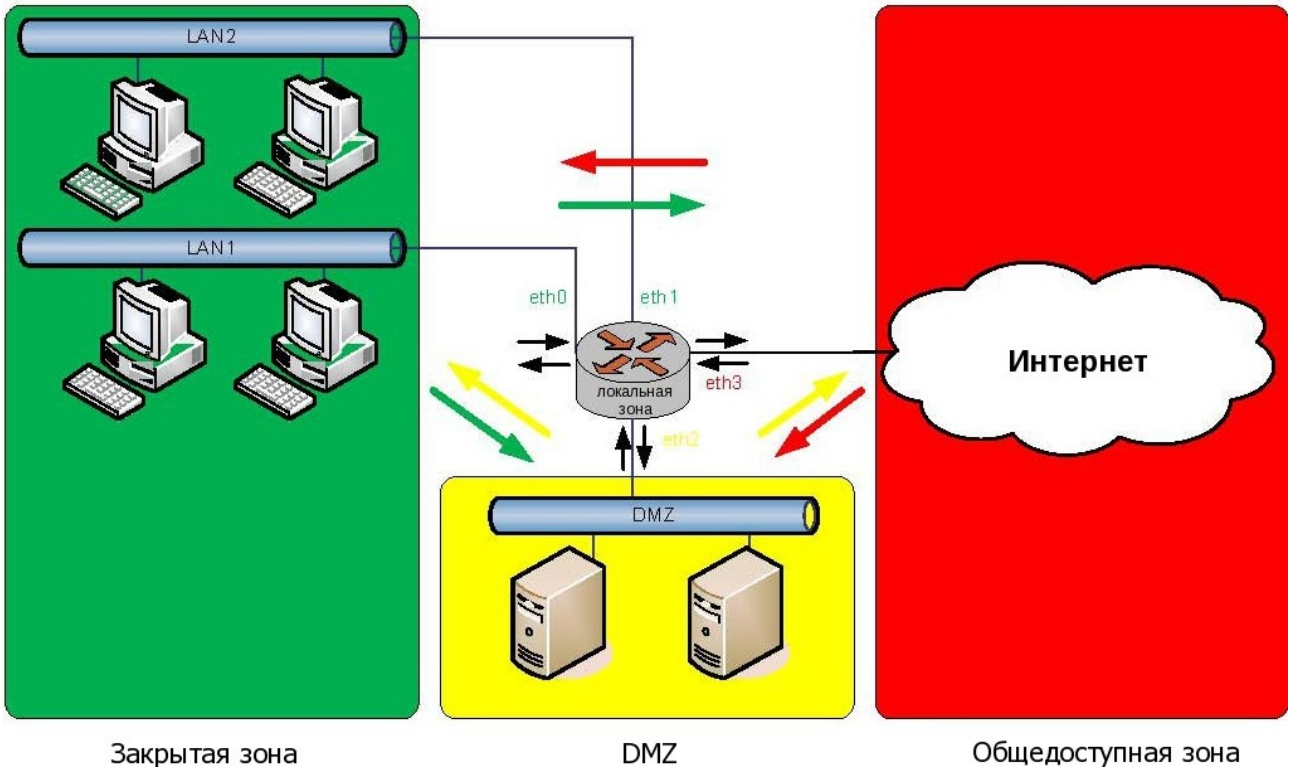
| Действие | Команда |
|---|---|
| Применение набора правил to_public к трафику, передаваемому из зоны DMZ в общедоступную зону. | admin@R1# **set zone-policy zone public from dmz firewall name to_public**<br>[edit] |
| Применение набора правил to_pubic к трафику, передаваемому из закрытой зоны в общедоступную зону. | admin@R1# **set zone-policy zone public from private firewall name to_public**<br>[edit] |

| | |
|---|---|
| Фиксация настройки. | admin@R1# **commit**<br>[edit] |
| Вывод настройки политики для общедоступной зоны. | admin@R1# **show zone-policy zone public**<br>description "PUBLIC ZONE"<br>from dmz {<br>  firewall {<br>  name to_public<br>  }<br>}<br>from private {<br>  firewall {<br>  name to_public<br>  }<br>}<br>interface eth3<br>[edit] |

### 14.2.15. Фильтрация трафика из локальной зоны и в локальную зону

Локальная зона - это особая зона, относящаяся к самой системе Altell NEO. По умолчанию разрешается прохождение всего трафика, предназначенного для системы и исходящего из неё. На рис. 54 изображены стрелки, символизирующие передачу трафика в транзитные зоны и из транзитных зон (закрытой (зеленый цвет), DMZ (желтый цвет) и общедоступной (красный цвет)), а также в локальную зону и из локальной зоны.

*Рисунок 54 - Передача трафика в транзитные зоны и из транзитных зон*




Для создания настройки, ограничивающей доступ к системе Altell NEO узлами, расположенными в закрытой зоне, выполните следующие действия в режиме настройки:

В данный момент разрешено прохождение только трафика из закрытой зоны, предназначенного системе Altell NEO.

*Пример 14.20 - Ограничение доступа к системе Altell NEO узлами, расположенными в закрытой зоне*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для набора правил **private_to_neo** и ввод описания для этого набора правил. | `admin@R1# set firewall name private_to_neo description "filter traffic from PRIVATE zone to local-zone"`<br>`[edit]` |
| Разрешается прохождение всего | `admin@R1# set firewall name` |

| | |
|---|---|
| трафика. | **private_to_neo rule 1 action accept**<br>[edit] |
| Фиксация настройки. | admin@R1# **commit**<br>[edit] |
| Вывод настройки межсетевого экрана **private_to_neo**. | admin@R1# **show firewall name private_to_neo**<br>description "filter traffic from PRIVATE zone to local-zone"<br>rule 1{<br>action accept<br>}<br>[edit] |
| Применение набора правил **private_to_neo** к передаче трафика между закрытой зоной и локальной зоной. | admin@R1# **set zone-policy zone neo from private firewall name private_to_neo**<br>[edit] |
| Установка локальной зоны. | admin@R1# **set zone-policy zone neo local-zone**<br>[edit] |
| Фиксация настройки. | admin@R1# **commit**<br>[edit] |
| Вывод настройки политики для локальной зоны. | admin@R1# **show zone-policy zone neo**<br>from private {<br>firewall {<br>name private_to_neo<br>}<br>} |

```
local-zone
[edit]
```

Трафик изо всех других зон игнорируется. Однако прохождение любого трафика, исходящего из системы Altell NEO, остается разрешенным во все зоны.

***ПРИМЕЧАНИЕ*** *При определении локальной зоны следует соблюдать осторожность. Если при выполнении настройки системы по удаленному подключению (например по* ***ssh****) ограничить доступ из зоны, из которой производится настройка, то сеанс настройки будет прерван. Следует убедиться, что прохождение трафика из зоны, из которой осуществляется настройка, к системе Altell NEO разрешено.*

Не следует забывать, что есть службы (например, передача DNS и веб-прокси), которые помещают свои оконечные точки в системе Altell NEO и затем инициируют подключения к другому узлу. В случае передачи DNS пакеты, предназначенные для другого маршрутизатора для поиска некэшированной записи DNS, приводят к инициированию механизмом передачи DNS подключения ко внешнему серверу имен для получения записи DNS и последующей обратной передачи ее к клиенту, от которого исходил запрос. В приведенном выше примере настройки, где пакеты, предназначенные маршрутизатору, разрешены только из закрытой зоны, ответы на запросы поиска DNS, приходящие на маршрутизатор с внешнего сервера имен в общедоступной зоне, будут проигнорированы. Таким образом, для разрешения прохождения предназначенных для маршрутизатора пакетов из общедоступной зоны определяется набор правил, который потом применяется к локальной зоне следующим образом:

По умолчанию разрешается прохождение всего трафика, исходящего из локальной зоны.

*Пример 14.21 - Фильтрация трафика из общедоступной зоны в систему Altell NEO*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для набора правил public_to_neo и ввод описания для этого набора. | `admin@R1#` **`set firewall name public_to_neo description "filter traffic from PUBLIC zone to`** |

| | |
|---|---|
| | **local-zone”**<br>[edit] |
| Разрешение прохождения указанного трафика. | admin@R1# **set firewall name public_to_neo rule 1 action accept**<br>[edit]<br>admin@R1# **set firewall name public_to_neo rule 1 protocol all**<br>[edit]<br>admin@R1# **set firewall name public_to_neo rule 1 state established enable**<br>[edit]<br>admin@R1# **set firewall name public_to_neo rule 1 state related enable**<br>[edit] |
| Фиксация настройки. | admin@R1# **commit**<br>[edit] |
| Вывод настройки межсетевого экрана public_to_neo. | admin@R1# **show firewall name public_to_neo**<br>description "filter traffic from PUBLIC zone to local-zone"<br>rule 1{<br>action accept<br>protocol all<br>state {<br>established enable<br>related enable<br>}<br>} |

| | |
|---|---|
| | `[edit]` |
| Применение набора правил public_to_neo к трафику, передаваемому из общедоступной зоны в локальную зону. | `admin@R1# set zone-policy zone neo from public firewall name public_to_neo`<br>`[edit]` |
| Фиксация настройки. | `admin@R1# commit`<br>`[edit]` |
| Вывод новой настройки политики для локальной зоны. | `admin@R1# show zone-policy zone neo`<br>`from private {`<br>`  firewall {`<br>`  name private_to_neo`<br>`  }`<br>`}`<br>`from public {`<br>`  firewall {`<br>`  name public_to_neo`<br>`  }`<br>`}`<br>`local-zone`<br>`[edit]` |

Если нужно ограничить этот трафик, необходимо в определении транзитной зоны определить локальную зону как “зону-отправитель”. Если локальная зона используется в качестве “зоны-отправителя”, весь трафик из системы Altell NEO во все другие зоны блокируется, если он явно не разрешен с помощью набора правил, разрешающего прохождение трафика в конкретную зону.

Например, чтобы разрешить прохождение трафика из системы Altell NEO только в закрытую зону, нужно было бы выполнить следующие действия:

*Пример 14.22 - Разрешение прохождения трафика из системы Altell NEO в закрытую зону*

| Действие | Команда |
|---|---|

Создание узла конфигурации для набора правил from_neo и ввод описания для этого набора.

```
admin@R1# set firewall name
from_neo description “allow all
traffic from local-zone”
[edit]
```

Разрешение прохождения указанного трафика.

```
admin@R1# set firewall name
from_neo rule 1 action accept
[edit]
admin@R1# set firewall name
from_neo rule 1 protocol all
[edit]
```

Фиксация настройки.

```
admin@R1# commit
[edit]
```

Вывод настройки межсетевого экрана from_neo.

```
admin@R1# show firewall name
from_neo
description "allow all traffic
from local-zone"
rule 1{
     action accept
     protocol all
}
[edit]
```

Применение набора правил from_neo к трафику из локальной зоны в закрытую зону.

```
admin@R1# set zone-policy zone
private from neo firewall name
from_neo
[edit]
```

Фиксация настройки.

```
admin@R1# commit
[edit]
```

Вывод новой настройки политики для закрытой зоны.

```
admin@R1# show zone-policy zone
private
description "PRIVATE ZONE"
```

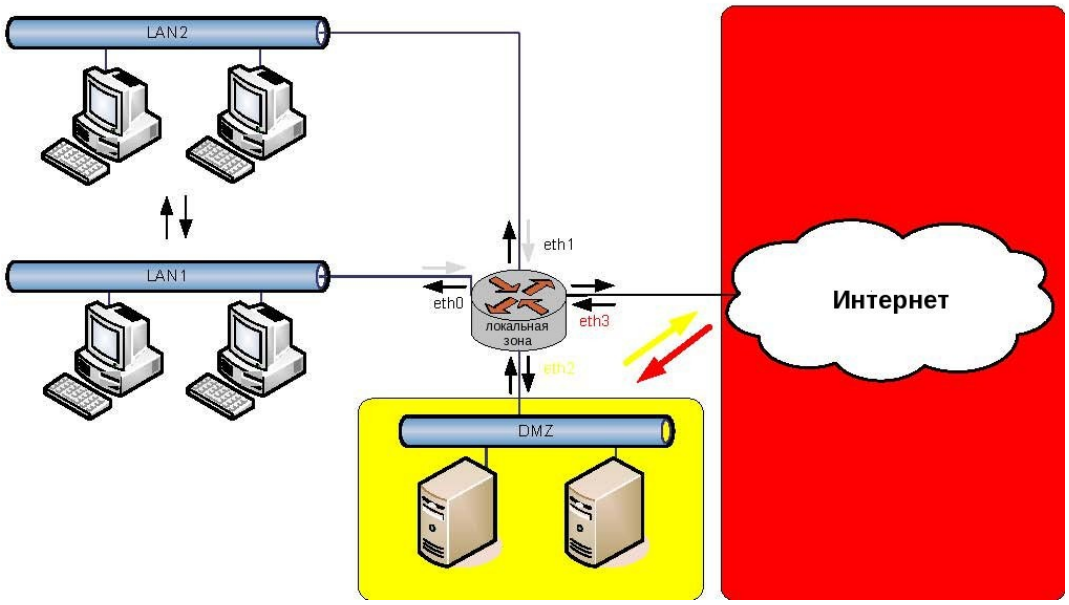
```
from dmz {
     firewall {
          name to_private
     }
}
from public {
     firewall {
          name to_private
     }
}
from neo {
     firewall {
          name from_neo
     }
}
interface eth0
interface eth1
[edit]
```

Не следует забывать, что для служб, которым требуется трафик, исходящий из системы Altell NEO, требуется надлежащая фильтрация из локальной зоны в эти зоны. Например, для работы передачи DNS должно быть разрешено прохождение трафика из системы Altell NEO в общедоступную зону.

### 14.2.16. Использование наборов правил межсетевого экрана, связанных с интерфейсами, одновременно с межсетевым экраном на основе зон

После создания транзитной или локальной зоны прохождение трафика в эту зону из другой зоны может быть разрешено только с помощью наборов правил межсетевого экрана для фильтрации трафика из этой зоны. Таким образом, интерфейсы, не включенные ни в одну из зон в качестве ее части, не смогут отправлять трафик ни в одну из зон. Однако трафик между интерфейсами, не являющимися частью ни одной из зон, передается беспрепятственно и может фильтроваться с помощью наборов правил межсетевого экрана, связанных с интерфейсами. Рассмотрим приведенный ниже пример.

*Рисунок 55 - Передача трафика в транзитные зоны и из транзитных зон*




В данной топологии определены три зоны - DMZ, общедоступная и локальная. Образец настройки политик зон для может выглядеть примерно следующим образом.

*Пример 14.23 - Политика зон для топологии с тремя зонами (DMZ, общедоступная и локальная)*

| Действие | Команда |
|---|---|
| Вывод настройки политики для зон. | admin@R1# **show zone-policy**<br>zone dmz {<br>default-action drop<br>description "DMZ ZONE"<br>from public {<br>firewall {<br>name public_to_dmz<br>}<br>}<br>interface eth2<br>} |

```
zone public {
     default-action drop
     description "PUBLIC ZONE"
     from dmz {
          firewall {
               name to_public
          }
     }
     interface eth3
}
zone neo {
     default-action drop
     from dmz {
          firewall {
               name dmz_to_neo
          }
     }
     from public {
          firewall {
               name public_to_neo
          }
     }
     local-zone
}
[edit]
```

Интерфейсы eth0 и eth1 не являются частью ни одной из зон. Таким образом, трафик в любую из указанных трех зон с этих интерфейсов будет проигнорирован. Трафик между LAN1 и LAN2 будет передаваться беспрепятственно и без фильтрации. Кроме того, трафик, исходящий из eth0 и eth1 от любой из зон (DMZ, общедоступной и локальной) будет передаваться без фильтрации. Теперь предположим, что нужно отклонить весь трафик от любой из зон, исходящий из eth0 и eth1, и, кроме того, разрешить прохождение только пакетов ICMP между LAN1 и LAN2. Систему следовало бы настроить следующим образом.

*Пример 14.24 - Отклонение трафика из зон и разрешение передачи только ICMP между LAN1 и LAN2*

| Действие | Команда |
|---|---|
| Вывод настройки межсетевого экрана allow_ping_only.<br>ПРИМЕЧАНИЕ: “not_allowed_nets” - это сетевая группа, содержащая подсети зон DMZ и общедоступной. | admin@R1# s**how firewall name allow_ping_only**<br>description "allow nothing from zones. allow icmp packets between LANs"<br>rule 1 {<br>action reject<br>protocol all<br>source {<br>group {<br>network-group not_allowed_nets<br>}<br>}<br>}<br>rule 2 {<br>action accept<br>icmp {<br>type-name any<br>}<br>protocol icmp<br>}<br>[edit] |
| Вывод настройки межсетевого экрана для eth0 и eth1. | admin@R1# **show interfaces ethernet eth0 firewall**<br>out {<br>name allow_ping_only<br>} |

```
[edit]
admin@R1# show interfaces
ethernet eth1 firewall
out {
     name allow_ping_only
}
[edit]
```

Трафик, исходящий из системы Altell NEO и выходящий через интерфейсы eth0 и eth1, в этом случае не фильтруется. Команд для поинтерфейсной фильтрации трафика, исходящего из системы, нет. Если бы в настройке политики зон в этом примере локальная зона (зона neo) использовалась как зона-отправитель под DMZ или общедоступной зоной, тогда трафик, исходящий из системы, выходил бы только в эти зоны и никуда более.

## 14.3. Просмотр сведений о межсетевом экране

В этом разделе рассматриваются следующие вопросы:

- Вывод сведений об экземпляре межсетевого экрана.
- Вывод настройки межсетевого экрана на интерфейсах.
- Вывод настройки межсетевого экрана.

В этом разделе есть следующие примеры:

- Пример 14.25 Вывод экземпляров межсетевого экрана.
- Пример 14.26 Вывод настройки межсетевого экрана на интерфейсе.
- Пример 14.27 Отображение узла конфигурации “firewall”.

### 14.3.1. Вывод сведений об экземпляре межсетевого экрана

Вывести настройку экземпляров межсетевого экрана можно с помощью команды **show firewall** в эксплуатационном режиме, указав имя экземпляра. Если экземпляр не указан, отображаются все определенные экземпляры.

В примере 14.25 выводятся сведения, настроенные для экземпляров FWTEST-1 и FWTEST-3 межсетевого экрана.

*Пример 14.25 - Вывод экземпляров межсетевого экрана*

```
admin@R1:~$ show firewall FWTEST-1
```

```
Active on (eth0, IN)

State Codes: E - Established, I - Invalid, N - New, R - Related

rule action source      destination proto state
-- --- ---      ------ --- ---
1    REJECT 172.16.0.26 0.0.0.0/0   all   any
1025 DROP   0.0.0.0/0   0.0.0.0/0   all   any

admin@R1:~$ show firewall FWTEST-3

Active on (eth1, LOCAL)

State Codes: E - Established, I - Invalid, N - New, R — Related

rule action source      destination proto state
-- --- ---      ------ --- ---
1    ACCEPT 10.10.30.46 0.0.0.0/0   tcp   any
                        dst ports: telnet
1025 DROP   0.0.0.0/0   0.0.0.0/0   all   any
```

### 14.3.2. Вывод настройки межсетевого экрана на интерфейсах

В примере 14.26 показано применение экземпляра FWTEST-1 межсетевого экрана к интерфейсу eth0.

*Пример 14.26 - Вывод настройки межсетевого экрана на интерфейсе*

```
admin@R1# show interfaces ethernet eth0 firewall
in {
     name FWTEST-1
}
[edit]
```

### 14.3.3. Вывод настройки межсетевого экрана

Всегда можно просмотреть сведения в узлах конфигурации с помощью команды **show** в режиме настройки. В этом случае просмотреть настройку межсетевого экрана можно с помощью команды **show firewall** в режиме настройки, как показано в примере 14.27.

*Пример 14.27 - Отображение узла конфигурации "firewall"*

```
admin@R1# show firewall
name FWTEST-1 {
     rule 1 {
          action reject
          source {
               address 172.16.0.26
          }
     }
}
name FWTEST-2 {
     rule 1 {
          action accept
          destination {
               address 10.10.40.101
          }
          source {
               address 10.10.30.46
          }
     }
}
name FWTEST-3 {
     rule 1 {
          action accept
          destination {
               port telnet
          }
          protocol tcp
```

```
          source {
               address 10.10.30.46
          }
     }
}
name FWTEST-4 {
     rule 1 {
          action accept
          destination {
               address 172.16.0.0/24
          }
          source {
               address 10.10.40.0/24
          }
     }
}
name FWTEST-5 {
     rule 1 {
          action accept
          source {
               mac-addr 00:13:ce:29:be:e7
          }
     }
}
[edit]
```

## 14.4. Глобальные команды межсетевого экрана

В этом разделе описаны команды межсетевого экрана системы Altell NEO, относящиеся к обоим межсетевым экранам IPv4 и IPv6.

Следует обратить внимание на то, что поддержка протокола IPv6 в системе Altell NEO в настоящее время является экспериментальной.

В данном разделе приведены следующие команды:

*Таблица 32 - Глобальные команды межсетевого экрана*

| Команды настройки | |
|---|---|
| `firewall` | Включение межсетевого экрана на системе Altell NEO. |
| `firewall conntrack-table-size <размер>` | Установка размера таблицы отслеживания подключений для сетевого фильтра. |
| `firewall conntrack-tcp-loose <состояние>` | Указание необходимости отслеживания ранее установленных подключений для фильтрации трафика с поддержкой состояния. |
| Эксплуатационные команды | |
| `show firewall` | Отображение сведений о настроенных экземплярах межсетевого экрана. |

### 14.4.1. firewall

Включение межсетевого экрана на системе Altell NEO.

**Синтаксис**

```
set firewall
delete firewall
show firewall
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {}
```

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для определения параметров настройки и наборов правил межсетевого экрана при помощи других команд **firewall**. После определения наборов правил межсетевого экрана их необходимо применить в качестве фильтров пакетов к интерфейсам при помощи команд **interface**,

относящихся к межсетевому экрану. Пока набор правил межсетевого экрана не применен к интерфейсу, он не имеет никакого влияния на трафик, предназначенный для системы или проходящий через неё.

Следует обратить внимание на то, что после выполнения последнего определенного пользователем правила в наборе правил вступает в силу правило по умолчанию **reject all**.

Форма **set** этой команды используется для создания настройки межсетевого экрана.

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

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

### 14.4.2. firewall conntrack-table-size <размер>

Установка размера таблицы отслеживания подключений для сетевого фильтра.

**Синтаксис**

```
set firewall conntrack-table-size размер
delete firewall conntrack-table-size
show firewall conntrack-table-size
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    conntrack-table-size целоебеззнака32разр
}
```

**Параметры**

*размер*

Размер таблицы отслеживания подключений сетевого фильтра в килобайтах. Диапазон значений от 1 до 50000000.

**Значение по умолчанию**

Когда межсетевой фильтр не включен, размер таблицы отслеживания подключений составляет 16384 кб; когда межсетевой фильтр включен,

размер по умолчанию таблицы отслеживания подключений составляет 32768 кБ.

**Указания по использованию**

Эта команда используется для указания размера таблицы отслеживания 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 размера таблицы отслеживания подключений.

Форма **delete** этой команды используется для восстановления размера по умолчанию для таблицы отслеживания подключений.

Форма **show** этой команды используется для просмотра настройки таблицы отслеживания подключений.

### 14.4.3. firewall conntrack-tcp-loose <состояние>

Указание необходимости отслеживания ранее установленных подключений для фильтрации трафика с поддержкой состояния.

**Синтаксис**

```
set firewall conntrack-tcp-loose {enable | disable}
delete firewall conntrack-tcp-loose
show firewall conntrack-tcp-loose
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    conntrack-tcp-loose [enable|disable]
}
```

**Параметры**

**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.

## 14.4.4. show firewall

Отображение сведений о настроенных экземплярах межсетевого экрана.

**Синтаксис**

**show firewall [name** *имя* **| detail | statistics]**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**name** *имя*

Отображение сведений об указанном наборе правил: выводятся сведения о том, к каким интерфейсам или зонам он применен в настоящий момент.

**detail**

Отображение подробных сведений обо всех наборах правил межсетевого

экрана.

**statistics**

Отображение статистики для всех наборов правил межсетевого экрана.

**Значение по умолчанию**

При использовании без параметров отображается сводка для всех наборов правил межсетевого экрана.

**Указания по использованию**

Эта команда используется для отображения сведений обо всех настроенных наборах правил (экземплярах) межсетевого экрана. Отображаются сведения для всех наборов правил для протоколов IPv4 и IPv6.

Следует заметить, что отображаются только сведения о наборах правил (экземплярах); сведения об интерфейсах, к которым применены экземпляры межсетевого экрана, не выводятся. Для просмотра сведений об экземплярах межсетевого экрана, примененных к интерфейсу, следует применять команду **show interfaces** для интерфейса.

**Примеры**

В примере 14.28 выводятся зоны, к которым в качестве пакетного фильтра применен набор правил межсетевого экрана “**allow_all**”.

*Пример 14.28 - Вывод зон, на которых используются наборы правил межсетевого экрана*

```
admin@R1:~$ show firewall name allow_all
IPv4 Firewall "allow_all":

 Active on (eth1,IN)

 Active on traffic to -

 zone [private] from zones [dmz, public]

(State Codes: E - Established, I - Invalid, N - New, R — Related)
```

```
rule action source    destination proto state
-- --- ---    ------ --- ---
1    ACCEPT 0.0.0.0/0 0.0.0.0/0   all   any
1025 DROP   0.0.0.0/0 0.0.0.0/0   all   any
```

В примере 14.29 выводится сводка по наборам правил, настроенных на R1. В этом примере определен только один набор правил (TEST).

*Пример 14.29 - Отображение сведений о межсетевом экране*

```
admin@R1:~$ show firewall
IPv4 Firewall "TEST":

 Active on (eth0,IN)

 (State Codes: E - Established, I - Invalid, N - New, R -
Related)
rule action source          destination proto state
-- --- ---          ------ --- ---
10   ACCEPT 192.168.0.0/24  0.0.0.0/0   all   any
20   DROP   192.168.74.0/24 0.0.0.0/0   icmp  any
30   ACCEPT 0.0.0.0/0       0.0.0.0/0   tcp   E,N
1025 DROP   0.0.0.0/0       0.0.0.0/0   all   any
```

В примере 14.30 показаны подробные сведения для всех правил межсетевого экрана на R1. В этом примере определен только один набор правил (TEST).

*Пример 14.30 - Отображение подробных сведений о наборах правил межсетевого экрана*

```
admin@R1:~$ show firewall detail
-------------------------
 IPv4 Firewall "TEST": Active on (eth0,IN)
rule action proto packets bytes
-- --- --- ---- ---
10   accept all   0       0
```

```
  condition - saddr 192.168.0.0/24
20   drop   icmp  0       0
  condition - saddr 192.168.74.0/24
30   accept tcp   0       0
  condition - state NEW,ESTABLISHED
1025 drop   all   0       0
```

В примере 14.31 выводится статистика для всех правил межсетевого экрана на R1.

*Пример 14.31 - Вывод статистики для правил*

```
admin@R1:~$ show firewall statistics
IPv4 Firewall "TEST": Active on (eth0,IN)
rule packets bytes action source          destination
-- ---- --- --- ---          ------
10   0       0     ACCEPT 192.168.0.0/24  0.0.0.0/0
20   0       0     DROP   192.168.74.0/24 0.0.0.0/0
30   0       0     ACCEPT 0.0.0.0/0       0.0.0.0/0
1025 0       0     DROP   0.0.0.0/0       0.0.0.0/0
```

## 14.5. Команды межсетевого экрана IPv4

В этом разделе приведены команды, позволяющие определить фильтры IPv4 для межсетевого экрана.

В этом разделе рассматриваются следующие команды.

*Таблица 33 - Команды настройки*

| Команды настройки | |
|---|---|
| Команды для интерфейса | |
| `interfaces <интерфейс> firewall <направление> name <имя_межсетевого_экрана>` | Применение экземпляра межсетевого экрана IPv4 к определенному интерфейсу. |
| Системные настройки | |

| | |
|---|---|
| `firewall all-ping <состояние>` | Включение или выключение ответа на эхо-запрос IPv4 ICMP (ping). |
| `firewall broadcast-ping <состояние>` | Включение или выключение ответа на широковещательные эхо-запросы IPv4 ICMP и запросы метки времени. |
| `firewall ip-src-route <состояние>` | Обработка пакетов с опциями IP гибкой маршрутизации от источника (Loose Source Route) или жесткой маршрутизации от источника (Strict Source Route). |
| `firewall l7-numpackets <количество_пакетов>` | Установка количества анализируемых на прикладном уровне пакетов. |
| `firewall log-martians <состояние>` | Регистрация пакетов с недопустимыми адресами. |
| `firewall receive-redirects <состояние>` | Обработка сообщений IPv4 ICMP о перенаправлении (тип 5). |
| `firewall send-redirects <состояние>` | Отправка сообщений IPv4 ICMP о перенаправлении (тип 5). |
| `firewall source-validation <состояние>` | Отправка сообщений IPv4 ICMP о перенаправлении (тип 5). |
| `firewall syn-cookies <состояние>` | Определение политики для проверки отправителя на основе обратного пути, как определено в RFC 3704. |
| Группы фильтрации | |
| `firewall group` | Определение группы объектов для ссылки в правилах межсетевого экрана. |
| `firewall group address-group <имя_группы>` | Определение группы IP-адресов для ссылки в правилах межсетевого экрана. |
| `firewall group network-group <имя_группы>` | Определение группы сетей для ссылки в правилах межсетевого экрана. |
| `firewall group port-group <имя_группы>` | Определение группы портов для ссылки в правилах межсетевого экрана. |

| Правила и наборы правил | |
|---|---|
| `firewall name <имя>` | Определение набора правил межсетевого экрана IPv4. |
| `firewall name <имя> default-action <действие>` | Установка действия по умолчанию для набора правил IPv4. |
| `firewall name <имя> description <описание>` | Указание краткого описания для набора правил межсетевого экрана IPv4. |
| `firewall name <имя> rule <номер_правила>` | Определение правила в наборе правил межсетевого экрана IPv4. |
| `firewall name <имя> rule <номер_правила> action <действие>` | Указание действия, которое будет применяться к пакетам, для которых было установлено соответствие правилу. |
| `firewall name <имя> rule <номер_правила> description <описание>` | Указание краткого описания для правила межсетевого экрана IPv4. |
| `firewall name <имя> rule <номер_правила> destination` | Указание адреса получателя и номера сетевого порта для проверки соответствия в правиле межсетевого экрана IPv4. |
| `firewall name <имя> rule <номер_правила> destination group` | Указание группы адресов, сетевых портов или сетей для проверки соответствия адреса получателя сетевого пакета в правиле межсетевого экрана IPv4. |
| `firewall name <имя> rule <номер_правила> destination ldap` | Указание имени пользователя LDAP для проверки соответствия в правиле межсетевого экрана IPv4. |
| `firewall name <имя> rule <номер_правила> disable` | Отключение правила межсетевого экрана. |
| `firewall name <имя> rule <номер_правила> fragment` | Установление соответствия для фрагментированных пакетов. |
| `firewall name <имя> rule <номер_правила> icmp` | Указание кода и типа ICMP для правила межсетевого экрана. |

| | |
|---|---|
| `firewall name <имя> rule <номер_правила> ipsec` | Установка соответствия для пакетов IPSec. |
| `firewall name <имя> rule <номер_правила> l7protocol <протокол>` | Указание протокола для фильтрации пакетов на прикладном уровне. |
| `firewall name <имя> rule <номер_правила> limit` | Указание параметров, ограничивающих скорость трафика для правила межсетевого экрана. |
| `firewall name <имя> rule <номер_правила> log <состояние>` | Включение или отключение регистрации для действий правил межсетевого экрана. |
| `firewall name <имя> rule <номер_правила> p2p <имя_приложения>` | Указание однорангового приложения, к которому применяется правило межсетевого экрана. |
| `firewall name <имя> rule <номер_правила> protocol <протокол>` | Указание протокола, к которому применяется правило межсетевого экрана. |
| `firewall name <имя> rule <номер_правила> recent` | Установка соответствия для сетевых пакетов недавно встречавшихся отправителей. |
| `firewall name <имя> rule <номер_правила> source` | Указание адреса отправителя и сетевого порта, по которым будет осуществляться проверка соответствия в правиле межсетевого экрана. |
| `firewall name <имя> rule <номер_правила> source group` | Указание группы адресов, сетевых портов или сетей для проверки соответствия адреса отправителя в правиле межсетевого экрана IPv4. |
| `firewall name <имя> rule <номер_правила> source ldap` | Указание имени пользователя и группы LDAP, по которым будет осуществляться проверка соответствия в правиле межсетевого экрана. |
| `firewall name <имя> rule <номер_правила> state` | Указание типов пакетов, к которым применяется правило. |

| | |
|---|---|
| `firewall name <имя> rule <номер_правила> tcp flags` | Указание флагов TCP для проверки соответствия в правиле межсетевого экрана. |
| `firewall name <имя> rule <номер_правила> time` | Применение правил межсетевого экрана с учетом даты и времени. |
| Эксплуатационные команды | |
| `clear firewall name <имя> counters` | Очистка статистики для набора правил межсетевого экрана. |
| `show firewall group` | Вывод сведений о группе фильтрации. |
| `show firewall name` | Вывод сведений об указанных наборах правил IPv4, показывающих к каким интерфейсам или зонам они применяются. |

### 14.5.1. clear firewall name <имя> counters

Очистка статистики для набора правил межсетевого экрана.

**Синтаксис**

**clear firewall name** *имя* [**rule** *номер_правила* ] **counters**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*имя*

Имя набора правил межсетевого экрана, для которого требуется очистить статистику.

**rule** *номер_правила*

Очистка статистики для конкретного правила в указанном наборе правил межсетевого экрана.

**Значение по умолчанию**

В том случае если правило явно не указано, статистика очищается для всех правил в наборе.

**Указания по использованию**

Данная команда позволяет очистить статистику для набора правил межсетевого экрана IPv4 или конкретного правила в наборе.

### 14.5.2. firewall all-ping <состояние>

Включение или выключение ответа на эхо-запрос IPv4 ICMP (ping).

**Синтаксис**

```
set firewall all-ping {enable | disable}
delete firewall all-ping
show firewall all-ping
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    all-ping [enable|disable]
}
```

**Параметры**

**enable**

Система будет отправлять ответы на эхо-запросы IPv4 ICMP.

**disable**

Система не будет отправлять ответы на эхо-запросы IPv4 ICMP.

**Значение по умолчанию**

Система отправляет ответы на эхо-запросы IPv4 ICMP.

**Указания по использованию**

Данная команда позволяет разрешить или запретить отвечать на эхо-запросы 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.

### 14.5.3. firewall broadcast-ping <состояние>

Включение или выключение ответа на широковещательные эхо-запросы IPv4 ICMP и запросы метки времени.

**Синтаксис**

```
set firewall broadcast-ping {enable | disable}
delete firewall broadcast-ping
show firewall broadcast-ping
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    broadcast-ping [enable|disable]
}
```

**Параметры**

**enable**

Система отправляет ответы на широковещательные эхо-запросы IPv4 ICMP и запросы метки времени.

**disable**

Система не отправляет ответы на 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 отвечать на широковещательные эхо-запросы IPv4 ICMP и широковещательные запросы 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.

### 14.5.4. firewall group

Определение группы объектов для ссылки в правилах межсетевого экрана.

**Синтаксис**

```
set firewall group
delete firewall group
show firewall group
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    group {}
}
```

**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.

узел конфигурации **firewall group** является множественным: можно определить несколько групп, создав соответствующее количество узлов конфигурации **firewall group**.

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.

### 14.5.5. firewall group address-group <имя_группы>

Определение группы IP-адресов для ссылки в правилах межсетевого экрана.

**Синтаксис**

**set firewall group address-group** *имя_группы* {**address** *адрес* | **description** *описание* }

**delete firewall group address-group** *имя_группы* {**address** *адрес* | **description**}

**show firewall group address-group** *имя_группы* {**address** *адрес* | **description**}

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    group {
        address-group текст {
            address текст
            description текст
        }
    }
}
```

**Параметры**

*имя_группы*

Обязательный. Имя группы адресов.

**address** *адрес*

Обязательный. Добавление указанного IPv4-адреса или диапазона IPv4-адресов в указанную группу. Диапазон IPv4-адресов указывается при помощи дефиса; например, 10.0.0.1-10.0.0.50.

**description** *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 или диапазонов IP-адресов узлов, на которую можно указать ссылку в правиле межсетевого экрана.

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.

## 14.5.6. firewall group network-group <имя_группы>

Определение группы сетей для ссылки в правилах межсетевого экрана.

**Синтаксис**

```
set firewall group network-group имя_группы {network
ipv4-сеть | description описание}

delete firewall group network-group имя_группы {network
ipv4-сеть | description описание}

show firewall group network-group имя_группы {network
ipv4-сеть | description}
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    group {
        network-group текст {
            description текст
            network ipv4-сеть
        }
    }
}
```

**Параметры**

*имя_группы*

Обязательный. Имя группы сетей.

**network** *ipv4-сеть*

Обязательный. Добавление IPv4-сети в указанную группу. Для указания сети используется следующий формат: *ip-адрес/префикс*.

**description** *описание*

Позволяет указать краткое описание для группы сетей.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет определить группу сетей. Группа сетей представляет собой набор адресов сетей, что позволяет после определения группы указать одну ссылку на все ее элементы в правиле межсетевого экрана.

Соответствие группе сетей устанавливается в том случае, если адрес пакета совпадает с любым адресом сети или диапазоном адресов, входящих в группу.

Форма **set** данной команды позволяет определить группу сетей.

Форма **delete** используется для удаления группы сетей или ее элемента.

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

группы сетей.

### 14.5.7. firewall group port-group <имя_группы>

Определение группы портов для ссылки в правилах межсетевого экрана.

**Синтаксис**

**set firewall group port-group** *имя_группы* {**port** *порт* | **description** *описание* }

**delete firewall group port-group** *имя_группы* {**port** *порт* | **description**}

**show firewall group port-group** *имя_группы* {**port** *порт* | **description**}

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    group {
        port-group текст {
            description текст
            port текст
        }
    }
}
```

**Параметры**

*имя_группы*

Обязательный. Имя группы портов.

**port** *порт*

Обязательный. Добавление номера порта в указанную группу портов. Используемый формат: (любое имя, указанное в файле **/etc/services**), номер порта, или диапазон номеров портов, указанный через дефис; например, 1001-1050.

**description** *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 межсетевого экрана.

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.

## 14.5.8. firewall ip-src-route <состояние>

Обработка пакетов с опциями IP гибкой маршрутизации от источника (Loose Source Route) или жесткой маршрутизации от источника (Strict Source Route).

**Синтаксис**

```
set firewall ip-src-route {enable | disable}
delete firewall ip-src-route
show firewall ip-src-route
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    ip-src-route [enable|disable]
}
```

**Параметры**

**enable**

Обрабатывать пакеты с установленной опциями IP маршрутизацией от

источника.

**disable**

Не обрабатывать пакеты с установленной опциями IP маршрутизацией от источника.

**Значение по умолчанию**

По умолчанию установлено значение **disable**.

**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.

## 14.5.9. firewall l7-numpackets <количество_пакетов>

Установка количества анализируемых на прикладном уровне пакетов.

**Синтаксис**

**set firewall l7-numpackets** *количество_пакетов*

**delete firewall l7-numpackets**

**show firewall l7-numpackets**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
```

```
        l7-numpackets 1-320
    }
```

**Параметры**

*количество_пакетов*

Позволяет установить количество анализируемых на прикладном уровне пакетов.

**Значение по умолчанию**

По умолчанию просматриваются первые 10 пакетов или 12 Кб каждого соединения.

**Указания по использованию**

Данная команда позволяет указать количество пакетов, анализируемых на прикладном уровне. По умолчанию просматриваются первые 10 пакетов или 12 Кб каждого соединения. Данное значение является достаточным в большинстве случаев, однако в некоторых случаях, например, в соединениях HTTP, включающих cookies большого размера, может потребоваться изменение значения для данного параметра.

Форма **set** данной команды позволяет указать количество пакетов, анализируемых на прикладном уровне.

Форма **delete** данной команды позволяет удалить настройку и восстановить значение, принятое по умолчанию.

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

## 14.5.10. firewall log-martians <состояние>

Регистрация пакетов с недопустимыми адресами.

**Синтаксис**

**set firewall log-martians** *состояние*

**delete firewall log-martians**

**show firewall log-martians**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
```

```
        log-martians [enable|disable]
    }
```

**Параметры**

*состояние*

Позволяет включить или отключить регистрацию пакетов с недопустимыми адресами. Поддерживаются следующие значения:

**enable**: Включение регистрации пакетов с недопустимыми адресами.

**disable**: Отключение регистрации пакетов 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.

## 14.5.11. firewall name <имя>

Определение набора правил межсетевого экрана.

**Синтаксис**

**set firewall name** *имя*

**delete firewall name** [*имя* ]

**show firewall name** [*имя* ]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    name текст {}
}
```

**Параметры**

*имя*

Множественный узел. Имя набора правил межсетевого экрана.

Можно определить несколько наборов правил межсетевого экрана IPv4, создав соответствующее количество узлов конфигурации **name**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет определить набор правил межсетевого экрана IPv4.

Набор правил межсетевого экрана может включать в себя до 9999 правил. После настраиваемых правил следует неявное правило, правило 10000, которое запрещает весь трафик.

> ***ПРИМЕЧАНИЕ*** *Запрещающее правило "**deny all**" остается в силе до тех пор, пока не будут удалены все ссылки на набор правил; то есть, до тех пор пока для всех интерфейсов не будут удалены все пакетные фильтры, ссылающиеся на указанный набор правил.*

Форма **set** данной команды используется для создания и изменения набора правил межсетевого экрана.

Форма **delete** данной команды используется для удаления набора правил межсетевого экрана.

Форма **show** данной команды используется для отображения настройки набора правил межсетевого экрана.

## 14.5.12. firewall name <имя> default-action <действие>

Установка действия по умолчанию для набора правил IPv4.

**Синтаксис**

```
set firewall name имя default-action действие
delete firewall name имя default-action
show firewall name имя default-action
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    name текст {
        default-action [accept|drop|reject]
    }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

Действие по умолчанию, которое осуществляется в том случае, если для набора правил не было установлено ни одного соответствия. Поддерживаются следующие значения:

**accept**: Принять пакет.

**drop**: Отбросить пакет.

**reject**: Отбросить пакет и отправить сообщение ICMP с уведомлением о том, что адресат недоступен.

**Значение по умолчанию**

В том случае если действие по умолчанию явно не указано, если для пакета не было установлено ни одного соответствия правилам набора, пакет отбрасывается.

**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 набора.

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.

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.

### 14.5.13. firewall name <имя> description <описание>

Указание краткого описания для набора правил межсетевого экрана IPv4.

**Синтаксис**

```
set firewall name имя description описание
delete firewall name имя description
show firewall name имя description
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    name текст {
        description текст
    }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*описание*

Описание набора правил. 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 набора правил межсетевого экрана.

Форма **set** данной команды используется для создания и изменения

описания.

Форма **delete** используется для удаления описания.

Форма **show** используется для отображения настройки описания.

### 14.5.14. firewall name <имя> rule <номер_правила>

Определение правила в наборе правил межсетевого экрана IPv4.

**Синтаксис**

```
set firewall name имя rule номер_правила
delete firewall name имя rule [номер_правила ]
show firewall name имя rule [номер_правила ]
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
     name текст {
          rule 1-9999 {}
     }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*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**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет определить правило в наборе правил межсетевого экрана.

Набор правил межсетевого экрана может включать в себя до 9999 настраиваемых правил. За последним настраиваемым правилом следует системное правило (правило с номером 10000), которое запрещает весь трафик.

Правила межсетевого экрана 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 наборе правил межсетевого экрана.

Форма **delete** данной команды используется для удаления правила из набора правил межсетевого экрана.

Форма **show** данной команды используется для отображения настройки правила межсетевого экрана.

## 14.5.15. firewall name <имя> rule <номер_правила> action <действие>

Указание действия, которое будет применяться к пакетам, для которых было установлено соответствие правилу.

**Синтаксис**

```
set firewall name имя rule номер_правила action действие
delete firewall name имя rule номер_правила action
show firewall name имя rule номер_правила action
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    name текст {
        rule 1-9999 {
            action [accept|drop|inspect|reject]
```

```
                }
            }
        }
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

*действие*

Действие, которое будет выполнено, в том случае если пакет удовлетворяет критериям, указанным в правиле. Поддерживаются следующие значения:

**accept**: Принять и переслать пакет, для которого было установлено соответствие.

**drop**: Отбросить пакет, для которого было установлено соответствие.

**inspect**: Пересылка пакета, для которого было установлено соответствие системе предотвращения вторжений (IPS). Система предотвращения вторжений при этом должна быть включена. Подробная информация о настройке IDS/IPS приведена в разделе 32. Система обнаружения и предотвращения вторжений.

**reject**: Отбросить пакет, для которого было установлено соответствие с помощью опции TCP reset.

**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 межсетевого экрана.

### 14.5.16. firewall name <имя> rule <номер_правила> description <описание>

Указание краткого описания для правила межсетевого экрана IPv4.

**Синтаксис**

**set firewall name** *имя* **rule** *номер_правила* **description** *описание*

**delete firewall name** *имя* **rule** *номер_правила* **description**
**show firewall name** *имя* **rule** *номер_правила* **description**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
     name текст {
          rule 1-9999 {
               description текст
          }
     }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

*описание*

Краткое 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 краткое описание для правила межсетевого экрана.

Форма **set** данной команды используется для создания описания.

Форма **delete** используется для удаления описания.

Форма **show** используется для отображения настройки описания.

## 14.5.17. firewall name <имя> rule <номер_правила> destination

Указание адреса получателя и номера сетевого порта для проверки соответствия в правиле межсетевого экрана IPv4.

**Синтаксис**

**set firewall name** *имя* **rule** *номер_правила* **destination** [**address** *адрес* | **port** *порт*]

**delete firewall name** *имя* **rule** *номер_правила* **destination** [**address** | ***port***]

**show firewall name** *имя* **rule** *номер_правила* **destination** [**address** | **port**]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    name текст {
        rule 1-9999 {
            destination {
                address текст
                port текст
            }
        }
    }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

*адрес*

Адрес получателя, который будет использоваться для проверки соответствия. Поддерживаются следующие значения:

*ip-адрес* : IPv4-адрес.

*ip-адрес/префикс*: Адрес сети, где 0.0.0.0/0 соответствует любой сети.

*ip-адрес–ip-адрес*: Диапазон IP-адресов; например, 192.168.1.1–192.168.1.150.

**!***ip-адрес*: Соответствие будет установлено для всех IP-адресов кроме указанного.

**!***ip-адрес/префикс*: Соответствие буден установлено для всех адресов кроме указанного.

**!***ip-адрес–ip-адрес*: Соответствие будет установлено для всех адресов кроме адресов, входящих в указанный диапазон.

*порт*

Может быть указан только для протоколов TCP или UDP. 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 межсетевого

экрана.

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.

## 14.5.18. firewall name <имя> rule <номер_правила> destination ldap

Указание имени пользователя LDAP для проверки соответствия в правиле межсетевого экрана IPv4.

**Синтаксис**

**set firewall name** *имя* **rule** *номер_правила* **destination ldap user** *имя_пользователя* | **group** *имя_группы*

**delete firewall name** *имя* **rule** *номер_правила* **destination ldap** [**user** | **group**]

**show firewall name** *имя* **rule** *номер_правила* **destination ldap** [**user** | **group**]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    name текст {
        rule 1-9999 {
            destination {
                ldap {
                    user текст
                    group текст
                }
            }
        }
    }
```

}

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

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.

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.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет указать имя пользователя LDAP в правиле межсетевого экрана для проверки на соответствие, для тех случаев когда получателем является клиент PPTP/L2TP, который был аутентифицирован на основе учетной записи пользователя LDAP с указанным именем. См. раздел 18.1.2.3. Аутентификация клиентов PPTP и L2TP на основе протокола LDAP.

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.

## 14.5.19. firewall name <имя> rule <номер_правила> destination group

Указание группы адресов, сетевых портов или сетей для проверки соответствия адреса получателя сетевого пакета в правиле межсетевого экрана IPv4.

**Синтаксис**

**set firewall name** *имя* **rule** *номер_правила* **destination group** [**address-group** *имя_группы_адресов* | **network-group** *имя_группы_сетей* | **port-group** *имя_группы_портов* ]

**delete firewall name** *имя* **rule** *номер_правила* **destination group** [**address-group** *имя_группы_адресов* | **network-group** *имя_группы_сетей* | **port-group** *имя_группы_портов*]

**show firewall name** *имя* **rule** *номер_правила* **destination group** [**address-group** | **network-group**| **port-group**]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    name текст {
        rule 1-9999 {
            destination {
                group {
                    address-group текст
                    network-group текст
                    port-group текст
                }
            }
        }
    }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

**address-group** *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.

**network group** *имя_группы_сетей*

Проверка соответствия IP-адреса сети получателя сетевого пакета на основе адресов, входящих в указанную группу сетей. Соответствие для пакета устанавливается, в том случае если адрес сети получателя совпадает с одним из адресов, входящих в группу. Может быть указана только одна группа сетей. Группа сетей должна быть заранее определена.

**port-group** *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.

**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, сеть и порт совпадает с одним из адресов, сетей или портов, входящих в состав указанной группы. Однако, в том случае если указано более одной группы, для сетевого пакета должно быть установлено соответствие для всех групп. Например, если указаны группа адресов и группа портов, указанный в сетевом пакете получатель должен совпадать как минимум с одним элементом группы адресов и одним элементом группы портов.

Группа адресов может быть указана совместно с группой портов, а также группа сетей может быть указана совместно с группой портов. Группа адресов и группа сетей не могут быть указаны вместе.

Форма **set** данной команды используется для указания группы получателя для проверки соответствия.

Форма **delete** данной команды используется для удаления группы

получателя.

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

## 14.5.20. firewall name <имя> rule <номер_правила> disable

Отключение правила межсетевого экрана.

**Синтаксис**

**set firewall name** *имя* **rule** *номер_правила* **disable**

**delete firewall name** *имя* **rule** *номер_правила* **disable**

**show firewall name** *имя* **rule** *номер_правила*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
     name текст {
          rule 1-9999 {
               disable
          }
     }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

**disable**

Отключение указанного правила межсетевого экрана.

**Значение по умолчанию**

Правило включено (используется).

**Указания по использованию**

Данная команда позволяет отключить правило межсетевого экрана. Это

может быть полезно при проверке того, как межсетевой экран функционирует без указанного правила без его удаления и создания заново.

Форма **set** данной команды используется для отключения правила межсетевого экрана.

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

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

## 14.5.21. firewall name <имя> rule <номер_правила> fragment

Установление соответствия для фрагментированных пакетов.

**Синтаксис**

**set firewall name** *имя* **rule** *номер_правила* **fragment** [**match-frag**|**match-non-frag**]

**delete firewall name** *имя* **rule** *номер_правила* **fragment** [**match-frag**|**match-non-frag**]

**show firewall name** *имя* **rule** *номер_правила* **fragment**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    name текст {
        rule 1-9999 {
            fragment {
                match-frag
                match-non-frag
            }
        }
    }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

**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 проверку соответствия для фрагментированных пакетов.

Форма **set** данной команды позволяет указать проверку соответствия для фрагментированных пакетов.

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

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

## 14.5.22. firewall name <имя> rule <номер_правила> icmp

Указание кода и типа ICMP для правила межсетевого экрана.

**Синтаксис**

```
set firewall name имя rule номер_правила icmp {type тип |
code код | type-name имя_типа}

delete firewall name имя rule номер_правила icmp [type |
code | type-name]

show firewall name имя rule номер_правила icmp [type |
code | type-name]
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    name текст {
        rule 1-9999 {
```

```
                    icmp {
                        type целоебеззнака32разр
                        code целоебеззнака32разр
                        type-name текст
                    }
                }
            }
        }
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

*тип*

Корректный тип и код ICMP. Значение должно лежать в диапазоне от 0 до 255; например, 8 (эхо-запрос), или 0 (эхо-ответ). Список типов и кодов ICMP приведен в «Приложение 1. Типы ICMP ».

*код*

Код типа ICMP, связанный с указанным типом ICMP. Значение должно лежать в диапазоне от 0 до 255. Список типов и кодов ICMP приведен в “Приложение 1. Типы ICMP ”

*имя_типа*

Название типа ICMP. По умолчанию установлено значение **any**. Список типов и кодов ICMP приведен в “Приложение 1. Типы ICMP ”

**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.

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.

### 14.5.23. firewall name <имя> rule <номер_правила> ipsec

Установка соответствия для пакетов IPSec.

#### Синтаксис

**set firewall name** *имя* **rule** *номер_правила* **ipsec** {**match-ipsec**|**match-none**}

**delete firewall name** *имя* **rule** *номер_правила* **ipsec** [**match-ipsec**|**match-none**]

**show firewall name** *имя* **rule** *номер_правила* **ipsec**

#### Режим интерфейса

Режим настройки.

#### Ветвь конфигурации

```
firewall {
    name текст {
        rule 1-9999 {
            ipsec {
                match-ipsec
                match-none
            }
        }
    }
}
```

#### Параметры

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

**match-ipsec**

Установка соответствия для входящих пакетов IPSec.

**match-none**

Установка соответствия для входящих пакетов за исключением пакетов IPSec.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда используется для установки соответствия для входящих пакетов 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** используется для отображения настройки.

## 14.5.24. firewall name <имя> rule <номер_правила> l7protocol <протокол>

Указание протокола для фильтрации пакетов на прикладном уровне.

**Синтаксис**

**set firewall name** *имя* **rule** *номер_правила* **l7protocol** *протокол*

**delete firewall name** *имя* **rule** *номер_правила* **l7protocol**

**show firewall name** *имя* **rule** *номер_правила* **l7protocol**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    name текст {
        rule 1-9999 {
```

```
                    l7protocol текст
                }
            }
        }
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

*протокол*

Имя протокола прикладного уровня, используемого для фильтрации пакетов. Список допустимых значений приведен в приложении 5 на стр. 2113.

**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 следует помнить, что для корректной работы механизма классификатор трафика должен видеть весь имеющий значение для классификации трафик. Для этого под правило межсетевого экрана, 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 (список протоколов см. в приложении 5), 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.

## 14.5.25. firewall name <имя> rule <номер_правила> limit

Указание параметров, ограничивающих скорость трафика для правила межсетевого экрана.

**Синтаксис**

```
set firewall name имя rule номер_правила limit {burst
размер | rate скорость}
```

**delete firewall name** *имя* **rule** *номер_правила* **limit** [**burst** | **rate**]

**show firewall name** *имя* **rule** *номер_правила* **limit** [**burst** | **rate**]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    name текст {
        rule 1-9999 {
            limit {
                burst целоебеззнака32разр
                rate текст
            }
        }
    }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать 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.

*скорость*

Максимальная средняя скорость 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). Скорость указывается в следующем формате "*X*/<*единица времени*>". Например, "**2/second**" ограничит скорость двумя пакетами в секунду для сетевых пакетов, для которых было установлено соответствие.

**Значение по умолчанию**

Ограничения не установлено.

**Указания по использованию**

Данная команда используется для ограничения скорости сетевых пакетов, для которых установлено соответствие данному правилу. Для ограничения скорости входящих сетевых пакетов используется фильтр TBF (Token Bucket Filter), который позволяет административно задать требуемую скорость, а также ее превышение 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 связывании данного алгоритма с двумя потоками - маркеров и данных, 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. Далее, накопленные маркеры могут использоваться для передачи групп пакетов со скоростью, превышающей установленную скорость прибывающих маркеров.

- Данные прибывают быстрее, чем маркеры. Это означает, что в буфере скоро не останется маркеров, что заставит алгоритм приостановить передачу данных. Эта ситуация называется "превышением". Если пакеты продолжают поступать, они начинают уничтожаться.

Параметр "**rate**" позволяет установить скорость маркеров (token rate),

параметр "**burst**" позволяет установить размер буфера. Описание используемых параметров:

**rate** - В том случае если данное значение явно указано, проверка соответствия для сетевых пакетов осуществляется с указанной максимальной средней скоростью. Время может быть указано в следующих единицах: **second** (секунды), **minute** (минуты), **hour** (часы), а также **day** (дни).

Например, "**1/second**" ограничит скорость проверки соответствия одним пакетом в секунду.

**burst** - В том случае если данное значение указано явно, проверка соответствия для сетевых пакетов, определяемых данным значением, осуществляется с превышением указанной скорости. По умолчанию установлено значение равное 1. Таким образом, в том случае если не требуется обрабатывать короткие группы пакетов с превышением скорости, данный параметр можно оставить прежним.

Форма **set** данной команды позволяет ограничить трафик для указанного правила.

Форма **delete** данной команды используется для удаления ограничения трафика для указанного правила.

Форма **show** данной команды используется для отображения установленного ограничения трафика.

## 14.5.26. firewall name <имя> rule <номер_правила> log <состояние>

Включение или отключение регистрации для действий правил межсетевого экрана.

**Синтаксис**

```
set firewall name имя rule номер_правила log состояние
delete firewall name имя rule номер_правила log
show firewall name имя rule номер_правила log
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
```

```
        name текст {
            rule 1-9999 {
                log [enable|disable]
            }
        }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

*состояние*

Включение или отключение регистрации действий межсетевого экрана. Поддерживаются следующие 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 для указанного правила. В том случае если регистрация включена, в журнал заносятся все выполненные действия.

Сообщения регистрации для правил межсетевого экрана записываются в журнал регистрации от имени программы **kernel**. При регистрации пакета в журнале регистрации указывается название экземпляра межсетевого экрана, номер правила, критериям которого соответствует данный пакет, а также префикс действия, которое было применено к сетевому пакету. Используемые префиксы действий:

**A** – (**accept**) пакет принят;

**R** – (**reject**) пакет отброшен, отправителю пакета передано сообщение об ошибке;

**D** – (**drop**) пакет отброшен;

**I** – (**inspect**) пакет перенаправлен системе обнаружения вторжений.

Например, для сетевого пакета прошедшего проверку на соответствие правилу 1 экземпляра межсетевого экрана с именем **test**, к которому было применено действие **drop**, в журнал регистрации будет помещена запись [test-1-D].

Форма **set** данной команды позволяет включить регистрацию указанного правила.

Форма **delete** используется для удаления установленного значения.

Форма **show** данной команды используется для отображения установленного значения.

## 14.5.27. firewall name <имя> rule <номер_правила> p2p <имя_приложения>

Указание однорангового приложения, к которому применяется правило межсетевого экрана.

**Синтаксис**

```
set firewall name имя rule номер_правила p2p
имя_приложения

delete firewall name имя rule номер_правила p2p
имя_приложения

show firewall name имя rule номер_правила p2p
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    name текст {
        rule 1-9999 {
            p2p {
                [all|applejuice|bittorrent|
directconnect|edonkey|gnutella|
                    kazaa]
            }
```

```
                }
            }
        }
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

*имя_приложения*

Обязательный. Соответствие устанавливается для пакетов однорангового приложения. Поддерживаются следующие значения:

**all**: Соответствие устанавливается для пакетов любого из приложений, перечисленных в списке ниже.

**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 одноранговых приложений, к пакетам которых применяется правило. 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.

## 14.5.28. firewall name <имя> rule <номер_правила> protocol <протокол>

Указание протокола, к которому применяется правило межсетевого экрана.

**Синтаксис**

**set firewall name** *имя* **rule** *номер_правила* **protocol** *протокол*

**delete firewall name** *имя* **rule** *номер_правила* **protocol**

**show firewall name** *имя* **rule** *номер_правила* **protocol**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    name текст {
        rule 1-9999 {
            protocol текст
        }
    }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

*протокол*

Обязательный. Могут быть использованы любые наименования протоколов или их номера, определенные в файле **/etc/protocols**. Ключевые слова

**tcp_udp** (для протоколов TCP и UDP) и **all** (для всех протоколов) также поддерживаются.

При указании перед названием протокола восклицательного знака (“!”) соответствие будет установлено для любого протокола за исключением указанного. Например, при указании **!tcp** соответствие будет установлено для всех протоколов за исключением TCP.

**Значение по умолчанию**

По умолчанию определены все (**all**) протоколы.

**Указания по использованию**

Данная команда используется для определения протоколов, к пакетам которых применяется правило. Для пакетов указанного протокола будет установлено соответствие критериям данного правила.

Следует с осторожностью включать в набор правил более одного правила, определяющего исключения (правило, в котором указывается восклицательный знак "!"). Правила межсетевого экрана 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** используется для удаления установленного значения.

Форма **show** данной команды используется для отображения установленного значения для протоколов.

## 14.5.29. firewall name <имя> rule <номер_правила> recent

Установка соответствия для сетевых пакетов недавно встречавшихся отправителей.

**Синтаксис**

```
set firewall name имя rule номер_правила recent [count
счетчик | time секунды ]

delete firewall name имя rule номер_правила recent [count
| time]

show firewall name имя rule номер_правила recent [count |
time]
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    name текст {
        rule 1-9999 {
            recent {
                count целоебеззнака32разр
                time целоебеззнака32разр
            }
        }
    }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

*счетчик*

Обязательный. Количество пакетов с одинаковым IP-адресом отправителя, пришедших в систему в течение указанного периода времени.

*секунды*

Обязательный. Количество времени, указываемое в секундах, в течение которого будет происходить подсчет пакетов от одного отправителя.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет установить соответствие для сетевых пакетов, пришедших от недавно встречавшихся отправителей. Данная команда может использовать для предотвращения атак, использующих перебор (“brute force” attacks), когда внешнее устройство открывает непрерывный поток

подключений (например, к порту SSH) в попытке взломать систему. Несмотря на то, что адрес внешнего узла заранее неизвестен, список недавно встречавшихся отправителей позволит устанавливать соответствие для сетевых пакетов на основе данного адреса.

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.

## 14.5.30. firewall name <имя> rule <номер_правила> source

Указание адреса отправителя и сетевого порта, по которым будет осуществляться проверка соответствия в правиле межсетевого экрана.

**Синтаксис**

**set firewall name** *имя* **rule** *номер_правила* **source** [**address** *адрес* | **mac-address** *mac-адрес*| **port** *порт* ]

**delete firewall name** *имя* **rule** *номер_правила* **source** [**address** | **mac-address** | **port**]

**show firewall name** *имя* **rule** *номер_правила* **source** [**address** | **mac-address** | **port**]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    name текст {
        rule 1-9999 {
            source {
                address текст
                mac-address текст
                port текст
            }
        }
    }
```

```
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

*адрес*

Адрес отправителя для проверки соответствия. Поддерживаются следующие форматы:

*ip-адрес*: Проверка соответствия указанному адресу.

*ip-адрес/префикс*: Адрес сети, где 0.0.0.0/0 соответствует любой сети.

*ip-адрес–ip-адрес*: Соответствие будет установлено для диапазона IP-адресов; например, 192.168.1.1–192.168.1.150.

**!***ip-адрес*: Соответствие будет установлено для всех IP-адресов кроме указанного.

**!***ip-адрес/префикс*: Соответствие буден установлено для всех адресов сетей кроме указанного.

**!***ip-адрес–ip-адрес*: Соответствие будет установлено для всех адресов кроме входящих в указанный диапазон.

*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.

*порт*

Порт источника для проверки соответствия. 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 адрес источника, по которому будет осуществляться проверка соответствия пакета критериям правила межсетевого экрана. Следует с осторожностью включать в набор правил более одного правила, определяющего исключения (правило, в котором указывается восклицательный знак "!").

Правила межсетевого экранирования выполняются последовательно, и набор правил, содержащий более одного "исключающего" правила, может привести к результатам отличным от ожидаемых.

Форма **set** используется для создания адреса отправителя для правила межсетевого экрана.

Форма **delete** данной команды используется для удаления настройки отправителя для правила межсетевого экрана.

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

## 14.5.31. firewall name <имя> rule <номер_правила> source ldap

Указание имени пользователя и группы LDAP, по которым будет осуществляться проверка соответствия в правиле межсетевого экрана.

**Синтаксис**

```
set firewall name имя rule номер_правила source ldap
[user имя_пользователя | group имя_группы]

delete firewall name имя rule номер_правила source ldap
[user | group]

show firewall name имя rule номер_правила source ldap
[user | group]
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
     name текст {
          rule 1-9999 {
               source {
                    ldap {

     user текст

     group текст
                    }
               }
          }
     }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

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.

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.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет указать имя пользователя LDAP в правиле межсетевого экрана для проверки на соответствие, для тех случаев когда отправителем является клиент PPTP/L2TP, который был аутентифицирован на основе учетной записи пользователя LDAP с указанным именем. См. раздел 18.1.2.3. Аутентификация клиентов PPTP и L2TP на основе протокола LDAP.

Форма **set** используется для создания настройки отправителя для правила межсетевого экрана.

Форма **delete** данной команды используется для удаления настройки отправителя для правила межсетевого экрана.

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

## 14.5.32. firewall name <имя> rule <номер_правила> source group

Указание группы адресов, сетевых портов или сетей для проверки соответствия адреса отправителя в правиле межсетевого экрана IPv4.

**Синтаксис**

**set firewall name** *имя* **rule** *номер_правила* **source group** [**address-group** *имя_группы_адресов* | **network-group** *имя_группы_сетей* | **port-group** *имя_группы_портов* ]

**delete firewall name** *имя* **rule** *номер_правила* **source group** [**address-group** *имя_группы_адресов* | **network-group** *имя_группы_сетей* | **port-group** *имя_группы_портов* ]

**show firewall name** *имя* **rule** *номер_правила* **source group** [**address-group** | **network-group** | **port-group**]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    name текст {
        rule 1-9999 {
            source {
                group {
```

```
                                address-group текст
                                network-group текст
                                port-group текст
                            }
                        }
                    }
                }
            }
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

**address-group** *имя_группы_адресов*

Множественный узел. 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.

**network group** *имя_группы_сетей*

Множественный узел. Проверка соответствия IP-адреса сети отправителя сетевого пакета на основе адресов, входящих в указанную группу сетей. Может быть указана только одна группа сетей. Группа сетей должна быть заранее определена.

**port-group** *имя_группы_портов*

Проверка соответствия порта отправителя сетевого пакета на основе портов, входящих в указанную группу портов. Может быть указана только одна группа портов. Группа портов должна быть заранее определена.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет указать адрес источника, по которому будет осуществляться проверка соответствия пакета критериям правила межсетевого экрана. Следует с осторожностью включать в набор правил более одного правила, определяющего исключения (правило, в котором указывается восклицательный знак "!").

Правила межсетевого экрана выполняются по порядку, при этом последовательность правил, определяющих исключения, может привести к результатам отличным от ожидаемых.

Форма **set** данной команды используется для указания группы отправителя для проверки соответствия.

Форма **delete** данной команды используется для удаления группы получателя.

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

## 14.5.33. firewall name <имя> rule <номер_правила> state

Указание типов пакетов, к которым применяется правило.

**Синтаксис**

**set firewall name** *имя* **rule** *номер_правила* **state** {**established** *состояние* | **invalid** *состояние* | **new** *состояние* | **related** *состояние*}

**delete firewall name** *имя* **rule** *номер_правила* **state**

**show firewall name** *имя* **rule** *номер_правила* **state**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    name текст {
        rule 1-9999 {
            state {
                established [enable|disable]
                invalid [enable|disable]
```

```
                    new [enable|disable]
                    related [enable|disable]
                }
            }
        }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

**established** *состояние*

Позволяет указать следует ли применять данное правило к пакетам, относящимся к установленному соединению. Поддерживаются следующие значения:

**enable**: Применить правило к пакетам, относящимся к установленному соединению.

**disable**: Не применять правило к пакетам, относящимся к установленному соединению.

**invalid** *состояние*

Позволяет указать следует ли применять данное правило к недопустимым пакетам. Поддерживаются следующие значения:

**enable**: Применить правило к недопустимым пакетам.

**disable**: Не применять правила к недопустимым пакетам.

**new** *состояние*

Позволяет указать следует ли применять данное правило к пакетам, относящимся к новому соединению. Поддерживаются следующие значения:

**enable**: Применить правило к пакетам, относящимся к новому соединению.

**disable**: Не применять правило к пакетам, относящимся к новому соединению.

**related** *состояние*

Позволяет указать, следует ли применять данное правило к пакетам, относящимся к связанному соединению. Поддерживаются следующие значения:

**enable**: Применить данное правило к пакетам, относящимся к связанному соединению.

**disable**: Не применять данное правило к пакетам, относящимся к связанному соединению.

**Значение по умолчанию**

Указанное правило применяется ко всем пакетам вне зависимости от состояния.

**Указания по использованию**

Данная команда позволяет указать, вид пакетов к которым будет применяться данное правило.

- *Established* - Пакеты, относящиеся к установленному соединению; например, пакет ответа, или исходящий пакет, для соединения установленного извне.

- *Invalid* - недопустимые пакеты, которые не могут быть идентифицированы по каким-либо причинам. В число этих причин может входить исчерпание ресурсов системы или ошибки ICMP, которые не могут быт соотнесены ни с одним известным соединением. Обычно эти пакеты отбрасываются.

- *New* - пакеты, относящиеся к новому соединению. Для протокола TCP, это пакеты с установленным флагом SYN.

- *Related* - пакеты, относящиеся к связанным соединениям.

Форма **set** данной команды позволяет указать тип пакетов, к которому будет применяться правило межсетевого экрана.

Форма **delete** данной команды позволяет восстановить поведение, принятое по умолчанию.

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

## 14.5.34. firewall name <имя> rule <номер_правила> tcp flags

Указание флагов TCP для проверки соответствия в правиле межсетевого экрана.

**Синтаксис**

**set firewall name** *имя* **rule** *номер_правила* **tcp flags** *флаги*

**delete firewall name** *имя* **rule** *номер_правила* **tcp flags**

**show firewall name** *имя* **rule** *номер_правила* **tcp flags**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    name текст {
        rule 1-9999 {
            tcp {
                flags текст
            }
        }
    }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

*флаги*

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 на основе флагов 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.

## 14.5.35. firewall name <имя> rule <номер_правила> time

Применение правил межсетевого экрана с учетом даты и времени.

**Синтаксис**

**set firewall name** *имя* **rule** *номер_правила* **time** {**monthdays** *дни_месяца* | **startdate** *дата* | **starttime** *время* | **stopdate** *дата* | **stoptime** *время* | **utc** | **weekdays** *дни_недели*}

**delete firewall name** *имя* **rule** *номер_правила* **time**

**show firewall name** *имя* **rule** *номер_правила* **time**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    name текст {
        rule 1-9999 {
            time {
                monthdays 1..31, ...
                startdate дата
                starttime время
                stopdate дата
```

```
                    stoptime время
                    utc
                    weekdays Mon...Sun, ...
                }
            }
        }
    }
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

**monthdays** *дни_месяца*

Дни месяца, в которые применяется указанное правило. Поддерживаются следующие значения: дни месяца (с 1 по 31), указанные через запятую (например, 2,12,21). Может быть указан восклицательный знак (“!”) для указания отрицания списка значений (например, !2,12,21). В данном случае правило межсетевого экрана будет применяться во все дни, кроме указанных.

**startdate** *дата*

Начало периода времени, в течение которого правило будет применяться. Дата (а также в случае необходимости время) указывается в следующем формате:

*гггг-мм-дд* (например, 2009-03-12)

*гггг-мм-дд***T***чч:мм:сс* (например, 2009-03-12T17:30:00)

По умолчанию установлено значение 1970-01-01. Время указывается в 24-часовом формате (значение должно лежать в диапазоне от 00:00:00 до 23:59:59). В том случае если время явно не указано, по умолчанию устанавливается начало указанного дня (то есть, 00:00:00). Для указания окончания периода действия правила используется параметр **stopdate** .

**starttime** *время*

Время начала периода, в течение которого правило будет применяться. Время указывается в следующем формате:

*чч:мм:сс* (например, 17:30:00).

Время указывается в 24-часовом формате (значение должно лежать в диапазоне от 00:00:00 до 23:59:59). Для указания времени окончания периода действия правила используется параметр **stoptime**.

**stopdate** *дата*

Указание даты и времени окончания периода действия правила. Дата (а также в случае необходимости время) указывается в следующем формате:

*гггг-мм-дд* (например, 2009-03-12)

*гггг-мм-дд***T***чч:мм:сс* (например, 2009-03-12T17:30:00)

По умолчанию установлено значение 2038-01-19. Время указывается в 24-часовом формате (значение должно лежать в диапазоне от 00:00:00 до 23:59:59). В том случае если время явно не указано, по умолчанию устанавливается начало указанного дня (то есть, 00:00:00). Параметр **startdate** используется для указания начала периода действия правила.

**stoptime** *время*

Время окончания периода, в течение которого правило будет применяться. Время указывается в следующем формате:

*чч:мм:сс* (например, 17:30:00).

Время указывается в 24-часовом формате (значение должно лежать в диапазоне от 00:00:00 до 23:59:59). Параметр **starttime** используется для указания окончания периода действия правила.

**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.

**weekdays** *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 межсетевого экрана будет применяться во все дни недели, кроме указанных.

**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.

Все параметры являются необязательными и в случае указания нескольких параметров объединяются с использованием логического И.

Форма **set** данной команды используется для указания периода действия правила межсетевого экрана.

Форма **delete** данной команды используется для восстановления поведения по умолчанию.

Форма **show** данной команды используется для отображения настройки периода действия правила межсетевого экрана.

## 14.5.36. firewall receive-redirects <состояние>

Обработка сообщений IPv4 ICMP о перенаправлении (тип 5).

**Синтаксис**

```
set firewall receive-redirects {enable | disable}
delete firewall receive-redirects
show firewall receive-redirects
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    receive-redirects [enable|disable]
}
```

**Параметры**

*состояние*

Разрешение или запрещение приема сообщений IPv4 ICMP о перенаправлении (тип 5). Поддерживаются следующие значения:

**enable**: Разрешение приема сообщений IPv4 ICMP о перенаправлении (тип 5).

**disable**: Запрещение приема сообщений IPv4 ICMP о перенаправлении.

**Значение по умолчанию**

По умолчанию установлено значение **disable**.

**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.

## 14.5.37. firewall send-redirects <состояние>

Отправка сообщений IPv4 ICMP о перенаправлении (тип 5).

**Синтаксис**

```
set firewall send-redirects [enable | disable]
delete firewall send-redirects
show firewall send-redirects
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    send-redirects [enable|disable]
}
```

**Параметры**

*состояние*

Разрешение или запрещение отправки сообщений IPv4 ICMP о перенаправлении. Поддерживаются следующие значения:

**enable**: Разрешение отправки сообщений IPv4 ICMP о перенаправлении.

**disable**: Запрет отправки сообщений IPv4 ICMP о перенаправлении.

**Значение по умолчанию**

По умолчанию установлено значение **enable**.

**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.

## 14.5.38. firewall source-validation <состояние>

Определение политики для проверки отправителя на основе обратного пути, как определено в RFC 3704.

**Синтаксис**

```
set firewall source-validation [disable | loose | strict]
delete firewall source-validation
show firewall source-validation
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    source-validation [disable|loose|strict]
}
```

**Параметры**

*состояние*

Определение политики для проверки отправителя на основе обратного пути, как определено в RFC 3704. Поддерживаются следующие значения:

**disable**: Проверка отправителя на основе обратного пути не используется.

**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 установлено значение **disable**.

**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.

## 14.5.39. firewall 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 firewall syn-cookies [enable | disable]
delete firewall syn-cookies
show firewall syn-cookies
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
```

```
        syn-cookies [enable|disable]
    }
```

**Параметры**

*состояние*

Включение или отключение механизма предотвращения атак, на основе формирования определенного номера последовательности. Поддерживаются следующие 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 установлено значение **enable**.

**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 хэш-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 хэш-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.

## 14.5.40. interfaces <интерфейс> firewall <направление> name <имя_межсетевого_экрана>

Применение экземпляра межсетевого экрана к определенному интерфейсу.

**Синтаксис**

```
set interfaces интерфейс firewall [in name
имя_межсетевого_экрана | local name
имя_межсетевого_экрана | out name имя_межсетевого_экрана]

delete interfaces интерфейс firewall [in name | local
name | out name]

show interfaces интерфейс firewall [in name | local name
| out name]
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces текст {
    firewall {
```

```
                in {
                     name текст
                }
                local {
                     name текст
                }
                out {
                     name текст
                }
           }
      }
```

**Параметры**

*интерфейс*

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице ниже в разделе Указания по использованию.

**in name** *имя_межсетевого_экрана*

Применение указанного экземпляра межсетевого экрана IPv4 к транзитному трафику, входящему на указанном интерфейсе.

**local name** *имя_межсетевого_экрана*

Применение указанного экземпляра межсетевого экрана IPv4 к трафику, принятому на указанном интерфейсе и предназначенному для локальной системы.

**out name** *имя_межсетевого_экрана*

Применение указанного экземпляра межсетевого экрана IPv4 к транзитному трафику, покидающему систему через указанный интерфейс.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет применить экземпляр межсетевого экрана, или набор правил, к интерфейсу.

Фильтрация транзитного трафика или трафика, предназначенного для локальной системы, не осуществляется до тех пор пока набор правил межсетевого экрана не будет применен к интерфейсу (реальному или виртуальному) с использованием данной команды.

Для включения межсетевого экранирования, следует определить набор правил межсетевого экрана, в качестве именованного экземпляра межсетевого экрана, с помощью команды **firewall** (см. стр. 897). Затем следует применить экземпляр межсетевого экрана к интерфейсам и/или виртуальным интерфейсам, с использованием данной команды. После чего данный экземпляр межсетевого экрана будет функционировать в качестве пакетного фильтра.

Экземпляр межсетевого экрана будет фильтровать сетевые пакеты одним из следующих способов, в зависимости от того, что было указано при его применении:

- **in**. Если применить набор правил с использованием ключевого слова **in**, межсетевой экран будет фильтровать транзитный сетевой трафик, принимаемый на интерфейсе.
- **out**. Если применить набор правил с использованием ключевого слова **out**, межсетевой экран будет фильтровать транзитный трафик, покидающий интерфейс.
- **local**. Если применить набор правил с использованием ключевого слова **local**, межсетевой фильтр будет фильтровать пакеты, предназначенные для системы Altell NEO, входящие на указанном интерфейсе.

На каждом интерфейсе можно применить до трех экземпляров межсетевого экрана: один экземпляр межсетевого экрана, фильтрующий транзитный трафик, принимаемый на интерфейсе (**in**), один экземпляр межсетевого экрана, фильтрующий транзитный трафик, покидающий интерфейс (**out**), и один экземпляр межсетевого экрана, фильтрующий трафик, предназначенный для локальной системы (**local**).

Следует удостовериться, что применяемый экземпляр межсетевого экрана заранее определен, в противном случае могут быть получены результаты, отличные от ожидаемых. При применении к интерфейсу экземпляра

межсетевого экрана, которого не существует, будет применено неявное разрешающее правило **allow all**.

В приведенной ниже таблице показан синтаксис и параметры поддерживаемых типов интерфейсов.

*Таблица 34 - Типы интерфейсов*

| Тип интерфейса | Синтаксис | Параметры |
|---|---|---|
| Агрегирование каналов | `bonding` *`bondx`* | *bondx* Идентификатор интерфейса агрегированных каналов. Поддерживаются значения в диапазоне от **bond0** до **bond99**. |
| Виртуальный интерфейс агрегированных каналов | `bonding` *`bondx`* `vif` *`идентификатор_vlan`* | *bondx* Идентификатор интерфейса агрегированных каналов. Поддерживаются значения в диапазоне от **bond0** до **bond99**.<br>*идентификатор_vlan* Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 0 до 4094. |
| Сетевой мост | `bridge` *`brx`* | *brx* Имя мостовой группы. Поддерживаются значения в диапазоне от **br0** до **br999**. |
| Ethernet | `ethernet` *`ethx`* | *ethx* Имя интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**, в зависимости от доступных в системе физических интерфейсов. |
| Ethernet PPPoE | `ethernet` *`ethx`* `pppoe` *`номер`* | *ethx* Имя интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**, в зависимости от доступных в системе физических интерфейсов.<br>*номер* Имя определенного блока PPPoE. Значение должно лежать в диапазоне от 0 до 15. |
| Виртуальный интерфейс Ethernet | `ethernet` *`ethx`* `vif` *`идентификатор_vlan`* | *ethx* Имя интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**, в зависимости от доступных в системе физических интерфейсов.<br>*идентификатор_vlan* Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 0 до 4094. |

| Тип интерфейса | Синтаксис | Параметры |
|---|---|---|
| Ethernet Vif PPPoE | `ethernet` *`ethx`* `vif` *`идентификатор_vlan`* `pppoe` *`номер`* | *ethx* Имя интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**, в зависимости от доступных в системе физических интерфейсов.<br>*идентификатор_vlan* Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 0 до 4094.<br>*номер* Имя определенного блока PPPoE. Значение должно лежать в диапазоне от 0 до 15. |
| Интерфейс заглушки | `loopback` *`lo`* | *lo* Имя интерфейса заглушки. |
| Многоканальная связь | `multilink` **`mlx`** `vif 1` | *mlx* Идентификатор многоканальной связки. Можно создать до двух многоканальных связок. Значение должно лежать в диапазоне от **ml0** (“эм эль ноль”) до **ml23** (“эм эль двадцать три”).<br>**1** Идентификатор виртуального интерфейса. На текущий момент, можно создать только один виртуальный интерфейс для многоканального интерфейса, с идентификатором 1. Виртуальный интерфейс должен быть заранее определен. |
| OpenVPN | `openvpn` *`vtunx`* | *vtunx* Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое число. |
| Псевдо-Ethernet | `pseudo-ethernet` *`pethx`* | *pethx* Имя интерфейса псевдо-Ethernet. Значение должно лежать в диапазоне от **peth0** до **peth999**. |
| Последовательный PPP | `serial` *`wanx`* `ppp vif 1` | *wanx* Последовательный интерфейс: значение должно лежать в диапазоне от **wan0** до **wan23**. Интерфейс должен быть заранее определен.<br>**1** Идентификатор виртуального интерфейса. На текущий момент, можно создать только один |

| Тип интерфейса | Синтаксис | Параметры |
|---|---|---|
| | | виртуальный интерфейс для интерфейса "точка-точка", с идентификатором **1**. Виртуальный интерфейс должен быть заранее определен. |
| Туннель | `tunnel` *`tunx`* | *tunx* Идентификатор туннельного интерфейса. Значение должно лежать в диапазоне от **tun0** до **tun23**. |

Форма **set** данной команды позволяет применить экземпляр межсетевого экрана к интерфейсу.

Форма **delete** данной команды позволяет удалить экземпляр межсетевого экрана для интерфейса.

Форма **show** данной команды используется для отображения настройки межсетевого экрана на интерфейсе.

## 14.5.41. show firewall group

Вывод сведений о группе фильтрации.

**Синтаксис**

**show firewall group** [*имя_группы*]

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*имя_группы*

Название группы межсетевого экрана.

**Значение по умолчанию**

Отображаются все группы.

**Указания по использованию**

Данная команда используется для вывода сведений о группе фильтрации. Поддерживаются группы адресов, группы сетей и группы портов.

**Примеры**

В примере 14.32 приведен вывод групп для R1.

*Пример 14.32 - "show firewall group": Вывод сведений об определенных группах межсетевого экрана*

```
admin@R1:~$ show firewall group
 Name        : SERVERS
 Type        : address
 Description: My set of blocked servers
 References : FW1-25-destination
 Members     :
               1.1.1.1
               1.1.1.2
               1.1.1.3
               1.1.1.5
               1.1.1.7
               3.3.3.3
 Name        : BAD-NETS
 Type        : network
 Description: my bad nets
 References : none
 Members     : 2.2.0.0/16 8.8.8.0/24 9.0.0.0/24
```

## 14.5.42. show firewall name

Вывод сведений об указанных наборах правил IPv4, показывающих к каким интерфейсам или зонам они применяются.

**Синтаксис**

**show firewall name** [**detail** | **statistics** | [*имя* [**detail** | **statistics** | **rule** *номер_правила* | **detail rule** *номер_правила* ]]]

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**detail**

Необязательный. Вывод подробных сведений обо всех экземплярах

межсетевого экрана, настроенных в ветви “**name**” дерева настройки.

**statistics**

Необязательный. Вывод статистических сведений обо всех экземплярах межсетевого экрана, настроенных в ветви "**name**" дерева настройки.

*имя*

Необязательный. Вывод сведений обо всех правилах межсетевого экрана, настроенных в указанном экземпляре.

*имя* **detail**

Необязательный. Вывод подробных сведений обо всех правилах межсетевого экрана, настроенных в указанном экземпляре межсетевого экрана.

*имя* **statistics**

Необязательный. Вывод статистических сведений обо всех правилах межсетевого экрана, настроенных в указанном экземпляре межсетевого экрана.

*имя* **rule** *номер_правила*

Необязательный. Вывод сведений об указанном правиле межсетевого экрана, настроенном в указанном экземпляре межсетевого экрана.

*имя* **detail rule** *номер_правила*

Необязательный. Вывод подробных сведений об указанном правиле межсетевого экрана, настроенном в указанном экземпляре межсетевого экрана.

**Значение по умолчанию**

По умолчанию выводятся сведения обо всех экземплярах межсетевого экрана, настроенных в ветви “**name**” дерева настройки.

**Указания по использованию**

Данная команда позволяет вывести сведения об экземплярах межсетевого экрана, настроенных в ветви "**name**" дерева настройки.

**Примеры**

В примере 14.33 приведен вывод общих сведений обо всех правилах межсетевого экрана, настроенных в ветви "**name**" дерева настройки .

*Пример 14.33 - "show firewall name": Вывод сведений о межсетевом экране*

```
admin@R1:~$ show firewall name

IPv4 Firewall "TEST": Active on (eth0,IN)

(State Codes: E - Established, I - Invalid, N - New, R -
Related)


rule  action    source           destination     proto
state

10    ACCEPT    192.168.0.0/24   0.0.0.0/0       all
any

20    DROP      192.168.74.0/24  0.0.0.0/0       icmp
any

30    ACCEPT    0.0.0.0/0        0.0.0.0/0       tcp
E,N

10000 DROP      0.0.0.0/0        0.0.0.0/0       all
any
```

В примере 14.34 приведен вывод детализированных сведений о правилах межсетевого экрана.

*Пример 14.34 - "show firewall name detail": Вывод детализированных сведений*

```
admin@R1:~$ show firewall name detail

IPv4 Firewall "TEST": Active on (eth0,IN)

rule  action      proto    packets     bytes

10    accept      all      0           0

      condition - saddr 192.168.0.0/24

20    drop        icmp     0           0

      condition - saddr 192.168.74.0/24

30    accept      tcp      44          2800

      condition - state NEW,ESTABLISHED

10000 drop        all      270         36738
```

В примере 14.35 приведен вывод статистических сведений.

*Пример 14.35 - "show firewall name statistics": Вывод статистики для правил*

```
admin@R1:~$ show firewall name statistics
```

```
IPv4 Firewall "TEST": Active on (eth0,IN)
rule  packets bytes action  source
destination
10    0       0     ACCEPT  192.168.0.0/24     0.0.0.0/0
20    0       0     DROP    192.168.74.0/24    0.0.0.0/0
30    71      4608  ACCEPT  0.0.0.0/0          0.0.0.0/0
10000 547     74020 DROP    0.0.0.0/0          0.0.0.0/0
```

## 14.6. Команды межсетевого экрана Ipv6

В этом разделе описаны команды для определения пакетных фильтров IPv6 в системе Altell NEO.

В этом разделе рассматриваются следующие команды:

*Таблица 35 - Команды межсетевого экрана IPv6*

| | |
|---|---|
| Команды настройки | |
| Команды для интерфейса | |
| `interfaces <интерфейс> firewall <направление> ipv6-name <имя_межсетевого экрана>` | Применение экземпляра межсетевого экрана IPv6 к определенному интерфейсу. |
| Системные настройки | |
| `firewall ipv6-receive-redirects <состояние>` | Обработка сообщений IPv6 ICMP о перенаправлении. |
| `firewall ipv6-src-route <состояние>` | Обработка пакетов IPv6 с расширенным заголовком маршрутизации. |
| Правила и наборы правил | |
| `firewall ipv6-name <имя>` | Определение набора правил IPv6 межсетевого экрана. |
| `firewall ipv6-name <имя> default-action <действие>` | Установка действия по умолчанию для набора правил IPv6. |
| `firewall ipv6-name <имя>` | Указание краткого описания для набора правил |

| | |
|---|---|
| | межсетевого экрана IPv6. |
| `firewall ipv6-name <имя> rule <номер_правила>` | Определение правила в наборе правил межсетевого экрана IPv6. |
| `firewall ipv6-name <имя> rule <номер_правила> action <действие>` | Указание действия, которое будет применяться к пакетам, для которых было установлено соответствие правилу. |
| `firewall ipv6-name <имя> rule <номер_правила> description <описание>` | Указание краткого описания для правила межсетевого экрана IPv6. |
| `firewall ipv6-name <имя> rule <номер_правила> destination` | Указание адреса получателя и номера сетевого порта для проверки соответствия в правиле межсетевого экрана IPv6. |
| `firewall ipv6-name <имя> rule <номер_правила> disable` | Отключение указанного правила межсетевого экрана IPv6. |
| `firewall ipv6-name <имя> rule <номер_правила> icmpv6 type` | Указание кода и типа ICMPv6 для правила межсетевого экрана IPv6. |
| `firewall ipv6-name <имя> rule <номер_правила> ipsec` | Установка соответствия для пакетов IPSec. |
| `firewall ipv6-name <имя> rule <номер_правила> limit` | Указание параметров, ограничивающих скорость трафика для правила межсетевого экрана IPv6. |
| `firewall ipv6-name <имя> rule <номер_правила> log <состояние>` | Включение или отключение регистрации для действий правил межсетевого экрана IPv6. |
| `firewall ipv6-name <имя> rule <номер_правила> p2p <имя_приложения>` | Указание однорангового приложения, к пакетам которого применяется правило межсетевого экрана IPv6. |
| `firewall ipv6-name <имя> rule <номер_правила> protocol <протокол>` | Указание протокола, к пакетам которого применяется правило межсетевого экрана IPv6. |
| `firewall ipv6-name <имя> rule` | Установка соответствия для сетевых пакетов |

| | |
|---|---|
| | недавно встречавшихся отправителей. |
| `firewall ipv6-name <имя> rule <номер_правила> source` | Указание адреса отправителя и номера сетевого порта для проверки соответствия в правиле межсетевого экрана IPv6. |
| `firewall ipv6-name <имя> rule <номер_правила> state` | Указание типов пакетов, к которым применяется правило. |
| `firewall ipv6-name <имя> rule <номер_правила> tcp flags` | Указание флагов TCP для проверки соответствия в правиле межсетевого экрана IPv6. |
| `firewall ipv6-name <имя> rule <номер_правила> time` | Применение правил межсетевого экрана с учетом даты и времени. |
| Эксплуатационные команды | |
| `clear firewall ipv6-name <имя> counters` | Очистка статистики для набора правил межсетевого экрана IPv6. |
| `show firewall ipv6-name` | Вывод сведений об указанных наборах правил IPv6, показывающих к каким интерфейсам или зонам они применяются. |

### 14.6.1. clear firewall ipv6-name <имя> counters

Очистка статистики для набора правил межсетевого экрана IPv6.

**Синтаксис**

**clear firewall ipv6-name** *имя* [**rule** *номер_правила*] **counters**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*имя*

Имя набора правил межсетевого экрана IPv6, для которого требуется очистить статистику.

**rule** *номер_правила*

Очистка статистики для указанного правила, входящего в указанный набор правил IPv6 межсетевого экрана.

**Значение по умолчанию**

В том случае если правило явно не указано, статистика очищается для всех правил в наборе.

**Указания по использованию**

Данная команда позволяет очистить статистику для набора правил межсетевого экрана IPv6 или конкретного правила в наборе.

## 14.6.2. firewall ipv6-name <имя>

Определение набора правил IPv6 межсетевого экрана.

**Синтаксис**

```
set firewall ipv6-name имя
delete firewall ipv6-name [имя ]
show firewall ipv6-name [имя ]
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    ipv6-name текст {}
}
```

**Параметры**

*имя*

Множественный узел. Имя набора правил межсетевого экрана.

Можно определить несколько наборов правил межсетевого экрана IPv6, создав соответствующее количество узлов конфигурации **name**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет определить набор правил межсетевого экрана IPv6.

Набор правил межсетевого экрана может включать в себя до 9999 правил. После настраиваемых правил следует неявное правило, правило 10000, которое запрещает весь трафик.

***ПРИМЕЧАНИЕ*** *Запрещающее правило "**deny all**" остается в силе до тех пор, пока не будут удалены все ссылки на набор правил; то есть, до тех пор пока для всех интерфейсов не будут удалены все пакетные фильтры, ссылающиеся на указанный набор правил.*

Форма **set** данной команды используется для создания и изменения набора правил межсетевого экрана IPv6.

Форма **delete** данной команды используется для удаления набора правил межсетевого экрана IPv6.

Форма **show** данной команды используется для отображения настройки набора правил межсетевого экрана.

### 14.6.3. firewall ipv6-name <имя> default-action <действие>

Установка действия по умолчанию для набора правил IPv6.

**Синтаксис**

```
set firewall ipv6-name имя default-action действие
delete firewall ipv6-name имя default-action
show firewall ipv6-name имя default-action
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    ipv6-name текст {
        default-action [accept|drop|reject]
    }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*действие*

Действие по умолчанию, которое осуществляется в том случае, если для

набора правил не было установлено ни одного соответствия. Поддерживаются следующие значения:

**accept**: Принять пакет.

**drop**: Отбросить пакет.

**reject**: Отбросить пакет и отправить сообщение ICMP с уведомлением о том, что адресат недоступен.

**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.

**Указания по использованию**

Данная команда позволяет установить действие по умолчанию для сетевых пакетов, для которых не было установлено соответствия ни одному из правил в наборе правил 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.

## 14.6.4. firewall ipv6-name <имя> description <описание>

Указание краткого описания для набора правил межсетевого экрана IPv6.

**Синтаксис**

```
set firewall ipv6-name имя description описание
delete firewall ipv6-name имя description
show firewall ipv6-name имя description
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    ipv6-name текст {
        description текст
    }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*описание*

Описание набора правил. 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 набора правил межсетевого экрана IPv6.

Форма **set** данной команды используется для создания и изменения описания.

Форма **delete** используется для удаления описания.

Форма **show** используется для отображения настройки описания.

## 14.6.5. firewall ipv6-name <имя> rule <номер_правила>

Определение правила в наборе правил межсетевого экрана IPv6.

**Синтаксис**

**set firewall ipv6-name** *имя* **rule** *номер_правила*

**delete firewall ipv6-name** *имя* **rule** [*номер_правила* ]

**show firewall ipv6-name** *имя* **rule** [*номер_правила*]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
     ipv6-name текст {
          rule 1-9999 {}
     }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*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**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет определить правило в наборе правил межсетевого экрана IPv6.

Набор правил межсетевого экрана может включать в себя до 9999 настраиваемых правил. За последним настраиваемым правилом следует системное правило (правило с номером 10000), которое запрещает весь трафик.

Правила межсетевого экрана 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 наборе правил межсетевого экрана IPv6.

Форма **delete** данной команды используется для удаления правила из набора правил межсетевого экрана IPv6.

Форма **show** данной команды используется для отображения настройки правила межсетевого экрана.

### 14.6.6. firewall ipv6-name <имя> rule <номер_правила> action <действие>

Указание действия, которое будет применяться к пакетам, для которых было установлено соответствие правилу.

**Синтаксис**

**set firewall ipv6-name** *имя* **rule** *номер_правила* **action** *действие*

**delete firewall ipv6-name** *имя* **rule** *номер_правила* **action**

**show firewall ipv6-name** *имя* **rule** *номер_правила* **action**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
     ipv6-name текст {
          rule 1-9999 {
               action [accept|drop|inspect|reject]
          }
     }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

*действие*

Действие, которое будет выполнено, в том случае если пакет удовлетворяет критериям, указанным в правиле. Поддерживаются следующие значения:

**accept**: Принять и переслать пакет, для которого было установлено соответствие.

**drop**: Отбросить пакет, для которого было установлено соответствие.

**inspect**: Пересылка пакета, для которого было установлено соответствие системе предотвращения вторжений (IPS). Система предотвращения вторжений при этом должна быть включена. Подробная информация о настройке IDS/IPS приведена в разделе 32. Система обнаружения и предотвращения вторжений.

**reject**: Отбросить пакет, для которого было установлено соответствие с помощью опции TCP reset.

**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 межсетевого экрана.

## 14.6.7. firewall ipv6-name <имя> rule <номер_правила> description <описание>

Указание краткого описания для правила межсетевого экрана IPv6.

**Синтаксис**

**set firewall ipv6-name** *имя* ***rule*** *номер_правила* **description** *описание*

**delete firewall ipv6-name** *имя* **rule** *номер_правила*

**description**

**show firewall ipv6-name** *имя* **rule** *номер_правила* **description**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    ipv6-name текст {
        rule 1-9999 {
            description текст
        }
    }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

*описание*

Краткое 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 краткое описание для правила межсетевого экрана IPv6.

Форма **set** данной команды используется для создания описания.

Форма **delete** используется для удаления описания.

Форма **show** используется для отображения настройки описания.

### 14.6.8. firewall ipv6-name <имя> rule <номер_правила> destination

Указание адреса получателя и номера сетевого порта для проверки соответствия в правиле межсетевого экрана IPv6.

**Синтаксис**

```
set firewall ipv6-name имя rule номер_правила destination
[address адрес | port порт ]

delete firewall ipv6-name имя rule номер_правила
destination [address | port]

show firewall ipv6-name имя rule номер_правила
destination [address | port]
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    ipv6-name текст {
        rule 1-9999 {
            destination {
                address текст
                port текст
            }
        }
    }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

*адрес*

Адрес назначения для проверки соответствия. Допустимые форматы:

*ipv6-адрес*: IPv6-адрес; например, fe80::20c:29fe:fe47:f89.

*ipv6-адрес*/*префикс*: Адрес сети, где ::/0 соответствует любой сети; например, fe80::20c:29fe:fe47:f88/64

*ipv6-адрес–ipv6-адрес*: Диапазон IPv6-адресов; например, fe80::20c:29fe:fe47:f00–fe80::20c:29fe:fe47:f89.

**!***ipv6-адрес*: Соответствие будет установлено для всех IPv6-адресов кроме указанного.

**!***ipv6-адрес*/*префикс*: Соответствие буден установлено для всех адресов сетей кроме указанного.

**!***ipv6-адрес–ipv6-адрес*: Соответствие будет установлено для всех IPv6-адресов кроме входящих в указанный диапазон.

*порт*

Может быть указан только для протоколов TCP или UDP. 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 межсетевого экрана 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 получателя.

Форма **delete** данной команды позволяет удалить настройку получателя.

Форма **show** данной команды позволяет отобразить настройку получателя.

### 14.6.9. firewall ipv6-name <имя> rule <номер_правила> disable

Отключение указанного правила межсетевого экрана IPv6.

#### Синтаксис

**set firewall ipv6-name** *имя* **rule** *номер_правила* **disable**

**delete firewall ipv6-name** *имя* **rule** *номер_правила* **disable**

**show firewall ipv6-name** *имя* **rule** *номер_правила*

#### Режим интерфейса

Режим настройки.

#### Ветвь конфигурации

```
firewall {
    ipv6-name текст {
        rule 1-9999 {
            disable
        }
    }
}
```

#### Параметры

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

#### Значение по умолчанию

Правило включено (используется).

#### Указания по использованию

Данная команда позволяет отключить правило межсетевого экрана IPv6.

Форма **set** данной команды используется для отключения указанного правила.

Форма **delete** данной команды используется для включения указанного правила.

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

## 14.6.10. firewall ipv6-name <имя> rule <номер_правила> icmpv6 type

Указание кода и типа ICMPv6 для правила межсетевого экрана IPv6.

**Синтаксис**

**set firewall ipv6-name** *имя* **rule** *номер_правила* **icmpv6 type** *тип*

**delete firewall ipv6-name** *имя* **rule** *номер_правила* **icmpv6 type**

**show firewall ipv6-name** *имя* **rule** *номер_правила* **icmpv6 type**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
     ipv6-name текст {
          rule 1-9999 {
               icmpv6 {
                    type текст
               }
          }
     }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

*тип*

Корректный тип и код ICMPv6 от 0 до 255; например, 128 (эхо-запрос), или

пара тип/код (каждое от 0 до 255); например, 1/4 (порт недоступен). Также можно указать символьное обозначение типа ICMPv6; например, **echo-request** (эхо-запрос). Список типов и кодов ICMPv6 приведен в “Приложение 2: Типы ICMPv6 ”

**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. Следует отметить, что при использовании данной команды необходимо, чтобы протокол был установлен в "**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.

## 14.6.11. firewall ipv6-name <имя> rule <номер_правила> ipsec

Установка соответствия для пакетов IPSec.

**Синтаксис**

```
set firewall ipv6-name имя rule номер_правила ipsec
[match-ipsec|match-none]

delete firewall ipv6-name имя rule номер_правила ipsec
[match-ipsec|match-none]

show firewall ipv6-name имя rule номер_правила ipsec
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    ipv6-name текст {
        rule 1-9999 {
```

```
                    ipsec {
                        match-ipsec
                        match-none
                    }
                }
            }
        }
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

***match-ipsec***

Установка соответствия для входящих пакетов IPSec.

**match-none**

Установка соответствия для входящих пакетов за исключением пакетов IPSec.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда используется для установки соответствия входящих 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** используется для отображения настройки.

**firewall ipv6-name <имя> rule <номер_правила> limit**

Указание параметров, ограничивающих скорость трафика для правила межсетевого экрана IPv6.

**Синтаксис**

**set firewall ipv6-name** *имя* **rule** *номер_правила* **limit** [**burst** *размер* | **rate** *скорость* ]

**delete firewall ipv6-name** *имя* **rule** *номер_правила* **limit** [**burst** | **rate**]

**show firewall ipv6-name** *имя* **rule** *номер_правила* **limit** [**burst** | **rate**]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    ipv6-name текст {
        rule 1-9999 {
            limit {
                burst целоебеззнака32разр
                rate текст
            }
        }
    }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать 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.

*скорость*

Максимальная средняя скорость 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). Скорость указывается в следующем формате "*X*/<*единица времени*>". Например, "**2/second**" ограничит скорость для сетевых пакетов, для которых было установлено соответствие, двумя пакетами в секунду.

**Значение по умолчанию**

Ограничения не установлено.

**Указания по использованию**

Данная команда используется для ограничения скорости сетевых пакетов, для которых установлено соответствие данному правилу. Для ограничения скорости входящих сетевых пакетов используется фильтр TBF (Token Bucket Filter), который позволяет административно задать требуемую скорость, а также ее превышение для коротких групп пакетов.

Для реализации TBF используется буфер (bucket), который постоянно заполняется маркерами 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 связывании данного алгоритма с двумя потоками - маркеров и данных, 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. Далее, накопленные маркеры могут использоваться для передачи групп пакетов со скоростью, превышающей установленную скорость прибывающих маркеров.

- Данные прибывают быстрее, чем маркеры. Это означает, что в буфере скоро не останется маркеров, что заставит алгоритм приостановить передачу

данных. Эта ситуация называется "превышением". Если пакеты продолжают поступать, они начинают уничтожаться.

Параметр "**rate**" позволяет установить скорость маркеров (token rate), параметр "**burst**" позволяет установить размер буфера. Описание используемых параметров:

**rate** - В том случае если данное значение явно указано, проверка соответствия для сетевых пакетов осуществляется с указанной максимальной средней скоростью. Время может быть указано в следующих единицах: **second** (секунды), **minute** (минуты), **hour** (часы), а также **day** (дни).

Например, "**1/second**" ограничит скорость проверки соответствия одним пакетом в секунду.

**burst** - В том случае если данное значение указано явно, проверка соответствия для сетевых пакетов, определяемых данным значением, осуществляется с превышением указанной скорости. По умолчанию установлено значение равное 1. Таким образом, в том случае если не требуется обрабатывать короткие группы пакетов с превышением скорости, данный параметр можно оставить прежним.

Форма **set** данной команды позволяет ограничить трафик для указанного правила.

Форма **delete** данной команды используется для удаления ограничения трафика для указанного правила.

Форма **show** данной команды используется для отображения установленного ограничения трафика.

### 14.6.12. firewall ipv6-name <имя> rule <номер_правила> l7protocol <протокол>

Указание протокола для фильтрации пакетов на прикладном уровне.

**Синтаксис**

**set firewall ipv6-name** *имя* **rule** *номер_правила* **l7protocol** *протокол*

**delete firewall ipv6-name** *имя* **rule** *номер_правила* **l7protocol**

**show firewall ipv6-name** *имя* **rule** *номер_правила* **l7protocol**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    ipv6-name текст {
        rule 1-9999 {
            l7protocol текст
        }
    }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

*протокол*

Имя протокола прикладного уровня, используемого для фильтрации пакетов. Список допустимых значений приведен в приложении 5 на стр. 2113.

**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 следует помнить, что для корректной работы механизма классификатор трафика должен видеть весь имеющий значение для классификации трафик. Для этого под правило межсетевого экрана, 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 (список протоколов см. в приложении 5), 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.

## 14.6.13. firewall ipv6-name <имя> rule <номер_правила> log <состояние>

Включение или отключение регистрации для действий правил межсетевого экрана IPv6.

**Синтаксис**

**set firewall ipv6-name** *имя* **rule** *номер_правила* **log** *состояние*

**delete firewall ipv6-name** *имя* **rule** *номер_правила* **log**

**show firewall ipv6-name** *имя* **rule** *номер_правила* **log**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    ipv6-name текст {
        rule 1-9999 {
            log [enable|disable]
        }
    }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

*состояние*

Включение или отключение регистрации действий межсетевого экрана. Поддерживаются следующие 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 для указанного правила. В том случае если регистрация включена, в журнал заносятся все выполненные действия .

Форма **set** данной команды используется для включения регистрации указанного правила.

Форма **delete** данной команды используется для удаления установленного значения.

Форма **show** данной команды используется для отображения установленного значения.

### 14.6.14. firewall ipv6-name <имя> rule <номер_правила> p2p <имя_приложения>

Указание однорангового приложения, к которому применяется правило межсетевого экрана IPv6.

**Синтаксис**

**set firewall ipv6-name** *имя* **rule** *номер_правила* **p2p** *имя_приложения*

**delete firewall ipv6-name** *имя* **rule** *номер_правила* **p2p** *имя_приложения*

**show firewall ipv6-name** *имя* **rule** *номер_правила* **p2p**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    ipv6-name текст {
        rule 1-9999 {
            p2p {
                [all|applejuice|bittorrent|
directconnect| edonkey|gnutella|kazaa]
            }
        }
    }
```

}

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

*имя_приложения*

Обязательный. Соответствие устанавливается для пакетов однорангового приложения. Поддерживаются следующие значения:

**all**: Соответствие устанавливается для пакетов любого из приложений, перечисленных в списке ниже.

**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 одноранговых приложений, к пакетам которых применяется правило. 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.

## 14.6.15. firewall ipv6-name <имя> rule <номер_правила> protocol <протокол>

Указание протокола, к которому применяется правило межсетевого экрана IPv6.

**Синтаксис**

**set firewall ipv6-name** *имя* **rule** *номер_правила* **protocol** *протокол*

**delete firewall ipv6-name** *имя* **rule** *номер_правила* **protocol**

**show firewall ipv6-name** *имя* **rule** *номер_правила* **protocol**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    ipv6-name текст {
        rule 1-9999 {
            protocol текст
        }
    }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

*протокол*

Обязательный. Могут быть использованы любые наименования протоколов или их номера, определенные в файле **/etc/protocols**. Ключевые слова **icmpv6** и all также могут быть использованы.

При указании перед названием протокола восклицательного знака (“!”) соответствие будет установлено для любого протокола за исключением указанного. Например, при указании **!tcp** соответствие будет установлено для всех протоколов за исключением TCP.

**Значение по умолчанию**

По умолчанию определены все (**all**) протоколы.

**Указания по использованию**

Данная команда используется для определения протоколов, к пакетам которых применяется правило IPv6. Для пакетов указанного протокола будет установлено соответствие критериям данного правила.

Следует с осторожностью включать в набор правил более одного правила, определяющего исключения (правило, в котором указывается восклицательный знак "!").

Также следует отметить, что этот параметр работает несколько иначе, чем такой же для протокола IPv4. Для протокола IPv4, это поле строго соответствует полю идентификатора протокола ("protocol ID") заголовка IPv4. Для IPv6, этот параметр соответствует полю последнего следующего заголовка ("last" next-header field) в цепочке заголовков IPv6. Это означает, что если у сетевого пакета нет расширенных заголовков, оно будет соответствовать полю следующего заголовка (next-header field) основного заголовка IPv6. Если у пакета есть расширенные заголовки, этот параметр будет соответствовать полю следующего заголовка последнего расширенного заголовка в цепочке. Другими словами, этот параметр всегда соответствует идентификатору транспортного уровня сетевого пакета.

Форма **set** данной команды позволяет указать 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.

### 14.6.16. firewall ipv6-name <имя> rule <номер_правила> recent

Установка соответствия для сетевых пакетов недавно встречавшихся отправителей.

**Синтаксис**

**set firewall ipv6-name** *имя* **rule** *номер_правила* **recent** [**count** *счетчик* | **time** *секунды* ]

**delete firewall ipv6-name** *имя* **rule** *номер_правила* **recent** [**count** | **time**]

**show firewall ipv6-name** *имя* **rule** *номер_правила* **recent** [**count** | **time**]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    ipv6-name текст {
        rule 1-9999 {
            recent {
                count целоебеззнака32разр
                time целоебеззнака32разр
            }
        }
    }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

*счетчик*

Обязательный. Количество пакетов с одинаковым IP-адресом отправителя, пришедших в систему в течение указанного периода времени.

*секунды*

Обязательный. Количество времени, указываемое в секундах, в течение которого будет происходить подсчет пакетов от одного отправителя.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет установить соответствие для сетевых пакетов, пришедших от недавно встречавшихся отправителей. Данная команда может использовать для предотвращения атак, использующих перебор (“brute force” attacks), когда внешнее устройство открывает непрерывный поток подключений (например, к порту SSH) в попытке взломать систему. Несмотря на то, что адрес внешнего узла заранее неизвестен, список недавно встречавшихся отправителей позволит устанавливать соответствие для сетевых пакетов на основе данного адреса.

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.

## 14.6.17. firewall ipv6-name <имя> rule <номер_правила> source

Указание адреса отправителя и номера сетевого порта для проверки соответствия в правиле межсетевого экрана IPv6.

**Синтаксис**

```
set firewall ipv6-name имя rule номер_правила source
[address адрес | mac-address mac-адрес | port порт ]

delete firewall ipv6-name имя rule номер_правила source
[address | mac-address | port]

show firewall ipv6-name имя rule номер_правила source
[address | mac-address | port]
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {

    ipv6-name текст {
```

```
            rule 1-9999 {
                source {
                    address текст
                    mac-address текст
                    port текст
                }
            }
        }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

*адрес*

Адрес отправителя для проверки соответствия. Допустимые форматы:

*ipv6-адрес*: IPv6-адрес; например, fe80::20c:29fe:fe47:f89.

*ipv6-адрес*/*префикс*: Адрес сети, где ::/0 соответствует любой сети; например, fe80::20c:29fe:fe47:f88/64

*ipv6-адрес*–*ipv6-адрес*: Диапазон IPv6-адресов; например, fe80::20c:29fe:fe47:f00–fe80::20c:29fe:fe47:f89.

**!***ipv6-адрес*: Соответствие будет установлено для всех IPv6-адресов кроме указанного.

**!***ipv6-адрес*/*префикс*: Соответствие буден установлено для всех адресов сетей кроме указанного.

**!***ipv6-адрес*–*ipv6-адрес*: Соответствие будет установлено для всех IPv6-адресов кроме входящих в указанный диапазон.

*mac-адрес*: MAC-адрес. Адрес указывается в формате шести разделенных двоеточиями 8-битных шестнадцатеричных чисел, например, 00:0a:59:9a:f2:ba.

`порт`

Порт источника для проверки соответствия. 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 адрес источника, по которому будет осуществляться проверка соответствия пакета критериям правила IPv6 межсетевого экрана.

Следует с осторожностью включать в набор правил более одного правила, определяющего исключения (правило, в котором указывается восклицательный знак "!").

Форма **set** используется для создания адреса отправителя для правила межсетевого экрана.

Форма **delete** данной команды используется для удаления настройки отправителя для правила межсетевого экрана.

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

## 14.6.18. firewall ipv6-name <имя> rule <номер_правила> state

Указание типов пакетов, к которым применяется правило.

**Синтаксис**

```
set firewall ipv6-name имя rule номер_правила state
[established состояние | invalid состояние | new
состояние | related состояние ]
```

**delete firewall ipv6-name** *имя* **rule** *номер_правила* **state**

**show firewall ipv6-name** *имя* **rule** *номер_правила* **state**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    ipv6-name текст {
        rule 1-9999 {
            state {
                established [enable|disable]
                invalid [enable|disable]
                new [enable|disable]
                related [enable|disable]
            }
        }
    }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

**established** *состояние*

Позволяет указать следует ли применять данное правило к пакетам, относящимся к установленному соединению. Поддерживаются следующие значения:

**enable**: Применить правило к пакетам, относящимся к установленному соединению.

**disable**: Не применять правило к пакетам, относящимся к установленному соединению.

**invalid** *состояние*

Позволяет указать следует ли применять данное правило к недопустимым пакетам. Поддерживаются следующие значения:

**enable**: Применить правило к недопустимым пакетам.

**disable**: Не применять правила к недопустимым пакетам.

**new** *состояние*

Позволяет указать следует ли применять данное правило к пакетам, относящимся к новому соединению. Поддерживаются следующие значения:

**enable**: Применить правило к пакетам, относящимся к новому соединению.

**disable**: Не применять правило к пакетам, относящимся к новому соединению.

**related** *состояние*

Позволяет указать, следует ли применять данное правило к пакетам, относящимся к связанному соединению. Поддерживаются следующие значения:

**enable**: Применить данное правило к пакетам, относящимся к связанному соединению.

**disable**: Не применять данное правило к пакетам, относящимся к связанному соединению.

**Значение по умолчанию**

Указанное правило применяется ко всем пакетам вне зависимости от состояния.

**Указания по использованию**

Данная команда позволяет указать, вид пакетов к которым будет применяться данное правило.

- *Established* - Пакеты, относящиеся к установленному соединению; например, пакет ответа, или исходящий пакет, для соединения установленного извне.

- *Invalid* - недопустимые пакеты, которые не могут быть идентифицированы по каким-либо причинам. В число этих причин может входить исчерпание ресурсов системы или ошибки ICMP, которые не могут быт соотнесены ни с одним известным соединением. Обычно эти пакеты отбрасываются.

- *New* - пакеты, относящиеся к новому соединению. Для протокола TCP, это пакеты с установленным флагом SYN.

- *Related* - пакеты, относящиеся к связанным соединениям.

Форма **set** данной команды позволяет указать тип пакетов, к которому будет применяться правило IPv6 межсетевого экрана.

Форма **delete** данной команды позволяет восстановить поведение, принятое по умолчанию.

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

### 14.6.19. firewall ipv6-name <имя> rule <номер_правила> tcp flags

Указание флагов TCP для проверки соответствия в правиле межсетевого экрана IPv6.

#### Синтаксис

**set firewall ipv6-name** *имя* **rule** *номер_правила* **tcp flags** *флаги*

**delete firewall ipv6-name** *имя* **rule** *номер_правила* **tcp flags**

**show firewall ipv6-name** *имя* **rule** *номер_правила* **tcp flags**

#### Режим интерфейса

Режим настройки.

#### Ветвь конфигурации

```
firewall {
    ipv6-name текст {
        rule 1-9999 {
            tcp {
                flags текст
            }
        }
    }
}
```

#### Параметры

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет проверять соответствие сетевых пакетов критериям правила IPv6 на основе флагов 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.

## 14.6.20. firewall ipv6-name <имя> rule <номер_правила> time

Применение правил межсетевого экрана с учетом даты и времени.

**Синтаксис**

**set firewall ipv6-name** *имя* **rule** *номер_правила* **time** [**monthdays** *дни_месяца* | **startdate** *дата* | **starttime** *время* | **stopdate** *дата* | **stoptime** *время* | **utc** | **weekdays** *дни_недели*]

**delete firewall ipv6-name** *имя* **rule** *номер_правила* **time**

**show firewall ipv6-name** *имя* **rule** *номер_правила* **time**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    ipv6-name текст {
        rule 1-9999 {
            time {
                monthdays 1..31, ...
                startdate дата
                starttime время
```

```
                    stopdate дата
                    stoptime время
                    utc
                    weekdays Mon...Sun, ...
                }
            }
        }
    }
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана.

*номер_правила*

Численный идентификатор правила. Значение должно лежать в диапазоне от 1 до 9999.

**monthdays** *дни_месяца*

Дни месяца, в которые применяется указанное правило. Поддерживаются следующие значения: дни месяца (с 1 по 31), указанные через запятую (например, 2,12,21). Может быть указан восклицательный знак (“!”) для указания отрицания списка значений (например, !2,12,21). В данном случае правило межсетевого экрана будет применяться во все дни, кроме указанных.

**startdate** *дата*

Начало периода времени, в течение которого правило будет применяться. Дата (а также в случае необходимости время) указывается в следующем формате:

*гггг-мм-дд* (например, 2009-03-12)

*гггг-мм-дд***T***чч:мм:сс* (например, 2009-03-12T17:30:00)

По умолчанию установлено значение 1970-01-01. Время указывается в 24-часовом формате (значение должно лежать в диапазоне от 00:00:00 до 23:59:59). В том случае если время явно не указано, по умолчанию устанавливается начало указанного дня (то есть, 00:00:00). Для указания

окончания периода действия правила используется параметр **stopdate** .

**starttime** *время*

Время начала периода, в течение которого правило будет применяться. Время указывается в следующем формате:

*чч:мм:сс* (например, 17:30:00).

Время указывается в 24-часовом формате (значение должно лежать в диапазоне от 00:00:00 до 23:59:59). Для указания времени окончания периода действия правила используется параметр **stoptime**.

**stopdate** *дата*

Указание даты и времени окончания периода действия правила. Дата (а также в случае необходимости время) указывается в следующем формате:

*гггг-мм-дд* (например, 2009-03-12)

*гггг-мм-дд***T***чч:мм:сс* (например, 2009-03-12T17:30:00)

По умолчанию установлено значение 2038-01-19. Время указывается в 24-часовом формате (значение должно лежать в диапазоне от 00:00:00 до 23:59:59). В том случае если время явно не указано, по умолчанию устанавливается начало указанного дня (то есть, 00:00:00). Параметр **startdate** используется для указания начала периода действия правила.

**stoptime** *время*

Время окончания периода, в течение которого правило будет применяться. Время указывается в следующем формате:

чч:мм:сс (например, 17:30:00).

Время указывается в 24-часовом формате (значение должно лежать в диапазоне от 00:00:00 до 23:59:59). Параметр starttime используется для указания окончания периода действия правила.

**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.

**weekdays** *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 межсетевого экрана будет применяться во все дни недели, кроме указанных.

**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.

Все значения являются необязательными, в случае указания нескольких параметров объединяются логическим И.

Форма **set** данной команды используется для указания периода действия правила межсетевого экрана IPv6.

Форма **delete** данной команды используется для восстановления поведения по умолчанию.

Форма **show** данной команды используется для отображения настройки периода действия правила межсетевого экрана.

## 14.6.21. firewall ipv6-receive-redirects <состояние>

Обработка сообщений IPv6 ICMP о перенаправлении.

**Синтаксис**

```
set firewall ipv6-receive-redirects [enable | disable]
delete firewall ipv6-receive-redirects
show firewall ipv6-receive-redirects
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    ipv6-receive-redirects [enable|disable]
}
```

**Параметры**

**enable**

Обрабатывать полученные сообщения ICMPv6 о перенаправлении (тип 5).

**disable**

Не обрабатывать полученные сообщения ICMPv6 о перенаправлении (тип 5).

**Значение по умолчанию**

По умолчанию установлено значение **disable**.

**Указания по использованию**

Данная команда позволяет указать, следует ли обрабатывать полученные сообщения ICMPv6 о перенаправлении (тип 5).

Форма **set** позволяет разрешить или запретить обработку полученных сообщений ICMPv6 о перенаправлении.

Форма **delete** используется для удаления установленного значения.

Форма **show** используется для отображения установленного значения.

## 14.6.22. firewall ipv6-src-route <состояние>

Обработка пакетов IPv6 с расширенным заголовком маршрутизации.

**Синтаксис**

```
set firewall ipv6-src-route [enable | disable]
delete firewall ipv6-src-route
show firewall ipv6-src-route
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
firewall {
    ipv6-src-route [enable|disable]
}
```

**Параметры**

**enable**

Обрабатывать пакеты IPv6 с заголовком маршрутизации типа 2.

**disable**

Не обрабатывать пакеты IPv6 с заголовком маршрутизации.

**Значение по умолчанию**

По умолчанию установлено значение **disable**.

**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.

## 14.6.23. interfaces <интерфейс> firewall <направление> ipv6-name <имя_межсетевого экрана>

Применение экземпляра межсетевого экрана IPv6 к определенному интерфейсу.

**Синтаксис**

```
set interfaces интерфейс firewall [in ipv6-name
имя_межсетевого_экрана | local ipv6-name
имя_межсетевого_экрана | out ipv6-name
имя_межсетевого_экрана ]

delete interfaces интерфейс firewall [in ipv6-name |
local ipv6-name | out ipv6-name]

show interfaces интерфейс firewall [in ipv6-name | local
ipv6-name | out ipv6-name]
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces текст {
    firewall {
```

```
                in {
                     ipv6-name текст
                }
                local {
                     ipv6-name текст
                }
                out {
                     ipv6-name текст
                }
           }
      }
```

**Параметры**

*интерфейс*

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице ниже в разделе Указания по использованию.

**in ipv6-name** *имя_межсетевого_экрана*

Применить указанный экземпляр межсетевого экрана IPv6 на указанном интерфейсе.

**local ipv6-name** *имя_межсетевого_экрана*

Применить указанный экземпляр межсетевого экрана IPv6 к сетевому трафику, приходящему на указанный интерфейс и предназначенному для локальной системы.

**out ipv6-name** *имя_межсетевого_экрана*

Применить указанный экземпляр межсетевого экрана IPv6 к сетевому трафику, отправляемому через указанный интерфейс.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет применить экземпляр межсетевого экрана IPv6, или набор правил, к интерфейсу.

Межсетевой экран никак не влияет на трафик, проходящий через систему, или предназначенный для локальной системы, до тех пор пока набор правил межсетевого экрана не будет применен к интерфейсу (реальному или виртуальному) с использованием данной команды.

Для включения межсетевого экранирования, следует определить набор правил межсетевого экрана, в качестве именованного экземпляра межсетевого экрана, с помощью команды **firewall** (см. стр. 897). Затем следует применить экземпляр межсетевого экрана к интерфейсам и/или виртуальным интерфейсам, с помощью данной команды. После чего данный экземпляр межсетевого экрана будет функционировать в качестве пакетного фильтра.

Экземпляр межсетевого экрана будет фильтровать сетевые пакеты одним из следующих способов, в зависимости от того, что было указано при его применении:

- **in**. Если применить набор правил с помощью ключевого слова **in**, межсетевой экран будет фильтровать пакеты, принимаемые на интерфейсе.
- **out**. Если применить набор правил с использованием ключевого слова **out**, межсетевой экран будет фильтровать пакеты, покидающие интерфейс.
- **local**. Если применить набор правил с использованием ключевого слова **local**, межсетевой фильтр будет фильтровать пакеты, предназначенные для системы Altell NEO.

На каждом интерфейсе можно применить до трех экземпляров межсетевого экрана: один экземпляр межсетевого экрана, фильтрующий транзитный трафик, принимаемый на интерфейсе (**in**), один экземпляр межсетевого экрана, фильтрующий транзитный трафик, покидающий интерфейс (**out**), и один экземпляр межсетевого экрана, фильтрующий трафик, предназначенный для локальной системы (**local**).

Следует удостовериться, что применяемый экземпляр межсетевого экрана заранее определен, в противном случае могут быть получены результаты, отличные от ожидаемых. При применении к интерфейсу экземпляра межсетевого экрана, которого не существует, будет применено неявное разрешающее правило **allow all**.

В приведенной ниже таблице показан синтаксис и параметры поддерживаемых типов интерфейсов.

*Таблица 36 - Типы интерфейсов*

| Тип интерфейса | Синтаксис | Параметры |
|---|---|---|
| Агрегирование каналов | `bonding` *`bondx`* | *bondx* Идентификатор интерфейса агрегированных каналов. Поддерживаются значения в диапазоне от **bond0** до **bond99**. |
| Виртуальный интерфейс агрегированных каналов | `bonding` *`bondx`* `vif` *`идентификатор_vlan`* | *bondx* Идентификатор интерфейса агрегированных каналов. Поддерживаются значения в диапазоне от **bond0** до **bond99**.<br>*идентификатор_vlan* Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 0 до 4094. |
| Сетевой мост | `bridge` *`brx`* | *brx* Имя мостовой группы. Поддерживаются значения в диапазоне от **br0** до **br999**. |
| Ethernet | `ethernet` *`ethx`* | *ethx* Имя интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**, в зависимости от доступных в системе физических интерфейсов. |
| Ethernet PPPoE | `ethernet` *`ethx`* `pppoe` *`номер`* | *ethx* Имя интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**, в зависимости от доступных в системе физических интерфейсов.<br>*номер* Имя определенного блока PPPoE. Значение должно лежать в диапазоне от 0 до 15. |
| Виртуальный интерфейс Ethernet | `ethernet` *`ethx`* `vif` *`идентификатор_vlan`* | *ethx* Имя интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**, в зависимости от доступных в системе физических интерфейсов.<br>*идентификатор_vlan* Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 0 до 4094. |
| Ethernet Vif PPPoE | `ethernet` *`ethx`* `vif` | *ethx* Имя интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**, в зависимости от |

| Тип интерфейса | Синтаксис | Параметры |
|---|---|---|
| | *идентификатор_vlan* pppoe *номер* | доступных в системе физических интерфейсов.<br>*идентификатор_vlan* Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 0 до 4094.<br>*номер* Имя определенного блока PPPoE. Значение должно лежать в диапазоне от 0 до 15. |
| Интерфейс заглушки | loopback *lo* | *lo* Имя интерфейса заглушки. |
| Многоканальная связь | multilink *mlx* vif 1 | *mlx* Идентификатор многоканальной связки. Можно создать до двух многоканальных связок. Значение должно лежать в диапазоне от ml0 (“эм эль ноль”) до ml23 (“эм эль двадцать три”).<br>**1** Идентификатор виртуального интерфейса. На текущий момент, можно создать только один виртуальный интерфейс для многоканального интерфейса, с идентификатором 1. Виртуальный интерфейс должен быть заранее определен. |
| OpenVPN | openvpn *vtunx* | *vtunx* Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое число. |
| Псевдо-Ethernet | pseudo-ethernet *pethx* | *pethx* Имя интерфейса псевдо-Ethernet. Значение должно лежать в диапазоне от **peth0** до **peth999**. |
| Последовательный PPP | serial *wanx* ppp vif 1 | *wanx* Последовательный интерфейс: значение должно лежать в диапазоне от **wan0** до **wan23**. Интерфейс должен быть заранее определен.<br>**1** Идентификатор виртуального интерфейса. На текущий момент, можно создать только один виртуальный интерфейс для интерфейса "точка-точка", с идентификатором 1. Виртуальный интерфейс должен |

| Тип интерфейса | Синтаксис | Параметры |
|---|---|---|
| | | быть заранее определен. |
| Туннель | `tunnel` *tunx* | *tunx* Идентификатор туннельного интерфейса. Значение должно лежать в диапазоне от **tun0** до **tun23**. |

Форма **set** данной команды позволяет применить экземпляр межсетевого экрана IPv6 к интерфейсу.

Форма **delete** данной команды позволяет удалить экземпляр межсетевого экрана IPv6 для интерфейса.

Форма **show** данной команды позволяет отобразить настройку экземпляра межсетевого экрана IPv6 для интерфейса.

## 14.6.24. show firewall ipv6-name

Вывод сведений об указанных наборах правил IPv6, показывающих к каким интерфейсам или зонам они применяются.

**Синтаксис**

```
show firewall ipv6-name [detail | statistics | [имя
[detail | statistics | rule номер_правила | detail rule
номер_правила ]]]
```

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

**detail**

Необязательный. Вывод подробных сведений обо всех экземплярах межсетевого экрана, настроенных в ветви “**ipv6-name**” дерева настройки.

**statistics**

Необязательный. Вывод статистики для всех экземплярах межсетевого экрана, настроенных в ветви “**ipv6-name**” дерева настройки.

*имя*

Необязательный. Вывод сведений обо всех правилах межсетевого экрана, настроенных в указанном экземпляре.

*имя* **detail**

Необязательный. Вывод подробных сведений обо всех правилах

межсетевого экрана, настроенных в указанном экземпляре межсетевого экрана.

*имя* **statistics**

Необязательный. Вывод статистических сведений обо всех правилах межсетевого экрана, настроенных в указанном экземпляре межсетевого экрана.

*имя* **rule** *номер_правила*

Необязательный. Вывод сведений об указанном правиле межсетевого экрана, настроенном в указанном экземпляре межсетевого экрана.

*имя* **detail rule** *номер_правила*

Необязательный. Вывод подробных сведений об указанном правиле межсетевого экрана, настроенном в указанном экземпляре межсетевого экрана.

**Значение по умолчанию**

По умолчанию выводятся сведения обо всех экземплярах межсетевого экрана, настроенных в ветви “**ipv6-name**” дерева настройки.

**Указания по использованию**

Данная команда позволяет вывести сведения о экземплярах межсетевого экрана, настроенных в ветви "**ipv6-name**" дерева настройки.

**Примеры**

В примере 14.36 приведен вывод краткой информации обо всех правилах межсетевого экрана, настроенных в ветви “**ipv6-name**” дерева настройки для R1.

*Пример 14.36 - "show firewall ipv6-name": Вывод сведений о межсетевом экране*

```
admin@R1:~$ show firewall ipv6-name
IPv6 Firewall "TEST2": Active on (eth0,IN) (
State Codes: E - Established, I - Invalid, N - New, R -
Related)
rule   action   source   destination  proto state
10     ACCEPT   ::/0     ::/0         tcp   any
10000  DROP     ::/0     ::/0         all   any
```

В примере 14.37 приведен вывод подробных сведений обо всех правилах межсетевого экрана, настроенных в ветви “ipv6-name” дерева настройки для R1.

*Пример 14.37 - “show firewall ipv6-name detail”: Вывод детализированных сведений о правиле*

```
admin@R1:~$ show firewall ipv6-name detail
IPv6 Firewall "TEST2": Active on (eth0,IN)
rule   action   proto packets bytes
10     accept   tcp    0 0
10000  drop     all    0 0
```

В примере 14.38 приведен вывод статистики для всех правил межсетевого экрана, настроенных в ветви “ipv6-name” в дереве настройки для R1.

*Пример 14.38 - “show firewall ipv6-name statistics”: Вывод статистики для правила.*

```
admin@R1:~$ show firewall ipv6-name statistics
IPv6 Firewall "TEST2": Active on (eth0,IN)
rule   packets bytes action  source  destination
10     0       0     ACCEPT  ::/0    ::/0
1000   0       3     DROP    ::/0    ::/0
```

## 14.7. Команды межсетевого экрана на основе зон

В этом разделе описаны команды для реализации межсетевого экрана на основе зон в системе Altell NEO.

В данном разделе описаны следующие команды:

*Таблица 37 -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> firewall ipv6-name <имя>` | Применение фильтрации пакетов в соответствии с определением в наборе правил межсетевого экрана для IPv6 к трафику, приходящему из указанной зоны-“отправителя”. |
| `zone-policy zone <зона-получатель> from <зона-отправитель> firewall name <имя>` | Применение фильтрации пакетов в соответствии с определением в наборе правил межсетевого экрана для IPv4 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”. |

## 14.7.1. 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` *текст* {

}

**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 системе Altell NEO 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 применен набор правил межсетевого экрана.

- 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.

## 14.7.2. 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 текст {
    default-action [drop|reject]
}
```

**Параметры**

*действие*

Действие, которое должно быть выполнено для трафика, приходящего в зону безопасности. Поддерживаются следующие значения:

- **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 для выполнения 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 данной 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.

### 14.7.3. 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 текст {
    description текст
}
```

**Параметры**

*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.

## 14.7.4. 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** *зона-отправитель*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
zone-policy zone текст {
    from-zone текст
}
```

**Параметры**

*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.

## 14.7.5. zone-policy zone <зона-получатель> from <зона-отправитель> firewall ipv6-name <имя>

Применение фильтрации пакетов в соответствии с определением в наборе правил межсетевого экрана для IPv6 к трафику, приходящему из указанной зоны-“отправителя”.

**Синтаксис**

```
set zone-policy zone зона-получатель from зона-
отправитель firewall ipv6-name имя

delete zone-policy zone зона-получатель from зона-
отправитель firewall ipv6-name

show zone-policy zone зона-получатель from зона-
отправитель firewall ipv6-name
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
zone-policy zone текст {
     from-zone текст {
     firewall {
          ipv6-name текст
          }
     }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана для IPv6.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для применения набора правил для протокола IP версии 6 (IPv6) в качестве фильтра пакетов к любому трафику, приходящему из зоны-“отправителя”.

В качестве фильтров пакетов для зоны-“отправителя” можно применить один набор правил для IPv6 и один набор правил для IPv4.

Форма **set** этой команды используется для указания набора правил для IPv6 в качестве фильтра пакетов для зоны-“отправителя”.

Форма **delete** этой команды используется для удаления набора правил для IPv6 из состава фильтров пакетов, определенных для зоны-“отправителя”.

Форма **show** используется для вывода имени фильтра пакетов, примененного к зоне-“отправителю” (если таковой имеется).

## 14.7.6. zone-policy zone <зона-получатель> from <зона-отправитель> firewall name <имя>

Применение фильтрации пакетов в соответствии с определением в наборе правил межсетевого экрана для IPv4 к трафику, приходящему из указанной зоны-“отправителя”.

**Синтаксис**

```
set zone-policy zone зона-получатель from зона-
отправитель firewall name имя
```

**delete zone-policy zone** *зона-получатель* **from** *зона-отправитель* **firewall name**

**show zone-policy zone** *зона-получатель* **from** *зона-отправитель* **firewall name**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
zone-policy zone текст {
    from-zone текст {
        firewall {
            name текст
        }
    }
}
```

**Параметры**

*имя*

Имя набора правил межсетевого экрана для IPv4.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для применения набора правил для протокола IP версии 4 (IPv4) в качестве фильтра пакетов к любому трафику, приходящему из зоны-“отправителя”.

В качестве фильтров пакетов для зоны-“отправителя” можно применить один набор правил для IPv4 и один набор правил для IPv6.

Форма **set** этой команды используется для указания набора правил для IPv4 в качестве фильтра пакетов для зоны-“отправителя”.

Форма **delete** этой команды используется для удаления набора правил для IPv4 из состава фильтров пакетов, определенных для зоны-“отправителя”.

Форма **show** используется для вывода имени фильтра пакетов для IPv4, примененного к зоне-“отправителю” (если таковой имеется).

### 14.7.7. 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** *имя_интерфейса*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
zone-policy zone текст {
    interface текст {
    }
}
```

**Параметры**

*имя*

Множественный узел. Имя интерфейса, 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.

### 14.7.8. 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 текст {
    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 системы Altell NEO. Если указать зону безопасности как локальную, то политики межсетевого экрана, указанные для этой зоны, будут фильтровать пакеты, предназначенные для самой системы Altell NEO. 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.

# 15. ВВЕДЕНИЕ В ТЕХНОЛОГИЮ VPN

В данном разделе приведен краткий обзор различных видов частных виртуальных сетей (VPN).

В данном разделе рассматриваются следующие вопросы:

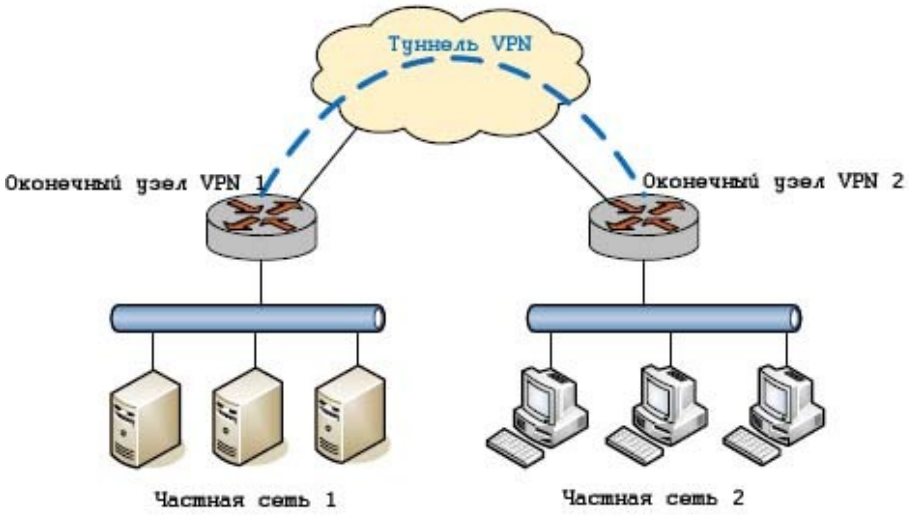
- Виды VPN.
- Поддерживаемые решения.
- Сравнение решений VPN.
- VPN и NAT.

## 15.1. Виды VPN

Altell NEO поддерживает два вида решений для построения виртуальных частных сетей VPN:

- “Межфилиальный” режим VPN ("site-to-site" VPN) позволяет соединить филиалы в одну сеть через глобальную вычислительную сеть (WAN) так, как если бы они находились в единой частной сети. Филиалы соединяются с помощью “туннеля”, как показано на рисунке 56.

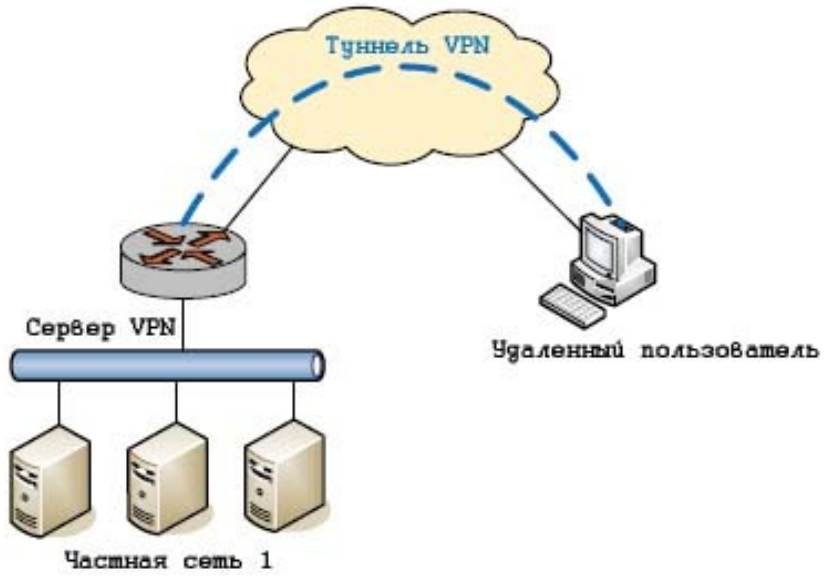
*Рисунок 56 - VPN в межфилиальном режиме*




- VPN «удаленного доступа» (remote access VPN) позволяет установить туннель VPN

между удаленным пользователем и сервером VPN. Что позволяет, например, удаленному пользователю получить доступ к корпоративной сети из дома. Данный вариант приведен на рисунке 57.

*Рисунок 57 - VPN удаленного доступа*




По существу, межфилиальный режим и режим удаленного доступа очень похожи, оба этих режима используют туннелирование, для того чтобы два оконечных устройства находились в одной сети. Различия в решениях заключаются в том, каким образом устанавливается туннель.

## 15.2. Поддерживаемые решения

Системой Altell NEO поддерживаются следующие решения:

- Межфилиальный режим на базе протоколов IPSec.
- Режим удаленного доступа на базе протокола PPTP.
- Режим удаленного доступа с использованием L2TP и IPSec.
- Межфилиальный режим и режим удаленного доступа с использованием OpenVPN.

### 15.2.1. Межфилиальный режим с использованием IPSec

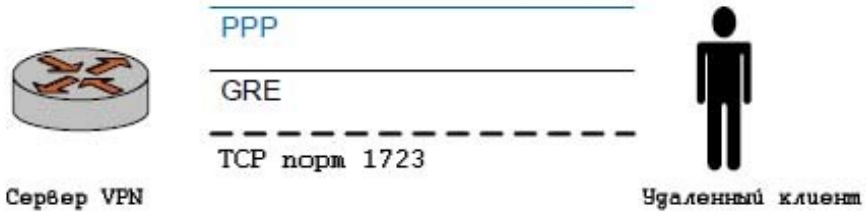
На рисунке 58 приведена схема межфилиального режима VPN с использованием IPSec.

*Рисунок 58 - Межфилиальный режим IPSec*


### 15.2.2. Удаленный доступ с использованием PPTP

На рисунке 59 приведена схема использования режима удаленного доступа VPN с использованием PPTP.

*Рисунок 59 - VPN удаленного доступа на основе протокола PPTP*



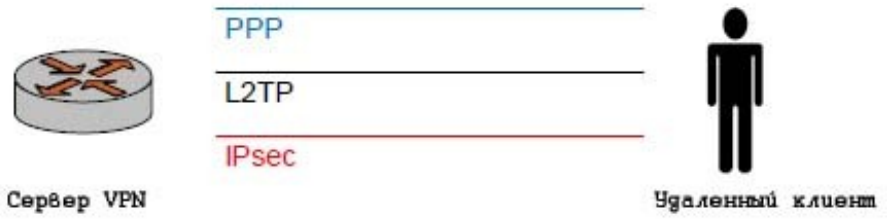

При использовании такого решения:

- Клиент PPTP устанавливает соединение TCP с сервером (порт 1723).
- Через установленное соединение, клиент PPTP и сервер устанавливают туннель GRE (Generic Routing Encapsulation).
- После чего поверх туннеля GRE устанавливается сеанс протокола PPP (Point-to-Point Protocol); то есть, пакеты PPP инкапсулируются и принимаются/отправляются через туннель GRE.

### 15.2.3. Удаленный доступ с использованием L2TP и IPSec

На рисунке 60 приведен режим VPN удаленного доступа с использованием протокола L2TP (Layer 2 Tunneling Protocol) и IPSec.

*Рисунок 60 - VPN удаленного доступа на основе L2TP/IPSec*



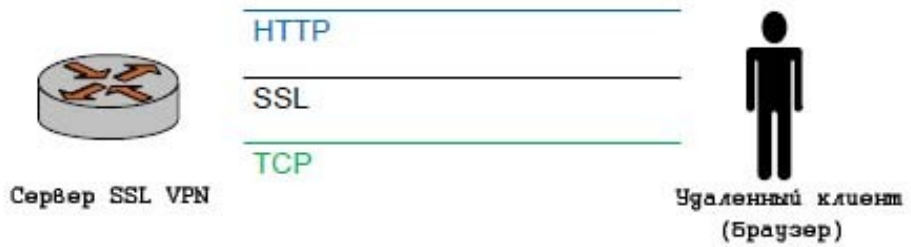

При использовании такого решения:

- Удаленный компьютер сначала устанавливает туннель IPSec к серверу VPN.
- Затем клиент и сервер L2TP устанавливают туннель L2TP поверх туннеля IPSec.
- После чего, сеанс PPP устанавливается поверх туннеля L2TP; то есть, пакеты PPP инкапсулируются и принимаются/отправляются через туннель L2TP.

### 15.2.4. Межфилиальный режим и режим удаленного доступа с использованием OpenVPN

OpenVPN представляет собой решение для построения VPN с открытым исходным кодом, которое поддерживает межфилиальный режим, а также режим удаленного доступа. Несмотря на то, что OpenVPN иногда именуется SSL (Secure Sockets Layer protocol) VPN решением, его не следует путать с “SSL VPN”, под которым в общем случае понимается продукт, использующий веб-браузер. В общем случае, основанное на использовании веб-браузера решение «SSL VPN» работает так, как показано на рисунке 61.

*Рисунок 61 - SSL VPN*




По существу, на клиентской стороне, удаленный пользователь указывает веб-браузеру защищенный (HTTPS) веб-сайт. Браузер устанавливает соединение TCP с сервером, затем

через данное соединение устанавливается сеанс SSL, после чего поверх сеанса SSL устанавливается сеанс HTTP. Сеанс SSL обеспечивает защищенный “туннель” для аутентификации сеанса HTTP.

В большинстве случаев, после того как пользователь прошел аутентификацию, веб-браузер динамически загружает фрагмент кода (например, компонент ActiveX) для запуска на клиентском устройстве. После чего такой код может, например, создать виртуальный интерфейс, для того чтобы маршрутизировать трафик VPN через туннель. В названии решения “SSL VPN” отражен тот факт, что безопасность обеспечивается протоколом SSL.

*Рисунок 62 - OpenVPN*


В OpenVPN, напротив, реализован свой собственный протокол коммуникации. Этот протокол передается поверх протокола UDP или TCP и обеспечивает защищенный туннель для трафика VPN. По умолчанию, используется протокол UDP.

Причина по которой OpenVPN иногда называют “SSL VPN” заключается в том, что в одном из режимов работы используется протокол SSL (поверх протокола OpenVPN), а также потому, что OpenVPN использует библиотеку с открытым исходным кодом OpenSSL. Решение OpenVPN отличается по принципу работы от традиционных решений “SSL VPN”, и при этом между ними нет функциональной совместимости. При использовании данного решения OpenVPN должен быть установлен на обоих оконечных точках туннеля.

## 15.3. Сравнение решений VPN

Каждое из решений имеет свои преимущества и недостатки, которые необходимо учитывать при выборе технологии построения VPN.

В данном разделе рассматриваются вопросы развертывания следующих типов решений:

- PPTP.

- L2TP/IPSec.
  - С использованием предварительных ключей.
  - С использованием сертификатов стандарта X.509.

### 15.3.1. 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 стойкости паролей, которые используются пользователями. По этой причине при использовании в практических условиях следует внимательно следить за стойкостью используемых паролей.

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.

### 15.3.2. L2TP/IPSec

L2TP (Layer 2 Tunneling Protocol) — туннельный протокол, использующийся для поддержки виртуальных частных сетей. Для обеспечения безопасности пакетов L2TP используется набор протоколов IPSec, которые обеспечивают 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 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.

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 Altell NEO). (Соединения L2TP без использования IPSec могут быть заблокированы правилом **default-drop**).

```
rule 10 {
   action accept
      destination {
         port 1701
      }
      ipsec {
         match-ipsec
      }
      protocol udp
   }
```

#### *15.3.2.1. L2TP/IPSec с использованием предварительных ключей*

Настройка режима с использованием предварительных ключей проще, чем настройка режима с использованием сертификатов стандарта X.509. Однако, 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.

#### *15.3.2.2. L2TP/IPSec с использованием сертификатов стандарта X.509*

Использование сертификатов X.509 совместно с L2TP/IPSec позволит предотвратить вышеуказанную 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 Altell NEO. 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 флэш-накопитель и перенести их на каждое из клиентских устройств, также можно передать сертификаты 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.

## 15.4. VPN и NAT

При совместном использовании NAT и VPN на одном устройстве, для получения требуемого результата необходимо соблюдать специальные меры. Более подробно данные вопросы рассматриваются в разделе 13.3.10. Маскировка и VPN .

# 16. ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ

В систему Altell NEO 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 Altell NEO.

Сервисы управления PKI реализованы на базе библиотеки OpenSSL, и предоставляют возможности по созданию сертификата пользователя и его подписание на базе российских криптографических алгоритмов (функции хэширования ГОСТ Р34.11-94, цифровой подписи — ГОСТ Р34.10-2001), 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. Однако, следует учитывать, что в настоящее время в системе Altell NEO отсутствует поддержка протокола OCSP, а возможность экспорта списка отозванных сертификатов предусмотрена только совместно с экспортом сертификатов пользователей. В связи с этим при необходимости управления крупной распределенной структурой сертификатов субъектов, рекомендуется использовать сторонние УЦ, поддерживающие оперативное управление сертификатами.

## 16.1. 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.

## 16.2. Пример настройки PKI

В этом наборе примеров приведено создание инфраструктуры открытых ключей в системе Altell NEO, генерация сертификатов, экспорт/импорт сертификатов. В данном наборе примеров используются две системы Altell NEO, имеющие имена NEO-1 и NEO-2 соответственно.

В этом разделе рассматриваются следующие вопросы:

- Создание удостоверяющего центра.
- Генерация сертификата узла NEO-1.
- Генерация сертификата узла NEO-2.
- Доставка сертификата на узел NEO-2.

### 16.2.1. 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 NEO-1.

На базе созданного удостоверяющего центра будет осуществляться централизованное создание и управление ключевыми парами и сертификатами узлов NEO-1 и NEO-2.

Для создания нового удостоверяющего центра необходимо выполнить следующие шаги на узле NEO-1 в режиме настройки.

*Пример 16.1 - Создание удостоверяющего центра на узле NEO-1*

| Действие | Команда |
|---|---|
| Создание удостоверяющего центра. | `admin@NEO-1# **set pki ca MainCA**`<br>`[edit]` |
| Указание общего имени (common name) удостоверяющего центра. | `admin@NEO-1# **set pki ca MainCA cn "Main Certification Authority"**`<br>`[edit]` |
| Указание города, в качестве одного из атрибутов идентификатора УЦ. | `admin@NEO-1# **set pki ca MainCA city SPb**`<br>`[edit]` |
| Указание страны, в качестве одного из атрибутов идентификатора УЦ. | `admin@NEO-1# **set pki ca MainCA country RU**`<br>`[edit]` |
| Указание периода действия сертификата удостоверяющего центра. | `admin@NEO-1# **set pki ca MainCA expiration 365**`<br>`[edit]` |
| Фиксация настройки. | `admin@NEO-1# **commit**`<br>`[edit]` |
| Вывод настройки. | `admin@NEO-1# **show -all pki ca MainCA**` |

| Действие | Команда |
|---|---|
| | city SPb<br>cn "Main Certification Authority"<br>country RU<br>expiration 365<br>key-type gost2001<br>[edit] |

#### *16.2.1.1. Генерация сертификата узла NEO-1*

В данном примере будет приведено создание сертификата узла NEO-1.

Для создания сертификата узла NEO-1 необходимо выполнить следующие шаги на узле NEO-1 в режиме настройки.

*Пример 16.2 - Создание сертификата узла NEO-1*

| Действие | Команда |
|---|---|
| Создание сертификата для узла NEO-1. | admin@NEO-1# **set pki ca MainCA certificate NEO-1-cert**<br>[edit] |
| Указание общего имени (common name), которое будет указано в сертификате узла NEO-1. | admin@NEO-1# **set pki ca MainCA certificate NEO-1-cert cn "NEO-1 VPN Peer certificate"**<br>[edit] |
| Фиксация настройки. | admin@NEO-1# **commit**<br>[edit] |
| Вывод настройки созданного сертификата. | admin@NEO-1# **show -all pki ca MainCA certificate NEO-1-cert**<br>cn "NEO-1 VPN Peer certificate"<br>expiration 365 |

| Действие | Команда |
|---|---|
| | `[edit]` |

#### *16.2.1.2. Генерация сертификата узла NEO-2*

В данном примере будет приведено создание сертификата узла NEO-2.

Для создания сертификата узла NEO-2 необходимо выполнить следующие шаги на узле NEO-1 в режиме настройки.

*Пример 16.3 - Создание сертификата узла NEO-2*

| Действие | Команда |
|---|---|
| Создание сертификата для узла NEO-2. | `admin@NEO-1#` **`set pki ca MainCA certificate NEO-2-cert`**<br>`[edit]` |
| Указание общего имени (common name), которое будет указано в сертификате узла NEO-2. | `admin@NEO-1#` **`set pki ca MainCA certificate NEO-2-cert cn "NEO-2 VPN Peer certificate"`**<br>`[edit]` |
| Фиксация настройки. | `admin@NEO-1#` **`commit`**<br>`[edit]` |
| Вывод настройки. | `admin@NEO-1#` **`show -all pki ca MainCA certificate`**<br>`NEO-2-cert {`<br>`cn "NEO-2 VPN Peer certificate"`<br>`expiration 365`<br>`}`<br>`NEO-1-cert {`<br>`cn "NEO-1 VPN Peer certificate"`<br>`expiration 365` |

| Действие | Команда |
|---|---|
| | } |
| | [edit] |

### *16.2.1.3. Экспорт сертификата узла NEO-2*

В данном примере приведен экспорт сертификата узла NEO-2 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 NEO-2 на флэш-накопитель необходимо выполнить следующие шаги на узле NEO-1 в эксплуатационном режиме, к устройству должен быть заранее подключен флэш-накопитель.

*Пример 16.4 - Экспортирование сертификата узла NEO-2*

| Действие | Команда |
|---|---|
| Экспортирование сертификата узла NEO-2, секретного ключа узла NEO-2, сертификата удостоверяющего центра. | admin@NEO-1:~$ **pki export certificate NEO-2-cert** |

После осуществления экспорта в корневой директории флэш-накопителя будут содержаться следующие файлы:

- cacert-MainCA.pem: сертификат удостоверяющего центра;
- cert-MainCA-NEO-2-cert.pem: сертификат узла NEO-2;
- crl-MainCA.pem: список отозванных сертификатов;

- pkey-MainCA-NEO-2-cert.pem: секретный ключ узла NEO-2.

#### *16.2.1.4. Импорт сертификата узла NEO-2*

В данном примере приведен импорт сертификата узла NEO-2 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 NEO-2;
- список отозванных сертификатов;
- секретный ключ узла NEO-2.

Монтирование и размонтирование флэш-накопителя осуществляется автоматически. В результате выполнения указанной команды в систему на узле NEO-2 будут добавлены сертификат удостоверяющего центра, сертификат узла NEO-2, подписанный указанным удостоверяющим центром, секретный ключ, а также файл, содержащий список аннулированных сертификатов.

Для импорта сертификата узла NEO-2 необходимо выполнить следующие шаги на узле NEO-2 в эксплуатационном режиме, к устройству должен быть заранее подключен флэш-накопитель.

*Пример 16.5 - Импорт сертификата узла NEO-2*

| Действие | Команда |
|---|---|
| Импорт сертификата узла NEO-2, секретного ключа узла NEO-2, сертификата удостоверяющего центра, списка отозванных сертификатов. | `admin@NEO-2:~$ pki import`<br>`Импортируется CA: Main Certification Authority`<br>`Импортируется CRL для Main_Certification_Authority`<br>`Импортируется сертификат: NEO-2 VPN Peer certificate` |

## 16.3. Команды управления PKI

В этом разделе приведены следующие команды:

*Таблица 38 - 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> 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> 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> 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> city <город>` | Указание названия города, в качестве одного из атрибутов идентификатора субъекта. |
| `pki ca <имя> certificate` | Указание названия страны, 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> 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> cn <общее_имя>` | Указание общего имени, которое входит в идентификатор 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> province <регион>` | Указание названия региона, в качестве одного из атрибутов идентификатора субъекта. |
| Эксплуатационные команды | |
| `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 субъекта, ключевой пары субъекта, сертификата УЦ, списка отозванных |

| | |
|---|---|
| | сертификатов. |
| `pki import-pkcs12 password <пароль>` | Импорт сертификата субъекта, ключевой пары субъекта, сертификата УЦ, списка отозванных сертификатов в формате PKCS12. |

### 16.3.1. 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 текст {
    }
}
```

**Параметры**

*имя*

Множественный. Название 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 его названия.

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.

### 16.3.2. 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 текст {
        city текст
    }
}
```

**Параметры**

*имя*

Название 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.

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.

### 16.3.3. 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 текст {
          cn текст
     }
}
```

**Параметры**

*имя*

Название 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.

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.

### 16.3.4. 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 текст {
        country текст
    }
}
```

**Параметры**

*имя*

Название 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.

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.

### 16.3.5. 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 текст {
          email текст
     }
}
```

**Параметры**

*имя*

Название 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.

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.

## 16.3.6. 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 текст {
          expiration целоебеззнака32разр
     }
}
```

**Параметры**

*имя*

Название 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).

**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.

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.

### 16.3.7. 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** *длина_ключа*

**show pki ca** *имя* **key-size** *длина_ключа*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
pki {
    ca текст {
        key-size [256-8192]
    }
}
```

**Параметры**

*имя*

Название удостоверяющего центра.

*длина_ключа*

Длина используемого ключа в битах. Допустимые значения:

- **256**: если в качестве используемого алгоритма используется алгоритм ГОСТ 34.10-2001 (для параметра **key-type** установлено значение **gost2001**);

- целое число в диапазоне от **256** до **8192**: если используется алгоритм RSA (для параметра **key-type** установлено значение **rsa**). Рекомендуемая минимальная длина ключа RSA 2048 бит.

**Значение по умолчанию**

При использовании алгоритма ГОСТ 34.10-2001 устанавливается длина ключа 256 бит.

При использовании алгоритма RSA устанавливается длина ключа 2048 бит.

**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 RSA допустимая длина ключа должна лежать в диапазоне от 256 до 8192 бит. В настоящее время к использованию рекомендованы длины ключей RSA от 2048 бит.

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.

## 16.3.8. 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** *тип_ключа*

**show pki ca** *имя* **key-type** *тип_ключа*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
pki {
    ca текст {
        key-type [gost2001|rsa]
    }
}
```

**Параметры**

*имя*

Название удостоверяющего центра.

*тип_ключа*

Используемый криптографический алгоритм. Допустимые значения:

**gost2001**: Использование алгоритма ГОСТ 34.10-2001. Данное значение установлено по умолчанию.

**rsa**: Использование криптосистемы RSA.

**Значение по умолчанию**

По умолчанию установлено значение **gost2001**.

**Указания по использованию**

Данная команда позволяет указать тип используемого для защиты данных криптографического алгоритма. По умолчанию используется алгоритм ГОСТ 34.10-2001.

Значения параметров УЦ, в том числе тип используемого криптографического алгоритма, 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.

## 16.3.9. 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** *организация*

**show pki ca** *имя* **organization** *организация*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
pki {
     ca текст {
          organisation текст
     }
}
```

**Параметры**

*имя*

Название 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.

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.

## 16.3.10. 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** *подразделение*

**show pki ca** *имя* **organization-unit** *подразделение*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
pki {
     ca текст {
          organisation-unit текст
     }
}
```

**Параметры**

*имя*

Название 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.

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.

## 16.3.11. 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** *регион*

**show pki ca** *имя* **province** *регион*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
pki {
     ca текст {
          province текст
     }
}
```

**Параметры**

*имя*

Название 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.

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.

### 16.3.12. 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** *имя_сертификата*

**show pki ca** *имя* **certificate** *имя_сертификата*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
pki {
     ca текст {
          certificate текст
     }
}
```

**Параметры**

*имя*

Название удостоверяющего центра.

*имя_сертификата*

Название 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.

### 16.3.13. 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** *город*

**show pki ca** *имя* **certificate** *имя_сертификата* **city** *город*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
pki {
    ca текст {
```

```
                certificate текст {
                     city текст
                }
           }
      }
```

**Параметры**

*имя*

Название удостоверяющего центра.

*имя_сертификата*

Название 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.

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.

### 16.3.14. 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** *страна*

**show pki ca** *имя* **certificate** *имя_сертификата* **country** *страна*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
pki {
    ca текст {
        certificate текст {
            country текст
        }
    }
}
```

**Параметры**

*имя*

Название удостоверяющего центра.

*имя_сертификата*

Название 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.

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.

### 16.3.15. 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 текст {
        certificate текст {
            expiration текст
        }
```

```
        }
    }
```

**Параметры**

*имя*

Название удостоверяющего центра.

*имя_сертификата*

Название 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**

Отсутствует.

**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.

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.

### 16.3.16. 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** *организация*

**show pki ca** *имя* **certificate** *имя_сертификата* **organization** *организация*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
pki {
    ca текст {
        certificate текст {
            organization текст
        }
    }
}
```

**Параметры**

*имя*

Название удостоверяющего центра.

*имя_сертификата*

Название 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.

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.

### 16.3.17. 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** *подразделение*

**show pki ca** *имя* **certificate** *имя_сертификата* **organization-unit** *подразделение*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
pki {
    ca текст {
        certificate текст {
            organization-unit текст
        }
```

```
        }
    }
```

**Параметры**

*имя*

Название удостоверяющего центра.

*имя_сертификата*

Название 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.

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.

### 16.3.18. 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** *общее_имя*

**show pki ca** *имя* **certificate** *имя_сертификата* **cn** *общее_имя*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
pki {
    ca текст {
        certificate текст {
            cn текст
        }
    }
}
```

**Параметры**

*имя*

Название удостоверяющего центра.

*имя_сертификата*

Название 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.

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.

## 16.3.19. 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** *email*

**show pki ca** *имя* **certificate** *имя_сертификата* **email** *email*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
pki {
    ca текст {
        certificate текст {
```

```
                email текст
            }
        }
    }
```

**Параметры**

*имя*

Название удостоверяющего центра.

*имя_сертификата*

Название 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.

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.

### 16.3.20. 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** *регион*

**show pki ca** *имя* **certificate** *имя_сертификата* **province** *регион*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
pki {
    ca текст {
        certificate текст {
            province текст
        }
    }
}
```

**Параметры**

*имя*

Название удостоверяющего центра.

*имя_сертификата*

Название 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.

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.

## 16.3.21. 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.

При указании параметра «**to**» производится экспорт в архив формата tar 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 39 - 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 параметра *имя_файла*: **ftp**://*пользователь*:*пароль*@*узел*/*архив* где *пользователь* это имя пользователя на узле, *пароль* это пароль, связанный с именем пользователя, *узел* это имя узла или IP-адрес сервера FTP, а *архив* это название архива, содержащего сертификат субъекта, секретный ключ, сертификат УЦ, а также список отозванных сертификатов, с указанием пути. Если *пользователь* и *пароль* не указаны, будет выдан запрос на их ввод. |

| Местоположение | Способ указания |
|---|---|
| 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. После того как узел будет добавлен в список известных узлов, может быть использован следующий синтаксис: scp://*пользователь:пароль@узел*/*файл_конфигурации*, где *пароль* это пароль, ассоциированный с пользователем. Если *пользователь* и *пароль* не указаны, будет выдан запрос на их ввод. |
| 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.*

## 16.3.22. 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.

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 удостоверяющего центра, сертификат клиента, подписанный указанным удостоверяющим центром, секретный ключ клиента и файл, содержащий список отозванных сертификатов.

> ***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.*

## 16.3.23. pki import

Импорт 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, список отозванных сертификатов.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет импортировать сертификат субъекта, сертификат УЦ, секретный ключ субъекта, а также список отозванных сертификатов. Поддерживается импорт сертификатов формата v3. По умолчанию импортируется сертификат с подключенного флэш-накопителя. При выполнении команды **pki import** к устройству должен быть подключен флэш-накопитель, в корневой директории которого должны размещаться следующие файлы:

- сертификат удостоверяющего центра;
- сертификат субъекта;
- список отозванных сертификатов;
- секретный ключ субъекта.

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, а также файл, содержащий список отозванных сертификатов.

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.

В приведенной ниже таблице показан синтаксис указания файла для

различных местоположений файла.

*Таблица 40 - 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:пароль@узел*/*архив* где *пользователь* это имя пользователя на узле, *пароль* это пароль, связанный с именем пользователя, *узел* это имя узла или IP-адрес сервера FTP, а *архив* это название архива, содержащего сертификат субъекта, секретный ключ, сертификат УЦ, а также список отозванных сертификатов, с указанием пути. Если *пользователь* и *пароль* не указаны, будет выдан запрос на их ввод. |
| 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. После того как узел будет добавлен в список известных узлов, может быть использован следующий синтаксис: scp://*пользователь:пароль@узел*/*файл_конфигурации*, где *пароль* это пароль, ассоциированный с пользователем. Если *пользователь* и *пароль* не указаны, будет выдан запрос на их ввод. |
| 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 |

| Местоположение | Способ указания |
|---|---|
| | относительно корневого каталога TFTP. |

## 16.3.24. pki import-pkcs12 password <пароль>

Импорт сертификата субъекта, ключевой пары субъекта, сертификата УЦ, списка отозванных сертификатов в формате PKCS12.

**Синтаксис**

**pki import-pkcs12 password** *пароль*

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*пароль*

Пароль, который был указан при экспорте сертификата в формате PKCS12.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет импортировать сертификат субъекта, сертификат УЦ, секретный ключ субъекта, а также список отозванных сертификатов с флэш-накопителя. Поддерживается импорт сертификатов формата v3.

При выполнении команды **pki import-pkcs12 password <***пароль***>** к устройству должен быть подключен флэш-накопитель, в корне которого должен размещаться файл в формате PKCS12 (имеющий расширение p12), содержащий:

- сертификат удостоверяющего центра;
- сертификат клиента;
- список отозванных сертификатов;
- секретный ключ клиента.

Монтирование и размонтирование флэш-накопителя осуществляется автоматически. В результате выполнения указанной команды в систему будут добавлены сертификат удостоверяющего центра, сертификат клиента, подписанный указанным удостоверяющим центром, секретный ключ, а также файл, содержащий список отозванных сертификатов.

# 17. МЕЖФИЛИАЛЬНЫЙ РЕЖИМ IPSEC

В этом разделе описано, как настроить в системе Altell NEO подключение VPN в межфилиальном режиме IPSec.

В этом разделе рассматриваются следующие вопросы:

- Настройка VPN в межфилиальном режиме IPSec.
- Команды отображения состояния IPSec в межфилиальном режиме.
- Команды IPSec в межфилиальном режиме.

## 17.1. Настройка VPN в межфилиальном режиме IPSec

В данном разделе описано как настроить VPN с использованием межфилиального режима IPSec в системе Altell NEO.

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 с использованием электронной цифровой подписи на основе RSA.
- Создание подключения VPN с использованием NAT.
- Настройка туннелей IPSec между тремя шлюзами.
- Защита туннеля GRE с использованием IPSec.
- Узлы VPN, имеющие динамические IP-адреса.

### 17.1.1. 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 хэширования.
- Предварительные ключи.

- Электронные цифровые подписи.
- Группы Диффи-Хеллмана.
- Режимы IPSec.
- Полная безопасность пересылки.

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 хэширования.
- Аутентификация. Аутентификация гарантирует, что полученные данные были отправлены заявленным отправителем, а не кем-либо, выдающим себя за него. Аутентификация также обеспечивается при помощи алгоритмов хэширования.
- 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.

Altell NEO 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.

#### *17.1.1.1. 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, хэширование 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.

#### *17.1.1.2. 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 хэширование. 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.

#### *17.1.1.3. 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 хэширования.
- 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 Altell NEO, 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.

#### *17.1.1.4. Алгоритмы шифрования*

Шифрование позволяет защитить данные при их передаче по незащищенным каналам. Altell NEO поддерживает российский стандарт симметричного шифрования ГОСТ 28147-89 (**gost**). Altell NEO поддерживает следующие алгоритмы шифрования:

- des;
- 3des;
- blowfish;
- cast128;
- aes;
- camellia;
- gost.

#### *17.1.1.5. Алгоритмы хэширования*

Хэш-функция — это функция, принимающая на вход строку битов произвольной длины и выдающая результат фиксированной длины, который называется дайджестом (digest) сообщения или хэш-значением. Хэш-функции могут использоваться для аутентификации сообщений.

Altell NEO поддерживает следующие алгоритмы хэширования:

- md5;

- sha1;
- sha256;
- sha384;
- sha512;
- gosthash.

#### *17.1.1.6. 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 хэш-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 хэшируется 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 хэш-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.*

#### *17.1.1.7. 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 (хэш-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 значение 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.

#### *17.1.1.8. 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.

#### *17.1.1.9. 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.

Altell NEO 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.

#### *17.1.1.10. Режимы IPSec*

IPSec, в общем случае, поддерживает два режима функционирования: *агрессивный режим* и *основной режим*.

#### 17.1.1.10.1. Агрессивный режим

Агрессивный режим был создан для того, чтобы уменьшить задержки во время первой фазы согласования, но он является уязвимым к атакам.

#### 17.1.1.10.2. 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. Altell NEO поддерживает основной режим.

### *17.1.1.11. 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 течении 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.

## 17.1.2. 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, Altell NEO 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.

### 17.1.3. Настройка базового подключения в межфилиальном режиме

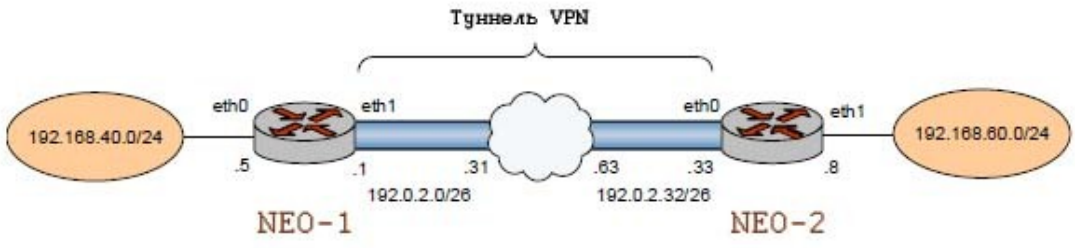
***ПРИМЕЧАНИЕ*** *Там где на практике должны быть использованы общедоступные IP-адреса, в примерах использованы IP-адреса из диапазона 192.0.2.0/24 (RFC 3330 “TEST-NET”)*

В этом разделе рассматриваются следующие вопросы:

- Настройка NEO-1.
- Настройка узла NEO-2.

В данном разделе представлены примеры настройки базового туннеля IPSec между системами Altell NEO, которые называются соответственно NEO-1 и NEO-2. Сначала настраивается узел NEO-1, затем NEO-2. После завершения настройки, узлы будут настроены как показано на рисунке 63.

*Рисунок 63 - Первичная настройка IPSec в межфилиальном режиме*




Перед началом настройки:

- В этом наборе примеров, используются две системы Altell NEO, с именами узлов NEO-1 и NEO-2. (Имена узлов из примеров указаны прописными буквами). Последний набор примеров предполагает наличие третьей системы Altell NEO с именем NEO-3.
- Все интерфейсы Ethernet используемые в IPSec VPN должны быть заранее настроены. В этом примере, используется интерфейс **eth1** на узле NEO-1 и интерфейс **eth0** на узле NEO-2.
- 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 192.0.2.1 назначен интерфейсу **eth1** узла NEO-1, и адрес 192.0.2.33 назначен интерфейсу **eth0** узла NEO-2.

***ПРИМЕЧАНИЕ*** *Отправка и получение сообщений ICMP о перенаправлении отключена при использовании IPSec VPN.*

#### *17.1.3.1. Настройка NEO-1*

В этом разделе рассматриваются следующие вопросы:

- Настройка группы IKE на узле NEO-1.
- Настройка группы ESP на узле NEO-1.
- Создание подключения к узлу NEO-2.

В данном разделе представлены следующие примеры:

- Пример 17.1 Настройка группы IKE на узле NEO-1.
- Пример 17.2 Настройка группы ESP на узле NEO-1.

- Пример 17.3 Создание подключения в межфилиальном режиме от узла NEO-1 к узлу NEO-2.

#### 17.1.3.1.1. Настройка группы IKE на узле NEO-1

Группа IKE позволяет предопределить набор из одного или более предложений, которые будут использованы 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.
- Хэш-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, хэширования 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 17.1 создается группа IKE с именем IKE-1W на узле NEO-1. Эта группа IKE включает в себя два предложения :

- В предложении 1 используется AES в качестве алгоритма шифрования и SHA-1 в качестве алгоритма хэширования.
- В предложении 2 используется DES в качестве алгоритма шифрования и SHA-1 в качестве алгоритма хэширования.

Время жизни для этой группы IKE устанавливается равным 3600 секундам. Для создания указанной группы IKE, необходимо выполнить следующие действия на узле NEO-1 в режиме настройки:

*Пример 17.1 - Настройка группы IKE на узле NEO-1*

| Действие | Команда |
|---|---|

| | |
|---|---|
| Создание узла конфигурации для предложения 1 группы IKE с именем IKE-1W. | admin@NEO-1# **set vpn ipsec ike-group IKE-1W proposal 1**<br>[edit] |
| Установка алгоритма шифрования для предложения 1. | admin@NEO-1# **set vpn ipsec ike-group IKE-1W proposal 1 encryption aes**<br>[edit] |
| Установка алгоритма хэширования для предложения 1. | admin@NEO-1# **set vpn ipsec ike-group IKE-1W proposal 1 hash sha1**<br>[edit] |
| Установка алгоритма шифрования для предложения 2. В результате выполнения данной команды также будет создан узел конфигурации для предложения 2 группы IKE с именем IKE-1W. | admin@NEO-1# **set vpn ipsec ike-group IKE-1W proposal 2 encryption des**<br>[edit] |
| Установка алгоритма хэширования для предложения 2. | admin@NEO-1# **set vpn ipsec ike-group IKE-1W proposal 2 hash sha1**<br>[edit] |
| Установка времени жизни для группы IKE. | admin@NEO-1# **set vpn ipsec ike-group IKE-1W lifetime 3600**<br>[edit] |
| Вывод настройки для группы IKE. На данном этапе настройки изменения не фиксируются. | admin@NEO-1# **show -all vpn ipsec**<br>ike-group IKE-1W<br>+lifetime 3600<br>+proposal 1 {<br>+ dh-group 2<br>+ encryption aes<br>+ hash sha1 |

```
  +}
  +proposal 2 {
  +    dh-group 2
  +    encryption des
  +    hash sha1
  +}
[edit]
```

#### 17.1.3.1.2. Настройка группы ESP на узле NEO-1

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 хэширования, который будет использоваться для аутентификации пакетов.

Altell NEO 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.
- Хэш-функция, используемая для аутентификации пакетов, передаваемых через туннель IPSec.
- Время жизни защищенного соединения IPSec SA.

В примере 17.2 создается группа ESP с именем ESP-1W на узле NEO-1. Группа ESP содержит два предложения:

- В предложении 1 используется AES в качестве алгоритма шифрования и SHA-1 в качестве алгоритма хэширования.
- В предложении 2 используется Triple-DES в качестве алгоритма шифрования и MD5 в качестве алгоритма хэширования.

Время жизни для этой группы ESP устанавливается равным 1800 секундам. Для

создания группы ESP, необходимо выполнить на узле NEO-1 следующие действия в режиме настройки:

*Пример 17.2 - Настройка группы ESP на узле NEO-1*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для предложения 1 группы ESP с именем ESP-1W | admin@NEO-1# **set vpn ipsec esp-group ESP-1W proposal 1**<br>[edit] |
| Установка алгоритма шифрования для предложения 1. | admin@NEO-1# **set vpn ipsec esp-group ESP-1W proposal 1 encryption aes**<br>[edit] |
| Установка алгоритма хэширования для предложения 1. | admin@NEO-1# **set vpn ipsec esp-group ESP-1W proposal 1 hash hmac_sha1**<br>[edit] |
| Установка алгоритма шифрования для предложения 2. В результате выполнения данной команды также будет создан узел конфигурации для предложения 2 группы ESP с именем ESP-1W. | admin@NEO-1# **set vpn ipsec esp-group ESP-1W proposal 2 encryption 3des**<br>[edit] |
| Установка алгоритма хэширования для предложения 2. | admin@NEO-1# **set vpn ipsec esp-group ESP-1W proposal 2 hash hmac_md5**<br>[edit] |
| Установка времени жизни для группы ESP. | admin@NEO-1# **set vpn ipsec esp-group ESP-1W lifetime 1800**<br>[edit] |
| Вывод настройки для группы ESP. На | admin@NEO-1# **show -all vpn ipsec** |

данном этапе настройки изменения не фиксируются.

```
esp-group ESP-1W
 +compression disable
  +lifetime 1800
  +mode tunnel
  +proposal 1 {
  +    encryption aes
  +    hash hmac_sha1
  +}
  +proposal 2 {
  +    encryption 3des
  +    hash hmac_md5
  +}
[edit]
```

#### 17.1.3.1.3. Создание подключения к узлу NEO-2

При определении подключения в межфилиальном режиме, указываются сведения политики IPSec (большинство из который уже настроены в группах IKE и ESP) и информация, необходимая для маршрутизации для двух оконечных устройств туннеля IPSec.

Локальная оконечная точка - Altell NEO. Удаленная оконечная точка - шлюз VPN, в качестве которого может быть использована другая система Altell NEO, 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 хэшированного ключа.
- Группа IKE, которая будет использоваться для данного подключения.
- Группа ESP, которая будет использоваться для данного подключения.

- IP-адрес данной системы Altell NEO, 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 хэш-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 хэшируется 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 17.3 определяется подключение в межфилиальном режиме к узлу NEO-2.

Для этого используется туннель, обеспечивающий взаимодействие между подсетью 192.168.40.0/24 на узле NEO-1 и подсетью 192.168.60.0/24 на узле NEO-2, с использование группы ESP с именем ESP-1W.

Используемые параметры:

- На узле NEO-1 интерфейсу eth1 назначен IP-адрес 192.0.2.1.
- На узле NEO-2 интерфейсу eth0 назначен IP-адрес 192.0.2.33.
- Используется группа IKE с именем IKE-1W
- Для аутентификации используются предварительные ключи. В качестве предварительного ключа используется строка “test_key_1”.

Для настройки указанного подключения необходимо выполнить на узле NEO-1 следующие действия в режиме настройки:

*Пример 17.3 - Создание подключения в межфилиальном режиме от узла NEO-1 к узлу NEO-2*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для туннеля к узлу NEO-2 и указание режима аутентификации. | admin@NEO-1# **set vpn ipsec site-to-site peer tunnel1 authentication method pre-shared-key**<br>[edit] |
| Переход к другому узлу конфигурации для более удобного редактирования. | admin@NEO-1# **edit vpn ipsec site-to-site peer tunnel1**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Ввод строки, которая будет использоваться в качестве | admin@NEO-1# **set authentication pre-shared-key test_key_1** |

| Действие | Команда |
|---|---|
| предварительного ключа. | [edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание группы IKE. | admin@NEO-1# **set ike-group IKE-1W**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание IP-адреса данной системы Altell NEO, который будет использоваться для данного туннеля. | admin@NEO-1# **set local-ip 192.0.2.1**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание IP-адреса удаленного узла VPN, который будет использоваться для данного туннеля. | admin@NEO-1# **set remote-ip 192.0.2.33**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание локальной подсети для данного туннеля. | admin@NEO-1# **set local-subnet 192.168.40.0/24**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание удаленной подсети для данного туннеля. | admin@NEO-1# **set remote-subnet 192.168.60.0/24**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание группы ESP для данного туннеля. | admin@NEO-1# **set esp-group ESP-1W**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Возврат к вершине дерева настройки. | admin@NEO-1# **top**<br>[edit] |
| Фиксация настройки. | admin@NEO-1# **commit** |

| Действие | Команда |
|---|---|
| | `[edit]` |
| Вывод настройки для подключения IPSec в межфилиальном режиме. | `admin@NEO-1# show -all vpn ipsec site-to-site peer tunnel1`<br>`authentication {`<br>`method pre-shared-key`<br>`pre-shared-key test_key_1`<br>`}`<br>`esp-group ESP-1W`<br>`ike-group IKE-1W`<br>`local-ip 192.0.2.1`<br>`local-subnet 192.168.40.0/24`<br>`nat-traversal off`<br>`remote-ip 192.0.2.33`<br>`remote-subnet 192.168.60.0/24`<br>`[edit]` |

#### 17.1.3.1.4. Определение статического маршрута на узле NEO-1

В примере 17.4 создается статический маршрут для трафика, предназначенного удаленному оконечному узлу туннеля.

Отправка трафика, предназначенного для подсети 192.168.60.0/24, к удаленной оконечной точке туннеля — 192.0.2.33. Для создания статического маршрута необходимо выполнить на узле NEO-1 следующие действия в режиме настройки:

*Пример 17.4 - Определение статического маршрута на узле NEO-1*

| Действие | Команда |
|---|---|
| Создание статического маршрута. | `admin@NEO-1# set protocols static route 192.168.60.0/24 next-hop 192.0.2.33`<br>`[edit]` |

| Действие | Команда |
|---|---|
| Фиксация настройки. | admin@NEO-1# **commit**<br>[edit] |
| Вывод настройки. | admin@NEO-1# **show protocols**<br>**static** route192.168.60.0/24 {<br>next-hop 192.0.2.33<br>}<br>[edit] |

#### *17.1.3.2. Настройка узла NEO-2*

В этом разделе рассматриваются следующие вопросы:

- Включение VPN на узле NEO-2.
- Настройка группы IKE на узле NEO-2.
- Настройка группы ESP на узле NEO-2.
- Создание подключения к узлу NEO-1.

В данном разделе приведены следующие примеры:

- Пример 17.5 Настройка группы IKE на узле NEO-2.
- Пример 17.6 Настройка группы ESP на узле NEO-2.
- Пример 17.7 Создание подключения в межфилиальном режиме от узла NEO-2 к узлу NEO-1.

##### 17.1.3.2.1. Настройка группы IKE на узле NEO-2

В примере 17.5 создается группа IKE с именем IKE-1E на узле NEO-2. Группа IKE содержит два предложения:

- В предложении 1 используется AES в качестве алгоритма шифрования и SHA-1 в качестве алгоритма хэширования.
- В предложении 2 используется DES в качестве алгоритма шифрования и SHA-1 в качестве алгоритма хэширования.

Время жизни для этой группы IKE устанавливается равным 3600 секундам.

Следует учесть, что указанные параметры соответствуют параметрам, установленным в группе IKE-1W на узле NEO-1. Необходимо убедиться при определении предложений, что

указаны такие алгоритмы шифрования и хэширования, что два узла смогут согласовать хотя бы одну комбинацию параметров.

Для создания указанной группы IKE, необходимо выполнить на узле NEO-2 следующие действия в режиме настройки:

*Пример 17.5 - Настройка группы IKE на узле NEO-2*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для предложения 1 группы IKE с именем IKE-1E. | admin@NEO-2# **set vpn ipsec ike-group IKE-1E proposal 1**<br>[edit] |
| Установка алгоритма шифрования для предложения 1. | admin@NEO-2# **set vpn ipsec ike-group IKE-1E proposal 1 encryption aes**<br>[edit] |
| Установка алгоритма хэширования для предложения 1. | admin@NEO-2# **set vpn ipsec ike-group IKE-1E proposal 1 hash sha1**<br>[edit] |
| Установка алгоритма шифрования для предложения 2. В результате выполнения данной команды также будет создан узел конфигурации для предложения 2 группы IKE с именем IKE-1E. | admin@NEO-2# **set vpn ipsec ike-group IKE-1E proposal 2 encryption des**<br>[edit] |
| Установка алгоритма хэширования для предложения 2. | admin@NEO-2# **set vpn ipsec ike-group IKE-1E proposal 2 hash sha1**<br>[edit] |
| Установка времени жизни для группы IKE. | admin@NEO-2# **set vpn ipsec ike-group IKE-1E lifetime 3600**<br>[edit] |
| Вывод настройки для группы IKE. На | admin@NEO-2# **show -all vpn ipsec** |

| Действие | Команда |
|---|---|
| данном этапе настройки изменения не фиксируются. | ike-group IKE-1E<br>+lifetime 3600<br>+proposal 1 {<br>+ dh-group 2<br>+ encryption aes<br>+ hash sha1<br>+}<br>+proposal 2 {<br>+ dh-group 2<br>+ encryption des<br>+ hash sha1<br>+}<br>[edit] |

#### 17.1.3.2.2. Настройка группы ESP на узле NEO-2

В примере 17.6 создается группа ESP с именем ESP-1E на узле NEO-2. Группа ESP содержит два предложения:

- В предложении 1 используется AES в качестве алгоритма шифрования и SHA-1 в качестве алгоритма хэширования.
- В предложении 2 используется Triple-DES в качестве алгоритма шифрования и MD5 в качестве алгоритма хэширования.
- Время жизни для этой группы ESP устанавливается равным 1800 секундам. Для создания указанной группы ESP необходимо выполнить следующие действия на узле NEO-2 в режиме настройки:

*Пример 17.6 - Настройка группы ESP на узле NEO-2*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для предложения 1 группы ESP с именем ESP-1E. | admin@NEO-2# **set vpn ipsec esp-group ESP-1E proposal 1**<br>[edit] |

| Действие | Команда |
|---|---|
| Установка алгоритма шифрования для предложения 1. | admin@NEO-2# **set vpn ipsec esp-group ESP-1E proposal 1 encryption aes**<br>[edit] |
| Установка алгоритма хэширования для предложения 1. | admin@NEO-2# **set vpn ipsec esp-group ESP-1E proposal 1 hash hmac_sha1**<br>[edit] |
| Установка алгоритма шифрования для предложения 2. В результате выполнения данной команды также будет создан узел конфигурации для предложения 2 группы ESP с именем ESP-1E. | admin@NEO-2# **set vpn ipsec esp-group ESP-1E proposal 2 encryption 3des**<br>[edit] |
| Установка алгоритма хэширования для предложения 2. | admin@NEO-2# **set vpn ipsec esp-group ESP-1E proposal 2 hash hmac_md5**<br>[edit] |
| Установка времени жизни для группы ESP. | admin@NEO-2# **set vpn ipsec esp-group ESP-1E lifetime 1800**<br>[edit] |
| Вывод настройки для группы ESP. На данном этапе настройки изменения не фиксируются. | admin@NEO-2# **show -all vpn ipsec esp-group ESP-1E**<br>+compression disable<br>+lifetime 1800<br>+mode tunnel<br>+proposal 1 {<br>+ encryption aes |

| Действие | Команда |
|---|---|
| | +  hash hmac_sha1<br>+}<br>+proposal 2 {<br>+  encryption 3des<br>+  hash hmac_md5<br>+}<br>[edit] |

#### 17.1.3.2.3. Создание подключения к узлу NEO-1

В примере 17.7 определяется подключение в межфилиальном режиме к узлу NEO-1. В этом примере:

- Для этого используется туннель, обеспечивающий взаимодействие между подсетью 192.168.60.0/24 на узле NEO-2 и подсетью 192.168.40.0/24 на узле NEO-1, с использованием группы ESP с именем ESP-1E.
- На узле NEO-2 интерфейсу eth0 назначен IP-адрес 192.0.2.33.
- На узле NEO-1 интерфейсу eth1 назначен IP-адрес 192.0.2.1.
- Используется группа IKE с именем IKE-1E.
- Для аутентификации используются предварительные ключи. В качестве предварительного ключа используется строка “test_key_1”.

Для настройки этого подключения необходимо выполнить следующие действия на узле NEO-2 в режиме настройки:

*Пример 17.7 - Создание подключения в межфилиальном режиме от узла NEO-2 к узлу NEO-1*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для туннеля к узлу NEO-1 и указание режима аутентификации. | admin@NEO-2# **set vpn ipsec site-to-site peer tunnel1 authentication method pre-shared-key**<br>[edit] |
| Переход к другому узлу конфигурации | admin@NEO-2# **edit vpn ipsec site-** |

| Действие | Команда |
|---|---|
| | **to-site peer tunnel1** |
| для удобства редактирования. | [edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Ввод строки, которая будет использоваться в качестве предварительного ключа. | admin@NEO-2# **set authentication pre-shared-key test_key_1** [edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание группы IKE. | admin@NEO-2# **set ike-group IKE-1E** [edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание IP-адреса данной системы Altell NEO, который будет использоваться для данного подключения. | admin@NEO-2# **set local-ip 192.0.2.33** [edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание локальной подсети для данного туннеля. | admin@NEO-2# **set local-subnet 192.168.60.0/24** [edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание IP-адреса удаленного узла VPN, который будет использоваться для данного подключения. | admin@NEO-2# **set remote-ip 192.0.2.1** [edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание удаленной подсети для данного туннеля. | admin@NEO-2# **set remote-subnet 192.168.40.0/24** [edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание группы ESP для данного туннеля. | admin@NEO-2# **set esp-group ESP-1E** [edit vpn/ipsec/site-to- |

| Действие | Команда |
|---|---|
| | site/peer/tunnel1] |
| Возврат к вершине дерева настройки. | admin@NEO-2# **top**<br>[edit] |
| Фиксация настройки. | admin@NEO-2# **commit**<br>[edit] |
| Вывод настройки для подключения IPSec в межфилиальном режиме. | admin@NEO-2# **show -all vpn ipsec site-to-site peer tunnel1**<br>authentication {<br>method pre-shared-key<br>pre-shared-key test_key_1<br>}<br>esp-group ESP-1E<br>ike-group IKE-1E<br>local-ip 192.0.2.33<br>local-subnet 192.168.60.0/24<br>nat-traversal off<br>remote-ip 192.0.2.1<br>remote-subnet 192.168.40.0/24<br>[edit] |

#### 17.1.3.2.4. Определение статического маршрута на узле NEO-2

В примере 17.8 создается статический маршрут для трафика, предназначенного удаленному оконечному узлу туннеля.

Отправить трафик, предназначенный для подсети 192.168.40.0/24 к удаленной оконечной точке туннеля - 192.0.2.1.

Для создания статического маршрута необходимо выполнить следующие действия на узле NEO-2 в режиме настройки:

*Пример 17.8 - Определение статического маршрута на узле NEO-2*

| Действие | Команда |
|---|---|
| Создание статического маршрута | admin@NEO-2# **set protocols static route 192.168.40.0/24 next-hop 192.0.2.1**<br>[edit] |
| Фиксация настройки. | admin@NEO-2# **commit**<br>[edit] |
| Вывод настройки. | admin@NEO-2# **show protocols static**<br>route 192.168.40.0/24 {<br>  next-hop 192.0.2.1<br>}<br>[edit] |

### 17.1.4. Аутентификация на основе схемы ЭЦП на базе RSA

В этом разделе рассматриваются следующие вопросы:

- Генерация ключевой пары RSA на узле NEO-1.
- Генерация ключевой пары RSA на узле NEO-2.
- Доставка открытого ключа узла NEO-2 на узел NEO-1.
- Изменение настроек подключения к узлу NEO-2 на узле NEO-1.
- Доставка открытого ключа узла NEO-1 на узел NEO-2.
- Изменение настроек подключения к узлу NEO-1 на узле NEO-2.

В этом наборе примеров изменяются параметры подключения VPN, настроенного в предыдущем наборе примеров (17.1.3. Настройка базового подключения в межфилиальном режиме см. стр. 1099). 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.

#### *17.1.4.1. Генерация ключевой пары RSA на узле NEO-1*

В данном примере приведена генерация ключевой пары узла NEO-1, которая будет использована для аутентификации на базе криптосистемы RSA. Ключевая пара состоит из открытого ключа и закрытого ключа. Открытый ключ должен быть доставлен узлу NEO-2; закрытый ключ должен храниться в секрете.

Для генерации ключевой пары RSA необходимо выполнить следующие шаги на узле NEO-1 в эксплуатационном режиме.

*Пример 17.9 - Создание ключевой пары RSA на узле NEO-1*

| Действие | Команда |
|---|---|
| Генерация ключевой пары. | `admin@NEO-1$ **vpn rsa-key generate**` |
| Система выдает предупреждение о том, что существующая ключевая пара RSA будет перезаписана. Для отмены генерации следует нажать <Ctrl>+c. | `A local RSA key file already exists and will be overwritten <CTRL>C to exit: 8` |
| Система выводит расположение файла, в который будет записана ключевая пара. | `Generating rsa-key to /opt/vyatta/etc/config/ipsec.d/rsa-keys/localhost.key` |
| Также на экран выводится открытый ключ. По умолчанию ключевая пара (открытый и секретный ключ) хранится в файле /opt/vyatta/etc/config/ipsec.d/rsa-keys/localhost.key | `Your new local RSA key has been generated. The public portion of the key is: 0sAQPEOQvukvkv1ofuO8gEKp7IFFZz4lQ qMZyVMInoQKUU/T0iKSK/0NSH9Ldrr8yQ UFayzKag6wM7ASXWXKyt0LS1Gn8tJVsjK GaOkFgLREtVJD3pRzoc7DSUOBViCD6f/T loTkPepRUtW1bmYev2H7tajSO0K0 rqu+7nlocZI0ppMAyF6CS+Wd5W1JBpVGL +EkKfyEl9RagKxRW82XJbgY4LG77K2YDN 90Wd2GgMY3kf+YJLIzFEt/xRbh2/380FM pdaUYcbY31o/5PedUutJCK5RMwl+IJGax` |

| Действие | Команда |
|---|---|
| | rKf1OmCQfzXlkM09ijZx8kzPIlBk<br>5hulZrbUWjzBJdFcwFAyPM3yCuv3+ndFX<br>00t3ZLfKu+/wX595J<br>admin@NEO-1> |

#### *17.1.4.2. Генерация ключевой пары RSA на узле NEO-2*

В данном примере приведена генерация ключевой пары RSA узла NEO-2. Ключевая пара состоит из открытого ключа и закрытого (секретного) ключа. Открытый ключ должен быть доставлен узлу NEO-1; закрытый ключ должен сохраняться в секрете.

Для генерации ключевой пары RSA для узла NEO-2, необходимо выполнить следующие шаги в эксплуатационном режиме.

*Пример 17.10 - Генерация ключевой пары на узле NEO-2*

| Действие | Команда |
|---|---|
| Генерация ключевой пары. | admin@NEO-2$ **vpn rsa-key generate** |
| Система выдает предупреждение о том, что существующая ключевая пара RSA будет перезаписана. Для отмены генерации следует нажать <Ctrl>+c. | A local RSA key file already exists and will be overwritten<br><CTRL>C to exit: 5 |
| Система выводит расположение файла, в который будет записана ключевая пара. | Generating rsa-key to /opt/vyatta/etc/config/ipsec.d/rsa-keys/localhost.key |
| Также на экран выводится открытый ключ. По умолчанию ключевая пара (открытый и секретный ключ) хранится в файле /opt/vyatta/etc/config/ipsec.d/rsa-keys/localhost.key | Your new local RSA key has been generatedThe public portion of the key is:<br>0sAQOVBIJL+rIkpTuwh8FPeceAF0bhgLr+<br>+W51bOAIjFbRDbR8gX3Vlz6wiUbMgGwQx<br>WlYQiqsCeacicsfZx/amlEn9PkSE4e7tq |

| Действие | Команда |
| --- | --- |
| | K/JQo40L5C7gcNM24mup1d+0WmN3zLb9Q<br>hmq5q3pNJxEwnVbPPQeIdZMJxnb1+lA8D<br>PC3SIxJM/3at1/KrwqCAhX3QNFY/zNmOt<br>FogELCeyl4+d54wQljA+3dwFAQ4bboJ7Y<br>IDs+rqORxWd3l3I7IajT/pLrwr5eZ8OA9<br>NtAedbMiCwxyuyUbznxXZ8Z/MAi3xjL1p<br>jYyWjNNiOij82QJfMOrjoXVCfcPn96ZN+<br>Jqk+KknoVeNDwzpoahFOseJREeXzkw3/l<br>kMN9N1 |

### *17.1.4.3. Доставка открытого ключа узла NEO-2 на узел NEO-1*

Для осуществления проверки подлинности узлу NEO-1 должен быть известен открытый ключ узла NEO-2.

В данном примере производится запись открытого ключа, полученного от узла NEO-2, на узле NEO-1. Ключ на узле NEO-1 должен быть сохранен под именем, которое в последствии необходимо указать в настройке подключения.

Открытый ключ можно ввести вручную, но сделать это довольно проблематично, так как для обеспечения требуемой стойкости используются ключи большого размера. Гораздо легче скопировать открытый ключ в буфер обмена и затем вставить его из буфера обмена при внесении изменений в настройку. Это можно сделать несколькими способами; например:

- Скопировать открытый ключ из сертификата X.509, подписанного доверенным удостоверяющим центром.
- Подключиться к узлу VPN напрямую по протоколу SSH. Вывести открытый ключ с помощью команды **show vpn ike rsa-keys**, выделить текст, и скопировать текстовое значение ключа в буфер обмена.

В примере 17.11 приведено добавление открытого ключа узла NEO-2 в настройку RSA на узле NEO-1. Имя “NEO-2 -key” используется в качестве идентификатора ключа.

Первоначально необходимо скопировать открытый ключ узла NEO-2 в буфер обмена.

Если на узле NEO-1 включен эксплуатационный режим, следует перейти в режим настройки и выполнить следующие действия:

*Пример 17.11 - Запись открытого ключа узла NEO-2 на узле NEO-1*

| Действие | Команда |
|---|---|
| Указание имени для открытого ключа узла NEO-2 и вставка открытого ключа узла NEO-2 из буфера обмена в настройку на узле NEO-1. | admin@NEO-1# **set vpn rsa-keys rsa-key-name NEO-2-key rsa-key** 0sAQOVBIJL+rIkpTuwh8FPeceAF0bhgLr+ +W51bOAIjFbRDbR8gX3Vlz6wiUbMgGwQx WlYQiqsCeacicsfZx/amlEn9PkSE4e7tq K/JQo40L5C7gcNM24mup1d+0WmN3zLb9Q hmq5q3pNJxEwnVbPPQeIdZMJxnb1+lA8D PC3SIxJM/3at1/KrwqCAhX3QNFY/zNmOt FogELCeyl4+d54wQljA+3dwFAQ4bboJ7Y IDs+rqORxWd3l3I7IajT/pLrwr5eZ8OA9 NtAedbMiCwxyuyUbznxXZ8Z/MAi3xjL1p jYyWjNNiOij82QJfMOrjoXVCfcPn96ZN+ Jqk+KknoVeNDwzpoahFOseJREeXzkw3/l kMN9N1[edit] |
| Фиксация настройки. | admin@NEO-1# **commit** [edit] |
| Отображение настройки ключей RSA. Если настройка локального ключа не была изменена, она не будет выведена на экран. | admin@NEO-1# **show vpn rsa-keys rsa-key-name NEO-2-key** { rsa-key 0sAQOVBIJL+rIkpTuwh8FPeceAF0bhgLr+ +W51bOAIjFbRDbR8gX3Vlz6wiUbMgGwQx WlYQiqsCeacicsfZx/amlEn9PkSE4e7tq K/JQo40L5C7gcNM24mup1d+0WmN3zLb9Q hmq5q3pNJxEwnVbPPQeIdZMJxnb1+lA8D |

| Действие | Команда |
|---|---|
| | PC3SIxJM/3at1/KrwqCAhX3QNFY/zNmOt<br>FogELCeyl4+d54wQljA+3dwFAQ4bboJ7Y<br>IDs+rqORxWd3l3I7IajT/pLrwr5eZ8OA9<br>NtAedbMiCwxyuyUbznxXZ8Z/MAi3xjL1p<br>jYyWjNNiOij82QJfMOrjoXVCfcPn96ZN+<br>Jqk+KknoVeNDwzpoahFOseJREeXzkw3/l<br>kMN9N1 }<br>[edit] |

### *17.1.4.4. Изменение настроек подключения к узлу NEO-2 на узле NEO-1*

В примере 17.12 изменяются параметры подключения от узла NEO-1 к узлу NEO-2, таким образом, чтобы использовалась аутентификация на базе RSA. В этом примере:

- Установленный режим аутентификации с использованием предварительных ключей заменяется на аутентификацию на базе RSA.
- Открытый ключ узла NEO-2 указывается в качестве удаленного ключа под именем, созданным на предыдущем шаге (17.1.4.3. Доставка открытого ключа узла NEO-2 на узел NEO-1 см. стр. 1120).

Для изменения настройки аутентификации на использование криптосистемы RSA необходимо выполнить следующие шаги:

*Пример 17.12 - Настройка узла NEO-1 на использование аутентификации на базе криптосистемы RSA*

| Действие | Команда |
|---|---|
| Изменение режима аутентификации. | admin@NEO-1# **set vpn ipsec site-to-site peer tunnel1 authentication method plain-rsa**<br>[edit] |
| Указание идентификатора открытого ключа узла NEO-2. | admin@NEO-1# **set vpn ipsec site-to-site peer tunnel1** |

| Действие | Команда |
|---|---|
| | **authentication rsa-key-name NEO-2-key** |
| Фиксация настройки. | admin@NEO-1# **commit**<br>[edit] |
| Вывод измененной настройки. | admin@NEO-1# **show -all vpn ipsec site-to-site peer tunnel1**<br>authentication {<br>method plain-rsa<br>rsa-key-name NEO-2-key<br>}<br>esp-group ESP-1W<br>ike-group IKE-1W<br>local-ip 192.0.2.1<br>local-subnet 192.168.40.0/24<br>nat-traversal off<br>remote-ip 192.0.2.33<br>remote-subnet 192.168.60.0/24<br>[edit] |

#### *17.1.4.5. Доставка открытого ключа узла NEO-1 на узел NEO-2*

В примере 17.13 приведена вставка открытого ключа узла NEO-1 в настройку RSA. Имя “NEO-1 -key” используется в качестве идентификатора ключа.

Первоначально необходимо скопировать открытый ключ NEO-1 в буфер обмена. Если на узле NEO-2 используется эксплуатационный режим, следует перейти в режим настройки и выполнить следующие шаги:

*Пример 17.13 - Запись открытого ключа узла NEO-1 на узле NEO-2*

| Действие | Команда |
|---|---|
| Указание имени открытого ключа узла | admin@NEO-2# **set vpn rsa-keys** |

| Действие | Команда |
| --- | --- |
| NEO-1 и вставка открытого ключа узла NEO-1 из буфера обмена в настройку на узле NEO-2. | **rsa-key-name NEO-1-key rsa-key**<br>0sAQPEOQvukvkv1ofuO8gEKp7IFFZz4lQ<br>qMZyVMInoQKUU/T0iKSK/0NSH9Ldrr8yQ<br>UFayzKag6wM7ASXWXKyt0LS1Gn8tJVsjK<br>GaOkFgLREtVJD3pRzoc7DSUOBViCD6f/T<br>loTkPepRUtW1bmYev2H7tajSO0K0<br>rqu+7nlocZI0ppMAyF6CS+Wd5W1JBpVGL<br>+EkKfyEl9RagKxRW82XJbgY4LG77K2YDN<br>90Wd2GgMY3kf+YJLIzFEt/xRbh2/380FM<br>pdaUYcbY31o/5PedUutJCK5RMwl+IJGax<br>rKf1OmCQfzXlkM09ijZx8kzPIlBk<br>5hulZrbUWjzBJdFcwFAyPM3yCuv3+ndFX<br>00t3ZLfKu+/wX595J<br>[edit] |
| Фиксация настройки. | admin@NEO-2# **commit**<br>[edit] |
| Отображение настройки ключей RSA. Если настройка локального ключа не была изменена, она не будет выведена на экран. | admin@NEO-2# **show vpn rsa-keys rsa-key-name NEO-1-key**<br>{ rsa-key<br>0sAQPEOQvukvkv1ofuO8gEKp7IFFZz4lQ<br>qMZyVMInoQKUU/T0iKSK/0NSH9Ldrr8yQ<br>UFayzKag6wM7ASXWXKyt0LS1Gn8tJVsjK<br>GaOkFgLREtVJD3pRzoc7DSUOBViCD6f/T<br>loTkPepRUtW1bmYev2H7tajSO0K0<br>rqu+7nlocZI0ppMAyF6CS+Wd5W1JBpVGL<br>+EkKfyEl9RagKxRW82XJbgY4LG77K2YDN<br>90Wd2GgMY3kf+YJLIzFEt/xRbh2/380FM<br>pdaUYcbY31o/5PedUutJCK5RMwl+IJGax<br>rKf1OmCQfzXlkM09ijZx8kzPIlBk<br>5hulZrbUWjzBJdFcwFAyPM3yCuv3+ndFX |

| Действие | Команда |
|---|---|
| | 00t3ZLfKu+/wX595J<br>}<br>[edit] |

#### *17.1.4.6. Изменение настроек подключения к узлу NEO-1 на узле NEO-2*

В примере 17.14 изменяются параметры подключения от узла NEO-2 к узлу NEO-1 таким образом, чтобы для аутентификации использовалась криптосистема RSA.

В этом примере:

- Ранее установленный режим аутентификации с использованием предварительных ключей заменяется на аутентификацию на основе криптосистемы RSA.
- Открытый ключ узла NEO-1 указывается как удаленный ключ под идентификатором, настроенным на предыдущем шаге (17.1.4.3. Доставка открытого ключа узла NEO-2 на узел NEO-1 см. стр. 1120).

Для изменения настройки аутентификации на использование RSA необходимо выполнить следующие шаги:

*Пример 17.14 - Настройка узла NEO-2 для аутентификации с использованием RSA*

| Действие | Команда |
|---|---|
| Изменение режима аутентификации. | admin@NEO-2# **set vpn ipsec site-to-site peer tunnel1 authentication method plain-rsa**<br>[edit] |
| Указание идентификатора открытого ключа узла NEO-1. | admin@NEO-2# **set vpn ipsec site-to-site peer tunnel1 authentication rsa-key-name NEO-1-key** |
| Фиксация настройки. | admin@NEO-2# **commit**<br>[edit] |
| Отображение измененной настройки для | admin@NEO-2# **show -all vpn ipsec** |

| Действие | Команда |
| --- | --- |
| подключения в межфилиальном режиме. | **site-to-site peer tunnel1**<br>authentication {<br>method plain-rsa<br>rsa-key-name NEO-1-key<br>}<br>esp-group ESP-1E<br>ike-group IKE-1E<br>local-ip 192.0.2.33<br>local-subnet 192.168.60.0/24<br>nat-traversal off<br>remote-ip 192.0.2.1<br>remote-subnet 192.168.40.0/24<br>[edit] |

### 17.1.5. Аутентификация на базе PKI

В этом разделе рассматриваются следующие вопросы:

- Создание удостоверяющего центра.
- Генерация сертификата узла NEO-1.
- Генерация сертификата узла NEO-2.
- Доставка сертификата на узел NEO-2.
- Изменение настроек подключения к узлу NEO-2 на узле NEO-1.
- Изменение настроек подключения к узлу NEO-1 на узле NEO-2.

В этом наборе примеров изменяются параметры подключения VPN, настроенного в наборе примеров, приведенном в разделе 17.1.3. 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.

#### *17.1.5.1. 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 NEO-1.

На базе созданного удостоверяющего центра будет осуществляться централизованное создание и управление ключевыми парами и сертификатами узлов NEO-1 и NEO-2.

Для создания нового удостоверяющего центра необходимо выполнить следующие шаги на узле NEO-1 в режиме настройки.

*Пример 17.15 - Создание удостоверяющего центра на узле NEO-1*

| Действие | Команда |
|---|---|
| Создание удостоверяющего центра. | admin@NEO-1# **set pki ca MainCA**<br>[edit] |
| Указание общего имени (common name) удостоверяющего центра. | admin@NEO-1# **set pki ca MainCA cn "Main Certification Authority"**<br>[edit] |
| Указание города, в качестве одного из атрибутов идентификатора УЦ. | admin@NEO-1# **set pki ca MainCA city SPb**<br>[edit] |
| Указание страны, в качестве одного из атрибутов идентификатора УЦ. | admin@NEO-1# **set pki ca MainCA country RU**<br>[edit] |
| Указание периода действия сертификата удостоверяющего центра. | admin@NEO-1# **set pki ca MainCA** expiration 365<br>[edit] |
| Фиксация настройки. | admin@NEO-1# **commit**<br>[edit] |
| Вывод настройки. | admin@NEO-1# **show -all pki ca** |

| Действие | Команда |
|---|---|
| | MainCA<br>city SPb<br>cn "Main Certification Authority"<br>country RU<br>expiration 365<br>key-type gost2001<br>[edit] |

#### *17.1.5.2. Генерация сертификата узла NEO-1*

В данном примере будет приведено создание сертификата узла NEO-1, который будет использован при аутентификации узлов VPN на базе инфраструктуры открытых ключей.

Для создания сертификата узла NEO-1 необходимо выполнить следующие шаги на узле NEO-1 в режиме настройки.

*Пример 17.16 - Создание сертификата узла NEO-1*

| Действие | Команда |
|---|---|
| Создание сертификата для узла NEO-1. | admin@NEO-1# **set pki ca MainCA certificate NEO-1-cert**<br>[edit] |
| Указание общего имени (common name), которое будет указано в сертификате узла NEO-1. | admin@NEO-1# **set pki ca MainCA certificate NEO-1-cert cn "NEO-1 VPN Peer certificate"**<br>[edit] |
| Фиксация настройки. | admin@NEO-1# **commit**<br>[edit] |
| Вывод настройки созданного сертификата. | admin@NEO-1# **show -all pki ca MainCA certificate NEO-1-cert**<br>cn "NEO-1 VPN Peer |

| Действие | Команда |
|---|---|
| | certificate"<br>expiration 365<br>[edit] |

#### *17.1.5.3. Генерация сертификата узла NEO-2*

В данном примере будет приведено создание сертификата узла NEO-2, который будет использован при аутентификации узлов VPN на базе инфраструктуры открытых ключей.

Для создания сертификата узла NEO-2 необходимо выполнить следующие шаги на узле NEO-1 в режиме настройки.

*Пример 17.17 - Создание сертификата узла NEO-2*

| Действие | Команда |
|---|---|
| Создание сертификата для узла NEO-2. | admin@NEO-1# **set pki ca MainCA certificate NEO-2-cert**<br>[edit] |
| Указание общего имени (common name), которое будет указано в сертификате узла NEO-2. | admin@NEO-1# **set pki ca MainCA certificate NEO-2-cert cn "NEO-2 VPN Peer certificate"**<br>[edit] |
| Фиксация настройки. | admin@NEO-1# **commit**<br>[edit] |
| Вывод настройки. | admin@NEO-1# **show -all pki ca MainCA certificate**<br>NEO-2-cert {<br>cn "NEO-2 VPN Peer certificate"<br>expiration 365<br>}<br>NEO-1-cert { |

| Действие | Команда |
|---|---|
| | cn "NEO-1 VPN Peer certificate"<br>expiration 365<br>}<br>[edit] |

### *17.1.5.4. Экспорт сертификата узла NEO-2*

В данном примере приведен экспорт сертификата узла NEO-2 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 NEO-2 на флэш-накопитель необходимо выполнить следующие шаги на узле NEO-1 в эксплуатационном режиме, к устройству должен быть заранее подключен флэш-накопитель.

*Пример 17.18 - Экспортирование сертификата узла NEO-2*

| Действие | Команда |
|---|---|
| Экспортирование сертификата узла NEO-2, секретного ключа узла NEO-2, сертификата удостоверяющего центра. | admin@NEO-1:~$ **pki export certificate NEO-2-cert** |

После осуществления экспорта в корневой директории флэш-накопителя будут содержаться следующие файлы:

- cacert-MainCA.pem: сертификат удостоверяющего центра;
- cert-MainCA-NEO-2-cert.pem: сертификат узла NEO-2;
- crl-MainCA.pem: список отозванных сертификатов;
- pkey-MainCA-NEO-2-cert.pem: секретный ключ узла NEO-2.

#### *17.1.5.5. Импорт сертификата узла NEO-2*

В данном примере приведен импорт сертификата узла NEO-2 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 NEO-2;
- список отозванных сертификатов;
- секретный ключ узла NEO-2.

Монтирование и размонтирование флэш-накопителя осуществляется автоматически. В результате выполнения указанной команды в систему на узле NEO-2 будут добавлены сертификат удостоверяющего центра, сертификат узла NEO-2, подписанный указанным удостоверяющим центром, секретный ключ, а также файл, содержащий список аннулированных сертификатов.

Для импорта сертификата узла NEO-2 необходимо выполнить следующие шаги на узле NEO-2 в эксплуатационном режиме, к устройству должен быть заранее подключен флэш-накопитель.

*Пример 17.19 - Импорт сертификата узла NEO-2*

| Действие | Команда |
|---|---|
| Импорт сертификата узла NEO-2, секретного ключа узла NEO-2, сертификата удостоверяющего центра, списка отозванных сертификатов. | admin@NEO-2:~$ **pki import**<br>Импортируется CA: Main Certification Authority<br>Импортируется CRL для Main_Certification_Authority<br>Импортируется сертификат: NEO-2 VPN Peer certificate |

### *17.1.5.6. Изменение настроек подключения к узлу NEO-2 на узле NEO-1*

В примере 17.20 изменяются параметры подключения от узла NEO-1 к узлу NEO-2, 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 NEO-1, созданный на предыдущем шаге (см. Генерация сертификата узла NEO-1 на стр. 1128).

Для изменения настройки аутентификации на использование инфраструктуры открытых ключей на базе X.509 необходимо выполнить следующие шаги в режиме настройки на узле NEO-1:

*Пример 17.20 - Настройка узла NEO-1 на использование аутентификации на базе инфраструктуры открытых ключей*

| Действие | Команда |
|---|---|
| Изменение режима аутентификации. | admin@NEO-1# **set vpn ipsec site-to-site peer tunnel1 authentication method x509**<br>[edit] |
| Указание используемого сертификата узла NEO-1. | admin@NEO-1# **set vpn ipsec site-to-site peer tunnel1 authentication x509-cert NEO-1-cert**<br>[edit] |
| Фиксация настройки. | admin@NEO-1# **commit**<br>[edit] |
| Отображение измененной настройки подключения в межфилиальном режиме. | admin@NEO-1# **show -all vpn ipsec site-to-site peer**<br>tunnel1 {<br>authentication { |

| Действие | Команда |
|---|---|
| | method x509<br>x509-cert NEO-1-cert<br>}<br>esp-group ESP-1W<br>ike-group IKE-1W<br>local-ip 192.0.2.1<br>local-subnet 192.168.40.0/24<br>nat-traversal off<br>remote-ip 192.0.2.33<br>remote-subnet 192.168.60.0/24<br>}<br>[edit] |

#### *17.1.5.7. Изменение настроек подключения к узлу NEO-1 на узле NEO-2*

В примере 17.21 изменяются параметры подключения от узла NEO-2 к узлу NEO-1 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 NEO-2, импортированный на предыдущем шаге (см. раздел Импорт сертификата узла NEO-2Импорт сертификата узла NEO-21131 на стр. 1131).

Для изменения настройки аутентификации на использование инфраструктуры открытых ключей необходимо выполнить следующие шаги в режиме настройки на узле NEO-2:

*Пример 17.21 - Настройка узла NEO-2 для аутентификации с использованием X.509*

| Действие | Команда |
|---|---|
| Изменение режима аутентификации. | admin@NEO-2# **set vpn ipsec site-to-site peer 192.0.2.1 authentication method x509**<br>[edit] |
| Указание используемого сертификата узла NEO-1. | admin@NEO-2# **set vpn ipsec site-to-site peer 192.0.2.1 authentication x509-cert NEO-2_VPN_Peer_certificate**<br>[edit] |
| Фиксация настройки. | admin@NEO-2# **commit**<br>[edit] |
| Отображение измененной настройки подключения в межфилиальном режиме. | admin@NEO-2# **show -all vpn ipsec site-to-site peer**<br>192.0.2.1 {<br>authentication {<br>method x509<br>x509-cert NEO-2_VPN_Peer_certificate<br>}<br>esp-group ESP-1E<br>ike-group IKE-1E<br>local-ip 192.0.2.33<br>local-subnet 192.168.60.0/24<br>nat-traversal off<br>remote-ip 192.0.2.1<br>remote-subnet 192.168.40.0/24 |

| Действие | Команда |
|---|---|
| | } |
| | [edit] |

### 17.1.6. Создание подключения VPN с использованием NAT

В этом разделе рассматриваются следующие вопросы:

- Настройка NEO-1.
- Настройка узла NEO-2.

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.

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.*

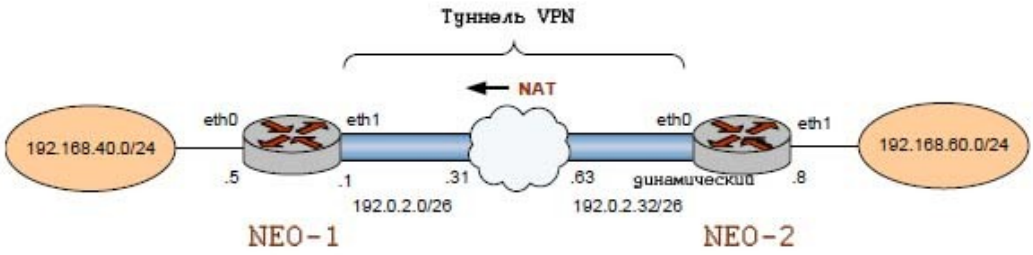
В данном разделе представлен пример настройки подключения, проходящего через NAT между узлами NEO-1 и NEO-2. В этом примере:

- Узел NEO-2 расположен за устройством, осуществляющим NAT, и по этой причине с точки зрения узла NEO-1 имеет динамический IP-адрес.
- Узел NEO-1 сохраняет фиксированный IP-адрес.

Указанный пример настройки аналогичен случаю, когда оконечный узел IPSec располагается за подключением DSL, когда общедоступный адрес узла DSL является динамическим и узел DSL осуществляет NAT.

После завершения настройки примеров данного раздела, узлы будут настроены как показано на рисунке 64.

*Рисунок 64 - Настройка узла NEO-2 для аутентификации с использованием X.509*




Перед началом настройки:

Данный пример предполагает, что основное подключение в межфилиальном режиме уже было настроено с использованием предварительных ключей для аутентификации между узлами NEO-1 и NEO-2, см. раздел Настройка базового подключения в межфилиальном режиме на стр. 1099. В данном разделе представлены только необходимые изменения в настройке.

### *17.1.6.1. Настройка NEO-1*

Для того чтобы разрешить динамический IP-адрес узла NEO-2, на узле NEO-1 необходимо создать новое подключение в межфилиальном режиме к узлу, имеющему динамический IP-адрес.

В примере 17.22 определяется новое подключение к узлу NEO-2.

- Основным отличием является то, что не указывается IP-адреса узла. Отсутствие указания параметра **remote-ip** означает, что может использоваться "любой" адрес. При этом необходимо для аутентификации узлов VPN при помощи команды vpn ipsec site-to-site peer <туннель> authentication указать значение идентификаторов (узлы конфигурации **id**, **remote-id**).
- Значения всех остальных параметров совпадают с указанными для базового подключения.

Для настройки этого подключения необходимо выполнить следующие шаги на узле NEO-1 в режиме настройки:

*Пример 17.22 - Создание подключения в межфилиальном режиме к узлу, имеющему динамический IP-адрес*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для узла NEO-2, установка IP-адреса, и установка режима аутентификации. | admin@NEO-1# **set vpn ipsec site-to-site peer tunnel1 authentication method pre-shared-key**<br>**[edit]** |
| Переход к другому узлу конфигурации для более удобного редактирования. | admin@NEO-1# edit vpn ipsec site-to-site peer **tunnel1**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Ввод строки, которая будет использоваться в качестве предварительного ключа. | admin@NEO-1# **set authentication pre-shared-key test_key_1**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание группы IKE. | admin@NEO-1# **set ike-group IKE-1W**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание идентификатора локального узла. | admin@NEO-1# **set id neo-1**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание идентификатора удаленного узла. | admin@NEO-1# **set remote-id neo-2**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание IP-адреса данной системы Altell NEO, который будет использоваться для этого подключения. | admin@NEO-1# **set local-ip 192.0.2.1**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |

| Действие | Команда |
|---|---|
| Создание настройки туннеля, и указание локальной подсети для данного туннеля. | admin@NEO-1# **set local-subnet 192.168.40.0/24**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание удаленной подсетти для данного туннеля. | admin@NEO-1# **set remote-subnet 192.168.60.0/24**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание группы ESP для данного туннеля. | admin@NEO-1# **set esp-group ESP-1W**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Возврат к вершине дерева настройки. | admin@NEO-1# **top**<br>[edit] |
| Фиксация настройки. | admin@NEO-1# **commit**<br>[edit] |
| Вывод настройки для подключения IPSec в межфилиальном режиме. | admin@NEO-1# **show -all vpn ipsec site-to-site peer tunnel1**<br>authentication<br>{<br>id neo-1<br>method pre-shared-key<br>pre-shared-key test_key_1<br>remote-id neo-2<br>}<br>ike-group IKE-1W<br>local-ip 192.0.2.1<br>local-subnet 192.168.40.0/24<br>remote-subnet 192.168.60.0/24<br>esp-group ESP-1W |

| Действие | Команда |
|---|---|
| | `[edit]` |

#### *17.1.6.2. Настройка узла NEO-2*

В конфигурацию узла NEO-2 необходимо добавить настройку аутентификации узлов:

*Пример 17.23 - Изменение настройки подключения от узла NEO-2 к узлу NEO-1*

| Действие | Команда |
|---|---|
| Указание идентификатора локального узла. | `admin@NEO-2# **set id neo-2**`<br>`[edit vpn/ipsec/site-to-site/peer/tunnel1]` |
| Указание идентификатора удаленного узла. | `admin@NEO-2# **set remote-id neo-1**`<br>`[edit vpn/ipsec/site-to-site/peer/tunnel1]` |
| Указание того, что локальный узел имеет динамический адрес. | `admin@NEO-2# **set local-ip 0.0.0.0**`<br>`[edit vpn/ipsec/site-to-site/peer/tunnel1]` |

Устройство, осуществляющее NAT, отслеживает фиксированный IP-адрес узла NEO-2 и корректно маршрутизирует узлу NEO-2 входящие пакеты, внося все необходимые изменения в исходящие пакеты

Узел NEO-1 сохраняет фиксированный IP-адрес, таким образом, не требуется никаких дополнительных изменений IP-адреса удаленного узла.

### 17.1.7. Настройка туннелей IPSec между тремя шлюзами

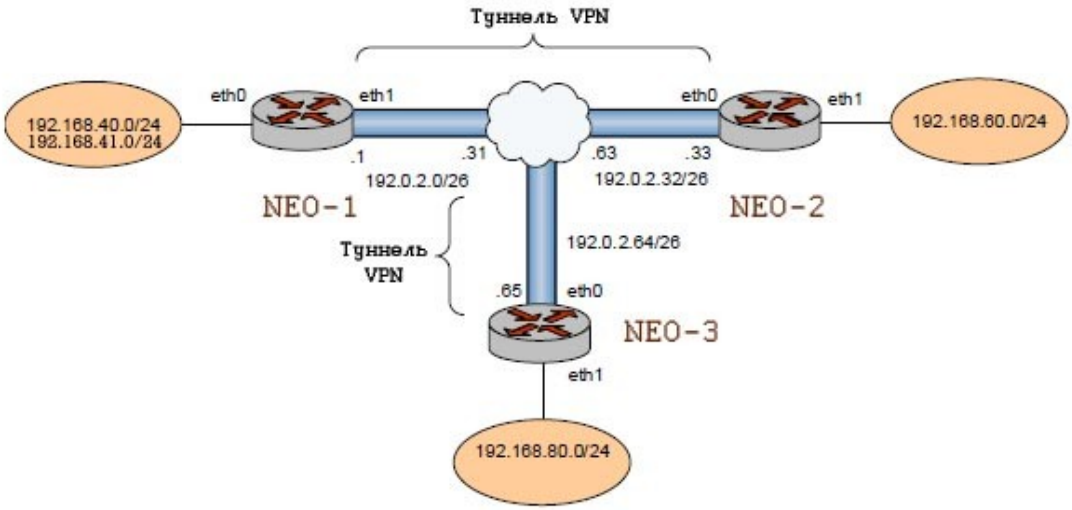
В этом разделе рассматриваются следующие вопросы:

- Настройка NEO-1.
- Настройка узла NEO-2.
- Настройка узла NEO-3.

В данном разделе представлен пример настройки подключения в межфилиальном режиме между тремя шлюзами: NEO-1, NEO-2, и NEO-3. После завершения настройки все

узлы будут настроены как показано на рисунке 65.

*Рисунок 65 - Настройка туннелей IPSec между тремя шлюзами*




### *17.1.7.1. Настройка NEO-1*

В этом разделе рассматриваются следующие вопросы:

- Настройка второй группы ESP на узле NEO-1.
- Добавление еще одного туннеля к узлу NEO-2.
- Создание подключения к узлу NEO-3.

В данном примере предполагается, что на узле NEO-1 уже настроено базовое подключение к узлу NEO-2, как показано в примере Настройка базового подключения в межфилиальном режиме на стр. 1099.

Дополнительная настройка узла NEO-1 для данного примера заключается в следующем:

- Дополнительная группа ESP.
- Настройка нового туннеля к узлу NEO-2 в межфилиальном режиме.
- Новое подключение в межфилиальном режиме к узлу NEO-3.

В данном разделе представлены следующие примеры:

- Пример 17.24 Настройка второй группы ESP на узле NEO-1.

- Пример 17.25 Добавление туннеля к узлу NEO-2.
- Пример 17.27 Создание подключения от узла NEO-1 к узлу NEO-3 в межфилиальном режиме.

#### 17.1.7.1.1. Настройка второй группы ESP на узле NEO-1

В примере 17.24 приведено создание второй группы ESP с именем ESP-2W на узле NEO-1.

Группа ESP содержит одно предложение:

- В предложении 1 используется AES в качестве алгоритма шифрования и SHA-1 в качестве алгоритма хэширования.
- Время жизни для предложений, относящихся к этой группе ESP, устанавливается равным 600 секундам. Для создания группы ESP, необходимо выполнить на узле NEO-1 следующие действия в режиме настройки:

*Пример 17.24 - Настройка второй группы ESP на узле NEO-1*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для предложения 1 группы ESP с именем ESP-2W. | admin@NEO-1# **set vpn ipsec esp-group ESP-2W proposal 1**<br>[edit] |
| Установка алгоритма шифрования для предложения 1. | admin@NEO-1# **set vpn ipsec esp-group ESP-2W proposal 1 encryption aes**<br>[edit] |
| Установка алгоритма хэширования для предложения 1 группы ESP-2W. | admin@NEO-1# **set vpn ipsec esp-group ESP-2W proposal 1 hash hmac_sha1**<br>[edit] |
| Установка времени жизни для группы ESP-2W. | admin@NEO-1# **set vpn ipsec esp-group ESP-2W lifetime 600**<br>[edit] |

| Действие | Команда |
|---|---|
| Вывод настройки для группы ESP. На данном этапе настройки изменения не фиксируются. | admin@NEO-1# **show -all vpn ipsec esp-group ESP-2W**<br>esp-group ESP-2W {<br>compression disable<br>lifetime 600<br>mode tunnel<br>proposal 1 {<br>encryption aes<br>hash hmac_sha1<br>}<br>}<br>[edit] |

#### 17.1.7.1.2. Добавление туннеля к узлу NEO-2

В примере 17.25 добавляется туннель в межфилиальном режиме от узла NEO-1 к узлу NEO-2.

Туннель обеспечивает взаимодействие между подсетью 192.168.41.0/24 на узле NEO-1 и подсетью 192.168.60.0/24 на узле NEO-2, с использованием группы ESP с именем ESP-2W.

Для настройки этого подключения необходимо выполнить следующие шаги на узле NEO-1 в режиме настройки:

*Пример 17.25 - Добавление туннеля от узла NEO-1 к узлу NEO-2*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для туннеля к узлу NEO-2 и указание режима аутентификации. | admin@NEO-1# **set vpn ipsec site-to-site peer tunnel2 authentication method pre-shared-key**<br>[edit] |
| Переход к другому узлу конфигурации для более удобного редактирования. | admin@NEO-1# **edit vpn ipsec site-to-site peer tunnel2** |

| Действие | Команда |
|---|---|
| | [edit vpn/ipsec/site-to-site/peer/tunnel2] |
| Ввод строки, которая будет использоваться в качестве предварительного ключа. | admin@NEO-1# **set authentication pre-shared-key test_key_1**<br>[edit vpn/ipsec/site-to-site/peer/tunnel2] |
| Указание группы IKE. | admin@NEO-1# **set ike-group IKE-1W**<br>[edit vpn/ipsec/site-to-site/peer/tunnel2] |
| Указание IP-адреса данной системы Altell NEO, который будет использоваться для этого подключения. | admin@NEO-1# **set local-ip 192.0.2.1**<br>[edit vpn/ipsec/site-to-site/peer/tunnel2] |
| Указание IP-адреса удаленного узла VPN, который будет использоваться для этого подключения. | admin@NEO-1# **set remote-ip 192.0.2.33**<br>[edit vpn/ipsec/site-to-site/peer/tunnel2] |
| Указание локальной подсети для данного туннеля. | admin@NEO-1# **set local-subnet 192.168.41.0/24**<br>[edit vpn/ipsec/site-to-site/peer/tunnel2] |
| Указание удаленной подсети для данного туннеля. | admin@NEO-1# **set remote-subnet 192.168.60.0/24**<br>[edit vpn/ipsec/site-to-site/peer/tunnel2] |
| Указание группы ESP для данного туннеля. | admin@NEO-1# **set esp-group ESP-2W**<br>[edit vpn/ipsec/site-to-site/peer/tunnel2] |

| Действие | Команда |
|---|---|
| Возврат к вершине дерева настройки. | admin@NEO-1# **top**<br>[edit] |
| Фиксация настройки. | admin@NEO-1# **commit**<br>[edit] |
| Вывод настройки для подключения IPSec в межфилиальном режиме. | admin@NEO-1# **show -all vpn ipsec site-to-site peer tunnel2**<br>authentication {<br>method pre-shared-key<br>pre-shared-key test_key_1<br>}<br>esp-group ESP-2W<br>ike-group IKE-1W<br>local-ip 192.0.2.1<br>local-subnet 192.168.41.0/24<br>nat-traversal off<br>remote-ip 192.0.2.33<br>remote-subnet 192.168.60.0/24<br>[edit] |

#### 17.1.7.1.3. Определение статического маршрута на узле NEO-1

В примере 17.26 создается статический маршрут для трафика, предназначенного удаленному оконечному узлу туннеля.

Отправка трафика, предназначенного для подсети 192.168.60.0/24, к удаленной оконечной точке туннеля — 192.0.2.33. Для создания статического маршрута необходимо выполнить на узле NEO-1 следующие действия в режиме настройки:

*Пример 17.26 - Определение статического маршрута на узле NEO-1*

| Действие | Команда |
|---|---|
| Создание статического маршрута. | admin@NEO-1# **set protocols static** |

| Действие | Команда |
|---|---|
| | **route 192.168.60.0/24 next-hop 192.0.2.33**<br>[edit] |
| Фиксация настройки. | admin@NEO-1# **commit**<br>[edit] |
| Вывод настройки. | admin@NEO-1# **show protocols static** route192.168.60.0/24 {<br>next-hop 192.0.2.33<br>}<br>[edit] |

#### 17.1.7.1.4. Создание подключения к узлу NEO-3

В примере 17.27 определяется подключение в межфилиальном режиме от узла NEO-1 к узлу NEO-3.

Туннель обеспечит подключение между подсетью 192.168.40.0/24 на узле NEO-1 и подсетью 192.168.80.0/24 на узле NEO-3, с использованием группы ESP с именем ESP-1W.

- На узле NEO-1 интерфейсу eth1 назначен IP-адрес 192.0.2.1.
- На узле NEO-3 интерфейсу eth1 назначен IP-адрес 192.0.2.35.
- Используется группа IKE с именем IKE-1W
- В качестве предварительного ключа используется строка “test_key_2”.

Для настройки указанного туннеля необходимо выполнить следующие шаги на узле NEO-1 в режиме настройки:

*Пример 17.27 - Создание туннеля от узла NEO-1 к узлу NEO-3 в межфилиальном режиме*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для туннеля к узлу NEO-3 и указание режима аутентификации. | admin@NEO-1# **set vpn ipsec site-to-site peer tunnel3 authentication method pre-shared-key** |

| Действие | Команда |
|---|---|
| | `[edit]` |
| Переход к другому узлу конфигурации для более удобного редактирования | `admin@NEO-1# **edit vpn ipsec site-to-site peer tunnel3**`<br>`[edit vpn/ipsec/site-to-site/peer/tunnel3]` |
| Ввод строки, которая будет использоваться в качестве предварительного ключа. | `admin@NEO-1# **set authentication pre-shared-key test_key_2**`<br>`[edit vpn/ipsec/site-to-site/peer/tunnel3]` |
| Указание группы IKE. | `admin@NEO-1# **set ike-group IKE-1W**`<br>`[edit vpn/ipsec/site-to-site/peer/tunnel3]` |
| Указание IP-адреса данной системы Altell NEO, который будет использоваться для этого подключения. | `admin@NEO-1# **set local-ip 192.0.2.1**`<br>`[edit vpn/ipsec/site-to-site/peer/tunnel3]` |
| Указание IP-адреса удаленного шлюза, который будет использоваться для этого подключения. | `admin@NEO-1# **set remote-ip 192.0.2.35**`<br>`[edit vpn/ipsec/site-to-site/peer/tunnel3]` |
| Указание локальной подсети для этого туннеля. | `admin@NEO-1# **set local-subnet 192.168.40.0/24**`<br>`[edit vpn/ipsec/site-to-site/peer/tunnel3]` |
| Указание удаленной подсети для туннеля. | `admin@NEO-1# **set remote-subnet 192.168.80.0/24**`<br>`[edit vpn/ipsec/site-to-site/peer/tunnel3]` |

| Действие | Команда |
|---|---|
| Указание группы ESP для туннеля. | admin@NEO-1# **set esp-group ESP-1W**<br>[edit vpn/ipsec/site-to-site/peer/tunnel3] |
| Возврат к вершине дерева настройки. | admin@NEO-1# **top**<br>[edit] |
| Фиксация настройки. | admin@NEO-1# **commit**<br>[edit] |
| Вывод настройки для подключения IPSec в межфилиальном режиме. | admin@NEO-1# **show -all vpn ipsec site-to-site peer**<br>authentication {<br>method pre-shared-key<br>pre-shared-key test_key_2<br>}<br>esp-group ESP-1W<br>ike-group IKE-1W<br>local-ip 192.0.2.1<br>local-subnet 192.168.40.0/24<br>nat-traversal off<br>remote-ip 192.0.2.35<br>remote-subnet 192.168.80.0/24<br>[edit] |

#### 17.1.7.1.5. Определение статического маршрута на узле NEO-1

В примере 17.28 создается статический маршрут для трафика, предназначенного удаленному оконечному узлу туннеля.

Отправка трафика, предназначенного для подсети 192.168.80.0/24, к удаленной оконечной точке туннеля — 192.0.2.64. Для создания статического маршрута необходимо выполнить на узле NEO-1 следующие действия в режиме настройки:

*Пример 17.28 - Определение статического маршрута на узле NEO-1*

| Действие | Команда |
|---|---|
| Создание статического маршрута. | admin@NEO-1# **set protocols static route 192.168.80.0/24 next-hop 192.0.2.64**<br>[edit] |
| Фиксация настройки. | admin@NEO-1# **commit**<br>[edit] |
| Вывод настройки. | admin@NEO-1# **show protocols static** route192.168.60.0/24 {<br>next-hop 192.0.2.33<br>}<br>route192.168.80.0/24 {<br>next-hop 192.0.2.64<br>}<br>[edit] |

### *17.1.7.2. Настройка узла NEO-2*

В этом разделе рассматриваются следующие вопросы:

- Настройка второй группы ESP на узле NEO-2.
- Добавление туннеля к узлу NEO-1.
- Создание подключения к узлу NEO-3.

В данном примере предполагается, что на узле NEO-2 уже настроено базовое подключение к узлу NEO-1, как показано в примере Настройка базового подключения в межфилиальном режиме на стр. 1099. Дополнительная настройка узла NEO-2 для данного примера заключается в следующем:

- Дополнительная группа ESP.
- Настройка нового туннеля для подключения к узлу NEO-1 в межфилиальном режиме.
- Новое подключение в межфилиальном режиме к узлу NEO-3.

В данном разделе представлены следующие примеры:

- Пример 17.29 Настройка второй группы ESP на узле NEO-2
- Пример 17.30 Добавление туннеля к узлу NEO-1
- Пример 17.31 Создание подключения в межфилиальном режиме от узла NEO-2 к узлу NEO-3

#### 17.1.7.2.1. Настройка второй группы ESP на узле NEO-2

В примере 17.29 приведено создание второй группы ESP с именем ESP-2W на узле NEO-2. Группа ESP содержит одно предложение:

- В предложении 1 используется AES в качестве алгоритма шифрования и SHA-1 в качестве алгоритма хэширования.

Время жизни для предложений, относящихся к этой группе ESP, устанавливается равным 600 секундам. Для создания этой группы ESP необходимо выполнить следующие действия на узле NEO-2 в режиме настройки:

*Пример 17.29 - Настройка второй группы ESP на узле NEO-2*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для предложения 1 группы ESP с именем ESP-2E. | admin@NEO-2# **set vpn ipsec esp-group ESP-2E proposal 1**<br>[edit] |
| Установка алгоритма шифрования для предложения 1. | admin@NEO-2# **set vpn ipsec esp-group ESP-2E proposal 1 encryption aes**<br>[edit] |
| Установка алгоритма хэширования для предложения 1 группы ESP-2E. | admin@NEO-2# **set vpn ipsec esp-group ESP-2E proposal 1 hash hmac_sha1**<br>[edit] |
| Установка времени жизни для группы ESP-2E. | admin@NEO-2# **set vpn ipsec esp-group ESP-2E lifetime 600**<br>[edit] |

| Действие | Команда |
|---|---|
| Вывод настройки для группы ESP. На данном этапе настройки изменения не фиксируются. | admin@NEO-2# **show -all vpn ipsec**<br>esp-group ESP-2E<br>compression disable<br>lifetime 600<br>mode tunnel<br>proposal 1 {<br>encryption aes<br>hash hmac_sha1<br>}<br>[edit] |

#### 17.1.7.2.2. Добавление туннеля к узлу NEO-1

В примере 17.30 добавляется новый туннель от узла NEO-2 к узлу NEO-1, обеспечивающий взаимодействие между подсетью 192.168.60.0/24 на узле NEO-2 и подсетью 192.168.41.0/24 на узле NEO-1 с использованием группы ESP с именем ESP-2E.

Для настройки этого туннеля необходимо выполнить следующие действия на узле NEO-2 в режиме настройки:

*Пример 17.30 - Создание туннеля в межфилиальном режиме от узла NEO-2 к узлу NEO-1*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для туннеля к узлу NEO-1 и указание режима аутентификации. | admin@NEO-2# **set vpn ipsec site-to-site peer tunnel2 authentication method pre-shared-key**<br>[edit] |
| Переход к другому узлу конфигурации для удобства редактирования. | admin@NEO-2# **edit vpn ipsec site-to-site peer tunnel2**<br>[edit vpn/ipsec/site-to-site/peer/tunnel2] |

| Действие | Команда |
|---|---|
| Ввод строки, которая будет использоваться в качестве предварительного ключа. | admin@NEO-2# **set authentication pre-shared-key test_key_1**<br>[edit vpn/ipsec/site-to-site/peer/tunnel2] |
| Указание группы IKE. | admin@NEO-2# **set ike-group IKE-1E**<br>[edit vpn/ipsec/site-to-site/peer/tunnel2] |
| Указание IP-адреса данной системы Altell NEO, который будет использоваться для данного подключения. | admin@NEO-2# **set local-ip 192.0.2.33**<br>[edit vpn/ipsec/site-to-site/peer/tunnel2] |
| Указание локальной подсети для данного туннеля. | admin@NEO-2# **set local-subnet 192.168.60.0/24**<br>[edit vpn/ipsec/site-to-site/peer/tunnel2] |
| Указание IP-адреса удаленного узла VPN, который будет использоваться для данного туннеля. | admin@NEO-2# **set remote-ip 192.0.2.1**<br>[edit vpn/ipsec/site-to-site/peer/tunnel2] |
| Указание удаленной подсети для данного туннеля. | admin@NEO-2# **set remote-subnet 192.168.41.0/24**<br>[edit vpn/ipsec/site-to-site/peer/tunnel2] |
| Указание группы ESP для данного туннеля. | admin@NEO-2# **set esp-group ESP-2E**<br>[edit vpn/ipsec/site-to-site/peer/tunnel2] |
| Возврат к вершине дерева настройки. | admin@NEO-2# **top**<br>[edit] |

| Действие | Команда |
|---|---|
| Фиксация настройки. | admin@NEO-2# **commit**<br>[edit] |
| Вывод настройки для туннеля IPSec в межфилиальном режиме. | admin@NEO-2# **show -all vpn ipsec site-to-site peer tunnel2**<br>authentication {<br>method pre-shared-key<br>pre-shared-key test_key_1<br>}<br>esp-group ESP-2E<br>ike-group IKE-1E<br>local-ip 192.0.2.33<br>local-subnet 192.168.60.0/24<br>nat-traversal off<br>remote-ip 192.0.2.1<br>remote-subnet 192.168.41.0/24<br>[edit] |

#### 17.1.7.2.3. Создание подключения к узлу NEO-3

В примере 17.31 определяется подключение в межфилиальном режиме от узла NEO-2 к узлу NEO-3.

Туннель, обеспечивающий взаимодействие между подсетью 192.168.60.0/24 на узле NEO-2 и подсетью 192.168.80.0/24 на узле NEO-3 с использованием группы ESP с именем ESP-1E.

На узле NEO-2 интерфейсу eth1 назначен IP-адрес 192.0.2.33.

На узле NEO-3 интерфейсу eth1 назначен IP-адрес 192.0.2.35.

Используется группа IKE с именем IKE-1E

В качестве предварительного ключа используется строка “test_key_2”. Для настройки этого подключения необходимо выполнить следующие действия на узле NEO-2 в режиме настройки:

*Пример 17.31 - Создание подключения в межфилиальном режиме от узла NEO-2 к узлу NEO-3*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для туннеля к узлу NEO-3 и указание режима аутентификации. | admin@NEO-2# **set vpn ipsec site-to-site peer tunnel3 authentication method pre-shared-key**<br>[edit] |
| Переход к другому узлу конфигурации для более удобного редактирования | admin@NEO-2# **edit vpn ipsec site-to-site peer tunnel3**<br>[edit vpn/ipsec/site-to-site/peer/tunnel3] |
| Ввод строки, которая будет использоваться в качестве предварительного ключа. | admin@NEO-2# **set authentication pre-shared-key test_key_2**<br>[edit vpn/ipsec/site-to-site/peer/tunnel3] |
| Указание группы IKE. | admin@NEO-2# **set ike-group IKE-1E**<br>[edit vpn/ipsec/site-to-site/peer/tunnel3] |
| Указание IP-адреса данной системы Altell NEO, который будет использоваться для этого подключения. | admin@NEO-2# **set local-ip 192.0.2.33**<br>[edit vpn/ipsec/site-to-site/peer/tunnel3] |
| Указание локальной подсети для этого туннеля. | admin@NEO-2# **set local-subnet 192.168.60.0/24**<br>[edit vpn/ipsec/site-to-site/peer/tunnel3] |
| Указание IP-адреса удаленного шлюза VPN. | admin@NEO-2# **set remote-ip 192.0.2.35** |

| Действие | Команда |
|---|---|
| | [edit vpn/ipsec/site-to-site/peer/tunnel3] |
| Указание удаленной подсети для туннеля. | admin@NEO-2# **set remote-subnet 192.168.80.0/24**<br>[edit vpn/ipsec/site-to-site/peer/tunnel3] |
| Указание группы ESP для туннеля. | admin@NEO-2# **set esp-group ESP-1E**<br>[edit vpn/ipsec/site-to-site/peer/tunnel3] |
| Возврат к вершине дерева настройки. | admin@NEO-2# **top**<br>[edit] |
| Фиксация настройки. | admin@NEO-2# **commit**<br>[edit] |
| Вывод настройки для подключения IPSec в межфилиальном режиме. | admin@NEO-2# **show -all vpn ipsec site-to-site peer tunnel3**<br>authentication {<br>method pre-shared-key<br>pre-shared-key test_key_2<br>}<br>esp-group ESP-1E<br>ike-group IKE-1E<br>local-ip 192.0.2.33<br>local-subnet 192.168.60.0/24<br>nat-traversal off<br>remote-ip 192.0.2.35<br>remote-subnet 192.168.80.0/24<br>[edit] |

#### 17.1.7.2.4. Определение статического маршрута на узле NEO-2

В примере 17.32 создается статический маршрут для трафика, предназначенного удаленному оконечному узлу туннеля.

Отправить трафик, предназначенный для подсети 192.168.80.0/24 к удаленной оконечной точке туннеля - 192.0.2.64.

Для создания статического маршрута необходимо выполнить следующие действия на узле NEO-2 в режиме настройки:

*Пример 17.32 - Определение статического маршрута на узле NEO-2*

| Действие | Команда |
|---|---|
| Создание статического маршрута | admin@NEO-2# **set protocols static route 192.168.80.0/24 next-hop 192.0.2.64**<br>[edit] |
| Фиксация настройки. | admin@NEO-2# **commit**<br>[edit] |
| Вывод настройки. | admin@NEO-2# **show protocols**<br>**static** route 192.168.40.0/24 {<br>  next-hop 192.0.2.1<br>}<br>route 192.168.80.0/24 {<br>  next-hop 192.0.2.64<br>}<br>[edit] |

### *17.1.7.3. Настройка узла NEO-3*

В этом разделе рассматриваются следующие вопросы:

- Настройка группы IKE на узле NEO-3.
- Настройка группы ESP на узле NEO-3.
- Создание подключения к узлу NEO-1.
- Создание подключения к узлу NEO-2.

В этом разделе представлены следующие примеры:

- Пример 17.33 Настройка группы IKE на узле NEO-3.
- Пример 17.34 Настройка группы ESP на узле NEO-3.
- Пример 17.35 Создание туннеля в межфилиальном режиме от узла NEO-3 к узлу NEO-1.
- Пример 17.37 Создание туннеля в межфилиальном режиме от узла NEO-3 к узлу NEO-2.

#### 17.1.7.3.1. Настройка группы IKE на узле NEO-3

В примере 17.33 приведено создание группы IKE с именем IKE-1S на узле NEO-3. Данная группа IKE содержит два предложения:

- В предложении 1 используется AES в качестве алгоритма шифрования и SHA-1 в качестве алгоритма хэширования.
- В предложении 2 используется 3DES в качестве алгоритма шифрования и SHA-1 в качестве алгоритма хэширования.

Время жизни для этой группы IKE устанавливается равным 3600 секундам.

Следует учесть, что указанные параметры соответствуют параметрам, установленным в группе IKE-1W на узле NEO-1 и в группе IKE-1E на узле NEO-2. Необходимо убедиться, при определении предложений, что указанные алгоритмы шифрования и хэширования таковы, что два узла смогут согласовать хотя бы одну комбинацию параметров.

Для создания указанной группы IKE необходимо выполнить следующие шаги на узле NEO-3 в режиме настройки:

*Пример 17.33 - Настройка группы IKE на узле NEO-3*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для предложения 1 группы IKE с именем IKE-1S. | admin@NEO-3# **set vpn ipsec ike-group IKE-1S proposal 1**<br>[edit] |
| Установка алгоритма шифрования для предложения 1. | admin@NEO-3# **set vpn ipsec ike-group IKE-1S proposal 1 encryption aes** |

| Действие | Команда |
|---|---|
| | `[edit]` |
| Установка алгоритма хэширования для предложения 1. | `admin@NEO-3# set vpn ipsec ike-group IKE-1S proposal 1 hash sha1`<br>`[edit]` |
| 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. | `admin@NEO-3# set vpn ipsec ike-group IKE-1S proposal 2 encryption 3des`<br>`[edit]` |
| Установка алгоритма хэширования для предложения 2. | `admin@NEO-3# set vpn ipsec ike-group IKE-1S proposal 2 hash sha1`<br>`[edit]` |
| Установка времени жизни для группы IKE. | `admin@NEO-3# set vpn ipsec ike-group IKE-1S lifetime 3600`<br>`[edit]` |
| Вывод настройки для группы IKE. На данном этапе настройки изменения не фиксируются. | `admin@NEO-3# show -all vpn ipsec`<br>`ike-group IKE-1S`<br>`lifetime 3600`<br>`proposal 1 {`<br>`  dh-group 2`<br>`  encryption aes`<br>`  hash sha1`<br>`}`<br>`proposal 2 {`<br>`  dh-group 2`<br>`  encryption 3des`<br>`  hash sha1` |

| Действие | Команда |
|---|---|
| | }<br>[edit] |

#### 17.1.7.3.2. Настройка группы ESP на узле NEO-3

В примере 17.34 приведено создание группы ESP с именем ESP-1S на узле NEO-3. Данная группа ESP содержит два предложения:

- В предложении 1 используется AES в качестве алгоритма шифрования и SHA-1 в качестве алгоритма хэширования.
- В предложении 2 используется Triple-DES в качестве алгоритма шифрования и MD5 в качестве алгоритма хэширования. Время жизни для предложений этой группы ESP устанавливается равным 1800 секундам. Для создания указанной группы ESP необходимо выполнить следующие шаги на узле NEO-3 в режиме настройки:

*Пример 17.34 - Настройка группы ESP на узле NEO-3*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для предложения 1 группы ESP с именем ESP-1S. | admin@NEO-3# **set vpn ipsec esp-group ESP-1S proposal 1**<br>[edit] |
| Установка алгоритма шифрования для предложения 1. | admin@NEO-3# **set vpn ipsec esp-group ESP-1S proposal 1 encryption aes**<br>[edit] |
| Установка алгоритма хэширования для предложения 1. | admin@NEO-3# **set vpn ipsec esp-group ESP-1S proposal 1 hash hmac_sha1**<br>[edit] |
| Установка алгоритма шифрования для предложения 2. В результате выполнения данной команды также | admin@NEO-3# **set vpn ipsec esp-group ESP-1S proposal 2 encryption 3des** |

| Действие | Команда |
|---|---|
| будет создан узел конфигурации для предложения 2 группы ESP с именем ESP-1S. | `[edit]` |
| Установка алгоритма хэширования для предложения 2. | `admin@NEO-3# **set vpn ipsec esp-group ESP-1S proposal 2 hash hmac_md5**`<br>`[edit]` |
| Установка времени жизни для группы ESP. | `admin@NEO-3# **set vpn ipsec esp-group ESP-1S lifetime 1800**`<br>`[edit]` |
| Вывод настройки для группы ESP. На данном этапе настройки изменения не фиксируются. | `admin@NEO-3# **show -all vpn ipsec esp-group ESP-1S**`<br>`compression disable`<br>`lifetime 1800`<br>`mode tunnel`<br>`proposal 1 {`<br>`  encryption aes`<br>`  hash hmac_sha1`<br>`}`<br>`proposal 2 {`<br>`  encryption 3des`<br>`  hash hmac_md5`<br>`}`<br>`[edit]` |

#### 17.1.7.3.3. Создание подключения к узлу NEO-1

В примере 17.35 приведено определение подключения в межфилиальном режиме к узлу NEO-1.

Туннель обеспечивает взаимодействие между подсетью 192.168.80.0/24 на узле NEO-3

и подсетью 192.168.40.0/24 на узле NEO-1 с использованием группы ESP с именем ESP-1S.

На узле NEO-3 интерфейсу eth1 назначен IP-адрес 192.0.2.35.

На узле NEO-1 интерфейсу eth1 назначен IP-адрес 192.0.2.1.

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 NEO-3 в режиме настройки:

*Пример 17.35 - Создание туннеля в межфилиальном режиме от узла NEO-3 к узлу NEO-1*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для туннеля к узлу NEO-1 и указание режима аутентификации | admin@NEO-3# **set vpn ipsec site-to-site peer tunnel1 authentication method pre-shared-key**<br>[edit] |
| Переход к другому узлу конфигурации для более удобного редактирования | admin@NEO-3# **edit vpn ipsec site-to-site peer tunnel1**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Ввод строки, которая будет использоваться в качестве предварительного ключа. | admin@NEO-3# **set authentication pre-shared-key test_key_2**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание группы IKE. | admin@NEO-3# **set ike-group IKE-1S**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание локального IP-адреса данной системы Altell NEO, который будет использоваться для этого подключения. | admin@NEO-3# **set local-ip 192.0.2.35**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |

| Действие | Команда |
|---|---|
| Указание локальной подсети для этого туннеля. | admin@NEO-3# **set local-subnet 192.168.80.0/24**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание IP-адреса удаленного шлюза VPN. | admin@NEO-3# **set remote-ip 192.0.2.1**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание удаленной подсети для туннеля 1. | admin@NEO-3# **set remote-subnet 192.168.40.0/24**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание группы ESP для туннеля. | admin@NEO-3# **set esp-group ESP-1S**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Возврат к вершине дерева настройки. | admin@NEO-3# **top**<br>[edit] |
| Фиксация настройки. | admin@NEO-3# **commit**<br>[edit] |
| Вывод настройки для подключения IPSec в межфилиальном режиме. | admin@NEO-3# **show -all vpn ipsec site-to-site peer tunnel1**<br>authentication {<br>method pre-shared-key<br>pre-shared-key test_key_2<br>}<br>esp-group ESP-1S<br>ike-group IKE-1S<br>local-ip 192.0.2.35 |

| Действие | Команда |
|---|---|
| | local-subnet 192.168.80.0/24<br>nat-traversal off<br>remote-ip 192.0.2.1<br>remote-subnet 192.168.40.0/24<br>[edit] |

#### 17.1.7.3.4. Определение статического маршрута на узле NEO-3

В примере 17.36 создается статический маршрут для трафика, предназначенного удаленному оконечному узлу туннеля.

Отправить трафик, предназначенный для подсети 192.168.40.0/24 к удаленной оконечной точке туннеля - 192.0.2.1.

Для создания статического маршрута необходимо выполнить следующие действия на узле NEO-3 в режиме настройки:

*Пример 17.36 - Определение статического маршрута на узле NEO-2*

| Действие | Команда |
|---|---|
| Создание статического маршрута | admin@NEO-2# **set protocols static route 192.168.40.0/24 next-hop 192.0.2.1**<br>[edit] |
| Фиксация настройки. | admin@NEO-2# **commit**<br>[edit] |
| Вывод настройки. | admin@NEO-2# **show protocols static** route 192.168.40.0/24 {<br>next-hop 192.0.2.1<br>}<br>[edit] |

#### 17.1.7.3.5. Создание подключения к узлу NEO-2

В примере 17.37 приведено определение подключения в межфилиальном режиме к узлу NEO-2.

Туннель обеспечивает взаимодействие между подсетью 192.168.80.0/24 на узле NEO-3 и подсетью 192.168.60.0/24 на узле NEO-2 с использованием группы ESP с именем ESP-1S.

На узле NEO-3 интерфейсу eth1 назначен IP-адрес 192.0.2.35.

На узле NEO-2 интерфейсу eth1 назначен IP-адрес 192.0.2.33.

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 NEO-3 в режиме настройки:

*Пример 17.37 - Создание подключения в межфилиальном режиме от узла NEO-3 к узлу NEO-2*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для туннеля к узлу NEO-2 и установка режима аутентификации. | admin@NEO-3# **set vpn ipsec site-to-site peer tunnel2**<br>[edit] |
| Переход к другому узлу конфигурации для более удобного редактирования. | admin@NEO-3# **edit vpn ipsec site-to-site peer tunnel2**<br>[edit vpn/ipsec/site-to-site/peer/tunnel2] |
| Ввод строки, которая будет использоваться в качестве предварительного ключа. | admin@NEO-3# **set authentication pre-shared-key test_key_2**<br>[edit vpn/ipsec/site-to-site/peer/tunnel2] |
| Указание группы IKE. | admin@NEO-3# **set ike-group IKE-1S**<br>[edit vpn/ipsec/site-to-site/peer/tunnel2] |
| Указание IP-адреса данной системы | admin@NEO-3# **set local-ip** |

| Действие | Команда |
|---|---|
| Altell NEO, который будет использоваться для этого подключения. | **192.0.2.35**<br>[edit vpn/ipsec/site-to-site/peer/tunnel2] |
| Указание локальной подсети для этого туннеля. | admin@NEO-3# **set local-subnet 192.168.80.0/24**<br>[edit vpn/ipsec/site-to-site/peer/tunnel2] |
| Указание IP-адреса шлюза VPN. | admin@NEO-3# **set remote-ip 192.0.2.33**<br>[edit vpn/ipsec/site-to-site/peer/tunnel2] |
| Указание удаленной подсети для туннеля. | admin@NEO-3# **set remote-subnet 192.168.60.0/24**<br>[edit vpn/ipsec/site-to-site/peer/tunnel2] |
| Указание группы ESP для туннеля. | admin@NEO-3# **set esp-group ESP-1S**<br>[edit vpn/ipsec/site-to-site/peer/tunnel2] |
| Возврат к вершине дерева настройки. | admin@NEO-3# **top**<br>[edit] |
| Фиксация настройки. | admin@NEO-3# **commit**<br>[edit] |
| Вывод настройки для подключения IPSec в межфилиальном режиме. | admin@NEO-3# **show -all vpn ipsec site-to-site peer tunnel2**<br>authentication {<br>method pre-shared-key<br>pre-shared-key test_key_2<br>} |

| Действие | Команда |
|---|---|
| | esp-group ESP-1S<br>ike-group IKE-1S<br>local-ip 192.0.2.35<br>local-subnet 192.168.80.0/24<br>nat-traversal off<br>remote-ip 192.0.2.33<br>remote-subnet 192.168.60.0/24<br>[edit] |

#### 17.1.7.3.6. Определение статического маршрута на узле NEO-3

В примере 17.38 создается статический маршрут для трафика, предназначенного удаленному оконечному узлу туннеля.

Отправить трафик, предназначенный для подсети 192.168.60.0/24 к удаленной оконечной точке туннеля - 192.0.2.33.

Для создания статического маршрута необходимо выполнить следующие действия на узле NEO-3 в режиме настройки:

*Пример 17.38 - Определение статического маршрута на узле NEO-2*

| Действие | Команда |
|---|---|
| Создание статического маршрута | admin@NEO-2# **set protocols static route 192.168.60.0/24 next-hop 192.0.2.33**<br>[edit] |
| Фиксация настройки. | admin@NEO-2# **commit**<br>[edit] |
| Вывод настройки. | admin@NEO-2# **show protocols static** route 192.168.40.0/24 {<br>next-hop 192.0.2.1<br>} |

| Действие | Команда |
|---|---|
| | route 192.168.60.0/24 {<br>  next-hop 192.0.2.33<br>}<br>[edit] |

### 17.1.8. 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 VPN позволяет обеспечить безопасные, маршрутизируемые подключения между шлюзами, которые имеют некоторые преимущества по сравнению с использованием туннелей на основе IPSec:

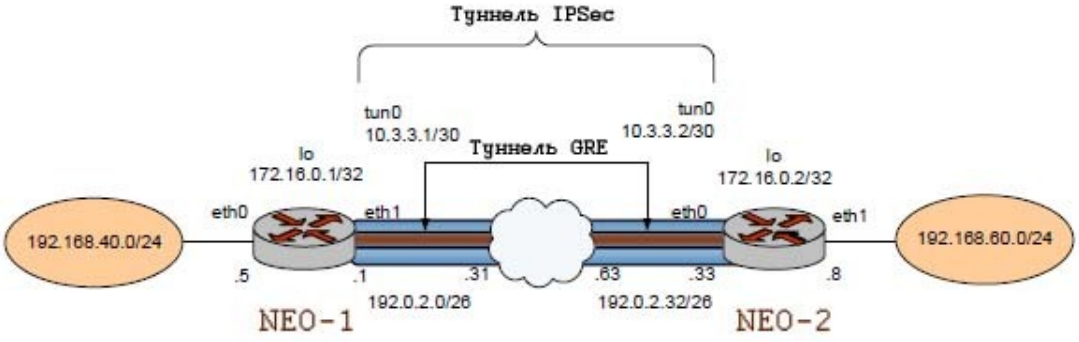
- Поддержка стандартных эксплуатационных команд, например, **show interfaces**.
- Поддержка таких средств, как **traceroute** и SNMP.
- Динамическое переключение на другой туннель в случае отказа.
- Упрощенные политики IPSec и выявление неисправностей.

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.

В данном наборе примеров приводится настройка туннеля GRE между узлами NEO-2 и NEO-1, а также обеспечивается защита этого туннеля с использованием туннеля IPSec между теми же оконечными точками.

После завершения настройки узлы NEO-1 и NEO-2 будут настроены как показано на рисунке 66.

*Рисунок 66 - Создание подключения в межфилиальном режиме от узла NEO-1 к узлу NEO-2*




### *17.1.8.1. Настройка NEO-1*

В этом разделе представлены следующие примеры:

- Пример 17.39 Определение туннеля GRE от узла NEO-1 к узлу NEO-2
- Пример 17.40 Определение туннеля IPSec от узла NEO-1 к узлу NEO-2
- Пример 17.41 Определение статического маршрута на узле NEO-1

#### 17.1.8.1.1. Определение туннеля GRE на узле NEO-1

В примере 17.39 определяется оконечный узел NEO-1 туннеля GRE. В этом примере:

- Туннельному интерфейсу tun0 на маршрутизаторе NEO-1 назначен IP-адрес 10.3.3.1/30.
- В качестве IP-адреса локального узла туннеля GRE (**local-ip**) назначен адрес интерфейса заглушки 172.16.0.1.
- В качестве IP-адреса удаленного оконечного узла туннеля GRE (**remote-ip**) назначен адрес интерфейса заглушки удаленной системы 172.16.0.2.

Для создания туннельного интерфейса и оконечного узла NEO-1 необходимо выполнить следующие действия в режиме настройки:

*Пример 17.39 - Определение туннеля GRE от узла NEO-1 к узлу NEO-2*

| Действие | Команда |
|---|---|
| Создание туннельного интерфейса GRE, | `admin@NEO-1# set interfaces` |

| Действие | Команда |
|---|---|
| и указание связанного с ним IP-адреса. | **tunnel tun0 address 10.3.3.1/30**<br>[edit] |
| Указание локального IP-адреса туннеля GRE. | admin@NEO-1# **set interfaces tunnel tun0 local-ip 172.16.0.1**<br>[edit] |
| Указание удаленного IP-адреса туннеля GRE. | admin@NEO-1# **set interfaces tunnel tun0 remote-ip 172.16.0.2**<br>[edit] |
| Указание режима инкапсуляции для туннеля. | admin@NEO-1# **set interfaces tunnel tun0 encapsulation gre**<br>[edit] |
| Создание краткого описания туннельного интерфейса GRE. | admin@NEO-1# **set interfaces tunnel tun0 description "GRE tunnel to router NEO-2"**<br>[edit] |
| Фиксация настройки. | admin@NEO-1# **commit**<br>[edit] |
| Вывод настройки. | admin@NEO-1# **show interfaces**<br>**tunnel** tun0 {<br>address 10.3.3.1/30<br>encapsulation gre<br>local-ip 172.16.0.1<br>multicast disable<br>remote-ip 172.16.0.2<br>ttl 255<br>}<br>[edit] |

#### 17.1.8.1.2. Определение туннеля IPSec на узле NEO-1

В примере 17.40 приведено создание туннеля IPSec от узла NEO-1 к узлу NEO-2.

- На узле NEO-1 интерфейсу eth1 назначен IP-адрес 192.0.2.1.
- На узле NEO-2 интерфейсу eth1 назначен IP-адрес 192.0.2.33.
- Используется группа IKE с именем IKE-1W.
- В качестве предварительного ключа используется строка “test_key_1”.
- Туннель IPSec обеспечивает взаимодействие между подсетью 172.16.0.1/32 на узле NEO-1 и подсетью 172.16.0.2/32 на узле NEO-2 и использует группу ESP с именем ESP-1W.

***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. Это сделано для того, чтобы показать, что этот туннель начинается и заканчивается там же, где и туннель GRE (то есть необязательно производить настройку именно таким образом).*

В данном примере предполагается, что уже настроено следующее:

- Группа IKE с именем IKE-1W (см. стр. 1101)
- Группа ESP с именем ESP-1W (см. стр. 1103)

Для создания туннеля IPSec от узла NEO-1 к узлу NEO-2, необходимо выполнить следующие шаги на узле NEO-1 в режиме настройки:

*Пример 17.40 - Определение туннеля IPSec от узла NEO-1 к узлу NEO-2*

| Действие | Команда |
|---|---|
| Определение туннеля в межфилиальном режиме к узлу NEO-2. Установка режима аутентификации. | admin@NEO-1# **set vpn ipsec site-to-site peer tunnel1 authentication method pre-shared-key**<br>[edit] |
| Переход к другому узлу конфигурации для более удобного редактирования. | admin@NEO-1# **edit vpn ipsec site-to-site peer tunnel1** |

| Действие | Команда |
|---|---|
| | [edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Ввод строки, которая будет использоваться для аутентификации узлов. | admin@NEO-1# **set authentication pre-shared-key test_key_1**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание группы IKE. | admin@NEO-1# **set ike-group IKE-1W**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание IP-адреса данной системы Altell NEO, который будет использоваться для этого подключения. | admin@NEO-1# **set local-ip 192.0.2.1**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание IP-адреса удаленного шлюза VPN. | admin@NEO-1# **set remote-ip 192.0.2.33**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Создание настройки туннеля, и указание локальной подсети для данного туннеля. | admin@NEO-1# **set local-subnet 172.16.0.1/32**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание удаленной подсети для туннеля. | admin@NEO-1# **set remote-subnet 172.16.0.2/32**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание группы ESP для данного туннеля. | admin@NEO-1# **set esp-group ESP-1W**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |

| Действие | Команда |
|---|---|
| Возврат к вершине дерева настройки. | admin@NEO-1# **top**<br>[edit] |
| Фиксация настройки. | admin@NEO-1# **commit**<br>[edit] |
| Вывод настройки. | admin@NEO-1# **show vpn ipsec site-to-site peer tunnel1**<br>authentication<br>{<br>method pre-shared-key<br>pre-shared-key test_key_1<br>}<br>ike-group IKE-1W<br>local-ip 192.0.2.1<br>local-subnet 172.16.0.1/32<br>remote-ip 192.0.2.33<br>remote-subnet 172.16.0.2/32<br>esp-group ESP-1W<br>[edit] |

#### 17.1.8.1.3. Определение статического маршрута на узле NEO-1

В примере 17.41 создается статический маршрут для трафика, предназначенного удаленному оконечному узлу туннеля GRE.

Отправка трафика, предназначенного для подсети 192.168.60.0/24, к удаленной оконечной точке туннеля GRE - 10.3.3.2. Для создания статического маршрута необходимо выполнить на узле NEO-1 следующие действия в режиме настройки:

*Пример 17.41 - Определение статического маршрута на узле NEO-1*

| Действие | Команда |
|---|---|
| Создание статического маршрута. | admin@NEO-1# **set protocols static** |

| Действие | Команда |
|---|---|
| | **route 192.168.60.0/24 next-hop 10.3.3.2**<br>[edit] |
| Фиксация настройки. | admin@NEO-1# **commit**<br>[edit] |
| Вывод настройки. | admin@NEO-1# **show protocols**<br>**static** route192.168.60.0/24 {<br>next-hop 10.3.3.2<br>}<br>[edit] |

#### *17.1.8.2. Настройка узла NEO-2*

В этом разделе представлены следующие примеры:

- Пример 17.42 Определение туннеля GRE от узла NEO-2 к узлу NEO-1.
- Пример 17.43 Создание туннеля IPSec от узла NEO-2 к узлу NEO-1.
- Пример 17.44 Определение статического маршрута на узле NEO-2.

##### 17.1.8.2.1. Определение туннеля GRE на узле NEO-2

В примере 17.42 приведено определение оконечного узла NEO-2 туннеля GRE. В этом примере:

- Туннельному интерфейсу tun0 на маршрутизаторе NEO-2 назначен IP-адрес 10.3.3.2/30.
- В качестве IP-адреса локального узла туннеля (**local-ip**) назначен адрес интерфейса заглушки 172.16.0.2.
- В качестве IP-адреса удаленного оконечного узла туннеля (**remote-ip**) назначен адрес интерфейса заглушки удаленной системы 172.16.0.1.

Для создания туннельного интерфейса и оконечного узла NEO-2 необходимо выполнить следующие действия в режиме настройки:

*Пример 17.42 - Определение туннеля GRE от узла NEO-2 к узлу NEO-1*

| Действие | Команда |
|---|---|
| Создание туннельного интерфейса GRE, и указание связанного с ним IP-адреса. | admin@NEO-2# **set interfaces tunnel tun0 address 10.3.3.2/30**<br>[edit] |
| Указание локального IP-адреса туннеля GRE. | admin@NEO-2# **set interfaces tunnel tun0 local-ip 172.16.0.1**<br>[edit] |
| Указание удаленного IP-адреса туннеля GRE. | admin@NEO-2# **set interfaces tunnel tun0 remote-ip 172.16.0.1**<br>[edit] |
| Указание режима инкапсуляции для туннеля. | admin@NEO-2# **set interfaces tunnel tun0 encapsulation gre**<br>[edit] |
| Создание краткого описания туннельного интерфейса GRE. | admin@NEO-2# **set interfaces tunnel tun0 description "GRE tunnel to router NEO-1"**<br>[edit] |
| Фиксация настройки. | admin@NEO-2# **commit**<br>[edit] |
| Вывод настройки. | admin@NEO-2# **show interfaces tunnel** tun0 address 10.3.3.2/30<br>description "GRE tunnel to router NEO-1"<br>encapsulation gre<br>local-ip 172.16.0.2<br>remote-ip 172.16.0.1<br>[edit] |

#### 17.1.8.2.2. Определение туннеля IPSec на узле NEO-2

В примере 17.43 приведено создание туннеля IPSec от узла NEO-2 к узлу NEO-1.

- На узле NEO-2 интерфейсу eth0 назначен IP-адрес 192.0.2.33.
- На узле NEO-1 интерфейсу eth1 назначен IP-адрес 192.0.2.1.
- Используется группа IKE с именем IKE-1E.
- В качестве предварительного ключа используется строка “test_key_1”.
- Туннель IPSec обеспечивает взаимодействие между подсетью 172.16.0.2/32 на узле NEO-2 и подсетью 172.16.0.1/32 на узле NEO-1 и использует группу ESP с именем ESP-1E.

***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. Это сделано для того, чтобы показать, что этот туннель начинается и заканчивается там же, где и туннель GRE (то есть необязательно производить настройку именно таким образом).*

В данном примере предполагается, что уже настроено следующее:

- Группа IKE с именем IKE-1E (см. стр. 1110).
- Группа ESP с именем ESP-1E (см. стр. 1112).

Для создания туннеля IPSec от узла NEO-2 к узлу NEO-1 необходимо выполнить следующие действия на узле NEO-2 в режиме настройки:

*Пример 17.43 - Создание туннеля IPSec от узла NEO-2 к узлу NEO-1*

| Действие | Команда |
|---|---|
| Определение туннеля в межфилиальном режиме к узлу NEO-1. Установка режима аутентификации. | admin@NEO-2# **set vpn ipsec site-to-site peer tunnel1 authentication method pre-shared-key**<br>[edit] |
| Переход к другому узлу конфигурации для более удобного редактирования. | admin@NEO-2# **edit vpn ipsec site-to-site peer tunnel1** |

| Действие | Команда |
|---|---|
| | [edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Ввод строки, которая будет использоваться для аутентификации узлов. | admin@NEO-2# **set authentication pre-shared-key test_key_1**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание группы IKE. | admin@NEO-2# **set ike-group IKE-1E**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание IP-адреса данной системы Altell NEO, который будет использоваться для этого подключения. | admin@NEO-2# **set local-ip 192.0.2.33**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание IP-адреса удаленного шлюза VPN. | admin@NEO-2# **set remote-ip 192.0.2.1**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Создание настройки туннеля, и указание локальной подсети для данного туннеля. | admin@NEO-2# **set local-subnet 172.16.0.2/32**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание удаленной подсети для туннеля. | admin@NEO-2# **set remote-subnet 172.16.0.1/32**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |
| Указание группы ESP для данного туннеля. | admin@NEO-2# **set esp-group ESP-1E**<br>[edit vpn/ipsec/site-to-site/peer/tunnel1] |

| Действие | Команда |
|---|---|
| Возврат к вершине дерева настройки. | admin@NEO-2# **top**<br>[edit] |
| Фиксация настройки. | admin@NEO-2# **commit**<br>[edit] |
| Вывод настройки. | admin@NEO-2# **show vpn ipsec site-to-site peer tunnel1**<br>authentication {<br>method pre-shared-key<br>pre-shared-key test_key_1<br>}<br>esp-group ESP-1E<br>ike-group IKE-1E<br>local-ip 192.0.2.33<br>local-subnet 172.16.0.2/32<br>nat-traversal off<br>remote-ip 192.0.2.1<br>remote-subnet 172.16.0.1/32<br>[edit] |

#### 17.1.8.2.3. Определение статического маршрута на узле NEO-2

В примере 17.44 создается статический маршрут для трафика, предназначенного удаленному оконечному узлу туннеля GRE.

Отправить трафик, предназначенный для подсети 192.168.40.0/24 к удаленной оконечной точке туннеля GRE к 10.3.3.1.

Для создания статического маршрута необходимо выполнить следующие действия на узле NEO-2 в режиме настройки:

*Пример 17.44 - Определение статического маршрута на узле NEO-2*

| Действие | Команда |
|---|---|
| Создание статического маршрута | admin@NEO-2# **set protocols static route 192.168.40.0/24 next-hop 10.3.3.1**<br>[edit] |
| Фиксация настройки. | admin@NEO-2# **commit**<br>[edit] |
| Вывод настройки. | admin@NEO-2# **show protocols static** route 192.168.40.0/24 {<br>  next-hop 10.3.3.1<br>}<br>[edit] |

## 17.1.9. 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).

### *17.1.9.1. Локальный узел имеет статический IP-адрес*

**local-ip**: IP-адрес локального интерфейса

**authentication id**: @id

### *17.1.9.2. Локальный узел имеет динамический IP-адрес*

**local-ip**: 0.0.0.0

**authentication id**: @id

### *17.1.9.3. Удаленный узел имеет статический адрес*

**remote-ip**: IP-адрес удаленного узла

**authentication remote-id**: @id

#### *17.1.9.4. Удаленный узел имеет динамический IP-адрес*

**remote-ip**: 0.0.0.0

**authentication remote-id**: @id

## 17.2. 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 главный файл журнала.

В данном разделе приведены следующие примеры:

- Пример 17.45 Вывод защищенных соединений IKE SA
- Пример 17.46 Вывод сведений о состоянии IKE
- Пример 17.47 Вывод защищенных соединений IPSec SA
- Пример 17.48 Вывод статистики IPSec
- Пример 17.49 Вывод сведений о состоянии IPSec

***ПРИМЕЧАНИЕ*** *Вывод, приведенный для данных примеров, может не соответствовать тестовой конфигурации.*

### 17.2.1. Вывод сведений IKE

Для просмотра IKE SA, используется команда **show vpn ike sa**, как показано в примере 17.45.

*Пример 17.45 - Вывод защищенных соединений IKE SA*

```
admin@NEO-1:~$ show vpn ike sa
Source   Destination   Cookies   ST S  V E Created    Phase2
192.0.2.33:500  192.0.2.1:500 ae43c3651b3f133c:f9f421307bd28e89  9
I 10 M 2010-11-19 17:39:02      3
```

Для вывода состояния процесса IKE, используется команда **show vpn ike status**, как

показано в примере 17.46.

*Пример 17.46 - Вывод сведений о состоянии IKE*

```
admin@NEO-1:~$ show vpn ike status
IKE Process Running PID: 5832
```

### 17.2.2. Вывод сведений IPSec

Для просмотра защищенных соединений IPSec SA, используется команда **show vpn ipsec sa**, как показано в примере 17.47.

*Пример 17.47 - Вывод защищенных соединений IPSec SA*

```
admin@NEO-1:~$ show vpn ipsec sa
Peer IP Dir SPI Encrypt Hash Active Lifetime
10.6.0.57 in bf8ea130 aes128 sha1 565 3600
10.6.0.57 out 5818d99e aes128 sha1 565 3600
admin@NEO-1:~$
```

Для вывода статистики IPSec, используется команда **show vpn ipsec statistics**, как показано в примере 17.48.

*Пример 17.48 - Вывод статистики IPSec*

```
admin@NEO-1:~$ show vpn ipsec sa statistics
```

Для отображения состояния процесса IPSec, используется команда **show vpn ipsec status**, как показано в примере 17.49.

*Пример 17.49 - Вывод сведений о состоянии IPSec*

```
admin@NEO-1:~$ show vpn ipsec status
IPSec Process Running PID: 5832 4 Active IPSec Tunnels
IPSec Interfaces: eth1 (10.6.0.55)
```

### 17.2.3. Отправка сообщений IPSec VPN в основной файл журнала

Процесс IPSec генерирует сообщения системного журнала во время исполнения.

Следует учитывать, что в текущей реализации в главный файл системного журнала записываются только сообщения с уровнем серьезности **notice** и выше.

Настройка режима регистрации является необязательной. По умолчанию в файл журнала 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 (см. раздел Уровни серьезности сообщений).

Altell NEO поддерживает следующие режимы регистрации для IPSec VPN.

*Таблица 41 - 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. |
| **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.*

## 17.3. Команды IPSec в межфилиальном режиме

В данном разделе приведены следующие команды:

*Таблица 42 - 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_хэширования>` | Указание алгоритма хэширования, 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_хэширования>` | Определение алгоритма хэширования 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_хэширования>` | Определение алгоритма хэширования для указанного предложения группы IKE. |
| Туннель IPSec | |
| `vpn ipsec site-to-site peer <туннель>` | Определение подключения в межфилиальном режиме между системой Altell NEO 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> ike-group <имя_группы>` | Указание поименованной настройки IKE, которая будет использована при подключении к данному узлу. |
| `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> 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` | 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. |
| Ключи RSA | |
| `vpn rsa-key generate` | Создание ключевой пары RSA для локальной системы. |
| `vpn rsa-keys` | Добавление записи о ключах RSA в локальной системе. |
| 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. |

### 17.3.1. 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.

## 17.3.2. 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.

## 17.3.3. 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 17.50 приведен вывод для команды **show vpn ike rsa-keys**, в котором отображены открытые ключи, о которых есть записи на узле NEO-1:

- выведен открытый ключ локальной системы, при этом секретный ключ локальной системы не выводится;
- выведен открытый ключ узла NEO-2.

*Пример 17.50 - "show vpn ike rsa-keys"*

```
admin@NEO-1:~$ show vpn ike rsa-keys

Local public
key0sAQNfpZicOXWl1rMvNWLIfFppq1uWtUvj8esyjBl/zBfrK4ecZbt7
WzMdMLiLugYtVgo+zJQV5dmQnN+n3qkU9ZLM5QWBxG4iLFtYcwC5fCMx0
hBJfnIEd68d11h7Ea6J4IAm3ZWXcBeOV4S8mC4HV+mqZfv3xyh1ELjfmL
M3fWkp8g5mX7ymgcTpneHiSYX1T9NU3i2CHjYfeKPFb4zJIopu2R654kO
DGOa+4r241Zx3cDIJgHBYSYOiSFYbcdQhKQS3cclFPGVMHYGXjjoiUSA7
d2eMabDtIU4FwnqH3qVN/kdedK34sEJiMUgieT6pJQ6W8y+5PgESvouyk
x8cyTiOobnx0G9oqFcxYLknQ3GbrPej

==========================================================
====== Peer IP: 10.1.0.55 (NEO-2)

0sAQOVBIJL+rIkpTuwh8FPeceAF0bhgLr+
+W51bOAIjFbRDbR8gX3Vlz6wiUbMgGwQxWlYQiqsCeacicsfZx/amlEn9
PkSE4e7tqK/JQo40L5C7gcNM24mup1d+0WmN3zLb9Qhmq5q3pNJxEwnVb
PPQeIdZMJxnb1+lA8DPC3SIxJM/3at1/KrwqCAhX3QNFY/zNmOtFogELC
eyl4+d54wQljA+3dwFAQ4bboJ7YIDs+rqORxWd3l3I7IajT/pLrwr5eZ8
OA9NtAedbMiCwxyuyUbznxXZ8Z/MAi3xjL1pjYyWjNNiOij82QJfMOrjo
XVCfcPn96ZN+Jqk+KknoVeNDwzpoahFOseJREeXzkw3/lkMN9N1

admin@NEO-1:~$
```

## 17.3.4. 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 хэширования.
- 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 17.51 приведен вывод команды **show vpn ike sa**.

*Пример 17.51 - "show vpn ike sa"*

```
admin@NEO-1:~$ 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 2010-11-19
12:50:53 3
```

```
admin@NEO-1:~$
```

### 17.3.5. 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 17.52 приведен вывод команды **show vpn ike secrets**.

*Пример 17.52 - "show vpn ike secrets"*

```
admin@NEO-1:~$ 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
```

### 17.3.6. 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 хэширования.
- Установленное время жизни для защищенного соединения (SA).

**Примеры**

В примере 17.53 приведен вывод для команды **show vpn ipsec sa**.

*Пример 17.53 - "show vpn ipsec sa"*

```
admin@NEO-1:~$ 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: Nov 19 13:14:55 2010   current: Nov 19
13:32:12 2010

   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: Nov 19 13:14:55 2010   current: Nov 19
13:32:12 2010

   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
```

### 17.3.7. 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 17.54 приведен вывод для команды **show vpn ipsec status**.

*Пример 17.54 - "show vpn ipsec status"*

```
admin@NEO-1:~$ show vpn ipsec status
IPSec running
4 active tunnels.
admin@NEO-1:~$
```

### 17.3.8. vpn ipsec

Включение IPSec VPN в системе Altell NEO.

**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 Altell NEO.

> ***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.

### 17.3.9. 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 текст {}
    }
}
```

**Параметры**

*имя_группы*

Множественный узел. Имя, используемое для обозначения настройки AH.

Можно определить несколько настроек AH, создав соответствующее количество узлов конфигурации **ah-group**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда используется для создания группы AH.

Группа AH позволяет задать параметры AH (Authentication Header).

Форма **set** данной команды используется для создания и изменения группы AH.

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

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

### 17.3.10. vpn ipsec ah-group <имя_группы> hash <алгоритм_хэширования>

Указание алгоритма хэширования, используемого для создания заголовка аутентификации.

**Синтаксис**

**set vpn ipsec ah-group** *имя_группы* **hash** *алгоритм_хэширования*

**delete vpn ipsec ah-group hash**

**show vpn ipsec ah-group hash**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
vpn {
     ipsec {
          ah-group текст {
               hash [des|3des|des_iv64|des_iv32|
hmac_sha1|hmac_sha512|hmac_gosthash|hmac_sha256|non_auth|
hmac_md5|hmac_sha384]
          }
     }
}
```

**Параметры**

*имя*

Имя, используемое для обозначения настройки АН.

*алгоритм_хэширования*

Используемый алгоритм хэширования. Поддерживаются следующие значения:

- **des;**
- **3des**;
- **des_iv64**;
- **des_iv32**;
- **hmac_sha1**;
- **hmac_sha512**;

- **hmac_gosthash**;
- **hmac_sha256**;
- **non_auth**;
- **hmac_md5**;
- **hmac_sha384**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда используется для указания алгоритма хэширования, который будет использован для создания заголовка аутентификации.

Altell NEO поддерживает российский криптографический стандарт вычисления хэш-функции ГОСТ Р34.11-94 (**hmac_gosthash**).

> ***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 хэширования, 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 хэширования.

## 17.3.11. 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 текст {}
     }
}
```

**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.

## 17.3.12. 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 текст {
            compression [enable|disable]
        }
    }
}
```

**Параметры**

*имя*

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.

### 17.3.13. 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 текст {
               lifetime 30-86400
          }
     }
}
```

**Параметры**

*имя*

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.

## 17.3.14. 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 текст {
            mode [tunnel|transport]
        }
    }
}
```

**Параметры**

имя

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.

## 17.3.15. 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 текст {
            pfs-group [2 | 5]
        }
    }
}
```

**Параметры**

*имя*

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.

## 17.3.16. 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 proposal**

**show vpn ipsec esp-group proposal**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
vpn {
     ipsec {
          esp-group текст {
               proposal 1-65535 {}
          }
     }
}
```

**Параметры**

*имя*

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.

## 17.3.17. 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 текст {
               proposal 1-65535 {
                    encryption [3des|blowfish|cast128|
des_iv32|gost|rc4|twofish|aes|camellia|des|des_iv64|
null_enc|rijndael]
               }
          }
     }
}
```

**Параметры**

*имя*

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:

- **3des**;
- **blowfish**;
- **cast128**;
- **des_iv32**;

- **gost**;
- **rc4**;
- **twofish**;
- **aes**;
- **camellia**;
- **des**;
- **des_iv64**;
- **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. Altell NEO 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.

## 17.3.18. vpn ipsec esp-group <имя_группы> proposal <номер> hash <алгоритм_хэширования>

Указание алгоритма хэширования для предложения ESP.

**Синтаксис**

**set vpn ipsec esp-group** *имя_группы* **proposal** *номер* **hash** *алгоритм_хэширования*

**delete vpn ipsec esp-group proposal** *номер* **hash**

**show vpn ipsec esp-group proposal** *номер* **hash**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
vpn {
     ipsec {
          esp-group текст {
               proposal 1-65535 {
                    hash [3des|des_iv64|hmac_sha1|
hmac_sha512|des|hmac_gosthash|hmac_sha256|non_auth|
des_iv32|hmac_md5|hmac_sha384]
               }
          }
     }
}
```

**Параметры**

*имя*

Имя, используемое для обозначения настройки ESP.

*номер*

Целое число, уникально идентифицирующее предложение, используемое при согласовании второй фазы IKE.

*алгоритм_хэширования*

Используемый алгоритм хэширования. Поддерживаются следующие значения:

- **3des**;
- **des_iv64**;
- **hmac_sha1**;
- **hmac_sha512**;
- **des**;
- **hmac_gosthash**;
- **hmac_sha256**;
- **non_auth**;
- **des_iv32**;

- **hmac_md5**;
- **hmac_sha384**.

**Значение по умолчанию**

По умолчанию установлено значение **sha1**.

**Указания по использованию**

Данная команда используется для указания алгоритма хэширования, который будет предложен в рамках предложения ESP.

Altell NEO поддерживает российский криптографический стандарт вычисления хэш-функции ГОСТ Р34.11-94 (**hmac_gosthash**).

> ***ПРИМЕЧАНИЕ*** *При использовании для аутентификации протокола AH для данного параметра необходимо установить значение* ***no_auth****. Алгоритм хэширования используемый для аутентификации в этом случае указывается при помощи команды* ***vpn ipsec ah-group <имя_группы> hash <алгоритм_хэширования>*** *(см. стр. 1194).*

Форма **set** данной команды позволяет указать алгоритм хэширования, 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 хэширования, указанного в предложении ESP.

## 17.3.19. 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 текст {}
    }
}
```

**Параметры**

*имя*

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. 1217).

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.

## 17.3.20. 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 текст {
               dead-peer-detection {
                    interval 15-86400
                    timeout 30-86400
               }
          }
     }
}
```

**Параметры**

*имя*

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.

## 17.3.21. 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 текст {
               lifetime 30-86400
          }
     }
}
```

**Параметры**

*имя*

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.

## 17.3.22. 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 proposal**

**show vpn ipsec ike-group proposal**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
vpn {
    ipsec {
        ike-group текст {
            proposal 1-65535 {}
        }
    }
}
```

**Параметры**

*имя*

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.

## 17.3.23. 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 proposal** *номер* **dh-group**

**show vpn ipsec ike-group proposal** *номер* **dh-group**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
vpn {
    ipsec {
        ike-group текст {
```

```
                    proposal 1-65535 {
                        dh-group [2|5]
                    }
                }
            }
        }
```

**Параметры**

*имя*

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.

## 17.3.24. 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 proposal** *номер* **encryption**

**show vpn ipsec ike-group proposal** *номер* **encryption**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
vpn {
     ipsec {
          ike-group текст {
               proposal 1-65535 {
                    encryption [3des|aes|blowfish|
camellia|cast128|des|gost]
               }
          }
     }
}
```

**Параметры**

*имя*

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:

- **3des;**
- **aes;**
- **blowfish;**
- **camellia;**
- **cast128;**
- **des;**

- **gost.**

**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.

Altell NEO 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.

## 17.3.25. vpn ipsec ike-group <имя_группы> proposal <номер> hash <алгоритм_хэширования>

Указание алгоритма хэширования для предложения.

**Синтаксис**

**set vpn ipsec ike-group** *имя_группы* **proposal** *номер* **hash** *алгоритм_хэширования*

**delete vpn ipsec ike-group proposal** *номер* **hash**

**show vpn ipsec ike-group proposal** *номер* **hash**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
vpn {
    ipsec {
        ike-group текст {
            proposal 1-65535 {
                hash [gosthash|md5|sha1|sha256|
sha384|sha512]
            }
```

```
            }
        }
    }
```

**Параметры**

*имя*

Имя, используемое для обозначения настройки IKE.

*номер*

Целое число, уникально идентифицирующее предложение IKE.

*алгоритм_хэширования*

Используемый алгоритм хэширования.

Поддерживаемые значения:

- **gosthash**;
- **md5**;
- **sha1**;
- **sha256**;
- **sha384**;
- **sha512**.

**Значение по умолчанию**

По умолчанию установлено значение **sha1**.

**Указания по использованию**

Данная команда используется для указания алгоритма хэширования, который будет предложен к использованию в рамках предложения IKE.

Altell NEO поддерживает российский криптографический стандарт вычисления хэш-функции ГОСТ Р34.11-94 (**gosthash**).

Форма **set** данной команды позволяет указать алгоритм хэширования, 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 хэширования.

## 17.3.26. 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 [debug|debug2|error|info|notify|
warning]
          }
     }
}
```

**Параметры**

`log-modes` *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. Подробно настройка регистрации описана в разделе Регистрация .

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.

## 17.3.27. vpn ipsec site-to-site peer <туннель>

Определение подключения в межфилиальном режиме между системой Altell NEO 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 [текст]{}
          }
     }
}
```

**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.

## 17.3.28. 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* | **method** *режим* | **pre-shared-key** *ключ* | **remote-id** *id* | **rsa-key-name** *имя*]

**delete vpn ipsec site-to-site peer** *туннель* **authentication** [**id** | **method** | **pre-shared-key** | **remote-id** | **rsa-key-name**]

**show vpn ipsec site-to-site peer** *туннель* **authentication** [**id** | **method** | **pre-shared-key** | **remote-id** | **rsa-key-name**]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
vpn {
     ipsec {
          site-to-site {
               peer [текст] {
                    authentication {
                         id текст
                         method [pre-shared-key|plain-
rsa|x509]
                         pre-shared-key текст
                         remote-id текст
                         rsa-key-name текст
                    }
               }
          }
     }
}
```

**Параметры**

*туннель*

Обязательный. Название туннеля к удаленному узлу IPSec.

**method** *режим*

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**: Использование инфраструктуры открытых ключей (PKI) для аутентификации.

**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.

**id** *id*

Идентификационные данные локального узла VPN, которые будут предъявляться удаленному узлу VPN. Значение указывается в следующем формате: *@идентификатор*.

**remote-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.

**rsa-key-name** *имя*

Имя открытого ключа RSA удаленного узла VPN. Для записи в систему открытого ключа RSA удаленного узла используется команда **set vpn rsa-keys** (см. стр. 1233). Указание значения для данного параметра является обязательным при использовании аутентификации на основе криптосистемы RSA (**authentication method plain-rsa**).

**x509-cert** *имя*

Имя сертификата X.509 локального узла VPN. Команды управления сертификатами описаны в разделе Команды управления PKI (см. стр. 1049). 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.

## 17.3.29. 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 [текст]{
                ike-group текст
            }
        }
```

```
        }
    }
```

**Параметры**

*туннель*

Обязательный. Название туннеля к удаленному узлу IPSec.

*группа*

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. 1206).

**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.

## 17.3.30. 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 [текст] {
            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. 1219).

**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.

## 17.3.31. 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 [текст] {
                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. 1219).

**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.

### 17.3.32. 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 [текст] {
                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.

## 17.3.33. 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 Altell NEO.

**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 [текст] {
                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.

## 17.3.34. 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 [текст] {
                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. 1193).

**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.

## 17.3.35. 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 [текст] {
                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. 1195).

**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.

## 17.3.36. 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 [текст] {
                nat-traversal [on | off | force]
            }
        }
    }
}
```

**Параметры**

*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 Altell NEO 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.

## 17.3.37. vpn rsa-key generate

Создание ключевой пары RSA для локальной системы.

**Синтаксис**

**vpn rsa-key generate** [**bits** *16-4096* [**random** *генератор*]]

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*bits*

Указание длины ключа в битах, значение должно быть кратно 16. Значение должно лежать в диапазоне от 16 до 4096. По умолчанию установлено значение 2192.

*генератор*

Указание специального символьного псевдоустройства, предоставляющего интерфейс к системному генератору случайных чисел. Поддерживаемые значения:

**/dev/random**: Использование специального символьного псевдоустройства /dev/random, предоставляющего интерфейс к системному генератору случайных чисел, который выводит шумы из драйверов устройств и других источников в пул энтропии (entropy pool). Генератор также сохраняет необходимое количество битов шума в этом пуле и формирует из него случайные числа. Использование данного устройства позволяет достичь очень высокого коэффициента случайности. Но следует учитывать, что если пул энтропии пуст, попытка чтения **/dev/random** приведёт к задержке, пока не будет собран дополнительный окружающий шум.

**/dev/urandom**: Использование псевдоустройства **/dev/urandom**, предоставляющего интерфейс к программному генератору случайных чисел.

По умолчанию используется устройство **/dev/random**.

**Указания по использованию**

Данная команда используется для генерации ключевой пары RSA для локального устройства. Данная команда доступна только для пользователей, обладающих правами администратора.

Для использования криптосистемы RSA для аутентификации, необходимо создать ключевую пару для локального устройства.

Ключевая пара состоит из открытого и закрытого ключа, открытый ключ должен быть доставлен на удаленный узел. Закрытый ключ должен сохраняться в секрете. Данная команда в эксплуатационном режиме позволяет создать ключевую пару для локального устройства, после создания ключевая пара содержится в файле, определяемом параметром **local-key rsa-key-name**, по умолчанию используется файл **localhost.key** в директории **/opt/vyatta/etc/config/ipsec.d/rsa-keys/**. Файл в котором хранится ключевая пара может быть задан при помощи команды **vpn rsa-keys** (см. стр. 1233).

Использование устройства **/dev/random** более безопасно по сравнению с использованием **/dev/urandom**, но при этом следует учитывать что генерация ключевой пары может занять длительное время.

## 17.3.38. vpn rsa-keys

Добавление в локальную систему записи о ключах RSA.

**Синтаксис**

**set vpn rsa-keys** [**local-key file** *file-name* | **rsa-key-name** *name* **rsa-key** *key*]

**delete vpn rsa-keys local-key file** [**local-key file** | **rsa-key-name** [*name* **rsa-key**]]

**show vpn rsa-keys local-key file** [**local-key file** | **rsa-key-name** [*name* **rsa-key**]]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
vpn {
    rsa-keys {
```

```
            local-key {
                file текст
            }
            rsa-key-name текст {
                rsa-key текст
            }
        }
    }
```

**Параметры**

**local-key file** *имя_файла*

Указание имени и месторасположения файла, содержащего ключевую пару RSA локального устройства. По умолчанию созданная ключевая пара записывается в файл /opt/vyatta/etc/config/ipsec.d/rsa-keys/localhost.key.

**rsa-key-name** *имя*

Мнемоническое имя удаленного открытого ключа, которое указывается при настройке использования RSA в параметрах подключения в межфилиальном режиме.

**rsa-key** *ключ*

Открытый ключ RSA удаленного узла.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда используется для отображения или изменения месторасположения файла, содержащего ключевую пару RSA данного устройства, а также для записи в данной системе открытого ключа RSA удаленного устройства. Ключевая пара RSA может быть сгенерирована для данного устройства при помощи команды **vpn rsa-key generate command** (см. стр. 1232) в эксплуатационном режиме. Созданный ключ хранится в файле, определяемом параметром **local-key file**. По умолчанию используется файл **localhost.key** в директории /opt/vyatta/etc/config/ipsec.d/rsa-keys/.

При использовании криптосистемы RSA для аутентификации узлов,

необходимо внести в систему открытый ключ удаленного узла, имя ключа затем должно быть указано в параметрах подключения.

Форма **set** данной команды используется для создания настройки ключа RSA.

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

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

# 18. VPN УДАЛЕННОГО ДОСТУПА

В этом разделе описано, как настроить доступ VPN для удаленных пользователей.

В этом разделе рассматриваются следующие вопросы:

- Настройка VPN удаленного доступа.
- Команды VPN удаленного доступа.

## 18.1. Настройка VPN удаленного доступа

В данном разделе описано, как настроить виртуальную частную сеть (VPN) для предоставления доступа удаленным пользователям.

В этом разделе рассматриваются следующие вопросы:

- Обзор VPN удаленного доступа.
- Примеры настройки VPN удаленного доступа.

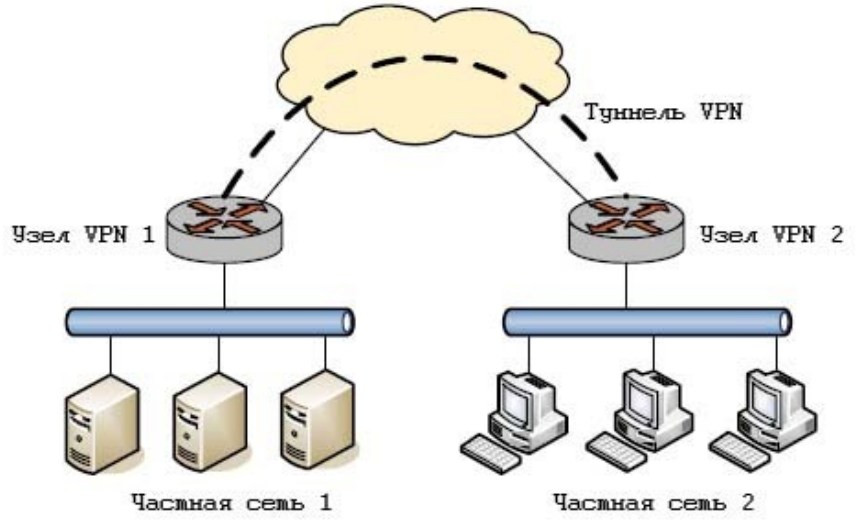
### 18.1.1. Обзор VPN удаленного доступа

В этом разделе рассматриваются следующие вопросы:

- VPN удаленного доступа на основе протокола PPTP.
- VPN удаленного доступа на основе протоколов L2TP/IPSec с использованием предварительных ключей.
- VPN удаленного доступа на основе протоколов L2TP/IPSec с использованием сертификатов стандарта X.509.
- VPN удаленного доступа на основе использования IPSec в межфилиальном режиме.

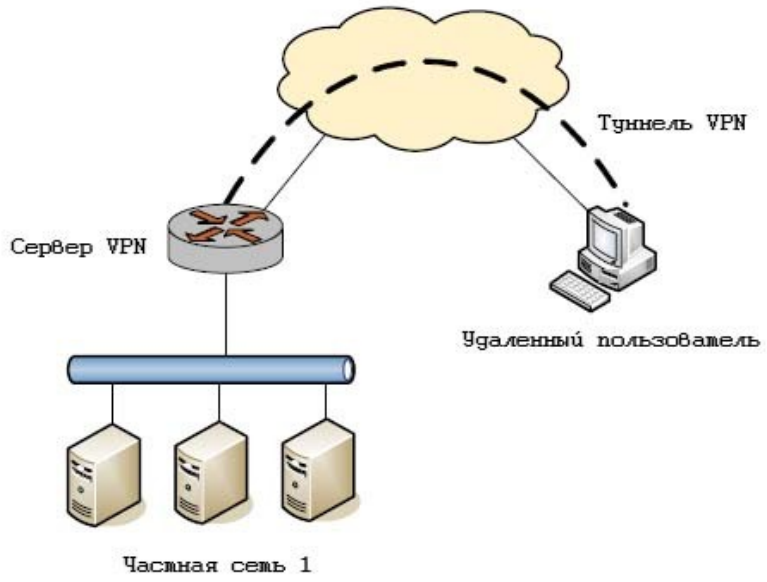
На данный момент в системе Altell NEO поддерживаются следующие механизмы построения виртуальных частных сетей: VPN с использованием межфилиального режима, а также VPN удаленного доступа (Remote Access VPN). Виртуальная частная сеть в межфилиальном режиме может быть построена на базе IPSec или OpenVPN. В межфилиальном режиме соединение VPN может быть установлено между двумя или более удаленными частными сетями, которые “объединяются” в единую сеть, как показано на рисунке 67.

*Рисунок 67 - Межфилиальный режим VPN*




При использовании VPN удаленного доступа Altell NEO функционирует в качестве сервера VPN, к которому подключаются удаленные пользователи, являющиеся клиентами VPN. Обычно виртуальные частные сети такого типа используются для обеспечения удаленного доступа сотрудников к ресурсам корпоративной сети через сеть Интернет. В этом случае удаленный пользователь может получить те же возможности по использованию внутренних ресурсов сети, как если бы он был подключен к ней напрямую. Данный вариант построения VPN приведен на рисунке 68.

*Рисунок 68 - VPN удаленного доступа*




Для реализации VPN удаленного доступа могут быть использованы технологии, поддерживаемые клиентами под управлением ОС Windows. Данная ОС имеет встроенные средства для организации VPN на основе протокола PPTP (Point-to-Point Tunnelling Protocol), а также протоколов L2TP/IPSec (Layer 2 Tunneling Protocol).

Клиент L2TP/IPSec под управлением ОС Windows поддерживает два механизма аутентификации IPSec:

- С использованием предварительных ключей (PSK), которые могут быть использованы взаимодействующими узлами IPSec для проверки подлинности друг друга. Проверка подлинности основывается на том факте, что предварительный ключ хранится в секрете и известен только соответствующим узлам IPSec.
- С использованием сертификатов стандарта X.509, действие которых основано на криптографии с открытым ключом.

Для клиентов L2TP/IPSec поддерживается как механизм аутентификации с использованием предварительных ключей, так и режим с использованием сертификатов X.509. Таким образом, в системе Altell NEO поддерживаются три различных варианта построения VPN удаленного доступа:

- PPTP.
- L2TP/IPSec с аутентификацией на основе предварительных ключей.

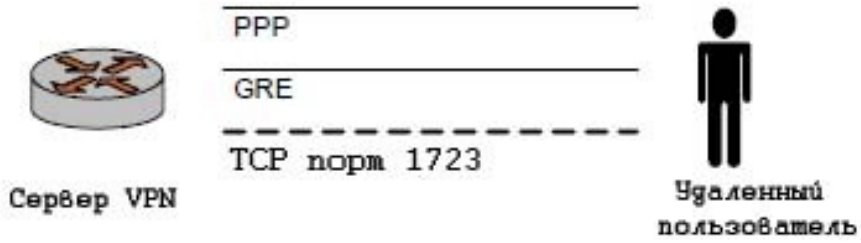
- L2TP/IPSec с аутентификацией на основе сертификатов стандарта X.509.

  Также VPN удаленного доступа может быть организована на основе OpenVPN, этот способ подробно рассматривается в разделе OpenVPN.

#### *18.1.1.1. VPN удаленного доступа на основе PPTP*

При использовании данного метода построения VPN удаленный пользователь устанавливает сеанс PPTP с сервером VPN, как показано на рисунке 69.

*Рисунок 69 - VPN удаленного доступа —PPTP*




1. Удаленный клиент устанавливает соединение TCP с сервером по порту 1723.
2. Через установленное соединение TCP, клиент и сервер PPTP устанавливают туннель GRE (Generic Routing Encapsulation).
3. Сеанс протокола PPP (Point-to-Point Protocol) устанавливается поверх туннеля GRE; то есть, пакеты PPP инкапсулируются и отправляются/принимаются через туннель GRE.

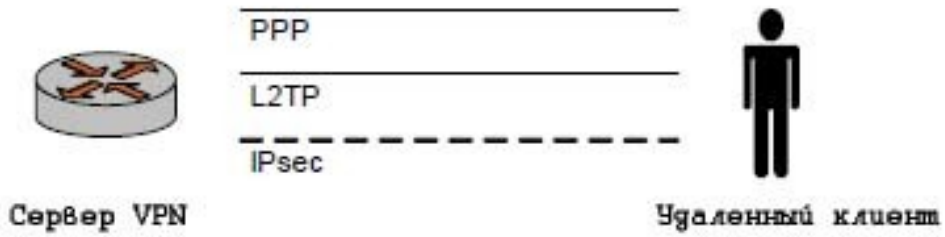
В этом случае аутентификация пользователей и шифрование данных осуществляется на уровне PPP, при помощи комбинации имени и пароля с использованием протокола MS CHAPv2 для аутентификации и протокола MPPE для шифрования.

Безопасность данного решения напрямую зависит от стойкости паролей, которые используются пользователями. Как следствие этого, решения на базе PPTP слабее по сравнению с другими решениями.

#### *18.1.1.2. VPN удаленного доступа на основе L2TP/IPSec с использованием предварительных ключей*

При использовании данного метода построения VPN удаленный пользователь устанавливает сеанс L2TP/IPSec с сервером VPN, как показано на рисунке 70.

*Рисунок 70 - VPN удаленного доступа — L2TP/IPSec с использованием предварительно распределяемых ключей*




1. Удаленный клиент сначала устанавливает туннель IPSec к серверу VPN.
2. Затем клиент и сервер L2TP устанавливают туннель L2TP поверх туннеля IPSec.
3. После чего поверх туннеля L2TP устанавливается сеанс PPP; то есть, пакеты PPP инкапсулируются и отправляются/принимаются через туннель L2TP.

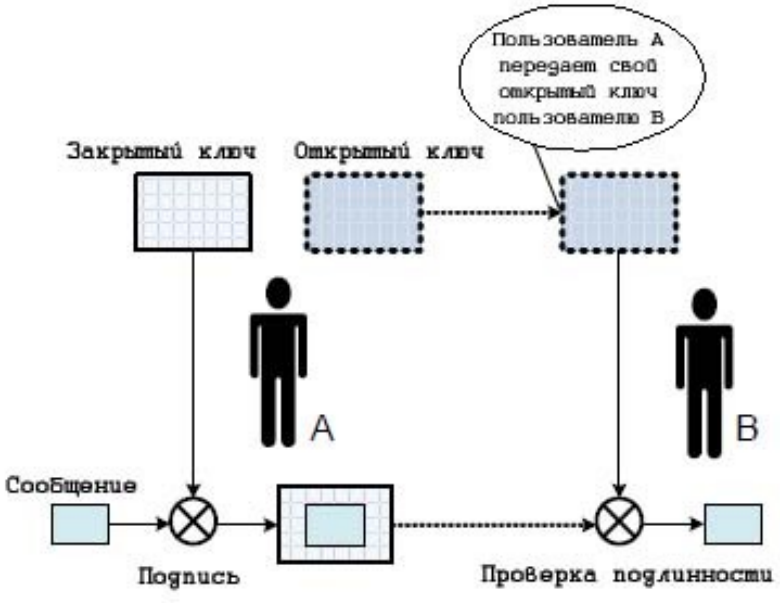
В этом случае на уровне PPP (с использованием имени и пароля) осуществляется только аутентификация пользователей. Шифрование данных обеспечивается средствами IPSec. Более того, для того чтобы осуществить шифрование, IPSec также требует аутентификации (использование IPSec в режиме, при котором осуществляется 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.

#### *18.1.1.3. VPN удаленного доступа с использованием L2TP/IPSec на основе сертификатов стандарта X.509*

На рисунке 71 приведена концептуальная схема работы электронной цифровой подписи.

*Рисунок 71 - Схема работы механизма электронной цифровой подписи*

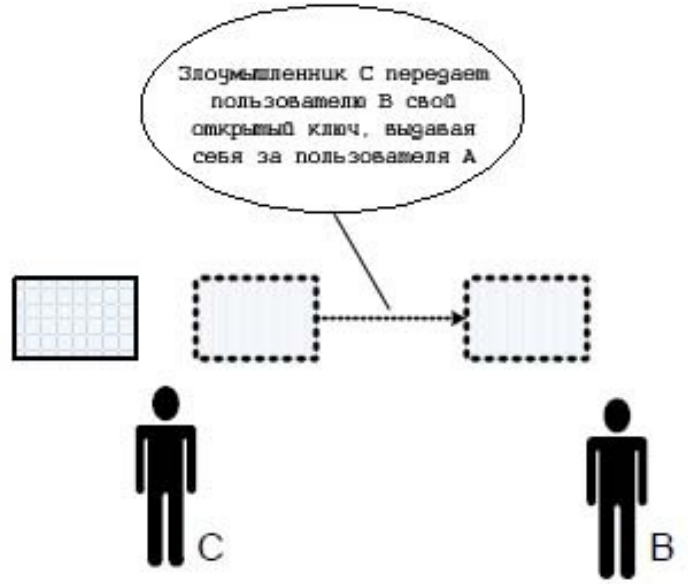



1. Узлы А и В взаимодействуют между собой. Узел А обладает ключевой парой, состоящей из открытого ключа и секретного ключа. Узел А передает свой открытый ключ узлу В.
2. Узел А “подписывает” (шифрует) сообщение с использованием своего секретного ключа и отправляет подписанное (зашифрованное) сообщение и исходное сообщение узлу В.
3. Узел В может “верифицировать” подпись (проверить подлинность подписи), расшифровав ее с использованием открытого ключа узла А и сравнив результат с исходным сообщением.

Как следствие, узел В может аутентифицировать узел А (проверить его подлинность), попросив узел А подписать сообщение и затем проверив подпись с использованием открытого ключа узла А. Так как секретный ключ А не известен никому кроме узла А, только он сможет создать подпись, которая затем будет верифицирована при помощи открытого ключа узла А.

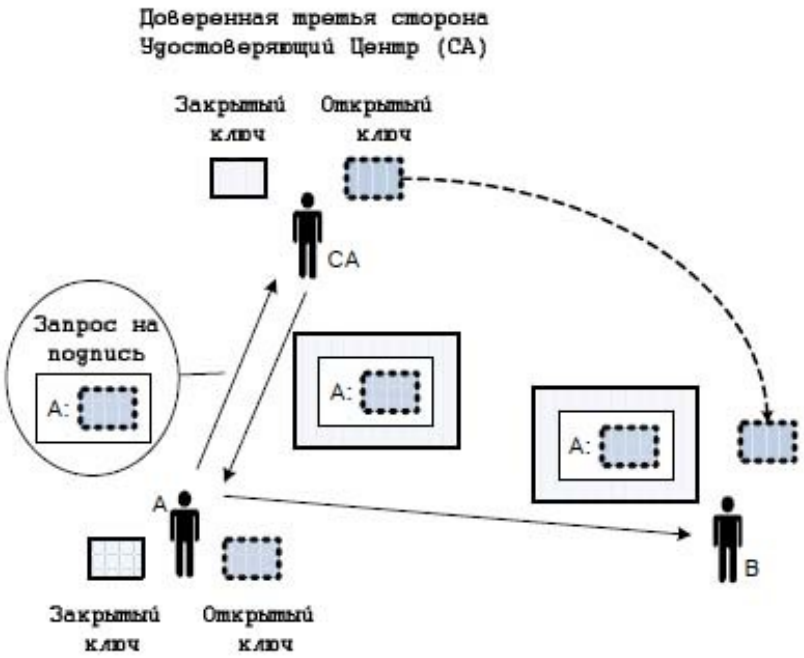
Проблема данной схемы аутентификации заключается в том, что узел В должен убедиться в том, что ключ который он получил, действительно является открытым ключом узла А. Например, на рисунке 72, злоумышленник С выдает себя за узел А и отправляет узлу В другой открытый ключ.

*Рисунок 72 - Атака "человек посередине"*




На практике эта проблема решается при помощи инфраструктуры открытых ключей (PKI), которая основана на доверенной третьей стороне - удостоверяющем центре (Certification Authority). На рисунке 73 приведена концептуальная схема работы инфраструктуры открытых ключей.

*Рисунок 73 - Доверенная третья сторона: Удостоверяющий центр*




1. Узлы A и B доверяют удостоверяющему центру (CA).
2. Узел A просит удостоверяющий центр подписать сообщение, верифицирующее открытый ключ узла A.
3. Удостоверяющий центр подписывает сообщение при помощи своего секретного ключа. Данное сообщение называется сертификатом.
4. Узел A передает сертификат узлу B.
5. Узел B верифицирует сертификат узла A (и, следовательно, открытый ключ узла A) при помощи открытого ключа удостоверяющего центра.

Стандарт X.509 определяет форматы данных и процедуры распределения общих ключей с помощью сертификатов с цифровыми подписями, которые предоставляются сертификационными органами (CA). Приведенная выше схема, L2TP/IPSec VPN с использованием сертификатов X.509 функционирует следующим образом.

1. Сетевой администратор получает сертификат, подписанный удостоверяющим центром для каждого удаленного пользователя, (например, для пользователя A) и распространяет их, совместно с пользовательскими открытыми/секретными ключами, пользователям через безопасные каналы.
2. Сетевой администратор настраивает сервер VPN (например, на узле B) 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.
5. После чего сервер может использовать данный открытый ключ для аутентификации, как указано выше.
6. 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.

#### *18.1.1.4. VPN удаленного доступа на основе использования IPSec в межфилиальном режиме*

Altell NEO поддерживает организацию доступа для удаленных клиентов, имеющих динамические адреса, с использованием межфилиального режима IPSec. Данный вопрос подробно описан в разделе Узлы VPN, имеющие динамические IP-адреса на стр. 1178.

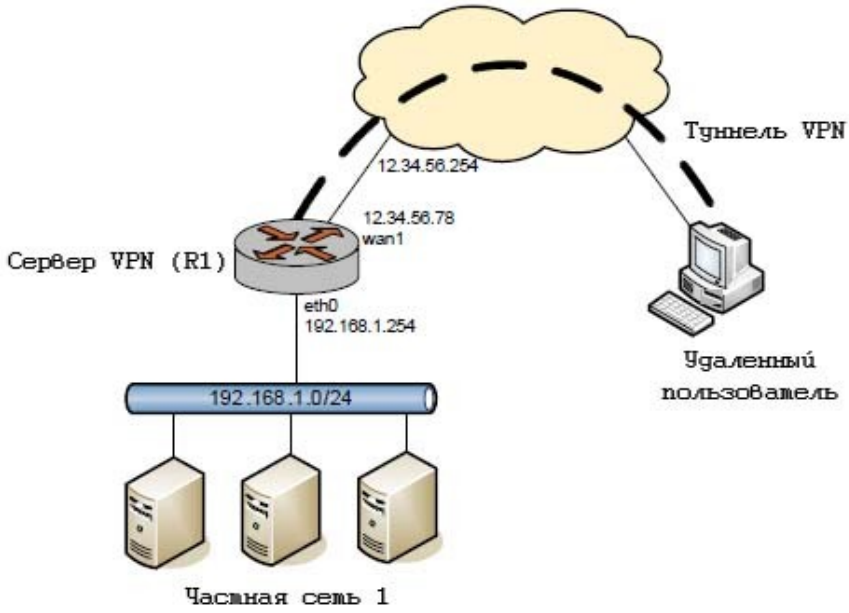
### 18.1.2. Примеры настройки VPN удаленного доступа

В этом разделе рассматриваются следующие вопросы:

- Пример организации VPN на базе протокола PPTP.
- Пример организации VPN на базе протоколов L2TP/IPSec с использованием аутентификации на основе предварительных ключей.
- Настройка трафика Интернет при использовании VPN.

В данном разделе приведены примеры настройки двух приведенных выше схем построения VPN удаленного доступа: на базе протокола PPTP, а также на базе протоколов L2TP/IPSec с использованием аутентификации на основе предварительных ключей. Каждый из приведенных примеров реализует схему, представленную на рисунке 74:

*Рисунок 74 - Пример настройки VPN удаленного доступа*




### *18.1.2.1. Пример построения VPN на базе протокола PPTP*

На первом этапе настройки удаленного доступа клиента под управлением ОС Windows XP на базе протокола PPTP необходимо настроить систему Altell NEO в качестве сервера PPTP. В данном примере настраиваемая система имеет имя R1. Предполагается, что на устройстве R1 настроен внешний IP-адрес 12.34.56.78 и внутренний IP-адрес 192.168.1.254. За данным устройством располагается внутренняя сеть с адресом 192.168.1.0/24, к которой необходимо обеспечить доступ для удаленного пользователя.

Для того чтобы настроить сервер PPTP, необходимо выполнить следующие действия на устройстве R1 в режиме настройки:

*Пример 18.1 - VPN удаленного доступа на базе протокола PPTP*

| Действие | Команда |
|---|---|
| Привязка сервера PPTP ко внешнему адресу. | admin@R1# **set vpn pptp remote-access outside-address 12.34.56.78**<br>[edit] |

Установка пула IP-адресов, которые будут присваиваться удаленным клиентам.

В этом случае доступными будут 10 адресов — в диапазоне от .101 до .110.

```
admin@R1# set vpn pptp remote-access client-ip-pool start 192.168.1.101
[edit]
admin@R1# set vpn pptp remote-access client-ip-pool stop 192.168.1.110
[edit]
```

Установка режима аутентификации - в данном случае режима локальной аутентификации (local).

```
admin@R1# set vpn pptp remote-access authentication mode local
[edit]
```

Установка имени пользователя (**testuser**) и пароля (**testpassword**).

```
admin@R1# set vpn pptp remote-access authentication local-users username testuser password testpassword
[edit]
```

Фиксация изменений.

```
admin@R1# commit
[edit]
```

Вывод настройки.

```
admin@R1# show vpn pptp remote-access
authentication {
   local-users {
      username testuser{
         password testpassword
      }
   }
mode local
}
client-ip-pool {
   start 192.168.1.101
```

```
    stop 192.168.1.110
}
outside-address 12.34.56.78
[edit]
```

Следующим шагом является настройка клиента PPTP VPN в ОС Windows XP SP2 (удаленный пользователь в данном примере). Для этого можно использовать “**New Connection Wizard**” ("Мастер нового подключения").

1. Следует выбрать **Start** (**Пуск**) > **Control Panel** (**Панель управления**) > **Network Connections** (**Сетевые подключения**).
2. Выбрать **Create a new connection** (**Создание нового подключения**). После чего запустится **New Connection Wizard** (**Мастер нового подключения**). Нажать на кнопку **Next**.
3. Выбрать **Connect to the network at my workplace** (**Подключить к сети на рабочем месте**). Нажать на кнопку **Next**.
4. Выбрать **Virtual Private Network connection** (**Подключение к виртуальной частной сети**). Нажать на кнопку **Next**.
5. Ввести имя подключения; например “PPTP.” Нажать на кнопку **Next**.
6. Выбрать **Do not dial the initial connection** (**Не набирать номер для предварительного подключения**). Нажать на кнопку **Next**.
7. Ввести адрес сервера VPN (12.34.56.78 в данном примере). Нажать на кнопку **Next**.
8. Выбрать **Do not use my smart card**. Нажать на кнопку **Next**.
9. Нажать на кнопку **Finish** (**Готово**).

Для подключения к серверу VPN, следует дважды щелкнуть на значке подключения VPN, ввести имя пользователя (“testuser” в данном примере) и пароль (“testpassword” в данном примере), а затем нажать на кнопку **Connect** (**Подключить**).

***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. (Следует проверить настройки межсетевого экрана, шлюз, модем DSL, ISP, и т.д.)*

#### *18.1.2.2. Пример построения VPN на базе L2TP/IPSec с использованием аутентификации на основе предварительных ключей*

На первом этапе настройки удаленного доступа необходимо настроить систему Altell NEO в качестве сервера VPN на основе L2TP/IPSec. В данном примере настраиваемая система имеет имя R1. Предполагается, что на устройстве R1 настроен внешний IP-адрес 12.34.56.78 и внутренний IP-адрес 192.168.1.254. За данным устройством располагается внутренняя сеть с адресом 192.168.1.0/24, к которой необходимо обеспечить доступ для удаленного пользователя.

*Пример 18.2 - VPN удаленного доступа с использованием L2TP/IPSec*

| Действие | Пример |
|---|---|
| Привязка сервера L2TP ко внешнему адресу. | admin@R1# **set vpn l2tp remote-access outside-address 12.34.56.78**<br>[edit] |
| Установка пула IP-адресов, которые будут присваиваться удаленным клиентам VPN.<br>В данном случае доступными будут 10 адресов - от .101 до .110. | admin@R1# **set vpn l2tp remote-access client-ip-pool start 192.168.1.101**<br>[edit]<br>admin@R1# **set vpn l2tp remote-access client-ip-pool stop 192.168.1.110**<br>[edit] |
| Установка использования предварительных ключей в качестве режима аутентификации IPSec. | admin@R1# **set vpn l2tp remote-access ipsec-settings authentication method pre-shared-key**<br>[edit] |
| Установка предварительно распределяемого ключа. | admin@R1# **set vpn l2tp remote-access ipsec-settings authentication pre-shared-key ! secrettext!** |

| Действие | Пример |
|---|---|
| | `[edit]` |
| Установка режима аутентификации L2TP в "**local**". | `admin@R1# set vpn l2tp remote-access authentication mode local`<br>`[edit]` |
| Указание имени пользователя и пароля для удаленного доступа L2TP. | `admin@R1# set vpn l2tp remote-access authentication local-users username testuser password testpassword`<br>`[edit]` |
| Фиксация изменений. | `admin@R1# commit`<br>`[edit]` |
| Вывод настройки удаленного доступа l2tp. | `admin@R1# show vpn l2tp remote-access`<br>`authentication`<br>`{`<br>`  local-users {`<br>`  username testuser {`<br>`  password testpassword`<br>`  }`<br>`  }`<br>`  mode local`<br>`}`<br>`client-ip-pool {`<br>`  start 192.168.1.101`<br>`  stop 192.168.1.110`<br>`}`<br>`ipsec-settings {`<br>`  authentication {`<br>`  method pre-shared-key` |

| Действие | Пример |
| --- | --- |
| | pre-shared-key !secrettext!<br>}<br>}<br>outside-address 12.34.56.78<br>[edit] |

Следующим шагом является настройка клиента L2TP/IPSec в ОС Windows XP SP2 (удаленный пользователь в данном примере). Для этого можно использовать "**New Connection Wizard**" ("**Мастер нового подключения**").

1. Следует выбрать **Start** (**Пуск**) > **Control Panel** (**Панель управления**) > **Network Connections** (**Сетевые подключения**).
2. Нажать **Create a new connection** (**Создание нового подключения**). Запустится **New Connection Wizard** (**Мастер нового подключения**). Нажать на кнопку **Next**.
3. Выбрать **Connect to the network at my workplace** (**Подключить к сети на рабочем месте**). Нажать на кнопку **Next**.
4. Выбрать **Virtual Private Network connection** (**Подключение к виртуальной частной сети**). Нажать на кнопку **Next**.
5. Ввести имя подключения; например "L2TP." Нажать на кнопку **Next**.
6. Выбрать **Do not dial the initial connection** (**Не набирать номер для предварительного подключения**). Нажать на кнопку **Next**.
7. Ввести адрес сервера VPN (12.34.56.78 в данном примере). Нажать на кнопку **Next**.
8. В том случае, если запрашивается, выбрать "**Do not use my smart card**" (**Не использовать мою смарт-карту**). Нажать на кнопку **Next**.
9. Нажать на кнопку **Finish** (**Готово**).

По умолчанию, после создания настройки VPN, предварительно распределяемый ключ не настроен, и его необходимо добавить.

1. Следует выбрать "**Network Connections**" (**Сетевые подключения**) в "**Control Panel**" (**Панели управления**).
2. Нажать правой кнопкой мыши на значке "L2TP" (название соответствует ранее указанному). Выбрать "**Properties**" (**Свойства**).
3. Щелкнуть на вкладке "**Безопасность**". Нажать на кнопку "**IPSec Settings...**"

(**Параметры IPSec**).

4. Отметить “**Use pre-shared key for authentication**” (**Для проверки подлинности использовать предварительный ключ**).
5. Ввести предварительный ключ (!secrettext! в данном примере) в поле “**Key**” (**Ключ**).
6. Нажать на кнопку “OK”. Для подключения к серверу VPN, следует дважды щелкнуть на значке “L2TP”, ввести имя пользователя (“testuser” в данном примере) и пароль (“testpassword” в данном примере), после чего нажать на кнопку “**Connect**” (**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. (Следует проверить настройки межсетевого экрана, шлюз, модем DSL, ISP, и т.д.)*

#### *18.1.2.3. Аутентификация клиентов PPTP и L2TP на основе протокола LDAP*

В системе Altell NEO существует возможность настроить проверку подлинности клиентов PPTP и L2TP с использованием службы каталога на основе протокола LDAP.

Для этого необходимо настроить параметры подключения к серверу LDAP при помощи команд **system ldap-server** (см. разделы 3.3.43. - 3.3.51. ).

Для того чтобы использовать аутентификацию клиентов PPTP и L2TP на основе LDAP, необходимо чтобы на сервере LDAP были установлены следующие схемы:

- **samba.schema**: стандартная схема, используемая для хранения пользователей и групп Samba (поставляется на компакт-диске с документацией и дополнительным ПО в файле «Межсетевой экран Altell NEO/Серверное ПО/Схемы LDAP/samba.schema»);
- **radius.schema**: модифицированная схема (поставляется на компакт-диске с документацией и дополнительным ПО в файле «Межсетевой экран Altell NEO/Серверное ПО/Схемы LDAP/radius.schema»).

Для всех пользователей, которые должны проходить аутентификацию с использованием LDAP, обязательно должны выполняться следующие условия:

- В учетной записи пользователя на сервере LDAP должны быть использованы классы объектов **radiusprofile** и **sambaSamAccount.**

- Для атрибута **dialupAccess** должно быть установлено значение YES. В том случае если для данного атрибута установлено значение NO, аутентификация отклоняется.
- Для атрибута **radusAuthType** должно быть установлено значение LDAP.

Необходимо учитывать следующие особенности использования различных методов аутентификации при использовании LDAP:

- При аутентификации на основе протокола CHAP в качестве пароля пользователя используется значение атрибута **userPassword**, которое должно храниться на сервере LDAP в виде открытого текста.
- При аутентификации на основе протокола MSCHAP в качестве пароля пользователя может быть использовано значение атрибута **userPassword**, которое должно храниться в открытом тексте, либо значение атрибута **SambaNTPassword,** которое хранится в виде хэш-значения.

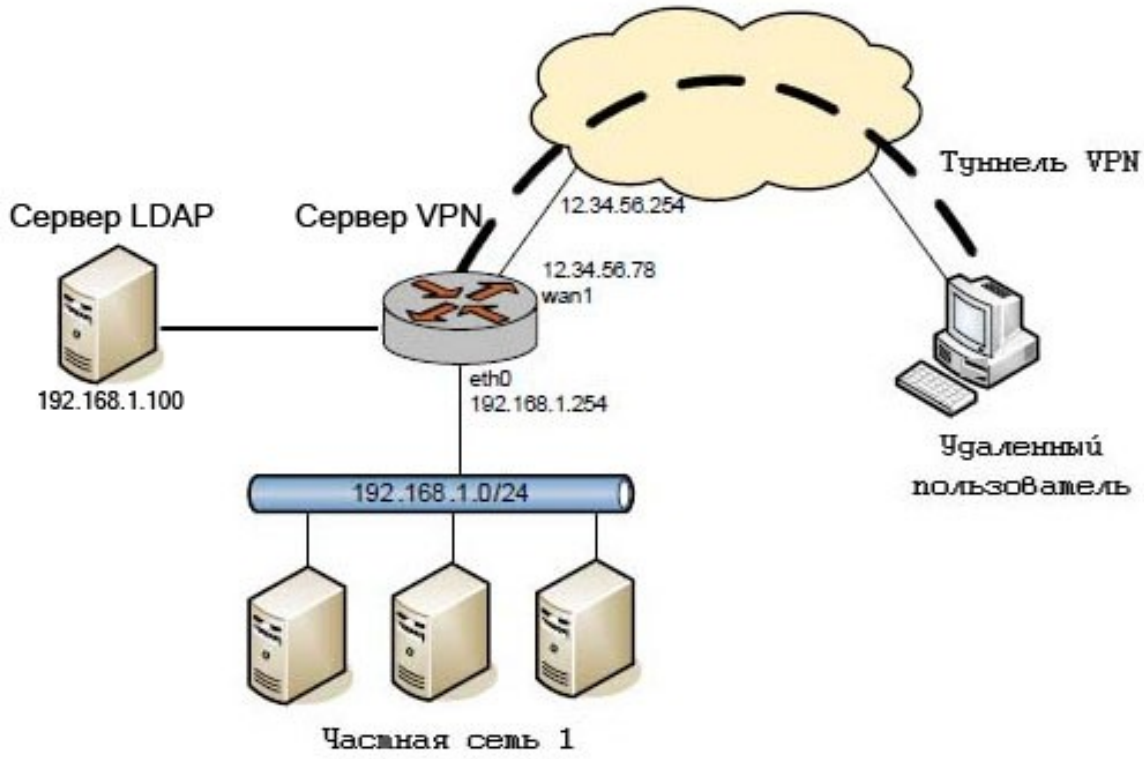
  ***ПРИМЕЧАНИЕ*** *В том случае если включена поддержка паролей LanManager, то пароль пользователя должен также храниться в атрибуте* ***SambaLMPassword****.*

- При аутентификации на основе протокола MSCHAP-V2 в качестве пароля пользователя может быть использовано значение атрибута **userPassword** (которое должно храниться в виде открытого текста), либо значение атрибута **SambaNTPassword**.

На рисунке 75 приведен пример системы, в которой используется удаленная аутентификация клиентов VPN на основе LDAP. В качестве сервера VPN используется Altell NEO. На сервере VPN необходимо указать в качестве используемого метода аутентификации клиентов удаленную аутентификацию на основе LDAP (**authentication mode ldap**), а также настроить параметры подключения сервера VPN к серверу LDAP.

В примере 18.3 приведена настройка параметров подключения к серверу LDAP, который будет использоваться для аутентификации удаленных клиентов VPN.

*Рисунок 75 - Построение VPN удаленного доступа с аутентификацией на основе LDAP*




В примере 18.3 настраиваются параметры подключения к серверу LDAP, который будет использоваться для аутентификации удаленных клиентов VPN.

*Пример 18.3 - Настройка параметров подключения к серверу LDAP*

| Действие | Команда |
|---|---|
| Указание IP-адреса сервера LDAP. | admin@neo# **set system ldap-server host 192.168.1.100**<br>[edit] |
| Указание имени привязки, используемого для подключения к серверу LDAP. | admin@neo# **set system ldap-server dn cn=pppd,dc=example,dc=com**<br>[edit] |
| Указание пароля для аутентификации на | admin@neo# **set system ldap-server** |

| | |
|---|---|
| сервере LDAP. | **password secret**<br>[edit] |
| Указание корневого объекта каталога, начиная от которого необходимо производить поиск пользователей. | admin@neo# **set system ldap-server userbasedn ou=Users,dc=example,dc=com**<br>[edit] |
| Указание корневого объекта каталога, начиная от которого необходимо производить поиск групп пользователей. | admin@neo# **set system ldap-server groupbasedn ou=Groups,dc=example,dc=com**<br>[edit] |
| Указание номера сетевого порта для подключения к серверу LDAP. | admin@neo# **set system ldap-server port 389**<br>[edit] |
| Фиксация настройки. | admin@neo# **commit**<br>[edit] |
| Отображение настройки. | admin@neo# **show system ldap-server**<br>dn cn=pppd,dc=example,dc=com<br>groupbasedn ou=Groups,dc=example,dc=com<br>host 192.168.1.100<br>password secret<br>port 389<br>tls disable<br>userbasedn ou=Users,dc=example,dc=com<br>[edit] |

#### 18.1.2.3.1. Пример настройки сервера PPTP с использованием аутентификации на основе LDAP

В примере 18.4 приведено изменение параметров сервера PPTP для осуществления аутентификации удаленных пользователей на основе LDAP. Все остальные параметры сервера PPTP аналогичны приведенным в примере 18.1. Настройка параметров подключения к серверу LDAP приведена в примере 18.3. После выполнения данного набора примеров конфигурация системы будет соответствовать приведенной на рисунке 75.

*Пример 18.4 - Настройка аутентификации удаленных клиентов PPTP на основе LDAP*

| Действие | Команда |
|---|---|
| Установка аутентификации на основе LDAP. | admin@neo# **set vpn pptp remote-access authentication mode ldap**<br>[edit] |
| Фиксация настройки. | admin@neo# **commit**<br>[edit] |
| Отображение настройки. | admin@neo# **show vpn pptp remote-access**<br>authentication<br>mode ldap<br>client-ip-pool {<br>start 192.168.1.101<br>stop 192.168.1.110<br>}<br>outside-address 12.34.56.78<br>[edit] |

Настройки клиента PPTP аналогичны приведенным ранее.

#### 18.1.2.3.2. Пример настройки сервера L2TP/IPSec с использованием аутентификации на основе LDAP

В примере 18.5 приведено изменение параметров сервера L2TP для осуществления аутентификации удаленных пользователей на основе LDAP. Все остальные параметры сервера L2TP/IPSec аналогичны приведенным в примере 18.2. Настройка параметров

подключения к серверу LDAP приведена в примере 18.3. После выполнения данного набора примеров конфигурация системы будет соответствовать приведенной на рисунке 75.

*Пример 18.5 - Настройка аутентификации удаленных клиентов L2TP на основе LDAP*

| Действие | Команда |
|---|---|
| Установка аутентификации на основе LDAP. | admin@neo# **set vpn l2tp remote-access authentication mode ldap**<br>[edit] |
| Фиксация настройки. | admin@neo# **commit**<br>[edit] |
| Отображение настройки. | admin@neo# **show vpn l2tp remote-access**<br>authentication<br>mode ldap<br>}<br>client-ip-pool {<br>start 192.168.1.101<br>stop 192.168.1.110<br>}<br>ipsec-settings {<br>authentication {<br>method pre-shared-key<br>pre-shared-key !secrettext!<br>}<br>}<br>outside-address 12.34.56.78<br>[edit] |

Настройки клиента L2TP аналогичны приведенным ранее.

#### *18.1.2.4. Настройка межсетевого экрана*

Так как интерфейсы для соединений L2TP/PPTP VPN выделяются автоматически

после аутентификации пользователя, применение правил МЭ на выделенный интерфейс осуществляется динамически после того, как пользователь был аутентифицирован и перед тем, как выделенный ему интерфейс был включен.

Применение правил межсетевого экрана к соединениям PPTP/L2TP VPN аналогично применению правил межсетевого экрана к интерфейсам другого типа за исключением того, что правила не будут привязаны к конкретному существующему интерфейсу в данный момент. Они будут применены ко всем L2TP или PPTP интерфейсам, выделенным после аутентификации пользователя. Действие экземпляра межсетевого экрана, примененного к L2TP/PPTP VPN, будет распространяться на пользователей, которые будут устанавливать подключения после применения правил межсетевого экрана, и не будет распространяться на пользователей, которые уже были подключены к серверу на момент применения правил.

Для настройки межсетевого экрана на устройстве V1, необходимо выполнить следующие действия в режиме настройки.

*Пример 18.6 - Настройка межсетевого экрана*

| Действие | Команда |
|---|---|
| Создание узла конфигурации сервера PPTP. | `admin@V1# set vpn pptp`<br>`[edit]` |
| Команды дополнительной настройки сервера PPTP. | `...` |
| Установка правила межсетевого экрана для входящего трафика подключения PPTP. | `admin@V1# set vpn pptp firewall in name rules-in`<br>`[edit]` |
| Команды дополнительной настройки. | `...` |
| Фиксация изменений. | `admin@V1# commit`<br>`[edit]` |
| Вывод настройки сервера PPTP. | `admin@V1# show vpn pptp`<br>`...`<br>`firewall {`<br>`  in {` |

| Действие | Команда |
|---|---|
| | name rules-in<br>}<br>}<br>...<br>[edit] |

Более подробная информация по настройке межсетевого экрана приведена в разделе 14. Настройка межсетевого экрана .

В том случае если используется аутентификация клиентов PPTP/L2TP на основе LDAP, существует возможность в качестве одного из критериев правила межсетевого экрана указать имя или группу пользователя LDAP. Такое правило может быть применено только к интерфейсам VPN PPTP/L2TP, для которых настроена аутентификация на основе LDAP.

Для указания в качестве критерия правила имени пользователя LDAP или имени группы LDAP используется следующий синтаксис:

- **firewall** [**name**|**modify**] **rule** <*номер*> **destination ldap user** <*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.

- **firewall** [**name**|**modify**] **rule** <*номер*> **destination ldap group** <*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.

- **firewall** [**name**|**modify**] **rule** <*номер*> **source ldap user** <*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.

- **firewall** [**name**|**modify**] **rule** <*номер*> **source ldap group** <*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.

В примере 18.7 приведена настройка межсетевого экрана для сервера PPTP, который был настроен ранее в примере 18.4. В данном примере создается экземпляр межсетевого экрана, включающий в себя следующие правила:

- Правило, запрещающее прохождение сетевых пакетов предназначенных компьютеру в локальной сети, имеющему адрес 192.168.1.10, отправителем которых является клиент PPTP, который был аутентифицирован на основе учетной записи пользователя LDAP с именем **testuser**.

*Пример 18.7 - Настройка межсетевого экрана для сервера PPTP*

| Действие | Команда |
|---|---|
| Добавление экземпляра межсетевого экрана. | admin@neo# **set firewall name example**<br>[edit] |
| Изменение действия по умолчанию. | admin@neo# **set firewall name example default-action accept**<br>[edit] |
| Установка действия, которое будет применено к сетевым пакетам, прошедшим проверку на соответствие правилу 1. | admin@neo# **set firewall name example rule 1 action reject**<br>[edit] |
| Установка адреса получателя в качестве критерия проверки для правила. | admin@neo# **set firewall name example rule 1 destination address 192.168.1.10**<br>[edit] |
| Установка имени пользователя LDAP в качестве критерия проверки для правила. | admin@neo# **set firewall name example rule 1 source ldap user testuser** |

| | |
|---|---|
| | [edit] |
| Фиксация настройки. | admin@neo# **commit**<br>[edit] |
| Применение экземпляра межсетевого экрана в настройке сервера PPTP. | admin@neo# **set vpn pptp firewall in name example**<br>[edit] |
| Фиксация настройки. | admin@neo# **commit**<br>[edit] |

Применение правил межсетевого экрана для клиентов сервера L2TP аналогично применению правил для клиентов сервера PPTP.

#### *18.1.2.5. 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, трафик Интернет будет маршрутизироваться через VPN. В том случае, если требуется сохранить текущий маршрут для трафика Интернет, следует настроить VPN следующим образом:

1. Следует выбрать **Start** (**Пуск**) > **Control Panel** (**Панель управления**) > **Network Connections** (**Сетевые подключения**).
2. Нажать правой кнопкой мыши на значке подключения VPN ("PPTP" в первом примере). Выбрать **Properties** (**Свойства**).
3. Выбрать вкладку **Networking** (**Сеть**). Выбрать "**Internet Protocol (TCP/IP)**" (**Протокол Интернета (TCP/IP)**), 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.

## 18.2. Команды VPN удаленного доступа

В этом разделе приведены следующие команды.

*Таблица 43 - Команды VPN удаленного доступа*

| | |
|---|---|
| Команды настройки | |
| Общие команды IPSec | |
| `vpn ipsec logging` | Данная команда приведена в разделе Межфилиальный режим IPSec . |
| Сервер L2TP | |
| `vpn l2tp` | Создание узла конфигурации для L2TP VPN. |
| `vpn l2tp remote-access authentication mode <режим>` | Указание режима аутентификации пользователей для подключений L2TP VPN. |
| `vpn l2tp remote-access authentication local-users username <имя_пользователя>` | Указание имени пользователя для аутентификации удаленных пользователей L2TP VPN. |
| `vpn l2tp remote-access client-ip-pool start <ipv4-адрес>` | Указание начального адреса пула IP-адресов, которые будут назначаться удаленным клиентам L2TP VPN. |
| `vpn l2tp remote-access client-ip-pool stop <ipv4-адрес>` | Указание конечного адреса пула IP-адресов, которые будут назначаться удаленным клиентам L2TP VPN. |
| `vpn l2tp remote-access dns-servers server-1 <ipv4-адрес>` | Указание IP-адреса основного сервера DNS для удаленных клиентов L2TP VPN. |
| `vpn l2tp remote-access dns-servers server-2 <ipv4-адрес>` | Указание IP-адреса вторичного сервера DNS для удаленных клиентов L2TP VPN. |
| `vpn l2tp remote-access ipsec-settings authentication method <режим>` | Установка режима, который будет использоваться при IPSec аутентификации подключений удаленного доступа L2TP VPN. |
| `vpn l2tp remote-access ipsec-settings` | Установка предварительного ключа, используемого при аутентификации IPSec |

| | |
|---|---|
| | подключений удаленного доступа L2TP VPN. |
| `vpn l2tp remote-access ipsec-settings authentication x509-cert <сертификат>` | Указание сертификата X.509, используемого при аутентификации IPSec подключений удаленного доступа L2TP VPN. |
| `vpn l2tp remote-access outside-address <ipv4-адрес>` | Указание внешнего IP-адреса сервера L2TP, на котором будут ожидаться входящие подключения. |
| `vpn l2tp remote-access wins-servers server-1 <ipv4-адрес>` | Указание IP-адреса основного сервера WINS для удаленных клиентов L2TP VPN. |
| `vpn l2tp remote-access 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 remote-access authentication mode <режим>` | Указание режима аутентификации пользователей для подключений PPTP VPN. |
| `vpn pptp remote-access authentication local-users username <имя_пользователя> password <пароль>` | Указание имени пользователя и пароля для аутентификации удаленных пользователей PPTP VPN. |
| `vpn pptp remote-access client-ip-pool start <ipv4-адрес>` | Указание начального адреса пула IP-адресов, которые будут назначаться удаленным клиентам PPTP VPN. |
| `vpn pptp remote-access client-ip-pool stop <ipv4-адрес>` | Указание конечного адреса пула IP-адресов, которые будут назначаться удаленным клиентам PPTP VPN. |
| `vpn pptp remote-access dns-servers server-1 <ipv4-` | Указание IP-адреса основного сервера DNS для удаленных клиентов PPTP VPN. |

| | |
|---|---|
| `vpn pptp remote-access dns-servers server-2 <ipv4-адрес>` | Указание IP-адреса вторичного сервера DNS для удаленных клиентов PPTP VPN. |
| `vpn pptp remote-access outside-address <ipv4-адрес>` | Указание внешнего IP-адреса сервера PPTP, на котором будут ожидаться входящие подключения. |
| `vpn pptp remote-access wins-servers server-1 <ipv4-адрес>` | Указание IP-адреса основного сервера WINS для удаленных клиентов PPTP VPN. |
| `vpn pptp remote-access 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 Altell NEO. |
| `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> 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 ipsec-process` | Перезапуск процесса IPSec. См. стр. 1186 в разделе Межфилиальный режим IPSec . |
| `clear vpn remote-access user <имя_пользователя>` | Завершение активного сеанса указанного пользователя. |
| `show vpn ipsec sa` | Вывод сведений обо всех активных безопасных соединениях IPSec. См. стр. 1189 в разделе Межфилиальный режим IPSec . |
| `show vpn ipsec status` | Вывод сведений о состоянии процессов IPSec. См. стр. 1191 в в разделе Межфилиальный режим IPSec . |
| `show vpn remote-access` | Вывод сведений о текущих активных сеансах удаленного доступа VPN. |

### 18.2.1. 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 18.8 приведено завершение всех активных сеансов пользователя robert.

*Пример 18.8 - "clear vpn remote access user": Завершение активных сеансов пользователя*

```
admin@neo# clear remote-access user robert
admin@neo#
```

### 18.2.2. 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 18.9 приведен вывод для команды **show vpn remote-access**.

*Пример 18.9 - "show vpn remote-access": Вывод удаленных сеансов VPN*

```
admin@neo# 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:~#
```

### 18.2.3. 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 Altell NEO.

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.

### 18.2.4. vpn l2tp remote-access authentication mode <режим>

Указание режима аутентификации пользователей для подключений L2TP VPN.

**Синтаксис**

**set vpn l2tp remote-access authentication mode** *режим*

**delete vpn l2tp remote-access authentication mode**

**show vpn l2tp remote-access authentication mode**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
vpn {
    l2tp {
        remote-access {
            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 remote-access authentication local-users username** <*имя_пользователя*> (см. стр. 1268), 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.

### 18.2.5. vpn l2tp remote-access authentication local-users username <имя_пользователя>

Указание имени пользователя для аутентификации удаленных пользователей L2TP VPN.

**Синтаксис**

**set vpn l2tp remote-access authentication local-users username** *имя_пользователя* [**disable** | **password** *пароль*]

**delete vpn l2tp remote-access authentication local-users username** *имя_пользователя* [**disable** | **password**]

**show vpn l2tp remote-access authentication local-users username** *имя_пользователя*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
vpn {
    l2tp {
        remote-access {
            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.

### 18.2.6. vpn l2tp remote-access client-ip-pool start <ipv4-адрес>

Указание начального адреса пула IP-адресов, которые назначаются удаленным клиентам L2TP VPN.

**Синтаксис**

**set vpn l2tp remote-access client-ip-pool start** *ipv4-адрес*

**delete vpn l2tp remote-access client-ip-pool start**

**show vpn l2tp remote-access client-ip-pool start**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
vpn {
    l2tp {
        remote-access {
            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 remote-access client-ip-pool start** <*ipv4-адрес*>, а конечный адрес задается командой **vpn l2tp remote-access 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.

## 18.2.7. vpn l2tp remote-access client-ip-pool stop <ipv4-адрес>

Указание конечного адреса пула IP-адресов, которые будут назначаться удаленным клиентам L2TP VPN.

**Синтаксис**

**set vpn l2tp remote-access client-ip-pool stop** *ipv4-адрес*

**delete vpn l2tp remote-access client-ip-pool stop**

**show vpn l2tp remote-access client-ip-pool stop**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
vpn {
    l2tp {
        remote-access {
            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 remote-access client-ip-pool start** <*ipv4-адрес*>, а конечный адрес задается командой **vpn l2tp remote-access 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.

## 18.2.8. vpn l2tp remote-access dns-servers server-1 <ipv4-адрес>

Указание IP-адреса основного сервера DNS для удаленных клиентов L2TP VPN.

**Синтаксис**

**set vpn l2tp remote-access dns-servers server-1** *ipv4-адрес*

**delete vpn l2tp remote-access dns-servers server-1**

**show vpn l2tp remote-access dns-servers server-1**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
vpn {
     l2tp {
          remote-access {
               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.

## 18.2.9. vpn l2tp remote-access dns-servers server-2 <ipv4-адрес>

Указание IP-адреса вторичного сервера DNS для удаленных клиентов L2TP VPN.

**Синтаксис**

**set vpn l2tp remote-access dns-servers server-2** *ipv4-адрес*

**delete vpn l2tp remote-access dns-servers server-2**

**show vpn l2tp remote-access dns-servers server-2**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
vpn {
    l2tp {
        remote-access {
            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.

## 18.2.10. vpn l2tp remote-access ipsec-settings authentication method <режим>

Установка режима, который будет использоваться при IPSec аутентификации подключений удаленного доступа L2TP VPN.

**Синтаксис**

**set vpn l2tp remote-access ipsec-settings authentication method** *режим*

**delete vpn l2tp remote-access ipsec-settings authentication method**

**show vpn l2tp remote-access ipsec-settings authentication method**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
vpn {
    l2tp {
        remote-access {
            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 хэш-значения, для того чтобы оконечные точки могли аутентифицировать друг друга.

При установке режима аутентификации с использованием предварительных ключей, необходимо настроить ключ с помощью команды **vpn l2tp remote-access ipsec-settings authentication pre-shared-key** <*ключ*> (см. стр. 1277).

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 Altell NEO.

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.

### 18.2.11. vpn l2tp remote-access ipsec-settings authentication pre-shared-key <ключ>

Установка предварительного ключа, используемого при IPSec аутентификации подключений удаленного доступа L2TP VPN.

**Синтаксис**

**set vpn l2tp remote-access ipsec-settings authentication pre-shared-key** *ключ*

**delete vpn l2tp remote-access ipsec-settings authentication pre-shared-key**

**show vpn l2tp remote-access ipsec-settings authentication pre-shared-key**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
vpn {
    l2tp {
        remote-access {
            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.

### 18.2.12. vpn l2tp remote-access ipsec-settings authentication x509-cert <сертификат>

Указание пути к файлу сертификата X.509, используемого при аутентификации IPSec подключений удаленного доступа L2TP VPN.

**Синтаксис**

**set vpn l2tp remote-access ipsec-settings authentication x509-cert** *сертификат*

**delete vpn l2tp remote-access ipsec-settings authentication x509-cert**

**show vpn l2tp remote-access ipsec-settings authentication x509-cert**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
vpn {
    l2tp {
        remote-access {
```

```
                    ipsec-settings {
                        authentication {
                            x509-cert текст
                        }
                    }
                }
            }
        }
```

**Параметры**

*сертификат*

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.

## 18.2.13. vpn l2tp remote-access outside-address <ipv4-адрес>

Указание внешнего IP-адреса сервера L2TP, на котором будут ожидаться входящие подключения.

**Синтаксис**

**set vpn l2tp remote-access outside-address** *ipv4-адрес*

**delete vpn l2tp remote-access**

**show vpn l2tp remote-access**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
vpn {
    l2tp {
        remote-access {
            outside-address 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.

## 18.2.14. vpn l2tp remote-access wins-servers server-1 <ipv4-адрес>

Указание IP-адреса основного сервера WINS для удаленных клиентов L2TP VPN.

**Синтаксис**

**set vpn l2tp remote-access wins-servers server-1** *ipv4-адрес*

**delete vpn l2tp remote-access wins-servers server-1**

**show vpn l2tp remote-access wins-servers server-1**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
vpn {
    l2tp {
        remote-access {
            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 основной 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.

### 18.2.15. vpn l2tp remote-access wins-servers server-2 <ipv4-адрес>

Указание IP-адреса вторичного сервера WINS для удаленных клиентов L2TP VPN.

**Синтаксис**

**set vpn l2tp remote-access wins-servers server-2** *ipv4-адрес*

**delete vpn l2tp remote-access wins-servers server-2**

**show vpn l2tp remote-access wins-servers server-2**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
vpn {
    l2tp {
        remote-access {
            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.

## 18.2.16. 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 Altell NEO.

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.

## 18.2.17. vpn pptp remote-access authentication mode <режим>

Указание режима аутентификации пользователей для подключений PPTP VPN.

**Синтаксис**

**set vpn pptp remote-access authentication mode** *режим*

**delete vpn pptp remote-access authentication mode**

**show vpn pptp remote-access authentication mode**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
vpn {
    pptp {
        remote-access {
            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 remote-access authentication local-users username** <*имя_пользователя*> **password** <*пароль*> (см. стр. 1285), 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.

## 18.2.18. vpn pptp remote-access authentication local-users username <имя_пользователя> password <пароль>

Указание имени пользователя и пароля для аутентификации удаленных пользователей PPTP VPN.

**Синтаксис**

```
set vpn pptp remote-access authentication local-users
username имя_пользователя password пароль

delete vpn pptp remote-access authentication local-users
username имя_пользователя [password]

show vpn pptp remote-access authentication local-users
username имя_пользователя [password]
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
vpn {
    pptp {
        remote-access {
            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.

## 18.2.19. vpn pptp remote-access client-ip-pool start <ipv4-адрес>

Указание начального адреса пула IP-адресов, которые будут назначаться удаленным клиентам PPTP VPN.

**Синтаксис**

**set vpn pptp remote-access client-ip-pool start** *ipv4-адрес*

**delete vpn pptp remote-access client-ip-pool start**

**show vpn pptp remote-access client-ip-pool start**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
vpn {
    pptp {
        remote-access {
            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 remote-access client-ip-pool stop <***ipv4-адрес***>** (см. стр. 1288).

Форма **set** данной команды используется для определения начального адреса.

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

Форма **show** данной команды используется для отображения начального адреса.

## 18.2.20. vpn pptp remote-access client-ip-pool stop <ipv4-адрес>

Указание конечного адреса пула IP-адресов, которые будут назначаться удаленным клиентам PPTP VPN.

**Синтаксис**

**set vpn pptp remote-access client-ip-pool stop** *ipv4-адрес*

**delete vpn pptp remote-access client-ip-pool stop**

**show vpn pptp remote-access client-ip-pool stop**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
vpn {
    pptp {
        remote-access {
            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 remote-access client-ip-pool start <***ipv4-адрес***>** (см. стр. 1287).

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.

## 18.2.21. vpn pptp remote-access dns-servers server-1 <ipv4-адрес>

Указание IP-адреса основного сервера DNS для удаленных клиентов PPTP VPN.

**Синтаксис**

**set vpn pptp remote-access dns-servers server-1** *ipv4-адрес*

**delete vpn pptp remote-access dns-servers server-1**

**show vpn pptp remote-access dns-servers server-1**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
vpn {
    pptp {
        remote-access {
            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.

## 18.2.22. vpn pptp remote-access dns-servers server-2 <ipv4-адрес>

Указание IP-адреса вторичного сервера DNS для удаленных клиентов PPTP VPN.

**Синтаксис**

**set vpn pptp remote-access dns-servers server-2** *ipv4-адрес*

**delete vpn pptp remote-access dns-servers server-2**

**show vpn pptp remote-access dns-servers server-2**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
vpn {
    pptp {
        remote-access {
            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.

## 18.2.23. vpn pptp remote-access outside-address <ipv4-адрес>

Указание внешнего IP-адреса сервера PPTP, на котором будут ожидаться входящие подключения.

**Синтаксис**

**set vpn pptp remote-access outside-address** *ipv4-адрес*

**delete vpn pptp remote-access**

**show vpn pptp remote-access**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
vpn {
    pptp {
        remote-access {
            outside-address ipv4-адрес
```

```
                }
            }
        }
```

**Параметры**

*ipv4-адрес*

Обязательный. Внешний IPv4-адрес сервера PPTP, на котором он будет принимать входящие подключения.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда используется для установки внешнего адреса, на котором сервер PPTP будет ожидать входящие подключения.

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 PPTP VPN.

Форма **delete** данной команды используется для удаления настройки внешнего адреса PPTP VPN.

Форма **show** используется для отображения настройки PPTP VPN.

## 18.2.24. vpn pptp remote-access wins-servers server-1 <ipv4-адрес>

Указание IP-адреса основного сервера WINS для удаленных клиентов PPTP VPN.

**Синтаксис**

**set vpn pptp remote-access wins-servers server-1** *ipv4-адрес*

**delete vpn pptp remote-access wins-servers server-1**

**show vpn pptp remote-access wins-servers server-1**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
vpn {
    pptp {
        remote-access {
            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.

## 18.2.25. vpn pptp remote-access wins-servers server-2 <ipv4-адрес>

Указание IP-адреса вторичного сервера WINS для удаленных клиентов PPTP VPN.

**Синтаксис**

**set vpn pptp remote-access wins-servers server-2** *ipv4-адрес*

**delete vpn pptp remote-access wins-servers server-2**

**show vpn pptp remote-access wins-servers server-2**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
vpn {
    pptp {
        remote-access {
            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.

## 18.2.26. interfaces pptp <pptpx>

Создание узла конфигурации клиента PPTP в системе Altell NEO.

**Синтаксис**

**set interfaces pptp** *pptpx*

**delete interfaces pptp**

**show interfaces pptp**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации.**

```
interfaces
    pptp pptp0..pptp99
    {
    }
```

**Параметры**

**pptp***x*

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.

## 18.2.27. 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**

**pptp***x*

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.

## 18.2.28. 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**

**pptp***x*

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.

## 18.2.29. 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**

**pptp***x*

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.

## 18.2.30. 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**

**pptp***x*

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.

## 18.2.31. 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**

**pptp***x*

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.

## 18.2.32. 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.

## 18.2.33. 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
{
}
```

**Параметры**

**pptp***x*

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.

## 18.2.34. 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**

**pptp***x*

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.

## 18.2.35. 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**

**pptp***x*

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.

## 18.2.36. 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
    {
    }
```

**Параметры**

**pptp***x*

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.

# 19. OPENVPN

В этом разделе рассматривается настройка VPN удаленного доступа и настройка VPN в межфилиальном режиме на базе OpenVPN.

В данном разделе рассматриваются следующие вопросы:

- Настройка OpenVPN.
- Команды OpenVPN.

## 19.1. Настройка OpenVPN

В этом разделе рассматриваются следующие вопросы:

- Механизмы безопасности OpenVPN.
- Режимы функционирования OpenVPN.
- Примеры базовой настройки.
- Примеры настройки для использования дополнительных параметров.
- Не поддерживаемые параметры OpenVPN.

### 19.1.1. Механизмы безопасности OpenVPN

В данном разделе представлен краткий обзор механизмов безопасности и режимов эксплуатации OpenVPN.

В этом разделе рассматриваются следующие вопросы:

- Предварительные ключи.
- TLS.

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 предварительных 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.*

#### *19.1.1.1. Предварительные ключи*

При использовании предварительных ключей, OpenVPN функционирует следующим образом:

1. Администратор, используя команду эксплуатационного режима **vpn openvpn-key generate <имя_файла>**, генерирует файл, содержащий определенное число случайных байтов данных. Эти данные представляют собой секретный ключ, который позволит обеспечить безопасность.
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.
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 предварительный ключ известен только второму оконечному устройству; то есть, проверка подлинности осуществляется исходя из предположения, что если некоторому устройству известен предварительный ключ, это устройство является правомерным оконечным устройством.
4. После осуществления проверки подлинности оконечных узлов, OpenVPN формирует на каждой из сторон набор ключей из предварительного ключа. Данные ключи используются в следующих целях:

   - Некоторые из них используется 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.

#### *19.1.1.2. TLS*

TLS — криптографический протокол, обеспечивающий защищённую передачу данных между узлами в сети Интернет, не требующий наличия предварительного 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. (Краткий обзор сертификатов стандарта X.509 приведен в разделе 16. Инфраструктура открытых ключей на стр. 1042.) 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 предварительные 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 предварительные 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.

## 19.1.2. Режимы функционирования OpenVPN

OpenVPN поддерживает как межфилиальный режим, позволяющий создать туннель VPN между двумя маршрутизаторами, так и клиент-серверный режим, позволяющий организовать VPN удаленного доступа. Также доступен прием на клиентской стороне данных настройки от сервера OpenVPN.

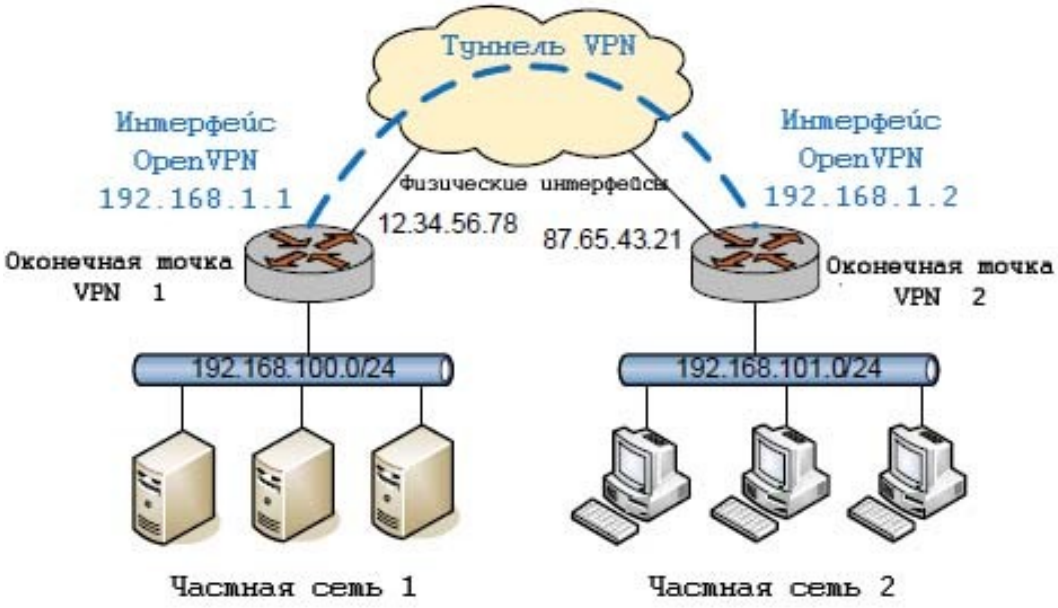
В данном разделе представлена более детальная информация по следующим вопросам:

- Межфилиальный режим.
- Клиент-серверный режим.

### *19.1.2.1. Межфилиальный режим*

На рисунке 76 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 76 - 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 76, IP-адресами туннеля являются адреса 192.168.1.1 и 192.168.1.2.
- Физический IP-адрес: IP-адрес, назначаемый физическому интерфейсу поверх которого устанавливается туннель VPN. В данном примере, физический IP-адресами являются адреса 12.34.56.78 и 87.65.43.21.

В большинстве случаев, туннель VPN используется для передачи трафика между частными подсетями через глобальную вычислительную сеть (WAN). В текущем примере,

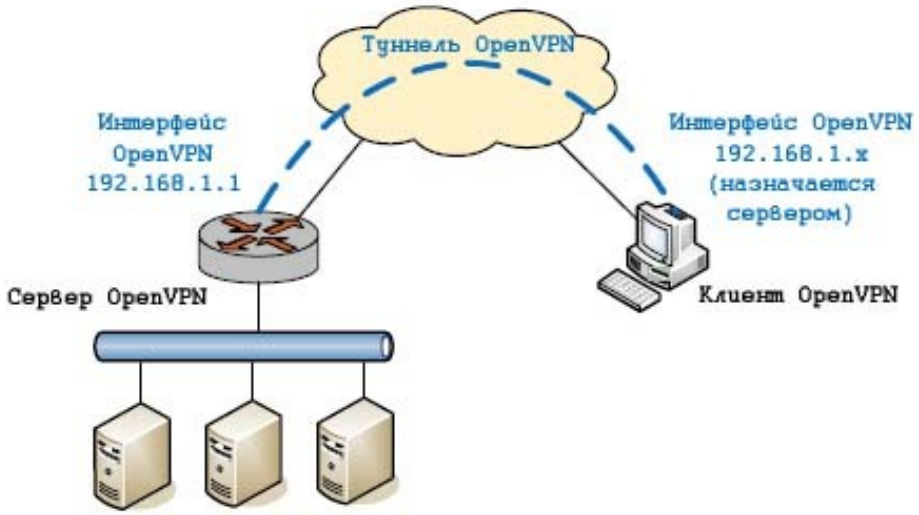
частные сети 192.168.100.0/24 и 192.168.101.0/24 расположены за оконечными узлами туннеля VPN. При этом на каждом оконечном устройстве следует добавить статический маршрут направляющий трафик от и к удаленной частной подсети через туннельный интерфейс.

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.

#### *19.1.2.2. Клиент-серверный режим*

OpenVPN также поддерживает клиент-серверный режим, на базе которого можно построить виртуальную частную сеть удаленного доступа. В этом режиме, одно из оконечных устройств OpenVPN функционирует как сервер, а все остальные удаленные оконечные устройства функционируют как клиенты, которые подключаются к серверу OpenVPN для установления туннелей VPN, таким образом, каждый клиент устанавливает независимый туннель к серверу. Простой пример настройки удаленного доступа VPN приведен на рисунке 77.

*Рисунок 77 - VPN удаленного доступа на базе OpenVPN*




Основное отличие между межфилиальным режимом и клиент-серверным режимом заключается в том, что при использовании клиент-серверного режима все туннели VPN на

стороне сервера привязаны к одному и тому же туннельному интерфейсу. Существование единой точки исключает необходимость назначения отдельного IP-адреса туннельного интерфейса для каждого туннеля VPN. Это более удобно и существенно упрощает настройку удаленного доступа.

Другим отличием является то, что в клиент-серверном режиме, на стороне сервера процесс OpenVPN динамически выделяет туннельные IP-адреса из настроенной подсети (192.168.1.0/24 в примере) вместо использования фиксированных туннельных IP-адресов для оконечных устройств. Таким образом, когда процесс OpenVPN запускается на сервере, он создает туннельный интерфейс и назначает ему IP-адрес из указанной подсети (например, 192.168.1.1). Затем, когда клиент устанавливает туннель VPN с сервером, на стороне сервера процесс OpenVPN также выделяет клиенту IP-адрес из той же подсети (например, 192.168.1.4) и туннельному интерфейсу клиента назначается указанный адрес.

## 19.1.3. 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 предварительных ключей.
- Межфилиальный режим с использованием TLS.
- Клиент-серверный режим.
- Настройка межсетевого экрана.

### *19.1.3.1. Межфилиальный режим с использованием предварительных ключей*

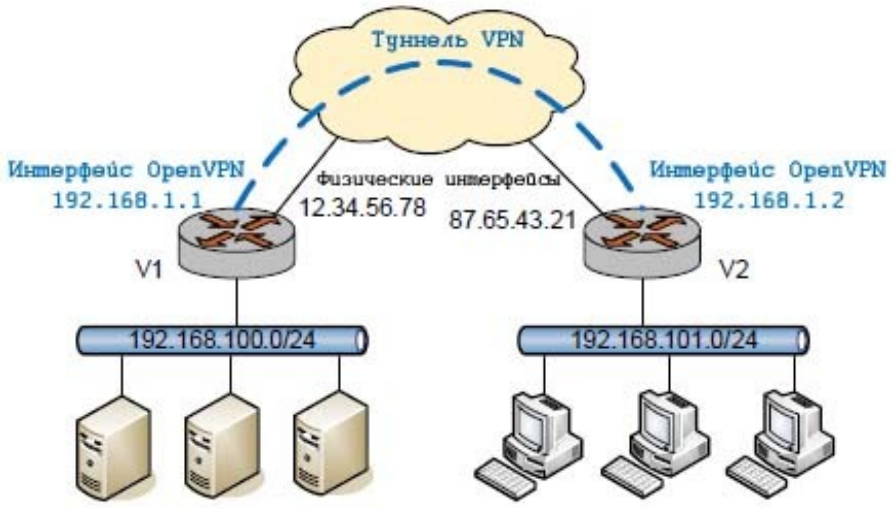
На рисунке 78 приведен вариант подключения VPN в межфилиальном режиме между узлами V1 и V2 с использованием предварительных ключей. В данном примере:

- Физические IP-адреса для узлов V1 и V2 - 12.34.56.78 и 87.65.43.21соответственно.
- Туннельные IP-адреса для узлов V1 и V2 - 192.168.1.1 и 192.168.1.2 соответственно.
- Подсети, между которыми организуется взаимодействие:
  - Подсеть, которая расположена за узлом V1 - 192.168.100.0/24.
  - Подсеть, которая расположена за узлом V2 - 192.168.101.0/24.
- Файл, содержащий предварительный ключ заранее создан при помощи команды **vpn openvpn-key generate /home/admin/secret**.

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**. (Сведения об установке статических маршрутов приведены в разделе Статическая маршрутизация.)

*Рисунок 78 - Пример подключения в межфилиальном режиме между узлами V1 и V2 с использованием предварительных ключей*




В этом разделе представлены следующие примеры:

- Пример 19.1 Межфилиальный режим с использованием предварительных ключей: оконечное устройство V1.
- Пример 19.2 Межфилиальный режим с использованием предварительных ключей: статический маршрут V1.
- Пример 19.4 Межфилиальный режим с использованием предварительных ключей: оконечное устройство V2.
- Пример 19.5 Межфилиальный режим с использованием предварительных ключей: статический маршрут V2.

Для настройки оконечного устройства V1, следует выполнить указанные шаги в режиме настройки.

*Пример 19.1 - Межфилиальный режим с использованием предварительных ключей: оконечное устройство V1*

| Действие | Команда |
|---|---|
| Создание узла конфигурации vtun0. | admin@V1# **set interfaces openvpn vtun0**<br>[edit] |
| Назначение туннельного IP-адреса локальному оконечному устройству. | admin@V1# **set interfaces openvpn vtun0 local-address 192.168.1.1**<br>[edit] |
| Установка межфилиального режима OpenVPN. | admin@V1# **set interfaces openvpn vtun0 mode site-to-site**<br>[edit] |
| Назначение туннельного IP-адреса удаленного оконечного устройства. | admin@V1# **set interfaces openvpn vtun0 remote-address 192.168.1.2**<br>[edit] |
| Указание физического IP-адреса удаленного устройства. | admin@V1# **set interfaces openvpn vtun0 remote-host 87.65.43.21**<br>[edit] |
| Указание расположения файла, содержащего предварительный ключ. | admin@V1# **set interfaces openvpn vtun0 shared-secret-key-file /home/admin/secret**<br>[edit] |
| Указание используемого алгоритма шифрования. | admin@V1# **set interfaces openvpn vtun0 encryption bf128**<br>[edit] |
| Фиксация изменений. | admin@V1# **commit**<br>[edit] |
| Вывод настройки OpenVPN. | admin@V1# **show interfaces openvpn vtun0** |

| Действие | Команда |
|---|---|
| | encryption bf128<br>local-address 192.168.1.1<br>mode site-to-site<br>remote-address 192.168.1.2<br>remote-host 87.65.43.21<br>shared-secret-key-file /home/admin/secret<br>[edit] |

Для настройки статического маршрута к удаленной подсети через туннель OpenVPN, необходимо выполнить следующие шаги в режиме настройки.

*Пример 19.2 - Межфилиальный режим с использованием предварительных ключей: статический маршрут на узле V1*

| Действие | Команда |
|---|---|
| Создание статического маршрута для получения доступа к удаленной подсети через туннель OpenVPN. | admin@V1# **set protocols static interface-route 192.168.101.0/24 next-hop-interface vtun0**<br>[edit] |
| Фиксация изменений. | admin@V1# **commit**<br>[edit] |
| Вывод статических маршрутов. | admin@V1# **show protocols static interface-route 192.168.101.0/24**<br>{<br>next-hop-interface vtun0 {}<br>}<br>[edit] |

Настройка оконечного устройства VPN V2 аналогична настройке V1, за исключением того, что локальный и удаленный туннельные IP-адреса меняются местами. Предварительно на устройство V2 необходимо передать файл, содержащий предварительный ключ, при этом следует помнить, что предварительный ключ следует сохранять в секрете и для его передачи

должны использоваться только защищенные каналы. Например, файл предварительного ключа можно передать на другое оконечное устройство с использованием флэш-накопителя или протокола SCP. Для передачи файла предварительного ключа по протоколу SCP следует выполнить на устройстве V1 следующую команду:

scp <*имя_локального_файла*> <*пользователь*>@<*ipv4-адрес*>:<*имя_удаленного_файла*>,

где

*имя_локального_файла*

Имя файла предварительного ключа с указанием полного пути на устройстве V1.

*пользователь*

Имя пользователя на устройстве V2.

*ipv4-адрес*

IP-адрес устройства V2.

*имя_удаленного_файла*

Имя файла предварительного ключа с указанием полного пути на устройстве V2.

В примере 19.3 приведена передача файла предварительного ключа (/home/admin/secret) на устройство V2 по протоколу SCP.

*Пример 19.3 - Передача файла предварительного ключа по протоколу SCP*

```
scp /home/admin/secret admin@87.65.43.21:/home/admin/secret
```

Для настройки оконечного устройства V2, необходимо выполнить следующие шаги в режиме настройки.

*Пример 19.4 - Межфилиальный режим с использованием предварительных ключей: оконечное устройство V2*

| Действие | Команда |
|---|---|
| Создание узла конфигурации vtun0. | admin@V2# **set interfaces openvpn vtun0** [edit] |
| Назначение туннельного IP-адреса | admin@V2# **set interfaces openvpn** |

| Действие | Команда |
|---|---|
| локальному оконечному устройству. | **vtun0 local-address 192.168.1.2**<br>[edit] |
| Установка межфилиального режима OpenVPN. | admin@V2# **set interfaces openvpn vtun0 mode site-to-site**<br>[edit] |
| Назначение туннельного IP-адреса удаленного оконечного устройства. | admin@V2# **set interfaces openvpn vtun0 remote-address 192.168.1.1**<br>[edit] |
| Указание физического IP-адреса удаленного устройства. | admin@V2# **set interfaces openvpn vtun0 remote-host 12.34.56.78**<br>[edit] |
| Указание расположения файла, содержащего предварительный ключ. | admin@V2# **set interfaces openvpn vtun0 shared-secret-key-file /root/secret**<br>[edit] |
| Указание используемого алгоритма шифрования. | admin@V2# **set interfaces openvpn vtun0 encryption bf128**<br>[edit] |
| Фиксация изменений. | admin@V2# **commit**<br>[edit] |
| Вывод настройки OpenVPN. | admin@V2# **show interfaces openvpn vtun0**<br>encryption bf128<br>local-address 192.168.1.2<br>mode site-to-site<br>remote-address 192.168.1.1<br>remote-host 12.34.56.78<br>shared-secret-key-file |

| Действие | Команда |
|---|---|
| | `/root/secret[edit]` |

Также, разделяемый секретный файл должен быть один и тот же на обоих оконечных узлах (путь к файлу может отличаться, но содержимое файла должно совпадать). Следует отметить, что параметр **remote-host** требуется только на одном из оконечных устройств; таким образом, межфилиальный туннель VPN может быть установлен при условии, что хотя бы одно из оконечных устройств имеет достаточно информации для установки соединения с другим.

Для настройки статического маршрута к удаленной подсети через туннель OpenVPN, необходимо выполнить следующие шаги в режиме настройки.

*Пример 19.5 - Межфилиальный режим OpenVPN с использованием предварительных ключей: статический маршрут на узле V2*

| Действие | Команда |
|---|---|
| Создание статического маршрута для получения доступа к удаленной подсети через туннель OpenVPN. | `admin@V2# set protocols static interface-route 192.168.100.0/24 next-hop-interface vtun0`<br>`[edit]` |
| Фиксация изменений. | `admin@V2# commit`<br>`[edit]` |
| Вывод настройки статических маршрутов. | `admin@V2# show protocols static interface-route 192.168.100.0/24`<br>`{`<br>`  next-hop-interface vtun0 {}`<br>`}`<br>`[edit]` |

### *19.1.3.2. 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-file**. Как было указано

выше, одно оконечное устройство выполняет пассивную роль, а другое активную роль.

Предварительно необходимо создать сертификаты, которые будут использоваться для безопасного взаимодействия между узлами. Подробно создание, а также экспорт/импорт сертификатов рассматривается в разделе 16.2. Пример настройки PKI. На каждом оконечном устройстве должен присутствовать сертификат и секретный ключ данного оконечного устройства, а также сертификат удостоверяющего центра.

Следующая настройка аналогична настройке для примера в предыдущем разделе. Предполагается, что все необходимые файлы созданы и доставлены каждому из оконечных устройств, а также что V1 и V2 исполняют пассивную и активную роль соответственно. Инфраструктура открытых ключей для создания сертификатов узлов V1 и V2 была создана на базе примеров, приведенных в разделе 16.2. Пример настройки PKI на стр. 1044.

Для настройки V1 в межфилиальном режиме VPN с использованием TLS, необходимо выполнить следующие действия в режиме настройки.

*Пример 19.6 - V1- Настройка OpenVPN - межфилиальный режим с использованием TLS*

| Действие | Команда |
|---|---|
| Создание узла конфигурации vtun0. | admin@V1# **set interfaces openvpn vtun0**<br>[edit] |
| Назначение локального IP-адреса туннеля VPN. | admin@V1# **set interfaces openvpn vtun0 local-address 192.168.1.1**<br>[edit] |
| Установка режима OpenVPN. | admin@V1# **set interfaces openvpn vtun0 mode site-to-site**<br>[edit] |
| Установка удаленного IP-адреса туннеля VPN. | admin@V1# **set interfaces openvpn vtun0 remote-address 192.168.1.2**<br>[edit] |
| Указание физического IP-адреса удаленного устройства. | admin@V1# **set interfaces openvpn vtun0 remote-host 87.65.43.21** |

| Действие | Команда |
|---|---|
| | `[edit]` |
| Установка роли данного оконечного устройства. | `admin@V1# set interfaces openvpn vtun0 tls role passive`<br>`[edit]` |
| Указание пути к файлу сертификата локального узла. | `admin@V1# set interfaces openvpn vtun0 tls x509-cert V1-cert`<br>`[edit]` |
| Фиксация изменений. | `admin@V1# commit`<br>`[edit]` |
| Вывод настройки OpenVPN. | `admin@V1# show interfaces openvpn vtun0`<br>`  local-address 192.168.1.1`<br>`  mode site-to-site`<br>`  remote-address 192.168.1.2`<br>`  remote-host 87.65.43.21`<br>`  tls {`<br>`  role passive`<br>`  x509-cert V1-cert`<br>`  }`<br>`[edit]` |

Следует отметить, что приведенная настройка аналогична приведенной в предыдущем разделе за исключением того, что параметр **shared-secret-key-file** заменен на параметр **tls**.

Для настройки V2 в межфилиальном режиме VPN с использованием TLS, необходимо выполнить следующие шаги в режиме настройки.

*Пример 19.7 - V2 - Настройка OpenVPN - межфилиальный режим с использованием TLS*

| Действие | Команда |
|---|---|
| Создание узла конфигурации vtun0. | `admin@V2# set interfaces openvpn vtun0` |

| Действие | Команда |
|---|---|
| | `[edit]` |
| Назначение локального IP-адреса туннеля VPN. | `admin@V2#` **`set interfaces openvpn vtun0 local-address 192.168.1.2`**<br>`[edit]` |
| Установка режима OpenVPN. | `admin@V2#` **`set interfaces openvpn vtun0 mode site-to-site`**<br>`[edit]` |
| Установка удаленного IP-адреса туннеля VPN. | `admin@V2#` **`set interfaces openvpn vtun0 remote-address 192.168.1.1`**<br>`[edit]` |
| Указание физического IP-адреса удаленного устройства. | `admin@V2#` **`set interfaces openvpn vtun0 remote-host 12.34.56.78`**<br>`[edit]` |
| Установка роли данного оконечного устройства. | `admin@V2#` **`set interfaces openvpn vtun0 tls role active`**<br>`[edit]` |
| Указание пути к файлу сертификата локального узла. | `admin@V2#` **`set interfaces openvpn vtun0 tls x509-cert V2-cert`**<br>`[edit]` |
| Фиксация изменений. | `admin@V2#` **`commit`**<br>`[edit]` |
| Вывод настройки OpenVPN. | `admin@V2#` **`show interfaces openvpn vtun0`**<br>`local-address 192.168.1.2`<br>`mode site-to-site`<br>`remote-address 192.168.1.1`<br>`remote-host 12.34.56.78` |

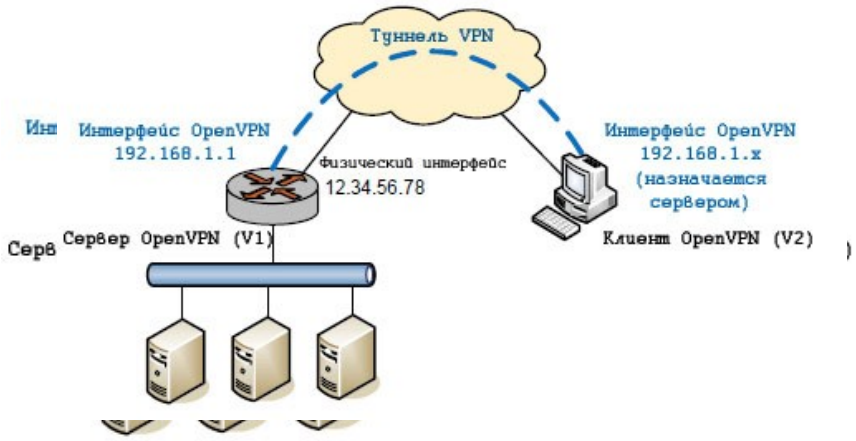
| Действие | Команда |
|---|---|
| | tls {<br>role active<br>x509-cert V2-cert<br>}<br>[edit] |

Настройка аналогична приведенной в предыдущем примере, за исключением того, что указан параметр **tls**.

### *19.1.3.3. 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 79.

*Рисунок 79 - 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 V1 является сервером, а устройство V2 является клиентом.

Для того чтобы настроить V1 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 192.168.1.0/24, из которой сервер будет назначать клиентам туннельные IP-адреса. Также этот параметр определяет туннельный IP-адрес сервера (адрес vtun0 на сервере) 192.168.1.1.
- Значение для параметра **remote-host** не устанавливается, так как инициировать подключения к серверу будут клиенты.

*Пример 19.8 - V1 - Настройки OpenVPN - клиент-серверный режим с использованием TLS (сервер)*

| Действие | Команда |
|---|---|
| Создание настройки vtun0. | admin@V1# **set interfaces openvpn vtun0**<br>[edit] |
| Установка режима OpenVPN. | admin@V1# **set interfaces openvpn vtun0 mode server**<br>[edit] |
| Указание физического адреса, на котором будут приниматься входящие подключения. | admin@V1# **set interfaces openvpn vtun0 local-host 12.34.56.78**<br>[edit] |
| Установка подсети для туннеля OpenVPN. | admin@V1# **set interfaces openvpn vtun0 server subnet 192.168.1.0/24**<br>[edit] |
| Указание пути к файлу сертификата локального узла. | admin@V1# **set interfaces openvpn vtun0 tls x509-cert V1-cert**<br>[edit] |

| Действие | Команда |
|---|---|
| Фиксация изменений. | admin@V1# **commit**<br>[edit] |
| Вывод настройки OpenVPN. | admin@V1# **show interfaces openvpn vtun0**<br>local-host 12.34.56.78<br>mode server<br>server {<br>  subnet 192.168.1.0/24<br>}<br>tls {<br>  x509-cert V1-cert<br>}<br>[edit] |

Для того чтобы экспортировать файл настройки клиента, а также сертификат и секретный ключ клиента используется команда **vpn openvpn-export <vtunx>** .

Для настройки V2 для работы в клиент-серверном режиме с использованием TLS, необходимо выполнить следующие действия в режиме настройки. В этом примере:

- V2 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 V2 (то есть, адрес vtun0 на V2) будет назначен устройством V1 из подсети 192.168.1.0/24.

*Пример 19.9 - V2 Настройка OpenVPN - клиент-серверный режим с использованием TLS (клиент)*

| Действие | Команда |
|---|---|
| Создание узла конфигурации vtun0. | admin@V2# **set interfaces openvpn vtun0**<br>[edit] |

| Действие | Команда |
|---|---|
| Установка режима OpenVPN. | admin@V2# **set interfaces openvpn vtun0 mode client**<br>[edit] |
| Указание физического IP-адреса удаленного устройства. | admin@V2# **set interfaces openvpn vtun0 remote-host 12.34.56.78**<br>[edit] |
| Указание пути к файлу сертификата локального устройства. | admin@V2# **set interfaces openvpn vtun0 tls x509-cert V2-cert**<br>[edit] |
| Фиксация изменений. | admin@V2# **commit**<br>[edit] |
| Вывод настройки OpenVPN. | admin@V2# **show interfaces openvpn vtun0**<br>mode client<br>remote-host 12.34.56.78<br>tls {<br>x509-cert V2-cert<br>}<br>[edit] |

#### *19.1.3.4. Использование клиента Altell NEO VPN на устройствах под управлением ОС Windows*

Как было указано ранее, OpenVPN отличается от других решений “SSL VPN”, представленных на рынке и не может с ними взаимодействовать, как следствие OpenVPN должен быть установлен на всех узлах VPN. При настройке удаленного доступа VPN в качестве удаленных клиентов OpenVPN могут быть использованы устройства под управлением ОС Windows.

В качестве клиента OpenVPN в ОС Windows может быть использовано приложение Altell NEO VPN, которое поставляется вместе с системой Altell NEO. Altell NEO VPN

предоставляет удобный графический интерфейс пользователя, а также обладает встроенной поддержкой российских криптографических алгоритмов.

После настройки сервера OpenVPN в системе Altell NEO можно автоматически создать настройку клиента, а также экспортировать ее на флэш-накопитель с помощью команды **vpn openvpn-export <vtunx>** . Файл с настройкой клиента, а также все необходимые файлы (файлы сертификатов, ключей и т.д) будут сохранены на флэш-накопителе в директории **/openvpn**.

Для экспорта настройки клиента V2 для работы в клиент-серверном режиме с использованием TLS, необходимо выполнить следующую команду в эксплуатационном режиме на узле V1:

```
admin@V1:~$ vpn openvpn-export vtun0 client-cert V2-cert
```

После чего необходимо перенести указанные файлы на клиентский компьютер. При выполнении команды **vpn openvpn-export <vtunx>** также экспортируется командный файл **setupvpn.js**, который позволяет автоматически настроить клиент OpenVPN в соответствии с экспортированной конфигурацией. После этого для установки подключения к серверу достаточно запустить приложение Altell NEO VPN, при этом в области уведомлений Windows будет выведен соответствующий значок. Для того чтобы установить туннель OpenVPN, следует нажать правой кнопкой мыши на значок и выбрать **Соединить** из раскрывающегося меню. В том случае если в директории находится несколько файлов настроек с расширением **avpn**, действия для каждого из них представлены в отдельных раскрывающихся меню.

#### *19.1.3.5. Настройка межсетевого экрана*

Применение правил межсетевого экрана к туннельному интерфейсу OpenVPN аналогично применению правил к интерфейсам другого типа.

Для настройки межсетевого экрана на устройстве V1, необходимо выполнить следующие действия в режиме настройки.

*Пример 19.10 - Настройка правил межсетевого экрана для интерфейса OpenVPN*

| Действие | Команда |
|---|---|
| Создание узла конфигурации vtun0. | `admin@V1# set interfaces openvpn` |

| Действие | Команда |
|---|---|
| | **vtun0**<br>[edit] |
| Команды дополнительной настройки. | ... |
| Установка правила межсетевого экрана для входящего трафика на интерфейсе vtun0. | admin@V1# **set interfaces openvpn vtun0 firewall in name rules-in**<br>[edit] |
| Команды дополнительной настройки. | ... |
| Фиксация изменений. | admin@V1# **commit**<br>[edit] |
| Вывод настройки OpenVPN. | admin@V1# **show interfaces openvpn vtun0**<br>...<br>firewall {<br>in {<br>name rules-in<br>}<br>}<br>...<br>[edit] |

Более подробная информация по настройке межсетевого экрана приведена в разделе 14. Настройка межсетевого экрана .

### 19.1.4. 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).
- Криптографические алгоритмы (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).

### 19.1.5. 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 19.11 и описаны ниже.

*Пример 19.11 - Настройка параметра типа протокола*

```
interfaces {
   openvpn <интерфейс> {
      protocol <протокол>
      local-host <ipv4-адрес>
```

```
      local-port <порт>
      remote-port <порт>
   }
}
```

- **protocol**: Корректные значения для данного параметра: **udp**, **tcp-active**, и **tcp-passive**. В том случае если значение для параметра **protocol** явно не определено или указано значение **udp**, 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**), должен быть установлен параметр **remote-host**, для того чтобы данное устройство имело возможность устанавливать соединения.
  - Если на устройстве, работающем в пассивном режиме (**tcp-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**), а сервер в пассивном режиме (**tcp-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**) 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**) 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**) 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 в том случае 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**) при использовании протокола TCP в межфилиальном режиме.

#### *19.1.5.1. Криптографические алгоритмы (межфилиальный режим, режим клиента, режим сервера)*

Как было указано выше, вне зависимости от используемого механизма безопасности (предварительных ключей или TLS), после того как туннель VPN установлен, оконечные устройства применяют алгоритмы шифрования и хэширования к данным, передаваемым по туннелю VPN, для обеспечения конфиденциальности и целостности. По умолчанию, OpenVPN использует алгоритмов Blowfish (с ключом 128 бит) и алгоритм SHA-1.

Altell NEO поддерживает российские криптографические алгоритмы: алгоритм шифрования ГОСТ 28147-89 (**encryption gost89**), а также аутентификацию на основе режима выработки имитовставки ГОСТ 28147-89 (**hash gost**). Алгоритм шифрования ГОСТ 28147-89 может быть использован только в режиме TLS.

Для установки какого-либо конкретного алгоритма используются параметры настройки, приведенные в примере 19.12.

*Пример 19.12 - Настройка параметров, относящихся к безопасности*

```
interfaces {
   openvpn <интерфейс> {
      encryption <алгоритм>
      hash <алгоритм>
   }
}
```

- **encryption**: Данный параметр определяет используемый алгоритм шифрования, допустимы следующие значения.
  - **des**: Алгоритм DES;
  - **3des**: Алгоритм DES с тремя циклами шифрования;
  - **bf128**: Алгоритм Blowfish с ключом длины 128 бит;
  - **bf256**: Алгоритм Blowfish с ключом длины 256 бит;
  - **aes128**: Алгоритм AES с ключом длины 128 бит;
  - **aes192**: Алгоритм AES с ключом длины 192 бит;

- **aes256**: Алгоритм AES с ключом 256 бит;
- **gost89**: Алгоритм ГОСТ 28147-89.

- **hash**: Данный параметр определяет используемый хэш-алгоритм, допустимы следующие значения.
  - **md5**: Алгоритм MD5
  - **sha1**: Алгоритм SHA-1
  - **sha256**: Алгоритм SHA-256
  - **sha512**: Алгоритм SHA-512
  - **gost**: Алгоритм ГОСТ 28147-98 в режиме выработки имитовставки.

#### *19.1.5.2. 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 в Интернете, 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.

С одной стороны, разделение трафика позволяет повысить эффективность, так как трафик, не относящийся к VPN (например, трафик Интернет) отправляется по обычному маршруту. Например, при установке удаленного доступа VPN, это означает, что трафик Интернет удаленного пользователя направляется от/к провайдеру (ISP) напрямую, без отправки на сервер VPN, сеть компании, межсетевой экран, и так далее. С другой стороны, в этом случае трафик Интернет не фильтруется, либо движется в обход защитных механизмов, предусмотренных политикой безопасности компании.

Для того чтобы отключить разделение трафика, следует использовать настройку, которая приведена в примере 19.13.

*Пример 19.13 - 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:
    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.

  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.

#### *19.1.5.3. 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 подключится к другому. Для того чтобы указать список серверов, следует указать множественные узлы настройки **remote-host**.

Для того чтобы настроить несколько оконечных устройств на V2, необходимо выполнить следующие действия в режиме настройки.

*Пример 19.14 - V2 - Настройка нескольких оконечных устройств OpenVPN*

| Действие | Команда |
|---|---|
| Создание узла конфигурации vtun0. | admin@V2# **set interfaces openvpn vtun0**<br>[edit] |
| Команды дополнительной настройки. | ... |
| Указание физического IP-адреса первого удаленного устройства. | admin@V1# **set interfaces openvpn vtun0 remote-host 12.34.56.78**<br>[edit] |
| Указание физического IP-адреса второго удаленного устройства. | admin@V1# **set interfaces openvpn vtun0 remote-host 12.34.56.79**<br>[edit] |
| Указание физического IP-адреса третьего удаленного устройства. | admin@V1# **set interfaces openvpn vtun0 remote-host12.34.56.80**<br>[edit] |
| Установка правила межсетевого экрана | admin@V2# **set interfaces openvpn** |

| Действие | Команда |
|---|---|
| для входящего трафика на интерфейсе vtun0. | **vtun0 firewall in name rules-in**<br>[edit] |
| Команды дополнительной настройки. | ... |
| Фиксация изменений. | admin@V2# **commit**<br>[edit] |
| Вывод настройки OpenVPN. | admin@V2# **show interfaces openvpn vtun0**<br>...<br>remote-host 12.34.56.78<br>remote-host 12.34.56.79<br>remote-host 12.34.56.80<br>...<br>[edit] |

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.

#### *19.1.5.4. 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 19.15.

*Пример 19.15 - 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:

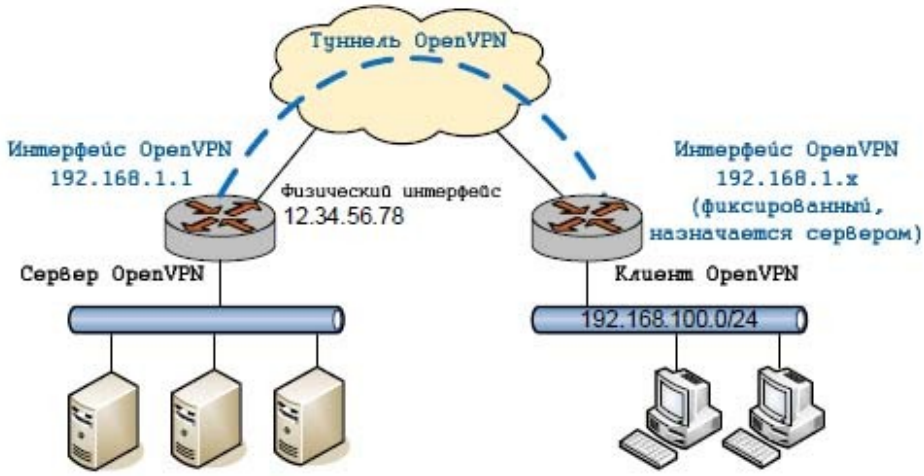
- **subnet**: Данная топология совместима с клиентами под управлением ОС Windows и принята по умолчанию, в том случае если значение для параметра **topology** явно не указано. При использовании топологии такого типа будут функционировать протоколы маршрутизации, использующие широковещательные рассылки. 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. Однако, данная технология обеспечивает изоляцию клиентов.

#### *19.1.5.5. Настройки клиента (режим сервера)*

Обычно VPN удаленного доступа используется для предоставления доступа к ресурсам внутренней локальной сети удаленным пользователям — например, сотрудникам, получающим доступ к корпоративной сети из дома. В этом случае необходимо убедиться, что при подключении к серверу VPN, соответствующим образом настроена маршрутизация и клиентский компьютер имеет доступ к частной сети.

Также 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 80.

*Рисунок 80 - 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 19.16.

*Пример 19.16 - 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 (в том случае 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, также должен быть отдельно добавлен статический маршрут для направления данного трафика на туннельный интерфейс.

В вышеприведенном примере, сервер V1 может быть настроен с указанием IP-адреса и подсети клиента V2 (следует отметить, что также должен быть добавлен статический маршрут к подсети V2).

Для настройки данного варианта подключения, необходимо выполнить следующие действия в режиме настройки.

*Пример 19.17 - V1 - Настройка OpenVPN - межфилиальное подключение с использованием предварительного ключа*

| Действие | Команда |
|---|---|
| Создание узла конфигурации vtun0. | admin@V1# **set interfaces openvpn vtun0**<br>[edit] |
| Команды дополнительной настройки. | ... |
| Создание конфигурационного узла сервера. | admin@V1# **set interfaces openvpn vtun0 server**<br>[edit] |
| Команды дополнительной настройки. | ... |

| Действие | Команда |
|---|---|
| Создание узла конфигурации клиента V2. | admin@V1# **set interfaces openvpn vtun0 server client V2**<br>[edit] |
| Установка подсети клиента. | admin@V1# **set interfaces openvpn vtun0 server client V2 subnet 192.168.100.0/24**<br>[edit] |
| Указание IP-адреса клиента. | admin@V1# **set interfaces openvpn vtun0 server client V2 ip 192.168.1.100**<br>[edit] |
| Команды дополнительной настройки. | ... |
| Фиксация изменений. | admin@V1# **commit**<br>[edit] |
| Вывод настройки OpenVPN. | admin@V1# **show interfaces openvpn vtun0**<br>...<br>server {<br>...<br>client V2 {<br>ip 192.168.1.100<br>subnet 192.168.100.0/24<br>}<br>...<br>}<br>...<br>[edit] |

Для настройки статического маршрута, который позволит обеспечить доступ к удаленной подсети через туннель OpenVPN, необходимо выполнить следующие действия в

режиме настройки.

*Пример 19.18 - Настройка статического маршрута на узле V1*

| Действие | Команда |
|---|---|
| Создание статического маршрута для получения доступа к удаленной подсети через туннель OpenVPN. | admin@V1# **set protocols static interface-route 192.168.100.0/24 next-hop-interface vtun0**<br>[edit] |
| Фиксация изменений. | admin@V1# **commit**<br>[edit] |
| Вывод настройки статических маршрутов. | admin@V1# **show protocols static interface-route 192.168.100.0/24**<br>{<br>next-hop-interface vtun0 {}<br>}<br>[edit] |

### 19.1.6. Неподдерживаемые параметры OpenVPN

OpenVPN имеет более двухсот параметров, не все из которых поддерживаются в настройке Altell NEO. В то же время администратору в некоторых случаях могут потребоваться параметры OpenVPN, не поддерживаемые при настройке Altell NEO. Для таких случаев в системе существует атрибут настройки **openvpn-option**; этот атрибут позволяет определить любой параметр OpenVPN, см. пример 19.19.

*Пример 19.19 - 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 19.20 - Ввод нескольких параметров OpenVPN при помощи "openvpn-option"*

| Действие | Команда |
|---|---|
| Создание узла конфигурации vtun0. | admin@V1# **set interfaces openvpn vtun0**<br>[edit] |
| Команды дополнительной настройки. | ... |
| Установка требуемых параметров OpenVPN. | admin@V1# **set interfaces openvpn vtun0 openvpn-option "-verb 5 -secret /root/secret 1"**<br>[edit] |
| Команды дополнительной настройки. | ... |
| Фиксация изменений. | admin@V1# **commit**<br>[edit] |
| Вывод настройки OpenVPN. | admin@V1# **show interfaces openvpn vtun0**<br>...<br>openvpn-option "-verb 5<br>-secret /root/secret 1"<br>...<br>[edit] |

Для данного параметра не выполняется никакой проверки 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.

## 19.2. Команды OpenVPN

В данном разделе приведены следующие команды:

*Таблица 44 - Команды OpenVPN*

| Команды настройки | |
|---|---|
| Общие команды OpenVPN | |
| `interfaces openvpn <vtunx>` | Определение интерфейса OpenVPN. |
| `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 <ipv4-адрес>` | Указание IP-адреса физического интерфейса, на котором будут ожидаться входящие подключения. |
| `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>` | 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. |
| `interfaces openvpn <vtunx> shared-secret-key-file <имя_файла>` | Указание файла, содержащего секретный ключ, разделяемый с удаленным оконечным узлом туннеля. |
| Сервер OpenVPN | |
| `interfaces openvpn <vtunx> server` | Определение режима сервера для оконечного узла OpenVPN. |
| `interfaces openvpn <vtunx> server client <имя_клиента>` | Определение клиентского узла на данном сервере. |
| `interfaces openvpn <vtunx> server client <client-name> ip <ipv4-адрес>` | Указание IP-адреса клиента. |
| `interfaces openvpn <vtunx> server client <имя_клиента> subnet <ipv4-сеть>` | Указание подсети на клиентском узле. |
| `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. |
| TLS | |
| `interfaces openvpn <vtunx> tls` | Определение настройки TLS (Transport Layer Security). |
| `interfaces openvpn <vtunx> x509-cert <имя_файла>` | Указание сертификата данного оконечного узла. |
| `interfaces openvpn <vtunx>` | Указание роли TLS данного оконечного |

| | |
|---|---|
| | устройства. |
| Эксплуатационные команды | |
| `vpn openvpn-key generate <имя_файла>` | Генерация разделяемого секретного файла. |
| `vpn openvpn-export <vtunx>` | Экспорт файлов настройки клиента. |
| `show interfaces openvpn` | Вывод состояния всех интерфейсов OpenVPN. |
| `show interfaces openvpn <интерфейс>` | Вывод детализированных сведений о состоянии интерфейса OpenVPN. |
| `show interfaces openvpn <интерфейс> brief` | Вывод кратких сведений о состоянии интерфейса OpenVPN. |
| `show interfaces openvpn <интерфейс> capture` | Запись данных, проходящих через интерфейс OpenVPN. |
| `show interfaces openvpn detail` | Вывод детализированных сведений о состоянии всех интерфейсов OpenVPN в системе. |
| `show openvpn server-status` | Вывод сведений о подключенных клиентах (в режиме сервера). |

Команды настройки межсетевого экрана для интерфейсов OpenVPN приведены в разделе 14. Настройка межсетевого экрана .

### 19.2.1. 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 vtun0..vtunx {}
}
```

**Параметры**

*vtunx*

Обязательный. Множественный узел. Идентификатор определяемого интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое.

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.

## 19.2.2. 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 vtun0..vtunx {
        encryption [3des|aes128|aes192|aes256|bf128|
bf256|des|gost89]
```

```
        }
    }
```

**Параметры**

*vtunx*

Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое число.

*алгоритм*

Алгоритм шифрования, который используется для туннеля OpenVPN. Допустимы следующие значения:

**3des**: Алгоритм DES с тройным шифрованием;

**aes128**: Алгоритм AES с ключом длины 128 бит;

**aes192**: Алгоритм AES с ключом длины 192 бит;

**aes256**: Алгоритм AES с ключом длины 256 бит;

**bf128**: Алгоритм Blowfish с ключом длины 128 бит;

**bf256**: Алгоритм Blowfish с ключом длины 256 бит;

**des**: Алгоритм DES;

**gost89**: Алгоритм ГОСТ 28147-89.

По умолчанию установлено значение **gost89**.

> ***ПРИМЕЧАНИЕ*** *В алгоритме ГОСТ 28147-89 не определен режим CBC (сцепления блоков шифртекста). OpenVPN поддерживает использование алгоритмов шифрования в режимах, отличных от CBC, только в режиме TLS.*

**Значение по умолчанию**

По умолчанию используется алгоритм ГОСТ 28147-89.

**Указания по использованию**

Данная команда используется для настройки алгоритма шифрования, который применяется к данным, передаваемым по туннелю OpenVPN.

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.

### 19.2.3. 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 vtun0..vtunx {
        hash [md5|sha1|sha256|sha512|gost]
    }
}
```

#### Параметры

*vtunx*

Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое число.

*алгоритм*

Хэш-алгоритм, который используется для указанного туннеля OpenVPN. Поддерживаемые значения:

**md5**: Алгоритм MD5;

**sha1**: Алгоритм SHA-1;

**sha256**: Алгоритм SHA-256;

**sha512**: Алгоритм SHA-512;

**gost**: Алгоритм ГОСТ 28147-89 в режиме выработки имитовставки.

По умолчанию установлено значение **sha1**.

**Значение по умолчанию**

Используется алгоритм SHA-1.

**Указания по использованию**

Данная команда используется для настройки хэш-алгоритма, которые применяется для данного туннеля OpenVPN.

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.

### 19.2.4. 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 vtun0..vtunx {
        local-address ipv4-адрес
    }
}
```

**Параметры**

*vtunx*

Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое число.

*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.

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.

### 19.2.5. interfaces openvpn <vtunx> local-host <ipv4-адрес>

Указание физического IP-адреса, на котором будут приниматься входящие подключения.

**Синтаксис**

```
set interfaces openvpn vtunx local-host ipv4-адрес
delete interfaces openvpn vtunx local-host
show interfaces openvpn vtunx local-host
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    openvpn vtun0..vtunx {
        local-host ipv4-адрес
    }
}
```

**Параметры**

*vtunx*

Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое число.

*ipv4-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.

**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**) 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.

### 19.2.6. 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 vtun0..vtunx {
        local-port целоебеззнака32разр
    }
}
```

**Параметры**

*vtunx*

Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое число.

*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.

## 19.2.7. interfaces openvpn <vtunx> mode <режим>

Указание режима функционирования интерфейса OpenVPN.

**Синтаксис**

```
set interfaces openvpn vtunx mode режим
delete interfaces openvpn vtunx mode
show interfaces openvpn vtunx mode
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    openvpn vtun0..vtunx {
        mode [client|server|site-to-site]
    }
}
```

**Параметры**

*vtunx*

Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое число.

*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.

**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.

### 19.2.8. 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 vtun0..vtunx {
        openvpn-option текст
    }
}
```

**Параметры**

*vtunx*

Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое число.

*параметры*

Строка параметров, которые будут переданы процессу OpenVPN.

**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 системы Altell NEO. Так как процесс OpenVPN имеет более двухсот команд, только основные из них могут быть настроены при помощи команд Altell NEO. 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.

## 19.2.9. 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 vtun0..vtunx {
        protocol [tcp-active|tcp-passive|udp]
```

```
        }
    }
```

**Параметры**

*vtunx*

Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое число.

*протокол*

Транспортный протокол, используемый OpenVPN. Поддерживаемые значения:

**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.

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.

## 19.2.10. 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 vtun0..vtunx {
        remote-address ipv4-адрес
    }
}
```

**Параметры**

*vtunx*

Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое число.

*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.

## 19.2.11. 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 vtun0..vtunx {
        remote-host [ipv4-адрес| текст]
    }
}
```

**Параметры**

*vtunx*

Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое число.

*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.

## 19.2.12. 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 vtun0..vtunx {
        remote-port целоебеззнака32
    }
}
```

**Параметры**

*vtunx*

Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое число.

*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.

## 19.2.13. 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 vtun0..vtunx {
        replace-default-route {
            local
        }
    }
}
```

**Параметры**

*vtunx*

Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне

от **vtun0** до **vtun***x*, где *x* неотрицательное целое число.

**`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.

## 19.2.14. 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 vtun0..vtunx {
        server {}
    }
}
```

**Параметры**

*vtunx*

Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое число.

**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.

## 19.2.15. interfaces openvpn <vtunx> server client <имя_клиента>

Определение настройки клиентского узла для данного сервера.

**Синтаксис**

**set interfaces openvpn** *vtunx* **server client** *имя_клиента*

**delete interfaces openvpn** *vtunx* **server client** [*имя_клиента*]

**show interfaces openvpn** *vtunx* **server client** [*имя_клиента*]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    openvpn vtun0..vtunx {
        server {
            client текст {}
        }
    }
}
```

**Параметры**

*vtunx*

Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое число.

*имя_клиента*

Обязательный. Имя клиентского узла. Данное имя соответствует имени сертификата клиента.

Когда клиент инициирует сессию VPN, сервер проверяет имя сертификата и применяет настройки, предназначенные для данного клиента (в том случае если они существуют).

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет определить настройки клиентского узла на данном сервере.

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.

## 19.2.16. 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_клиента* **ip** *ipv4-адрес*

**delete interfaces openvpn** *vtunx* **server client** *имя_клиента* **ip**

**show interfaces openvpn** *vtunx* **server client** *имя_клиента* **ip**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    openvpn vtun0..vtunx {
        server {
            client текст {
                ip ipv4-адрес
            }
        }
    }
```

```
}
```

**Параметры**

*vtunx*

Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое число.

*имя_клиента*

Обязательный. Имя клиентского узла. Данное имя соответствует имени сертификата клиента.

Когда клиент инициирует сессию VPN, сервер проверяет имя сертификата и применяет настройки, предназначенные для данного клиента (в том случае если они существуют).

*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.

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.

## 19.2.17. interfaces openvpn <vtunx> server client <имя_клиента> subnet <ipv4-сеть>

Указание подсети на клиентском узле при использовании клиент-серверной топологии.

**Синтаксис**

```
set interfaces openvpn vtunx server client имя_клиента
subnet ipv4-сеть

delete interfaces openvpn vtunx server client
```

*имя_клиента* **subnet**

**show interfaces openvpn** *vtunx* **server client** *имя_клиента* **subnet**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    openvpn vtun0..vtunx {
        server {
            client текст {
                subnet ipv4-сеть
            }
        }
    }
}
```

**Параметры**

*vtunx*

Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое число.

*имя_клиента*

Обязательный. Имя клиентского узла. Данное имя соответствует имени сертификата клиента.

Когда клиент инициирует сессию VPN, сервер проверяет имя сертификата и применяет настройки, предназначенные для данного клиента (в том случае если они существуют).

*ipv4-сеть*

Подсеть, расположенная за клиентским узлом.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет указать частную подсеть, расположенную за клиентским узлом. 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, 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.

## 19.2.18. 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 vtun0..vtunx {
        server {
            subnet ipv4-сеть
        }
```

```
        }
    }
```

**Параметры**

*vtunx*

Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое число.

*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.

## 19.2.19. 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 vtun0..vtunx {
    server {
        topology [point-to-point|subnet]
    }
}
```

**Параметры**

*vtunx*

Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое число.

*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.

## 19.2.20. interfaces openvpn <vtunx> shared-secret-key-file <имя_файла>

Указание файла, содержащего секретный ключ, разделяемый с удаленным оконечным узлом туннеля.

**Синтаксис**

**set interfaces openvpn** *vtunx* **shared-secret-key-file** *имя_файла*

**delete interfaces openvpn** *vtunx* **shared-secret-key-file**

**show interfaces openvpn** *vtunx* **shared-secret-key-file**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    openvpn vtun0..vtunx {
        shared-secret-key-file текст
    }
}
```

**Параметры**

*vtunx*

Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где **x** неотрицательное целое число.

*имя_файла*

Полный путь к разделяемому секретному файлу. Файл может быть создан при помощи эксплуатационной команды **vpn openvpn-key generate**, на другом оконечном устройстве должен быть тот же файл для корректной работы.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда используется для указания файла, содержащего секретный

ключ, разделяемый с удаленным оконечным узлом туннеля.

Форма **set** данной команды используется для указания файла, содержащего разделяемый секретный ключ.

Форма **delete** данной команды используется для удаления настройки файла разделяемого секретного ключа.

Форма **show** данной команды используется для отображения настройки файла секретного ключа.

## 19.2.21. 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 vtun0..vtunx {
        tls {}
    }
}
```

**Параметры**

*vtunx*

Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое число.

**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.

## 19.2.22. interfaces openvpn <vtunx> x509-cert <имя_файла>

Указание сертификата локального оконечного узла OpenVPN.

**Синтаксис**

```
set interfaces openvpn vtunx tls x509-cert сертификат
delete interfaces openvpn vtunx tls x509-cert
show interfaces openvpn vtunx tls x509-cert
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    openvpn vtun0..vtunx {
        tls {
            x509-cert текст
        }
    }
}
```

**Параметры**

*vtunx*

Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое число.

*сертификат*

Сертификат локального оконечного узла.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет указать сертификат локального оконечного узла.

Указание значения для данного параметра является обязательным, если

используется режим TLS. Вопросы управления сертификатами подробно рассмотрены в разделе 16. Инфраструктура открытых ключей.

Форма **set** данной команды используется для указания сертификата локального оконечного узла.

Форма **delete** данной команды используется для удаления настройки сертификата локального оконечного узла.

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

### 19.2.23. 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 vtun0..vtunx {
        tls {
            role [active|passive]
        }
    }
}
```

#### Параметры

*vtunx*

Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое число.

*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.

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.

## 19.2.24. vpn openvpn-key generate <имя_файла>

Генерация файла, содержащего предварительный ключ.

**Синтаксис**

**vpn openvpn-key generate** *имя_файла*

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*имя_файла*

Обязательный. Имя разделяемого секретного файла, который будет создан.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда используется для создания разделяемого секретного файла, который требуется при применении механизма безопасности с использованием предварительных ключей. Данная команда доступна только для пользователей, обладающих правами администратора.

## 19.2.25. 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 Altell NEO.

**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 Altell NEO VPN, которое поставляется вместе с системой Altell NEO 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.*

## 19.2.26. show interfaces openvpn

Вывод состояния всех интерфейсов OpenVPN.

**Синтаксис**

**show interfaces openvpn**

**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**

В примере 19.21 приведен вывод для команды **show interfaces openvpn**.

*Пример 19.21 - "show interfaces openvpn": Отображение состояния интерфейса OpenVPN*

```
admin@neo:~$ show interfaces openvpn
Interface IP Address State Link Description
vtun0 192.168.1.1/32 up up
admin@neo:~$
```

## 19.2.27. show interfaces openvpn <интерфейс>

Вывод детализированных сведений о состоянии интерфейса OpenVPN.

**Синтаксис**

**show interfaces openvpn** *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 19.22 приведен вывод для команды **show interfaces openvpn <*интерфейс*>**.

*Пример 19.22 - "show interfaces openvpn vtun0": Отображение состояния интерфейса OpenVPN*

```
admin@neo:~$ show interfaces openvpn vtun0

vtun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500
qdisc pfifo_fast state

UNKNOWN qlen 100link/[65534]inet 192.168.1.1 peer
192.168.1.2/32 scope global vtun0

RX: bytes packets errors dropped overrun mcast 1216 16 0
0 0 0 TX: bytes packets errors dropped carrier collisions
0 0 0 0 0 0
```

## 19.2.28. show interfaces openvpn <интерфейс> brief

Вывод кратких сведений о состоянии интерфейса OpenVPN.

**Синтаксис**

**show interfaces openvpn** *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 19.23 приведен вывод для команды **show interfaces openvpn <*интерфейс*> brief**.

*Пример 19.23 - "show interfaces openvpn vtun0 brief": Отображение состояния интерфейса OpenVPN*

```
admin@neo:~$ show interfaces openvpn vtun0 brief
Interface IP Address State Link Description vtun0
192.168.1.1/32 up up
```

## 19.2.29. show interfaces openvpn <интерфейс> capture

Запись данных, проходящих через интерфейс OpenVPN.

**Синтаксис**

**show interfaces openvpn** *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 19.24 приведен вывод для команды **show interfaces openvpn <*интерфейс*> capture**.

*Пример 19.24 - "show interfaces openvpn vtun0 capture": Запись трафика на интерфейсе OpenVPN*

```
admin@neo:~$ show interfaces openvpn vtun0 capture
```

```
Capturing traffic on vtun0 ...
```

## 19.2.30. show interfaces openvpn detail

Вывод детализированных сведений о состоянии всех интерфейсов OpenVPN в системе.

**Синтаксис**

**show interfaces openvpn 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 19.25 приведен вывод для команды **show interfaces openvpn detail**.

*Пример 19.25 - "show interfaces openvpn vtun0 detail": Запись трафика на интерфейсе OpenVPN*

```
admin@neo:~$ show interfaces openvpn detail

vtun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500
qdisc pfifo_fast state

UNKNOWN qlen 100link/[65534]inet 192.168.1.1 peer
192.168.1.2/32 scope global vtun0

RX: bytes packets errors dropped overrun mcast 1216 16 0
0 0 0 TX: bytes packets errors dropped carrier collisions
0 0 0 0 0 0
```

## 19.2.31. show openvpn server-status

Вывод сведений о подключенных клиентах (в режиме сервера).

**Синтаксис**

**show openvpn 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 19.26 приведен вывод для команды **show openvpn server-status**.

*Пример 19.26 - "show openvpn server-status": Отображение состояния сервера OpenVPN*

```
admin@neo:~$ show openvpn server-status

OpenVPN server status on vtun0 (last updated on Wed Oct
29 22:34:18 2008)

Client Remote IP Tunnel IP TX byte RX byte Connected
Since vclient1 192.168.252.3 192.168.1.4 16.0K 16.5K Wed
Oct 29

21:59:50 2008
```

# 20. SSH

## 20.1. Настройка SSH

Протокол SSH (Secure Shell) обеспечивает безопасный механизм входа в систему NEO и получения доступа к интерфейсу командной строки. В поставляемом Altell NEO по умолчанию настроен сервис SSH на управляющем интерфейсе на стандартном для SSH порту (22). По умолчанию управляющий порт NEO 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.

В примере 20.1 показано включение протокола SSH с использованием порта по умолчанию (порт 22) и аутентификации по паролю на сконфигурированном в системе адресе 192.168.10.1.

*Пример 20.1 - Включение доступа по SSH на адресе 192.168.10.1*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для службы SSH на адресе 192.168.10.1 | admin@R1# **set service ssh address 192.168.10.1**<br>[edit] |
| Фиксация изменений. | admin@R1# **commit**<br>[edit] |
| Вывод настройки. | admin@R1# **show service ssh**<br>address 192.168.10.1 {<br>}<br>cipher gost89<br>[edit] |

## 20.2. Команды SSH

В этом разделе приведены следующие команды.

*Таблица 45 - Команды SSH*

| Команды настройки | |
|---|---|
| `service ssh address <адрес> port <порт>` | Включение SSH как протокола доступа в систему NEO на определённом адресе и порту. |
| `service ssh cipher <алгоритм>` | Указание допустимых для использования алгоритмов шифрования. |
| `service ssh disable-password-authentication` | Отключение парольной аутентификации при получении доступа по протоколу SSH. |

Эксплуатационные команды отсутствуют.

### 20.2.1. service ssh address <адрес> port <порт>

Включение SSH как протокола доступа в систему NEO 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 ipv4-адрес {
            port 1-65535
        }
    }
}
```

**Параметры**

*адрес*

Адрес, на котором будет принимать соединения сервис SSH.

*порт*

Номер порта, который будет использоваться службой SSH. Значение должно лежать в диапазоне от 1 до 65535. Значение по умолчанию равно 22.

**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.

Создание узла конфигурации адреса SSH делает возможным использование протокола SSH для получения доступа к системе по этому адресу. По умолчанию маршрутизатор использует для службы SSH порт 22. Поддерживается только вторая версия протокола SSH.

Форма **set** данной команды используется для создания настройки SSH.

Форма **delete** данной команды используется для удаления настройки SSH. При удалении узла конфигурации SSH доступ к системе по протоколу SSH будет отключен на всех портах, за исключением управляющего.

Форма **show** данной команды используется для отображения настройки прослушиваемых адресов сервиса SSH.

## 20.2.2. 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*

Допустимый для использования протоколом SSH алгоритм шифрования. Множественный узел.

**Значение по умолчанию**

По умолчанию разрешён только алгоритм ГОСТ 28147-89 («**gost89**»).

**Указания по использованию**

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

Форма **set** этой команды используется для указания того, чтобы разрешить использование того или иного алгоритма шифрования при подключении по SSH. Возможно задание нескольких поддерживаемых алгоритмов.

Форма **delete** этой команды используется для запрещения использования того или иного алгоритма при подключении по SSH.

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

### 20.2.3. 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. Сведения по настройке открытых ключей для аутентификации приведены в разделе 4.1.3. Настройка для доступа по SSH с помощью общих открытых ключей .*

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 отмены парольной аутентификации.

Форма **delete** данной команды используется для восстановления настройки по умолчанию и включения парольной аутентификации.

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

# 21. НАСТРОЙКА ДОСТУПА К WEB-ИНТЕРФЕЙСУ

## 21.1. Настройка HTTPS

Безопасный механизм входа в систему Altell NEO 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). 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.

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 Altell NEO должен быть в обязательном порядке указан используемый Web-сервером сертификат. По умолчанию в системе Altell NEO 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.

По умолчанию для аутентификации Web-сервера используется криптографический алгоритм ГОСТ 34.10-2001, для шифрования и аутентификации передаваемых данных используется криптографический алгоритм ГОСТ 28147-89. По этой причине необходимо использовать браузер, который поддерживает данный набор криптографических алгоритмов. В комплекте с Altell NEO на диске с дополнительным программным обеспечением поставляется браузер для операционных систем Windows 2000/XP/2003/Vista/Windows 7.

В примере 21.1 приведено разрешение доступа к Web-интерфейсу по заранее настроенному в системе адресу 192.168.10.1, а также изменение сертификата, используемого по умолчанию для получения доступа к Web-интерфейсу на основе HTTPS, на сертификат

созданный сторонним удостоверяющим центром. Подробнее об импорте сертификатов см. раздел 16.3.23. pki import.

*Пример 21.1 - Разрешение доступа к Web-интерфейсу по указанному адресу*

| Действие | Команда |
|---|---|
| Импорт сертификата веб-сервера, сгенерированного сторонним удостоверяющим центром с подключенного флэш-накопителя. | admin@neo:~$ **pki import**<br>Импортируется CA: Test CA<br>Test_CA130071181<br>Импортируется CRL для Test_CA<br>Импортируется сертификат: Test NEO |
| Отображение настройки. | admin@neo# **show pki**<br>ca defaultca {<br>certificate neo_web_cert {<br>cn "Altell NEO Web Interface"<br>email root@altell-neo<br>expiration 1825<br>}<br>cn "Default NEO CA"<br>expiration 1825<br>}<br>ca Test_CA {<br>certificate Test_NEO {<br>cn "Test NEO"<br>}<br>cn "Test CA"<br>}<br>[edit] |
| Указание адреса, который будет прослушиваться на предмет входящих | admin@neo# **set service https address 192.168.10.1** |

| | |
|---|---|
| подключений. | `[edit]` |
| Указание сертификата, который будет использоваться для подключения к Web-интерфейсу с использованием HTTPS. | `admin@neo# set service https x509-cert Test_NEO`<br>`[edit]` |
| Фиксация настройки. | `admin@neo# commit` |
| Просмотр настройки. | `admin@neo# show service https`<br>`address 192.168.10.1 {`<br>`https-port 443`<br>`www-port 80`<br>`}`<br>`x509-cert Test_NEO`<br>`[edit]` |

## 21.2. Команды HTTPS

| Команды настройки | |
|---|---|
| service https address <адрес> | Включение доступа к Web-интерфейсу на определённом адресе. |
| service https address <адрес> https-port | 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. |

### 21.2.1. service https address <адрес>

Включение доступа к Web-интерфейсу Altell NEO 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 ipv4-адрес {
        }
    }
}
```

**Параметры**

*адрес*

Адрес, на котором будут приниматься запросы 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 HTTPS от удаленных систем на конкретных адресах локальной системы.

Создание узла конфигурации адреса HTTPS делает возможным использование протокола HTTPS для получения доступа к системе по этому адресу.

Форма **set** данной команды используется для создания настройки HTTPS.

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

При удалении узла конфигурации HTTPS доступ к системе по протоколу HTTPS будет отключен на всех портах, за исключением управляющего.

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

прослушиваемых адресов сервиса HTTPS.

### 21.2.2. service https address <адрес> https-port

Включение доступа к Web-интерфейсу Altell NEO 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 ipv4-адрес {
            https-port 0-65535
        }
    }
}
```

**Параметры**

*адрес*

Адрес, на котором будут приниматься запросы HTTPS.

*порт*

Номер сетевого порта, на котором будут приниматься запросы HTTPS.

**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 .

По умолчанию для доступа к Web-интерфейсу на основе протокола HTTPS

используется порт 443.

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.

### 21.2.3. 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 ipv4-адрес {
            www-port 0-65535
        }
    }
}
```

**Параметры**

*адрес*

Адрес, на котором будут приниматься запросы HTTP.

*порт*

Номер сетевого порта, на котором будут приниматься запросы HTTP.

**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 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.

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.

### 21.2.4. service https x509-cert <имя_сертификата>

Указание сертификата Web-сервера, используемого для проверки подлинности при подключении к Web-интерфейсу Altell NEO.

**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 текст
        }
    }
}
```

**Параметры**

*имя_сертификата*

Обязательный. Имя сертификата Web-сервера, используемого для проверки

подлинности.

**Значение по умолчанию**

По умолчанию в системе Altell NEO предустановлен удостоверяющий центр (CN = Default NEO CA), на базе которого создан и заверен сертификат Web-сервера (CN=Altell NEO 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 Altell NEO. Может быть использован, как сертификат созданный при помощи модуля PKI (см. раздел 16. на стр. 1042), так и сертификат, созданный при помощи стороннего удостоверяющего центра. В этом случае сертификат необходимо предварительно импортировать в систему при помощи команды **pki import** (см. раздел 16.3.23. на стр.1083). Тип открытого ключа указанного в сертификате определяет набор криптографических алгоритмов, которые используются для обеспечения безопасности передаваемых данных.

По умолчанию для аутентификации Web-сервера используется криптографический алгоритм ГОСТ 34.10-2001, для шифрования и аутентификации передаваемых данных используется криптографический алгоритм ГОСТ 28147-89. По этой причине необходимо использовать браузер, который поддерживает данный набор криптографических алгоритмов. В комплекте с Altell NEO на диске с дополнительным программным обеспечением поставляется браузер для операционных систем Windows 2000/XP/2003/Vista/Windows 7.

Форма **set** данной команды используется для указания сертификата, используемого для подключения к Web-интерфейсу Altell NEO при помощи HTTPS.

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

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

# 22. DHCP

## 22.1. 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 Altell NEO, 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 NEO можно настроить в качестве клиентов DHCP. Более подробные сведения о клиентских настройках представлены в разделах документации Altell NEO по настройке интерфейсов, которые требуется настроить в качестве клиентов DHCP (для интерфейсов Ethernet см. раздел 6.2.3. interfaces ethernet <ethx> address ).

В поставляемом Altell NEO 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.

## 22.2. Настройка DHCP

В разделе приводятся следующие примеры:

- Настройка пулов адресов DHCP.
- Резервирование адресов.
- Установка дополнительных параметров настройки DHCP.

### 22.2.1. Настройка пулов адресов DHCP

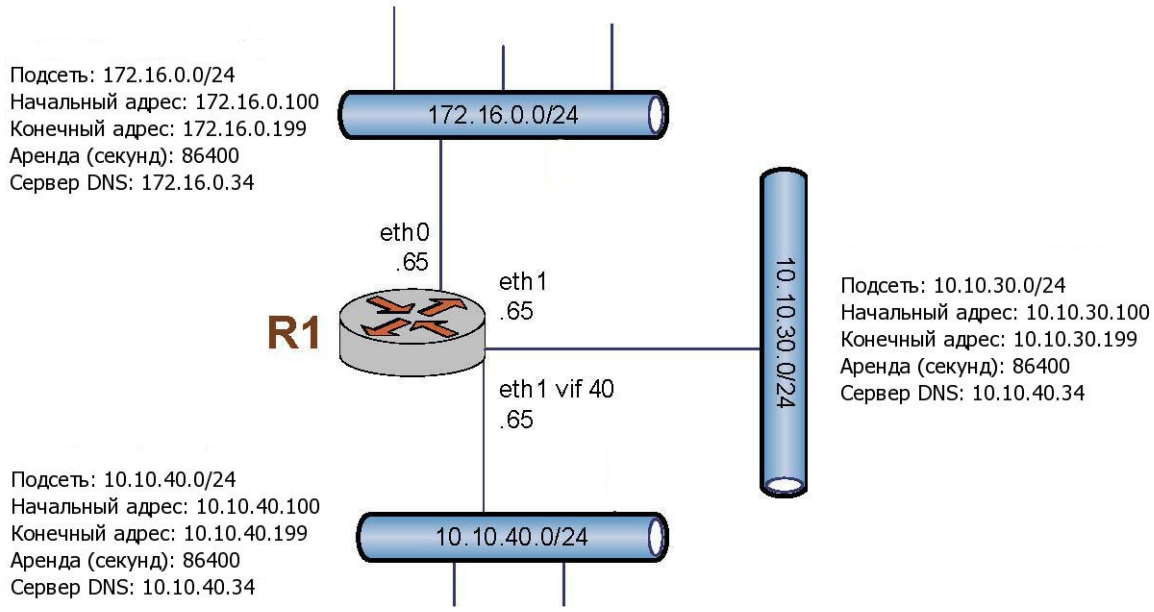
При необходимости настройки системы в качестве сервера DHCP для сети, следует настроить пулы адресов DHCP.

В примере 22.1 выполняется создание трех пулов адресов:

- **172.16.0.100-172.16.0.199**. Этот пул адресов обслуживает подсеть 172.16.0.0/24, подключенную к интерфейсу eth0. Для времени аренды оставлено значение по умолчанию 24 часа (86400 секунд). Для этого пула адресов будет использоваться сервер имен DNS с адресом 172.16.0.34.
- **10.10.30.100-10.10.30.199**. Этот пул адресов обслуживает подсеть 10.10.30.0/24, подключенную напрямую к интерфейсу eth1. Для времени аренды оставлено значение по умолчанию 24 часа (86400 секунд). В этом пуле адресов будет использоваться сервер имен DNS по адресу 10.10.40.34, который непосредственно подключен к интерфейсу eth1.40 (то есть к eth1 vif 40).
- **10.10.40.100-10.10.40.199**. Этот пул адресов обслуживает подсеть 10.10.40.0/24, подключенную к интерфейсу eth1.40. Для времени аренды оставлено значение по умолчанию 24 часа (86400 секунд). В этом пуле адресов будет использоваться сервер имен DNS по адресу 10.10.40.34, который непосредственно подключен к интерфейсу eth1.40.

На рисунке 81 показан пример настройки пулов адресов.

*Рисунок 81 - Настройка пулов адресов*




Для настройки пулов адресов DHCP выполните следующие действия в режиме настройки:

*Пример 22.1 - Настройка пулов адресов DHCP*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для подсети 172.16.0.0/24. Ввод начального и конечного IP-адресов для пула. | `admin@R1# set service dhcp-server subnet 172.16.0.0/24 start 172.16.0.100 stop 172.16.0.199 [edit]` |
| Ввод маршрутизатора по умолчанию для клиентов подсети 172.16.0.0/24. | `admin@R1# set service dhcp-server subnet 172.16.0.0/24 default-router 172.16.0.65 [edit]` |
| Ввод сервера DNS для клиентов подсети 172.16.0.0/24. | `admin@R1# set service dhcp-server subnet 172.16.0.0/24 dns-server` |

| | |
|---|---|
| | **172.16.0.34**<br>[edit] |
| Создание узла конфигурации для подсети 10.10.30.0/24. Ввод начального и конечного IP-адресов для пула. | admin@R1# **set service dhcp-server subnet 10.10.30.0/24 start 10.10.30.100 stop 10.10.30.199**<br>[edit] |
| Ввод маршрутизатора по умолчанию для клиентов подсети 10.10.30.0/24. | admin@R1# **set service dhcp-server subnet 10.10.30.0/24 default-router 10.10.30.65**<br>[edit] |
| Ввод сервера DNS для клиентов подсети 10.10.30.0/24. | admin@R1# **set service dhcp-server subnet 10.10.30.0/24 dns-server 10.10.40.34**<br>[edit] |
| Создание узла конфигурации для подсети 10.10.40.0/24. Ввод начального и конечного IP-адресов для пула. | admin@R1# **set service dhcp-server subnet 10.10.40.0/24 start 10.10.40.100 stop 10.10.40.199**<br>[edit] |
| Ввод маршрутизатора по умолчанию клиентов подсети 10.10.40.0/24. | admin@R1# **set service dhcp-server subnet 10.10.40.0/24 default-router 10.10.40.65**<br>[edit] |
| Ввод сервера DNS для клиентов подсети 10.10.40.0/24. | admin@R1# **set service dhcp-server subnet 10.10.40.0/24 dns-server 10.10.40.34**<br>[edit] |
| Фиксация изменений. | admin@R1# **commit**<br>[edit] |
| Вывод настройки. | admin@R1# **show service dhcp-** |

```
server
   subnet 10.10.30.0/24 {
       default-router 10.10.30.65
       dns-server 10.10.40.34
       start 10.10.30.100 {
           stop 10.10.30.199
       }
   }
   subnet 10.10.40.0/24 {
       default-router 10.10.40.65
       dns-server 10.10.40.34
       start 10.10.40.100 {
           stop 10.10.40.199
       }
   }
   subnet 172.16.0.0/24 {
       default-router 172.16.0.65
       dns-server 172.16.0.34
       start 172.16.0.100 {
           stop 172.16.0.199
       }
   }
[edit]
```

Вывод настройки интерфейсов.

```
admin@R1# show interfaces
ethernet eth0 {
     address 172.16.0.65/24
}
ethernet eth1 {
     address 10.10.30.65/24
     vif 40 {
          address 10.10.40.65/24
```

```
        }
    }
    [edit]
```

### 22.2.2. 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 22.1. В примере 22.2 выполняется следующая операция:

- Резервирование IP-адреса 172.16.0.101 для устройства с MAC-адресом 00:15:c5:b3:2e:65.

*Пример 22.2 - Резервирование адреса для клиента*

| Действие | Команда |
|---|---|
| Создание резерва с именем “lab” и ввод статического IP-адреса из диапазона для подсети 172.16.0.0/24 . | admin@R1# **set service dhcp-server subnet 172.16.0.0/24 static-mapping lab ip-address 172.16.0.101**<br>[edit] |
| Ввод соответствующего MAC-адреса для резерва из подсети 172.16.0.0/24. | admin@R1# **set service dhcp-server subnet 172.16.0.0/24 static-mapping lab mac-address 00:15:c5:b3:2e:65**<br>[edit] |
| Фиксация изменений. | admin@R1# **commit**<br>[edit] |
| Вывод настройки. | admin@R1# **show service dhcp-server subnet 172.16.0.0/24** |

```
    default-router 172.16.0.65
    dns-server 172.16.0.34
    start 172.16.0.100 {
        stop 172.16.0.199
    }
    static-mapping lab {
        ip-address 172.16.0.101
        mac-address
00:15:c5:b3:2e:65
    }
[edit]
```

### 22.2.3. 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 маршрутизуемого IP-адреса, а также ему не известен 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.

Интерфейсы, задействованные в ретрансляции DHCP, должны быть в обязательном порядке указаны в настройке агента ретрансляции при помощи команд **service dhcp-relay client-interface** и **service dhcp-relay server-interface**. Например, если запросы от клиентов DHCP принимаются на интерфейсе **eth0**, а указанный в настройке сервер DHCP достижим через интерфейс **eth1**, оба этих интерфейса должны быть указаны в настройке агента ретрансляции DHCP. При этом указанные интерфейсы должны быть заранее определены, а также им должны быть назначены IP-адреса.

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 (**client-interface**).

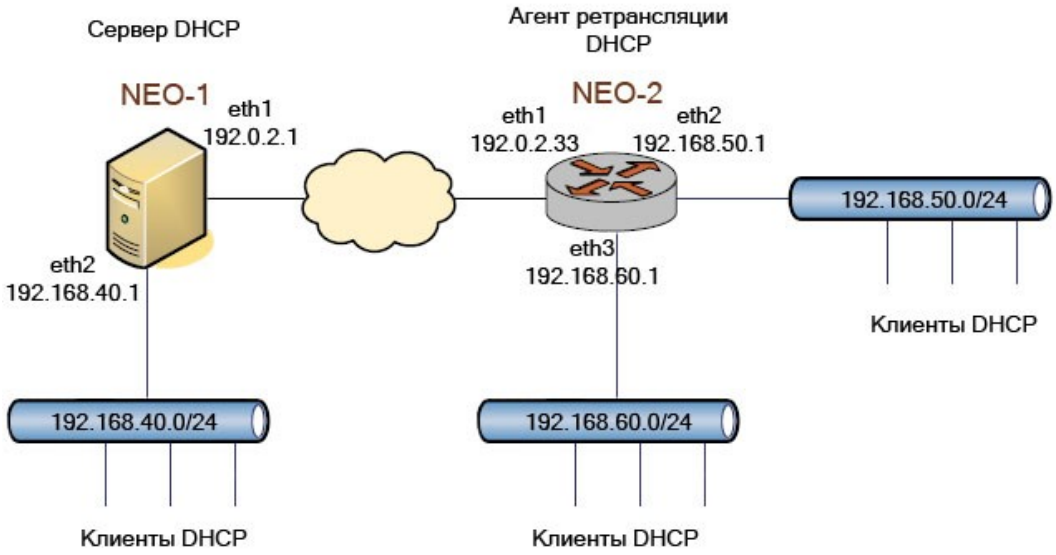
Сервер DHCP направляет ответы на адрес интерфейса агента ретрансляции, на котором был получен запрос от клиента, таким образом, необходимо соответствующим образом настроить маршрутизацию на сервере DHCP.

В данном разделе приведены следующие примеры:

- Пример 22.3 - Настройка ретрансляции DHCP.
- Пример 22.4 - Настройка сервера DHCP.
- Пример 22.5 - Определение статического маршрута на сервере DHCP.

В результате выполнения данных примеров система будет настроена в соответствии с рисунком 82.

*Рисунок 82 - Ретрансляция DHCP*




В примере 22.3 приведена настройка узла NEO-2 в качестве агента ретрансляции DHCP.

*Пример 22.3 - Настройка ретрансляции DHCP*

| Действие | Команда |
|---|---|
| Указание интерфейсов, на котором будут приниматься запросы от клиентов DHCP. | `admin@NEO-2# set service dhcp-relay client-interface eth2 [edit]`<br>`admin@NEO-2# set service dhcp-relay client-interface eth3 [edit]` |
| Указание интерфейса, через который запросы от клиентов DHCP будут перенаправляться на сервер DHCP. | `admin@NEO-2# set service dhcp-relay server-interface eth1 [edit]` |
| Указание адреса сервера DHCP, которому будут перенаправляться запросы. | `admin@NEO-2# set service dhcp-relay server-address 192.2.0.1 [edit]` |
| Фиксация настройки. | `admin@NEO-2# commit` |

```
[edit]
```

Отображение настройки.

```
admin@NEO-2# show service dhcp-
relay
   client-interface eth2
   client-interface eth3
   server-interface eth1
[edit]
```

В примере 22.4 приведена настройка узла NEO-1 в качестве сервера DHCP.

*Пример 22.4 - Настройка сервера DHCP*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для подсети 192.168.40.0/24. Ввод начального и конечного IP-адресов для пула. | `admin@NEO-1# set service dhcp-server subnet 192.168.40.0/24 start 192.168.40.101 stop 192.168.40.111`<br>`[edit]` |
| Ввод маршрутизатора по умолчанию для клиентов подсети 192.168.40.0/24. | `admin@NEO-1# set service dhcp-server subnet 192.168.40.0/24 default-router 192.168.40.1`<br>`[edit]` |
| Ввод сервера DNS для клиентов подсети 192.168.40.0/24. | `admin@NEO-1# set service dhcp-server subnet 192.168.40.0/24 dns-server 192.168.40.1`<br>`[edit]` |
| Создание узла конфигурации для подсети 192.168.50.0/24. Ввод начального и конечного IP-адресов для пула. | `admin@NEO-1# set service dhcp-server subnet 192.168.50.0/24 start 192.168.50.101 stop 192.168.50.111`<br>`[edit]` |
| Ввод маршрутизатора по умолчанию для | `admin@NEO-1# set service dhcp-` |

| | |
|---|---|
| клиентов подсети 192.168.50.0/24. | **server subnet 192.168.50.0/24 default-router 192.168.50.1**<br>[edit] |
| Ввод сервера DNS для клиентов подсети 192.168.50.0/24. | admin@NEO-1# **set service dhcp-server subnet 192.168.50.0/24 dns-server 192.168.50.1**<br>[edit] |
| Создание узла конфигурации для подсети 192.168.60.0/24. Ввод начального и конечного IP-адресов для пула. | admin@NEO-1# **set service dhcp-server subnet 192.168.60.0/24 start 192.168.60.101 stop 192.168.60.111**<br>[edit] |
| Ввод маршрутизатора по умолчанию для клиентов подсети 192.168.60.0/24. | admin@NEO-1# **set service dhcp-server subnet 192.168.60.0/24 default-router 192.168.60.1**<br>[edit] |
| Ввод сервера DNS для клиентов подсети 192.168.60.0/24. | admin@NEO-1# **set service dhcp-server subnet 192.168.60.0/24 dns-server 192.168.60.1**<br>[edit] |
| Создание статического маршрута к подсети 192.168.50.0/24. | admin@NEO-1# **set protocols static route 192.168.50.0/24 next-hop 192.0.2.33** |
| Создание статического маршрута к подсети 192.168.60.0/24. | admin@NEO-1# **set protocols static route 192.168.60.0/24 next-hop 192.0.2.33** |
| Фиксация настройки. | admin@NEO-1# **commit**<br>[edit] |
| Вывод настройки | admin@NEO-1# **show service dhcp-** |

```
server
   subnet 192.168.40.0/24 {
       default-router
192.168.40.1
       dns-server 192.168.40.1
       start 192.168.40.101 {
           stop 192.168.40.111
       }
   }
subnet 192.168.50.0/24 {
       default-router
192.168.50.1
       start 192.168.50.101 {
           stop 192.168.50.111
       }
   }
   subnet 192.168.60.0/24 {
       default-router
192.168.60.1
       start 192.168.60.101 {
           stop 192.168.60.111
       }
   }
[edit]
```

В примере 22.5 приведено определение статических маршрутов к удаленным подсетям на сервере DHCP.

Для того чтобы указать внешний интерфейс агента ретрансляции (192.0.2.33) в качестве следующего транзитного участка для трафика, предназначенного подсетям 192.168.50.0/24 и 192.168.60.0/24, необходимо выполнить следующие действия в режиме настройки:

*Пример 22.5 - Определение статического маршрута на сервере DHCP*

| Действие | **Команда** |
|---|---|
| Создание статического маршрута к подсети 192.168.50.0/24. | admin@NEO-1# **set protocols static route 192.168.50.0/24 next-hop 192.0.2.33** |
| Создание статического маршрута к подсети 192.168.60.0/24. | admin@NEO-1# **set protocols static route 192.168.60.0/24 next-hop 192.0.2.33** |
| Фиксация настройки. | admin@NEO-1# **commit**<br>[edit] |
| Отображение настройки. | admin@NEO-1# **show protocols**<br>static {<br>route 192.168.50.0/24 {<br>next-hop 192.0.2.33 {<br>}<br>}<br>route 192.168.60.0/24 {<br>next-hop 192.0.2.33 {<br>}<br>}<br>}<br>[edit] |

## 22.3. Команды DHCP

В данном разделе представлены следующие команды:

*Таблица 46 - Команды DHCP*

| Команды настройки сервера DHCP | |
|---|---|
| service dhcp-server | Включение функциональности сервера DHCP. |
| service dhcp-server disabled | Возможность отключения сервера DHCP без |

| | |
|---|---|
| | отбрасывания настройки. |
| `service dhcp-server authoritative <состояние>` | Указание полномочности сервера DHCP. |
| `service dhcp-server subnet <подсеть_ipv4>` | Указание сети IPv4, которая будет обслуживаться пулом адресов DHCP. |
| `service dhcp-server subnet <подсеть_ipv4> bootfile-name <файл_загрузки>` | 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 <префикс_ipv4> default-router <ipv4-адрес>` | Указание маршрутизатора по умолчанию для клиентов DHCP в данной подсети. |
| `service dhcp-server subnet <подсеть_ipv4> dns-server <ipv4-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> ntp-server <ipv4-адрес>` | Указание адреса сервера протокола NTP, доступного для клиентов. |
| `service dhcp-server subnet <подсеть_ipv4> pop-server` | Указание адреса сервера протокола POP3, доступного для клиентов. |

| | |
|---|---|
| `service dhcp-server subnet <подсеть_ipv4> server-identifier <ipv4-адрес>` | Указание адреса идентифицирующего сервер DHCP. |
| `service dhcp-server subnet <подсеть_ipv4> smtp-server <ipv4-адрес>` | Указание адреса сервера протокола SMTP, доступного для клиентов. |
| `service dhcp-server subnet <подсеть_ipv4> start <ipv4-адрес> stop <ipv4-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 <ipv4-адрес>` | Указание статического IP-адреса для конкретного клиента DHCP. |
| `service dhcp-server subnet <подсеть_ipv4> static-mapping <имя_резерва> mac-address <mac-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 <ipv4-адрес>` | Указание шлюза для статического маршрута, передаваемого клиентам. |
| `service dhcp-server subnet` | 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 <ipv4-адрес>` | Указание адреса сервера времени RFC868, доступного для клиентов. |
| `service dhcp-server subnet <подсеть_ipv4> wins-server <ipv4-адрес>` | Указание адреса сервера WINS, доступного для клиентов DHCP. |
| `service dhcp-server subnet <подсеть_ipv4> wpad-url <url-адрес>` | Указание URL-адреса службы автоопределения веб-прокси (WPAD). |
| Ретрансляция DHCP | |
| `service dhcp-relay` | Настройка системы в качестве агента ретрансляции DHCP. |
| `service dhcp-relay client-interface <интерфейс>` | Указание интерфейса, на котором будут приниматься запросы от клиентов DHCP. |
| `service dhcp-relay server-interface <интерфейс>` | Указание интерфейса, через который запросы от клиентов DHCP будут передаваться на сервер DHCP. |
| `service dhcp-relay server-address <ipv4-адрес>` | Указание IP-адреса сервера DHCP, которому будут передаваться запросы от клиентов DHCP. |
| `service dhcp-relay disabled <состояние>` | Отключение ретрансляции DHCP с сохранением настройки. |
| Эксплуатационные команды | |
| `release dhcp interface <интерфейс>` | Освобождение текущей аренды клиента DHCP на интерфейсе. |
| `renew dhcp interface <интерфейс>` | Обновление текущей аренды клиента DHCP на интерфейсе. |

| | |
|---|---|
| `show dhcp client leases` | Отображение сведений DHCP для интерфейсов, настроенных как клиенты DHCP. |
| `show dhcp leases` | Отображение сведений о текущих арендах DHCP. |

### 22.3.1. release dhcp interface <интерфейс>

Освобождение текущей клиентской аренды DHCP на интерфейсе.

**Синтаксис**

**`release dhcp 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.

### 22.3.2. renew dhcp interface <интерфейс>

Обновление текущей клиентской аренды DHCP на интерфейсе.

**Синтаксис**

**`renew dhcp 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.

### 22.3.3. service dhcp-relay

Настройка системы в качестве агента ретрансляции DHCP.

**Синтаксис**

```
set service dhcp-relay
delete service dhcp-relay
show service dhcp-relay
```

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    dhcp-relay {
    }
}
```

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для настройки системы Altell NEO 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, устанавливает адрес интерфейса, на котором был получен запрос, в поле GIADDR пакета

DHCP, затем передает его серверу. Сервер возвращает ответ агенту ретрансляции, после чего агент транслирует его с помощью широковещательной рассылки.

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.

### 22.3.4. service dhcp-relay client-interface <интерфейс>

Указание интерфейса, на котором будут приниматься запросы от клиентов DHCP.

**Синтаксис**

```
set service dhcp-relay client-interface интерфейс
delete service dhcp-relay client-interface
show service dhcp-relay client-interface
```

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    dhcp-relay {
        client-interface текст
    }
}
```

**Параметры**

*интерфейс*

Обязательный. Множественный узел. Идентификатор интерфейса, на котором будут приниматься запросы от клиентов DHCP. Для того чтобы указать несколько интерфейсов, следует создать соответствующее количество узлов конфигурации **client-interface**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет указать интерфейс, на котором будут приниматься запросы от клиентов DHCP, которые затем будут переданы серверу DHCP.

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 интерфейсах, задействованных при ретрансляции (указанных в настройке агента ретрансляции при помощи команд **service dhcp-relay server-interface** и **service dhcp-relay client-interface**).

Форма **set** этой команды используется для указания интерфейса, на котором будут приниматься запросы от клиентов DHCP.

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

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

## 22.3.5. service dhcp-relay server-interface <интерфейс>

Указание интерфейса, через который запросы от клиентов DHCP будут передаваться серверу DHCP.

**Синтаксис**

**set service dhcp-relay server-interface** *интерфейс*

**delete service dhcp-relay server-interface**

**show service dhcp-relay server-interface**

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    dhcp-relay {
        server-interface текст
    }
}
```

**Параметры**

*интерфейс*

Обязательный. Множественный узел. Идентификатор интерфейса, через который запросы от клиентов DHCP будут передаваться серверу DHCP. Для того чтобы указать несколько интерфейсов, следует создать соответствующее количество узлов конфигурации **server-interface**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет указать интерфейс, через который запросы от клиентов DHCP будут передаваться серверу DHCP.

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 интерфейсах, задействованных при ретрансляции (указанных в настройке агента ретрансляции при помощи команд **service dhcp-relay server-interface** и **service dhcp-relay client-interface**).

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.

## 22.3.6. service dhcp-relay server-address <ipv4-адрес>

Указание IP-адреса сервера DHCP, которому будут передаваться запросы от клиентов DHCP.

**Синтаксис**

```
set service dhcp-relay server-address ipv4-адрес
delete service dhcp-relay server-address
show service dhcp-relay server-address
```

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    dhcp-relay {
        server-address ipv4-адрес
```

```
        }
    }
```

**Параметры**

*ipv4-адрес*

Множественный. IP-адрес сервера DHCP, которому будут перенаправляться запросы от клиентов. Для того чтобы указать несколько серверов DHCP в настройке агента ретрансляции, следует создать соответствующее количество узлов конфигурации **server-address**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет указать адрес сервера DHCP, которому будут передаваться запросы от клиентов DHCP. В том случае если адрес сервера явно не указан, агент ретрансляции для передачи сообщений от клиентов DHCP использует широковещательную рассылку в подсети, к которой подключен интерфейс, указанный с помощью команды **service dhcp-relay server-interface**.

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.

## 22.3.7. service dhcp-relay disabled <состояние>

Отключение ретрансляции DHCP с сохранением настройки.

**Синтаксис**

```
set service dhcp-relay disabled [true|false]
delete service dhcp-relay
show service dhcp-relay
```

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    dhcp-relay {
```

```
        }
    }
```

**Параметры**

`состояние`

Административное состояние агента ретрансляции DHCP. Допустимые значения:

**true**: Отключение ретрансляции DHCP с сохранением настройки.

**false**: Включение ретрансляции DHCP.

**Значение по умолчанию**

По умолчанию установлено значение **false**.

**Указания по использованию**

Данная команда позволяет отключить ретрансляцию DHCP без удаления настройки.

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 интерфейсах, задействованных при ретрансляции (указанных в настройке агента ретрансляции при помощи команд **service dhcp-relay server-interface** и **service dhcp-relay client-interface**). При отключении ретрансляции DHCP происходит перезапуск сервера DHCP, после чего он будет отвечать на запросы клиентов на всех интерфейсах.

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 настройки.

## 22.3.8. 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.

## 22.3.9. service dhcp-server disabled <состояние>

Возможность отключения сервера DHCP без удаления настройки.

**Синтаксис**

```
set service dhcp-server disabled состояние
delete service dhcp-server disabled
show service dhcp-server disabled
```

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    dhcp-server {
        disabled [true|false]
    }
}
```

**Параметры**

*состояние*

Административное состояние сервера DHCP. Поддерживаются следующие значения:

**true**: Отключение сервера DHCP без отбрасывания настройки.

**false**: Включение сервера DHCP.

**Значение по умолчанию**

Функциональность сервера DHCP включена.

**Указания по использованию**

Эта команда используется для отключения сервера DHCP без отбрасывания 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 настройки сервера DHCP.

## 22.3.10. service dhcp-server authoritative <состояние>

Указание полномочности 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 [enable|disable]
    }
}
```

**Параметры**

*состояние*

Указание полномочности сервера DHCP. Поддерживаются следующие значения:

**enable**: Полномочное состояние включено.

**disable**: Полномочное состояние отключено.

**Значение по умолчанию**

Сервер DHCP не является полномочным.

**Указания по использованию**

Эта команда используется для установки сервера в качестве полномочного сервера DHCP.

Установка сервера в качестве полномочного делает его главным сервером и позволяет ему защититься от неавторизованных серверов DHCP или неправильно настроенных клиентов DHCP. Если сервер является полномочным, 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 полномочного состояния для сервера DHCP.

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

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

### 22.3.11. service dhcp-server subnet <подсеть_ipv4>

Указание сети IPv4, которая будет обслуживаться пулом адресов DHCP.

**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*

Обязательный параметр. Множественный узел. Подсеть IPv4, которая должна обслуживаться адресами, определенными в указанном пуле адресов. Используется формат *ip-адрес/префикс*.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для указания подсети IPv4, которая должна обслуживаться адресами, определенными в указанном пуле адресов. Запросы DHCP от устройств из этой подсети обслуживаются адресами заданного пула или статическим назначением адресов.

Форма **set** этой команды используется для указания подсети пула адресов DHCP.

Форма **delete** этой команды используется для удаления настройки подсети пула адресов DHCP.

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

пула адресов DHCP.

### 22.3.12. service dhcp-server subnet <подсеть_ipv4> bootfile-name <файл_загрузки>

Указание файла начальной загрузки, который могут использовать для загрузки бездисковые ПК.

**Синтаксис**

**set service dhcp-server subnet** *подсеть_ipv4* **bootfile-name** *файл_загрузки*

**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 текст
        }
    }
}
```

**Параметры**

*подсеть_ipv4*

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Используется формат *ip-адрес/префикс*.

*файл_загрузки*

Имя файла начальной загрузки, используемого для загрузки.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для указания файла начальной загрузки, из которого могут загружаться бездисковые ПК.

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.

## 22.3.13. service dhcp-server subnet <подсеть_ipv4> bootfile-server <адрес>

Указание сервера начальной загрузки, с которого могут загружаться бездисковые ПК.

**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 ipv4
        }
    }
}
```

**Параметры**

*подсеть_ipv4*

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Используется формат *ip-*

*адрес/префикс*.

*ipv4*

IPv4-адрес сервера, хранящего файл начальной загрузки.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для указания сервера начальной загрузки, с которого могут загружаться бездисковые ПК.

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.

### 22.3.14. 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 0-32
        }
```

```
        }
    }
```

**Параметры**

*подсеть_ipv4*

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Используется формат *ip-адрес/префикс*.

*префикс*

Необязательный параметр. Данное значение длины префикса подсети будет назначено каждому клиенту. Значение должно лежать 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**.

## 22.3.15. service dhcp-server subnet <префикс_ipv4> default-router <ipv4-адрес>

Указание маршрутизатора по умолчанию для клиентов DHCP в данной подсети.

**Синтаксис**

**set service dhcp-server subnet** *подсеть_ipv4* **default-router** *ipv4-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 ipv4-адрес
        }
    }
}
```

**Параметры**

*подсеть_ipv4*

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Используется формат *ip-адрес/префикс*.

*ipv4-адрес*

Необязательный параметр. Маршрутизатор по умолчанию для клиентов DHCP в данной подсети. Маршрутизатор по умолчанию должен быть расположен в той же подсети, что и клиент. Используется формат IP-адреса.

**Значение по умолчанию**

По умолчанию используется IP адрес системы в обслуживаемой сервисом DHCP сети.

**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**.

## 22.3.16. service dhcp-server subnet <подсеть_ipv4> dns-server <ipv4-адрес>

Указание сервера DNS для клиентов DHCP.

### Синтаксис

**set service dhcp-server subnet** *подсеть_ipv4* **dns-server** *ipv4-адрес*

**delete service dhcp-server subnet** *подсеть_ipv4* **dns-server** *ipv4-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 ipv4-адрес
        }
    }
}
```

### Параметры

*подсеть_ipv4*

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Используется формат *ip-адрес/префикс*.

*ipv4-адрес*

Необязательный параметр. Множественный узел. IPv4-адрес сервера DNS. Можно указать более одного сервера DNS, выдав эту команду несколько раз.

**Значение по умолчанию**

По умолчанию используется IP адрес системы в обслуживаемой сервисом DHCP сети.

**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.

## 22.3.17. 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 текст
        }
    }
}
```

**Параметры**

*подсеть_ipv4*

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Используется формат *ip-адрес/префикс*.

*имя_домена*

Необязательный параметр. 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.

## 22.3.18. service dhcp-server subnet <подсеть_ipv4> lease <секунды>

Указание времени действительности адреса, назначенного сервером DHCP.

**Синтаксис**

**set service dhcp-server subnet** *подсеть_ipv4* **lease** *секунды*

**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 целоебеззнака32разр
            }
        }
    }
```

**Параметры**

*подсеть_ipv4*

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Используется формат *ip-адрес/префикс*.

*секунды*

Необязательный параметр. Указание времени (в секундах) действительности адреса, назначенного сервером DHCP. Значение должно лежать в диапазоне от 120 до 4294967296.

**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.

## 22.3.19. service dhcp-server subnet <подсеть_ipv4> ntp-server <ipv4-адрес>

Указание адреса сервера протокола NTP, доступного для клиентов.

**Синтаксис**

**set service dhcp-server subnet** *подсеть_ipv4* **ntp-server** *ipv4-адрес*

**delete service dhcp-server subnet** *подсеть_ipv4* **ntp-server** *ipv4-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 ipv4-адрес
        }
    }
}
```

**Параметры**

*подсеть_ipv4*

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Используется формат *ip-адрес/префикс*.

*ipv4-адрес*

Необязательный параметр. Указание IP-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.

## 22.3.20. service dhcp-server subnet <подсеть_ipv4> pop-server <ipv4-адрес>

Указание адреса сервера протокола POP3, доступного для клиентов.

**Синтаксис**

**set service dhcp-server subnet** *подсеть_ipv4* **pop-server** *ipv4-адрес*

**delete service dhcp-server subnet** *подсеть_ipv4* **pop-server** *ipv4-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 ipv4-адрес
        }
    }
}
```

**Параметры**

*подсеть_ipv4*

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Используется формат *ip-адрес/префикс*.

*ipv4-адрес*

Необязательный параметр. Указание IP-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.

## 22.3.21. service dhcp-server subnet <подсеть_ipv4> server-identifier <ipv4-адрес>

Указание адреса идентифицирующего сервер DHCP.

**Синтаксис**

```
set service dhcp-server subnet подсеть_ipv4 server-identifier ipv4-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 ipv4-адрес
        }
    }
}
```

**Параметры**

*подсеть_ipv4*

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Используется формат *ip-адрес/префикс*.

*ipv4-адрес*

Необязательный параметр. Указание 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.

## 22.3.22. service dhcp-server subnet <подсеть_ipv4> smtp-server <ipv4-адрес>

Указание адреса сервера протокола SMTP, доступного для клиентов.

**Синтаксис**

**set service dhcp-server subnet** *подсеть_ipv4* **smtp-server** *ipv4-адрес*

**delete service dhcp-server subnet** *подсеть_ipv4* **smtp-server** *ipv4-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 ipv4-адрес
            }
        }
    }
```

**Параметры**

*подсеть_ipv4*

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Используется формат *ip-адрес/префикс*.

*ipv4-адрес*

Необязательный параметр. Указание IP-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.

## 22.3.23. service dhcp-server subnet <подсеть_ipv4> start <ipv4-адрес> stop <ipv4-адрес>

Указание диапазона адресов, которые будут назначаться клиентам DHCP.

**Синтаксис**

**set service dhcp-server subnet** *подсеть_ipv4* **start** *ipv4-адрес* **stop** *ipv4-адрес*

**delete service dhcp-server subnet** *подсеть_ipv4* **start [***ipv4-адрес* **[stop]]**

**show service dhcp-server subnet** *подсеть_ipv4* **start [***ipv4-адрес***]**

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    dhcp-server {
        subnet подсеть_ipv4 {
            start ipv4-адрес {
                stop ipv4-адрес
            }
        }
    }
}
```

**Параметры**

*подсеть_ipv4*

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Используется формат *ip-адрес/префикс*.

*start*

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.

*stop*

Обязательный параметр. Конечный адрес в диапазоне адресов. Это последний адрес в диапазоне, из которого могут назначаться адреса.

**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.

## 22.3.24. 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 текст {
            }
        }
    }
}
```

**Параметры**

*подсеть_ipv4*

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Используется формат *ip-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.

## 22.3.25. 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 текст {
            disable
        }
    }
}
```

**Параметры**

*подсеть_ipv4*

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Используется формат *ip-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 временного отключения настройки конкретного резерва IP.

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.

## 22.3.26. service dhcp-server subnet <подсеть_ipv4> static-mapping <имя_резерва> ip-address <ipv4-адрес>

Указание статического IP-адреса для конкретного клиента DHCP.

**Синтаксис**

**set service dhcp-server subnet** *подсеть_ipv4* **static-mapping** *имя_резерва* **ip-address** *ipv4-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 текст {
                ip-address ipv4-адрес
            }
        }
    }
}
```

**Параметры**

*подсеть_ipv4*

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Используется формат *ip-адрес/префикс*.

*имя_резерва*

Множественный узел. Имя для резерва IP-адреса. Можно определить несколько резервов, создав несколько узлов конфигурации **static-mapping**.

*ipv4-адрес*

Обязательный параметр. IP-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.

## 22.3.27. service dhcp-server subnet <подсеть_ipv4> static-mapping <имя_резерва> mac-address <mac-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** *mac-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 текст {
                mac-address текст
            }
        }
    }
}
```

**Параметры**

*подсеть_ipv4*

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Используется формат *ip-адрес/префикс*.

*имя_резерва*

Множественный узел. Имя для резерва IP-адреса. Можно определить несколько резервов, создав несколько узлов конфигурации **static-mapping**.

*mac-адрес*

Обязательный параметр. MAC-адрес, который следует статически сопоставить с указанным IP-адресом. Адрес указывается в формате шести разделенных двоеточиями 8-битовых шестнадцатеричных чисел, например, 00:0a:59:9a:f2:ba.

**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.

## 22.3.28. service dhcp-server subnet <подсеть_ipv4> static-route destination-subnet <подсеть_ipv4> gateway <ipv4-адрес>

Указание шлюза для статического маршрута, передаваемого клиентам.

**Синтаксис**

```
set service dhcp-server subnet подсеть_ipv4 static-route
destination-subnet подсеть_ipv4_2 gateway ipv4-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_2* **gateway** *ipv4-адрес*

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    dhcp-server {
        subnet подсеть_ipv4 {
            static-route {
                destination-subnet подсеть_ipv4 {
                    gateway ipv4-адрес
                }
            }
        }
    }
}
```

**Параметры**

*подсеть_ipv4*

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Используется формат *ip-адрес/префикс*.

*подсеть_ipv4_2*

Необязательный параметр. Множественный параметр. Подсеть назначения для статического маршрута, передаваемого для сохранения в таблицах маршрутизации клиентов.

*ipv4-адрес*

Обязательный параметр. 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.

## 22.3.29. 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 текст
        }
    }
}
```

**Параметры**

*подсеть_ipv4*

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Используется формат *ip-*

*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.

## 22.3.30. 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 целоебеззнака32разр
        }
```

```
        }
    }
```

**Параметры**

*подсеть_ipv4*

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Используется формат *ip-адрес/префикс*.

*секунды*

Указание сдвига времени в клиентской подсети от гринвичского (координированного всемирного) времени.

**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.

## 22.3.31. service dhcp-server subnet <подсеть_ipv4> time-server <ipv4-адрес>

Указание адреса сервера времени RFC868, доступного для клиентов.

**Синтаксис**

**set service dhcp-server subnet** *подсеть_ipv4* **time-server** *ipv4-адрес*

**delete service dhcp-server subnet** *подсеть_ipv4* **time-server** *ipv4-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 ipv4-адрес
        }
    }
}
```

**Параметры**

*подсеть_ipv4*

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Используется формат *ip-адрес/префикс*.

*ipv4-адрес*

Необязательный параметр. Указание IP-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 RFC 868, 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.

## 22.3.32. service dhcp-server subnet <подсеть_ipv4> wins-server <ipv4-адрес>

Указание адреса сервера WINS, доступного для клиентов DHCP.

**Синтаксис**

**set service dhcp-server subnet** *подсеть_ipv4* **wins-server** *ipv4-адрес*

**delete service dhcp-server subnet** *подсеть_ipv4* **wins-server** *ipv4-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 ipv4-адрес
        }
    }
}
```

**Параметры**

*подсеть_ipv4*

Обязательный параметр. Множественный узел. Подсеть IPv4, обслуживаемая пулом адресов DHCP. Используется формат *ip-адрес/префикс*.

*ipv4-адрес*

Необязательный параметр. Множественный узел. 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. Используется формат IP-адреса.

**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**.

## 22.3.33. service dhcp-server subnet <подсеть_ipv4> wpad-url <url-адрес>

Указание URL-адреса службы автоопределения веб-прокси (WPAD)

**Синтаксис**

**set service dhcp-server subnet** *подсеть_ipv4* **wpad-url** *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. Используется формат *ip-адрес/префикс*.

*url-адрес*

Необязательный параметр. Указание URL-адреса службы автоопределения веб-прокси (WPAD)

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для указания URL-адреса службы автоопределения веб-прокси (WPAD).

Форма **set** этой команды используется для указания URL-адреса службы автоопределения 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.

## 22.3.34. show dhcp client leases

Отображение сведений DHCP для интерфейсов, настроенных как клиенты DHCP.

**Синтаксис**

**show dhcp client leases [interface** *ethx***]**

**Режим ввода команды**

Эксплуатационный режим.

**Параметры**

*ethx*

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 22.6 приведен образец вывода команды **show dhcp client leases** без параметра.

*Пример 22.6 - Вывод команды "show dhcp client leases"*

```
admin@neo:~$ show dhcp client leases

interface : eth0

ip address : 192.168.1.157      [Active]

subnet mask: 255.255.255.0

router : 192.168.1.254

name server: 192.168.1.254 74.150.163.68 74.150.163.100
dhcp server: 192.168.1.254

lease time : 86400

last update: Wed Feb 17 02:18:20 GMT 2010

expiry : Thu Feb 18 02:18:18 GMT 2010

reason : BOUND
```

## 22.3.35. show dhcp leases

Отображение сведений о текущих арендах DHCP.

**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** (см. раздел 22.3.8. ).

**Примеры**

В примере 22.7 приведен образец вывода команды **show dhcp leases** без параметров.

*Пример 22.7 - Вывод команды "show dhcp leases"*

```
admin@neo:~$ 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
2010  default
```

# 23. DNS

В этом разделе описано использование системы доменных имен (DNS) в системе NEO.

Рассматриваются следующие вопросы:

- Настройка DNS.
- Команды DNS.

## 23.1. Настройка DNS

В этом разделе рассматриваются следующие вопросы:

- Обзор DNS.
- Примеры настройки DNS.

### 23.1.1. 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 NEO поддерживает три основные функции, относящиеся к DNS:

- Системная DNS.
- Динамическая DNS.
- Ретрансляция DNS.

#### *23.1.1.1. Системная DNS*

В системной DNS пользователь определяет список серверов имен, которые система NEO может использовать для разрешения имен узлов в IP-адреса. Этот список задается при помощи команды **system name-server**. (Команда **system name-server** описана в разделе 3.3.36. ; пример системной DNS дан в текущем разделе под заголовком “Пример 23.1 - Настройка статического доступа к серверу имен DNS”.)

#### *23.1.1.2. 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 NEO извещает поставщика службы DDNS об изменении. Поставщик службы DDNS несет ответственность за распространение изменения на другие серверы DNS. Система NEO поддерживает несколько поставщиков службы DDNS.

#### *23.1.1.3. 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 Altell NEO 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 NEO (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.

### 23.1.2. Примеры настройки DNS

В этом разделе рассматриваются следующие вопросы:

- Настройка доступа к серверу имен.
- Настройка динамической DNS.
- Настройка ретрансляции DNS.
- Статически настроенные записи и ретрансляция DNS.

В этом разделе есть следующие примеры:

- Пример 23.1 Настройка статического доступа к серверу имен DNS.
- Пример 23.2 Настройка динамической DNS.
- Пример 23.3 Настройка ретрансляции DNS.

#### *23.1.2.1. Настройка доступа к серверу имен*

Для получения возможности перевода имен узлов (например, www.altell.ru) в IP-адреса (например, 217.112.37.67) система должна иметь возможность доступа к серверу DNS.

Настройка доступа к серверу DNS описана в разделе 3.3.36. . Для удобства читателя пример повторен в данном разделе.

В примере 23.1 выполняется настройка статического IP-адреса для сервера DNS с адресом 12.34.56.78. Для соответствующей настройки системы NEO выполните следующие действия.

*Пример 23.1 - Настройка статического доступа к серверу имен DNS*

| Действие | Команда |
|---|---|
| Указание IP-адреса сервера DNS. | `admin@R1# set system name-server 12.34.56.78`<br>`[edit]` |

#### *23.1.2.2. Настройка динамической DNS*

На рисунке 83 показана типичная картина DDNS. В этой картине:

- Altell NEO (R1) подключена к провайдеру Интернета через интерфейс eth0.
- Сетевой домен - **company.com**.
- Имя узла системы Altell NEO - **r1.company.com**.
- Веб-сервер компании расположен за системой NEO. Имя его узла **www.company.com**.
- Провайдер Интернета предоставляет своим клиентам динамические IP-адреса с помощью DHCP.
- IP-адрес интерфейса eth0 системы NEO время от времени меняется вследствие динамического назначения провайдером Интернета.
- Веб-сервер компании расположен за устройством с преобразованием сетевых адресов (NAT) под управлением системы NEO, так что его IP-адрес (как он видится из Интернета) изменяется, когда провайдер Интернета назначает новый адрес интерфейсу eth0.
- Так как адрес веб-сервера меняется, ответы на запросы к DNS на разрешение имени **www.company.com** также должны меняться, отражая новый IP-адрес. DDNS решает

эту проблему.

DDNS позволяет NEO (R1) обновлять сведения об IP-адресах для любых локальных имен узлов (например, **r1.company.com** и **www.company.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:

- DNS Park: www.dnspark.com;
- 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.

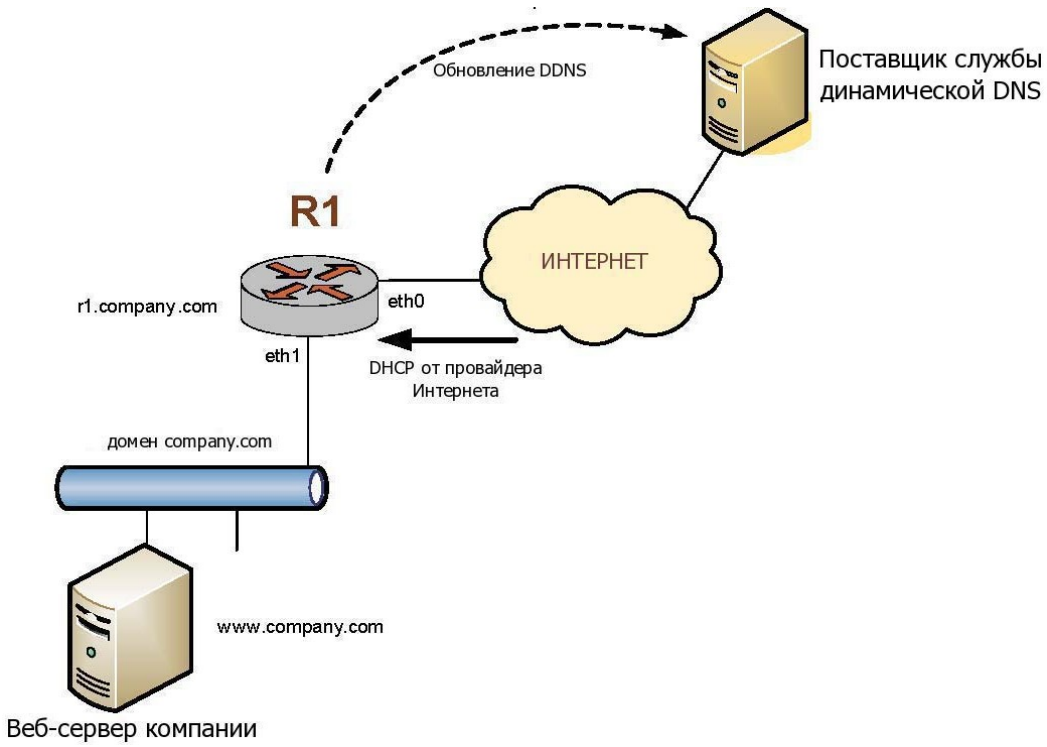
Указания по подключению доступны у поставщиков служб.

2. Настройка системы Altell NEO (R1 в примере) 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 Altell NEO.

***ПРИМЕЧАНИЕ*** *В зависимости от поставщика службы, включение имени домена в имя узла может требоваться или нет (например, “www” вместо “www.company.com”).*

*Рисунок 83 - Динамическая DNS*




В примере 23.2 выполняется настройка DDNS для поставщика службы DynDNS. В примере предполагается, что подписка на услуги DynDNS уже имеется). Для соответствующей настройки системы NEO выполните следующие действия в режиме настройки.

*Пример 23.2 - Настройка динамической DNS*

| Действие | Команда |
|---|---|
| Настройка поставщика службы. | `admin@R1# set service dns dynamic interface eth0 service dyndns [edit]` |
| Установка идентификатора входа для поставщика службы DDNS (например, vtest). | `admin@R1# set service dns dynamic interface eth0 service dyndns login vtest [edit]` |
| Установка пароля для поставщика | `admin@R1# set service dns dynamic` |

| | |
|---|---|
| службы DDNS (например, testpwd). | **interface eth0 service dyndns password testpwd**<br>[edit] |
| Указание r1 в качестве имени узла, запись DNS которого нуждается в обновлении при изменении IP-адреса на интерфейсе eth0. | admin@R1# **set service dns dynamic interface eth0 service dyndns host-name r1.company.com**<br>[edit] |
| Указание www в качестве имени узла, запись DNS которого нуждается в обновлении при изменении IP-адреса на интерфейсе eth0. | admin@R1# **set service dns dynamic interface eth0 service dyndns host-name www.company.com**<br>[edit] |
| Фиксация изменения. | admin@R1# **commit**<br>OK<br>[edit] |
| Вывод настройки динамической DNS. | admin@R1# **show service dns dynamic**<br>interface eth0 {<br>service dyndns {<br>host-name r1.company.com<br>host-name www.company.com<br>login vtest<br>password testpwd<br>}<br>}<br>[edit] |

Теперь, если IP-адрес интерфейса eth0 изменится, Altell NEO автоматически подключится к службе DynDNS с идентификатором входа **vtest** и паролем **testpwd**. Она отправит обновления для имен узлов **r1.company.com** и **www.company.com**, в которых будет

указан новый IP-адрес, требуемый для доступа к этим узлам в домене **company.com**. Внешние пользователи, запрашивающие DNS для разрешения имен **r1.company.com** или **www.company.com**, получат от системы DNS ответ с новым адресом.

#### *23.1.2.3. Настройка ретрансляции DNS*

Настройка Altell NEO для ретрансляции DNS состоит из двух основных этапов:

1. Указание серверов имен DNS, на которые следует передавать запросы

2. Указание интерфейсов, на которых будет выполняться прослушивание запросов DNS

##### 23.1.2.3.1. Указание серверов имен DNS

Местонахождение серверов имен можно получить из трех мест:

- Из системного списка серверов имен, определенного при помощи команды **set system name-server**.
- По DHCP.
- Из перечня добавочных серверов имен установленных при помощи команды **set service dns forwarding dhcp**.

По умолчанию система направляет запросы DNS на серверы имен из системного списка серверов имен, а также из списка серверов имен, полученного через DHCP. Поведение по умолчанию можно переопределить, указав как минимум один из приведенных ниже пунктов.

- Использовать только системные серверы имен. Для этого используется команда системы **set service dns forwarding**.
- Использовать только те серверы имен, которые передаёт сервер DHCP клиенту на интерфейсе, настроенном в качестве клиента DHCP. Для этого используется команда **set service dns forwarding dhcp**.
- Использовать дополнительные серверы имен, определённые при помощи команды **set service dns forwarding name-server**.

При запуске или перезапуске службы ретрансляции DNS она отправляет сообщения всем серверам имен в пуле и выбирает первый ответивший сервер имен. Этот сервер имен используется до тех пор, пока он не станет недоступным, в этом случае система отправляет новое сообщение оставшимся серверам имен в пуле.

#### 23.1.2.3.2. Указание прослушиваемых интерфейсов

Прослушиваемые интерфейсы — это интерфейсы, на которые внутренние клиенты будут посылать запросы DNS. Служба ретрансляции DNS получает эти сообщения и передает на сервер имен.

Для установки прослушиваемого интерфейса используется команда **set service dns forwarding listen-on**. Можно указать более одного интерфейса, выдав эту команду несколько раз.

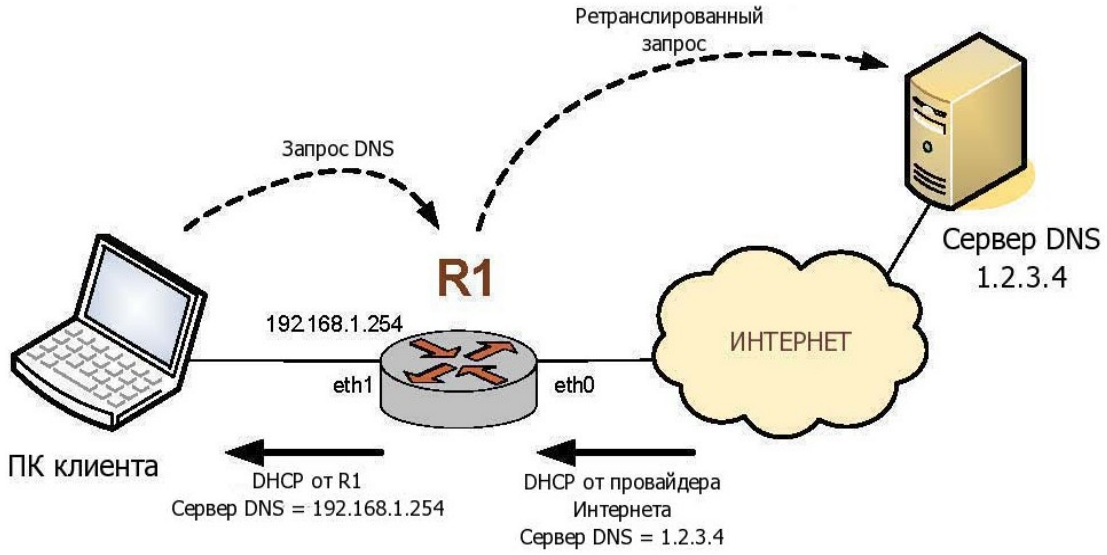
#### 23.1.2.3.3. Схема ретрансляции DNS

После выполнения вышеуказанных действий служба ретрансляция DNS будет настроена. Теперь можно настроить сервер DHCP NEO для распространения прослушивающегося адреса ретрансляции DNS клиентам DHCP. (Сведения о настройке сервера DHCP в системе Altell NEO приведены в разделе 22. DHCP .)

На рисунке 84 показана типичная схема применения ретрансляции DNS. На этой схеме:

- Провайдер Интернета (ПИ) выдает своим клиентам, в том числе системе Altell NEO (R1), динамические IP-адреса по DHCP.
- Altell NEO (R1) обеспечивает службу DHCP для клиентов в своей локальной сети.
- Локальные клиенты отправляют запросы DNS устройству под управлением NEO.
- Служба ретрансляции DNS на устройстве под управлением NEO передает запросы на сервер DNS провайдера Интернета.

*Рисунок 84 - Схема использования ретрансляции DNS*




В примере 23.3 выполняется настройка ключевых компонентов NEO для описанной выше схемы. Для соответствующей настройки системы NEO выполните следующие действия в режиме настройки.

*Пример 23.3 - Настройка ретрансляции DNS*

| Действие | Команда |
|---|---|
| Настройка IP-адреса и префикса на eth1 | `admin@R1# set interfaces ethernet eth1 address 192.168.1.254/24`<br>`[edit]` |
| Установка eth0 в качестве клиента DHCP | `admin@R1# set interfaces ethernet eth0 address dhcp`<br>`[edit]` |
| Установка сервера DHCP на R1 путем создания узла конфигурации для подсети 192.168.1.0/24. Ввод начального и конечного IP-адресов для пула. | `admin@R1# set service dhcp-server subnet 192.168.1.0/24 start 192.168.1.100 stop 192.168.1.199`<br>`[edit]` |
| Указание маршрутизатора по умолчанию для клиентов DHCP подсети | `admin@R1# set service dhcp-server subnet 192.168.1.0/24 default-` |

| | |
|---|---|
| 192.168.1.0/24. | **router 192.168.1.254**<br>[edit] |
| Создание списка серверов DNS с использованием сведений о серверах DNS, предоставляемых сервером DHCP провайдера (на eth0). | admin@R1# **set service dns forwarding dhcp eth0**<br>[edit] |
| Прослушивание запросов DNS на eth1 | admin@R1# **set service dns forwarding listen-on eth1**<br>[edit] |
| Указание сервера DNS для клиентов DHCP (в этом случае устройство будет работать как ретранслятор DNS в сети 192.168.1.0/24). | admin@R1# **set service dhcp-server subnet 192.168.1.0/24 dns-server 192.168.1.254**<br>[edit] |
| Фиксация изменения. | admin@R1# **commit**<br>[edit] |
| Вывод настройки, относящейся к DNS. | admin@R1# **show service dns**<br>forwarding {<br>dhcp eth0<br>listen-on eth1<br>}<br>[edit] |

### 23.1.3. 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 Altell NEO при помощи команды **system static-host-mapping**. Любые записи, созданные подобным образом, используются при обработке входящих запросов DNS ещё до передачи запросов на ретрансляцию. Если соответствие находится, возвращается соответствующий IP-адрес.

В примере 23.4 выполняется настройка системы на возвращение IP-адреса 12.34.56.78 при получении запроса DNS на “example.com” либо “vhost1”

*Пример 23.4 - Настройка статических записей*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для статического сопоставления узла. | admin@R1# **set system static-host-mapping host-name example.com**<br>[edit] |
| Ввод псевдонима для узла (не обязательно). | admin@R1# **set system static-host-mapping host-name example.com alias vhost1**<br>[edit] |
| Указание IP-адреса для возвращения в ответ на запрос к DNS. | admin@R1# **set system static-host-mapping host-name example.com inet 12.34.56.78**<br>[edit] |
| Фиксация изменения. | admin@R1# **commit**<br>[edit] |
| Вывод настройки статического сопоставления узлов. | admin@R1# **show system static-host-mapping**<br>host-name example.com{<br>alias vhost1<br>inet 12.34.56.78<br>}<br>[edit] |

## 23.2. Команды DNS

Команды настройки динамической DNS:

*Таблица 47 - Команды DNS*

| Команда настройки |
|---|

| | |
|---|---|
| `service dns dynamic interface <интерфейс>` | Включение поддержки DDNS на интерфейсе. |
| `service dns dynamic interface <интерфейс> service <служба>` | Указание поставщика службы DDNS. |
| `service dns dynamic interface <интерфейс> service <служба> host-name <имя_узла>` | Указание имени узла, для которого требуется обновление записи DNS у поставщика службы DDNS. |
| `service dns dynamic interface <интерфейс> service <служба> login <имя_входа_службы>` | Ввод идентификатора входа для аутентификации у поставщика службы DDNS. |
| `service dns dynamic interface <интерфейс> service <служба> password <пароль_службы>` | Ввод пароля для аутентификации у поставщика службы DDNS. |
| `service dns dynamic interface <интерфейс> service <служба> server <адрес>` | Указание сервера, на который следует отправлять обновления DDNS. |
| Команды настройки ретрансляции DNS | |
| `service dns forwarding cache-size <размер>` | Указание размера кэша службы ретрансляции DNS. |
| `service dns forwarding dhcp <интерфейс>` | Указание интерфейса, из клиентских параметров DHCP которого будут приниматься сведения о серверах имен. |
| `service dns forwarding listen-on <интерфейс>` | Указание интерфейса, на котором будут прослушиваться запросы DNS. |
| `service dns forwarding name-server <ipv4-адрес>` | Указание сервера имен, на который будут передаваться запросы DNS. |
| `service dns forwarding system` | Указание использовать в качестве вышестоящих серверов DNS системные сервера имен. |
| Эксплуатационные команды | |
| `clear dns forwarding all` | Очистка всех связанных с DNS счетчиков и кэша ретрансляции DNS. |

| | |
|---|---|
| `clear dns forwarding cache` | Удаление всех записей из кэша ретрансляции DNS. |
| `show dns dynamic status` | Отображение состояния обновления для всех узлов, настроенных для обновления динамической DNS. |
| `show dns forwarding nameservers` | Отображение серверов имен, используемых для ретрансляции DNS. |
| `show dns forwarding statistics` | Отображение счетчиков, имеющих отношение к ретрансляции DNS. |
| `update dns dynamic interface <интерфейс>` | Отправка принудительного обновления поставщику службы DDNS на указанном интерфейсе. |

## 23.2.1. clear dns forwarding all

Очистка всех связанных с DNS счетчиков и кэша ретрансляции DNS.

**Синтаксис**

**`clear dns 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.

## 23.2.2. clear dns forwarding cache

Удаление всех записей из кэша ретрансляции DNS.

**Синтаксис**

**`clear dns 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.

### 23.2.3. 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 текст {
            }
        }
    }
}
```

**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 динамическую 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.

### 23.2.4. service dns dynamic interface <интерфейс> service <служба>

Указание поставщика службы DDNS.

**Синтаксис**

**set service dns dynamic interface** *интерфейс* **service** *служба*

**delete service dns dynamic interface** *интерфейс* **service** *служба*

**show service dns dynamic** *interface* **интерфейс service** *служба*

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    dns {
        dynamic {
            interface текст {
                service текст {
                }
            }
        }
    }
}
```

**Параметры**

*интерфейс*

Множественный узел. Интерфейс, поддерживающий DDNS.

*служба*

Множественный узел. Имя поставщика службы 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 службу динамической DNS (DDNS) для системы NEO.

Форма **set** этой команды используется для указания поставщика службы DDNS.

Форма **delete** этой команды используется для удаления поставщика службы DDNS из настройки.

Форма **show** этой команды используется для просмотра сведений о поставщике службы DDNS.

### 23.2.5. service dns dynamic interface <интерфейс> service <служба> host-name <имя_узла>

Указание имени узла, для которого требуется обновление записи DNS у поставщика службы DDNS.

**Синтаксис**

```
set service dns dynamic interface интерфейс service
служба host-name имя_узла

delete service dns dynamic interface интерфейс service
служба host-name имя_узла

show service dns dynamic interface интерфейс service
служба host-name
```

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    dns {
        dynamic {
```

```
                    interface текст {
                        service текст {
                            host-name текст
                        }
                    }
                }
            }
        }
```

**Параметры**

*интерфейс*

Множественный узел. Интерфейс, поддерживающий DDNS.

*служба*

Множественный узел. Имя поставщика службы 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 службы 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.

### 23.2.6. service dns dynamic interface <интерфейс> service <служба> login <имя_входа_службы>

Ввод идентификатора входа для аутентификации у поставщика службы DDNS.

**Синтаксис**

**set service dns dynamic interface** *интерфейс* **service** *служба* **login** *имя_входа_службы*

**delete service dns dynamic interface** *интерфейс* **service** *служба* **login**

**show service dns dynamic interface** *интерфейс* **service** *служба* **login**

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    dns {
        dynamic {
            interface текст {
                service текст {
                    login текст
                }
            }
        }
    }
}
```

**Параметры**

*интерфейс*

Множественный узел. Интерфейс, поддерживающий DDNS.

*служба*

Множественный узел. Имя поставщика службы DDNS. Поддерживаются следующие значения: **dnspark**, **dslreports**, **dyndns**, **easydns**, **namecheap**, **sitelutions** и **zoneedit**.

*имя_входа_службы*

Идентификатор входа, который система должна использовать при входе на систему поставщика службы DDNS.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для указания идентификатора входа, который система должна использовать при входе на систему поставщика службы DDNS.

Форма **set** этой команды используется для указания идентификатора входа, который система должна использовать при входе на систему поставщика службы DDNS.

Форма **delete** этой команды используется для удаления идентификатора ввода для поставщика службы DDNS.

Форма **show** этой команды используется для просмотра настройки идентификатора входа для поставщика службы DDNS.

## 23.2.7. service dns dynamic interface <интерфейс> service <служба> password <пароль_службы>

Ввод пароля для аутентификации у поставщика службы DDNS.

**Синтаксис**

**set service dns dynamic interface** *интерфейс* **service** *служба* **password** *пароль_службы*

**delete service dns dynamic interface** *интерфейс* **service** *служба* **password**

**show service dns dynamic interface** *интерфейс* **service** *служба* **password**

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    dns {
        dynamic {
            interface текст {
                service текст {
                    password текст
```

```
                                }
                            }
                        }
                    }
                }
```

**Параметры**

*интерфейс*

Множественный узел. Интерфейс, поддерживающий DDNS.

*служба*

Множественный узел. Имя поставщика службы DDNS. Поддерживаются следующие значения: **dnspark**, **dslreports**, **dyndns**, **easydns**, **namecheap**, **sitelutions** и **zoneedit**.

*пароль_службы*

Пароль для использования системой при входе в систему поставщика службы DDNS.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для указания пароля, который система должна использовать при входе на систему поставщика службы DDNS.

Форма **set** этой команды используется для указания пароля для поставщика службы DDNS.

Форма **delete** этой команды используется для удаления пароля поставщика службы DDNS.

Форма **show** этой команды используется для просмотра настройки пароля поставщика службы DDNS.

### 23.2.8. service dns dynamic interface <интерфейс> service <служба> server <адрес>

Указание сервера, на который следует отправлять обновления DDNS.

**Синтаксис**

**set service dns dynamic interface** *интерфейс* **service**

*служба* **server** *адрес*

**delete service dns dynamic interface** *интерфейс* **service** *служба* **server**

**show service dns dynamic interface** *интерфейс* **service** *служба* **server**

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    dns {
        dynamic {
            interface текст {
                service текст {
                    server текст
                }
            }
        }
    }
}
```

**Параметры**

*интерфейс*

Множественный узел. Интерфейс, поддерживающий DDNS.

*служба*

Множественный узел. Имя поставщика службы DDNS. Поддерживаются следующие значения: **dnspark**, **dslreports**, **dyndns**, **easydns**, **namecheap**, **sitelutions** и **zoneedit**.

*адрес*

IP-адрес или имя узла сервера поставщика службы DDNS, на который следует отправлять обновления DDNS. Требуется не для всех поставщиков службы DDNS.

**Значение по умолчанию**

Используются серверы по умолчанию поставщика службы DDNS.

**Указания по использованию**

Эта команда используется для указания IP-адреса или имени узла сервера поставщика службы DDNS, на который следует отправлять обновления DDNS. Установка сервера требуется только в том случае, если он специфицируется поставщиком службы 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 службы DDNS.

Форма **show** этой команды используется для просмотра настройки серверов поставщика службы DDNS.

## 23.2.9. service dns forwarding cache-size <размер>

Указание размера кэша службы ретрансляции DNS.

**Синтаксис**

```
set service dns forwarding cache-size размер
delete service dns forwarding cache-size
show service dns forwarding cache-size
```

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    dns {
        forwarding {
            cache-size целоебеззнака32разр
        }
    }
}
```

**Параметры**

*размер*

Необязательный параметр. 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 настройки размера кэша службы ретрансляции DNS.

## 23.2.10. service dns forwarding dhcp <интерфейс>

Указание интерфейса, из клиентских параметров DHCP которого будут приниматься сведения о серверах имен.

**Синтаксис**

**set service dns forwarding dhcp** *интерфейс*

**delete service dns forwarding dhcp** *интерфейс*

**show service dns forwarding dhcp** *интерфейс*

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    dns {
        forwarding {
            dhcp текст
        }
    }
}
```

**Параметры**

*интерфейс*

Множественный узел. Интерфейс, который должен принимать обновления сведений о серверах имен с сервера DHCP.

**Значение по умолчанию**

Система ретранслирует запросы DNS на все системные серверы имен и все серверы имен, указанные через DHCP.

**Указания по использованию**

Эта команда используется для указания интерфейса, который будет действовать в качестве клиента DHCP и принимать обновления сведений о серверах имен DNS. NEO будет использовать эти сведения для ретрансляции запросов DNS от своих локальных клиентов на сервер имен.

Чтобы интерфейс можно было настроить на прослушивание обновлений для сведений о серверах имен, интерфейс нужно настроить на получение его собственного IP-адреса через DHCP, то есть его нужно настроить в качестве клиента DHCP. Сведения о настройке IP-адреса для физических интерфейсов приведены в соответствующих разделах документации согласно типам интерфейсов (например, для устройств Ethernet см. раздел 6.2.3. ).

По умолчанию служба ретрансляции DNS создает пул серверов имен, к которым выполняется ретрансляция запросов DNS; в их число входят все статически настроенные (при помощи команды **system name-server <адрес>** ) в системе серверы имен, и серверы, о которых система извещается через DHCP. Эта команда используется для переопределения поведения по умолчанию: когда интерфейс указывается при помощи данной команды, система будет использовать только сведения о серверах имен полученные через DHCP на указанном интерфейсе.

Чтобы обеспечить более многочисленный пул применимых серверов имен, эту команду можно применять в сочетании с командами service dns forwarding name-server <ipv4-адрес> и service dns forwarding system .

Форма **set** этой команды используется для указания интерфейса, который должен использоваться в качестве источника обновлений сведений о

серверах имен, поступающих из DHCP.

Форма **delete** этой команды используется для восстановления принятого по умолчанию метода получения обновлений сведений о серверах имен.

Форма **show** этой команды используется для просмотра настройки использования DHCP для обновления сведений для ретрансляции DNS.

## 23.2.11. service dns forwarding listen-on <интерфейс>

Указание интерфейса, на котором будут прослушиваться запросы DNS.

**Синтаксис**

```
set service dns forwarding listen-on интерфейс
delete service dns forwarding listen-on интерфейс
show service dns forwarding listen-on интерфейс
```

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    dns {
        forwarding {
            listen-on текст {
            }
        }
    }
}
```

**Параметры**

*интерфейс*

Обязательный параметр. Множественный узел. Интерфейс, на котором следует прослушивать клиентские запросы DNS.

Можно указать более одного интерфейса для приема клиентских запросов DNS путем создания нескольких узлов конфигурации **listen-on**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для указания интерфейсов, на которых следует прослушивать клиентских запросов DNS. Ответы DNS будут отправлены только на запросы, принятые на интерфейсах, указанных с помощью данной команды. Для работы ретрансляции DNS нужно указать как минимум один интерфейс.

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.

## 23.2.12. service dns forwarding name-server <ipv4-адрес>

Указание сервера имен, на который будут передаваться запросы DNS.

**Синтаксис**

```
set service dns forwarding name-server ipv4-адрес
delete service dns forwarding name-server ipv4-адрес
show service dns forwarding name-server ipv4-адрес
```

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    dns {
        forwarding {
            name-server ipv4-адрес
        }
    }
}
```

**Параметры**

*ipv4-адрес*

Необязательный параметр. Множественный узел. IPv4-адрес сервера имен,

на который следует ретранслировать запросы DNS.

Можно ретранслировать запросы DNS более чем на один сервер имен путем создания нескольких узлов конфигурации **name-server**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для указания сервера имен, на который следует ретранслировать запросы DNS.

Использование этой команды не является обязательным. По умолчанию служба ретрансляции DNS создает пул серверов имен по умолчанию, в состав которого входят все серверы имен, статически настроенные в системе при помощи команды system name-server <адрес> , и серверы, о которых система была извещена через DHCP. Эта команда используется для переопределения поведения по умолчанию: когда выдается данная команда, система ретранслирует запросы DNS на указанный сервер (или серверы) имен.

Чтобы обеспечить более многочисленный пул применимых серверов имен, эту команду можно применять в сочетании с командами service dns forwarding dhcp <интерфейс> и service dns forwarding system .

Форма **set** этой команды используется для указания сервера имен, на который следует ретранслировать запросы DNS.

Форма **delete** этой команды используется для удаления сервера имен из списка серверов имен, на которые следует ретранслировать запросы DNS. Если удаляется последний настроенный сервер, восстанавливается поведение ретрансляции, принятое по умолчанию.

Форма **show** этой команды используется для просмотра списка серверов имен, на которые будут ретранслироваться запросы DNS.

## 23.2.13. service dns forwarding system

Указание использовать в качестве вышестоящих серверов DNS системные сервера имен.

**Синтаксис**

```
set service dns forwarding system
delete service dns forwarding system
show service dns forwarding
```

**Режим ввода команды**

Режим настройки.

**Ветвь конфигурации**

```
service {
    dns {
        forwarding {
            system
        }
    }
}
```

**Параметры**

Отсутствует

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется, чтобы предписать системе ретранслировать запросы DNS на серверы имен, настроенные статически с помощью команды system name-server <адрес> .

По умолчанию служба ретрансляции DNS ретранслирует запросы DNS на пул серверов имен, состоящий из статически настроенных серверов имен и из серверов, уведомление о которых было получено при помощи DHCP. Эта команда используется для переопределения поведения по умолчанию: когда выдается данная команда, система ретранслирует запросы DNS на статически настроенные серверы имен.

Чтобы обеспечить более многочисленный пул применимых серверов имен, эту команду можно применять в сочетании с командами service dns forwarding dhcp <интерфейс> и service dns forwarding name-server <ipv4-адрес> .

Форма **set** этой команды используется для указания системного набора серверов имен, на которые следует ретранслировать запросы DNS.

Форма **delete** этой команды используется для восстановления поведения по умолчанию для ретрансляции DNS.

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

## 23.2.14. show dns dynamic status

Отображение состояния обновления для всех узлов, настроенных для обновления динамической DNS.

**Синтаксис**

```
show dns 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 динамической DNS (DDNS).

**Примеры**

В примере 23.5 показан образец вывода команды **show dns dynamic status**.

*Пример 23.5 - Вывод сведений для узлов, настроенных для DDNS*

```
admin@neo:~$ show dns dynamic status
show dns dynamic status
interface    : eth2
ip address   : 1.2.3.4
host-name    : test1.getmyip.com
last update  : Thu Sep 11 19:30:43 2008
update-status: good
```

```
interface    : eth2
ip address   : 1.2.3.5
host-name    : test2.getmyip.com
last update  : Thu Sep 11 19:30:43 2008
update-status: good

interface    : eth3
ip address   : 1.3.4.5
host-name    : test4
last update  : Thu Sep 11 19:34:16 2008
update-status: good
```

### 23.2.15. show dns forwarding nameservers

Отображение серверов имен, используемых для ретрансляции DNS.

#### Синтаксис

**show dns forwarding nameservers**

#### Режим ввода команды

Эксплуатационный режим.

#### Параметры

Отсутствует

#### Указания по использованию

Эта команда используется для отображения серверов имен, которые в текущий момент используются для ретрансляции DNS, а также серверов имен, которые доступны, но в настоящий момент для ретрансляции DNS не используются.

#### Примеры

В примере 23.6 показан образец вывода команды **show dns forwarding nameservers**.

*Пример 23.6 - Вывод сведений о серверах имен, касающихся ретрансляции DNS*

```
admin@neo:~$ show dns forwarding nameservers
---------------------
```

```
Nameservers configured for DNS forwarding
---------------------
  10.0.0.30 available via 'system'


---------------------
Nameservers NOT configured for DNS forwarding
---------------------
  10.0.0.31 available via 'dhcp eth3'
```

### 23.2.16. show dns forwarding statistics

Отображение счетчиков, имеющих отношение к ретрансляции DNS.

**Синтаксис**

**show dns 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 серверов имен, 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 23.7 показан образец вывода команды **show dns forwarding statistics**.

*Пример 23.7 - Отображение статистики ретрансляции DNS*

```
admin@neo:~$ show dns forwarding statistics
--------
Cache statistics
```

```
--------
Cache size: 150
Queries forwarded: 5
Queries answered locally: 2
Total DNS entries inserted into cache: 23
DNS entries removed from cache before expiry: 0
-----------
Nameserver statistics
-----------
Server: 10.0.0.30
Queries sent: 5
Queries retried or failed: 0
```

### 23.2.17. update dns dynamic interface <интерфейс>

Отправка принудительного обновления поставщику службы DDNS на указанном интерфейсе.

**Синтаксис**

**update dns 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 службы динамической DNS (DDNS). Принудительное обновление предоставляет поставщику службы DDNS сведения о текущем состоянии указанного интерфейса.

Обратите внимание, что частые ненужные обновления могут вызвать блокировку имени узла поставщиком службы DDNS, поэтому эту команду не следует использовать регулярно.

# 24. SNMP

## 24.1. 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 из себя набор переменных, характеризующих состояние объекта управления.

Поддерживаются следующие стандартные базы управляющей информации:

*Таблица 48 - Поддерживаемые стандартные базы управляющей информации*

| Название MIB | Документ | Примечание |
|---|---|---|
| BGP4-MIB | 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 состояние с меньшим номером (bgpBackwardTransition trap). |
| HOST-RESOURCES-MIB | RFC 2790, Host Resources MIB | |
| IF-MIB | RFC 2863, The Interfaces Group MIB | Поддерживаются уведомительные сообщения при разрыве / восстановлении соединения (linkUp, linkDown traps). |
| IP-MIB | RFC 2011, SNMPv2 Management Information Base for the Internet Protocol using SMIv2 | |

| | | |
|---|---|---|
| IPV6-TC | RFC2465, Management Information Base for IP Version 6: Textual Conventions and General Group | |
| IPV6-UDP-MIB | RFC 2454, IP Version 6 Management Information Base for the User Datagram Protocol | |
| OSPF-MIB | RFC 1850, OSPF Version 2 Management Information Base | |
| RFC1213-MIB | RFC 1213, Management Information Base for Network Management of TCP/IP-based internets: MIB-II | |
| RIPv2-MIB | RFC 1724, RIP Version 2 MIB Extension | |
| SNMPv2-MIB | 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 | RFC 4022, Management Information Base for the Transmission Control Protocol (TCP) | |
| UDP-MIB | RFC 4113, Management Information Base for the 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 <ipv4-адрес>.

В Altell NEO по умолчанию определены следующие идентификаторы объектов:

- sysObjectID = 1.3.6.1.4.1.8072.3.2.10;
- sysDescr = Altell NEO.

Значение для sysDescr может быть изменено при помощи команды service snmp description <описание>.

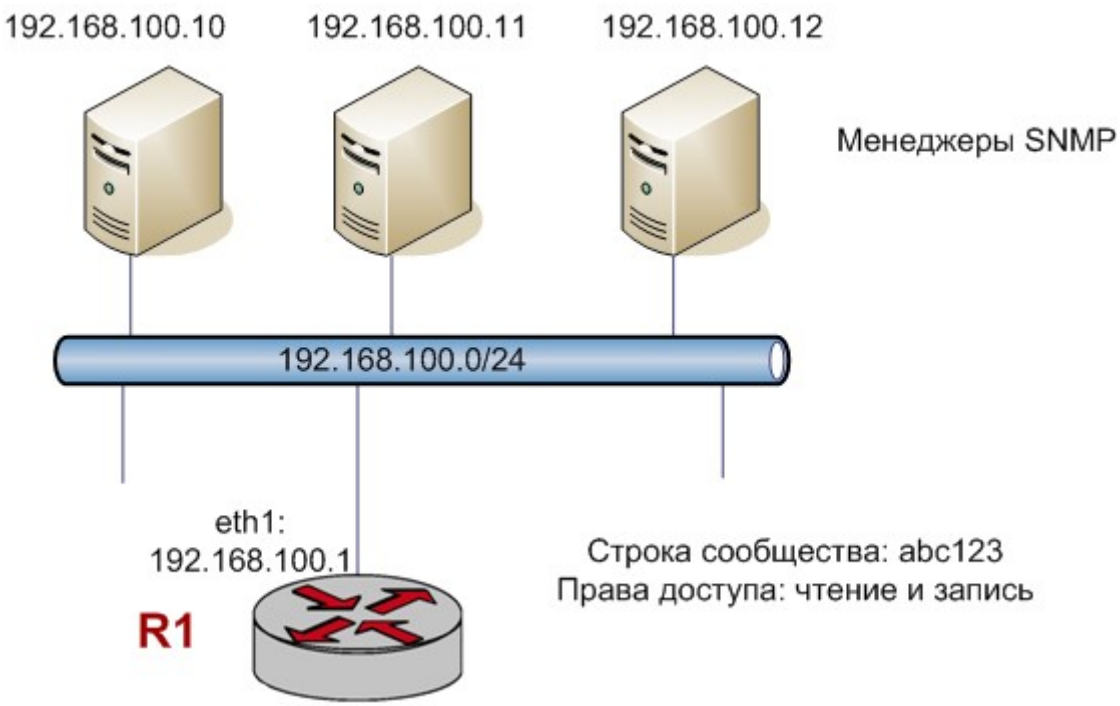
## 24.2. Примеры настройки SNMP

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. Altell NEO настраивается таким образом, чтобы отправлять уведомительные сообщения (trap) всем этим менеджерам SNMP. После выполнения всех настроек, Altell NEO будет настроен в соответствии с рисунком 85.

*Рисунок 85 - SNMP*




В этом разделе есть следующие примеры:

- Пример 24.1 - Определение сообщества SNMP.
- Пример 23.6 - Вывод сведений о серверах имен, касающихся ретрансляции DNS.

### 24.2.1. Определение 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 24.1 в качестве строки сообщества SNMP указывается abc123, а также определяются 3 клиента для данного сообщества: 192.168.100.10, 192.168.100.11 и 192.168.100.12. Для данного сообщества устанавливается доступ на чтение и на запись.

Для указания параметров сообщества SNMP необходимо выполнить следующие шаги в режиме настройки:

*Пример 24.1 - Определение сообщества SNMP*

| Действие | Команда |
|---|---|
| Создание узлов конфигурации **snmp** и **community**. Указание строки сообщества. | admin@R1# **set service snmp community abc123**<br>[edit] |
| Переход к узлу конфигурации сообщества. | admin@R1# **edit service snmp community abc123**<br>[edit service snmp community abc123] |
| Указание списка клиентов SNMP для данного сообщества. | admin@R1# **set client 192.168.100.10**<br>[edit service snmp community abc123]<br>admin@R1# **set client 192.168.100.11**<br>[edit service snmp community abc123]<br>admin@R1# **set client 192.168.100.12**<br>[edit service snmp community abc123] |
| Для данного сообщества | admin@R1# **set authorization rw** |

| | |
|---|---|
| устанавливается доступ на чтение и на запись. | `[edit service snmp community abc123]` |
| Фиксация изменений и переход к вершине дерева конфигурации. | `admin@R1# commit`<br>`[edit service snmp community abc123]`<br>`admin@R1# top`<br>`[edit]` |

## 24.3. Указание параметров получателя уведомительных сообщений о событиях

В примере 24.2 определяются параметры получателей для уведомительных сообщений о событиях: 192.168.100.10, 192.168.100.11 и 192.168.100.12.

Для указания параметров получателей уведомительных сообщений SNMP необходимо выполнить следующие шаги в режиме настройки:

*Пример 24.2 - Указание параметров получателей уведомительных сообщений о событиях*

| Действие | Команда |
|---|---|
| Указание получателей. | `admin@R1# set service snmp trap-target 192.168.100.10`<br>`[edit]`<br>`admin@R1# set service snmp trap-target 192.168.100.11`<br>`[edit]`<br>`admin@R1# set service snmp trap-target 192.168.100.12`<br>`[edit]` |
| Фиксация изменений. | `admin@R1# commit`<br>`[edit]` |

## 24.4. Команды SNMP

| Команды настройки | |
|---|---|
| service snmp | Указание параметров SNMP. |
| 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 <ipv4-адрес> | Указание клиентов SNMP для данного сообщества, которые могут иметь доступ к системе. |
| service snmp community <сообщество> network <ipv4-сеть> | 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 location <местоположение> | Указание местоположения. |
| service snmp trap-source <ipv4-адрес> | Указание IP-адреса источника для уведомительных сообщений о событиях (SNMP traps). |
| service snmp trap-target <ipv4-адрес> | Указание адреса назначения для уведомительных сообщений о событиях SNMP (traps). |
| Эксплуатационные команды | |
| show snmp | Отображение сведений для SNMP. |

### 24.4.1. 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.

### 24.4.2. 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 текст
    }
}
```

**Параметры**

*сообщество*

Необязательный. Множественный узел. Указание сообщества SNMP. Значение данного параметра определяет строку сообщества, которая используется для авторизации менеджеров SNMP, отправляющих запросы Altell NEO. 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.

### 24.4.3. 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 текст
        authorization [ro|rw]
    }
}
```

**Параметры**

*сообщество*

Необязательный. Множественный узел. Указание сообщества SNMP. Значение данного параметра определяет строку сообщества, которая используется для авторизации менеджеров SNMP, отправляющих запросы Altell NEO. Допустимо использование букв, цифр, а также дефиса.

Для того чтобы определить несколько сообществ, необходимо создать соответствующее количество узлов конфигурации **community**.

*доступ*

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.

### 24.4.4. service snmp community <сообщество> client <ipv4-адрес>

Указание клиентов SNMP для данного сообщества, которые могут иметь доступ к системе.

**Синтаксис**

**set service snmp community** *сообщество* **client** *ipv4-адрес*

**delete service snmp community** *сообщество* **client** *ipv4-адрес*

**show service snmp community** *сообщество* **client**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
    snmp {
        community текст
        client ipv4-адрес
    }
}
```

**Параметры**

*сообщество*

Необязательный. Множественный узел. Указание сообщества SNMP. Значение данного параметра определяет строку сообщества, которая используется для авторизации менеджеров SNMP, отправляющих запросы Altell NEO. Допустимо использование букв, цифр, а также дефиса.

Для того чтобы определить несколько сообществ, необходимо создать соответствующее количество узлов конфигурации **community**.

*ipv4-адрес*

Необязательный. Множественный узел. Клиенты SNMP, которые могут

иметь доступ к данной системе.

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.

### 24.4.5. service snmp community <сообщество> network <ipv4-сеть>

Указание сети клиентов SNMP для данного сообщества, которые могут получить доступ к системе.

**Синтаксис**

**set service snmp community** *сообщество* **network** *ipv4-сеть*

**delete service snmp community** *сообщество* **network** *ipv4-сеть*

**show service snmp community** *сообщество* **network**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
```

```
        snmp {
            community текст
            network ipv4-сеть
        }
}
```

**Параметры**

*сообщество*

Необязательный. Множественный узел. Указание сообщества SNMP. Значение данного параметра определяет строку сообщества, которая используется для авторизации менеджеров SNMP, отправляющих запросы Altell NEO. Допустимо использование букв, цифр, а также дефиса.

Для того чтобы определить несколько сообществ, необходимо создать соответствующее количество узлов конфигурации **community**.

*ipv4-сеть*

Необязательный. Множественный узел. Сеть клиентов SNMP для данного сообщества, которые могут получить доступ к системе.

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.

### 24.4.6. 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 текст
    }
}
```

**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.

### 24.4.7. 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 текст
    }
}
```

**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 Altell NEO.*

**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

### 24.4.8. 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 0-4294967295]
    }
}
```

**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 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.

### 24.4.9. 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 текст
    }
}
```

**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.

### 24.4.10. service snmp trap-source <ipv4-адрес>

Указание IP-адреса источника для уведомительных сообщений о событиях (SNMP

traps).

**Синтаксис**

**set service snmp trap-source** *ipv4-адрес*

**delete service snmp trap-source** *ipv4-адрес*

**show service snmp trap-source**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
    snmp {
        trap-source ipv4-адрес
    }
}
```

**Параметры**

*ipv4-адрес*

IP-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 Altell NEO. 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.

## 24.4.11. service snmp trap-target <ipv4-адрес>

Указание адреса назначения для уведомительных сообщений о событиях SNMP (traps ).

**Синтаксис**

**set service snmp trap-target** *ipv4-адрес* [**community** *сообщество* | **port** *порт* ]

**delete service snmp trap-target** *ipv4-адрес* [**community** | **port**]

**show service snmp trap-target** *ipv4-адрес* [**community** | **port**]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
Service {
    snmp {
        trap-target ipv4 {
            community текст
            port целое32разр
        }
    }
}
```

**Параметры**

*ipv4-адрес*

Необязательный. Множественный узел. IP-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 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.

## 24.4.12. 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.

# 25. УЧЕТ СЕТЕВОГО ТРАФИКА

## 25.1. Настройка системы учета сетевого трафика

### 25.1.1. Общие сведения

Altell NEO 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 учетных данных в формате Netflow или SFlow.

Сетевой поток представляет собой однонаправленную последовательность пакетов, имеющих одинаковые IP-адрес источника, порт источника (для UDP или TCP, и 0 для остальных протоколов), IP-адрес назначения, порт назначения (для UDP и TCP, тип и код ICMP, 0 для остальных протоколов), протокол IP, входящий интерфейс, а также поле ToS.

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 приемлимую точность.

### 25.1.2. Настройка интерфейса для учета сетевого трафика

Для того чтобы включить учет сетевых потоков на интерфейсе, его необходимо соответствующим образом настроить. В следующем примере приведена настройка учета сетевых потоков на интерфейсе **eth0**.

*Пример 25.1 - Настройка интерфейса для учета сетевого трафика*

| Действие | Команда |
|---|---|
| Настройка учета сетевого трафика на интерфейсе eth0 | admin@neo#**set system flow-accounting interface eth1**<br>[edit] |
| Фиксация конфигурации. | admin@neo# **commit**<br>[edit] |

### 25.1.3. Вывод данных учета сетевого трафика

После включения учета сетевого трафика на выбранном интерфейсе, предоставляется возможность вывода сведений о сетевом трафика на основе интерфейса, сетевого узла, сетевого порта, а также объема сетевого трафика. В следующем примере приведен вывод данных учета трафика для интерфейса **eth1**.

*Пример 25.2 - Вывод данных учета для интерфейса eth1*

```
admin@neo:~$ show flow-accounting interface eth1
          flow-accounting for [eth1]

          Src Addr         Dst Addr         Sport Dport Proto
          Packets      Bytes   Flows

          192.168.1.94     226.94.1.1       3999  4000    udp
          167      18370       1

          192.168.1.109    192.168.1.235    36095 22      tcp
          22       1536        1

          192.168.1.158    192.168.7.255    138   138     udp
          4        912         1

          192.168.1.109    192.168.7.255    138   138     udp
          2        497         1

          192.168.1.111    192.168.1.255    17500 17500   udp
```

```
2        272       1

192.168.1.111   255.255.255.255 17500 17500   udp
2        272       1

192.168.1.110   192.168.1.255   17500 17500   udp
2        272       1

192.168.1.110   255.255.255.255 17500 17500   udp
2        272       1

192.168.1.164   192.168.7.255   138   138     udp
1        229       1

192.168.1.159   192.168.7.255   138   138     udp
1        229       1

192.168.1.148   192.168.7.255   138   138     udp
1        229       1

192.168.1.158   192.168.7.255   137   137     udp
2        192       1

192.168.1.110   192.168.1.255   53913 137     udp
1         78       1

192.168.1.77    192.168.7.255   137   137     udp
1         78       1

192.168.1.95    226.94.1.1      0     0      igmp
1         32       1

192.168.1.186   233.0.0.1       0     0      igmp
1         32       1

192.168.1.218   224.0.0.1       0     0      igmp
1         32       1

192.168.7.53    224.0.0.252     0     0      igmp
1         28       1

192.168.7.53    224.0.0.1       0     0      igmp
1         28       1


Total entries: 19

Total flows  : 19

Total pkts   : 215

Total bytes  : 23,590
```

В следующем примере приведен вывод данных учета для сетевого узла 192.168.1.111

на интерфейсе **eth1**.

*Пример 25.3 - Вывод данных учета для узла 192.168.1.111 на интерфейсе eth1*

```
admin@neo:~$ show flow-accounting interface eth0 host
192.168.1.111
          Src Addr         Dst Addr         Sport Dport Proto
          Packets      Bytes   Flows

          192.168.1.111    192.168.1.255    17500 17500   udp
          6        816       1

          192.168.1.111    255.255.255.255 17500 17500   udp
          6        816       1


          Total entries: 2

          Total flows  : 2

          Total pkts   : 12

          Total bytes  : 1,632
```

### 25.1.4. Экспорт данных учета сетевого трафика

В дополнение к локальному выводу данных, существует возможность экспортировать их на сервер сбора данных Netflow или SFlow. В следующем примере приведена настройка экспорта данных учета сетевого трафика в формате Netflow на удаленный сервер сбора, имеющий IP-адрес 192.168.1.20 и порт по умолчанию.

*Пример 25.4 - Экспорт данных в формате Netflow на узел 192.168.1.20*

| Действие | Команда |
|---|---|
| Настройка экспорта данных в формате Netflow на узел 192.168.1.20. | admin@neo# **set system flow-accounting netflow server 192.168.1.20**<br>[edit] |
| Фиксация конфигурации. | admin@neo# **commit**<br>[edit] |

## 25.2. Команды системы учета сетевого трафика

| Команды настройки | |
|---|---|
| `system flow-accounting interface <интерфейс>` | Указание интерфейса, для которого будет производиться учет входящего трафика. |
| `system flow-accounting netflow engine-id <идентификатор>` | Указание идентификатора системы ID, которое будет включено в данные Netflow. |
| `system flow-accounting netflow sampling-rate <частота>` | Указание частоты отсчетов, с которой сетевые пакеты будут учитываться в статистике. |
| `system flow-accounting netflow server <ipv4-адрес>` | Указание сборщика Netflow для экспорта данных Netflow. |
| `system flow-accounting netflow timeout expiry-interval <интервал>` | Указание интервала, через который будут отправляться отчеты сборщику данных Netflow. |
| `system flow-accounting netflow timeout flow-generic <таймаут>` | Указание таймаута сетевого потока для трафика IP. |
| `system flow-accounting netflow timeout icmp <таймаут>` | Указание таймаута сетевого потока для трафика ICMP. |
| `system flow-accounting netflow timeout max-active-life <время_жизни>` | Указание максимального интервала времени, в течении которого будет учитываться трафик, относящийся к сетевому потоку. |
| `system flow-accounting netflow timeout tcp-fin <таймаут>` | Указание таймаута сетевого потока TCP после получения пакета TCP с флагом FIN. |

| | |
|---|---|
| `system flow-accounting netflow timeout tcp-generic <таймаут>` | Указание таймаута сетевого потока TCP. |
| `system flow-accounting netflow timeout tcp-rst <таймаут>` | Указание таймаута сетевого потока TCP после получения пакета TCP с флагом RST. |
| `system flow-accounting netflow timeout udp <таймаут>` | Указание таймаута сетевого потока для трафика UDP. |
| `system flow-accounting netflow version <версия>` | Указание формата Netflow, в котором будут экспортированы данные учета. |
| `system flow-accounting sflow agent-address <адрес>` | Указание IP-адреса агента sFlow. |
| `system flow-accounting sflow sampling-rate <частота_выборки>` | Указание частоты выборки для статистики sFlow. |
| `system flow-accounting sflow server <ipv4-адрес>` | Указание адреса сборщика SFlow для экспорта данных учета. |
| `system flow-accounting syslog-facility <источник>` | Указание типов сообщений, относящихся к учету трафика, которые будут регистрироваться в журнале. |
| Эксплуатационные команды | |
| `clear flow-accounting counters` | Очистка всех счетчиков учета трафика. |
| `clear flow-accounting process` | Перезапуск процесса учета сетевых потоков. |
| `show flow-accounting` | Отображение статистики для всех интерфейсов, на которых ведется учет трафика. |

| | |
|---|---|
| `show flow-accounting interface <интерфейс>` | Вывод статистических данных для указанного интерфейса. |

### 25.2.1. clear flow-accounting counters

Очистка всех счетчиков учета трафика.

**Синтаксис**

**`clear flow-accounting 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.

### 25.2.2. clear flow-accounting process

Перезапуск процесса учета сетевых потоков.

**Синтаксис**

**`clear flow-accounting process`**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда используется для перезапуска процесса учета трафика.

### 25.2.3. show flow-accounting

Отображение статистики для всех интерфейсов, на которых ведется учет трафика.

**Синтаксис**

**show flow-accounting**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет отобразить статистические данные для всех интерфейсов, на которых ведется учет трафика.

### 25.2.4. show flow-accounting interface <интерфейс>

Вывод статистических данных для указанного интерфейса.

**Синтаксис**

**show flow-accounting interface** *интерфейс* [**host** *узел*] [**port** *порт*] [**top** *число*]

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*интерфейс*

Интерфейс, для которого будет выведена статистика (например, eth0). На интерфейсе должен быть настроен учет сетевого трафика.

*узел*

IP-адрес узла, статистические данные для которого будут выведены.

*порт*

Номер сетевого порта, для которого будут выведены статистические данные.

*число*

Число потоков с максимальным объемом трафика, которые будут отображены. Они будут выведены в убывающем порядке, на основе количества байт, полученных на интерфейсе.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет вывести данные учета трафика на указанном интерфейсе. На интерфейсе должен быть предварительно настроен учет сетевого трафика.

## 25.2.5. system flow-accounting interface <интерфейс>

Указание интерфейса, для которого будет производиться учет входящего трафика.

**Синтаксис**

**set system flow-accounting interface** *интерфейс*

**delete system flow-accounting interface** *интерфейс*

**show system flow-accounting interface**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
    flow-accounting {
        interface текст
    }
}
```

**Параметры**

*интерфейс*

Множественный узел. Интерфейс, для которого будет осуществляться учет входящего трафика (например, eth0).

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 записи учетных данных.

Форма **show** данной команды используется для отображения интерфейсов, на которых ведется учет трафика.

### 25.2.6. system flow-accounting netflow engine-id <идентификатор>

Указание идентификатора системы, который будет включен в данные Netflow.

**Синтаксис**

**set system flow-accounting netflow engine-id** *идентификатор*

**delete system flow-accounting netflow engine-id**

**show system flow-accounting netflow engine-id**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
    flow-accounting {
        netflow {
            engine-id целое32разрядн
        }
    }
}
```

**Параметры**

*идентификатор*

Идентификатор системы, который указывается в данных Netflow, позволяющий идентифицировать маршрутизатор, отправивший отчет. Значение должно лежать в диапазоне от 0 до 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.

### 25.2.7. system flow-accounting netflow sampling-rate <частота>

Указание частоты отсчетов, с которой сетевые пакеты будут учитываться в статистике.

**Синтаксис**

**set system flow-accounting netflow sampling-rate** *частота*

**delete system flow-accounting netflow sampling-rate**

**show system flow-accounting netflow sampling-rate**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
    flow-accounting {
        netflow {
            sampling-rate целое32разрядн
        }
    }
}
```

**Параметры**

*частота_выборки*

Частота, с которой будут отбираться пакеты (например, при установке значения 100 будет учитываться каждый 100-ый пакет).

**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, настроенное для узла **sampling-rate**.

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.

Форма **delete** данной команды используется для удаления конфигурации и восстановления значения, принятого по умолчанию.

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

## 25.2.8. system flow-accounting netflow server <ipv4-адрес>

Указание коллектора Netflow для экспорта данных Netflow.

**Синтаксис**

**set system flow-accounting netflow server** *ipv4-адрес* [**port** *порт*]

**delete system flow-accounting netflow server** *ipv4-адрес* [**port**]

**show system flow-accounting netflow server** *ipv4-адрес* [**port**]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
    flow-accounting {
        netflow {
            server ipv4 {
                port целое32разрядн
            }
        }
    }
}
```

**Параметры**

*ipv4-адрес*

Множественный узел. Указание IP-адреса коллектора Netflow 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 по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет указать коллектор Netflow, на который будут экспортироваться данные учета.

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.

## 25.2.9. system flow-accounting netflow timeout expiry-interval <интервал>

Указание интервала, через который будут отправляться отчеты коллектору данных Netflow.

**Синтаксис**

**set system flow-accounting netflow timeout expiry-interval** *интервал*

**delete system flow-accounting netflow timeout expiry-interval**

**show system flow-accounting netflow timeout expiry-interval**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
    flow-accounting {
        netflow {
            timeout {
                expiry-interval целое32разрядн
            }
        }
    }
}
```

**Параметры**

*интервал*

Интервал времени, через который будут отправляться отчеты коллектору Netflow.

**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 <ipv4-адрес>.

Форма **set** данной команды используется для указания интервала времени для отправки отчетов.

Форма **delete** данной команды используется для удаления конфигурации и восстановления значения, принятого по умолчанию.

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

## 25.2.10. system flow-accounting netflow timeout flow-generic <таймаут>

Указание таймаута сетевого потока для трафика IP.

**Синтаксис**

**set system flow-accounting netflow timeout flow-generic** *таймаут*

**delete system flow-accounting netflow timeout flow-generic**

**show system flow-accounting netflow timeout flow-generic**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
    flow-accounting {
        netflow {
            timeout {
                flow-generic целое32разрядн
            }
        }
    }
}
```

**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 от 1 до 4294967296. Значение по умолчанию 3600 (1 час).

**Значение по умолчанию**

Сетевые потоки, относящиеся к общему трафику IP, считаются завершенными по истечению 3600 секунд.

**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.

## 25.2.11. system flow-accounting netflow timeout icmp <таймаут>

Указание таймаута сетевого потока для трафика ICMP.

**Синтаксис**

**set system flow-accounting netflow timeout icmp** *таймаут*

**delete system flow-accounting netflow timeout icmp**

**show system flow-accounting netflow timeout icmp**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
     flow-accounting {
          netflow {
               timeout {
                    icmp целое32разрядн
               }
          }
     }
}
```

**Параметры**

*таймаут*

Таймаут сетевого потока, в секундах, для трафика ICMP. Значение должно лежать в диапазоне от 1 до 4294967296. По умолчанию установлено значение 300 (5 минут).

**Значение по умолчанию**

Для сетевых потоков трафика ICMP установлен таймаут 300 секунд.

**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.

## 25.2.12. system 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 system flow-accounting netflow timeout max-active-life** *время_жизни*

**delete system flow-accounting netflow timeout max-active-life**

**show system flow-accounting netflow timeout max-active-life**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
    flow-accounting {
        netflow {
            timeout {
                max-active-life целое32разрядн
            }
        }
```

```
        }
    }
```

**Параметры**

*время_жизни*

Интервал времени, в секундах, определяющий максимальное время учета трафика, относящегося к сетевому потоку любого типа. Значение должно лежать в диапазоне от 1 до 4294967296. По умолчанию установлено значение 604800 (7 дней).

**Значение по умолчанию**

Сетевые потоки любого типа считаются завершенными по истечении 604,800 секунд.

**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.

## 25.2.13. system flow-accounting netflow timeout tcp-fin <таймаут>

Указание таймаута сетевого потока TCP после получения пакета TCP с флагом FIN.

**Синтаксис**

**set system flow-accounting netflow timeout tcp-fin** *таймаут*

**delete system flow-accounting netflow timeout tcp-fin**

**show system flow-accounting netflow timeout tcp-fin**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
    flow-accounting {
        netflow {
            timeout {
                tcp-fin целое32разрядн
            }
        }
    }
}
```

**Параметры**

*таймаут*

Таймаут сетевого потока, в секундах, после получения пакета TCP с флагом FIN. Значение должно лежать в диапазоне от 1 до 4294967296. По умолчанию установлено значение 300 (5 минут).

**Значение по умолчанию**

Сетевой поток TCP считается завершенным с точки зрения системы учета трафика через 300 секунд 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.

## 25.2.14. system flow-accounting netflow timeout tcp-generic <таймаут>

Указание таймаута сетевого потока TCP.

**Синтаксис**

**set system flow-accounting netflow timeout tcp-generic** *таймаут*

**delete system flow-accounting netflow timeout tcp-generic**

**show system flow-accounting netflow timeout tcp-generic**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
    flow-accounting {
        netflow {
            timeout {
                tcp-generic целое32разрядн
            }
        }
    }
}
```

**Параметры**

*таймаут*

Таймаут для потока TCP, в секундах. Значение должно лежать в диапазоне от 1 до 4294967296. Значение по умолчанию 3600 (1 час).

**Значение по умолчанию**

В том случае если в течении 3600 секунд 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.

## 25.2.15. system flow-accounting netflow timeout tcp-rst <таймаут>

Указание таймаута сетевого потока TCP после получения пакета TCP с флагом RST.

**Синтаксис**

**set system flow-accounting netflow timeout tcp-rst** *таймаут*

**delete system flow-accounting netflow timeout tcp-rst**

**show system flow-accounting netflow timeout tcp-rst**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
    flow-accounting {
        netflow {
            timeout {
                tcp-rst целое32разрядн
            }
        }
    }
}
```

**Параметры**

*таймаут*

Таймаут сетевого потока, в секундах, после получения пакета TCP RST. Значение должно лежать в диапазоне от 1 до 4294967296. По умолчанию установлено значение 120 (2 минуты).

**Значение по умолчанию**

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.

## 25.2.16. system flow-accounting netflow timeout udp <таймаут>

Указание таймаута сетевого потока для трафика UDP.

**Синтаксис**

**set system flow-accounting netflow timeout udp** *таймаут*

**delete system flow-accounting netflow timeout udp**

**show system flow-accounting netflow timeout udp**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
    flow-accounting {
        netflow {
            timeout {
                udp целое32разрядн
            }
        }
    }
}
```

**Параметры**

*таймаут*

Таймаут сетевого потока для трафика UDP. Значение должно лежать в диапазоне от 1 до 4294967296. По умолчанию установлено значение 300 (5 минут).

**Значение по умолчанию**

Для сетевого потока трафика UDP установлено значение таймаута 300 секунд.

**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.

## 25.2.17. system flow-accounting netflow version <версия>

Указание формата Netflow, в котором будут экспортированы данные учета.

**Синтаксис**

**set system flow-accounting netflow version** *версия*

**delete system flow-accounting netflow version**

**show system flow-accounting netflow version**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
    flow-accounting {
        netflow {
            version целое32разрядн
        }
    }
}
```

**Параметры**

*версия*

Номер версии Netflow, в формате которой будут экспортированы данные учета. Допустимые значения: 1, 5, 9. По умолчанию установлено значение 5.

**Значение 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.

## 25.2.18. system flow-accounting sflow agent-address <адрес>

Указание IP-адреса агента sFlow.

**Синтаксис**

**set system flow-accounting sflow agent-address** *адрес*

**delete system flow-accounting sflow agent-address**

**show system flow-accounting sflow agent-address**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
    flow-accounting {
        sflow {
            agent-address текст
        }
    }
}
```

**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) или IPv4-адрес. По умолчанию установлено значение **auto**.

**Значение по умолчанию**

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 Altell NEO.

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.

## 25.2.19. system flow-accounting sflow sampling-rate <частота_выборки>

Указание частоты выборки для статистики sFlow.

**Синтаксис**

**set system flow-accounting sflow sampling-rate** *частота_выборки*

**delete system flow-accounting sflow sampling-rate**

**show system flow-accounting sflow sampling-rate**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
    flow-accounting {
        sflow {
            sampling-rate целое32разрядн
        }
    }
}
```

**Параметры**

*частота_выборки*

Частота, с которой будут отбираться пакеты (то есть, каждый n-ный пакет по порядку будет учитываться, если *n* - частота).

**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.

## 25.2.20. system flow-accounting sflow server <ipv4-адрес>

Указание адреса коллектора SFlow для экспорта данных учета.

**Синтаксис**

**set system flow-accounting sflow server** *ipv4-адрес* [**port** *порт*]

**delete system flow-accounting sflow server** *ipv4-адрес* [**port**]

**show system flow-accounting sflow server** *ipv4-адрес* [**port** ]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
    flow-accounting {
        sflow {
            server ipv4-адрес {
                port целое32разрядн
            }
        }
    }
}
```

**Параметры**

*ipv4-адрес*

Множественный узел. IP-адрес коллектора sFlow для экспорта учетных данных.

Для того чтобы настроить экспорт на несколько удаленных серверов, следует создать соответствующее количество узлов конфигурации.

*порт*

Порт, на котором коллекор SFlow принимает отчеты. По умолчанию используется порт 6343.

**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.

## 25.2.21. system flow-accounting syslog-facility <источник>

Указание типов сообщений, относящихся к учету трафика, которые будут регистрироваться в журнале.

**Синтаксис**

**set system flow-accounting syslog-facility** *источник*

**delete system flow-accounting syslog-facility**

**show system flow-accounting syslog-facility**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
system {
    flow-accounting {
        syslog-facility текст
    }
}
```

**Параметры**

*источник*

Источник сообщений, от имени которого сообщения, связанные с учетом трафика, будут регистрироваться в журнале. Более подробная информация о

поддерживаемых типах источников приведена в описании команды system syslog.

По умолчанию используется значение **daemon**.

**Значение 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.

# 26. QOS

В данном разделе представлен краткий обзор функций качества обслуживания (QoS) в Altell NEO.

Рассматриваются следующие вопросы:

- Механизмы QoS.
- Приоритизация трафика по умолчанию.
- Механизмы для исходящего трафика.
- Механизмы для входящего трафика.

## 26.1. Механизмы QoS

Качество обслуживания (Quality of service, QoS) - это функция, дающая сетевым администраторам возможность определять различные потоки трафика и затем выполнять над ними нужные действия в соответствии с их индивидуальными требованиями вместо простого использования механизма по умолчанию.

В Altell NEO механизм QoS по умолчанию основан на приоритизации очереди. Помимо механизма работы с очередью по умолчанию, в Altell NEO имеется ряд механизмов QoS для определения различных потоков трафика, проходящих через интерфейс, и выполнения нужных действий над ними. В общем, эти механизмы можно разделить на применяемые ко входящему трафику и применяемые к исходящему трафику.

Общий порядок работы с механизмами QoS, отличными от механизма по умолчанию, таков.

1. Создание политики QoS. Политика служит для определения потоков трафика и указания действий, которые следует выполнить над каждым потоком.
2. Применение политики к интерфейсу.

## 26.2. Приоритизация трафика по умолчанию

По умолчанию, весь трафик, отправляемый с Altell NEO наружу, распределяется по приоритету на основе значения поля типа обслуживания (Type of Service, ToS) в одну из трех приоритетных очередей. Пакеты из очереди с наивысшим приоритетом отправляются первыми, потом отправляются пакеты из очереди со следующим приоритетом и, наконец, пакеты из очереди с наименьшим приоритетом. Внутри каждой очереди все пакеты

отправляются на основе дисциплины "первым пришел - первым ушел" (First In First Out, FIFO) и доставляются настолько быстро, насколько возможно. Если трафик появляется в очереди быстрее, чем он может быть доставлен (например, из-за ограничений, связанных с пропускной способностью), он буферизуется внутри системы. Если приходит больше данных, чем система может буферизовать, то избыток данных отбрасывается.

Трафик данных делится указанным образом, так как предоставление одинакового уровня обслуживания для всего трафика не всегда желательно. По отношению к некотором типам трафика в силу их природы следует выполнять иные действия, чем по отношению к другим типам. Например, голосовой трафик очень чувствителен к задержкам и при отсутствии надлежащей обработки может быть искажен до неузнаваемости. С другой стороны, данные чувствительны не к задержкам, а к повреждению.

## 26.3. Механизмы для исходящего трафика

Altell NEO поддерживает следующие механизмы QoS для контроля над исходящим трафиком.

- Отбрасывание конца очереди (обрубание хвоста).
- Справедливая очередь.
- Циклический перебор.
- Управление загрузкой канала.
- Ограничение скорости.
- Имитация сети.
- Случайное определение.

### 26.3.1. Отбрасывание конца очереди (обрубание хвоста)

Механизм отбрасывания конца очереди - это алгоритм планирования. Он обеспечивает работу с очередями по принципу FIFO; другими словами, пакеты данных передаются в том же порядке, в котором они приходят. Если очередь заполняется, "хвост" очереди (то есть группа пакетов, приходящих в очередь в данный момент) отбрасывается. Если используется механизм отбрасывания конца очереди, то имеется только одна очередь, а надо всем трафиком выполняются одни и те же действия; в отличие от случая по умолчанию, трафик не приоритизируется.

### 26.3.2. Справедливая очередь

Механизм справедливой очереди - это алгоритм планирования. Он обеспечивает работу с очередями на основе алгоритма SFQ. В этом алгоритме работы с очередями потоки трафика определяются по протоколу IP, адресу отправителя и/или адресу получателя. Так определенные потоки получают справедливый доступ к ресурсам сети таким образом, чтобы никакой поток не мог использовать большую долю пропускной способности.

### 26.3.3. Циклический перебор

Механизм циклического перебора - это простой алгоритм планирования. При работе с очередями методом циклического перебора определяются классы трафика, и пропускная способность делится поровну между определенными классами.

### 26.3.4. Управление загрузкой канала

Механизм управления загрузкой канала обеспечивает работу с очередями на основе алгоритма "маркерного ведра". Алгоритм допускает "всплески" (кратковременные контролируемые передачи групп пакетов со скоростью превосходящей административно установленную), если в "ведре" есть "избыточные" маркеры. 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 поровну между определенными классами.

### 26.3.5. Ограничение скорости

Механизм ограничения скорости - это алгоритм планирования. Он обеспечивает работу с очередями на основе алгоритма "маркерного ведра". Этот алгоритм пропускает только пакеты, приходящие со скоростью, не превосходящей административно установленной скорости. Тем не менее, возможно кратковременное превышение трафиком этой скорости.

### 26.3.6. Случайное определение

Механизм случайного определения - это механизм предотвращения перегрузки, в

состав которого входят случайное ранее определение (Random Early Detection, RED) и взвешенное случайное раннее определение (Weighted Random Early Detection, WRED).

Состояние перегрузки возникает, когда выходные буферы заполняются до такой степени, что возникает необходимость в отбрасывании пакетов. Перегрузка может вызвать глобальную пересинхронизацию узлов TCP в ситуации, когда несколько узлов снижают скорость передачи в попытке избавиться от перегрузки; такие действия могут существенно повлиять на работоспособность сети. После ликвидации перегрузки скорость передачи в сети 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 сети путем случайного отбрасывания пакетов в ситуации, когда на выходном интерфейсе начинают появляться признаки перегрузки. Отбрасывание пакетов дает отправителю пакетов сигнал о том, что необходимо снизить скорость передачи; в свою очередь, это помогает избежать возникновения перегрузки и уменьшает вероятность глобальной синхронизации, что способствует улучшению использования пропускной способности сети.

WRED - это развитие RED еще на одну ступень: во WRED есть способ добавить предпочтительность к различным потокам трафика. Таким способом можно обеспечить раздельное качество обслуживания для различных потоков трафика путем отбрасывания из одних потоков большего числа пакетов, чем из других.

### 26.3.7. Имитация сети

Механизм имитации сети предоставляет способ имитации трафика ГВС. Обычно он используется для тестирования системы.

## 26.4. Механизмы для входящего трафика

Altell NEO поддерживает следующий механизм QoS для входящего трафика:

- Ограничение трафика.

### 26.4.1. Ограничение трафика

Механизм ограничения трафика можно использовать для регулирования входящего трафика. Механизм назначает каждому потоку трафика ограничение пропускной

способности. Весь приходящий трафик потока, выходящий за ограничение пропускной способности, отбрасывается.

## 26.5. Примеры настройки QoS

В данном разделе приведены следующие примеры настройки реализации качества обслуживания (QoS) в Altell NEO.

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.

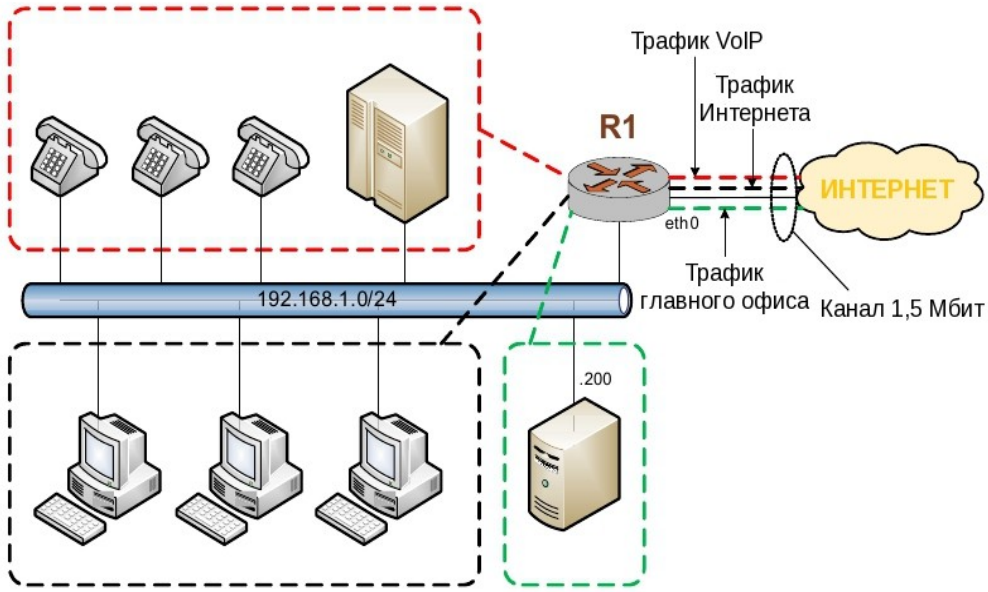
## 26.6. Пример на исходящий трафик - управление загрузкой канала

На рисунке 86 показана простая сеть филиала с использованием QoS в Altell NEO (R1) для выполнения различных действий над тремя потоками трафика. В схеме представлен один филиал с телефонной системой VoIP (голос по IP), пользователями, подключающимися к Интернету, и сервером, которому требуется относительно высокоскоростное подключение к главному офису. В приведенном примере:

- Весь трафик проходит по каналу 1,5 Мбит до поставщика услуг доступа к Интернету.
- Минимум 50% пропускной способности следует зарезервировать для трафика VoIP, 35% для трафика главного офиса и 15% для всего остального трафика.
- Все потоки трафика будут использовать доступную пропускную способность сверх настроенных для них минимальных скоростей.
- Кроме того, трафик VoIP должен быть классифицирован в два различных потока:
  - 5% пропускной способности следует использовать для трафика контроля (в примере - сигналы протокола SIP для установки вызовов).
  - 45% пропускной способности следует использовать для носителей протокола RTP (Real Time Protocol, протокол реального времени). Различные потоки определяются по их значению поля DSCP: трафику SIP присваивается значение DSCP 26, а трафику RTP - 46.)

- Трафик главного офиса приходит с одного сервера с IP-адресом 192.168.1.200.

*Рисунок 86 - Пример филиала с VoIP с использованием QoS*




Для настройки данной схемы нужно выполнить следующие действия в режиме настройки.

*Пример 26.1 - Управление загрузкой канала*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для политики QoS. | `admin@R1# set traffic-policy shaper OFFICE`<br>`[edit]` |
| Добавление описания. | `admin@R1# set traffic-policy shaper OFFICE description "QoS policy for office WAN"`<br>`[edit]` |
| Установка суммарной пропускной способности канала. | `admin@R1# set traffic-policy shaper OFFICE bandwidth 1500kbit`<br>`[edit]` |

| | |
|---|---|
| Добавление описания для трафика первого класса - трафика данных VOIP. | admin@R1# **set traffic-policy shaper OFFICE class 10 description "VOIP - RTP traffic"**<br>[edit] |
| Назначение пропускной способности для трафика данных VOIP. | admin@R1# **set traffic-policy shaper OFFICE class 10 bandwidth 45%**<br>[edit] |
| Разрешение трафику данных VOIP использовать всю доступную пропускную способность. | admin@R1# **set traffic-policy shaper OFFICE class 10 ceiling 100%**<br>[edit] |
| Определение трафика данных VOIP (DSCP=46). | admin@R1# **set traffic-policy shaper OFFICE class 10 match VOIP-RTP ip dscp 46**<br>[edit] |
| Добавление описания для второго класса трафика - трафика контроля VOIP. | admin@R1# **set traffic-policy shaper OFFICE class 20 description "VOIP -SIP traffic"**<br>[edit] |
| Назначение пропускной способности для трафика контроля VOIP. | admin@R1# **set traffic-policy shaper OFFICE class 20 bandwidth 5%**<br>[edit] |
| Разрешение трафику контроля VOIP использовать всю доступную пропускную способность. | admin@R1# **set traffic-policy shaper OFFICE class 20 ceiling 100%**<br>[edit] |
| Определение трафика контроля VOIP | admin@R1# **set traffic-policy** |

| | |
|---|---|
| (DSCP=26). | **shaper OFFICE class 20 match VOIP-SIP ip dscp 26**<br>[edit] |
| Добавление описания для третьего класса трафика - трафика главного офиса. | admin@R1# **set traffic-policy shaper OFFICE class 30 description "Head office traffic"**<br>[edit] |
| Назначение пропускной способности для трафика главного офиса. | admin@R1# **set traffic-policy shaper OFFICE class 30 bandwidth 35%**<br>[edit] |
| Разрешение трафику главного офиса использовать всю доступную пропускную способность. | admin@R1# **set traffic-policy shaper OFFICE class 30 ceiling 100%**<br>[edit] |
| Определение трафика главного офиса (IP-адрес=192.168.1.200/24). | admin@R1# **set traffic-policy shaper OFFICE class 30 match HO-TRAFFIC ip source address 192.168.1.200/24**<br>[edit] |
| Назначение пропускной способности для остатка трафика. | admin@R1# **set traffic-policy shaper OFFICE default bandwidth 15%**<br>[edit] |
| Разрешение трафику по умолчанию использовать всю доступную пропускную способность. | admin@R1# **set traffic-policy shaper OFFICE default ceiling 100%**<br>[edit] |
| Фиксация изменения. | admin@R1# **commit** |

```
[edit]
```

Вывод настройки **traffic-policy**.

```
admin@R1# show traffic-policy
shaper OFFICE {
     bandwidth 1500kbit
     class 10 {
          bandwidth 45%
          ceiling 100%
          description “VOIP - RTP
traffic”
          match VOIP-RTP {
               ip {
                    dscp 46
               }
          }
     }
     class 20 {
          bandwidth 5%
          ceiling 100%
          description “VOIP - SIP
traffic”
          match VOIP-SIP {
               ip {
                    dscp 26
               }
          }
     }
     class 30 {
          bandwidth 35%
          ceiling 100%
          description “Head
office traffic”
```

```
                match HO-TRAFFIC {
                     ip {
                          source {
                               address
192.168.1.200/24
                          }
                     }
                }
           }
           default {
                bandwidth 15%
                ceiling 100%
           }
           description “QoS policy for
office WAN”
}
[edit]
```

| | |
|---|---|
| Назначение политики QoS интерфейсу ГВС. | admin@R1# **set interfaces ethernet eth0 traffic-policy out OFFICE**<br>[edit] |

## 26.7. Пример на входящий трафик - ограничение трафика

В данном примере выполняется ограничение входящего трафика электронной почты (порт 25) до 300 кбит/с. Для настройки данной схемы нужно выполнить следующие действия в режиме настройки.

*Пример 26.2 - Ограничение трафика*

| Действие | Команда |
|---|---|
| Создание узла конфигурации для данной политики QoS. | admin@R1# **set traffic-policy limiter LIMIT-MAIL**<br>[edit] |

Добавление описания для класса трафика - трафик почты.

```
admin@R1# set traffic-policy limiter LIMIT-MAIL class 10 description "Limit inbound mail traffic"
[edit]
```

Назначение пропускной способности для трафика данных почты.

```
admin@R1# set traffic-policy limiter LIMIT-MAIL class 10 bandwidth 300kbit
[edit]
```

Определение трафика данных почты (порт=25).

```
admin@R1# set traffic-policy limiter LIMIT-MAIL class 10 match MAIL-TRAFFIC ip destination port 25
[edit]
```

Фиксация изменения.

```
admin@R1# commit
[edit]
```

Отображение настройки **traffic-policy**.

```
admin@R1# show traffic-policy
 limiter LIMIT-MAIL {
     class 10 {
          bandwidth 300kbit
          description "Limit
inbound mail traffic"
          match MAIL-TRAFFIC {
               ip {
                    destination {
                         port 25
                    }
               }
          }
     }
```

| | |
|---|---|
| | }<br>[edit] |
| Назначение политики QoS входящему трафику на eth0. | admin@R1# **set interfaces ethernet eth0 traffic-policy in LIMIT-MAIL**<br>[edit] |

## 26.8. Пример на входящий трафик - контроль пропускной способности на нескольких интерфейсах

В данном примере суммарный входящий трафик с интерфейсов eth0, eth1 и eth2 не должен превосходить 1 Гбит/с. Для контроля этого ограничения входящий трафик с этих интерфейсов перенаправляется на входной интерфейс ifb0. Создается политика контроля скорости для ограничения трафика величиной 1 Гбит/с, после чего она назначается интерфейсу ifb0.

Для настройки данной схемы нужно выполнить следующие действия в режиме настройки.

*Пример 26.3 - Ограничение трафика на нескольких интерфейсах*

| Действие | Команда |
|---|---|
| Перенаправление трафика eth0 на входной интерфейс ifb0. | admin@R1# **set interfaces ethernet eth0 redirect ifb0**<br>[edit] |
| Перенаправление трафика eth1 на входной интерфейс ifb0. | admin@R1# **set interfaces ethernet eth1 redirect ifb0**<br>[edit] |
| Перенаправление трафика eth2 на входной интерфейс ifb0. | admin@R1# **set interfaces ethernet eth2 redirect ifb0**<br>[edit] |
| Создание узла конфигурации для данной политики QoS. | admin@R1# **set traffic-policy limiter LIMIT-1Gbit**<br>[edit] |

| | |
|---|---|
| Добавление описания для политики QoS. | admin@R1# **set traffic-policy rate-control LIMIT-1Gbit description "Limit traffic to 1Gbit"**<br>[edit] |
| Назначение ограничения пропускной способности трафику. | admin@R1# **set traffic-policy rate-control LIMIT-1Gbit bandwidth 1gbit**<br>[edit] |
| Фиксация изменения. | admin@R1# **commit**<br>[edit] |
| Отображение настройки **traffic-policy**. | admin@R1# **show traffic-policy**<br>rate-control LIMIT-1Gbit {<br>bandwidth 1gbit<br>description "Limit traffic to 1Gbit"<br>}<br>[edit] |
| Применение политики QoS к исходящему трафику на ifb0 (состоящему из суммарного трафика с eth0, eth1 и eth2). Исходящий трафик со входного интерфейса является внутренним для устройства Altell NEO. | admin@R1# **set interfaces input ifb0 traffic-policy out LIMIT-1Gbit**<br>[edit] |

## 26.9. Команды QoS

В данном разделе описаны команды для функций QoS, поддерживаемых Altell NEO.

В данном разделе приведены следующие команды.

| Команды настройки | |
|---|---|
| **Применение политик QoS к интерфейсам** | |
| `interfaces <интерфейс> traffic-policy` | Применение политики QoS к указанному интерфейсу. |
| **Политики отбрасывания конца очереди** | |
| `traffic-policy drop-tail <имя_политики>` | Определение политики QoS с отбрасыванием конца очереди (чистая дисциплина FIFO). |
| `traffic-policy drop-tail <имя_политики> queue-limit <ограничение>` | Установка верхней границы разрешенного числа пакетов в очереди для политики отбрасывания конца очереди. |
| **Политики справедливой очереди** | |
| `traffic-policy fair-queue <имя_политики>` | Определение политики QoS со справедливой очередью. |
| `traffic-policy fair-queue <имя_политики> description <описание>` | Ввод описания для политики справедливой очереди. |
| `traffic-policy fair-queue <имя_политики> hash-interval <секунды>` | Указание интервала между обновлениями функции хэширования потока для политики справедливой очереди. |
| `traffic-policy fair-queue <имя_политики> queue-limit <ограничение>` | Установка верхней границы разрешенного числа пакетов в очереди для политики справедливой очереди. |
| **Политики имитации сети** | |
| `traffic-policy network-emulator <имя_политики>` | Определение политики QoS с имитацией сети. |
| `traffic-policy network-emulator <имя_политики>` | Указание ограничения пропускной способности для всего суммарного трафика, |

| | |
|---|---|
| | ограничиваемого данной политикой. |
| `traffic-policy network-emulator <имя_политики> burst` | Установка размера непрерывной серии пакетов для политики QoS с имитацией сети. |
| `traffic-policy network-emulator <имя_политики> description <описание>` | Ввод описания для политики имитации сети. |
| `traffic-policy network-emulator <имя_политики> network-delay` | Установка величины задержки между пакетами для политики QoS с имитацией сети. |
| `traffic-policy network-emulator <имя_политики> packet-corruption <процент>` | Установка процентной доли пакетов, подлежащих повреждению, в политике QoS с имитацией сети. |
| `traffic-policy network-emulator <имя_политики> packet-loss <процент>` | Установка процентной доли пакетов, подлежащих потере, в политике QoS с имитацией сети. |
| `traffic-policy network-emulator <имя_политики> packet-reordering <процент>` | Установка процентной доли пакетов, подлежащих изменению порядка следования, в политике QoS с имитацией сети. |
| `traffic-policy network-emulator <имя_политики> queue-limit <ограничение>` | Установка верхней границы разрешенного числа пакетов в очереди для политики QoS с имитацией сети. |
| Политики случайного определения | |
| `traffic-policy random-detect <имя_политики>` | Определение политики QoS со взвешенным случайным ранним определением (WRED). |
| `traffic-policy random-detect <имя_политики> bandwidth` | Указание ограничения пропускной способности для всего суммарного трафика, ограничиваемого данной политикой. |

| | |
|---|---|
| `traffic-policy random-detect <имя_политики> description <описание>` | Ввод описания для политики случайного определения. |
| `traffic-policy random-detect <имя_политики> precedence <предпочтительность>` | Установка параметров отбрасывания пакетов на основе предпочтительности для политики случайного определения. |
| Политики ограничения скорости | |
| `traffic-policy rate-control <имя_политики>` | Определение политики QoS с ограничением скорости. |
| `traffic-policy rate-control <имя_политики> bandwidth` | Указание ограничения пропускной способности для всего суммарного трафика, ограничиваемого данной политикой. |
| `traffic-policy rate-control <имя_политики> burst` | Установка размера непрерывной серии пакетов для политики QoS с ограничением скорости. |
| `traffic-policy rate-control <имя_политики> description <описание>` | Ввод описания для политики ограничения скорости. |
| `traffic-policy rate-control <имя_политики> latency` | Установка ограничения на размер очереди на основе задержки для политики QoS с ограничением скорости. |
| Политики циклического перебора | |
| `traffic-policy round-robin <имя_политики>` | Определение политики QoS с циклическим перебором. |
| `traffic-policy round-robin <имя_политики> description <описание>` | Ввод описания для политики QoS с циклическим перебором. |

| Классы для политики циклического перебора | |
|---|---|
| `traffic-policy round-robin <имя_политики> class <класс>` | Определение класса трафика для политики QoS с циклическим перебором. |
| `traffic-policy round-robin <имя_политики> class <класс> description <описание>` | Ввод описания для класса трафика. |
| `traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия>` | Определение правила для проверки соответствия классов трафика. |
| `traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> description <описание>` | Ввод описания для правила соответствия. |
| `traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> ether destination <mac-адрес>` | Указание критерия соответствия на основе MAC-адреса получателя. |
| `traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> ether protocol <число>` | Указание критерия соответствия на основе типа пакета Ethernet. |
| `traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> ether source <mac-адрес>` | Указание критерия соответствия на основе MAC-адреса отправителя. |
| `traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> interface <интерфейс>` | Указание критерия соответствия на основе интерфейса для входящих пакетов. |

| | |
|---|---|
| `traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> ip destination` | Указание критерия соответствия на основе сведений IP о получателе. |
| `traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> ip dscp <значение>` | Указание критерия соответствия на основе значения поля DSCP. |
| `traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> ip protocol <протокол>` | Указание критерия соответствия на основе протокола IP. |
| `traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> ip source` | Указание критерия соответствия на основе сведений IP об отправителе. |
| `traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> ipv6 destination` | Указание критерия соответствия на основе сведений IPv6 о получателе. |
| `traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> ipv6 dscp <значение>` | Указание критерия соответствия на основе значения поля DSCP. |
| `traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> ipv6 protocol <протокол>` | Указание критерия соответствия на основе протокола IPv6. |
| `traffic-policy round-robin` | Указание критерия соответствия на основе |

| | |
|---|---|
| | сведений IPv6 об отправителе. |
| `traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> vif <идентификатор_vlan>` | Указание критерия соответствия на основе идентификатора VLAN. |
| `traffic-policy round-robin <имя_политики> class <класс> quantum <число_пакетов>` | Указание числа пакетов, которые могут быть отправлены за квант планирования. |
| `traffic-policy round-robin <имя_политики> class <класс> queue-limit <ограничение>` | Указание максимального размера очереди для класса трафика. |
| `traffic-policy 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 | |
| `traffic-policy round-robin <имя_политики> default` | Определение политики QoS по умолчанию с циклическим перебором. |
| `traffic-policy round-robin <имя_политики> default quantum <число_пакетов>` | Указание числа пакетов, которые могут быть отправлены за квант планирования. |
| `traffic-policy round-robin <имя_политики> default queue-limit <ограничение>` | Указание максимального размера очереди для класса трафика по умолчанию. |
| `traffic-policy round-robin <имя_политики> default queue-type <тип>` | Указание типа работы с очередью, используемого для класса трафика по умолчанию. |

| Политики ограничения трафика | |
|---|---|
| `traffic-policy limiter <имя_политики>` | Определение политики QoS с ограничением трафика. |
| `traffic-policy limiter <имя_политики> description <описание>` | Ввод описания для политики QoS с ограничением трафика. |
| **Классы для политики ограничения трафика** | |
| `traffic-policy limiter <имя_политики> class <класс>` | Определение класса трафика для политики QoS с ограничением трафика. |
| `traffic-policy limiter <имя_политики> class <класс> bandwidth` | Указание ограничения пропускной способности для класса трафика. |
| `traffic-policy limiter <имя_политики> class <класс> burst` | Установка размера непрерывной серии пакетов для класса трафика. |
| `traffic-policy limiter <имя_политики> class <класс> description <описание>` | Ввод описания для класса трафика. |
| `traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия>` | Определение правила для проверки соответствия классов трафика. |
| `traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> description <описание>` | Ввод описания для правила соответствия. |
| `traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия>` | Указание критерия соответствия на основе MAC-адреса получателя. |

| | |
|---|---|
| `traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> ether protocol <число>` | Указание критерия соответствия на основе типа пакета Ethernet. |
| `traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> ether source <mac-адрес>` | Указание критерия соответствия на основе MAC-адреса отправителя. |
| `traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> ip destination` | Указание критерия соответствия на основе сведений IP о получателе. |
| `traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> ip dscp <значение>` | Указание критерия соответствия на основе значения поля DSCP. |
| `traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> ip protocol <протокол>` | Указание критерия соответствия на основе протокола IP. |
| `traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> ip source` | Указание критерия соответствия на основе сведений IP об отправителе. |
| `traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> ipv6 destination` | Указание критерия соответствия на основе сведений IPv6 о получателе. |

| | |
|---|---|
| `traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> ipv6 dscp <значение>` | Указание критерия соответствия на основе значения поля DSCP. |
| `traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> ipv6 protocol <протокол>` | Указание критерия соответствия на основе протокола IPv6. |
| `traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> ipv6 source` | Указание критерия соответствия на основе сведений IPv6 об отправителе. |
| `traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> vif <идентификатор_vlan>` | Указание критерия соответствия на основе идентификатора VLAN. |
| `traffic-policy limiter <имя_политики> class <класс> priority <приоритет>` | Указания порядка обработки правил соответствия. |
| Политики управления загрузкой канала | |
| `traffic-policy shaper <имя_политики>` | Определение политики QoS с управлением загрузкой канала. |
| `traffic-policy shaper <имя_политики> bandwidth` | Указание пропускной способности, доступной для всего суммарного трафика, ограничиваемого данной политикой. |
| `traffic-policy shaper <имя_политики> description <описание>` | Ввод описания для политики QoS с управлением загрузкой канала. |

| Классы для политики управления загрузкой канала | |
|---|---|
| `traffic-policy shaper <имя_политики> class <класс>` | Определение класса трафика для политики QoS с управлением загрузкой канала. |
| `traffic-policy shaper <имя_политики> class <класс> bandwidth` | Указание базовой гарантированной пропускной способности для класса трафика. |
| `traffic-policy shaper <имя_политики> class <класс> burst` | Установка размера непрерывной серии пакетов для класса трафика. |
| `traffic-policy shaper <имя_политики> class <класс> ceiling` | Установка верхней границы пропускной способности для класса трафика. |
| `traffic-policy shaper <имя_политики> class <класс> description <описание>` | Ввод описания для класса трафика. |
| `traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия>` | Определение правила для проверки соответствия классов трафика. |
| `traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> description <описание>` | Ввод описания для правила соответствия. |
| `traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> ether destination <mac-адрес>` | Указание критерия соответствия на основе MAC-адреса получателя. |
| `traffic-policy shaper <имя_политики> class <класс>` | Указание критерия соответствия на основе типа пакета Ethernet. |

| | |
|---|---|
| `traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> ether source <mac-адрес>` | Указание критерия соответствия на основе MAC-адреса отправителя. |
| `traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> interface <интерфейс>` | Указание критерия соответствия на основе интерфейса для входящих пакетов. |
| `traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> ip destination` | Указание критерия соответствия на основе сведений IP о получателе. |
| `traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> ip dscp <значение>` | Указание критерия соответствия на основе значения поля DSCP. |
| `traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> ip protocol <протокол>` | Указание критерия соответствия на основе протокола IP. |
| `traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> ip source` | Указание критерия соответствия на основе сведений IP об отправителе. |
| `traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> ipv6` | Указание критерия соответствия на основе сведений IPv6 о получателе. |

| | |
|---|---|
| `traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> ipv6 dscp <значение>` | Указание критерия соответствия на основе значения поля DSCP. |
| `traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> ipv6 protocol <протокол>` | Указание критерия соответствия на основе протокола IPv6. |
| `traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> ipv6 source` | Указание критерия соответствия на основе сведений IPv6 об отправителе. |
| `traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> vif <идентификатор_vlan>` | Указание критерия соответствия на основе идентификатора VLAN. |
| `traffic-policy shaper <имя_политики> class <класс> priority <приоритет>` | Указание приоритета класса трафика при выделении дополнительной пропускной способности. |
| `traffic-policy shaper <имя_политики> class <класс> queue-limit <ограничение>` | Указание максимального размера очереди для класса трафика. |
| `traffic-policy shaper <имя_политики> class <класс> queue-type <тип>` | Указание типа работы с очередью, используемого для класса трафика. |
| `traffic-policy shaper <имя_политики> class <класс> set-dscp <значение>` | Перезапись поля DSCP в пакетах в данном классе трафика указанным значением. |

| Класс по умолчанию для политики управления загрузкой канала | |
|---|---|
| `traffic-policy shaper <имя_политики> default` | Определение политики QoS по умолчанию с управлением загрузкой канала. |
| `traffic-policy shaper <имя_политики> default bandwidth` | Указание базовой гарантированной пропускной способности для класса трафика по умолчанию. |
| `traffic-policy shaper <имя_политики> default burst` | Установка размера непрерывной серии пакетов для класса трафика по умолчанию. |
| `traffic-policy shaper <имя_политики> default ceiling` | Установка верхней границы пропускной способности для класса трафика по умолчанию. |
| `traffic-policy shaper <имя_политики> default priority <приоритет>` | Указание приоритета класса трафика по умолчанию при выделении дополнительной пропускной способности. |
| `traffic-policy shaper <имя_политики> default queue-limit <ограничение>` | Указание максимального размера очереди для класса трафика по умолчанию. |
| `traffic-policy shaper <имя_политики> default queue-type <тип>` | Указание типа работы с очередью, используемого для класса трафика по умолчанию. |
| `traffic-policy shaper <имя_политики> default set-dscp <значение>` | Перезапись поля DSCP в пакетах в классе трафика по умолчанию указанным значением. |
| Эксплуатационные команды | |
| `show queueing` | Отображение текущих политик QoS. |

### 26.9.1. interfaces <интерфейс> traffic-policy

Применение политики QoS к указанному интерфейсу.

**Синтаксис**

```
set interfaces интерфейс traffic-policy {in
имя_политики_для_входящих | out
имя_политики_для_исходящих}

delete interfaces интерфейс traffic-policy {in | out}

show interfaces интерфейс traffic-policy {in | out}
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces текст {
          traffic-policy {
               in текст
               out текст
          }
}
```

**Параметры**

*интерфейс*

Обязательный. Тип интерфейса. Подробное описание ключевых слов и аргументов приведено в таблице в Приложении 3.

*имя_политики_для_входящих*

Имя политики QoS для входящего трафика, применяемой к данному интерфейсу.

*имя_политики_для_исходящих*

Имя политики QoS для исходящего трафика, применяемой к данному интерфейсу.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для применения политики QoS к интерфейсу.

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.

## 26.9.2. traffic-policy drop-tail <имя_политики>

Определение политики QoS с отбрасыванием конца очереди (чистая дисциплина FIFO).

**Синтаксис**

**set traffic-policy drop-tail** *имя_политики*

**delete traffic-policy drop-tail** *имя_политики*

**show traffic-policy drop-tail** *имя_политики*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        drop-tail текст {
        }
}
```

**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 чистой 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.

### 26.9.3. traffic-policy drop-tail <имя_политики> queue-limit <ограничение>

Установка верхней границы разрешенного числа пакетов в очереди для политики отбрасывания конца очереди.

**Синтаксис**

**set traffic-policy drop-tail** *имя_политики* **queue-limit** *ограничение*

**delete traffic-policy drop-tail** *имя_политики* **queue-limit**

**show traffic-policy drop-tail** *имя_политики* **queue-limit**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
          drop-tail текст {
          queue-limit целоебеззнака32разр
          }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики отбрасывания конца очереди.

*ограничение*

Необязательный. Максимальный размер очереди в пакетах. Значение должно лежать в диапазоне от 1 до 4294967295. Значение по умолчанию совпадает с длиной очереди передачи по умолчанию у нижележащего оборудования. Для Ethernet это, как правило, 1000 пакетов.

**Значение по умолчанию**

Для Ethernet длина очереди, как правило, 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.

### 26.9.4. traffic-policy fair-queue <имя_политики>

Определение политики QoS со справедливой очередью.

**Синтаксис**

**set traffic-policy fair-queue** *имя_политики*

**delete traffic-policy fair-queue** *имя_политики*

**show traffic-policy fair-queue** *имя_политики*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        fair-queue текст {
        }
}
```

**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 Altell NEO 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 FQ.

Форма **delete** этой команды используется для удаления политики FQ.

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

### 26.9.5. traffic-policy fair-queue <имя_политики> description <описание>

Ввод описания для политики справедливой очереди.

**Синтаксис**

**set traffic-policy fair-queue** *имя_политики* **description** *описание*

**delete traffic-policy fair-queue** *имя_политики* **description**

**show traffic-policy fair-queue** *имя_политики* **description**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        fair-queue текст {
            description описание
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики справедливой очереди.

*описание*

Обязательный. 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.

## 26.9.6. traffic-policy fair-queue <имя_политики> hash-interval <секунды>

Указание интервала между обновлениями функции хэширования потока для политики справедливой очереди.

**Синтаксис**

**set traffic-policy fair-queue** *имя_политики* **hash-interval** секунды

**delete traffic-policy fair-queue** *имя_политики* **hash-interval**

**show traffic-policy fair-queue** *имя_политики* **hash-interval**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        fair-queue текст {
            hash-interval целоебеззнака32разр
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики справедливой очереди.

*секунды*

Обязательный. Интервал повторного вычисления функции контрольной суммы (хэширования) в секундах. Значение должно лежать в диапазоне от 0 до 4294967295, где 0 означает, что функция хэширования никогда не обновляется.

**Значение по умолчанию**

Функция хэширования никогда не обновляется.

**Указания по использованию**

Эта команда используется для установки интервала обновления функции хэширования потока.

Регулярное обновление функции хэширования 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 хэширования потока.

Форма **delete** этой команды используется для восстановления интервала хэширования по умолчанию.

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

## 26.9.7. traffic-policy fair-queue <имя_политики> queue-limit <ограничение>

Установка верхней границы разрешенного числа пакетов в очереди для политики справедливой очереди.

**Синтаксис**

**set traffic-policy fair-queue** *имя_политики* **queue-limit** *ограничение*

**delete traffic-policy fair-queue** *имя_политики* **queue-limit**

**show traffic-policy fair-queue** *имя_политики* **queue-limit**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        fair-queue текст {
            queue-limit целоебеззнака32разр
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики справедливой очереди.

*ограничение*

Обязательный. Максимальный размер очереди в пакетах. Значение должно лежать в диапазоне от 2 до 127. Значение по умолчанию равно 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.

## 26.9.8. traffic-policy network-emulator <имя_политики>

Определение политики QoS с имитацией сети.

**Синтаксис**

**set traffic-policy network-emulator** *имя_политики*

**delete traffic-policy network-emulator** *имя_политики*

**show traffic-policy network-emulator** *имя_политики*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        network-emulator текст {
        }
}
```

**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 создании 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.

## 26.9.9. traffic-policy network-emulator <имя_политики> bandwidth

Указание ограничения пропускной способности для всего суммарного трафика, ограничиваемого данной политикой.

**Синтаксис**

**set traffic-policy network-emulator** *имя_политики* **bandwidth** [*скорость* | *скорость_в_единицах*]

**delete traffic-policy network-emulator** *имя_политики* **bandwidth**

**show traffic-policy network-emulator** *имя_политики* **bandwidth**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        network-emulator текст {
            bandwidth текст
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики имитации сети.

*скорость*

Необязательный. Пропускная способность, указанная в килобитах в секунду.

*скорость_в_единицах*

Пропускная способность, указанная в виде числа и единицы измерения (например, 10mbit). Поддерживаются следующие единицы измерения:

**kbit**: килобитов в секунду.

**mbit**: мегабитов в секунду.

**gbit**: гигабитов в секунду.

**kbps**: килобайтов в секунду.

**mbps**: мегабайтов в секунду.

**gbps**: гигабайтов 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.

## 26.9.10. traffic-policy network-emulator <имя_политики> burst

Установка размера непрерывной серии пакетов для политики QoS с имитацией сети.

**Синтаксис**

**set traffic-policy network-emulator** *имя_политики* **burst** [*число* | *число_в_единицах*]

**delete traffic-policy network-emulator** *имя_политики* **burst**

**show traffic-policy network-emulator** *имя_политики* **burst**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        network-emulator текст {
            burst текст
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики имитации сети.

*число*

Размер непрерывной серии, указанный в байтах.

*число_в_единицах*

Размер непрерывной серии, указанный в виде числа и единицы измерения (например, 10mb). Поддерживаются следующие единицы измерения:

**kb**: килобайты.

**mb**: мегабайты.

**gb**: гигабайты.

**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.

Размер непрерывной серии должен находиться в промежутке между 15 КБ и 32 МБ.

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.

## 26.9.11. traffic-policy network-emulator <имя_политики> description <описание>

Ввод описания для политики имитации сети.

**Синтаксис**

**set traffic-policy network-emulator** *имя_политики* **description** *описание*

**delete traffic-policy network-emulator** *имя_политики* **description**

**show traffic-policy network-emulator** *имя_политики* **description**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        network-emulator текст {
            description описание
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики имитации сети.

*описание*

Обязательный. 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.

## 26.9.12. traffic-policy network-emulator <имя_политики> network-delay

Установка величины задержки между пакетами для политики QoS с имитацией сети.

**Синтаксис**

**set traffic-policy network-emulator** *имя_политики* **network-delay** [*число* | *число_в_единицах*]

**delete traffic-policy network-emulator** *имя_политики* **network-delay**

**show traffic-policy network-emulator** *имя_политики* **network-delay**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        network-emulator текст {
            network-delay текст
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики имитации сети.

*число*

Задержка, указанная в миллисекундах.

*число_в_единицах*

Задержка, указанная в виде числа и единицы измерения (например, 10ms). 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.

## 26.9.13. traffic-policy network-emulator <имя_политики> packet-corruption <процент>

Установка процентной доли пакетов, подлежащих повреждению, в политике QoS с имитацией сети.

**Синтаксис**

**set traffic-policy network-emulator** *имя_политики* **packet-corruption** *процент*[%]

**delete traffic-policy network-emulator** *имя_политики* **packet-corruption**

**show traffic-policy network-emulator** *имя_политики* **packet-corruption**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        network-emulator текст {
            packet-corruption текст
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики имитации сети.

*процент*

Процентная доля пакетов, подлежащих случайному повреждению.

**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.

## 26.9.14. traffic-policy network-emulator <имя_политики> packet-loss <процент>

Установка процентной доли пакетов, подлежащих потере, в политике QoS с имитацией сети.

**Синтаксис**

**set traffic-policy network-emulator** *имя_политики* **packet-loss** *процент*[%]

**delete traffic-policy network-emulator** *имя_политики* **packet-loss**

**show traffic-policy network-emulator** *имя_политики* **packet-loss**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        network-emulator текст {
            packet-loss текст
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики имитации сети.

*процент*

Процентная доля пакетов, подлежащих случайному отбрасыванию.

**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.

## 26.9.15. traffic-policy network-emulator <имя_политики> packet-reordering <процент>

Установка процентной доли пакетов, подлежащих изменению порядка следования, в политике QoS с имитацией сети.

**Синтаксис**

**set traffic-policy network-emulator** *имя_политики* **packet-reordering** *процент*[%]

**delete traffic-policy network-emulator** *имя_политики* **packet-reordering**

**show traffic-policy network-emulator** *имя_политики* **packet-reordering**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        network-emulator текст {
            packet-reordering текст
        }
}
```

**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.

## 26.9.16. traffic-policy network-emulator <имя_политики> queue-limit <ограничение>

Установка верхней границы разрешенного числа пакетов в очереди для политики QoS с имитацией сети.

**Синтаксис**

**set traffic-policy network-emulator** *имя_политики* **queue-limit** *ограничение*

**delete traffic-policy network-emulator** *имя_политики* **queue-limit**

**show traffic-policy network-emulator** *имя_политики* **queue-limit**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        network-emulator текст {
```

```
                    queue-limit целоебеззнака32разр
                }
        }
```

**Параметры**

*имя_политики*

Обязательный. Имя политики имитации сети.

*ограничение*

Обязательный. Максимальный размер очереди в пакетах. Значение должно лежать в диапазоне от 1 до 4294967295. Значение по умолчанию равно 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.

## 26.9.17. traffic-policy random-detect <имя_политики>

Определение политики QoS со взвешенным случайным ранним определением (WRED).

**Синтаксис**

**set traffic-policy random-detect** *имя_политики*

**delete traffic-policy random-detec**t *имя_политики*

**show traffic-policy random-detect** *имя_политики*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        random-detect текст {
        }
}
```

**Параметры**

*имя_политики*

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.

## 26.9.18. traffic-policy random-detect <имя_политики> bandwidth

Указание ограничения пропускной способности для всего суммарного трафика, ограничиваемого данной политикой.

**Синтаксис**

**set traffic-policy random-detect** *имя_политики* **bandwidth** [**auto** | *скорость* | *скорость_в_единицах*]

**delete traffic-policy random-detect** *имя_политики* **bandwidth**

**show traffic-policy random-detect** *имя_политики* **bandwidth**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        random-detect текст {
            bandwidth текст
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики случайного определения.

**auto**

Пропускная способность основана на скорости интерфейса. Это режим по умолчанию.

*скорость*

Пропускная способность, указанная в килобитах в секунду.

*скорость_в_единицах*

Пропускная способность, указанная в виде числа и единицы измерения (например, 10mbit). Поддерживаются следующие единицы измерения:

**kbit**: килобитов в секунду.

**mbit**: мегабитов в секунду.

**gbit**: гигабитов в секунду.

**kbps**: килобайтов в секунду.

**mbps**: мегабайтов в секунду.

**gbps**: гигабайтов 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.

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.

## 26.9.19. traffic-policy random-detect <имя_политики> description <описание>

Ввод описания для политики случайного определения.

**Синтаксис**

**set traffic-policy random-detect** *имя_политики* **description** *описание*

**delete traffic-policy random-detect** *имя_политики* **description**

**show traffic-policy random-detect** *имя_политики* **description**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        random-detect текст {
            description описание
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики случайного определения.

*описание*

Обязательный. 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.

## 26.9.20. traffic-policy random-detect <имя_политики> precedence <предпочтительность>

Установка параметров отбрасывания пакетов на основе предпочтительности для

политики случайного определения.

**Синтаксис**

**set traffic-policy random-detect** *имя_политики* **precedence** *предпочтительность* [**average-packet** *байты* | **mark-probability** *вероятность* | **maximum-threshold** *максимум* | **minimum-threshold** *минимум* | **queue-limit** *число_пакетов*]

**delete traffic-policy random-detect** *имя_политики* **precedence** *предпочтительность* [**average-packet** | **mark-probability** | **maximum-threshold** | **minimum-threshold** | **queue-limit**]

**show traffic-policy random-detect** *имя_политики* **precedence** *предпочтительность* [**average-packet** | **mark-probability** | **maximum-threshold** | **minimum-threshold** | **queue-limit**]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        random-detect текст {
            precedence 0-7 {
                average-packet 16-10240
                mark-probability целоебеззнака32разр
                maximum-threshold 0-4096
                minimum-threshold 0-4096
                queue-limit целоебеззнака32разр
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики случайного определения.

*байты*

Средний размер пакета в байтах. Значение по умолчанию равно 1024.

Значение должно лежать в интервале от 16 до 10240.

*предпочтительность*

Предпочтительность IP (первые три бита поля TOS) пакета.

*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 лежать 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 лежать 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**

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.*

Эта команда используется для указания параметров отбрасывания пакетов в политике случайного определения.

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.

## 26.9.21. traffic-policy rate-control <имя_политики>

Определение политики QoS с ограничением скорости.

**Синтаксис**

**set traffic-policy rate-control** *имя_политики*

**delete traffic-policy rate-control** *имя_политики*

**show traffic-policy rate-control** *имя_политики*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        rate-control текст {
        }
}
```

**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 Altell NEO 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.

## 26.9.22. traffic-policy rate-control <имя_политики> bandwidth

Указание ограничения пропускной способности для всего суммарного трафика, ограничиваемого данной политикой.

**Синтаксис**

**set traffic-policy rate-control** *имя_политики* **bandwidth** [*скорость* | *скорость_в_единицах*]

**delete traffic-policy rate-control** *имя_политики* **bandwidth**

**show traffic-policy rate-control** *имя_политики* **bandwidth**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        rate-control текст {
            bandwidth текст
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения скорости.

*скорость*

Пропускная способность, указанная в килобитах в секунду.

*скорость_в_единицах*

Пропускная способность, указанная в виде числа и единицы измерения (например, 10mbit). Поддерживаются следующие единицы измерения:

**kbit**: килобитов в секунду.

**mbit**: мегабитов в секунду.

**gbit**: гигабитов в секунду.

**kbps**: килобайтов в секунду.

**mbps**: мегабайтов в секунду.

**gbps**: гигабайтов 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. В Altell NEO удаление параметра **bandwidth** для политики ограничения скорости без удаления всей политики невозможно, попытка фиксации настройки после выдачи формы **delete** данной команды завершается сбоем.

Форма **show** этой команды используется для отображения настройки пропускной способности, выделенной политике.

## 26.9.23. traffic-policy rate-control <имя_политики> burst

Установка размера непрерывной серии пакетов для политики QoS с ограничением скорости.

**Синтаксис**

**set traffic-policy rate-control** *имя_политики* **burst** [*число* | *число_в_единицах*]

**delete traffic-policy rate-control** *имя_политики* **burst**

**show traffic-policy rate-control** *имя_политики* **burst**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        rate-control текст {
            burst текст
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения скорости.

*число*

Размер непрерывной серии, указанный в байтах.

*число_в_единицах*

Размер непрерывной серии, указанный в виде числа и единицы измерения (например, 10mb). Поддерживаются следующие единицы измерения:

**kb**: килобайты.

**mb**: мегабайты.

**gb**: гигабайты.

**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.

## 26.9.24. traffic-policy rate-control <имя_политики> description <описание>

Ввод описания для политики ограничения скорости.

**Синтаксис**

**set traffic-policy rate-control** *имя_политики* **description** *описание*

**delete traffic-policy rate-control** *имя_политики* **description**

**show traffic-policy rate-control** *имя_политики* **description**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        rate-control текст {
            description описание
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения скорости.

*описание*

Обязательный. 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.

## 26.9.25. traffic-policy rate-control <имя_политики> latency

Установка ограничения на размер очереди на основе задержки для политики QoS с ограничением скорости.

**Синтаксис**

**set traffic-policy rate-control** *имя_политики* **latency** [*число* | *число_в_единицах*]

**delete traffic-policy rate-control** *имя_политики* **latency**

**show traffic-policy rate-control** *имя_политики* **latency**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        rate-control текст {
            latency текст
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения скорости.

*число*

Задержка, указанная в миллисекундах.

*число_в_единицах*

Задержка, указанная в виде числа и единицы измерения (например, 10ms). Поддерживаются следующие единицы измерения:

**secs**: секунды.

**ms**: миллисекунды.

**us**: микросекунды.

**Значение по умолчанию**

Задержка по умолчанию равна 50 миллисекундам.

**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.

## 26.9.26. traffic-policy round-robin <имя_политики>

Определение политики QoS с циклическим перебором.

**Синтаксис**

**set traffic-policy round-robin** *имя_политики*

**delete traffic-policy round-robin** *имя_политики*

**show traffic-policy round-robin** *имя_политики*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        round-robin текст {
        }
}
```

**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 создании политики QoS с циклическим перебором. До фиксации настройки данной политики

циклического перебора необходимо определить класс по умолчанию при помощи команды **set traffic-policy <имя_политики> default**, в противном случае фиксация завершится сбоем.

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.

## 26.9.27. traffic-policy round-robin <имя_политики> class <класс>

Определение класса трафика для политики QoS с циклическим перебором.

**Синтаксис**

**set traffic-policy round-robin** *имя_политики* **class** *класс*

**delete traffic-policy round-robin** *имя_политики* **class** *класс*

**show traffic-policy round-robin** *имя_политики* **class** *класс*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        round-robin текст {
            class 2-4095 {
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики циклического перебора.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 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.

## 26.9.28. traffic-policy round-robin <имя_политики> class <класс> description <описание>

Ввод описания для класса трафика.

**Синтаксис**

**set traffic-policy round-robin** *имя_политики* **class** *класс* **description** *описание*

**delete traffic-policy round-robin** *имя_политики* **class** *класс* **description**

**show traffic-policy round-robin** *имя_политики* **class** *класс* **description**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        round-robin текст {
            class 2-4095 {
                description описание
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики циклического перебора.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*описание*

Обязательный. 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.

## 26.9.29. traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия>

Определение правила для проверки соответствия классов трафика.

**Синтаксис**

**set traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия*

**delete traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия*

**show traffic-policy round-robin** *имя_политики* **class** класс **match** *имя_соответствия*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        round-robin текст {
            class 2-4095 {
```

```
                    match текст {
                    }
                }
            }
        }
```

**Параметры**

*имя_политики*

Обязательный. Имя политики циклического перебора.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. 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.

## 26.9.30. traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> description <описание>

Ввод описания для правила соответствия.

**Синтаксис**

**set traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **description** *описание*

**delete traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **description**

**show traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **description**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        round-robin текст {
            class 2-4095 {
                match текст {
                    description описание
                }
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики циклического перебора.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*описание*

Обязательный. 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.

### 26.9.31. traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> ether destination <mac-адрес>

Указание критерия соответствия на основе MAC-адреса получателя.

#### Синтаксис

**set traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether destination** *mac-адрес*

**delete traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether destination**

**show traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether destination**

#### Режим интерфейса

Режим настройки.

#### Ветвь конфигурации

```
traffic-policy {
          round-robin текст {
               class 2-4095 {
                    match текст {
                         ether {
     destination mac-адрес
                         }
                    }
               }
          }
}
```

#### Параметры

*имя_политики*

Обязательный. Имя политики циклического перебора.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*mac-адрес*

MAC-адрес получателя, на соответствие которому выполняется проверка. Формат адреса - 6 8-битовых шестнадцатеричных чисел, разделенных двоеточиями, например, 00:0a:59:9a:f2:ba.

**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.

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.

## 26.9.32. traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> ether protocol <число>

Указание критерия соответствия на основе типа пакета Ethernet.

**Синтаксис**

**set traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether protocol** *число*

**delete traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether protocol**

**show traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether protocol**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
```

```
                round-robin текст {
                     class 2-4095 {
                          match текст {
                               ether {

        protocol число
                               }
                          }
                     }
                }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики циклического перебора.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*число*

Тип пакета Ethernet (номер протокола), соответствие которому проверяется. Значение должно лежать в диапазоне от 0 до 65535.

**Значение по умолчанию**

Если параметр не установлен, пакеты не проверяются на соответствие типа пакета Ethernet.

**Указания по использованию**

Это команда используется для определения условия соответствия по типу пакета Ethernet в классе трафика.

Форма **set** этой команды используется для указания типа пакета, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления типа пакета в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки типа пакета в качестве проверяемого условия соответствия.

## 26.9.33. traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> ether source <mac-адрес>

Указание критерия соответствия на основе MAC-адреса отправителя.

**Синтаксис**

**set traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether source** *mac-адрес*

**delete traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether source**

**show traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether source**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
          round-robin текст {
               class 2-4095 {
                    match текст {
                         ether {

     source mac-адрес
                         }
                    }
               }
          }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики циклического перебора.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне

от 2 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*mac-адрес*

MAC-адрес отправителя, на соответствие которому выполняется проверка. Формат адреса - 6 8-битовых шестнадцатеричных чисел, разделенных двоеточиями, например, 00:0a:59:9a:f2:ba.

**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.

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.

## 26.9.34. traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> interface <интерфейс>

Указание критерия соответствия на основе интерфейса для входящих пакетов.

**Синтаксис**

**set traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **interface** *интерфейс*

**delete traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **interface**

**show traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **interface**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        round-robin текст {
            class 2-4095 {
                match текст {
                    interface текст
                }
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики циклического перебора.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*интерфейс*

Имя интерфейса Ethernet, на соответствие которому выполняется проверка. С указанным значением будет сравниваться входной интерфейс для входящего трафика.

**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).

Следует заметить, что нельзя проверять на соответствие “ip” и “vif” (или “interface”) одновременно внутри одной и той же настройки циклического

перебора.

Форма **set** этой команды используется для указания интерфейса, соответствие которому должно проверяться во входящих пакетах.

Форма **delete** этой команды используется для удаления соответствия по интерфейсу.

Форма **show** этой команды используется для отображения настройки соответствия по интерфейсу.

## 26.9.35. traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> ip destination

Указание критерия соответствия на основе сведений IP о получателе.

**Синтаксис**

**set traffic-policy round-robin** имя_политики **class** класс **match** имя_соответствия **ip destination** {**address** подсеть_ipv4 | **port** порт}

**delete traffic-policy round-robin** имя_политики **class** класс **match** имя_соответствия **ip destination** [**address** | **port**]

**show traffic-policy round-robin** имя_политики **class** класс **match** имя_соответствия **ip destination**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        round-robin текст {
            class 2-4095 {
                match текст {
                    ip {
destination {
        address подсеть_ipv4
        port текст
```

```
        }
                                    }
                                }
                            }
                        }
                    }
                }
```

**Параметры**

*имя_политики*

Обязательный. Имя политики циклического перебора.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*подсеть_ipv4*

Адрес подсети IP 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 номера порта должно лежать в диапазоне от 0 до 65535.

**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.

Следует заметить, что нельзя проверять на соответствие “ip” и “vif” (или

"interface"), а также "ip" и "ipv6" одновременно внутри одной и той же настройки циклического перебора.

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.

## 26.9.36. traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> ip dscp <значение>

Указание критерия соответствия на основе значения поля DSCP.

**Синтаксис**

**set traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip dscp** *значение*

**delete traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip dscp**

**show traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip dscp**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        round-robin текст {
            class 2-4095 {
                match текст {
                    ip {
dscp текст
                    }
                }
            }
        }
```

}

**Параметры**

*имя_политики*

Обязательный. Имя политики циклического перебора.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. 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. Значение DSCP может быть указано в форме десятичного числа (например, 12), шестнадцатеричного числа (например, 0x1D) или в форме стандартного имени из файла /etc/iproute2/rt_dsfield (например, **lowdelay**).

**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.

Следует заметить, что нельзя проверять на соответствие “ip” и “vif” (или “interface”), а также “ip” и “ipv6” одновременно внутри одной и той же настройки циклического перебора.

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.

## 26.9.37. traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> ip protocol <протокол>

Указание критерия соответствия на основе протокола IP.

**Синтаксис**

**set traffic-policy round-robin** имя_политики **class** класс **match** имя_соответствия **ip protocol** протокол

**delete traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip protocol**

**show traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip protocol**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
          round-robin текст {
               class 2-4095 {
                    match текст {
                         ip {

     protocol текст
                         }
                    }
               }
          }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики циклического перебора.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне

от 2 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

протокол

Имя протокола (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.

Следует заметить, что нельзя проверять на соответствие “ip” и “vif” (или “interface”), а также “ip” и “ipv6” одновременно внутри одной и той же настройки циклического перебора.

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.

## 26.9.38. traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> ip source

Указание критерия соответствия на основе сведений IP об отправителе.

**Синтаксис**

```
set traffic-policy round-robin имя_политики class класс
match имя_соответствия ip source {address подсеть_ipv4 |
port порт}

delete traffic-policy round-robin имя_политики class
класс match имя_соответствия ip source {address | port}

show traffic-policy round-robin имя_политики class класс
match имя_соответствия ip source
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        round-robin текст {
            class 2-4095 {
                match текст {
                    ip {
    source {
        address подсеть_ipv4
        port текст
    }
                    }
                }
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики циклического перебора.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*подсеть_ipv4*

Адрес подсети IP отправителя, соответствие которому проверяется в данном правиле.

*порт*

Порт отправителя, соответствие которому проверяется в данном правиле. Порт может быть указан в форме имени строчными буквами (например, **ssh**) или в форме числа. Значение номера порта должно лежать в диапазоне от 0 до 65535.

**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.

Следует заметить, что нельзя проверять на соответствие “ip” и “vif” (или “interface”), а также “ip” и “ipv6” одновременно внутри одной и той же настройки циклического перебора.

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.

## 26.9.39. traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> ipv6 destination

Указание критерия соответствия на основе сведений IPv6 о получателе.

**Синтаксис**

```
set traffic-policy round-robin имя_политики class класс
match имя_соответствия ipv6 destination {address
подсеть_ipv6 | port порт}

delete traffic-policy round-robin имя_политики class
класс match имя_соответствия ipv6 destination [address |
port]

show traffic-policy round-robin имя_политики class класс
match имя_соответствия ipv6 destination
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        round-robin текст {
            class 2-4095 {
                match текст {
                    ipv6 {
    destination {
        address подсеть_ipv6
        port текст
    }
                    }
                }
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики циклического перебора.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*подсеть_ipv6*

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 номера порта должно лежать в диапазоне от 0 до 65535.

**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.

Следует заметить, что нельзя проверять на соответствие “ipv6” и “vif” (или “interface”), а также “ip” и “ipv6” одновременно внутри одной и той же настройки циклического перебора.

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.

## 26.9.40. traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> ipv6 dscp <значение>

Указание критерия соответствия на основе значения поля DSCP.

**Синтаксис**

```
set traffic-policy round-robin имя_политики class класс
match имя_соответствия ipv6 dscp значение

delete traffic-policy round-robin имя_политики class
класс match имя_соответствия ipv6 dscp

show traffic-policy round-robin имя_политики class класс
match имя_соответствия ipv6 dscp
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        round-robin текст {
            class 2-4095 {
                match текст {
                    ipv6 {
    dscp текст
                    }
                }
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики циклического перебора.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. 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. Значение DSCP может быть указано в форме десятичного числа (например, 12), шестнадцатеричного числа (например, 0x1D) или в форме стандартного имени из файла /etc/iproute2/rt_dsfield (например, **lowdelay**).

**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.

Следует заметить, что нельзя проверять на соответствие “ipv6” и “vif” (или “interface”), а также “ip” и “ipv6” одновременно внутри одной и той же настройки циклического перебора.

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.

## 26.9.41. traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> ipv6 protocol <протокол>

Указание критерия соответствия на основе протокола IPv6.

**Синтаксис**

**set traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 protocol** *протокол*

**delete traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 protocol**

**show traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 protocol**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        round-robin текст {
            class 2-4095 {
```

```
                    match текст {
                        ipv6 {

    protocol текст
                        }
                    }
                }
            }
        }
```

**Параметры**

*имя_политики*

Обязательный. Имя политики циклического перебора.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*протокол*

Имя протокола (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.

Следует заметить, что нельзя проверять на соответствие “ipv6” и “vif” (или “interface”), а также “ip” и “ipv6” одновременно внутри одной и той же настройки циклического перебора.

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.

## 26.9.42. traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> ipv6 source

Указание критерия соответствия на основе сведений IPv6 об отправителе.

**Синтаксис**

**set traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 source** {**address** *подсеть_ipv6* | **port** *порт*}

**delete traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 source** {**address** | **port**}

**show traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 source**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        round-robin текст {
            class 2-4095 {
                match текст {
                    ipv6 {
source {
    address подсеть_ipv6
    port текст
}
                    }
                }
            }
```

```
            }
        }
```

**Параметры**

*имя_политики*

Обязательный. Имя политики циклического перебора.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 3 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*подсеть_ipv6*

Адрес подсети IPv6 отправителя, соответствие которому проверяется в данном правиле.

*порт*

Порт отправителя, соответствие которому проверяется в данном правиле. Порт может быть указан в форме имени строчными буквами (например, **ssh**) или в форме числа. Значение номера порта должно лежать в диапазоне от 0 до 65535. Указание порта возможно только для протоколов, поддерживающих порты (TCP/UDP/SCTP).

**Значение по умолчанию**

Если параметр не установлен, пакеты не проверяются на соответствие сведениям IPv6 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.

Следует заметить, что нельзя проверять на соответствие “ipv6” и “vif” (или “interface”), а также “ip” и “ipv6” одновременно внутри одной и той же настройки циклического перебора.

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.

## 26.9.43. traffic-policy round-robin <имя_политики> class <класс> match <имя_соответствия> vif <идентификатор_vlan>

Указание критерия соответствия на основе идентификатора VLAN.

**Синтаксис**

**set traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **vif** *идентификатор_vlan*

**delete traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **vif**

**show traffic-policy round-robin** *имя_политики* **class** *класс* **match** *имя_соответствия* **vif**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        round-robin текст {
            class 2-4095 {
                match текст {
                    vif 1-4096
                }
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики циклического перебора.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*идентификатор_vlan*

Идентификатор VLAN, соответствие которому проверяется. Значение должно лежать в диапазоне от 1 до 4096.

**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.

Следует заметить, что нельзя проверять на соответствие “ip” и “vif” (или “interface”) одновременно внутри одной и той же настройки циклического перебора.

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.

## 26.9.44. traffic-policy round-robin <имя_политики> class <класс> quantum <число_пакетов>

Указание числа пакетов, которые могут быть отправлены за квант планирования.

**Синтаксис**

**set traffic-policy round-robin** *имя_политики* **class** *класс* **quantum** *число_пакетов*

**delete traffic-policy round-robin** *имя_политики* **class** *класс* **quantum**

**show traffic-policy round-robin** *имя_политики* **class** *класс* **quantum**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        round-robin текст {
            class 2-4095
                quantum целоебеззнака32разр
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики циклического перебора.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 1 до 4095.

*число_пакетов*

Необязательный. Число пакетов, которые могут быть отправлены за квант планирования.

**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.

## 26.9.45. traffic-policy round-robin <имя_политики> class <класс> queue-limit <ограничение>

Указание максимального размера очереди для класса трафика.

**Синтаксис**

**set traffic-policy round-robin** *имя_политики* **class** *класс* **queue-limit** *ограничение*

**delete traffic-policy round-robin** *имя_политики* **class** *класс* **queue-limit**

**show traffic-policy round-robin** *имя_политики* **class** *класс* **queue-limit**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        round-robin текст {
            class 2-4095 {
                queue-limit 2-4294967295
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики циклического перебора.

*класс*

Обязательный. Идентификатор класса.

*ограничение*

Максимальный размер очереди в пакетах. Значение должно лежать в диапазоне от 2 до 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.

### 26.9.46. traffic-policy round-robin <имя_политики> class <класс> queue-type <тип>

Указание типа работы с очередью, используемого для класса трафика.

**Синтаксис**

**set traffic-policy round-robin** *имя_политики* **class** *класс* **queue-type** *тип*

**delete traffic-policy round-robin** *имя_политики* **class** *класс* **queue-type**

**show traffic-policy round-robin** *имя_политики* **class** *класс* **queue-type**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
          round-robin текст {
               class 2-4095 {
                    queue-type [fair-queue|drop-tail|
priority]
               }
          }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики циклического перебора.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*тип*

Используемый метод работы с очередями. Поддерживаются следующие

значения:

**fair-queue**: используется очередь SFQ.

**drop-tail**: используется очередь FIFO.

**priority**: приоритет в очереди устанавливается по значениям поля DSCP в байте ToS заголовка IP.

**Значение по умолчанию**

По умолчанию используется тип **drop-tail**.

**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.

## 26.9.47. traffic-policy round-robin <имя_политики> default

Определение политики QoS по умолчанию с циклическим перебором.

**Синтаксис**

**set traffic-policy round-robin** *имя_политики* **default**

**delete traffic-policy round-robin** *имя_политики* **default**

**show traffic-policy round-robin** *имя_политики* **default**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        round-robin текст {
            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. В Altell NEO удаление узла конфигурации класса по умолчанию для политики циклического перебора без удаления всей политики невозможно, попытка фиксации настройки после выдачи формы **delete** данной команды завершается сбоем.

Форма **show** этой команды используется для отображения узла конфигурации класса по умолчанию.

## 26.9.48. traffic-policy round-robin <имя_политики> default quantum <число_пакетов>

Указание числа пакетов, которые могут быть отправлены за квант планирования.

**Синтаксис**

**set traffic-policy round-robin** *имя_политики* **default quantum** *число_пакетов*

**delete traffic-policy round-robin** *имя_политики* **default quantum**

**show traffic-policy round-robin** *имя_политики* **default quantum**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        round-robin текст {
```

```
                    default
                        quantum целоебеззнака32разр
                    }
                }
            }
```

**Параметры**

*имя_политики*

Обязательный. Имя политики циклического перебора.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 1 до 4095.

*число_пакетов*

Необязательный. Число пакетов, которые могут быть отправлены за квант планирования.

**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.

## 26.9.49. traffic-policy round-robin <имя_политики> default queue-limit <ограничение>

Указание максимального размера очереди для класса трафика по умолчанию.

**Синтаксис**

**set traffic-policy round-robin** *имя_политики* **default queue-limit** *ограничение*

**delete traffic-policy round-robin** *имя_политики* **default queue-limit**

**show traffic-policy round-robin** *имя_политики* **default queue-limit**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        round-robin текст {
            default {
                queue-limit целоебеззнака32разр
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики циклического перебора.

*ограничение*

Максимальный размер очереди в пакетах. Значение должно лежать в диапазоне от 1 до 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.

## 26.9.50. traffic-policy round-robin <имя_политики> default queue-type <тип>

Указание типа работы с очередью, используемого для класса трафика по умолчанию.

**Синтаксис**

**set traffic-policy round-robin** *имя_политики* **default queue-type** *тип*

**delete traffic-policy round-robin** *имя_политики* **default queue-type**

**show traffic-policy round-robin** *имя_политики* **default queue-type**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        round-robin текст {
            default {
                queue-type [fair-queue|drop-tail|
priority]
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики циклического перебора.

*тип*

Используемый метод работы с очередями. Поддерживаются следующие значения:

**fair-queue**: используется очередь SFQ.

**drop-tail**: используется очередь FIFO.

**priority**: приоритет в очереди устанавливается по значениям поля DSCP в байте ToS заголовка IP.

**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.

## 26.9.51. traffic-policy round-robin <имя_политики> description <описание>

Ввод описания для политики QoS с циклическим перебором.

**Синтаксис**

**set traffic-policy round-robin** *имя_политики* **description** *описание*

**delete traffic-policy round-robin** *имя_политики* **description**

**show traffic-policy round-robin** *имя_политики* **description**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        round-robin текст {
            description описание
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики циклического перебора.

*описание*

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.

## 26.9.52. traffic-policy limiter <имя_политики>

Определение политики QoS с ограничением трафика.

**Синтаксис**

**set traffic-policy limiter** *имя_политики*

**delete traffic-policy limiter** *имя_политики*

**show traffic-policy limiter** *имя_политики*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        limiter текст {
        }
}
```

**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 исходящему 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 никаком 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.

## 26.9.53. traffic-policy limiter <имя_политики> class <класс>

Определение класса трафика для политики QoS с ограничением трафика.

**Синтаксис**

**set traffic-policy limiter** *имя_политики* **class** *класс*

**delete traffic-policy limiter** *имя_политики* **class** *класс*

**show traffic-policy limiter** *имя_политики* **class** *класс*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        limiter текст {
            class 1-4095 {
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения трафика.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне

от 1 до 4095.

**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.

## 26.9.54. traffic-policy limiter <имя_политики> class <класс> bandwidth

Указание ограничения пропускной способности для класса трафика.

**Синтаксис**

**set traffic-policy limiter** *имя_политики* **class** *класс* **bandwidth** [*скорость* | *скорость_в_единицах*]

**delete traffic-policy limiter** *имя_политики* **class** *класс* **bandwidth**

**show traffic-policy limiter** *имя_политики* **class** *класс* **bandwidth**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        limiter текст {
            class 1-4095 {
                bandwidth текст
```

```
                    }
                }
            }
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения трафика.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 1 до 4095.

*скорость*

Пропускная способность, указанная в килобитах в секунду.

*скорость_в_единицах*

Пропускная способность, указанная в виде числа и единицы измерения (например, 10mbit). Поддерживаются следующие единицы измерения:

**kbit**: килобитов в секунду.

**mbit**: мегабитов в секунду.

**gbit**: гигабитов в секунду.

**kbps**: килобайтов в секунду.

**mbps**: мегабайтов в секунду.

**gbps**: гигабайтов 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.

## 26.9.55. traffic-policy limiter <имя_политики> class <класс> burst

Установка размера непрерывной серии пакетов для класса трафика.

**Синтаксис**

**set traffic-policy limiter** *имя_политики* **class** *класс* **burst** [*число* | *число_в_единицах*]

**delete traffic-policy limiter** *имя_политики* **class** *класс* **burst**

**show traffic-policy limiter** *имя_политики* **class** *класс* **burst**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        limiter текст {
            class 1-4095 {
                burst текст
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения трафика.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 1 до 4095.

*число*

Размер непрерывной серии, указанный в байтах.

*число_в_единицах*

Размер непрерывной серии, указанный в виде числа и единицы измерения (например, 10mb). Поддерживаются следующие единицы измерения:

**kb**: килобайты.

**mb**: мегабайты.

**gb**: гигабайты.

**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.

## 26.9.56. traffic-policy limiter <имя_политики> class <класс> description <описание>

Ввод описания для класса трафика.

**Синтаксис**

**set traffic-policy limiter** *имя_политики* **class** *класс* **description** *описание*

**delete traffic-policy limiter** *имя_политики* **class** *класс* **description**

**show traffic-policy limiter** *имя_политики* **class** *класс* **description**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        limiter текст {
            class 1-4095 {
                description описание
            }
        }
```

```
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения трафика.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 1 до 4095.

*описание*

Обязательный. 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.

## 26.9.57. traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия>

Определение правила для проверки соответствия классов трафика.

**Синтаксис**

**set traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия*

**delete traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия*

**show traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        limiter текст {
```

```
                    class 1-4095 {
                        match текст {
                        }
                    }
                }
            }
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения трафика.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 1 до 4095.

*имя_соответствия*

Обязательный. 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. Следует заметить, что для изменения имени существующего правила соответствия в классе трафика нельзя использовать команду set. Для изменения правила следует удалить его и создать заново.

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.

## 26.9.58. traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> description <описание>

Ввод описания для правила соответствия.

**Синтаксис**

**set traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **description** *описание*

**delete traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **description**

**show traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **description**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        limiter текст {
            class 1-4095 {
                match текст {
                    description описание
                }
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения трафика.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 1 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*описание*

Обязательный. 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.

## 26.9.59. traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> ether destination <mac-адрес>

Указание критерия соответствия на основе MAC-адреса получателя.

**Синтаксис**

**set traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether destinatio**n *mac-адрес*

**delete traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether destination**

**show traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether destination**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
          limiter текст {
               class 1-4095 {
                    match текст {
                         ether {

     destination mac-адрес
                              }
                         }
                    }
               }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения трафика.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 1 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*mac-адрес*

MAC-адрес получателя, на соответствие которому выполняется проверка. Формат адреса - 6 8-битовых шестнадцатеричных чисел, разделенных двоеточиями, например, 00:0a:59:9a:f2:ba.

**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.

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.

## 26.9.60. traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> ether protocol <число>

Указание критерия соответствия на основе типа пакета Ethernet.

**Синтаксис**

**set traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether protocol** *число*

**delete traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether protocol**

**show traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether protocol**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
          limiter текст {
               class 1-4095 {
                    match текст {
                         ether {
    protocol число
                         }
                    }
               }
          }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения трафика.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 1 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*число*

Тип пакета Ethernet (номер протокола), соответствие которому проверяется. Значение должно лежать в диапазоне от 0 до 65535.

**Значение по умолчанию**

Если параметр не установлен, пакеты не проверяются на соответствие типа пакета Ethernet.

**Указания по использованию**

Это команда используется для определения условия соответствия по типу пакета Ethernet в классе трафика.

Форма **set** этой команды используется для указания типа пакета, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления типа пакета в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки типа пакета в качестве проверяемого условия соответствия.

### 26.9.61. traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> ether source <mac-адрес>

Указание критерия соответствия на основе MAC-адреса отправителя.

#### Синтаксис

**set traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether source** *mac-адрес*

**delete traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether source**

**show traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether source**

#### Режим интерфейса

Режим настройки.

#### Ветвь конфигурации

```
traffic-policy {
        limiter текст {
            class 1-4095 {
                match текст {
                    ether {
    source mac-адрес
                    }
                }
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения трафика.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 1 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*mac-адрес*

MAC-адрес отправителя, на соответствие которому выполняется проверка. Формат адреса - 6 8-битовых шестнадцатеричных чисел, разделенных двоеточиями, например, 00:0a:59:9a:f2:ba.

**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.

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.

## 26.9.62. traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> ip destination

Указание критерия соответствия на основе сведений IP о получателе.

**Синтаксис**

**set traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip destination** {**address** *подсеть_ipv4* | **port** *порт*}

**delete traffic-policy limiter** *имя_политики* **class** *класс*

**match** *имя_соответствия* **ip destination** [**address** | **port**]

**show traffic-policy limiter** *имя_политики* **class** *класс*
**match** *имя_соответствия* **ip destination**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
          текст {
               class 1-4095 {
                    match текст {
                         ip {

     destination {

          address подсеть_ipv4

          port текст

     }
                         }
                    }
               }
          }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения трафика.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 1 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*подсеть_ipv4*

Адрес подсети IP 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 номера порта должно лежать в диапазоне от 0 до 65535.

**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.

Следует заметить, что 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.

## 26.9.63. traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> ip dscp <значение>

Указание критерия соответствия на основе значения поля DSCP.

**Синтаксис**

**set traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip dscp** *значение*

**delete traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip dscp**

**show traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip dscp**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        limiter текст {
            class 1-4095 {
                match текст {
                    ip {
                        dscp текст
                    }
                }
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения трафика.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 1 до 4095.

*имя_соответствия*

Обязательный. 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. Значение DSCP может быть указано в форме десятичного числа (например, 12), шестнадцатеричного числа (например, 0x1D) или в форме стандартного имени из файла /etc/iproute2/rt_dsfield (например, **lowdelay**).

**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.

Следует заметить, что 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.

## 26.9.64. traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> ip protocol <протокол>

Указание критерия соответствия на основе протокола IP.

**Синтаксис**

**set traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip protocol** *протокол*

**delete traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip protocol**

**show traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip protocol**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
```

```
                limiter текст {
                     class 1-4095 {
                          match текст {
                               ip {

        protocol текст
                               }
                          }
                     }
                }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения трафика.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 1 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*протокол*

Имя протокола (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.

Следует заметить, что 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.

## 26.9.65. traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> ip source

Указание критерия соответствия на основе сведений IP об отправителе.

**Синтаксис**

**set traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip source** {**address** *подсеть_ipv4* | **port** *порт*}

**delete traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip source** {**address** | **port**}

**show traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip source**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        limiter текст {
            class 1-4095 {
                match текст {
                    ip {
source {
    address подсеть_ipv4
    port текст
}
                    }
```

```
                    }
                }
            }
        }
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения трафика.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 1 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*подсеть_ipv4*

Адрес подсети IP отправителя, соответствие которому проверяется в данном правиле.

*порт*

Порт отправителя, соответствие которому проверяется в данном правиле. Порт может быть указан в форме имени строчными буквами (например, **ssh**) или в форме числа. Значение номера порта должно лежать в диапазоне от 0 до 65535.

**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.

Следует заметить, что 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.

## 26.9.66. traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> ipv6 destination

Указание критерия соответствия на основе сведений IPv6 о получателе.

**Синтаксис**

**set traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 destination** {**address** *подсеть_ipv6* | **port** *порт*}

**delete traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **iv6 destination** [**address** | **port**]

**show traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 destination**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        limiter текст {
            class 1-4095 {
                match текст {
                    ipv6 {
    destination {
        address подсеть_ipv6
        port текст
    }
                    }
```

```
                    }
                }
            }
        }
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения трафика.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 1 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*подсеть_ipv6*

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 номера порта должно лежать в диапазоне от 0 до 65535.

**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.

Следует заметить, что нельзя проверять на соответствие “ipv6” 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.

## 26.9.67. traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> ipv6 dscp <значение>

Указание критерия соответствия на основе значения поля DSCP.

**Синтаксис**

**set traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 dscp** *значение*

**delete traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 dscp**

**show traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 dscp**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
          limiter текст {
               class 1-4095 {
                    match текст {
                         ipv6 {

    dscp текст
                         }
                    }
               }
          }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения трафика.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 1 до 4095.

*имя_соответствия*

Обязательный. 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. Значение DSCP может быть указано в форме десятичного числа (например, 12), шестнадцатеричного числа (например, 0x1D) или в форме стандартного имени из файла /etc/iproute2/rt_dsfield (например, **lowdelay**).

**Значение по умолчанию**

Если параметр не установлен, пакеты не проверяются на соответствие по полю DSCP.

**Указания по использованию**

Подробное описание ключевых слов и аргументов приведено в таблице в Приложении А.

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.

Следует заметить, что нельзя проверять на соответствие “ipv6” 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.

### 26.9.68. traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> ipv6 protocol <протокол>

Указание критерия соответствия на основе протокола IPv6.

**Синтаксис**

**set traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 protocol** *протокол*

**delete traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 protocol**

**show traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 protocol**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
          limiter текст {
               class 1-4095 {
                    match текст {
                         ipv6 {

     protocol текст
                         }
                    }
               }
          }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения трафика.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 1 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*протокол*

Имя протокола (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.

Следует заметить, что нельзя проверять на соответствие “ipv6” 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.

## 26.9.69. traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> ipv6 source

Указание критерия соответствия на основе сведений IPv6 об отправителе.

**Синтаксис**

**set traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 source** {**address** *подсеть_ipv6* | **port** *порт*}

**delete traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 source** {**address** | **port**}

**show traffic-policy limiter** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 source**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        limiter текст {
            class 1-4095 {
                match текст {
                    ipv6 {

    source {

        address подсеть_ipv6

        port текст

    }
                    }
                }
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения трафика.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 1 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*подсеть_ipv6*

Адрес подсети IPv6 отправителя, соответствие которому проверяется в данном правиле.

*порт*

Порт отправителя, соответствие которому проверяется в данном правиле.

Порт может быть указан в форме имени строчными буквами (например ssh) или в форме числа. Значение номера порта должно лежать в диапазоне от 0 до 65535.

**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.

Следует заметить, что нельзя проверять на соответствие “ipv6” 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.

## 26.9.70. traffic-policy limiter <имя_политики> class <класс> match <имя_соответствия> vif <идентификатор_vlan>

Указание критерия соответствия на основе идентификатора VLAN.

**Синтаксис**

```
set traffic-policy limiter имя_политики class класс match
имя_соответствия vif идентификатор_vlan

delete traffic-policy limiter имя_политики class класс
match имя_соответствия vif

show traffic-policy limiter имя_политики class класс
match имя_соответствия vif
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        limiter текст {
            class 1-4095 {
                match текст {
                    vif 1-4096
                }
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения трафика.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 1 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*идентификатор_vlan*

Идентификатор VLAN, соответствие которому проверяется. Значение должно лежать в диапазоне от 1 до 4096.

**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.

Следует заметить, что 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.

## 26.9.71. traffic-policy limiter <имя_политики> class <класс> priority <приоритет>

Указание порядка обработки правил соответствия.

**Синтаксис**

**set traffic-policy limiter** *имя_политики* **class** *класс* **priority** *приоритет*

**delete traffic-policy limiter** *имя_политики* **class** *класс* **priority**

**show traffic-policy limiter** *имя_политики* **class** *класс* **priority**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        limiter текст {
            class 1-4095 {
                priority целоебеззнака32разр
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения трафика.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 1 до 4095.

*приоритет*

Приоритет проверки правил соответствия. Значение должно лежать в

диапазоне от 0 до 20, причем чем больше значение, тем ниже приоритет. Значение по умолчанию равно 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.

## 26.9.72. traffic-policy limiter <имя_политики> description <описание>

Ввод описания для политики QoS с ограничением трафика.

**Синтаксис**

**set traffic-policy limiter** *имя_политики* **description** *описание*

**delete traffic-policy limiter** *имя_политики* **description**

**show traffic-policy limiter** *имя_политики* **description**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        limiter текст {
            description описание
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики ограничения трафика.

*описание*

Описание для данной политики ограничения трафика.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для записи 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.

## 26.9.73. traffic-policy shaper <имя_политики>

Определение политики QoS с управлением загрузкой канала.

**Синтаксис**

**set traffic-policy shaper** *имя_политики*

**delete traffic-policy shaper** *имя_политики*

**show traffic-policy -shaper** *имя_политики*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
        }
}
```

**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 Altell NEO 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.

## 26.9.74. traffic-policy shaper <имя_политики> bandwidth

Указание пропускной способности, доступной для всего суммарного трафика, ограничиваемого данной политикой.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **bandwidth** [**auto** | *скорость* | *скорость_в_единицах*]

**delete traffic-policy shaper** *имя_политики* **bandwidth**

**show traffic-policy shaper** *имя_политики* **bandwidth**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            bandwidth текст
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

**auto**

Пропускная способность автоматически основывается на скорости интерфейса.

*скорость*

Пропускная способность, указанная в килобитах в секунду.

*скорость_в_единицах*

Пропускная способность, указанная в виде числа и единицы измерения (например, 10mbit). Поддерживаются следующие единицы измерения:

**kbit**: килобитов в секунду.

**mbit**: мегабитов в секунду.

**gbit**: гигабитов в секунду.

**kbps**: килобайтов в секунду.

**mbps**: мегабайтов в секунду.

**gbps**: гигабайтов в секунду.

**Значение по умолчанию**

По умолчанию используется значение **auto**.

**Указания по использованию**

Эта команда используется для установки ограничений пропускной способности в политике QoS с управлением загрузкой канала. Данный параметр описывает максимальную пропускную способность, доступную всем классам.

Форма **set** этой команды используется для указания ограничений пропускной способности для политики. Значение по умолчанию равно 1024.

Форма **delete** этой команды используется для восстановления ограничений пропускной способности по умолчанию.

Форма **show** этой команды используется для отображения настройки пропускной способности, выделенной политике.

## 26.9.75. traffic-policy shaper <имя_политики> class <класс>

Определение класса трафика для политики QoS с управлением загрузкой канала.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **class** *класс*

**delete traffic-policy shaper** *имя_политики* **class** *класс*

**show traffic-policy shaper** *имя_политики* **class** *класс*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            class 2-4095 {
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать 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. 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 управлением загрузкой канала.

Форма **show** этой команды используется для отображения настройки класса трафика в политике QoS с управлением загрузкой канала.

## 26.9.76. traffic-policy shaper <имя_политики> class <класс> bandwidth

Указание базовой гарантированной пропускной способности для класса трафика.

**Синтаксис**

**set traffic-policy shaper** *управлением загрузкой канала* **bandwidth** [*скорость* | *скорость_в_процентах* | *скорость_в_единицах*]

**delete traffic-policy shaper** *имя_политики* **class** *класс* **bandwidth**

**show traffic-policy shaper** *имя_политики* **class** *класс* **bandwidth**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            class 2-4095 {
                bandwidth текст
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*скорость*

Пропускная способность, указанная в килобитах в секунду.

*скорость_в_процентах*

Пропускная способность, указанная в процентах от общей пропускной способности. Используется формат число% (например, 85%).

*скорость_в_единицах*

Пропускная способность, указанная в виде числа и единицы измерения (например, 10mbit). Поддерживаются следующие единицы измерения:

**kbit**: килобитов в секунду.

**mbit**: мегабитов в секунду.

**gbit**: гигабитов в секунду.

**kbps**: килобайтов в секунду.

**mbps**: мегабайтов в секунду.

**gbps**: гигабайтов 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.

## 26.9.77. traffic-policy shaper <имя_политики> class <класс> burst

Установка размера непрерывной серии пакетов для класса трафика.

#### Синтаксис

**set traffic-policy shaper** *имя_политики* **class** *класс* **burst** [*число* | *число_в_единицах*]

**delete traffic-policy shaper** *имя_политики* **class** *класс* **burst**

**show traffic-policy shaper** *имя_политики* **class** *класс* **burst**

#### Режим интерфейса

Режим настройки.

#### Ветвь конфигурации

```
traffic-policy {
        shaper текст {
```

```
                    class 2-4095 {
                        burst текст
                    }
                }
            }
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*число*

Размер непрерывной серии, указанный в байтах.

*число_в_единицах*

Размер непрерывной серии, указанный в виде числа и единицы измерения (например, 10mb). Поддерживаются следующие единицы измерения:

**kb**: килобайты.

**mb**: мегабайты.

**gb**: гигабайты.

**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.

## 26.9.78. traffic-policy shaper <имя_политики> class <класс> ceiling

Установка верхней границы пропускной способности для класса трафика.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **class** *класс* **ceiling** [*скорость* | *скорость_в_процентах* | *скорость_в_единицах*]

**delete traffic-policy shaper** *имя_политики* **class** *класс* **ceiling**

**show traffic-policy shaper** *имя_политики* **class** *класс* **ceiling**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            class 2-4095 {
                ceiling текст
            }
        }
}
```

**Параметры**

**имя_политики**

Обязательный. Имя политики управления загрузкой канала.

**класс**

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

**скорость**

Максимальная пропускная способность, указанная в килобитах в секунду.

**скорость_в_процентах**

Максимальная пропускная способность, указанная в процентах от скорости интерфейса. Используется формат число% (например, 85%).

**скорость_в_единицах**

Пропускная способность, указанная в виде числа и единицы измерения (например, 10mbit). Поддерживаются следующие единицы измерения:

**kbit**: килобитов в секунду.

**mbit**: мегабитов в секунду.

**gbit**: гигабитов 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.

## 26.9.79. traffic-policy shaper <имя_политики> class <класс> description <описание>

Ввод описания для класса трафика.

#### Синтаксис

```
set traffic-policy shaper имя_политики class класс
description описание

delete traffic-policy shaper имя_политики class класс
description

show traffic-policy shaper имя_политики class класс
description
```

#### Режим интерфейса

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            class 2-4095 {
                description описание
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*описание*

Обязательный. 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.

## 26.9.80. traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия>

Определение правила для проверки соответствия классов трафика.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия*

**delete traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия*

**show traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            class 2-4095 {
                match текст {
                }
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. 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.

Следует заметить, что для изменения имени существующего правила соответствия в классе трафика нельзя использовать команду **set**. Для изменения правила следует удалить его и создать заново.

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.

## 26.9.81. traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> description <описание>

Ввод описания для правила соответствия.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **description** *описание*

**delete traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **description**

**show traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **description**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
          shaper текст {
               class 2-4095 {
                    match текст {
                         description описание
                    }
               }
          }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*описание*

Обязательный. 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.

## 26.9.82. traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> ether destination <mac-адрес>

Указание критерия соответствия на основе MAC-адреса получателя.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether destination** *mac-адрес*

**delete traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether destination**

**show traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether destination**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            class 2-4095 {
                match текст {
                    ether {

    destination mac-адрес
```

```
                                    }
                                }
                            }
                        }
                }
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*mac-адрес*

MAC-адрес получателя, на соответствие которому выполняется проверка. Формат адреса - 6 8-битовых шестнадцатеричных чисел, разделенных двоеточиями, например, 00:0a:59:9a:f2:ba.

**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.

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.

## 26.9.83. traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> ether protocol <число>

Указание критерия соответствия на основе типа пакета Ethernet.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether protocol** *число*

**delete traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether protocol**

**show traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether protocol**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            class 2-4095 {
                match текст {
                    ether {

    protocol число
                    }
                }
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*число*

Тип пакета Ethernet (номер протокола), соответствие которому проверяется. Значение должно лежать в диапазоне от 0 до 65535.

**Значение по умолчанию**

Если параметр не установлен, пакеты не проверяются на соответствие типа пакета Ethernet.

**Указания по использованию**

Это команда используется для определения условия соответствия по типу пакета Ethernet в классе трафика.

Форма **set** этой команды используется для указания типа пакета, соответствие которому должно проверяться.

Форма **delete** этой команды используется для удаления типа пакета в качестве проверяемого условия соответствия.

Форма **show** этой команды используется для отображения настройки типа пакета в качестве проверяемого условия соответствия.

## 26.9.84. traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> ether source <mac-адрес>

Указание критерия соответствия на основе MAC-адреса отправителя.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether source** *mac-адрес*

**delete traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether source**

**show traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ether source**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            class 2-4095 {
```

```
                        match текст {
                              ether {

        source mac-адрес
                                    }
                              }
                        }
                  }
            }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*mac-адрес*

MAC-адрес отправителя, на соответствие которому выполняется проверка. Формат адреса - 6 8-битовых шестнадцатеричных чисел, разделенных двоеточиями, например, 00:0a:59:9a:f2:ba.

**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.

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.

### 26.9.85. traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> interface <интерфейс>

Указание критерия соответствия на основе интерфейса для входящих пакетов.

#### Синтаксис

**set traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **interface** *интерфейс*

**delete traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **interface**

**show traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **interface**

#### Режим интерфейса

Режим настройки.

#### Ветвь конфигурации

```
traffic-policy {
        shaper текст {
            class 2-4095 {
                match текст {
                    interface текст
                }
            }
        }
}
```

#### Параметры

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*интерфейс*

Имя интерфейса Ethernet, на соответствие которому выполняется проверка. С указанным значением будет сравниваться входной интерфейс для входящего трафика.

**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).

Следует заметить, что нельзя проверять на соответствие “ip” и “vif” (или “interface”) одновременно внутри одной и той же настройки управления загрузкой канала.

Форма **set** этой команды используется для указания интерфейса, соответствие которому должно проверяться во входящих пакетах.

Форма **delete** этой команды используется для удаления соответствия по интерфейсу.

Форма **show** этой команды используется для отображения настройки соответствия по интерфейсу.

## 26.9.86. traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> ip destination

Указание критерия соответствия на основе сведений IP о получателе.

**Синтаксис**

```
set traffic-policy shaper имя_политики class класс match
имя_соответствия ip destination {address подсеть_ipv4 |
port порт}

delete traffic-policy shaper имя_политики class класс
match имя_соответствия ip destination [address | port]

show traffic-policy shaper имя_политики class класс match
имя_соответствия ip destination
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            class 2-4095 {
                match текст {
                    ip {
    destination {
        address подсеть_ipv4
        port текст
    }
                    }
                }
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*подсеть_ipv4*

Адрес подсети IP 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 номера порта должно лежать в диапазоне от 0 до 65535.

**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.

Следует заметить, что нельзя проверять на соответствие “ip” и “vif” (или “interface”), а также “ip” и “ipv6” одновременно внутри одной и той же настройки управления загрузкой канала.

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.

## 26.9.87. traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> ip dscp <значение>

Указание критерия соответствия на основе значения поля DSCP.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip dscp** *значение*

**delete traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip dscp**

**show traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip dscp**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            class 2-4095 {
                match текст {
                    ip {
                        dscp текст
                    }
                }
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. 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. Значение DSCP может быть указано в форме десятичного числа (например, 12), шестнадцатеричного числа (например, 0x1D) или в форме стандартного имени из файла /etc/iproute2/rt_dsfield (например, **lowdelay**).

**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.

Следует заметить, что нельзя проверять на соответствие “ip” и “vif” (или “interface”), а также “ip” и “ipv6” одновременно внутри одной и той же настройки управления загрузкой канала.

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.

## 26.9.88. traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> ip protocol <протокол>

Указание критерия соответствия на основе протокола IP.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip protocol** *протокол*

**delete traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip protocol**

**show traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip protocol**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            class 2-4095 {
                match текст {
                    ip {
```

```
        protocol текст
                                }
                            }
                        }
                    }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*протокол*

Имя протокола (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.

Следует заметить, что нельзя проверять на соответствие “ip” и “vif” (или “interface”), а также “ip” и “ipv6” одновременно внутри одной и той же настройки управления загрузкой канала.

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.

## 26.9.89. traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> ip source

Указание критерия соответствия на основе сведений IP об отправителе.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip source** {**address** *подсеть_ipv4* | **port** *порт*}

**delete traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip source** {**address** | **port**}

**show traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ip source**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            class 2-4095 {
                match текст {
                    ip {
    source {
        address подсеть_ipv4
        port текст
    }
                    }
                }
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*подсеть_ipv4*

Адрес подсети IP отправителя, соответствие которому проверяется в данном правиле.

*порт*

Порт отправителя, соответствие которому проверяется в данном правиле. Порт может быть указан в форме имени строчными буквами (например ssh) или в форме числа. Значение номера порта должно лежать в диапазоне от 0 до 65535.

**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.

Следует заметить, что нельзя проверять на соответствие “ip” и “vif” (или “interface”) одновременно внутри одной и той же настройки управления загрузкой канала.

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.

## 26.9.90. traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> ipv6 destination

Указание критерия соответствия на основе сведений IPv6 о получателе.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 destination** {**address** *подсеть_ipv6* | **port** *порт*}

**delete traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 destination** [**address** | **port**]

**show traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 destination**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            class 2-4095 {
                match текст {
                    ipv6 {
    destination {
        address подсеть_ipv6
        port текст
    }
                    }
                }
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*подсеть_ipv6*

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 номера порта должно лежать в диапазоне от 0 до 65535.

**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.

Следует заметить, что нельзя проверять на соответствие “ipv6” и “vif” (или “interface”), а также “ip” и “ipv6” одновременно внутри одной и той же настройки управления загрузкой канала.

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.

### 26.9.91. traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> ipv6 dscp <значение>

Указание критерия соответствия на основе значения поля DSCP.

#### Синтаксис

**set traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 dscp** *значение*

**delete traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 dscp**

**show traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 dscp**

#### Режим интерфейса

Режим настройки.

#### Ветвь конфигурации

```
traffic-policy {
          shaper текст {
               class 2-4095 {
                    match текст {
                         ipv6 {

     dscp текст
                         }
                    }
               }
          }
}
```

#### Параметры

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. 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. Значение DSCP может быть указано в форме десятичного числа (например, 12), шестнадцатеричного числа (например, 0x1D) или в форме стандартного имени из файла /etc/iproute2/rt_dsfield (например, **lowdelay**).

**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.

Следует заметить, что нельзя проверять на соответствие “ipv6” и “vif” (или “interface”) одновременно внутри одной и той же настройки управления загрузкой канала.

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.

## 26.9.92. traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> ipv6 protocol <протокол>

Указание критерия соответствия на основе протокола IPv6.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 protocol** *протокол*

**delete traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 protocol**

**show traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 protocol**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
          shaper текст {
               class 2-4095 {
                    match текст {
                         ipv6 {

     protocol текст
                         }
                    }
               }
          }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*протокол*

Имя протокола (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.

Следует заметить, что нельзя проверять на соответствие “ipv6” и “vif” (или “interface”) одновременно внутри одной и той же настройки управления загрузкой канала.

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.

## 26.9.93. traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> ipv6 source

Указание критерия соответствия на основе сведений IPv6 об отправителе.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 source** {**address** *подметь_ipv6* | **port** *порт*}

**delete traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 source** {**address** | **port**}

**show traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **ipv6 source**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            class 2-4095 {
                match текст {
```

```
                              ipv6 {

        source {

              address подсеть_ipv6

              port текст

        }
                              }
                         }
                    }
              }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*подсеть_ipv6*

Адрес подсети IPv6 отправителя, соответствие которому проверяется в данном правиле.

*порт*

Порт отправителя, соответствие которому проверяется в данном правиле. Порт может быть указан в форме имени строчными буквами (например, **ssh**) или в форме числа. Значение номера порта должно лежать в диапазоне от 0 до 65535.

**Значение по умолчанию**

Если параметр не установлен, пакеты не проверяются на соответствие

сведениям IPv6 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.

Следует заметить, что нельзя проверять на соответствие “ipv6” и “vif” (или “interface”) одновременно внутри одной и той же настройки управления загрузкой канала.

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.

## 26.9.94. traffic-policy shaper <имя_политики> class <класс> match <имя_соответствия> vif <идентификатор_vlan>

Указание критерия соответствия на основе идентификатора VLAN.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **vif** *идентификатор_vlan*

**delete traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **vif**

**show traffic-policy shaper** *имя_политики* **class** *класс* **match** *имя_соответствия* **vif**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            class 2-4095 {
                match текст {
```

```
                                vif 1-4096
                            }
                        }
                    }
            }
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*имя_соответствия*

Обязательный. Имя правила соответствия для класса.

*идентификатор_vlan*

Идентификатор VLAN, соответствие которому проверяется. Значение должно лежать в диапазоне от 1 до 4096.

**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.

Следует заметить, что нельзя проверять на соответствие “ip” и “vif” (или “interface”) одновременно внутри одной и той же настройки управления загрузкой канала.

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.

## 26.9.95. traffic-policy shaper <имя_политики> class <класс> priority <приоритет>

Указание приоритета класса трафика при выделении дополнительной пропускной способности.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **class** *класс* **priority** *приоритет*

**delete traffic-policy shaper** *имя_политики* **class** *класс* **priority**

**show traffic-policy shaper** *имя_политики* **class** *класс* **priority**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            class 2-4095 {
                priority целоебеззнака32разр
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*приоритет*

Приоритет, в соответствии с которым данному классу будет выделяться дополнительная пропускная способность. Значение должно лежать в диапазоне от 0 до 7, причем чем меньше значение, тем ниже приоритет. Значение по умолчанию равно 0.

**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.

## 26.9.96. traffic-policy shaper <имя_политики> class <класс> queue-limit <ограничение>

Указание максимального размера очереди для класса трафика.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **class** *класс* **queue-limit** *ограничение*

**delete traffic-policy shaper** *имя_политики* **class** *класс* **queue-limit**

**show traffic-policy shaper** *имя_политики* **class** *класс* **queue-limit**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            class 2-4095 {
                queue-limit 2..127
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*ограничение*

Максимальный размер очереди в пакетах. Обязательный. Максимальный размер очереди в пакетах. Значение должно лежать в диапазоне от 2 до 127.

**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.

## 26.9.97. traffic-policy shaper <имя_политики> class <класс> queue-type <тип>

Указание типа работы с очередью, используемого для класса трафика.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **class** *класс* **queue-type** *тип*

**delete traffic-policy shaper** *имя_политики* **class** *класс* **queue-type**

**show traffic-policy shaper** *имя_политики* **class** *класс* **queue-type**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            class 2-4095 {
                queue-type [fair-queue|drop-tail|
priority|random-detect]
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*тип*

Используемый метод работы с очередями. Поддерживаются следующие значения:

**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.

### 26.9.98. traffic-policy shaper <имя_политики> class <класс> set-dscp <значение>

Перезапись поля DSCP в пакетах в данном классе трафика указанным значением.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **class** *класс* **set-dscp** *значение*

**delete traffic-policy shaper** *имя_политики* **class** *класс* **set-dscp**

**show traffic-policy shaper** *имя_политики* **class** *класс* **set-dscp**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            class 2-4095 {
                set-dscp текст
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*класс*

Обязательный. Идентификатор класса. Значение должно лежать в диапазоне от 2 до 4095.

*значение*

Это значение записывается в поле DSCP пакетов данного класса трафика. Значение DSCP может быть указано в форме десятичного числа (например, 12), шестнадцатеричного числа (например, 0x1D) или в форме стандартного имени из файла /etc/iproute2/rt_dsfield (например, **lowdelay**). По умолчанию

поле DSCP не перезаписывается.

**Значение по умолчанию**

Если значение для перезаписи не установлено, поле DSCP не перезаписывается.

**Указания по использованию**

Эта команда используется, чтобы дать системе указание перезаписывать поле DSCP в пакетах данного класса трафика конкретным значением.

Путем перезаписи поля DSCP можно указать поведение сети при передаче пакетов, чтобы сделать возможным классификацию трафика в классы обслуживания и дальнейшую работу с трафиком наподобие измерения, применения политик и управления загрузкой каналов.

Стандартная семантика значений DSCP в соответствии с документом RFC 2474 приведена в приложении 4 на стр. 2112.

Форма **set** этой команды используется для перезаписи значений DSCP в пакетах данного класса трафика.

Форма **delete** используется для прекращения перезаписи значений DSCP.

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

## 26.9.99. traffic-policy shaper <имя_политики> default

Определение политики QoS по умолчанию с управлением загрузкой канала.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **default**

**delete traffic-policy shaper** *имя_политики* **default**

**show traffic-policy shaper** *имя_политики* **default**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            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.

## 26.9.100. traffic-policy shaper <имя_политики> default bandwidth

Указание базовой гарантированной пропускной способности для класса трафика по умолчанию.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **default bandwidth** [*скорость* | *скорость_в_процентах* | *скорость_в_единицах*]

**delete traffic-policy shaper** *имя_политики* **default bandwidth**

**show traffic-policy shaper** *имя_политики* **default bandwidth**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            default {
```

```
                    bandwidth текст
                }
            }
        }
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*скорость*

Пропускная способность в килобитах/с.

*скорость_в_процентах*

Пропускная способность, указанная в процентах от скорости интерфейса. Используется формат число% (например, 85%).

*скорость_в_единицах*

Пропускная способность, указанная в виде числа и единицы измерения (например, 10mbit). Поддерживаются следующие единицы измерения:

**kbit**: килобитов в секунду.

**mbit**: мегабитов в секунду.

**gbit**: гигабитов в секунду.

**kbps**: килобайтов в секунду.

**mbps**: мегабайтов в секунду.

**gbps**: гигабайтов 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.

## 26.9.101. traffic-policy shaper <имя_политики> default burst

Установка размера непрерывной серии пакетов для класса трафика по умолчанию.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **default burst** [*число* | *число_в_единицах*]

**delete traffic-policy shaper** *имя_политики* **default burst**

**show traffic-policy shaper** *имя_политики* **default burst**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            default {
                burst текст
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*число*

Размер непрерывной серии в байтах.

*число_в_единицах*

Размер непрерывной серии, указанный в виде числа и единицы измерения (например, 10mb). Поддерживаются следующие единицы измерения:

**kb**: килобайты.

**mb**: мегабайты.

**gb**: гигабайты.

**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.

## 26.9.102. traffic-policy shaper <имя_политики> default ceiling

Установка верхней границы пропускной способности для класса трафика по умолчанию.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **default ceiling** [*скорость* | *скорость_в_процентах* | *скорость_в_единицах*]

**delete traffic-policy shaper** *имя_политики* **default ceiling**

**show traffic-policy shaper** *имя_политики* **default ceiling**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            default {
                ceiling текст
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*скорость*

Ограничение в килобитах/с.

*скорость_в_процентах*

Пропускная способность, указанная в процентах от общей пропускной способности. Используется формат число% (например, 85%).

*скорость_в_единицах*

Пропускная способность, указанная в виде числа и единицы измерения (например, 10mbit). Поддерживаются следующие единицы измерения:

**kbit**: килобитов в секунду.

**mbit**: мегабитов в секунду.

**gbit**: гигабитов 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.

## 26.9.103. traffic-policy shaper <имя_политики> default priority <приоритет>

Указание приоритета класса трафика по умолчанию при выделении дополнительной пропускной способности.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **default priority** *приоритет*

**delete traffic-policy shaper** *имя_политики* **default priority**

**show traffic-policy shaper** *имя_политики* **default priority**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            default {
                priority 0-7
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*приоритет*

Приоритет, в соответствии с которым данному классу будет выделяться дополнительная пропускная способность. Значение должно лежать в диапазоне от 0 до 7, причем чем больше значение, тем ниже приоритет. Значение по умолчанию равно 0.

**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.

## 26.9.104. traffic-policy shaper <имя_политики> default queue-limit <ограничение>

Указание максимального размера очереди для класса трафика по умолчанию.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **default queue-limit** *ограничение*

**delete traffic-policy shaper** *имя_политики* **default queue-limit**

**show traffic-policy shaper** *имя_политики* **default queue-limit**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            default {
                queue-limit целоебеззнака32разр
            }
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*ограничение*

Максимальный размер очереди в пакетах. Значение должно лежать в диапазоне от 1 до 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.

## 26.9.105. traffic-policy shaper <имя_политики> default queue-type <тип>

Указание типа работы с очередью, используемого для класса трафика по умолчанию.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **default queue-type** *тип*

**delete traffic-policy shaper** *имя_политики* **default queue-type**

**show traffic-policy shaper** *имя_политики* **default queue-type**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
          shaper текст {
               default {
                    queue-type [fair-queue|drop-tail|
priority|random-detect]
               }
          }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*тип*

Используемый метод работы с очередями. Поддерживаются следующие значения:

**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.

## 26.9.106. traffic-policy shaper <имя_политики> default set-dscp <значение>

Перезапись поля DSCP в пакетах в классе трафика по умолчанию указанным значением.

#### Синтаксис

**set traffic-policy shaper** *имя_политики* **default set-dscp** *значение*

**delete traffic-policy shaper** *имя_политики* **default set-dscp**

**show traffic-policy shaper** *имя_политики* **default set-dscp**

#### Режим интерфейса

Режим настройки.

#### Ветвь конфигурации

```
traffic-policy {
        shaper текст {
            default {
                set-dscp текст
            }
        }
```

}

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*значение*

Это значение записывается в поле DSCP пакетов класса трафика по умолчанию. Значение DSCP может быть указано в форме десятичного числа (например, 12), шестнадцатеричного числа (например, 0x1D) или в форме стандартного имени из файла /etc/iproute2/rt_dsfield (например, **lowdelay**). По умолчанию поле DSCP не перезаписывается.

**Значение по умолчанию**

Если значение для перезаписи не установлено, поле DSCP не перезаписывается.

**Указания по использованию**

Эта команда используется, чтобы дать системе указание перезаписывать поле DSCP в пакетах класса трафика по умолчанию конкретным значением.

Путем перезаписи поля DSCP можно указать поведение сети при передаче пакетов, чтобы сделать возможным классификацию трафика в классы обслуживания и дальнейшую работу с трафиком наподобие измерения, применения политик и управления загрузкой каналов.

Стандартная семантика значений DSCP в соответствии с документом RFC 2474 приведена в приложении 4 на стр. 2112.

Форма **set** этой команды используется для перезаписи значений DSCP в пакетах класса трафика по умолчанию.

Форма **delete** используется для прекращения перезаписи значений DSCP в пакетах класса трафика по умолчанию.

Форма **show** этой команды используется для отображения настройки перезаписи DSCP в классе трафика по умолчанию.

## 26.9.107. traffic-policy shaper <имя_политики> description <описание>

Ввод описания для политики QoS с управлением загрузкой канала.

**Синтаксис**

**set traffic-policy shaper** *имя_политики* **description** *описание*

**delete traffic-policy shaper** *имя_политики* **description**

**show traffic-policy shaper** *имя_политики* **description**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
traffic-policy {
        shaper текст {
            description описание
        }
}
```

**Параметры**

*имя_политики*

Обязательный. Имя политики управления загрузкой канала.

*описание*

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.

## 26.9.108. show queueing

Отображение текущих политик QoS.

**Синтаксис**

**show queueing** [*тип_интерфейса* [*интерфейс*]]

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

*тип_интерфейса*

Необязательный. Тип интерфейса, политики QoS которого следует вывести.

Список возможных значений: **ethernet**, **adsl** и **serial**.

интерфейс

Необязательный. Конкретный интерфейс (например, **eth0**).

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для отображения текущих политик QoS.

**Примеры**

В примере 26.4 приведен вывод всех политик QoS.

*Пример 26.4 - "show queueing": отображение всех политик QoS*

```
admin@neo:~$ show queueing
Output queues:
Interface traffic-policy  Sent     Dropped   Overlimit eth0 shaper
     99277          0         0
admin@neo:~$
```

В примере 26.5 приведен вывод конкретных политик QoS.

*Пример 26.5 - "show queueing ethernet eth0": отображение политик QoS на конкретном интерфейсе*

```
admin@neo:~$ show queueing ethernet eth0
eth0 Output queue:
Class     traffic-policy Sent Dropped   Overlimit
1    shaper    106384    0    0
8001 fair-queue     48286     0    0
8002 fair-queue     58098     0    0
```

```
8003 drop-tail 0    0    0
admin@neo:~$
```

# 27. БАЛАНСИРОВКА НАГРУЗКИ ГВС

В этой главе даны указания по использованию функции балансировки нагрузки глобальной вычислительной сети (ГВС) системы Altell NEO.

В этой главе рассматриваются следующие вопросы:

- Настройка балансировки нагрузки ГВС.
- Команды балансировки нагрузки ГВС.

## 27.1. Настройка балансировки нагрузки ГВС

В этой главе даны указания по настройке балансировки нагрузки ГВС в системе Altell NEO.

В этом разделе рассматриваются следующие вопросы:

- Обзор балансировки нагрузки ГВС.
- Примеры настройки.

### 27.1.1. Обзор балансировки нагрузки ГВС

В этом разделе рассматриваются следующие вопросы:

- Что такое балансировка нагрузки.
- Алгоритм балансировки.
- Правила балансировки.
- Балансировка на основе потоков и на основе пакетов.
- Проверка работоспособности.
- Переход на резервный ресурс при сбое.
- Исключение трафика из балансировки нагрузки ГВС.
- Ограничение скорости.
- Выполнение сценария при изменении состояния интерфейса.
- Соглашения о шлюзе по умолчанию для сред DHCP и статических маршрутов.
- Действия по настройке балансировки нагрузки.

### 27.1.2. Что такое балансировка нагрузки

Altell NEO поддерживает автоматическую балансировку нагрузки по исходящему

трафику на двух или более выходных интерфейсах. Помимо балансировки нагрузок по трафику на интерфейсах, описываемая функция обеспечивает избыточность по путям на случай сбоя пути, так как трафик будет балансироваться на оставшихся работоспособных путях. Когда сбойный путь восстановит работоспособность, он будет добавлен к списку работоспособных путей, чтобы система балансировки нагрузки смогла использовать его снова. Система определяет работоспособность пути с помощью периодической проверки работоспособности опросом удаленной цели или нескольких целей.

Поддерживается балансировка нагрузки только для исходящего трафика. В балансировке нагрузки не участвуют пакеты, отправленные с самой системы, если явно не настроено противоположное поведение (с помощью команды **load-balancing wan enable-local-traffic**, см. раздел 27.3.4. ).

Для выполнения балансировки нагрузки необходимо наличие в таблице маршрутизации как минимум двух путей, выходящих наружу через интерфейсы, на которых осуществляется балансировка нагрузки. Процесс балансировки нагрузки ГВС автоматически устанавливает маршруты по умолчанию, настроенные администратором для каждого пути, и осуществляет балансировку трафика в соответствии с работоспособностью путей и весами, примененными к каждому интерфейсу. Пути, установленные в таблице маршрутизации, можно вывести командой **show ip route**.

### 27.1.3. Алгоритм балансировки

Балансировка нагрузки на исходящих пакетах выполняется с помощью алгоритма взвешенного случайного распределения. Если веса не назначены, шансы каждого интерфейса быть выбранным равны, в результате чего на каждый интерфейс отправляется примерно одно и то же число пакетов. Если у интерфейса больший вес, то в среднем он будет выбран чаще; например, если у интерфейса A вес 2, а у интерфейса B вес 1, интерфейс A будет выбран в среднем в 67% случаев.

### 27.1.4. Правила балансировки

Род трафика, подлежащего балансировке, набор интерфейсов и относительные веса для каждого интерфейса указываются в правиле балансировки нагрузки. В правиле балансировки нагрузки имеются набор критериев соответствия и набор интерфейсов с назначенными весами. Исходящие пакеты проверяются на соответствие по критериям,

указанным в правиле. Если пакет соответствует правилу, алгоритм балансировки нагрузки определяет, на какой интерфейс в указанном наборе следует отправить пакет.

Правила проверяются в порядке нумерации до тех пор, пока не будет найдено соответствие. Если соответствие найдено, то пакет отправляется на один из интерфейсов, указанных в правиле, за исключением случая, когда все указанные интерфейсы неактивны. В этом случае проверяется следующее правило, и так до тех пор, пока не будет найдено соответствующее правило с как минимум одним активным интерфейсом. Если соответствующие правила не найдены, используется основная таблица маршрутизации системы.

После настройки номера правил изменить нельзя. По этой причине рекомендуется настраивать правила с интервалами в номерах (например, правило 5, правило 10, правило 15 и т.д.) на случай необходимости вставки правила в будущем.

### 27.1.5. Балансировка на основе потоков и на основе пакетов

В общем случае балансировка нагрузки по трафику выполняется не на основе пакетов, а на основе потоков. Любой трафик, связанный с подключением, остаётся соответствующим образом связанным с интерфейсом, назначенным для балансировки нагрузки. Потоки отслеживаются с помощью элемента в таблице отслеживания потоков. Потоки определяются по кортежу, состоящему из адреса отправителя, адреса получателя и порта.

Если включена маршрутизация по отправителю, балансировка нагрузки по трафику выполняется на основе пакетов, а адрес отправителя учитывается при выборе интерфейса для передачи наружу. Кроме того, после очистки таблицы отслеживания подключений балансировка ранее установившихся потоков выполняется на основе пакетов вплоть до установки нового подключения в потоке.

### 27.1.6. Проверка работоспособности

Интерфейс ГВС, участвующий в балансировке нагрузки, считается активным членом пула интерфейсов, пока он проходит проверки работоспособности. Наблюдение за работоспособностью интерфейса осуществляется путем отправки с него сообщений эхо-запроса ICMP (“пинга”) на удаленную точку назначения через некоторый интервал времени. Если сообщение эхо-ответа ICMP от точки назначения принято успешно, это показывает, что интерфейс может как отправлять пакеты в Интернет, так и получать пакеты из Интернета.

Если проверка работоспособности интерфейса завершается сбоем, интерфейс удаляется из пула активных интерфейсов.

***ПРИМЕЧАНИЕ.*** *Также существует проверка на основе времени жизни (ttl), при которой на целевой адрес отправляется пакет UDP с ограничением ttl.*

На каждом интерфейсе, участвующем в балансировке нагрузки, необходимо настроить критерии работоспособности, в том числе число неудачных проверок работоспособности, после которого интерфейс объявляется неработоспособным, и число удачных проверок, необходимых для объявления о восстановлении работоспособности. 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.

Настройка проверки работоспособности состоит из следующих элементов:

- Удаленное место назначения, доступность которого будет проверяться. Используется команда **load-balancing wan interface-health <имя_интерфейса> test <номер_теста> target <адрес>** (см. раздел 27.3.12. ).
- Следующий транзитный участок на пути к целевому месту назначения. Используется команда **load-balancing wan interface-health <имя_интерфейса> nexthop <ipv4-адрес>** (см. раздел 27.3.9. ).
- Тип проверки, которую следует выполнить (либо **ping**, либо **ttl**). Используется команда **load-balancing wan interface-health <имя_интерфейса> test <номер_теста> type <тип>** (см. раздел 27.3.14. ).
- Максимальное время ожидания ответа на сообщение эхо-запроса, которое можно считать удачным выполнением проверки. Используется команда **load-balancing wan interface-health <имя_интерфейса> test <номер_теста> resp-time <секунды>** (см. раздел 27.3.11. ).
- Для проверок по ttl используется ограничение для ttl. Используется команда **load-balancing wan interface-health <имя_интерфейса> test <номер_теста> ttl-limit**

**<ограничение>** (см. раздел 27.3.13. ).

- Число сбоев проверки работоспособности, после которых интерфейс начинает считаться недоступным. Используется команда **load-balancing wan interface-health <имя_интерфейса> failure-count <число>** (см. раздел 27.3.8. ).
- Число удачных проверок работоспособности, после которых интерфейс возвращается в пул активных интерфейсов. Используется команда **load-balancing wan interface-health <имя_интерфейса> success-count <число>** (см. раздел 27.3.15. ).

### 27.1.7. Неявное преобразование сетевых адресов

При наличии нескольких внешних интерфейсов могут возникнуть трудности, состоящие в том, что ответный трафик может приходить не через тот интерфейс, через который был отправлен исходный трафик. Это называется асимметричной маршрутизацией и в целом нежелательно в силу ряда причин — в числе которых возможная разбалансировка нагрузки по входящему трафику и трудности при поиске и устранении проблем. Для предотвращения асимметричной маршрутизации служба балансировки нагрузки ГВС по умолчанию заменяет адрес отправителя всех пакетов IP, выходящих из системы через некоторый интерфейс, на адрес этого интерфейса (то есть выполняет преобразование сетевых адресов с маскировкой) таким образом, чтобы ответный трафик пришел через тот же интерфейс, через который был отправлен исходный трафик. Если это поведение, принятое по умолчанию, нежелательно, его можно отключить при помощи команды **load-balancing wan disable-source-nat** (см. раздел 27.3.3. ).

*Примечание. В том случае если требуется выполнять преобразование сетевых адресов только для некоторых потоков сетевого трафика, совместно с использованием команды **load-balancing wan disable-source-nat** может быть настроено явное преобразование адресов для заданных потоков трафика при помощи ветви конфигурации **service nat**. Подробная информация о настройке NAT приведена в разделе «Преобразование сетевых адресов (NAT)».*

### 27.1.8. Переход на резервный ресурс при сбое

Обычно в балансировке трафика задействованы все интерфейсы, выделенные для

балансировки. Однако для балансировки трафика ГВС Altell NEO поддерживает и режим перехода на резервный ресурс при сбое (при помощи команды **load-balancing wan rule <правило> failover** (см. раздел 27.3.21. )). В режиме перехода на резервный ресурс при сбое один интерфейс выбирается системой в качестве первичного, а оставшиеся назначаются вторичными или резервными.

Интерфейс выбирается первичным на основе его настроенного веса и достижимости цели. Если связь через первичный интерфейс прерывается, из набора вторичных интерфейсов выбирается следующий вторичный интерфейс.

Выбор первичного интерфейса может осуществляться не только на основе весов, но и на основе порядка правил. Так как трафик направляется наружу через первый работоспособный интерфейс, указанный в соответствующем правиле, правила можно упорядочить на основе предпочтительности выходных интерфейсов. Например, если в качестве первичного интерфейса вплоть до утраты им работоспособности должен использовать eth0, а в ее случае должен использоваться eth1, то можно включить eth0 в первое правило, а eth1 во второе.

Если канал переходит на резервный ресурс при сбое и выбирается новый первичный интерфейс, существующие сеансы не переходят автоматически на новый путь. Конечный пользователь наблюдает период неактивности сеанса. Для предотвращения этой задержки в случае смены состояния канала и сбоя сеанса можно очистить таблицу сеансов с помощью команды **load-balancing wan flush-connections** (см. раздел 27.3.5. ).

### 27.1.9. Исключение трафика из балансировки нагрузки ГВС

Бывают случаи, в которых нежелательно выполнять балансировку нагрузки для всего трафика, исходящего с указанного интерфейса. Например, в ситуации, когда есть две ЛВС с необходимостью балансировки нагрузки по восходящему трафику в каждой, трафик из одной ЛВС в другую также будет маршрутизироваться в вышестоящую сеть, что не является желательным поведением. Чтобы избежать этого, трафик между указанными ЛВС можно исключить из балансировки нагрузки. Исключение трафика настраивается с помощью команды **load-balancing wan rule <rule> exclude** (см. раздел 27.3.20. ).

### 27.1.10. Ограничение скорости

Ограничение скорости при балансировке нагрузки ГВС означает установку

ограничения скорости, при котором правило будет активно. Например, пусть нужно настроить систему на отправку всех пакетов через первый интерфейс до указанного ограничения, а пакеты, выходящие за ограничение, отправлять через второй интерфейс. В этой ситуации требуется два правила:

- Первое правило, в котором указано ограничение скорости, предназначено для отправки пакетов через интерфейс 1.
- Второе правило, в котором отсутствует ограничение скорости, предназначено для отправки пакетов через интерфейс 2. Ограничение скорости настраивается с помощью команды **load-balancing wan rule <правило> limit** (см. раздел 27.3.24. ).

### 27.1.11. Выполнение сценария при изменении состояния интерфейса

Чтобы обеспечить гибкость в выборе действий, предпринимаемых при смене состояния интерфейса, в системе Altell NEO предоставляется функция обработчика событий. Эта функция позволяет запустить сценарий при смене состояния интерфейса с активного на сбойное или наоборот.

Выполнение сценария по изменению состояния интерфейса настраивается при помощи команды **load-balancing wan hook <имя_сценария>** (см. раздел 27.3.6. ).

### 27.1.12. Соглашения о шлюзе по умолчанию для сред DHCP и статических маршрутов

В средах, где балансировка нагрузки ГВС настраивается для балансировки трафика, идущего по клиентским интерфейсам DHCP, и имеются также статические маршруты к шлюзу по умолчанию, балансировка нагрузки ГВС не будет работать должным образом до тех пор, пока расстояние до следующего транзитного участка в статических маршрутах по умолчанию не будет изменено с 1 на 2. Причина такого поведения состоит в том, что по умолчанию у статических маршрутов по умолчанию расстояние равно 1, а у маршрутов по умолчанию, установленных по DHCP, расстояние равно 2 и соответственно более низкий приоритет. Более высокий приоритет статических маршрутов по умолчанию ведет к тому, что они выбираются во всех случаях. Установка для них того же приоритета, что и для клиентских интерфейсов DHCP, позволяет им равноправно участвовать в обработке правил, в результате чего маршрутов по умолчанию получается несколько.

### 27.1.13. Действия по настройке балансировки нагрузки

Балансировка нагрузки ГВС настраивается в три этапа:

1. Определение цели (или целей), достижимых с каждого интерфейса,участвующего в балансировке нагрузки. Цель используется службой балансировки нагрузки для определения работоспособности интерфейса.
2. Настройка адреса следующего транзитного участка для каждой цели и для каждого интерфейса, участвующего в балансировке нагрузки. Служба балансировки нагрузки использует этот адрес для доступа к цели.
3. Настройка одной записи главного статического маршрута для каждой цели, чтобы обеспечить маршрутизацию для доступа к цели через нужный интерфейс.

## 27.2. Примеры настройки

В этом разделе рассматриваются следующие вопросы:

- Базовая настройка балансировки нагрузки ГВС.
- Переход на резервный ресурс при сбое с использованием весов интерфейсов.
- Переход на резервный ресурс при сбое с использованием порядка правил.
- Переход на резервный ресурс при сбое с использованием порядка правил — приоритетный трафик.
- Исключение трафика из балансировки нагрузки.

### 27.2.1. Базовая настройка балансировки нагрузки ГВС

В этом примере представлен образец базовой настройки балансировки нагрузки ГВС. Свойства приведенной настройки:

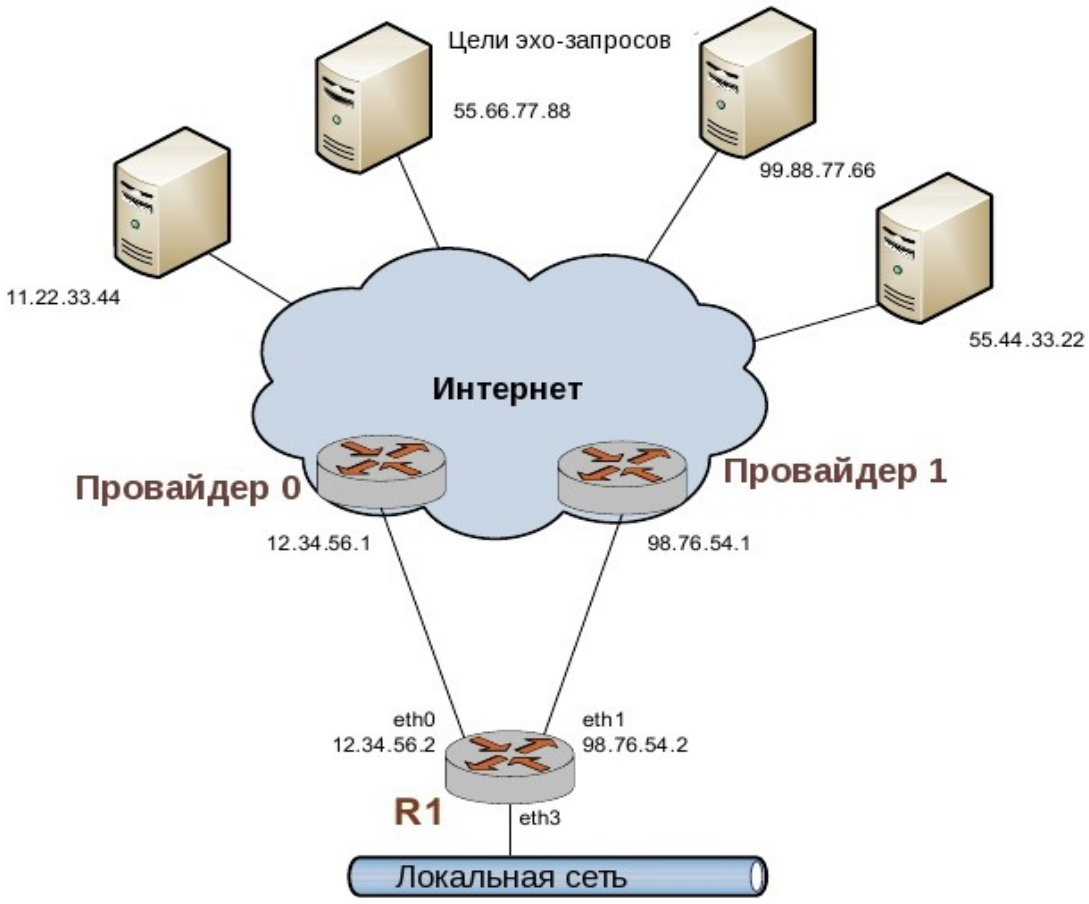
- Весь трафик, входящий на R1 через интерфейс eth3, балансируется на интерфейсах eth0 и eth1.
- Выходные интерфейсы eth0 и eth1 проверяются на работоспособность путем отправки с них эхо-запросов на удаленные цели. В примере используются следующие удаленные цели: 11.22.33.44, 55.66.77.88, 99.88.77.66 и 55.44.33.22.
- Исходящим пакетам назначается первичный адрес отправителя назначенного

интерфейса.

- Интерфейс eth1 должен быть удален из пула активных интерфейсов после четырех последовательных сбоев эхо-запроса, а интерфейс eth0 — после пяти последовательных сбоев.

После выполнения всех команд маршрутизатор R1 будет настроен так, как показано на рисунке 87.

*Рисунок 87 - Балансировка нагрузки ГВС*




В этом разделе имеются следующие примеры:

- Пример 27.1. Создание статических маршрутов к целям эхо-запроса
- Пример 27.2. Создание настройки балансировки нагрузки

В примере 27.1 выполняется создание статических маршрутов к двум поставщикам

услуг доступа к Интернету, между которыми будет балансироваться нагрузка: 12.34.56.1 и 98.76.54.1. Для создания этих статических маршрутов выполните следующие действия в режиме настройки:

*Пример 27.1 - Создание статических маршрутов к целям эхо-запроса*

| Действие | Команда |
|---|---|
| Создание статического маршрута к цели эхо-запроса для проверки работоспособности eth0. | admin@R1# **set protocols static route 11.22.33.44/32 next-hop 12.34.56.1**<br>[edit] |
| Создание статического маршрута ко второй цели эхо-запроса для проверки работоспособности eth0. | admin@R1# **set protocols static route 55.66.77.88/32 next-hop 12.34.56.1**<br>[edit] |
| Создание статического маршрута к цели эхо-запроса для проверки работоспособности eth1. | admin@R1# **set protocols static route 99.88.77.66/32 next-hop 98.76.54.1**<br>[edit] |
| Создание статического маршрута ко второй цели эхо-запроса для проверки работоспособности eth1. | admin@R1# **set protocols static route 55.44.33.22/32 next-hop 98.76.54.1**<br>[edit] |
| Фиксация настройки. | admin@R1# **commit**<br>[edit] |
| Отображение настройки. | admin@R1# **show protocols static**<br>route 11.22.33.44/32 {<br>next-hop 12.34.56.1 {<br>}<br>}<br>route 55.66.77.88/32 { |

```
        next-hop 12.34.56.1 {
        }
    }
    route 99.88.77.66/32 {
        next-hop 98.76.54.1 {
        }
    }
    route 55.44.33.22/32 {
        next-hop 98.76.54.1 {
        }
    }
    [edit]
```

В примере 27.2 на R1 выполняется установка настройки базовой балансировки нагрузки. Для создания настройки балансировки нагрузки выполните следующие действия в режиме настройки:

*Пример 27.2 - Создание настройки балансировки нагрузки*

| Действие | Команда |
|---|---|
| Установка счетчика сбоев для eth0. | admin@R1# **set load-balancing wan interface-health eth0 failure-count 5**<br>[edit] |
| Установка следующего транзитного участка для eth0. | admin@R1# **set load-balancing wan interface-health eth0 nexthop 12.34.56.1**<br>[edit] |
| Установка типа проверки для eth0. | admin@R1# **set load-balancing wan interface-health eth0 test 10 type ping**<br>[edit] |

| | |
|---|---|
| Установка цели эхо-запроса для eth0. | admin@R1# **set load-balancing wan interface-health eth0 test 10 target 11.22.33.44**<br>[edit] |
| Установка типа проверки для eth0. | admin@R1# **set load-balancing wan interface-health eth0 test 11 type ping**<br>[edit] |
| Установка второй цели эхо-запроса для eth0. | admin@R1# **set load-balancing wan interface-health eth0 test 11 target 55.66.77.88**<br>[edit] |
| Установка счетчика сбоев для eth1. | admin@R1# **set load-balancing wan interface-health eth1 failure-count 4**<br>[edit] |
| Установка следующего транзитного участка для eth1. | admin@R1# **set load-balancing wan interface-health eth1 nexthop 98.76.54.1**<br>[edit] |
| Установка типа проверки для eth1. | admin@R1# **set load-balancing wan interface-health eth1 test 10 type ping**<br>[edit] |
| Установка цели эхо-запроса для eth1. | admin@R1# **set load-balancing wan interface-health eth1 test 10 target 99.88.77.66**<br>[edit] |
| Установка типа проверки для eth1. | admin@R1# **set load-balancing wan** |

```
interface-health eth1 test 11
type ping
[edit]
```

Установка второй цели эхо-запроса для eth1.

```
admin@R1# set load-balancing wan
interface-health eth1 test 11
target 55.44.33.22
[edit]
```

Определение eth3 в качестве входного интерфейса.

```
admin@R1# set load-balancing wan
rule 10 inbound-interface eth3
[edit]
```

Определение eth0 в качестве одного из интерфейсов, участвующих в балансировке нагрузки.

```
admin@R1# set load-balancing wan
rule 10 interface eth0
[edit]
```

Определение eth1 в качестве второго интерфейса, участвующего в балансировке нагрузки.

```
admin@R1# set load-balancing wan
rule 10 interface eth1
[edit]
```

Фиксация настройки.

```
admin@R1# commit
[edit]
```

Отображение настройки.

```
admin@R1# show load-balancing
wan {
     interface-health eth0 {
          failure-count 5
          nexthop 12.34.56.1
          test 10 {
               target 11.22.33.44
               type ping
          }
          test 11 {
               target 55.66.77.88
```

```
                type ping
            }
        }
        interface-health eth1 {
            failure-count 4
            nexthop 98.76.54.1
            test 10 {
                target 99.88.77.66
                type ping
            }
            test 11 {
                target 55.44.33.22
                type ping
            }
        }
        rule 10 {
            inbound-interface eth3
            interface eth0 {
            }
            interface eth1 {
            }
        }
    }
    [edit]
```

### 27.2.2. Переход на резервный ресурс при сбое с использованием весов интерфейсов

В предыдущем примере система была настроена на балансировку нагрузки по трафику между eth0 и eth1. В примере, приведенном в данном разделе, вместо балансировки трафика eth0 настраивается в качестве первичного интерфейса, а eth1 в качестве резервного интерфейса, который будет использоваться в случае сбоя eth0. Изменение вносится только в правило 10.

В приведенном примере:

- Весь трафик, входящий через интерфейс eth3, отправляется наружу через интерфейс eth0.
- Если произойдет сбой eth0, весь трафик, входящий через интерфейс eth3, будет отправляться наружу через eth1. В примере 27.3 устанавливается правило настройки перехода на резервный ресурс при сбое на R1. Для создания из предыдущего примера настройки перехода на резервный интерфейс при сбое с использованием весов интерфейсов выполните следующие действия в режиме настройки:

*Пример 27.3 - Создание настройки перехода на резервный ресурс при сбое с использованием весов интерфейсов*

| Действие | Команда |
|---|---|
| Удаление существующего правила 10 из предыдущего примера. | admin@R1# **delete load-balancing wan rule 10**<br>[edit] |
| Включение режима перехода на резервный ресурс при сбое. | admin@R1# se**t load-balancing wan rule 10 failover**<br>[edit] |
| Определение eth3 в качестве входного интерфейса. | admin@R1# **set load-balancing wan rule 10 inbound-interface eth3**<br>[edit] |
| Определение eth0 в качестве первичного интерфейса, поскольку вес его будет наибольшим. | admin@R1# **set load-balancing wan rule 10 interface eth0 weight 10**<br>[edit] |
| Определение eth1 в качестве вторичного интерфейса, поскольку вес его будет наименьшим. | admin@R1# **set load-balancing wan rule 10 interface eth1 weight 1**<br>[edit] |
| Фиксация настройки. | admin@R1# **commit**<br>[edit] |
| Отображение настройки. | admin@R1# **show load-balancing** |

```
wan {
     interface-health eth0 {
          failure-count 5
          nexthop 12.34.56.1
          test 10 {
               target 11.22.33.44
               type ping
          }
          test 11 {
               target 55.66.77.88
               type ping
          }
     }
     interface-health eth1 {
          failure-count 4
          nexthop 98.76.54.1
          test 10 {
               target 99.88.77.66
               type ping
          }
          test 11 {
               target 55.44.33.22
               type ping
          }
     }
     rule 10 {
          failover
          inbound-interface eth3
          interface eth0 {
               weight 10
          }
          interface eth1 {
```

```
                    weight 1
                }
            }
        }
        [edit]
```

### 27.2.3. Переход на резервный ресурс при сбое с использованием порядка правил

В предыдущем примере система была настроена на отправку всего входящего трафика с eth3 наружу через eth0 до сбоя проверки работоспособности eth0. После сбоя проверки работоспособности eth0 весь входящий трафик с eth3 будет отправляться с eth1. Настройка была выполнена с помощью команды **failover** и назначения различных весов двум выходным интерфейсам. В примере, приведенном в данном разделе, переход на резервный ресурс при сбое выполняется на основе порядка правил. Опять же, весь трафик с eth3 отправляется наружу через eth0 до сбоя проверки его работоспособности, после чего отправляется через eth1.

Такое поведение реализуется с помощью двух правил. Одно правило направляет весь трафик с eth3 на eth0, другое — весь трафик с eth3 на eth1. Когда eth0 работоспособен, весь трафик с eth3 соответствует первому правилу и отправляется наружу через eth0. Если происходит сбой eth0, первое правило обходится из-за состояния работоспособности пути, и вступает в силу второе правило, направляющее весь трафик с eth3 на eth1. Как только eth0 становится работоспособным, трафик снова начинает соответствовать первому правилу и отправляется наружу через eth0.

В примере 27.4 устанавливаются правила настройки перехода на резервный ресурс при сбое на R1. Для создания из предыдущего примера настройки перехода на резервный интерфейс при сбое с использованием порядка правил выполните следующие действия в режиме настройки:

*Пример 27.4 - Создание настройки перехода на резервный ресурс при сбое с использованием порядка правил*

| Действие | Команда |
|---|---|

Удаление существующего правила 10 из предыдущего примера.

```
admin@R1# delete load-balancing wan rule 10
[edit]
```

Определение eth3 в качестве входного интерфейса для данного правила.

```
admin@R1# set load-balancing wan rule 10 inbound-interface eth3
[edit]
```

Определение eth0 в качестве первичного выходного интерфейса.

```
admin@R1# set load-balancing wan rule 10 interface eth0
[edit]
```

Определение eth3 в качестве входного интерфейса для данного правила.

```
admin@R1# set load-balancing wan rule 20 inbound-interface eth3
[edit]
```

Определение eth1 в качестве вторичного выходного интерфейса.

```
admin@R1# set load-balancing wan rule 20 interface eth1
[edit]
```

Фиксация настройки.

```
admin@R1# commit
[edit]
```

Отображение настройки.

```
admin@R1# show load-balancing
wan {
     interface-health eth0 {
          failure-count 5
          nexthop 12.34.56.1
          test 10 {
               target 11.22.33.44
               type ping
          }
          test 11 {
               target 11.22.33.44
               type ping
          }
```

```
        }
        interface-health eth1 {
            failure-count 4
            nexthop 98.76.54.1
            test 10 {
                target 99.88.77.66
                type ping
            }
            test 11 {
                target 55.44.33.22
                type ping
            }
        }
        rule 10 {
            inbound-interface eth3
            interface eth0 {
            }
        }
        rule 20 {
            inbound-interface eth3
            interface eth1 {
            }
        }
    }
    [edit]
```

### 27.2.4. Переход на резервный ресурс при сбое с использованием порядка правил — приоритетный трафик

Одним из преимуществ использования порядка правил для настройки перехода на резервный ресурс при сбое является дополнительная гибкость, которую оно предоставляет. Например, в ситуациях, где резервный канал имеет меньшую скорость, чем первичный, и способен пропускать только приоритетный трафик, требуется настройка с использованием

порядка правил.

В предыдущем примере система была настроена на отправку всего входящего трафика с eth3 наружу через eth0 до сбоя проверки работоспособности eth0. После сбоя проверки работоспособности eth0 весь входящий трафик с eth3 отправлялся с eth1. Это достигалось с помощью порядка правил. В примере, приведенном в данном разделе, принимается, что резервный канал имеет более низкую скорость и не способен принять весь трафик, так что для отправки наружу по резервному каналу в случае сбоя проверки работоспособности eth0 выбирается только высокоприоритетный трафик (в данном случае трафик VoIP).

В примере 27.5 устанавливаются правила настройки перехода на резервный ресурс при сбое на R1. Чтобы изменить предыдущий пример с целью создания настройки перехода на резервный ресурс при сбое с использованием порядка правил в случае, если после сбоя проверки работоспособности первичного интерфейса по вторичному отправляется наружу лишь часть трафика, выполните следующие действия в режиме настройки:

*Пример 27.5 - Создание настройки перехода на резервный ресурс при сбое с использованием порядка правил и резервного канала с меньшей скоростью*

| Действие | Команда |
|---|---|
| Удаление существующего правила 20 из предыдущего примера. | admin@R1# **delete load-balancing wan rule 20**<br>[edit] |
| Определение eth3 в качестве входного интерфейса для данного правила. | admin@R1# **set load-balancing wan rule 20 inbound-interface eth3**<br>[edit] |
| Определение eth1 в качестве вторичного выходного интерфейса. | admin@R1# **set load-balancing wan rule 20 interface eth1**<br>[edit] |
| Определение трафика соответствием по порту (трафик VoIP передается по порту sip) ... | admin@R1# **set load-balancing wan rule 20 destination port sip**<br>[edit] |
| ... и протоколу. | admin@R1# **set load-balancing wan rule 20 protocol tcp** |

```
[edit]
```

Разрешение трафику, проверяемому по правилам балансировки нагрузки, попробовать выйти через eth0, так как сбой проверки работоспособности может произойти вследствие проблем не на локальном канале, а на цели проверки работоспособности.

```
admin@R1# set protocols static
route 0.0.0.0/0 next-hop
12.34.56.1
[edit]
```

Фиксация настройки.

```
admin@R1# commit
[edit]
```

Отображение настройки балансировки нагрузки.

```
admin@R1# show load-balancing
wan {
     interface-health eth0 {
          failure-count 5
          nexthop 12.34.56.1
          test 10 {
               target 11.22.33.44
               type ping
          }
          test 11 {
               target 55.66.77.88
               type ping
          }
     }
     interface-health eth1 {
          failure-count 4
          nexthop 98.76.54.1
          test 10 {
               target 99.88.77.66
               type ping
          }
```

```
                    test 11 {
                        target 55.44.33.22
                        type ping
                    }
                }
                rule 10 {
                    inbound-interface eth3
                    interface eth0 {
                    }
                }
                rule 20 {
                    destination {
                        port sip
                    }
                    inbound-interface eth3
                    interface eth1 {
                    }
                    protocol tcp
                }
            }
            [edit]
```

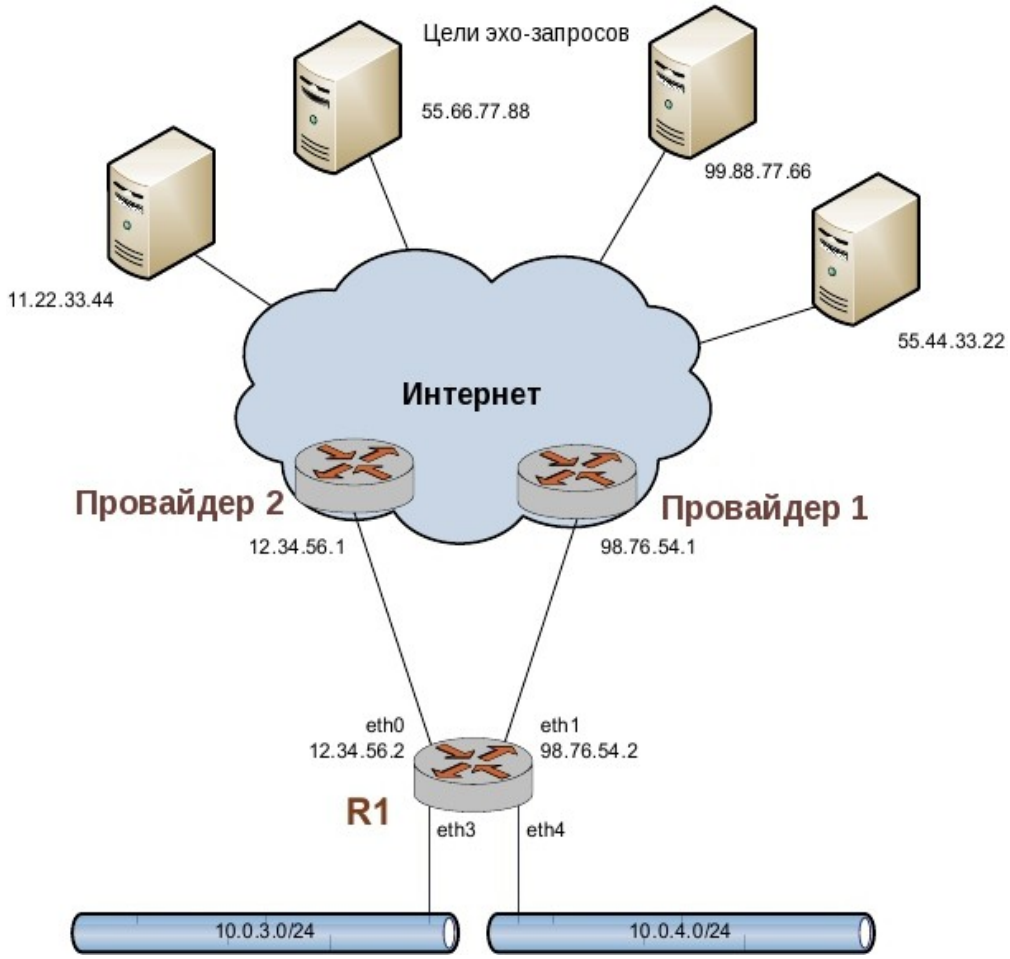
Отображение настройки статических маршрутов.

```
admin@R1# show protocols static
route 0.0.0.0/0 next-hop
12.34.56.1
[edit]
```

### 27.2.5. Исключение трафика из балансировки нагрузки

В этом примере используется настройка, почти совпадающая с настройкой из первого примера. Единственная разница состоит в том, что локальных сетей здесь не одна, а две; см. рисунок 88.

*Рисунок 88 - Балансировка нагрузки ГВС при двух локальных сетях*




На первый взгляд может показаться, что достаточно просто добавить еще одно правило для учета трафика из второго источника. Например, для балансировки нагрузки по трафику с eth4 можно было бы добавить правило, аналогичное правилу 20 в примере 27.6:

*Пример 27.6 - Добавление правила для второго источника трафика*

| Действие | Команда |
|---|---|
| Отображение настройки. | admin@R1# **show load-balancing wan rule 20**<br>inbound-interface eth4<br>interface eth0 {<br>} |

```
interface eth1 {
}
[edit]
```

Однако в этой настройке не учитывается трафик внутри ЛВС, и трафик, который должен был бы маршрутизироваться между локальными сетями, также будет направлен наружу через eth0 или eth1. Для предотвращения такой нежелательной отправки требуется дополнительное правило, исключающие применение балансировки нагрузки ко внутреннему трафику локальных сетей.

В примере 27.7 добавляется правило 5, исключающее весь трафик, направленный в любую из двух локальных сетей. В этом примере обратите внимание на запись **eth+**, используемую для ссылки на все интерфейсы Ethernet.

Следует также заметить, что данное правило исключает любые пакеты, отправленные с локальной системы и предназначенные для 10.0.0.0/8. Это необходимо при использовании балансировки нагрузки ГВС совместно со службами наподобие кэширования Интернета.

*Пример 27.7 - Добавление правила, исключающего трафик, предназначенный для локальных сетей*

| Действие | Команда |
|---|---|
| Отображение настройки. | admin@R1# **show load-balancing wan rule 5**<br>destination {<br>address 10.0.0.0/8<br>}<br>exclude<br>inbound-interface eth+<br>[edit] |

После выполнения всех команд настройка будет такой, как показано в примере 27.8.

*Пример 27.8 - Готовая настройка балансировки нагрузки ГВС*

```
admin@R1# show load-balancing
wan {
     interface-health eth0 {
```

```
        failure-count 5
        nexthop 12.34.56.1
        test 10 {
                target 11.22.33.44
                type ping
        }
        test 11 {
                target 55.66.77.88
                type ping
        }
}
interface-health eth1 {
        failure-count 4
        nexthop 98.76.54.1
        test 10 {
                target 99.88.77.66
                type ping
        }
        test 11 {
                target 55.44.33.22
                type ping
        }
}
rule 5 {
        destination {
                address 10.0.0.0/8
        }
        exclude
        inbound-interface eth+
}
rule 10 {
        inbound-interface eth3
```

```
          interface eth0 {
          }
          interface eth1 {
          }
     }
     rule 20 {
          inbound-interface eth4
          interface eth0 {
          }
          interface eth1 {
          }
     }
}
[edit]
```

## 27.3. Команды балансировки нагрузки ГВС

В этом разделе представлены следующие команды.

| Команды настройки | |
|---|---|
| Директивы обработки | |
| `load-balancing wan` | Включение балансировки нагрузки ГВС в системе. |
| `load-balancing wan disable-source-nat` | Отключение преобразования сетевых адресов отправителя для балансируемого трафика. |
| `load-balancing wan enable-local-traffic` | Включение балансировки нагрузки ГВС для трафика, отправленного с локальной системы. |
| `load-balancing wan flush-connections` | Указание системе очистить таблицу отслеживания подключений при изменении состояния подключения. |
| `load-balancing wan hook` | Указание сценария, выполняемого при |

| | |
|---|---|
| | изменениях состояния интерфейса. |
| Работоспособность интерфейсов | |
| `load-balancing wan interface-health <имя_интерфейса>` | Установка характеристик проверки работоспособности интерфейса, участвующего в балансировке нагрузки. |
| `load-balancing wan interface-health <имя_интерфейса> failure-count <число>` | Установка допустимого числа сбоев проверок работоспособности интерфейса. |
| `load-balancing wan interface-health <имя_интерфейса> nexthop <ipv4-адрес>` | Установка адреса следующего транзитного участка для проверок работоспособности интерфейса. |
| `load-balancing wan interface-health <имя_интерфейса> test <номер_теста>` | Определение теста работоспособности интерфейса. |
| `load-balancing wan interface-health <имя_интерфейса> test <номер_теста> resp-time <секунды>` | Установка максимального времени ожидания ответа, после которого объявляется о сбое сообщения проверки работоспособности. |
| `load-balancing wan interface-health <имя_интерфейса> test <номер_теста> target <узел>` | Указание адреса цели для проверки работоспособности. |
| `load-balancing wan interface-health <имя_интерфейса> test <номер_теста> ttl-limit <ограничение>` | Указание ограничения числа транзитных участков для теста по udp. |
| `load-balancing wan interface-health <имя_интерфейса> test <номер_теста> type <тип>` | Указание типа теста для проверки работоспособности интерфейса. |

| | |
|---|---|
| `load-balancing wan interface-health <имя_интерфейса> success-count <число>` | Установка числа удачных проверок работоспособности, необходимых для признания интерфейса работоспособным. |
| Правила балансировки | |
| `load-balancing wan rule <правило>` | Определение правила балансировки нагрузки ГВС. |
| `load-balancing wan rule <правило> description <описание>` | Ввод описания правила балансировки нагрузки ГВС. |
| `load-balancing wan rule <правило> destination` | Определение получателя в качестве критерия соответствия для правила балансировки нагрузки ГВС. |
| `load-balancing wan rule <правило> enable-source-based-routing` | Включение маршрутизации по отправителю для правила балансировки нагрузки ГВС. |
| `load-balancing wan rule <правило> exclude` | Исключение трафика, соответствующего правилу балансировки нагрузки ГВС, из балансировки нагрузки. |
| `load-balancing wan rule <правило> failover` | Перевод процесса балансировки нагрузки в режим перехода на резервный ресурс при сбое, при котором один интерфейс, участвующий в балансировке нагрузки, является активным, а остальные каналы — резервными. |
| `load-balancing wan rule <правило> inbound-interface <имя_интерфейса>` | Указание интерфейса, с которого приходит трафик, нагрузку по которому надо балансировать. |
| `load-balancing wan rule` | Добавление интерфейса к набору интерфейсов |

| | |
|---|---|
| | для балансировки нагрузки в правиле балансировки нагрузки ГВС. |
| `load-balancing wan rule <правило> limit` | Указание параметров ограничения скорости для правила балансировки нагрузки ГВС. |
| `load-balancing wan rule <правило> protocol <протокол>` | Указание протокола IP в качестве критерия соответствия для правила балансировки нагрузки ГВС. |
| `load-balancing wan rule <правило> source` | Указание отправителя в качестве критерия соответствия для правила балансировки нагрузки ГВС. |
| Эксплуатационные команды | |
| `restart wan-load-balance` | Перезапуск процесса балансировки нагрузки ГВС. |
| `show wan-load-balance` | Отображение сведений об интерфейсах, участвующих в балансировке нагрузки ГВС. |
| `show wan-load-balance connection` | Вывод данных о подключении, порожденных трафиком, по которому выполняется балансировка нагрузки. |
| `show wan-load-balance status` | Отображение сведений о состоянии балансировки нагрузки ГВС. |

### 27.3.1. restart wan-load-balance

Перезапуск процесса балансировки нагрузки ГВС.

**Синтаксис**

**`restart wan-load-balance`**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Команда используется для перезапуска процесса балансировки нагрузки ГВС.

## 27.3.2. load-balancing wan

Включение балансировки нагрузки ГВС в системе.

**Синтаксис**

```
set load-balancing wan
delete load-balancing wan
show load-balancing wan
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
        wan
}
```

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для включения балансировки нагрузки глобальной сети (ГВС) в системе.

Форма **set** этой команды используется для создания узла конфигурации балансировки нагрузки ГВС.

Форма **delete** этой команды используется для удаления настройки балансировки нагрузки ГВС и отключения балансировки нагрузки ГВС в системе.

Форма **show** этой команды используется для отображения указанного узла конфигурации.

### 27.3.3. load-balancing wan disable-source-nat

Отключение преобразования сетевых адресов отправителя для балансируемого трафика.

**Синтаксис**

```
set load-balancing wan disable-source-nat
delete load-balancing wan disable-source-nat
show load-balancing wan
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
        wan {
            disable-source-nat
        }
}
```

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Правила преобразования сетевых адресов отправителя создаются автоматически при изменении адреса отправителя.

**Указания по использованию**

Эта команда используется для отключения автоматического создания правил преобразования сетевых адресов отправителя (SNAT) для трафика, по которому выполняется балансировка нагрузки.

Обычно интерфейс, участвующий в балансировке нагрузки ГВС, заменяет IP-адрес отправителя в исходящем трафике своим собственным адресом, чтобы гарантировать, что ответный трафик придет на тот же интерфейс. Для этого процесс балансировки нагрузки ГВС автоматически создает правила SNAT. Эти правила SNAT характерны для балансировки нагрузки ГВС; они переписывают адрес отправителя только для трафика, по которому выполняется балансировка (то есть для трафика, соответствующего правилу балансировки нагрузки ГВС).

В некоторых ситуациях автоматическое создание правил SNAT нужно отключить — например, в случаях, когда друг к другу подключаются закрытые сети и в NAT нет необходимости, или в случаях, когда нужно задействовать другие правила SNAT вместо использования правил, автоматически созданных процессом балансировки нагрузки ГВС. После выдачи команды **load-balancing wan disable-source-nat** SNAT балансировки нагрузки ГВС на трафике, по которому балансируется нагрузка, не выполняется.

*Примечание. В том случае если требуется выполнять преобразование сетевых адресов только для некоторых потоков сетевого трафика, совместно с использованием команды **load-balancing wan disable-source-nat** может быть настроено явное преобразование адресов для заданных потоков трафика при помощи ветви конфигурации **service nat**. Подробная информация о настройке NAT приведена в разделе «Преобразование сетевых адресов (NAT)».*

Форма **set** этой команды используется для отключения SNAT на трафике, по которому балансируется нагрузка.

Форма **delete** этой команды используется для восстановления поведения по умолчанию в отношении SNAT.

Форма **show** этой команды используется для отображения настройки балансировки нагрузки ГВС.

### 27.3.4. load-balancing wan enable-local-traffic

Включение балансировки нагрузки ГВС для трафика, отправленного с локальной системы.

**Синтаксис**

```
set load-balancing wan enable-local-traffic
delete load-balancing wan enable-local-traffic
show load-balancing wan
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
        wan {
            enable-local-traffic
        }
}
```

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Трафик, отправленный с системы Altell NEO, не участвует в балансировке нагрузки ГВС.

**Указания по использованию**

Эта команда используется для включения балансировки нагрузки ГВС для трафика, отправленного с самой системы Altell NEO.

Обычно балансировка нагрузки ГВС может выполняться только по трафику, проходящему через систему Altell NEO. Установка данного параметра позволяет выполнять балансировку нагрузки ГВС как по проходящему трафику, таки по трафику, исходящему с самой системы Altell NEO.

Форма **set** этой команды используется для включения балансировки нагрузки ГВС по трафику, исходящему с локальной системы.

Форма **delete** этой команды используется для восстановления поведения по умолчанию для трафика, исходящего с локальной системы.

Форма **show** этой команды используется для отображения настройки балансировки нагрузки ГВС.

## 27.3.5. load-balancing wan flush-connections

Указание системе очистить таблицу отслеживания подключений при изменении состояния подключения.

**Синтаксис**

```
set load-balancing wan flush-connections
```

**delete load-balancing wan flush-connections**

**show load-balancing wan**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
        wan {
            flush-connections
        }
}
```

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Таблица отслеживания подключений не очищается при изменении состояния подключений.

**Указания по использованию**

Эта команда используется для выдачи указания системе очистить таблицу отслеживания подключений при изменении состояния любого подключения. Очищается вся таблица отслеживания подключений.

В таблице отслеживания подключений могут накапливаться неактуальные элементы — например, когда объявление DHCP вызывает изменение адреса для интерфейса, участвующего в балансировке, или когда происходит сбой такого интерфейса. При включении отслеживания подключений система получает указание очищать таблицу, когда состояние подключения изменяется подобным образом.

Следует заметить, что если включен такой режим, при изменении состояния любого интерфейса очищается вся таблица отслеживания подключений. При этом удаляются элементы для потоков, отличных от изменившегося, в том числе для установившихся и активных потоков.

В результате система не создает нового элемента в таблице отслеживания подключений до установления нового подключения в потоке (здесь поток — это кортеж из адреса отправителя, адреса получателя, IP-адреса и порта). До

этого момента ранее установившиеся потоки балансируются не на основе потоков, а на основе пакетов.

***ПРИМЕЧАНИЕ.*** *Эта функция не может использоваться совместно с режимом поддерживающего состояние перехода на резервный ресурс при сбое, так как в таком режиме для поддержания состояния и его синхронизации с резервными компонентами используется тот же самый механизм отслеживания подключений.*

Форма **set** этой команды используется для включения очистки таблицы отслеживания подключений.

Форма **delete** этой команды используется для восстановления поведения по умолчанию в отношении таблицы отслеживания подключений.

Форма **show** этой команды используется для отображения настройки балансировки нагрузки ГВС.

### 27.3.6. load-balancing wan hook <имя_сценария>

Указание сценария, выполняемого при изменениях состояния интерфейса.

**Синтаксис**

**set load-balancing wan hook** *имя_сценария*

**delete load-balancing wan hook**

**show load-balancing wan hook**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
        wan {
            hook текст
        }
}
```

Параметры

*имя_сценария*

Путь и имя файла сценария, который должен выполняться при изменении состояния интерфейса.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для указания имени файла сценария, который должен выполняться при каждом изменении состояния каждого интерфейса.

Сценарию доступны две переменные среды:

- WLB_INTERFACE_NAME=[имя_интерфейса] — интерфейс, за состоянием которого происходит наблюдение.
- WLB_INTERFACE_STATE=[ACTIVE|FAILED] — состояние интерфейса.

> ***ПРИМЕЧАНИЕ*** *Это блокирующий вызов, так что если выхода из сценария не происходит, то процесс балансировки нагрузки ГВС переходит в состояние ожидания навсегда, вследствие чего система перестает реагировать на запросы.*

Форма **set** этой команды используется для указания имени сценария, который должен выполняться при изменении состояния интерфейса.

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

Форма **show** этой команды используется для отображения настроенного имени сценария.

## 27.3.7. load-balancing wan interface-health <имя_интерфейса>

Установка характеристик проверки работоспособности интерфейса, участвующего в балансировке нагрузки.

**Синтаксис**

**set load-balancing wan interface-health** *имя_интерфейса*

**delete load-balancing wan interface-health** *имя_интерфейса*

**show load-balancing wan interface-health** *имя_интерфейса*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
        wan {
            interface-health текст
        }
}
```

**Параметры**

*имя_интерфейса*

Обязательный. Множественный узел. Имя физического или логического интерфейса. Это участвующий в балансировке нагрузки интерфейс, за состоянием работоспособности которого требуется наблюдать.

Проверку работоспособности можно определить для всех интерфейсов, участвующих в балансировке нагрузки, создав несколько узлов конфигурации **interface-health**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для установки характеристик проверки работоспособности выходного интерфейса, участвующего в балансировке нагрузки.

Форма **set** этой команды используется для включения проверки работоспособности на интерфейсе.

Форма **delete** этой команды используется для удаления проверки работоспособности на интерфейсе.

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

## 27.3.8. load-balancing wan interface-health <имя_интерфейса> failure-count <число>

Установка допустимого числа сбоев проверок работоспособности интерфейса.

**Синтаксис**

**set load-balancing wan interface-health** *имя_интерфейса* **failure-count** *число*

**delete load-balancing wan interface-health** *имя_интерфейса* **failure-count**

**show load-balancing wan interface-health** *число* **failure-count**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
        wan {
            interface-health текст {
                failure-count целоебеззнака32разр
            }
        }
}
```

**Параметры**

*имя_интерфейса*

Обязательный. Имя физического или логического интерфейса.

*число*

Максимальное допустимое число закончившихся сбоем проверок работоспособности, после которых интерфейс считается недоступным. Значение должно лежать в диапазоне от 1 до 10. Значение по умолчанию равно 1.

**Значение по умолчанию**

Если интерфейс не отвечает на запрос при одной проверке работоспособности, он считается недоступным.

**Указания по использованию**

Эта команда используется для установки числа сбоев при проверке работоспособности интерфейса. Число сбоев — это число последовательных сбоев эхо-запроса, необходимое для удаления интерфейса из пула активных интерфейсов, участвующих в балансировке нагрузки.

Форма **set** этой команды используется для установки числа сбоев.

Форма **delete** этой команды используется для восстановления значения

числа сбоев по умолчанию.

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

### 27.3.9. load-balancing wan interface-health <имя_интерфейса> nexthop <ipv4-адрес>

Установка адреса следующего транзитного участка для проверок работоспособности интерфейса.

**Синтаксис**

**set load-balancing wan interface-health** *имя_интерфейса* **nexthop** *ipv4-адрес*

**delete load-balancing wan interface-health** *имя_интерфейса* **nexthop**

**show load-balancing wan interface-health** *имя_интерфейса* **nexthop**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
        wan {
            interface-health текст {
                nexthop ipv4-адрес
            }
        }
}
```

**Параметры**

*имя_интерфейса*

Обязательный. Имя физического или логического интерфейса.

*ipv4-адрес*

IPv4-адрес следующего транзитного участка для проверок работоспособности интерфейса или ключевое слово **dhcp**, дающее системе указание получить IP-адрес от сервера DHCP.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для установки IPv4-адреса следующего транзитного участка, используемого в проверках работоспособности интерфейса.

Если адрес следующего транзитного участка указан с помощью ключевого слова **dhcp**, IP-адрес следующего транзитного участка будет получен из объявления DHCP. В этом случае применимое правило SNAT и таблица маршрутизации автоматически обновляются при выполнении нового назначения DHCP.

Форма **set** этой команды используется для указания IPv4-адреса следующего транзитного участка.

Форма **delete** этой команды используется для удаления IPv4-адреса следующего транзитного участка.

Форма **show** этой команды используется для отображения настройки следующего транзитного участка.

## 27.3.10. load-balancing wan interface-health <имя_интерфейса> test <номер_теста>

Определение теста работоспособности интерфейса.

**Синтаксис**

**set load-balancing wan interface-health** *имя_интерфейса* **test** *номер_теста*

**delete load-balancing wan interface-health** *имя_интерфейса* **test**

**show load-balancing wan interface-health** *имя_интерфейса* **test**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
        wan {
```

```
                    interface-health текст {
                        test целоебеззнака32разр {
                        }
                    }
                }
            }
```

**Параметры**

*имя_интерфейса*

Имя физического или логического интерфейса.

*номер_теста*

Идентификатор теста.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для определения теста работоспособности интерфейса. 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 данного интерфейса 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.

## 27.3.11. load-balancing wan interface-health <имя_интерфейса> test <номер_теста> resp-time <секунды>

Установка максимального времени ожидания ответа, после которого объявляется о сбое сообщения проверки работоспособности.

**Синтаксис**

```
set load-balancing wan interface-health имя_интерфейса
test номер_теста resp-time секунды
```

**delete load-balancing wan interface-health** *имя_интерфейса* **test** *номер_теста* **resp-time**

**show load-balancing wan interface-health** *имя_интерфейса* **test** *номер_теста* **resp-time**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
        wan {
            interface-health текст {
                test целоебеззнака32разр {
                    resp-time целоебеззнака32разр
                }
            }
        }
}
```

**Параметры**

*имя_интерфейса*

Имя физического или логического интерфейса.

*номер_теста*

Идентификатор теста.

*секунды*

Число секунд ожидания отклика на эхо-запрос, после которого объявляется о сбое эхо-запроса. Значение должно лежать в диапазоне от 1 до 30. Значение по умолчанию равно 5.

**Значение по умолчанию**

Если сообщение эхо-ответа ICMP не получено в течение 5 секунд, 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. На тестовый интерфейс отправляются эхо-запросы,

если для параметра **type** установлено значение **ping**.

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.

## 27.3.12. load-balancing wan interface-health <имя_интерфейса> test <номер_теста> target <узел>

Указание целевого узла для проверки работоспособности.

**Синтаксис**

**set load-balancing wan interface-health** *имя_интерфейса* **test** *номер_теста* **target** *узел*

**delete load-balancing wan interface-health** *имя_интерфейса* **test** *номер_теста* **target**

**show load-balancing wan interface-health** *имя_интерфейса* **test** *номер_теста* **target**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
        wan {
            interface-health текст {
                test целоебеззнака32разр {
                    target текст
                }
            }
        }
}
```

**Параметры**

*имя_интерфейса*

Имя физического или логического интерфейса.

*номер_теста*

Идентификатор теста.

*узел*

IPv4-адрес или имя узла цели проверки работоспособности интерфейса.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для настройки получателя сообщений эхо-запроса, отправляемых при проверке работоспособности интерфейса. 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-запроса, отправляемых при проверке работоспособности интерфейса.

Форма **delete** этой команды используется для удаления получателя сообщений эхо-запроса, отправляемых при проверке работоспособности интерфейса.

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

## 27.3.13. load-balancing wan interface-health <имя_интерфейса> test <номер_теста> ttl-limit <ограничение>

Указание ограничения числа транзитных участков для теста по udp.

**Синтаксис**

**set load-balancing wan interface-health** *имя_интерфейса* **test** *номер_теста* **ttl-limit** *ограничение*

**delete load-balancing wan interface-health** *имя_интерфейса* **test** *номер_теста* **ttl-limit**

**show load-balancing wan interface-health** *имя_интерфейса* **test** *номер_теста* **ttl-limit**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
```

```
                wan {
                     interface-health текст {
                          test целоебеззнака32разр {
                               ttl-limit целоебеззнака32разр
                          }
                     }
                }
          }
```

**Параметры**

*имя_интерфейса*

Имя физического или логического интерфейса.

*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 в тестах при проверке работоспособности по UDP.

Помимо тестов по эхо-запросам, можно выполнять и тесты по UDP. В таких тестах на цель отправляется пакет UDP с ограничением по времени жизни (ttl). Чтобы тест был успешным, ограничение по ttl должно быть 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 по UDP.

Форма **delete** этой команды используется для удаления ограничения числа транзитных участков.

Форма **show** этой команды используется для отображения настройки ttl-limit.

### 27.3.14. load-balancing wan interface-health <имя_интерфейса> test <номер_теста> type <тип>

Указание типа теста для проверки работоспособности интерфейса.

**Синтаксис**

**set load-balancing wan interface-health** *имя_интерфейса* **test** *номер_теста* **type [ping | ttl]**

**delete load-balancing wan interface-health** *имя_интерфейса* **test** *номер_теста* **type**

**show load-balancing wan interface-health** *имя_интерфейса* **test** *номер_теста* **type**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
        wan {
            interface-health текст {
                test целоебеззнака32разр {
                    type [ping|ttl]
                }
            }
        }
    }
```

**Параметры**

*имя_интерфейса*

Имя физического или логического интерфейса.

*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.

Форма **set** этой команды используется для указания выполняемого типа теста проверки работоспособности.

Форма **delete** используется для удаления настройки типа теста.

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

## 27.3.15. load-balancing wan interface-health <имя_интерфейса> success-count <число>

Установка числа удачных проверок работоспособности, необходимых для признания интерфейса работоспособным.

**Синтаксис**

**set load-balancing wan interface-health** *имя_интерфейса* **success-count** *число*

**delete load-balancing wan interface-health** *имя_интерфейса* **success-count**

**show load-balancing wan interface-health** *имя_интерфейса* **success-count**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
        wan {
            interface-health текст {
                success-count целоебеззнака32разр
            }
        }
}
```

**Параметры**

*имя_интерфейса*

Обязательный. Имя физического или логического интерфейса.

*число*

Число последовательных успешных откликов в тестах, необходимое для признания интерфейса работоспособным. Значение должно лежать в диапазоне от 1 до 10. Значение по умолчанию равно 1.

**Значение по умолчанию**

Если на интерфейсе успешно выполняется один тестовый цикл, он возвращается в пул активных интерфейсов, участвующих в балансировке нагрузки.

**Указания по использованию**

Эта команда используется для установки числа последовательных успешных откликов на эхо-запросы ICMP, необходимых для возвращения интерфейса в пул активных интерфейсов, участвующих в балансировке нагрузки.

Форма **set** этой команды используется для указания числа успешных запросов.

Форма **delete** этой команды используется для восстановления числа успешных эхо-запросов по умолчанию.

Форма **show** этой команды используется для отображения настройки числа успешных эхо-запросов.

## 27.3.16. load-balancing wan rule <правило>

Определение правила балансировки нагрузки ГВС.

**Синтаксис**

**set load-balancing wan rule** *правило*

**delete load-balancing wan rule** *правило*

**show load-balancing wan rule** *правило*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
```

```
            wan {
                rule целоебеззнака32разр {
                }
            }
        }
```

**Параметры0**

*правило*

Обязательный. Множественный узел. Уникальный номер, определяющий правило. Значение должно лежать в диапазоне от 1 до 4294967295.

Можно определить несколько правил балансировки нагрузки, создав несколько узлов конфигурации **rule**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для определения правила балансировки нагрузки ГВС.

После настройки номера правил изменить нельзя. По этой причине рекомендуется настраивать правила с интервалами в номерах (например, правило 5, правило 10, правило 15 и т.д.) на случай необходимости вставки правила в будущем.

Форма **set** этой команды используется для создания правила балансировки нагрузки. Следует заметить, что для изменения номера существующего правила нельзя использовать команду **set**. Для изменения номера правила следует удалить его и создать заново.

Форма **delete** этой команды используется для удаления правила балансировки нагрузки.

Форма **show** этой команды используется для отображения настройки правила балансировки нагрузки.

## 27.3.17. load-balancing wan rule <правило> description <описание>

Ввод описания правила балансировки нагрузки ГВС.

**Синтаксис**

**set load-balancing wan rule** *правило* **description** *описание*

**delete load-balancing wan rule** *правило* **description**

**show load-balancing wan rule** *правило* **description**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
        wan {
            rule целоебеззнака32разр {
                description текст
            }
        }
}
```

**Параметры**

*правило*

Обязательный. Номер настраиваемого правила.

*описание*

Описание правила балансировки нагрузки ГВС.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для ввода описания правила балансировки нагрузки ГВС.

Форма **set** этой команды используется для указания описания правила балансировки нагрузки ГВС.

Форма **delete** этой команды используется для удаления описания правила балансировки нагрузки ГВС.

Форма **show** этой команды используется для отображения описания правила балансировки нагрузки ГВС.

## 27.3.18. load-balancing wan rule <правило> destination

Определение получателя в качестве критерия соответствия для правила балансировки нагрузки ГВС.

**Синтаксис**

**set load-balancing wan rule** *правило* **destination {address** *адрес* **| port** *порт***}**

**delete load-balancing wan rule** *правило* **destination [address | port]**

**show load-balancing wan rule** *правило* **destination**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
        wan {
            rule целоебеззнака32разр {
                destination {
                    address текст
                    port текст
                }
            }
        }
}
```

**Параметры**

*правило*

Обязательный. Номер настраиваемого правила.

*адрес*

Адрес получателя для проверки соответствия. Поддерживаются следующие форматы:

*ip-адрес*: IPv4-адрес.

*ip-адрес/префикс*: Адрес подсети, причем 0.0.0.0/0 соответствует любой сети.

*ip-адрес–ip-адрес*: Диапазон последовательных IP-адресов; например,

192.168.1.1–192.168.1.150.

**!***ip-адрес*: Соответствует всем IP-адресам, кроме одного указанного.

**!***ip-адрес/префикс*: Соответствует всем адресам подсетей, кроме одного указанного.

**!***ip-адрес–ip-адрес*: Соответствует всем IP-адресам, кроме находящихся в указанном диапазоне.

Необходимо указать ровно один параметр — либо **адрес**, либо **порт**.

*порт*

Применимо только к протоколам TCP или UDP. Порт получателя для проверки соответствия. Поддерживаются следующие форматы:

*имя_порта*: Соответствует имени службы IP; например, **http**. Можно указывать любое имя службы из файла **/etc/services**.

*номер_порта*: Соответствует номеру порта. Значение должно лежать в диапазоне от 1 до 65535.

*начало–конец*: Соответствует указанному диапазону портов; например, 1001–1005.

Допускается использовать сочетание указанных форматов в списке через запятую. Кроме того, можно построить дополнение для всего списка, поставив перед ним восклицательный знак (“**!**”); например, **! 22,telnet,http,123,1001-1005**.

Необходимо указать ровно один параметр — либо **адрес**, либо **порт**.

**Значение по умолчанию**

Если параметр не установлен либо если узел конфигурации **destination** создается без атрибутов, пакет соответствует любому получателю.

**Указания по использованию**

Эта команда используется для определения условия соответствия по адресу получателя в правиле балансировки нагрузки.

Можно проверять соответствие для пакетов по получателю, представленному IP-адресом или портом.

Форма **set** этой команды используется для указания получателя, соответствие которому должно проверяться.

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

получателя.

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

### 27.3.19. load-balancing wan rule <правило> enable-source-based-routing

Включение маршрутизации по отправителю для правила балансировки нагрузки ГВС.

**Синтаксис**

**set load-balancing wan rule** *правило* **enable-source-based-routing**

**delete load-balancing wan rule** *правило* **enable-source-based-routing**

**show load-balancing wan rule** *правило*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
        wan {
            rule целоебеззнака32разр {
                enable-source-based-routing
            }
        }
}
```

**Параметры**

*правило*

Обязательный. Номер настраиваемого правила.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для включения маршрутизации по отправителю (называемой также маршрутизацией на основе политик) при балансировке нагрузки.

Обычно в системе Altell NEO балансировка нагрузки выполняется по

потокам на основе кортежа из адреса отправителя, адреса получателя и порта. Первый пакет потока инициирует подключение, а последующие пакеты, соответствующие кортежу потока, направляются на тот же интерфейс. Балансировка нагрузки по потокам помогает предотвратить проблемы, связанные с передачей пакетов вне порядка их отправки; например, в случаях, когда один канал в наборе намного быстрее или медленнее других каналов в том же наборе. (Передача пакетов вне порядка их отправки может повлиять на производительность вследствие обработки, необходимой для повторной сборки потока.)

В некоторых ситуациях — например, в ситуациях, когда порядок следования пакетов не существенен, — балансировка по потокам не требуется; достаточно балансировки по пакетам (то есть просто равномерного случайного распределения). При отключении балансировки по потокам передача пакетов может стать более экономичной; кроме того, балансировка пакетов может улучшиться.

Форма **set** этой команды используется для включения маршрутизации по отправителю.

Форма **delete** этой команды используется для отключения маршрутизации по отправителю.

Форма **show** этой команды используется для отображения настройки балансировки нагрузки ГВС.

## 27.3.20. load-balancing wan rule <правило> exclude

Исключение трафика, соответствующего правилу балансировки нагрузки ГВС, из балансировки нагрузки.

**Синтаксис**

**set load-balancing wan rule** *правило* **exclude**

**delete load-balancing wan rule** *правило* **exclude**

**show load-balancing wan rule** *правило*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
        wan {
            rule целоебеззнака32разр {
                exclude
            }
        }
}
```

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Трафик, соответствующий указанным в правиле характеристикам, участвует в балансировке нагрузки.

**Указания по использованию**

Эта команда используется для определения правила исключения, исключающего трафик из балансировки нагрузки.

Трафик, соответствующий указанным в правиле характеристикам, не участвует в балансировке нагрузки, а маршрутизируется обычным образом.

Форма **set** этой команды используется для исключения трафика, соответствующего правилу, из балансировки нагрузки.

Форма **delete** этой команды используется для восстановления поведения балансировки нагрузки по умолчанию.

Форма **show** этой команды используется для отображения настройки правила балансировки нагрузки ГВС.

## 27.3.21. load-balancing wan rule <правило> failover

Перевод процесса балансировки нагрузки в режим перехода на резервный ресурс при сбое, при котором один интерфейс, участвующий в балансировке нагрузки, является активным, а остальные каналы — резервными.

**Синтаксис**

**set load-balancing wan rule** *правило* **failover**

**delete load-balancing wan rule** *правило* **failover**

**show load-balancing wan rule** *правило*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
        wan {
            rule целоебеззнака32разр {
                failover
            }
        }
}
```

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Для балансировки трафика используются все каналы, настроенные на балансировку нагрузки.

**Указания по использованию**

Эта команда используется, чтобы выдать системе указание перевести процесс балансировки нагрузки в режим перехода на резервный ресурс при сбое. В режиме перехода на резервный ресурс при сбое один канал из участвующих в балансировке нагрузки выбирается системой в качестве активного канала; оставшиеся каналы, участвующие в балансировке нагрузки, резервируются в качестве горячего или холодного резерва на случай прерывания подключения по активному каналу.

Активный канал выбирается системой по настроенному весу и достижимости цели с интерфейса. Для передачи трафика используется только активный канал. Если активный канал выходит из строя, активным каналом становится интерфейс со следующим по величине сочетанием веса и достижимости.

Форма **set** этой команды используется для включения режима перехода на резервный ресурс при сбое.

Форма **delete** этой команды используется для восстановления поведения

балансировки нагрузки по умолчанию.

Форма **show** этой команды используется для отображения настройки правила балансировки нагрузки ГВС.

## 27.3.22. load-balancing wan rule <правило> inbound-interface <имя_интерфейса>

Указание интерфейса, с которого приходит трафик, нагрузку по которому надо балансировать.

**Синтаксис**

**set load-balancing wan rule** *правило* **inbound-interface** *имя_интерфейса*

**delete load-balancing wan rule** *правило* **inbound-interface** *имя_интерфейса*

**show load-balancing wan rule** *правило* **inbound-interface**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
        wan {
            rule целоебеззнака32разр {
                inbound-interface текст
            }
        }
}
```

**Параметры**

*правило*

Обязательный. Номер настраиваемого правила.

*имя_интерфейса*

Обязательный. Интерфейс, с которого должен приходить трафик для балансировки нагрузки.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для определения интерфейса, с которого должен приходить трафик для балансировки нагрузки.

Форма **set** этой команды используется для указания интерфейса, с которого должен приходить трафик для балансировки нагрузки.

Форма **delete** этой команды используется для удаления входного интерфейса их правила балансировки нагрузки.

Форма **show** этой команды используется для отображения настройки входного интерфейса в правиле балансировки нагрузки.

## 27.3.23. load-balancing wan rule <правило> interface <имя_интерфейса>

Добавление интерфейса к набору интерфейсов для балансировки нагрузки в правиле балансировки нагрузки ГВС.

**Синтаксис**

**set load-balancing wan rule** *правило* **interface** *имя_интерфейса* **[weight** *число***]**

**delete load-balancing wan rule** *правило* **interface** *имя_интерфейса* **[weight]**

**show load-balancing wan rule** *правило* **interface** *имя_интерфейса* **[weight]**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
        wan {
            rule целоебеззнака32разр {
                interface текст {
                    weight 1-255
                }
            }
        }
    }
```

**Параметры**

*правило*

Обязательный. Номер настраиваемого правила.

*имя_интерфейса*

Обязательный. Имя физического или логического интерфейса.

*вес*

Вес, связываемый с интерфейсом и представляющий долю пакетов, распределяемую на этот интерфейс. Значение должно лежать в диапазоне от 1 до 255. Значение по умолчанию равно 1.

**Значение по умолчанию**

Каждому интерфейсу назначается вес 1.

**Указания по использованию**

Эта команда используется для добавления интерфейса к набору интерфейсов, участвующих в балансировке нагрузки, в правиле балансировки нагрузки ГВС. Когда исходящий пакет соответствует правилу балансировки нагрузки, он отправляется наружу через один из интерфейсов, указанных в наборе, как определено алгоритмом балансировки нагрузки.

Форма **set** этой команды используется для добавления интерфейса в правило балансировки нагрузки или для изменения балансировочного веса интерфейса.

Форма **delete** этой команды используется для удаления интерфейса из правила балансировки нагрузки или для восстановления веса интерфейса по умолчанию.

Форма **show** этой команды используется для отображения настройки интерфейсов в правиле балансировки нагрузки.

## 27.3.24. load-balancing wan rule <правило> limit

Указание параметров ограничения скорости для правила балансировки нагрузки ГВС.

**Синтаксис**

```
set load-balancing wan rule правило limit {burst серия |
period [second | minute | hour] | rate скорость |
threshold [above | below]}

delete load-balancing wan rule правило limit [burst |
```

**period | rate | threshold]**

**show load-balancing wan rule** *правило* **limit [burst | period | rate | threshold]**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
        wan {
            rule целоебеззнака32разр {
                limit {
                    burst целоебеззнака32разр
                    period [second|minute|hour]
                    rate целоебеззнака32разр
                    threshold [above|below]
                }
            }
        }
}
```

**Параметры**

*правило*

Номер настраиваемого правила.

*серия*

Число пакетов сверх ограничения, разрешенных за указанный период. Значение по умолчанию равно 5.

*период*

Окно времени для расчета скорости. Поддерживаются следующие значения:

**second**: Одна секунда

**minute**: Одна минута

**hour**: Один час

Значение по умолчанию — **second**.

*скорость*

Число пакетов, используемое для ограничения скорости. Значение по

умолчанию равно 5.

*порог*

Тип порога (верхний или нижний) для ограничения. Поддерживаются следующие значения:

**above**: Правило применяется к пакетам сверх ограничения

**below**: правило применяется к пакетам ниже ограничения

Значение по умолчанию — **below**.

**Значение по умолчанию**

Ограничения не применяются.

**Указания по использованию**

Эта команда используется для установки ограничения скорости, при котором активируется правило. Оно может интерпретироваться как “Применить правило к трафику ниже (или выше) данной скорости. Кроме того, разрешить серии из x пакетов за единицу времени выше (ниже) этой скорости.”

Форма **set** этой команды используется для указания параметров ограничения скорости в правиле балансировки нагрузки ГВС.

Форма **delete** этой команды используется для удаления параметров ограничения скорости в правиле балансировки нагрузки ГВС.

Форма **show** этой команды используется для отображения параметров ограничения скорости в правиле балансировки нагрузки ГВС.

## 27.3.25. load-balancing wan rule <правило> protocol <протокол>

Указание протокола IP в качестве критерия соответствия для правила балансировки нагрузки ГВС.

**Синтаксис**

**set load-balancing wan rule** *правило* **protocol** *протокол*

**delete load-balancing wan rule** *правило* **protocol** *протокол*

**show load-balancing wan rule** *правило* **protocol** *протокол*

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
        wan {
            rule целоебеззнака32разр {
                protocol текст
            }
        }
}
```

**Параметры**

*правило*

Обязательный. Номер настраиваемого правила.

*протокол*

Сетевой протокол (протоколы), для которого осуществляется балансировка нагрузки. Могут быть использованы любые наименования протоколов или их номера, определенные в файле **/etc/protocols**. Кроме того, поддерживается ключевое слово **all**.

При указании перед названием протокола восклицательного знака (“**!**”) соответствие будет установлено для любого протокола, кроме указанного. Например, при указании **!tcp** соответствие будет установлено для всех протоколов, кроме TCP.

**Значение по умолчанию**

Правилу соответствуют все протоколы.

**Указания по использованию**

Эта команда используется для указания протокола (протоколов), на котором должно определяться соответствие.

Заметим, что при использовании сочетания двух и более правил “исключения” (то есть правил, в которых используется операция отрицания “**!**”) следует соблюдать осторожность. Правила балансировки нагрузки обрабатываются последовательно, и последовательность правил исключения может привести к непредсказуемому поведению.

Форма **set** этой команды используется для указания протокола, соответствие которому должно проверяться.

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

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

## 27.3.26. load-balancing wan rule <правило> source

Указание отправителя в качестве критерия соответствия для правила балансировки нагрузки ГВС.

**Синтаксис**

**set load-balancing wan rule** *правило* **source {address** *адрес* **| port** *порт***}**

**delete load-balancing wan rule** *правило* **source {address | port}**

**show load-balancing wan rule** *правило* **source**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
load-balancing {
        wan {
            rule целоебеззнака32разр {
                source {
                    address текст
                    port текст
                }
            }
            }
}
```

**Параметры**

*правило*

Обязательный. Номер настраиваемого правила.

*адрес*

Адрес получателя для проверки соответствия. Поддерживаются следующие

форматы:

*ip-адрес*: IPv4-адрес.

*ip-адрес/префикс*: Адрес подсети, причем 0.0.0.0/0 соответствует любой сети.

*ip-адрес–ip-адрес*: Диапазон последовательных IP-адресов; например, 192.168.1.1–192.168.1.150.

**!***ip-адрес*: Соответствует всем IP-адресам, кроме одного указанного.

**!***ip-адрес/префикс*: Соответствует всем адресам подсетей, кроме одного указанного.

**!***ip-адрес–ip-адрес*: Соответствует всем IP-адресам, кроме находящихся в указанном диапазоне.

Необходимо указать ровно один параметр — либо **адрес**, либо **порт**.

*порт*

Применимо только к протоколам TCP или UDP. Порт получателя для проверки соответствия. Поддерживаются следующие форматы:

*имя_порта*: Соответствует имени службы IP; например, **http**. Можно указывать любое имя службы из файла **/etc/services**.

*номер_порта*: Соответствует номеру порта. Значение должно лежать в диапазоне от 1 до 65535.

*начало–конец*: Соответствует указанному диапазону портов; например, 1001–1005.

Допускается использовать сочетание указанных форматов в списке через запятую. Кроме того, можно построить дополнение для всего списка, поставив перед ним восклицательный знак (“**!**”); например, **! 22,telnet,http,123,1001-1005**.

Необходимо указать ровно один параметр — либо **адрес**, либо **порт**.

**Значение по умолчанию**

Если параметр не установлен либо если узел конфигурации **source** создается без атрибутов, пакет соответствует любому отправителю.

**Указания по использованию**

Эта команда используется для определения критерия соответствия по адресу отправителя в правиле балансировки нагрузки.

Проверять соответствие пакетов можно по отправителю, представленному IP-адресом или портом.

Форма **set** этой команды используется для указания отправителя, соответствие которому должно проверяться.

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

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

## 27.3.27. show wan-load-balance

Отображение сведений об интерфейсах, участвующих в балансировке нагрузки ГВС.

**Синтаксис**

```
show wan-load-balance
```

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для вывода сведений о интерфейсах, участвующих в балансировке нагрузки ГВС. Команда отображает сведения для каждого интерфейса, участвующего в балансировке, и выдает отчет о текущем состоянии, в том числе время последней смены состояния интерфейса с активного на сбойный или со сбойного на активный.

Кроме того, команда выводит типы и цели тестов (в порядке настроенных номеров тестов). Символ в начале строки представляет состояние теста следующим образом:

+

Последний тест был успешным.

-

Последний тест завершился сбоем.

*

Тест не выполнялся.

**Примеры**

В примере 27.9 приведены сведения о балансировке нагрузки ГВС, выполняемой на интерфейсах eth0 и eth1.

*Пример 27.9 - Отображение сведений об интерфейсах, участвующих в балансировке нагрузки*

```
admin@neo:~$show wan-load-balance
Interface:     eth0
  Status: active
  Last Status Change:    Fri May 15 13:38:39 2009
  -Test:  Ping Target:   192.168.0.120
  +Test:  ttl  Target:   192.168.0.1
    Last Interface Success:
     0s
    Last Interface Failure:
     35s
    # Interface Failure(s):
     10


Interface:     eth1
  Status: active
  Last Status Change:    Fri May 15 13:38:39 2009
  +Test:  Ping Target:   192.168.0.1
  *Test:  Ping Target:   192.168.0.120
    Last Interface Success:
     10s
    Last Interface Failure:
     0s
```

```
# Interface Failure(s):
 0
```

## 27.3.28. show wan-load-balance connection

Вывод данных о подключении, порожденных трафиком, по которому выполняется балансировка нагрузки.

**Синтаксис**

**show wan-load-balance connection**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для вывода сведений о подключении, касающихся трафика, по которому балансируется нагрузка.

**Примеры**

В примере 27.10 приведены сведения о подключениях, участвующих в балансировке нагрузки ГВС.

*Пример 27.10 - Отображение сведений о подключении, касающихся балансировки нагрузки*

```
admin@neo:~$show wan-load-balance connection

Type State     Src  Dst  Packets
     Bytes

tcp  estab     172.16.117.1:123
     172.16.117.2:123    1
     11

icmp           172.16.117.1
          172.16.117.2
     1    11
```

## 27.3.29. show wan-load-balance status

Отображение сведений о состоянии балансировки нагрузки ГВС.

**Синтаксис**

**show wan-load-balance status**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда используется для вывода сведений о состоянии балансировки нагрузки ГВС.

**Примеры**

В примере 27.11 приведены сведения о балансировке нагрузки ГВС, выполняемой на интерфейсах eth0 и eth1.

*Пример 27.11 - Отображение состояния балансировки нагрузки*

```
admin@neo:~$show wan-load-balance status

Chain PREROUTING (policy ACCEPT 1415 packets, 96338
bytes)

pkts bytes target   prot opt in
     out source     destination

0    0     ISP_1    tcp  -
     any  any anywhere   anywhere multiport dports 223

           state    NEW  statistic mode random
probability 0.500000

0    0     ISP_2    tcp  -
     any  any anywhere   anywhere multiport dports 223
```

# 28. КЛАСТЕРИЗАЦИЯ

В этой главе описана настройка Altell NEO для построения на его основе отказоустойчивого кластера за счёт избыточности (и устройств, и служб).

## 28.1. Обзор реализации

В рамках подхода Altell NEO избыточность обеспечивается включением нескольких устройств в группу (кластер), в пределах которой обеспечивается обмен информацией о состоянии между устройствами и поддерживается единая, цельная конфигурация резервируемых служб. Взаимодействие кластерного ПО со службами происходит посредством так называемых «агентов ресурсов» — небольших программ, обычно написанных на интерпретируемых языках (чаще всего это язык командного интерпретатора системы). Каждый агент написан под конкретную службу и осуществляет запуск этой службы, её остановку и проверку состояния. Все агенты ресурсов поддерживают единый программный интерфейс, позволяющий кластерному ПО не заботиться об особенностях управления конкретной службой.

Отказоустойчивость служб обеспечивается кластером за счёт избыточности (дублирования служб, операционных систем и аппаратных устройств), постоянного наблюдения за состоянием, быстрого переключения и/или перезапуска в случае краха. Состояние кластера определяется поведением и составом компонент кластера относительно его действующей конфигурации, поэтому при отклонениях от неё кластерное ПО рассчитывает новое максимально близкое к исходному («идеальное» в текущих условиях) состояние и способы его достижения.

В рамках системы Altell NEO поддерживаются кластеры только из двух устройств, работающие по схеме «ведущий-ведомый».

### 28.1.1. Строение кластера

В реализации Altell NEO схемы «ведущий-ведомый» кластер включает в себя два устройства, исполняющих несколько ролей — «ведущий», «ведомый» и «узел наблюдения». При этом каждое устройство не может одновременно быть и ведущим, и ведомым, но может совмещать одну из этих ролей с ролью «узел наблюдения».

Ведущее устройство исполняет кластерное ПО, содержит у себя основную (главную)

копию конфигурации кластера, занимается вычислением нового идеального состояния и способа его достижения и выдаёт управляющие инструкции, исполнение которых кластером приводит его к новому идеальному состоянию. Ведомое устройство также исполняет кластерное ПО и при обнаружении краха ведущего устройства может запустить механизм выборов («election») и в случае их успеха для себя стать ведущим. Также на ведомом устройстве могут быть запущены сбоящие службы ведущего устройства, если кластерное ПО решит, что это необходимо для достижения нового идеального состояния кластера. Запуск службы на другом устройстве либо в ответ на её сбой на исходном устройстве, либо принудительно администратором называется переходом (переносом, перемещением) службы, при этом физического переноса каких-то файлов, напрямую связанных со службой, не происходит, так как все устройства кластера изначально имеют у себя копии всех файлов всех включённых в кластер служб.

Роль «узел наблюдения» — составная, с участием других (возможно сторонних) систем вне кластера (которые и называются «узлами наблюдения»), подключённых к внутренним и внешним каналам связи кластера и используемых для проверки доступности этих каналов. Проверка производится периодически соответствующим ПО кластера через отправку узлам наблюдения эхо-запросов ICMP («пингов»). Устанавливать дополнительное ПО на узлы наблюдения не нужно, от них требуется только поддержка ICMP и доступность по нему извне.

Для работы кластера и с кластером требуется несколько IP-адресов из сетей, к которым подключены интерфейсы систем кластера. Потребность в нескольких адресах объясняется тем, что каждая система кластера должна быть доступна и по своему собственному сетевому адресу.

### 28.1.2. Ресурсы и группы ресурсов

Ресурсом становится то, отказоустойчивость чего нужно обеспечить средствами кластера. В настоящее время наиболее распространены два стандарта ресурсов — LSB (Linux Standard Base) и OCF (Open Cluster Framework). От LSB в кластерах в настоящее время постепенно отказываются, так как возможность использования его ресурсов для кластера является только следствием принятых в стандарте общих правил, а не целью всего стандарта. Тем не менее, за время его применения было наработано много решений, которые используются и сейчас. OCF разработан в расчёте именно на кластеры и является

предпочтительным.

В случае с LSB ресурс и службу можно считать синонимами, в случае с OCF ресурс скорее является одним из вариантов конфигурации службы, то есть на базе одной и той же службы за счёт разных значений и набора параметров можно построить несколько ресурсов. IP-адреса (точнее, управляющие их привязкой к сетевым интерфейсам или отвязкой от них скрипты) также считаются службами, так как необходимо обеспечивать бесперебойность реакции систем на обращения по ним. Соответствующие системные скрипты поддерживают такие действия как start, stop и status. Поддержка этих действий позволяет считать IP-адреса такими же службами, как и «обычные» службы, поэтому они тоже могут перемещаться между системами кластера.

Для управления несколькими ресурсами как одним целым, кластерным ПО поддерживается абстракция «группа ресурсов». Она наделена следующими свойствами:

- группа может рассматриваться как отдельная единица конфигурации кластера, то есть сама может быть ресурсом (и называться «составным» или «сложным» ресурсом, в отличие от «примитивных», «обычных» ресурсов);
- перечисленные внутри группы ресурсы запускаются последовательно, в соответствии с порядком перечисления;
- перечисленные внутри группы ресурсы останавливаются последовательно, обратно порядку запуска;
- запуск ресурсов группы является зависимым в рамках этой группы: если текущий ресурс не получается запустить, то запуск остальных (следующих по порядку упоминания в группе) ресурсов группы прекращается, то есть следующие за ним ресурсы запущены не будут.

В Altell NEO можно использовать только одну группу ресурсов. Ресурсы одной группы могут исполняться и переноситься между системами кластера только как целое. Группа ресурсов не имеет собственных ограничений по количеству включённых в неё ресурсов.

### 28.1.3. Обнаружение сбоев в кластере

Кластер может выявлять сбои двух видов:

- сбой системы. Системы кластера регулярно обмениваются служебными сообщениями синхронизации, этот процесс называется «сердцебиение» («heartbeat»). Если одна из

систем кластера не получает таких сообщений от другой системы в течение определённого времени, то она заключает, что другая система неработоспособна. Если такое решение принимает ведущая система в отношении ведомой, то ведомая может быть исключена из кластера. Если такое решение принимает ведомая система в отношении ведущей, то она может либо запустить у себя процесс выборов и стать ведущей, либо дожидаться восстановления исходной ведущей системы.

- сбой связи. Обе системы кластера обычно работают с узлами наблюдения. Если ведущая система обнаруживает, что один из узлов наблюдения стал недоступным, то она считает себя неработоспособной и в результате ведомая система может стать новой ведущей.

### 28.1.4. Миграция

В контексте кластера Altell NEO миграцией ресурсов называется такое их перемещение между системами кластера, при котором не теряется информация об их состоянии. При этом должны быть выполнены следующие условия:

- агент ресурса должен соответствовать OCF;
- ресурс не должен быть в состоянии ошибки или частичной работоспособности («degraded»);
- ресурс не должен зависеть от любых других ресурсов ни явно, ни косвенно (в контексте конфигурации кластера, а не «вообще»).

Например, ресурс сервера FTP мигрировать не может, так как формально он зависит от IP-адресов, а фактически у кластера нет возможности скопировать в другую систему его действующие соединения в рамках TCP.

### 28.1.5. Роль «сердцебиения» при запуске кластера

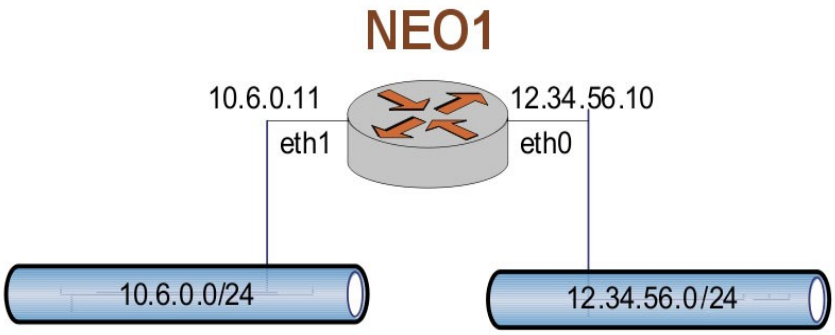
Обычно системы кластера запускаются последовательно, начиная с той, которую предполагается сделать ведущей. В процессе загрузки системы начинает свою работу служба «heartbeat», которая отправляет и принимает сообщения синхронизации. Ожидается, что это будут делать все описанные в конфигурации кластера системы, благодаря чему они узнают друг о друге. Отправка таких сообщений и ожидание их от других систем производятся в течение 120 секунд после старта службы, при этом возможны следующие варианты развития событий:

- при обнаружении системами друг друга, службы кластера на ведущей системе настраиваются на работу в ведущем режиме, а ведомая система переходит в резервный режим;
- если системы друг друга не обнаруживают (неправильные настройки сети, проблемы с каналом связи, крах одной из систем и так далее), то ведущей считает себя система с работающей службой «heartbeat» (или обе, при проблемах с обнаружением друг друга и порядком во всём остальном).

### 28.1.6. IP-адресация в кластере

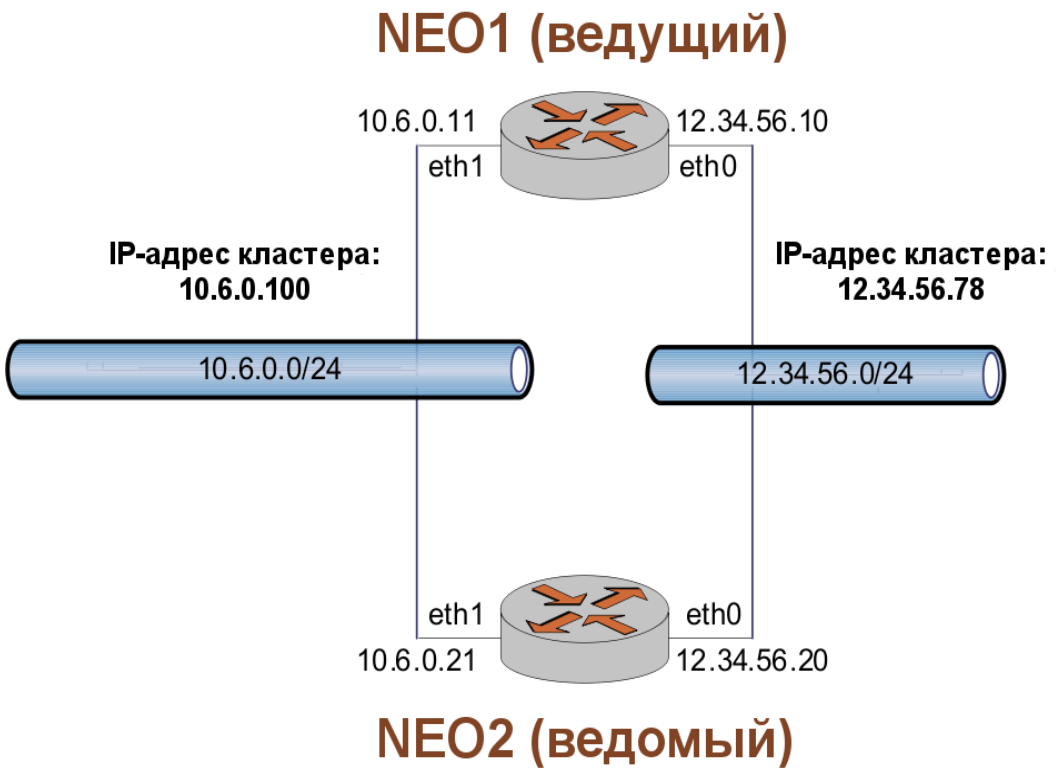
Вне кластера IP-адреса системам назначаются обычно так, как показано на рисунке 89:

*Рисунок 89 - Обычное подключение маршрутизатора*




В рамках кластера его IP-адрес рассматривается как ресурс, отказоустойчивое предоставление которого нужно обеспечить. Поскольку отказоустойчивость в данном случае обеспечивается избыточностью, то IP-адрес должен быть свободно перемещаемым между системами кластера. При этом надо учитывать то, что сам кластер и его службы должны быть доступны по одному и тому же адресу независимо от сбоев и то, что в одном сегменте сети несколько систем не могут использовать один и тот же IP-адрес одновременно. В то же время, нужно сохранить возможность обращения к каждой из систем кластера как к отдельной единице, что требует присвоения ей собственного, не перемещаемого IP-адреса. Для упрощения работы все эти адреса обычно выбирают из одинаковых подсетей, подобная схема приведена на рисунке 90.

*Рисунок 90 - Схема включения кластера вместо маршрутизатора*




Первоначально после запуска кластера его IP-адрес обслуживается ведущей системой. Поскольку с интерфейсом Ethernet может быть связан только один адрес, то адрес кластера связывается с интерфейсом через механизм псевдонимов (алиасов) интерфейсов.

Например, по схеме на рисунке 90 собственный адрес ведущей системы NEO1 12.34.56.10 связан с интерфейсом **eth0**, подключённым к подсети с адресом 12.34.56.0/24. Адрес кластера для подсети, к которой подключён этот интерфейс — 12.34.56.78 — будет связан с псевдоинтерфейсом **eth0:0**. Поскольку это адрес кластера, то он является ресурсом, перемещаемым между системами кластера, и при крахе системы NEO1 кластерное ПО автоматически создаст псевдоним интерфейса **eth0** в системе NEO2 с таким адресом. Благодаря этому кластер как целое по-прежнему будет доступен по своему адресу, хотя физически запросы обслуживать будет система NEO2, причём её собственный IP-адрес не изменится и останется 12.34.56.20.

***ПРИМЕЧАНИЕ**. Кластерное ПО управляет IP-адресами и псевдонимами*

*интерфейсов самостоятельно и не учитывает возможных посторонних действий, например, со стороны администраторов, поэтому настраивать эти ресурсы в обход кластерного ПО нельзя.*

***ПРИМЕЧАНИЕ**. Следует иметь в виду, что интерфейсы на узлах кластера должны совпадать, то есть, если перемещаемый IP-адрес связан с агрегированным интерфейсом (bondx), то агрегированный интерфейс должен присутствовать на обоих узлах кластера.*

## 28.2. Настройка кластера

**Изменять конфигурацию систем кластера в обход имеющихся для этого инструментов (например, прямым редактированием конфигурационных файлов) нельзя.** Кластерное ПО не учитывает такие изменения и скорее всего они приведут к краху кластера. После запуска системы в качестве действующей части кластера все настройки должны производиться только при помощи предназначенных для этого инструментов и команд.

### 28.2.1. Пример настройки кластера для поддержки туннелей VPN на базе IPsec

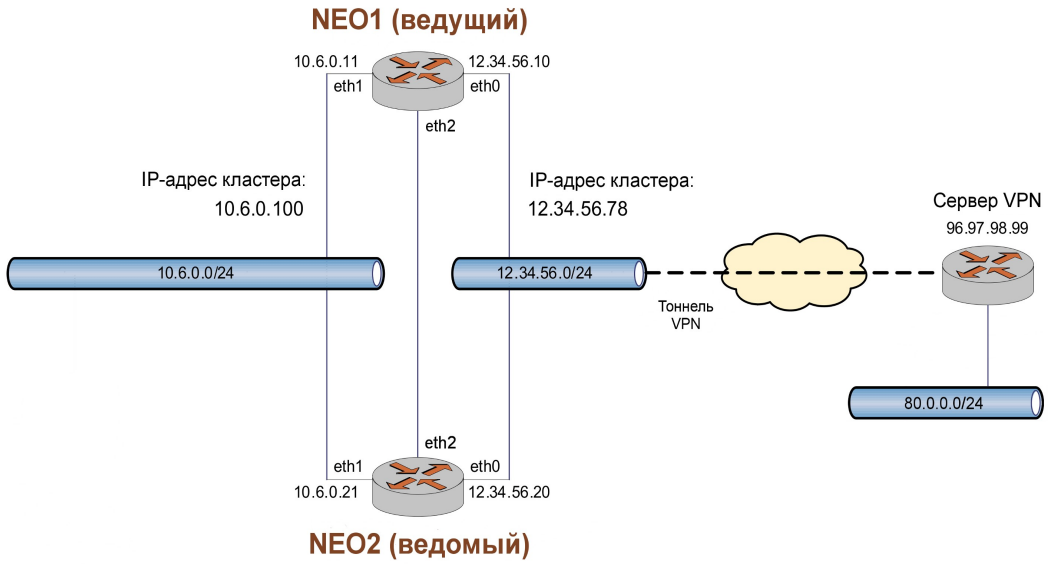
Рассмотрим организацию отказоустойчивого клиента VPN IPsec средствами двух устройств Altell NEO и установленного на них кластерного ПО. Для обеспечения отказоустойчивости потребуется следующее:

- отслеживать состояние IP-адреса кластера во внутренней сети (через интерфейсы **eth1**);
- отслеживать состояние IP-адреса кластера во внешней сети (через интерфейсы **eth0**);
- отслеживать состояние IP-адреса, под которым кластер выступает как клиент VPN и известен серверу VPN (обычно этот адрес совпадает с адресом кластера во внешней сети);
- отслеживать состояние сетевых соединений, осуществлённых через кластер — **conntrackd**;
- отслеживать состояние программы-демона управления ключами в рамках протокола IKE, использующегося в IPsec — **racoon**.

Отслеживание доступности каналов связи (роль «узел наблюдения») для упрощения примера опущено.

Пусть у нас имеется сетевая конфигурация, изображённая на следующем рисунке .

*Рисунок 91 - Схема включения кластера как отказоустойчивого клиента VPN*




Требуется обеспечить отказоустойчивое соединение через VPN двух локальных сетей — 10.0.0.0/24 и 80.0.0.0/24. Локальная сеть 10.0.0.0/24 находится за кластером из двух Altell NEO, удалённая сеть 80.0.0.0/24 подключена к серверу VPN с внешним (публичным) адресом 96.97.98.99. Для обмена внутренними данными кластера устройства Altell NEO используют отдельную физическую сеть с адресом 30.0.0.0/24, подключённую к их интерфейсам **eth2**. Внешней (публичной) сетью для кластера является сеть 12.34.56.0/24, подключённая к их интерфейсам **eth0**.

Предполагая, что интерфейсы устройств и подсистема VPN должным образом уже настроены, рассмотрим настройку кластерного ПО и служб кластера, призванных обеспечить отказоустойчивое соединение VPN. Начнём с настройки собственной инфраструктуры кластера на первом устройстве (**neo1**):

*Пример 28.1 - Настройка кластера для обеспечения отказоустойчивости соединения VPN на базе IPSec*

| Действие | Команда |
|---|---|

| | |
|---|---|
| Выключение аутентификации и шифрования обмена собственными данными кластера (для упрощения примера). | admin@neo1# **set cluster infrastructure secauth false**<br>[edit] |
| Выключение обмена собственными данными через широковещательные запросы. | admin@neo1# **set cluster infrastructure interface broadcast false**<br>[edit] |
| Привязка обмена собственными данными к интерфейсу с адресом сети 30.0.0.0. | admin@neo1# **set cluster infrastructure interface bind-net-addr 30.0.0.0**<br>[edit] |
| Просмотр конфигурации. | admin@neo1# **show cluster**<br>+infrastructure {<br>+ interface {<br>+ bind-net-addr 30.0.0.0<br>+ broadcast false<br>+ }<br>+ secauth false<br>+}<br>[edit] |

Теперь нужно разобраться с ресурсами. Отслеживанием сетевых соединений в рамках системы Netfilter и копированием информации о них между системами занимается программа **conntrackd**. Соответствующая ей служба называется **conntrack-failover**, а её агент разработан в соответствии со стандартом LSB (не OCF).

*Пример 28.2 - Настройка отказоустойчивости для службы* ***conntrack-failover***

| Действие | Команда |
|---|---|
| Сообщаем кластеру о необходимости наблюдения за состоянием службы. | admin@neo1# **set cluster group group1 lsb conntrack-failover** |

```
                                    operation action monitor
                                    [edit]
```

Задаём промежуток времени между проверками состояния службы (в секундах).

```
admin@neo1# set cluster group
group1 lsb conntrack-failover
operation interval 15
[edit]
```

Запускать службу без выполнения каких-либо дополнительных условий.

```
admin@neo1# set cluster group
group1 lsb conntrack-failover
operation requires nothing
[edit]
```

Запустить службу не сразу после применения конфигурации, а через 15 секунд.

```
admin@neo1# set cluster group
group1 lsb conntrack-failover
operation start-delay 15
[edit]
```

Каждая проверка состояния службы должна занимать меньше 15 секунд, иначе рассматривать её как сбой.

```
admin@neo1# set cluster group
group1 lsb conntrack-failover
operation timeout 15
[edit]
```

Просмотр конфигурации.

```
admin@neo1# show cluster group
  +group1 {
  +    lsb conntrack-failover {
  +        operation {
  +            action monitor
  +            interval 15
  +            requires nothing
  +            start-delay 15
  +            timeout 15
  +        }
  +    }
  +}
```

```
[edit]
```

Теперь переходим к настройке слежения за службой управления ключами — **racoon**:

*Пример 28.3 - Настройка отказоустойчивости для службы racoon*

| Действие | Команда |
|---|---|
| Сообщаем кластеру о необходимости наблюдения за состоянием службы. | admin@neo1# **set cluster group group1 lsb racoon operation action monitor**<br>[edit] |
| Задаём промежуток времени между проверками состояния службы (в секундах). | admin@neo1# **set cluster group group1 lsb racoon operation interval 15**<br>[edit] |
| Перезапустить службу в том случае, если проверка её состояния завершилась неудачно. | admin@neo1# **set cluster group group1 lsb racoon operation on-fail restart**<br>[edit] |
| Запускать службу без выполнения каких-либо дополнительных условий. | admin@neo1# **set cluster group group1 lsb racoon operation requires nothing**<br>[edit] |

Просмотр конфигурации.

```
admin@neo1# show cluster group
  +group1 {
  +    lsb conntrack-failover {
  +        operation {
  +            action monitor
  +            interval 15
  +            requires nothing
  +            start-delay 15
  +            timeout 15
  +        }
  +    }
  +    lsb racoon {
  +        operation {
  +            action monitor
  +            interval 15
  +            on-fail restart
  +            requires nothing
  +        }
  +    }
  +}
[edit]
```

Далее приведена настройка поведения кластера в отношении IP-адресов. В отличие от собственных адресов систем, IP-адреса, по которым кластер доступен извне (и из внутренней сети, и из внешней), имеют большое значение с точки зрения настройки кластеризации. Служба IP-адреса вместе со своим агентом разработана для стандарта OCF проектом heartbeat и называется **IPaddr2**. Сначала настраиваем публичный IP-адрес кластера (12.34.56.78) как ресурс:

*Пример 28.4 - Настройка публичного IP-адреса кластера*

| Действие | Команда |
|---|---|
| Одной командой создаём контейнер с | `admin@neo1# set cluster group` |

описанием нужного ресурса (**resIPext**) для указанной службы (**IPaddr2**) и добавляем параметр **cidr_netmask** (маска сети), который будет передан её агенту.

```
group1 ocf provider heartbeat
IPaddr2 name resIPext attribute
cidr_netmask value 24
[edit]
```

С этим IP-адресом агент создаст интерфейс-псевдоним и по нему кластер будет доступен для внешнего мира.

```
admin@neo1# set cluster group
group1 ocf provider heartbeat
IPaddr2 name resIPext attribute ip
value 12.34.56.78
[edit]
```

Интерфейс-псевдоним будет привязан к реальному интерфейсу **eth0**.

```
admin@neo1# set cluster group
group1 ocf provider heartbeat
IPaddr2 name resIPext attribute nic
value eth0
[edit]
```

Указываем кластеру переместить этот ресурс в другую систему если в текущей с ним произойдёт три сбоя.

```
admin@neo1# set cluster group
group1 ocf provider heartbeat
IPaddr2 name resIPext migration-
threshold 3
[edit]
```

Сообщаем кластеру о необходимости наблюдения за состоянием службы.

```
admin@neo1# set cluster group
group1 ocf provider heartbeat
IPaddr2 name resIPext operation
resIPext-op-monitor action monitor
[edit]
```

Задаём промежуток времени между проверками состояния службы (в секундах).

```
admin@neo1# set cluster group
group1 ocf provider heartbeat
IPaddr2 name resIPext operation
resIPext-op-monitor interval 10
[edit]
```

Перезапустить службу в том случае, если проверка её состояния завершилась неудачно.

```
admin@neo1# set cluster group
group1 ocf provider heartbeat
IPaddr2 name resIPext operation
resIPext-op-monitor on-fail restart
[edit]
```

Запускать службу без выполнения каких-либо дополнительных условий.

```
admin@neo1# set cluster group
group1 ocf provider heartbeat
IPaddr2 name resIPext operation
resIPext-op-monitor requires
nothing
[edit]
```

Запустить службу не сразу после применения конфигурации, а через 5 секунд.

```
admin@neo1# set cluster group
group1 ocf provider heartbeat
IPaddr2 name resIPext operation
resIPext-op-monitor start-delay 5
[edit]
```

Каждая проверка состояния службы должна занимать меньше 20 секунд, иначе рассматривать её как сбой.

```
admin@neo1# set cluster group
group1 ocf provider heartbeat
IPaddr2 name resIPext operation
resIPext-op-monitor timeout 20
[edit]
```

Просмотр конфигурации.

```
admin@neo1# show cluster group
group1 ocf
  +provider {
  +    heartbeat IPaddr2 {
  +        name resIPext {
  +            attribute
cidr_netmask {
  +                value 24
  +            }
```

```
  +            attribute ip {
  +                value
12.34.56.78
  +            }
  +            attribute nic {
  +                value eth0
  +            }
  +            migration-threshold
3
  +            operation resIPext-
op-monitor {
  +                action monitor
  +                interval 10
  +                on-fail restart
  +                requires nothing
  +                start-delay 5
  +                timeout 20
  +            }
  +        }
  +    }
  +}
[edit]
```

Проделываем то же самое для адреса 10.6.0.100, по которому кластер будет доступен из локальной сети:

*Пример 28.5 - Настройка локального IP-адреса кластера*

| Действие | Команда |
|---|---|
| Одной командой создаём контейнер с описанием нужного ресурса (**resIPext**) для указанной службы (**IPaddr2**) и добавляем параметр **cidr_netmask** | `admin@neo1#` **`set cluster group group1 ocf provider heartbeat IPaddr2 name resIPint attribute cidr_netmask value 24`** |

| | |
|---|---|
| (маска сети), который будет передан её агенту. | [edit] |
| С этим IP-адресом агент создаст интерфейс-псевдоним и по нему кластер будет доступен для внешнего мира. | admin@neo1# **set cluster group group1 ocf provider heartbeat IPaddr2 name resIPint attribute ip value 10.6.0.100**<br>[edit] |
| Интерфейс-псевдоним будет привязан с реальному интерфейсу **eth1**. | admin@neo1# **set cluster group group1 ocf provider heartbeat IPaddr2 name resIPint attribute nic value eth1**<br>[edit] |
| Указываем кластеру переместить этот ресурс в другую систему если в текущей с ним произойдёт три сбоя. | admin@neo1# **set cluster group group1 ocf provider heartbeat IPaddr2 name resIPint migration-threshold 3**<br>[edit] |
| Сообщаем кластеру о необходимости наблюдения за состоянием службы. | admin@neo1# **set cluster group group1 ocf provider heartbeat IPaddr2 name resIPint operation resIPint-op-monitor action monitor**<br>[edit] |
| Задаём промежуток времени между проверками состояния службы (в секундах). | admin@neo1# **set cluster group group1 ocf provider heartbeat IPaddr2 name resIPint operation resIPint-op-monitor interval 10**<br>[edit] |
| Перезапустить службу в том случае, если проверка её состояния | admin@neo1# **set cluster group group1 ocf provider heartbeat** |

завершилась неудачно.

```
IPaddr2 name resIPint operation
resIPint-op-monitor on-fail restart
[edit]
```

Запускать службу без выполнения каких-либо дополнительных условий.

```
admin@neo1# set cluster group
group1 ocf provider heartbeat
IPaddr2 name resIPint operation
resIPint-op-monitor requires
nothing
[edit]
```

Запустить службу не сразу после применения конфигурации, а через 5 секунд.

```
admin@neo1# set cluster group
group1 ocf provider heartbeat
IPaddr2 name resIPint operation
resIPint-op-monitor start-delay 5
[edit]
```

Каждая проверка состояния службы должна занимать меньше 20 секунд, иначе рассматривать её как сбой.

```
admin@neo1# set cluster group
group1 ocf provider heartbeat
IPaddr2 name resIPint operation
resIPint-op-monitor timeout 20
[edit]
```

Просмотр конфигурации.

```
admin@neo1# show cluster group
  +provider {
  +    heartbeat IPaddr2 {
  +        name resIPext {
  +            attribute
cidr_netmask {
  +                value 24
  +            }
  +            attribute ip {
  +                value
12.34.56.78
```

```
  +            }
  +            attribute nic {
  +                value eth0
  +            }
  +            migration-threshold
3
  +            operation resIPext-
op-monitor {
  +                action monitor
  +                interval 10
  +                on-fail restart
  +                requires nothing
  +                start-delay 5
  +                timeout 20
  +            }
  +        }
  +        name resIPint {
  +            attribute
cidr_netmask {
  +                value 24
  +            }
  +            attribute ip {
  +                value 10.6.0.100
  +            }
  +            attribute nic {
  +                value eth1
  +            }
  +            migration-threshold
3
  +            operation resIPint-
op-monitor {
  +                action monitor
```

```
+                interval 10
+                on-fail restart
+                requires nothing
+                start-delay 5
+                timeout 20
+            }
+        }
+    }
+}
[edit]
```

Применяем конфигурацию.

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

Для второго устройства — **neo2** — достаточно только настроить собственную инфраструктуру кластера и запустить кластерное ПО, остальное будет скопировано и применено автоматически:

*Пример 28.6 - Настройка узла neo2*

| Действие | Команда |
|---|---|
| Выключение аутентификации и шифрования обмена собственными данными кластера (для упрощения примера). | `admin@neo2# set cluster infrastructure secauth false`<br>`[edit]` |
| Выключение обмена собственными данными через широковещательные запросы. | `admin@neo2# set cluster infrastructure interface broadcast false`<br>`[edit]` |
| Привязка обмена собственными данными к интерфейсу с адресом сети 30.0.0.0. | `admin@neo2# set cluster infrastructure interface bind-net-addr 30.0.0.0`<br>`[edit]` |

Просмотр конфигурации.

```
admin@neo1# show cluster
  +infrastructure {
  +    interface {
  +        bind-net-addr 30.0.0.0
  +        broadcast false
  +    }
  +    secauth false
  +}
[edit]
```

Применение конфигурации.

```
admin@neo2# commit
[edit]
```

### 28.2.2. Краткие описания команд

| | |
|---|---|
| `cluster` | Включение или выключение поддержки кластеризации. |
| `cluster batch-limit <количество_заданий>` | Установка максимального числа заданий, которое механизму переходов разрешено выполнять параллельно. |
| `cluster cluster-delay <время>` | Установка максимального времени прохождения сетевого пакета от ведущей системы к ведомой и обратно («roundtrip»). |
| `cluster dc-deadtime <время>` | Установка длительности периода времени недоступности ведущей системы, по истечении которого ведущая система считается выбывшей из строя. |
| `cluster election-timeout <время>` | Установка периода времени, отводимого на выборы новой ведущей системы. |
| `cluster group <имя_группы>` | Создание пустой группы ресурсов. |
| `cluster group <имя_группы>` | Создание пустого контейнера для описания |

| | |
|---|---|
| | указанной службы с агентом из класса **lsb** и добавление её в указанную группу. |
| `cluster group <имя_группы> lsb <имя_службы> failure-timeout <время>` | Установка промежутка времени, по истечении которого службу можно будет вновь запускать в системе, в которой она до этого сбоила указанное в **lsb migration-threshold** число раз. |
| `cluster group <имя_группы> lsb <имя_службы> is-managed <состояние>` | Включение или выключение управления указанной службой со стороны кластера. |
| `cluster group <имя_группы> lsb <имя_службы> migration-threshold <количество_сбоев>` | Установка максимального количества сбоев службы в одной системе, превышение которого приведёт к переносу её в другую систему. |
| `cluster group <имя_группы> lsb <имя_ресурса> multiple-active <действие>` | Установка действия, которое будет предпринимать кластер при обнаружении работающих экземпляров указанной службы в более чем одной системе. |
| `cluster group <имя_группы> lsb <имя_службы> operation` | Создание контейнера для уточнения действий кластера по отношению к указанной службе. |
| `cluster group <имя_группы> lsb <имя_службы> operation action <действие>` | Установка действия, для которого будет уточняться поведение кластера. |
| `cluster group <имя_группы> lsb <имя_службы> operation enabled <состояние>` | Включение или выключение уточнения поведения кластера. |
| `cluster group <имя_группы> lsb <имя_службы> operation interval <время>` | Установка промежутка времени, через который нужно повторять указанное в атрибуте **lsb operation action** действие. |

| | |
|---|---|
| `cluster group <имя_группы> lsb <имя_службы> operation on-fail <действие>` | Установка действия, которое нужно предпринять кластеру, если текущее (то есть в рамках текущего контейнера **lsb operation**) уточнение его деятельности вызвало сбой. |
| `cluster group <имя_группы> lsb <имя_службы> operation requires <условие>` | Установка дополнительного условия, которое должно быть соблюдено перед запуском указанной службы. |
| `cluster group <имя_группы> lsb <имя_службы> operation start-delay <время>` | Установка промежутка времени, на который нужно отложить запуск указанной службы. |
| `cluster group <имя_группы> lsb <имя_службы> operation timeout <время>` | Установка длительности ожидания завершения действия в рамках текущего контейнера **lsb operation**. |
| `cluster group <имя_группы> lsb <имя_службы> priority <приоритет>` | Установка приоритета, определяющего возможность исполнения указанной службы при большой нагрузке на систему. |
| `cluster group <имя_группы> lsb <имя_службы> resource-stickiness <стоимость>` | Установка «стоимости» переноса службы между системами. |
| `cluster group <имя_группы> lsb <имя_службы> target-role <состояние>` | Установка состояния, в котором кластер должен стараться поддерживать службу-клон. |
| `cluster group <имя_группы> ocf` | Создание пустой группы для ресурсов с агентами из класса **ocf**. |
| `cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>` | Добавление указанной службы указанного производителя в указанную группу. |

| | |
|---|---|
| `cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса>` | Установка названия ресурса и создание пустого контейнера для его описания. |
| `cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> attribute <название> value <значение>` | Установка параметра, который будет передан агенту ресурса через переменную окружения. |
| `cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> failure-timeout <время>` | Установка промежутка времени, по истечении которого ресурс можно будет вновь запускать в системе, в которой он до этого сбоил указанное в **ocf migration-threshold** число раз. |
| `cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> is-managed <состояние>` | Включение или выключение управления ресурсом со стороны кластера. |
| `cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> migration-threshold <количество_сбоев>` | Установка максимального количества сбоев ресурса в одной системе, превышение которого приведёт к переносу ресурса в другую систему. |

| | |
|---|---|
| `cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> multiple-active <действие>` | Установка действия, которое будет предпринимать кластер при обнаружении работающих экземпляров указанного ресурса в более чем одной системе. |
| `cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> operation <название>` | Создание контейнера для уточнения действий кластера по отношению к указанному ресурсу. |
| `cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> operation <название> action <действие>` | Установка действия, для которого будет уточняться поведение кластера. |
| `cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> operation <название> enabled <состояние>` | Включение или выключение уточнения поведения кластера. |
| `cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name` | Установка промежутка времени, через который нужно повторять указанное в атрибуте **ocf operation action** действие. |

| | |
|---|---|
| `cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> operation <название> on-fail <действие>` | Указание действия, которое нужно предпринять кластеру, если текущее (то есть в рамках текущего контейнера **ocf operation**) уточнение его деятельности вызвало сбой. |
| `cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> operation <название> requires <условие>` | Установка дополнительного условия, которое должно быть соблюдено перед запуском указанного ресурса. |
| `cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> operation <название> start-delay <время>` | Установка промежутка времени, на который нужно отложить запуск указанного ресурса. |
| `cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> operation <название> timeout <время>` | Установка времени ожидания завершения действия в рамках текущего контейнера **ocf operation**. |
| `cluster group <имя_группы>` | Установка приоритета, определяющего |

| | |
|---|---|
| | возможность исполнения указанной службы при большой нагрузке на систему. |
| `cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> resource-stickiness <стоимость>` | Установка «стоимости» переноса ресурса между системами. |
| `cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> target-role <состояние>` | Установка состояния, в котором кластер должен стараться поддерживать службу-клон. |
| `cluster infrastructure` | Создание пустого контейнера для хранения параметров кластерной инфраструктуры, не связанной напрямую с управлением службами и узлами. |
| `cluster infrastructure interface` | Создание пустого контейнера для параметров сетевого интерфейса, через который будет производиться обмен собственными данными кластера. |
| `cluster infrastructure interface bind-net-addr <адрес_сети>` | Установка адреса *сети*, через сетевой интерфейс с которым будет производиться обмен собственными данными кластера. |
| `cluster infrastructure` | Включение или выключение использования |

| | |
|---|---|
| | широковещательной передачи для обмена собственными данными между системами кластера. |
| `cluster infrastructure interface mcast-addr <адрес>` | Включение обмена собственными данными между системами кластера через многоадресное вещание и задаёт адрес IPv4 для этого. |
| `cluster infrastructure interface mcast-port <порт>` | Установка порта UDP, на который будет вестись многоадресное вещание. |
| `cluster infrastructure net-mtu <mtu>` | Установка величины MTU. |
| `cluster infrastructure secauth <состояние>` | Включение или выключение аутентификации и шифрования внутренних данных кластера при обмене. |
| `cluster infrastructure threads <количество>` | Включение или выключение распараллеливания шифрования и отправки сообщений систем кластера на указанное количество потоков (нитей). |
| `cluster no-quorum-policy <действие>` | Установка реакции кластера на исчезновение кворума. |
| `cluster pe-error-series-max <количество>` | Установка количества вызвавших ошибки входящих сообщений движка политик (Policy Engine), информацию о которых нужно записать в журнал событий. |
| `cluster pe-input-series-max <количество>` | Установка количества «нормальных» входящих сообщений движка политик (Policy Engine), информацию о которых нужно записать в журнал событий. |
| `cluster pe-warn-series-max` | Установка количества вызвавших |

| | |
|---|---|
| | предупреждения входящих сообщений движка политик (Policy Engine), информацию о которых нужно записать в журнал событий. |
| `cluster start-failure-is-fatal <состояние>` | Включение или выключение восприятия кластером сбоев при запуске ресурса как фатальных. |
| `cluster stop-orphan-actions <состояние>` | Включение или выключение отмены действий, информация о которых стирается из конфигурации кластера. |
| `cluster stop-orphan-resources <состояние>` | Включение или выключение останова ресурсов, информация о которых стирается из конфигурации кластера. |
| `cluster symmetric-cluster <состояние>` | Включение или выключение возможности запуска всех ресурсов в любой из систем кластера. |

### 28.2.3. cluster

Включение или выключение поддержки кластеризации.

**Синтаксис**

**`set cluster`**

**`delete cluster`**

**`show cluster`**

**Режим команды**

Режим настройки.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Форма **set** этой команды используется для включения поддержки кластеризации.

Форма **delete** этой команды используется для выключения поддержки кластеризации.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### 28.2.4. cluster batch-limit <количество_заданий>

Установка максимального числа заданий, которое механизму переходов разрешено выполнять параллельно.

**Синтаксис**

**set cluster batch-limit** *количество_заданий*

**delete cluster batch-limit**

**show cluster batch-limit**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    batch-limit количество_заданий
}
```

**Параметры**

*количество_заданий*

Максимальное количество процессов, параллельно обрабатывающих граф переходов.

**Значение по умолчанию**

Граф переходов могут параллельно обрабатывать не больше **30** процессов.

**Указания по использованию**

Граф переходов может быть обработан несколькими процессами параллельно, при этом может потребоваться рассылка команд управления на другие системы кластера. При разумном количестве параллельно работающих процессов такой подход повышает производительность.

«Разумность» количества процессов определяется аппаратной производительностью устройств и загруженностью сети.

Форма **set** этой команды используется для выставления значения, отличного от значения по умолчанию.

Форма **delete** этой команды используется для возвращения параметру значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### 28.2.5. cluster cluster-delay <время>

Установка максимального времени прохождения сетевого пакета от ведущей системы к ведомой и обратно («roundtrip»).

**Синтаксис**

```
set cluster cluster-delay время
delete cluster cluster-delay
show cluster cluster-delay
```

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    cluster-delay время
}
```

**Параметры**

*время*

Максимальное время прохождения сетевого пакета в секундах.

**Значение по умолчанию**

**60** секунд.

**Указания по использованию**

Установка слишком маленького значения этого параметра может нарушить работу кластера. Значение используется как величина таймаута при сетевом обмене, поэтому для сохранения цельности кластера при большой нагрузке на системы кластера и/или сильной загруженности сети его можно

увеличивать.

Форма **set** этой команды используется для выставления значения, отличного от значения по умолчанию.

Форма **delete** этой команды используется для возвращения параметру значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### 28.2.6. cluster dc-deadtime <время>

Установка длительности (в секундах) периода времени недоступности ведущей системы, по истечении которого ведущая система считается выбывшей из строя.

**Синтаксис**

```
set cluster dc-deadtime время
delete cluster dc-deadtime
show cluster dc-deadtime
```

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    dc-deadtime время
}
```

**Параметры**

*время*

Длительность периода времени в секундах.

**Значение по умолчанию**

**10** секунд.

**Указания по использованию**

Если в течение указанного периода времени ведущая система не выходит на связь, то остальные системы кластера считают её вышедшей из строя и запускают процесс выбора новой ведущей системы.

Форма **set** этой команды используется для выставления значения, отличного от значения по умолчанию.

Форма **delete** этой команды используется для возвращения параметру значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### 28.2.7. cluster election-timeout <время>

Установка периода времени, отводимого на выборы новой ведущей системы.

**Синтаксис**

```
set cluster election-timeout время
delete cluster election-timeout
show cluster election-timeout
```

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    election-timeout время
}
```

**Параметры**

*время*

Длительность периода времени в секундах.

**Значение по умолчанию**

**10** секунд.

**Указания по использованию**

Если выборы новой ведущей системы не успевают пройти за указанный промежуток времени, то они считаются несостоявшимися. Необходимость в увеличении этого промежутка может возникнуть при высокой нагрузке на системы кластера и/или высокой загруженности сети.

Форма **set** этой команды используется для выставления значения, отличного от значения по умолчанию.

Форма **delete** этой команды используется для возвращения параметру значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния

конфигурации в этом контексте.

### 28.2.8. cluster group <имя_группы>

Создание пустой группы ресурсов.

#### Синтаксис

**set cluster group** *имя_группы*

**delete cluster group** *имя_группы*

**show cluster group**

#### Режим команды

Режим настройки.

#### Ветвь конфигурации

```
cluster {
    group имя_группы {
    }
}
```

#### Параметры

*имя_группы*

Множественный узел. Название создаваемой группы ресурсов.

#### Значение по умолчанию

Отсутствует.

#### Указания по использованию

Форма **set** этой команды используется для создания пустой группы ресурсов с указанным именем.

Форма **delete** этой команды используется для уничтожения существующей группы ресурсов с указанным именем.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### 28.2.9. cluster group <имя_группы> lsb <имя_службы>

Создание пустого контейнера для описания указанной службы с агентом из класса **lsb** и добавление её в указанную группу.

**Синтаксис**

**set cluster group** *имя_группы* **lsb** *имя_службы*

**delete cluster group** *имя_группы* **lsb** *имя_службы*

**show cluster group** *имя_группы* **lsb**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
     group имя_группы {
          lsb имя_службы }
          }
     }
}
```

**Параметры**

*имя_группы*

Множественный узел. Название группы ресурсов, в которую добавляется описание указанного ресурса.

*имя_службы*

Множественный узел. Название службы, описание которой создаётся и добавляется в указанную группу. Допустимые значения параметра:

- *conntrack-failover;*
- *pptpd;*
- *service-wireless;*
- *dnsmasq;*
- *racoon;*
- *uacctd;*
- *mrouted;*
- *service-l2tp;*
- *openvpn;*
- *service-snmpd.*

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Форма **set** этой команды используется для создания пустого описания указанной службы и вставки его в указанную группу.

Форма **delete** этой команды используется для уничтожения описания указанной службы и, соответственно, исключения его из группы.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.10. cluster group <имя_группы> lsb <имя_службы> failure-timeout <время>

Установка промежутка времени, по истечении которого службу можно будет вновь запускать в системе, в которой она до этого выходила из строя указанное в **lsb migration-threshold** число раз.

**Синтаксис**

**set cluster group** *имя_группы* **lsb** *имя_службы* **failure-timeout** *время*

**delete cluster group** *имя_группы* **lsb** *имя_службы* **failure-timeout**

**show cluster group** *имя_группы* **lsb** *имя_службы* **failure-timeout**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    group имя_группы {
        lsb имя_службы {
            failure-timeout время
        }
    }
}
```

**Параметры**

*имя_группы*

Множественный узел. Название группы, для службы из которой устанавливается значение атрибута **lsb failure-timeout**.

*имя_службы*

Множественный узел. Название службы, для которой устанавливается значение атрибута **lsb failure-timeout**. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> lsb <имя_службы>**.

*время*

Длительность промежутка времени в секундах.

**Значение по умолчанию**

**0** секунд, что означает невозможность автоматического возврата службы в систему, в которой она сбоила.

**Указания по использованию**

По умолчанию, если количество сбоев службы в одной системе достигает значения, указанного в атрибуте **lsb migration-threshold** (описан ниже), то служба перемещается в другую систему без возможности возврата в исходную систему до явного сброса счётчика сбоев ресурса администратором кластера. При помощи данной команды это ограничение можно обойти и позволить кластеру вернуть службу в исходную систему по истечении промежутка времени, задаваемого данной командой (счёт сбоев службы при этом перезапускается).

Форма **set** этой команды используется для указания длительности промежутка времени, отличной от значения по умолчанию.

Форма **delete** этой команды используется для возвращения параметру значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.11. cluster group <имя_группы> lsb <имя_службы> is-managed <состояние>

Включение или выключение управления указанной службой со стороны кластера.

**Синтаксис**

**set cluster group** *имя_группы* **lsb** *имя_службы* **is-managed** *состояние*

**delete cluster group** *имя_группы* **lsb** *имя_службы* **is-managed**

**show cluster group** *имя_группы* **lsb** *имя_службы* **is-managed**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    group имя_группы {
        lsb имя_службы {
            is-managed состояние
        }
    }
}
```

**Параметры**

*имя_группы*

Множественный узел. Название группы, для службы из которой устанавливается значение атрибута **lsb is-managed**..

*имя_службы*

Множественный узел. Название службы, для которой устанавливается значение атрибута **lsb is-managed**. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> lsb <имя_службы>**.

*состояние*

**true** или **false**. Значение **true** включает управление службой со стороны кластера, значение **false** выключает.

**Значение по умолчанию**

**true** — служба управляется кластером.

**Указания по использованию**

Эта команда позволяет, например, обновить ПО кластера без остановки ресурсов кластера, так как остановка кластерного ПО влечёт за собой и остановку всех ресурсов, находящихся под его управлением.

Форма **set** этой команды используется для установки нужного состояния службы в контексте управления им со стороны кластера.

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

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### 28.2.12. cluster group <имя_группы> lsb <имя_службы> migration-threshold <количество_сбоев>

Установка максимального количества сбоев службы в одной системе, превышение которого приведёт к переносу её в другую систему.

**Синтаксис**

**set cluster group** *имя_группы* **lsb** *имя_службы* **migration-threshold** *количество_сбоев*

**delete cluster group** *имя_группы* **lsb** *имя_службы* **migration-threshold**

**show cluster group** *имя_группы* **lsb** *имя_службы* **migration-threshold**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    group имя_группы {
        lsb имя_службы {
            migration-threshold количество_сбоев
        }
    }
}
```

**Параметры**

*имя_группы*

Множественный узел. Название группы, для службы из которой устанавливается значение атрибута **lsb migration-threshold**..

*имя_службы*

Множественный узел. Название службы, для которой устанавливается значение атрибута **lsb migration-threshold**. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> lsb <имя_службы>**.

*количество_сбоев*

Количество сбоев службы в «штуках».

**Значение по умолчанию**

**0**, то есть система может исполнять службу независимо от того, сколько сбоев службы уже произошло.

**Указания по использованию**

Сбои службы в конкретной системе могут происходить и из-за неполадок в этой системе (или аппаратном обеспечении, на котором она работает), а не из-за проблем с самой службой. При помощи данной команды можно указать количество сбоев, по достижению которого служба будет перемещена в другую систему без возможности автоматического (за исключением действия атрибута **lsb failure-timeout**, описанного выше) возвращения в сбоящую систему, с которой она был перемещена.

Форма **set** этой команды используется для установки количества сбоев.

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

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.13. cluster group <имя_группы> lsb <имя_ресурса> multiple-active <действие>

Установка действия, которое будет предпринимать кластер при обнаружении работающих экземпляров указанной службы в более чем одной системе.

**Синтаксис**

**set cluster group** *имя_группы* **lsb** *имя_службы* **multiple-active** *действие*

**delete cluster group** *имя_группы* **lsb** *имя_службы* **multiple-active**

**show cluster group** *имя_группы* **lsb** *имя_службы* **multiple-active**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    group имя_группы {
        lsb имя_службы {
            multiple-active действие
        }
    }
}
```

**Параметры**

*имя_группы*

Множественный узел. Название группы, для службы из которой устанавливается значение атрибута **lsb multiple-active**.

*имя_службы*

Множественный узел. Название службы, для которой устанавливается значение атрибута **lsb multiple-active**. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> lsb <имя_службы>**.

*действие*

Действие, предпринимаемое при обнаружении нескольких работающих экземпляров службы. Допустимые значения параметра:

- **block**: вывести службу из-под управления кластером;
- **stop_only**: остановить все экземпляры;
- **stop_start**: остановить все экземпляры и запустить какой-то один.

**Значение по умолчанию**

Установлено значение **stop_start**.

**Указания по использованию**

Эта команда используется для указания действий, которые кластерное ПО будет предпринимать при обнаружении одновременно работающих экземпляров (не клонов) указанной службы в нескольких системах, входящих в кластер.

Форма **set** этой команды используется для указания реакции кластера,

отличной от реакции по умолчанию.

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

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### 28.2.14. cluster group <имя_группы> lsb <имя_службы> operation

Создание контейнера для уточнения действий кластера по отношению к указанной службе.

**Синтаксис**

**set cluster group** *имя_группы* **lsb** *имя_службы* **operation**

**delete cluster group** *имя_группы* **lsb** *имя_службы* **operation**

**show cluster group** *имя_группы* **lsb** *имя_службы* **operation**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    group имя_группы {
        lsb имя_службы {
            operation {
            }
        }
    }
}
```

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Существует набор операций, которые ПО кластера неявным (для администратора) образом при необходимости выполняет по отношению к службам — **start**, **stop** и **monitor** (последнее используется однократно в

процедуре запуска службы для проверки её состояния перед собственно запуском). При помощи контейнера **lsb operation** можно через установку значений соответствующих атрибутов (описаны в командах ниже) влиять на поведение кластера во время исполнения этих операций.

Форма **set** этой команды используется для создания пустого контейнера для описания операций.

Форма **delete** этой команды используется для уничтожения существующего контейнера с операциями.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### 28.2.15. cluster group <имя_группы> lsb <имя_службы> operation action <действие>

Установка действия, для которого будет уточняться поведение кластера.

#### Синтаксис

**set cluster group** *имя_группы* **lsb** *имя_службы* **operation action** *действие*

**delete cluster group** *имя_группы* **lsb** *имя_службы* **operation action**

**show cluster group** *имя_группы* **lsb** *имя_службы* **operation action**

#### Режим команды

Режим настройки.

#### Ветвь конфигурации

```
cluster {
    group имя_группы {
        lsb имя_службы {
            operation {
                action действие
            }
        }
    }
}
```

**Параметры**

*имя_группы*

Множественный узел. Название группы, для службы из которой устанавливается значение атрибута **lsb operation action**.

*имя_службы*

Множественный узел. Название службы, для которой устанавливается значение атрибута **lsb operation action**. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> lsb <имя_службы>**.

*действие*

Действие, исполнение которого кластером будет уточняться. Допустимые значения параметра:

- **monitor**: проверка состояния службы;
- **start**: запуск службы;
- **status**: не используется;
- **stop**: остановка службы.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда предназначена для указания действия, для которого будет уточняться поведение кластера при помощи других атрибутов в рамках текущего контейнера **lsb operation**. Для класса **lsb** в рамках текущего контейнера можно уточнить поведение кластера только для одного действия.

Форма **set** этой команды используется для указания нужного действия.

Форма **delete** этой команды используется для исключения указанного действия.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### 28.2.16. cluster group <имя_группы> lsb <имя_службы> operation enabled <состояние>

Включение или выключение уточнения поведения кластера. Параметры, атрибуты и их значения при этом не теряются и не изменяются.

**Синтаксис**

**set cluster group** *имя_группы* **lsb** *имя_службы* **operation enabled** *состояние*

**delete cluster group** *имя_группы* **lsb** *имя_службы* **operation enabled**

**show cluster group** *имя_группы* **lsb** *имя_службы* **operation enabled**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    group имя_группы {
        lsb имя_службы {
            operation {
                enabled состояние
            }
        }
    }
}
```

**Параметры**

*имя_группы*

Множественный узел. Название группы, для службы из которой устанавливается значение атрибута **lsb operation enabled**.

*имя_службы*

Множественный узел. Название службы, для которой устанавливается значение атрибута **lsb operation enabled**. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> lsb <имя_службы>**.

*состояние*

**true** или **false**. **true** включает уточнение поведения кластера, **false** — выключает.

#### Значение по умолчанию

**true** — уточнение поведения кластера включено.

#### Указания по использованию

Эта команда предназначена для временного выключения уточнения поведения кластера без потери его атрибутов.

Форма **set** этой команды используется для установки нужного значения атрибута.

Форма **delete** этой команды используется для возвращения атрибуту значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### 28.2.17. cluster group <имя_группы> lsb <имя_службы> operation interval <время>

Установка промежутка времени, через который нужно повторять указанное в атрибуте **lsb operation action** действие.

#### Синтаксис

**set cluster group** *имя_группы* **lsb** *имя_службы* **operation interval** *время*

**delete cluster group** *имя_группы* **lsb** *имя_службы* **operation interval**

**show cluster group** *имя_группы* **lsb** *имя_службы* **operation interval**

#### Режим команды

Режим настройки.

#### Ветвь конфигурации

```
cluster {
    group имя_группы {
        lsb имя_службы {
            operation {
                interval время
```

```
                        }
                    }
                }
            }
```

**Параметры**

*имя_группы*

Множественный узел. Название группы, для службы из которой устанавливается значение атрибута **lsb operation interval**.

*имя_службы*

Множественный узел. Название службы, для которой устанавливается значение атрибута **lsb operation interval**. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> lsb <имя_службы>**.

*время*

Длительность промежутка времени (в секундах), через который нужно повторять исполнение указанного в атрибуте **lsb operation action** действия.

**Значение по умолчанию**

**0**, действие должно выполняться только один раз.

**Указания по использованию**

Эта команда предназначена для управления периодичностью исполнения действия. Значение по умолчанию выключает периодичность, указание любой длительности (в секундах) — включает периодическое исполнение действия через промежутки времени указанной длительности.

Форма **set** этой команды используется для установки нужного значения атрибута.

Форма **delete** этой команды используется для возвращения атрибуту значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.18. cluster group <имя_группы> lsb <имя_службы> operation on-fail <действие>

Установка действия, которое нужно предпринять кластеру, если текущее (то есть в рамках текущего контейнера **lsb operation**) уточнение его деятельности вызвало сбой.

**Синтаксис**

**set cluster group** *имя_группы* **lsb** *имя_службы* **operation on-fail** *действие*

**delete cluster group** *имя_группы* **lsb** *имя_службы* **operation on-fail**

**show cluster group** *имя_группы* **lsb** *имя_службы* **operation on-fail**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    group имя_группы {
        lsb имя_службы {
            operation {
                on-fail действие
            }
        }
    }
}
```

**Параметры**

*имя_группы*

Множественный узел. Название группы, для службы из которой устанавливается значение атрибута **lsb operation on-fail**.

*имя_службы*

Множественный узел. Название службы, для которой устанавливается значение атрибута **lsb operation on-fail**. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> lsb <имя_службы>**.

*действие*

Действие, предпринимаемое кластером в ответ на сбой текущего уточнения его деятельности. Допустимые значения параметра:

- **block**: прекратить использование уточнения;

- **ignore**: не обращать внимания на сбои;

- **restart**: остановить службу, в отношении которой сбоит уточнение, и запустить её снова (возможно, в другой системе кластера);

- **standby**: перенести куда-нибудь все ресурсы с системы, в которой сбоит уточнение;

- **stop**: остановить службу, в отношении которой сбоит уточнение и не запускать её в других системах кластера.

**Значение по умолчанию**

При уточнении операции **stop** действием по умолчанию является **block**. При уточнении других операций действием по умолчанию является **stop**.

**Указания по использованию**

Форма **set** этой команды используется для установки нужного значения атрибута.

Форма **delete** этой команды используется для возвращения атрибуту значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.19. cluster group <имя_группы> lsb <имя_службы> operation requires <условие>

Установка дополнительного условия, которое должно быть соблюдено перед запуском указанной службы.

**Синтаксис**

**set cluster group** *имя_группы* **lsb** *имя_службы* **operation requires** *условие*

**delete cluster group** *имя_группы* **lsb** *имя_службы* **operation requires**

**show cluster group** *имя_группы* **lsb** *имя_службы* **operation requires**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    group имя_группы {
        lsb имя_службы {
            operation {
                requires условие
            }
        }
    }
}
```

**Параметры**

*имя_группы*

Множественный узел. Название группы, для службы из которой устанавливается значение атрибута **lsb operation requires**.

*имя_службы*

Множественный узел. Название службы, для которой устанавливается значение атрибута **lsb operation requires**. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> lsb <имя_службы>**.

*условие*

Условие, соблюдение которого разрешит запуск службы. Допустимые значения параметра:

- **fencing**: службу можно запускать только тогда, когда большинство настроенных систем кластера активно, а системы, находящиеся в неопределённом состоянии или в состоянии сбоя — выключены;
- **nothing**: службу можно запускать без удовлетворения предварительных условий;
- **quorum**: службу можно запускать только тогда, когда большинство настроенных систем кластера активно.

**Значение по умолчанию**

**quorum**

#### Указания по использованию

Форма **set** этой команды используется для установки нужного значения атрибута.

Форма **delete** этой команды используется для возвращения атрибуту значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.20. cluster group <имя_группы> lsb <имя_службы> operation start-delay <время>

Установка промежутка времени (в секундах), на который нужно отложить запуск указанной службы.

#### Синтаксис

**set cluster group** *имя_группы* **lsb** *имя_службы* **operation start-delay** *время*

**delete cluster group** *имя_группы* **lsb** *имя_службы* **operation start-delay**

**show cluster group** *имя_группы* **lsb** *имя_службы* **operation start-delay**

#### Режим команды

Режим настройки.

#### Ветвь конфигурации

```
cluster {
    group имя_группы {
        lsb имя_службы {
            operation {
                start-delay время
            }
        }
    }
}
```

#### Параметры

*имя_группы*

Множественный узел. Название группы, для службы из которой устанавливается значение атрибута **lsb operation start-delay**.

*имя_службы*

Множественный узел. Название службы, для которой устанавливается значение атрибута **lsb operation start-delay**. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> lsb <имя_службы>**.

*время*

Отрезок времени в секундах, на который будет отложен запуск указанной в команде службы.

**Значение по умолчанию**

По умолчанию установлено значение 0.

**Указания по использованию**

Форма **set** этой команды используется для установки нужного значения атрибута.

Форма **delete** этой команды используется для возвращения атрибуту значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.21. cluster group <имя_группы> lsb <имя_службы> operation timeout <время>

Установка длительности ожидания (в секундах) завершения действия в рамках текущего контейнера **lsb operation**.

**Синтаксис**

**set cluster group** *имя_группы* **lsb** *имя_службы* **operation timeout** *время*

**delete cluster group** *имя_группы* **lsb** *имя_службы* **operation timeout**

**show cluster group** *имя_группы* **lsb** *имя_службы* **operation timeout**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    group имя_группы {
        lsb имя_службы {
            operation {
                timeout время
            }
        }
    }
}
```

**Параметры**

*имя_группы*

Множественный узел. Название группы, для службы из которой устанавливается значение атрибута **lsb operation timeout**.

*имя_службы*

Множественный узел. Название службы, для которой устанавливается значение атрибута **lsb operation timeout**. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> lsb <имя_службы>**.

*время*

Длительность отрезка времени (в секундах), в течение которого кластер будет ожидать завершения действия, указанного атрибутом **lsb operation action**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Отсутствие завершения операции в течение указанного времени рассматривается как сбой.

Форма **set** этой команды используется для установки нужного значения атрибута.

Форма **delete** этой команды используется для возвращения атрибуту значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния

конфигурации в этом контексте.

### 28.2.22. cluster group <имя_группы> lsb <имя_службы> priority <приоритет>

Установка приоритета, определяющего возможность исполнения указанной службы при большой нагрузке на систему.

#### Синтаксис

**set cluster group** *имя_группы* **lsb** *имя_службы* **priority** *приоритет*

**delete cluster group** *имя_группы* **lsb** *имя_службы* **priority**

**show cluster group** *имя_группы* **lsb** *имя_службы* **priority**

#### Режим команды

Режим настройки.

#### Ветвь конфигурации

```
cluster {
    group имя_группы {
        lsb имя_службы {
            priority приоритет
        }
    }
}
```

#### Параметры

*имя_группы*

Множественный узел. Название группы, для службы из которой устанавливается значение атрибута **lsb priority**.

*имя_службы*

Множественный узел. Название службы, для которой устанавливается значение атрибута **lsb priority**. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> lsb <имя_службы>**.

*приоритет*

Число от 0 до 4294967295.

#### Значение по умолчанию

По умолчанию установлено значение 0.

#### Указания по использованию

При большой нагрузке на систему кластерное ПО будет освобождать системные ресурсы за счёт останова ресурсов кластера, начиная с ресурсов с самым низким приоритетом. Значение имеет не абсолютная величина приоритета, а то, какова она относительно приоритетов других ресурсов. Например, само по себе значение приоритета 4000000000 у ресурса ничего не значит, хоть и выглядит огромным. Однако, если кластер исполняет ещё один ресурс, с приоритетом 4000000001, то при большой нагрузке в первую очередь будет остановлен ресурс с приоритетом 4000000000.

Форма **set** этой команды используется для установки нужного значения атрибута.

Форма **delete** этой команды используется для возвращения атрибуту значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### 28.2.23. cluster group <имя_группы> lsb <имя_службы> resource-stickiness <стоимость>

Установка «стоимости» переноса службы между системами.

#### Синтаксис

**set cluster group** *имя_группы* **lsb** *имя_службы* **resource-stickiness** *время*

**delete cluster group** *имя_группы* **lsb** *имя_службы* **resource-stickiness**

**show cluster group** *имя_группы* **lsb** *имя_службы* **resource-stickiness**

#### Режим команды

Режим настройки.

#### Ветвь конфигурации

```
cluster {
    group имя_группы {
```

```
            lsb имя_службы {
                resource-stickiness стоимость
            }
        }
    }
```

**Параметры**

*имя_группы*

Множественный узел. Название группы, для службы из которой устанавливается значение атрибута **lsb resource-stickiness**.

*имя_службы*

Множественный узел. Название службы, для которой устанавливается значение атрибута **lsb resource-stikiness**. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> lsb <имя_службы>**.

*стоимость*

Число от 0 до 4294967295.

**Значение по умолчанию**

По умолчанию установлено значение 0.

**Указания по использованию**

Этот атрибут определяет желательность отказа от переноса нормально работающей службы между системами. Число определяет «стоимость» переноса службы между системами (в контексте времени простоя в обслуживании, вызванного этим переносом): чем оно больше, тем более затратным кластеру следует считать перенос службы, из-за чего с ростом этого значения перенос становится всё менее желательным.

Форма **set** этой команды используется для установки нужного значения атрибута.

Форма **delete** этой команды используется для возвращения атрибуту значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### 28.2.24. cluster group <имя_группы> lsb <имя_службы> target-role <состояние>

Установка состояния, в котором кластер должен стараться поддерживать службу-клон.

#### Синтаксис

**set cluster group** *имя_группы* **lsb** *имя_службы* **target-role** *состояние*

**delete cluster group** *имя_группы* **lsb** *имя_службы* **target-role**

**show cluster group** *имя_группы* **lsb** *имя_службы* **target-role**

#### Режим команды

Режим настройки.

#### Ветвь конфигурации

```
cluster {
    group имя_группы {
        lsb имя_службы {
            target-role состояние
        }
    }
}
```

#### Параметры

*имя_группы*

Множественный узел. Название группы, для службы из которой устанавливается значение атрибута **lsb target-role**.

*имя_службы*

Множественный узел. Название службы, для которой устанавливается значение атрибута **lsb target-role**. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> lsb <имя_службы>**.

*состояние*

Состояние, в котором кластер будет стараться удерживать службу. Допустимые значения параметра:

- **stopped**: удерживать службу в остановленном состоянии;

- **started**: запустить службу и оставить её в состоянии «ведомый»;
- **master**: запустить службу с перевести её в состояние «ведущий».

**Значение по умолчанию**

По умолчанию установлено значение **started**.

**Указания по использованию**

Эта команда предназначена для управления состоянием служб-клонов, которые поддерживают работу в одном из двух режимов — «ведущий» или «ведомый». Эти режимы связаны с поведением экземпляров одной и той же службы в отношении друг друга при одновременной работе в разных системах кластера и не имеют отношения к схеме работы всего кластера с тем же названием («ведущий-ведомый»).

Форма **set** этой команды используется для установки нужного значения атрибута.

Форма **delete** этой команды используется для возвращения атрибуту значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.25. cluster group <имя_группы> ocf

Создание пустой группы для ресурсов с агентами из класса **ocf**.

**Синтаксис**

**set cluster** *имя_группы* **ocf**

**delete cluster** *имя_группы* **ocf**

**show cluster** *имя_группы*

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    group имя_группы {
        ocf {
        }
    }
```

```
}
```

**Параметры**

*имя_группы*

Название создаваемой группы ресурсов.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Форма **set** этой команды используется для создания пустой группы ресурсов с агентами из класса **ocf**.

Форма **delete** этой команды используется для уничтожения группы ресурсов с указанным именем.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### 28.2.26. cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>

Добавление указанной службы указанного производителя в указанную группу.

**Синтаксис**

**set cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы*

**delete cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы*

**show cluster group** *имя_группы* **ocf provider** *имя_производителя*

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    group имя_группы {
        ocf {
            provider {
                имя_производителя имя_службы {
                }
```

```
                    }
                }
            }
        }
```

**Параметры**

*имя_группы*

Название группы, в которую вносится ресурс.

*имя_производителя*

Множественный узел. Название производителя агента ресурса. Допустимые значения параметра:

*heartbeat*

*pacemaker*

*имя_службы*

Множественный узел. Название добавляемой в группу службы. Допустимые значения параметра для производителя **heartbeat**:

- *AoEtarget;*
- *Route;*
- *iSCSILogicalUnit;*
- *AudibleAlarm;*
- *SAPDatabase;*
- *iSCSITarget;*
- *CTDB;*
- *SAPInstance;*
- *ids;*
- *ClusterMon;*
- *SendArp;*
- *iscsi;*
- *Delay;*
- *ServeRAID;*
- *mysql;*
- *Dummy;*

- *SphinxSearchDaemon;*
- *mysql-proxy;*
- *EvmsSCC;*
- *Squid;*
- *nfsserver;*
- *Evmsd;*
- *Stateful;*
- *oracle;*
- *Filesystem;*
- *SysInfo;*
- *oralsnr;*
- *ICP;*
- *VIPArip;*
- *pgsql;*
- *Ipaddr;*
- *VirtualDomain;*
- *pingd;*
- *Ipaddr2;*
- *WAS;*
- *portblock;*
- *Ipsrcaddr;*
- *WAS6;*
- *postfix;*
- *Ipv6addr;*
- *WinPopup;*
- *proftpd;*
- *LVM;*
- *Xen;*
- *rsyncd;*
- *LinuxSCSI;*

- *Xinetd;*
- *scsi2reservation;*
- *MailTo;*
- *anything;*
- *sfex;*
- *ManageRAID;*
- *apache;*
- *syslog-ng;*
- *ManageVE;*
- *db2;*
- *tomcat;*
- *Pure-FTPd;*
- *drbd;*
- *vmware;*
- *Raid1;*
- *eDir88.*

Допустимые значения параметра для производителя **pacemaker**:

- *ClusterMon;*
- *HealthSMART;*
- *SystemHealth;*
- *ping;*
- *Dummy;*
- *Stateful;*
- *controld;*
- *pingd;*
- *HealthCPU;*
- *SysInfo;*
- *o2c.*

**Значение по умолчанию**

Отсутствует.

#### Указания по использованию

Форма **set** этой команды используется для добавления указанной службы указанного производителя в указанную группу.

Форма **delete** этой команды используется для исключения указанной службы указанного производителя из указанной группы.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.27. cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса>

Установка названия ресурса и создание пустого контейнера для его описания.

#### Синтаксис

**set cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса*

**delete cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса*

**show cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса*

#### Режим команды

Режим настройки.

#### Ветвь конфигурации

```
cluster {
    group имя_группы {
        ocf {
            provider {
                имя_производителя имя_службы {
                    name имя_ресурса {
                    }
                }
            }
        }
    }
}
```

**Параметры**

*имя_группы*

Название группы, в которую вносится ресурс.

*имя_производителя*

Множественный узел. Название производителя службы ресурса. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_службы*

Множественный узел. Название службы, для которой добавляется ресурс. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_ресурса*

Множественный узел. Название самого ресурса и контейнера для его атрибутов.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда предназначена для создания пустого контейнера для атрибутов ресурса. Поскольку это множественный узел, то для одной службы при помощи нескольких контейнеров можно задать несколько конфигураций (то есть фактически создать несколько ресурсов).

Форма **set** этой команды используется для создания нового ресурса на базе указанной службы.

Форма **delete** этой команды используется для уничтожения указанного ресурса.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.28. cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> attribute <название> value <значение>

Установка параметра, который будет передан агенту ресурса через переменную окружения.

**Синтаксис**

**set cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **attribute** *название* **value** *значение*

**delete cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **attribute** *название*

**show cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **attribute** *название*

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    group имя_группы {
        ocf {
            provider {
                имя_производителя имя_службы {
                    name имя_ресурса {

    attribute название {

        value значение

    }
                    }
                }
            }
        }
    }
}
```

**Параметры**

*имя_группы*

Название группы, в которую вносится ресурс.

*имя_производителя*

Множественный узел. Название производителя службы ресурса. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_службы*

Множественный узел. Название службы, для которой настраивается ресурс. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_ресурса*

Множественный узел. Название ресурса.

*название*

Множественный узел. Название параметра, который будет передан агенту ресурса. Параметр не может быть произвольным, он должен реально поддерживаться агентом.

*значение*

Значение передаваемого параметра. Если оно содержит пробелы, то его нужно заключить в кавычки.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда предназначена для передачи агенту ресурса дополнительных параметров. Задаваемые при помощи этой команды параметры будут переданы агенту через переменные окружения вида **OCF_RESKEY_название**. Передать получится только те параметры, которые явно распознаются агентом. Получить перечень параметров агента можно либо посмотрев его код, либо запустив его из командной строки с параметром **--meta-data**.

Форма **set** этой команды используется для введения в конфигурацию кластера параметра агента ресурса, который будет передан агенту при его вызове последнего.

Форма **delete** этой команды используется для уничтожения указанного параметра агента и, соответственно, отмены его передачи агенту при вызове

последнего.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### 28.2.29. cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> failure-timeout <время>

Установка промежутка времени, по истечении которого ресурс можно будет вновь запускать в системе, в которой он до этого сбоил указанное в **ocf migration-threshold** число раз.

#### Синтаксис

**set cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **failure-timeout** *время*

**delete cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **failure-timeout**

**show cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **failure-timeout**

#### Режим команды

Режим настройки.

#### Ветвь конфигурации

```
cluster {
    group имя_группы {
        ocf {
            provider {
                имя_производителя имя_службы {
                    name имя_ресурса {

failure-timeout время
                    }
                }
            }
        }
```

```
        }
}
```

**Параметры**

*имя_группы*

Название группы, в которую вносится ресурс.

*имя_производителя*

Множественный узел. Название производителя службы ресурса. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_службы*

Множественный узел. Название службы, для которой настраивается ресурс. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_ресурса*

Множественный узел. Название ресурса.

*время*

Длительность промежутка времени в секундах.

**Значение по умолчанию**

**0** секунд, что означает невозможность автоматического возврата ресурса в систему, в которой он сбоил.

**Указания по использованию**

По умолчанию, если количество сбоев ресурса в одной системе достигает значения, указанного в атрибуте **ocf migration-threshold** (описан ниже), то ресурс перемещается в другую систему без возможности возврата в исходную систему до явного сброса счётчика сбоев ресурса администратором кластера. При помощи данной команды это ограничение можно обойти и всё-таки позволить кластеру вернуть ресурс в исходную систему по истечении промежутка времени, задаваемого данной командой (счёт сбоев ресурса при этом перезапускается).

Форма **set** этой команды используется для указания длительности промежутка времени, отличной от значения по умолчанию.

Форма **delete** этой команды используется для возвращения параметру

значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### 28.2.30. cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> is-managed <состояние>

Включение или выключение управления ресурсом со стороны кластера.

#### Синтаксис

**set cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **is-managed** *состояние*

**delete cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **is-managed**

**show cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **is-managed**

#### Режим команды

Режим настройки.

#### Ветвь конфигурации

```
cluster {
    group имя_группы {
        ocf {
            provider {
                имя_производителя имя_службы {
                    name имя_ресурса {

    is-managed состояние
                    }
                }
            }
        }
    }
}
```

**Параметры**

*имя_группы*

Название группы, в которую вносится ресурс.

*имя_производителя*

Множественный узел. Название производителя службы ресурса. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_службы*

Множественный узел. Название службы, для которой настраивается ресурс. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_ресурса*

Множественный узел. Название ресурса.

*состояние*

**true** или **false**. Значение **true** включает управление ресурсом со стороны кластера, значение **false** выключает.

**Значение по умолчанию**

**true** — ресурс управляется кластером.

**Указания по использованию**

Эта команда позволяет, например, обновить ПО кластера без остановки ресурсов кластера, так как остановка кластерного ПО повлечёт за собой и остановку всех ресурсов, находящихся под его управлением.

Форма **set** этой команды используется для включения или выключения управления ресурсом со стороны кластера.

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

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### 28.2.31. cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> migration-threshold <количество_сбоев>

Установка максимального количества сбоев ресурса в одной системе, превышение которого приведёт к переносу ресурса в другую систему.

**Синтаксис**

**set cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **migration-threshold** *количество_сбоев*

**delete cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **migration-threshold**

**show cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **migration-threshold**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    group имя_группы {
        ocf {
            provider {
                имя_производителя имя_службы {
                    name имя_ресурса {

    migration-threshold количество_сбоев
                    }
                }
            }
        }
    }
}
```

**Параметры**

*имя_группы*

Название группы, в которую вносится ресурс.

*имя_производителя*

Множественный узел. Название производителя службы ресурса. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_службы*

Множественный узел. Название службы, для которой настраивается ресурс. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_ресурса*

Множественный узел. Название ресурса.

*количество_сбоев*

Количество сбоев ресурса в «штуках».

**Значение по умолчанию**

**0**, то есть система может исполнять ресурс независимо от того, сколько сбоев ресурса уже произошло.

**Указания по использованию**

Сбои ресурса в конкретной системе могут происходить и из-за неполадок в этой системе (или аппаратном обеспечении, на котором она работает), а не из-за проблем с самим ресурсом. При помощи данной команды можно указать количество сбоев, по достижению которого ресурс будет перемещён в другую систему без возможности автоматического (за исключением действия атрибута **ocf failure-timeout**, описанного выше) возвращения в сбоящую систему, с которой он был перемещён.

Форма **set** этой команды используется для установки количества сбоев.

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

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.32. cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> multiple-active <действие>

Установка действия, которое будет предпринимать кластер при обнаружении работающих экземпляров указанного ресурса в более чем одной системе.

**Синтаксис**

**set cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **multiple-active** *действие*

**delete cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **multiple-active**

**show cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **multiple-active**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    group имя_группы {
        ocf {
            provider {
                имя_производителя имя_службы {
                    name имя_ресурса {

    multiple-active действие
                    }
                }
            }
        }
    }
}
```

**Параметры**

*имя_группы*

Название группы, в которую вносится ресурс.

*имя_производителя*

Множественный узел. Название производителя службы ресурса. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_службы*

Множественный узел. Название службы, для которой настраивается ресурс. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_ресурса*

Множественный узел. Название ресурса.

*действие*

Действие, предпринимаемое при обнаружении нескольких работающих экземпляров ресурса. Допустимые значения параметра:

- **block**: вывести ресурс из-под управления кластером;
- **stop_only**: остановить все экземпляры;
- **stop_start**: остановить все экземпляры и запустить какой-то один.

**Значение по умолчанию**

Значение по умолчанию **stop_start**.

**Указания по использованию**

Эта команда используется для указания действий, которые кластерное ПО будет предпринимать при обнаружении одновременно работающих экземпляров (не клонов) указанного ресурса в нескольких системах, входящих в кластер.

Форма **set** этой команды используется для указания реакции кластера, отличной от реакции по умолчанию.

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

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.33. cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> operation <название>

Создание контейнера для уточнения действий кластера по отношению к указанному ресурсу.

**Синтаксис**

**set cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **operation** *название*

**delete cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **operation**

**show cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **operation**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    group имя_группы {
        ocf {
            provider {
                имя_производителя имя_службы {
                    name имя_ресурса {

    operation название {

    }
                    }
                }
            }
        }
    }
}
```

**Параметры**

*имя_группы*

Название группы, в которую вносится ресурс.

*имя_производителя*

Множественный узел. Название производителя службы ресурса. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_службы*

Множественный узел. Название службы, для которой настраивается ресурс. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_ресурса*

Множественный узел. Название ресурса.

*название*

Множественный узел. Название (идентификатор) операции, позволяющее различать их между собой.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Существует набор операций, которые ПО кластера неявным (для администратора) образом при необходимости выполняет по отношению к ресурсам — **start**, **stop** и **monitor** (последнее используется однократно в процедуре запуска ресурса для проверки его состояния перед собственно запуском). При помощи контейнера **ocf operation** можно через установку значений соответствующих атрибутов (описаны в командах ниже) влиять на поведение кластера во время исполнения этих операций.

Форма **set** этой команды используется для создания пустого контейнера для описания операций.

Форма **delete** этой команды используется для уничтожения существующего контейнера с операциями.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.34. cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> operation <название> action <действие>

Установка действия, для которого будет уточняться поведение кластера.

**Синтаксис**

**set cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **operation** *название* **action** *действие*

**delete cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **operation** *название* **action**

**show cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **operation** *название* **action**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    group имя_группы {
        ocf {
            provider {
                имя_производителя имя_службы {
                    name имя_ресурса {

operation название {

    action действие

}
                    }
                }
            }
        }
}
```

}

**Параметры**

*имя_группы*

Название группы, в которую вносится ресурс.

*имя_производителя*

Множественный узел. Название производителя службы ресурса. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_службы*

Множественный узел. Название службы, для которой настраивается ресурс. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_ресурса*

Множественный узел. Название ресурса.

*название*

Множественный узел. Название (идентификатор) операции, позволяющее различать их между собой.

*действие*

Действие, исполнение которого кластером будет уточняться. Допустимые значения параметра:

- **monitor**: проверка состояния ресурса;
- **start**: запуск ресурса;
- **status**: не используется;
- **stop**: остановка ресурса.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда предназначена для указания действия, для которого будет уточняться поведение кластера при помощи других атрибутов в рамках текущего контейнера **ocf operation**.

Форма **set** этой команды используется для указания нужного действия.

Форма **delete** этой команды используется для исключения указанного

действия.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### 28.2.35. cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> operation <название> enabled <состояние>

Включение или выключение уточнения поведения кластера. Параметры, атрибуты и их значения при этом не теряются и не изменяются.

#### Синтаксис

**set cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **operation** *название* **enabled** *состояние*

**delete cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **operation** *название* **enabled**

**show cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **operation** *название* **enabled**

#### Режим команды

Режим настройки.

#### Ветвь конфигурации

```
cluster {
    group имя_группы {
        ocf {
            provider {
                имя_производителя имя_службы {
                    name имя_ресурса {

operation название {

    enabled состояние

}
                    }
```

```
                    }
                }
            }
        }
    }
```

**Параметры**

*имя_группы*

Название группы, в которую вносится ресурс.

*имя_производителя*

Множественный узел. Название производителя службы ресурса. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_службы*

Множественный узел. Название службы, для которой настраивается ресурс. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_ресурса*

Множественный узел. Название ресурса.

*название*

Множественный узел. Название (идентификатор) операции, позволяющее различать их между собой.

*состояние*

**true** или **false**. **true** включает уточнение поведения кластера, **false** — выключает.

**Значение по умолчанию**

**true** — уточнение поведения кластера включено.

**Указания по использованию**

Эта команда предназначена для временного выключения уточнения поведения кластера без потери его атрибутов.

Форма **set** этой команды используется для установки нужного значения атрибута.

Форма **delete** этой команды используется для возвращения атрибуту значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### 28.2.36. cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> operation <название> interval <время>

Установка промежутка времени, через который нужно повторять указанное в атрибуте **ocf operation action** действие.

#### Синтаксис

**set cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **operation** *название* **interval** *время*

**delete cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **operation** *название* **interval**

**show cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **operation** *название* **interval**

#### Режим команды

Режим настройки.

#### Ветвь конфигурации

```
cluster {
    group имя_группы {
        ocf {
            provider {
                имя_производителя имя_службы {
                    name имя_ресурса {

operation название {

    interval время

}
```

```
                                    }
                                }
                            }
                        }
                    }
                }
```

**Параметры**

*имя_группы*

Название группы, в которую вносится ресурс.

*имя_производителя*

Множественный узел. Название производителя службы ресурса. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_службы*

Множественный узел. Название службы, для которой настраивается ресурс. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_ресурса*

Множественный узел. Название ресурса.

*название*

Множественный узел. Название (идентификатор) операции, позволяющее различать их между собой.

*время*

Длительность промежутка времени (в секундах), через который нужно повторять исполнение указанного в атрибуте **ocf operation action** действия.

**Значение по умолчанию**

По умолчанию установлено 0, действие должно выполняться только один раз.

**Указания по использованию**

Эта команда предназначена для управления периодичностью исполнения действия. Значение по умолчанию выключает периодичность, указание

любой длительности (в секундах) — включает периодическое исполнение действия через промежутки времени указанной длительности.

Форма **set** этой команды используется для установки нужного значения атрибута.

Форма **delete** этой команды используется для возвращения атрибуту значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### 28.2.37. cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> operation <название> on-fail <действие>

Указание действия, которое нужно предпринять кластеру, если текущее (то есть в рамках текущего контейнера **ocf operation**) уточнение его деятельности вызвало сбой.

#### Синтаксис

**set cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **operation** *название* **on-fail** *действие*

**delete cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **operation** *название* **on-fail**

**show cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **operation** *название* **on-fail**

#### Режим команды

Режим настройки.

#### Ветвь конфигурации

```
cluster {
    group имя_группы {
        ocf {
            provider {
                имя_производителя имя_службы {
                    name имя_ресурса {
```

```
        operation название {

              on-fail действие

        }
                              }
                        }
                  }
              }
        }
}
```

**Параметры**

*имя_группы*

Название группы, в которую вносится ресурс.

*имя_производителя*

Множественный узел. Название производителя службы ресурса. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_службы*

Множественный узел. Название службы, для которой настраивается ресурс. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_ресурса*

Множественный узел. Название ресурса.

*название*

Множественный узел. Название (идентификатор) операции, позволяющее различать их между собой.

*действие*

Действие, предпринимаемое кластером в ответ на сбой текущего уточнения его деятельности. Допустимые значения параметра:

- **block**: прекратить использование уточнения;
- **ignore**: не обращать внимания на сбои;

- **restart**: остановить ресурс, в отношении которого сбоит уточнение, и запустить его снова (возможно, в другой системе кластера);

- **standby**: перенести куда-нибудь все ресурсы с системы, в которой сбоит уточнение;

- **stop**: остановить ресурс, в отношении которого сбоит уточнение и не запускать его в других системах кластера.

**Значение по умолчанию**

При уточнении операции **stop** действием по умолчанию является **block**. При уточнении других операций действием по умолчанию является **stop**.

**Указания по использованию**

Форма **set** этой команды используется для установки нужного значения атрибута.

Форма **delete** этой команды используется для возвращения атрибуту значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.38. cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> operation <название> requires <условие>

Установка дополнительного условия, которое должно быть соблюдено перед запуском указанного ресурса.

**Синтаксис**

```
set cluster group имя_группы ocf provider
имя_производителя имя_службы name имя_ресурса operation
название requires условие

delete cluster group имя_группы ocf provider
имя_производителя имя_службы name имя_ресурса operation
название requires

show cluster group имя_группы ocf provider
имя_производителя имя_службы name имя_ресурса operation
название requires
```

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
     group имя_группы {
          ocf {
               provider {
                    имя_производителя имя_службы {
                         name имя_ресурса {

     operation название {

          requires условие

     }
                              }
                         }
                    }
               }
     }
}
```

**Параметры**

*имя_группы*

Название группы, в которую вносится ресурс.

*имя_производителя*

Множественный узел. Название производителя службы ресурса. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_службы*

Множественный узел. Название службы, для которой настраивается ресурс. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_ресурса*

Множественный узел. Название ресурса.

*название*

Множественный узел. Название (идентификатор) операции, позволяющее различать их между собой.

*условие*

Условие, соблюдение которого разрешит запуск ресурса. Допустимые значения параметра:

- **fencing**: ресурс можно запускать только тогда, когда большинство настроенных систем кластера активно, а системы, находящиеся в неопределённом состоянии или в состоянии сбоя — выключены;
- **nothing**: ресурс можно запускать без удовлетворения предварительных условий;
- **quorum**: ресурс можно запускать только тогда, когда большинство настроенных систем кластера активно.

**Значение по умолчанию**

По умолчанию установлено значение **quorum**.

**Указания по использованию**

Форма **set** этой команды используется для установки нужного значения атрибута.

Форма **delete** этой команды используется для возвращения атрибуту значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### 28.2.39. cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> operation <название> start-delay <время>

Установка промежутка времени (в секундах), на который нужно отложить запуск указанного ресурса.

**Синтаксис**

**set cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **operation** *название* **start-delay** *время*

**delete cluster group** *имя_группы* **ocf provider**

*имя_производителя имя_службы* **name** *имя_ресурса* **operation** *название* **start-delay**

**show cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **operation** *название* **start-delay**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    group имя_группы {
        ocf {
            provider {
                имя_производителя имя_службы {
                    name имя_ресурса {

operation название {

    start-delay время

}
                    }
                }
            }
        }
    }
}
```

**Параметры**

*имя_группы*

Название группы, в которую вносится ресурс.

*имя_производителя*

Множественный узел. Название производителя службы ресурса. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_службы*

Множественный узел. Название службы, для которой настраивается ресурс. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_ресурса*

Множественный узел. Название ресурса.

*название*

Множественный узел. Название (идентификатор) операции, позволяющее различать их между собой.

*время*

Отрезок времени в секундах, на который будет отложен запуск указанного в команде ресурса.

**Значение по умолчанию**

По умолчанию установлено значение 0.

**Указания по использованию**

Форма **set** этой команды используется для установки нужного значения атрибута.

Форма **delete** этой команды используется для возвращения атрибуту значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.40. cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> operation <название> timeout <время>

Установка времени ожидания (в секундах) завершения действия в рамках текущего контейнера **ocf operation**.

**Синтаксис**

**set cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **operation** *название* **timeout** *время*

**delete cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **operation** *название* **timeout**

**show cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **operation** *название* **timeout**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    group имя_группы {
        ocf {
            provider {
                имя_производителя имя_службы {
                    name имя_ресурса {

    operation название {

        timeout время

    }
                    }
                }
            }
        }
    }
}
```

**Параметры**

*имя_группы*

Название группы, в которую вносится ресурс.

*имя_производителя*

Множественный узел. Название производителя службы ресурса. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_службы*

Множественный узел. Название службы, для которой настраивается ресурс.

Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_ресурса*

Множественный узел. Название ресурса.

*название*

Множественный узел. Название (идентификатор) операции, позволяющее различать их между собой.

*время*

Длительность отрезка времени (в секундах), в течение которого кластер будет ожидать завершения действия, указанного атрибутом **ocf operation action**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Отсутствие завершения операции в течение указанного в команде времени рассматривается как сбой.

Форма **set** этой команды используется для установки нужного значения атрибута.

Форма **delete** этой команды используется для возвращения атрибуту значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.41. cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> priority <приоритет>

Установка приоритета, определяющего возможность исполнения указанной службы при большой нагрузке на систему.

**Синтаксис**

**set cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **priority** *приоритет*

**delete cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **priority**

**show cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **priority**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    group имя_группы {
        ocf {
            provider {
                имя_производителя имя_службы {
                    name имя_ресурса {

    priority приоритет
                    }
                }
            }
        }
    }
}
```

**Параметры**

*имя_группы*

Название группы, в которую вносится ресурс.

*имя_производителя*

Множественный узел. Название производителя службы ресурса. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_службы*

Множественный узел. Название службы, для которой настраивается ресурс. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_ресурса*

Множественный узел. Название ресурса.

*приоритет*

Число от 0 до 4294967295.

**Значение по умолчанию**

По умолчанию установлено значение 0.

**Указания по использованию**

При большой нагрузке на систему кластерное ПО будет освобождать системные ресурсы за счёт останова ресурсов кластера, начиная с ресурсов с самым низким приоритетом. Значение имеет не абсолютная величина приоритета, а то, какова она относительно приоритетов других ресурсов. Например, само по себе значение приоритета 4000000000 у ресурса ничего не значит, хоть и выглядит огромным. Однако, если кластер исполняет ещё один ресурс, с приоритетом 4000000001, то при большой нагрузке в первую очередь будет остановлен ресурс с приоритетом 4000000000.

Форма **set** этой команды используется для установки нужного значения атрибута.

Форма **delete** этой команды используется для возвращения атрибуту значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.42. cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> resource-stickiness <стоимость>

Установка «стоимости» переноса ресурса между системами.

**Синтаксис**

**set cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **resource-stickiness** *стоимость*

**delete cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **resource-stickiness**

**show cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **resource-stickiness**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    group имя_группы {
        ocf {
            provider {
                имя_производителя имя_службы {
                    name имя_ресурса {
                    resource-stickiness стоимость
                    }
                }
            }
        }
    }
}
```

**Параметры**

*имя_группы*

Название группы, в которую вносится ресурс.

*имя_производителя*

Множественный узел. Название производителя службы ресурса. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_службы*

Множественный узел. Название службы, для которой настраивается ресурс. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_ресурса*

Множественный узел. Название ресурса.

*стоимость*

Число от 0 до 4294967295.

**Значение по умолчанию**

По умолчанию установлено значение 0.

**Указания по использованию**

Этот атрибут определяет желательность отказа от переноса нормально работающей службы между системами. Число определяет «стоимость» (затратность) переноса службы между системами (в контексте времени простоя в обслуживании, вызванного этим переносом): чем оно больше, тем более затратным кластеру следует считать перенос службы, из-за чего с ростом этого значения перенос становится всё менее желательным.

Форма **set** этой команды используется для установки нужного значения атрибута.

Форма **delete** этой команды используется для возвращения атрибуту значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.43. cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы> name <имя_ресурса> target-role <состояние>

Установка состояния, в котором кластер должен стараться поддерживать службу-клон.

**Синтаксис**

**set cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **target-role** *состояние*

**delete cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **target-role**

**show cluster group** *имя_группы* **ocf provider** *имя_производителя имя_службы* **name** *имя_ресурса* **target-role**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    group имя_группы {
        ocf {
```

```
                    provider {
                        имя_производителя имя_службы {
                            name имя_ресурса {

        target-role состояние
                            }
                        }
                    }
                }
            }
        }
```

**Параметры**

*имя_группы*

Название группы, в которую вносится ресурс.

*имя_производителя*

Множественный узел. Название производителя службы ресурса. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_службы*

Множественный узел. Название службы, для которой настраивается ресурс. Допустимые значения параметра такие же, как в команде **cluster group <имя_группы> ocf provider <имя_производителя> <имя_службы>**.

*имя_ресурса*

Множественный узел. Название ресурса.

*состояние*

Состояние, в котором кластер будет стараться удерживать службу. Допустимые значения параметра:

- **stopped**: удерживать ресурс в остановленном состоянии;
- **started**: запустить ресурс и оставить его в состоянии «ведомый»;
- **master**: запустить ресурс с перевести его в состояние «ведущий».

**Значение по умолчанию**

По умолчанию установлено значение **started**.

**Указания по использованию**

Эта команда предназначена для управления состоянием ресурсов-клонов, которые поддерживают работу в одном из двух режимов — «ведущий» или «ведомый». Эти режимы связаны с поведением экземпляров одного и того же ресурса в отношении друг друга при одновременной работе в разных системах кластера и не имеют отношения к схеме работы всего кластера с тем же названием («ведущий-ведомый»).

Форма **set** этой команды используется для установки нужного значения атрибута.

Форма **delete** этой команды используется для возвращения атрибуту значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.44. cluster infrastructure

Создание пустого контейнера для хранения параметров кластерной инфраструктуры, не связанной напрямую с управлением службами и узлами.

**Синтаксис**

```
set cluster infrastructure
delete cluster infrastructure
show cluster infrastructure
```

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    infrastructure {
    }
}
```

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Форма **set** этой команды используется для создания пустого контейнера для параметров инфраструктуры кластера.

Форма **delete** этой команды используется для уничтожения контейнера с параметрами инфраструктуры кластера целиком.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.45. cluster infrastructure interface

Создание пустого контейнера для параметров сетевого интерфейса, через который будет производиться обмен собственными данными кластера.

**Синтаксис**

```
set cluster infrastructure interface
delete cluster infrastructure interface
show cluster infrastructure interface
```

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    infrastructure {
        interface {
        }
    }
}
```

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Из соображений надёжности выбранный для «сердцебиения» и обмена

другими собственными данными сетевой интерфейс стоит избавить от других задач (трафика) и физически изолировать от других сетей и сетевой инфраструктуры. То есть для обмена собственными данными кластера должна быть выделена отдельная сеть, как логически, так и физически.

Форма **set** этой команды используется для создания пустого контейнера для параметров сетевого интерфейса.

Форма **delete** этой команды используется для

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.46. cluster infrastructure interface bind-net-addr <адрес_сети>

Установка адреса *сети*, через сетевой интерфейс с которым будет производиться обмен собственными данными кластера.

**Синтаксис**

**set cluster infrastructure interface bind-net-addr** *адрес_сети*

**delete cluster infrastructure interface bind-net-addr**

**show cluster infrastructure interface bind-net-addr**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    infrastructure {
        interface {
            bind-net-addr адрес_сети
        }
    }
}
```

**Параметры**

*адрес_сети*

Адрес IPv4 сети в виде nnn.nnn.nnn.nnn, например: 192.168.1.0

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Форма **set** этой команды используется для указания кластерному ПО сетевого интерфейса устройства, через который нужно обмениваться собственными данными с другими системами кластера.

Форма **delete** этой команды используется для уничтожения привязки к интерфейсу.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.47. cluster infrastructure interface broadcast <состояние>

Включение или выключение использования широковещательной передачи для обмена собственными данными между системами кластера.

**Синтаксис**

**set cluster infrastructure interface broadcast** *состояние*

**delete cluster cluster infrastructure interface broadcast**

**show cluster cluster infrastructure interface broadcast**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    infrastructure {
        interface {
            broadcast состояние
        }
    }
}
```

**Параметры**

*состояние*

**true** или **false**. **true** включает использование широковещательной передачи для обмена собственными данными между системами кластера.

#### Значение по умолчанию

По умолчанию установлено значение **false**.

#### Указания по использованию

Этот параметр вступает в противоречие с параметром **mcast-addr** — их нельзя использовать совместно. Если предполагается использовать многоадресное вещание, а не широковещательное, то **broadcast** нужно установить в **false**.

Форма **set** этой команды используется для включения широковещательного обмена собственными данными между системами кластера.

Форма **delete** этой команды используется для возвращения параметру значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.48. cluster infrastructure interface mcast-addr <адрес>

Включение обмена собственными данными между системами кластера через многоадресное вещание и задаёт адрес IPv4 для этого.

#### Синтаксис

**set cluster infrastructure interface mcast-addr** *адрес*

**delete cluster infrastructure interface mcast-addr**

**show cluster infrastructure interface mcast-addr**

#### Режим команды

Режим настройки.

#### Ветвь конфигурации

```
cluster {
    infrastructure {
        interface {
            mcast-addr адрес
        }
    }
}
```

**Параметры**

*адрес*

Адрес IPv4, используемый для многоадресной передачи, в виде nnn.nnn.nnn.nnn, например: 226.94.1.1

**Значение по умолчанию**

**226.94.1.1**

**Указания по использованию**

Этот параметр вступает в противоречие с параметром **broadcast**, включаемый через оба эти параметра функционал нельзя использовать одновременно.

Форма **set** этой команды используется для включения многоадресного вещания и задания соответствующего адреса.

Форма **delete** этой команды используется для выключения многоадресного вещания, значение по умолчанию при этом не теряется.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

## 28.2.49. cluster infrastructure interface mcast-port <порт>

Установка порта UDP, на который будет вестись многоадресное вещание.

**Синтаксис**

**set cluster infrastructure interface mcast-port** *порт*

**delete cluster infrastructure interface mcast-port**

**show cluster infrastructure interface mcast-port**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    infrastructure {
        interface {
            mcast-port порт
        }
    }
```

```
}
```

**Параметры**

*порт*

Номер порта UDP.

**Значение по умолчанию**

По умолчанию установлено значение 5405.

**Указания по использованию**

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.

## 28.2.50. cluster infrastructure net-mtu <mtu>

Установка величины MTU.

**Синтаксис**

**set cluster infrastructure net-mtu** *mtu*

**delete cluster infrastructure net-mtu**

**show cluster infrastructure net-mtu**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
     infrastructure {
          net-mtu mtu
     }
}
```

**Параметры**

*mtu*

Число, в диапазоне от 1500 до 8982.

**Значение по умолчанию**

По умолчанию установлено значение 1500.

**Указания по использованию**

Эта команда используется для задания MTU (Maximum Transmit Unit) — максимального размера блока (в байтах), который может быть передан на канальном уровне сетевой модели OSI. Увеличение MTU обычно ускоряет передачу больших объёмов данных в основном за счёт сокращения количества разных операций, связанных с разбивкой данных на блоки заданного размера на передающей стороне и сборкой их обратно на принимающей. В то же время, «нестандартные» величины MTU должны поддерживаться всеми участниками обмена (включая сетевое оборудование — сетевые платы, коммутаторы и так далее).

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.

## 28.2.51. cluster infrastructure secauth <состояние>

Включение или выключение аутентификации и шифрования внутренних данных кластера при обмене.

**Синтаксис**

**set cluster infrastructure secauth** *состояние*

**delete cluster infrastructure secauth**

**show cluster infrastructure secauth**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    infrastructure {
        secauth состояние
```

```
        }
    }
```

**Параметры**

*состояние*

**true** или **false**. **true** включает аутентификацию и шифрование, **false** — выключает.

**Значение по умолчанию**

**true**

**Указания по использованию**

Эта команда предназначена для включения или выключения проверки подлинности (аутентификации) сообщений кластера и их шифрования. Поскольку это ресурсоёмкие операции (особенно шифрование), то рекомендуется их задействовать только когда безопасность обмена является ключевым требованием (например, при построении кластера на сетях, находящихся под чужим контролем). К примеру, в сети Ethernet в режиме 100 Мбит/с и MTU 1500 байт при включённых аутентификации и шифровании и 100% загрузке процессора, работающего на частоте 3 ГГц, пропускная способность составит примерно 9 МБайт/с. Отключение аутентификации и шифрования при сохранении прочих условий повысит пропускную способность до 10 Мбайт/с, а загрузку процессора понизит до 20%.

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.

## 28.2.52. cluster infrastructure threads <количество>

Включение или выключение распараллеливания шифрования и отправки сообщений систем кластера на указанное количество потоков (нитей).

**Синтаксис**

**set cluster infrastructure threads** *количество*

**delete cluster infrastructure threads**

**show cluster infrastructure threads**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    infrastructure {
        threads количество
    }
}
```

**Параметры**

*количество*

Количество параллельных системных потоков (нитей) исполнения, используемых для шифрования и отправки сообщений другим системам кластера. Обычно это число на 1 меньше количества процессорных ядер системы, но его можно устанавливать в 2 или 3 и для одноядерных однопроцессорных систем, если в целом они не сильно загружены, что может немного повысить степень использования («утилизацию») процессоров.

**Значение по умолчанию**

Значение по умолчанию 0, распараллеливание выключено.

**Указания по использованию**

Эта команда предназначена для повышения скорости шифрования и отправки сообщений кластера за счёт распараллеливания этой деятельности по указанному числу системных потоков (нитей) исполнения. Изменение параметра даёт эффект только тогда, когда аутентификация и шифрования сообщений включены (через параметр **secauth**, рассмотренный выше). Существенный прирост производительности от такого распараллеливания достигается только в многоядерных системах (с одним или несколькими процессорами).

Форма **set** этой команды используется для включения распараллеливания на указанное число потоков либо для его выключения через указание значения «**0**».

Форма **delete** этой команды используется для возвращения параметру значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### 28.2.53. cluster no-quorum-policy <действие>

Установка реакции кластера на исчезновение кворума.

**Синтаксис**

```
set cluster no-quorum-policy действие
delete cluster no-quorum-policy
show cluster no-quorum-policy
```

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    no-quorum-policy действие
}
```

**Параметры**

*действие*

Реакция кластера на отсутствие кворума. Допустимые значения параметра:

- **ignore**: не обращать на это внимания;
- **freeze**: продолжить управление ресурсами: не заниматься восстановлением ресурсов в системах, отвалившихся от текущего подкластера;
- **stop**: остановить все ресурсы в текущем подкластере;
- **suicide**: остановить («пристрелить») все системы в текущем подкластере.

**Значение по умолчанию**

Значение по умолчанию **stop**.

**Указания по использованию**

Эта команда предназначена для настройки поведения кластера при такой

потере связи с одной или несколькими системами-участниками, при которой потерялся и кворум. Поскольку состояние отвалившихся систем в общем случае неизвестно, то считается, что произошло разделение кластера на два или больше подкластера, в каждом из которых могут быть одна или больше работающих систем.

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.

## 28.2.54. cluster pe-error-series-max <количество>

Установка количества вызвавших ошибки входящих сообщений движка политик (Policy Engine), информацию о которых нужно записать в журнал событий.

**Синтаксис**

```
set cluster pe-error-series-max количество
delete cluster pe-error-series-max
show cluster pe-error-series-max
```

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    pe-error-series-max количество
}
```

**Параметры**

*количество*

В журнал событий будет помещена информация о не более чем указанном количестве сообщений, вызвавших ошибки.

**Значение по умолчанию**

Значение по умолчанию -1, в журнал помещается информация обо всех вызвавших ошибки сообщениях.

**Указания по использованию**

Эта команда предназначена для упрощения отладки и поиска источников проблем, ограничивая объём информации, требующей изучения.

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.

## 28.2.55. cluster pe-input-series-max <количество>

Установка количества «нормальных» входящих сообщений движка политик (Policy Engine), информацию о которых нужно записать в журнал событий.

**Синтаксис**

```
set cluster pe-input-series-max количество
delete cluster pe-input-series-max
show cluster pe-input-series-max
```

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    pe-input-series-max количество
}
```

**Параметры**

*количество*

В журнал событий будет помещена информация о не более чем указанном количестве «нормальных» сообщений.

**Значение по умолчанию**

Значение по умолчанию -1, в журнал помещается информация обо всех «нормальных» сообщениях.

**Указания по использованию**

Эта команда предназначена для упрощения отладки и поиска источников

проблем, ограничивая объём информации, требующей изучения.

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.

## 28.2.56. cluster pe-warn-series-max <количество>

Установка количества вызвавших предупреждения входящих сообщений движка политик (Policy Engine), информацию о которых нужно записать в журнал событий.

**Синтаксис**

```
set cluster pe-warn-series-max количество
delete cluster pe-warn-series-max
show cluster pe-warn-series-max
```

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    pe-warn-series-max количество
}
```

**Параметры**

*количество*

В журнал событий будет помещена информация о не более чем указанном количестве вызвавших предупреждения сообщений.

**Значение по умолчанию**

По умолчанию установлено значение -1, в журнал помещается информация обо всех вызвавших предупреждения сообщениях.

**Указания по использованию**

Эта команда предназначена для упрощения отладки и поиска источников проблем, ограничивая объём информации, требующей изучения.

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.

## 28.2.57. cluster start-failure-is-fatal <состояние>

Включение или выключение восприятия кластером сбоев при запуске ресурса как фатальных.

**Синтаксис**

**set cluster start-failure-is-fatal** *состояние*

**delete cluster start-failure-is-fatal**

**show cluster start-failure-is-fatal**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    start-failure-is-fatal состояние
}
```

**Параметры**

*состояние*

**true** или **false**. **true** включает восприятие кластером сбоев при запуске ресурса как фатальных, **false** выключает.

**Значение по умолчанию**

**true**

**Указания по использованию**

Эта команда предназначена для управления переносом ресурса в случае сбоев при его запуске. При значении **true** сбой ресурса при запуске обычно вызывает его перенос в какую-то другую систему кластера. При значении **false** просто наращивается счётчик сбоев ресурса и решение о его переносе принимается с учётом параметров **migration-threshold** и **resource-stickiness**.

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.

## 28.2.58. cluster stop-orphan-actions <состояние>

Включение или выключение отмены действий, информация о которых стирается из конфигурации кластера.

**Синтаксис**

**set cluster stop-orphan-actions** *состояние*

**delete cluster stop-orphan-actions**

**show cluster stop-orphan-actions**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    stop-orphan-actions состояние
}
```

**Параметры**

*состояние*

**true** или **false**. **true** включает отмену исключаемых из конфигурации кластера действий, **false** указывает кластеру оставить их в работе.

**Значение по умолчанию**

**true**

**Указания по использованию**

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.

## 28.2.59. cluster stop-orphan-resources <состояние>

Включение или выключение останова ресурсов, информация о которых стирается из конфигурации кластера.

**Синтаксис**

**set cluster stop-orphan-resources** *состояние*

**delete cluster stop-orphan-resources**

**show cluster stop-orphan-resources**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    stop-orphan-resources состояние
}
```

**Параметры**

*состояние*

**true** или **false**. **true** включает останов исключаемых из конфигурации кластера ресурсов, **false** указывает кластеру оставить их в работе.

**Значение по умолчанию**

**true**

**Указания по использованию**

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.

## 28.2.60. cluster symmetric-cluster <состояние>

Включение или выключение возможности запуска всех ресурсов в любой из систем кластера.

**Синтаксис**

**set cluster symmetric-cluster** *состояние*

**delete cluster symmetric-cluster**

**show cluster symmetric-cluster**

**Режим команды**

Режим настройки.

**Ветвь конфигурации**

```
cluster {
    symmetric-cluster состояние
}
```

**Параметры**

*состояние*

**true** или **false**. **true** разрешает запуск всех ресурсов в любой системе кластера, **false** — запрещает.

**Значение по умолчанию**

**true**

**Указания по использованию**

Эта команда предназначена для управления запуском ресурса в том случае, когда нет явного указания о том, в какой из систем кластера его запускать. Если этот параметр установлен в **false** и в параметрах ресурса нет указания где его запускать, то он запущен не будет. Если он установлен в **true**, то ресурс будет запускаться либо в указанной в его параметрах системе (при отсутствии каких-либо противопоказаний к этому), либо кластерное ПО выберет систему для него самостоятельно.

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.

# 29. СОХРАНЕНИЕ СОСТОЯНИЯ СИСТЕМЫ ОТСЛЕЖИВАНИЯ СОЕДИНЕНИЙ ПРИ СБОЯХ

В этом разделе описана настройка средств Altell NEO, обеспечивающих сохранение состояния системы отслеживания соединений при сбоях.

## 29.1. 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 информацией 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 Altell NEO этой потери можно избежать благодаря использованию установленного в них инструментария **conntrack-tools** и организации кластера.

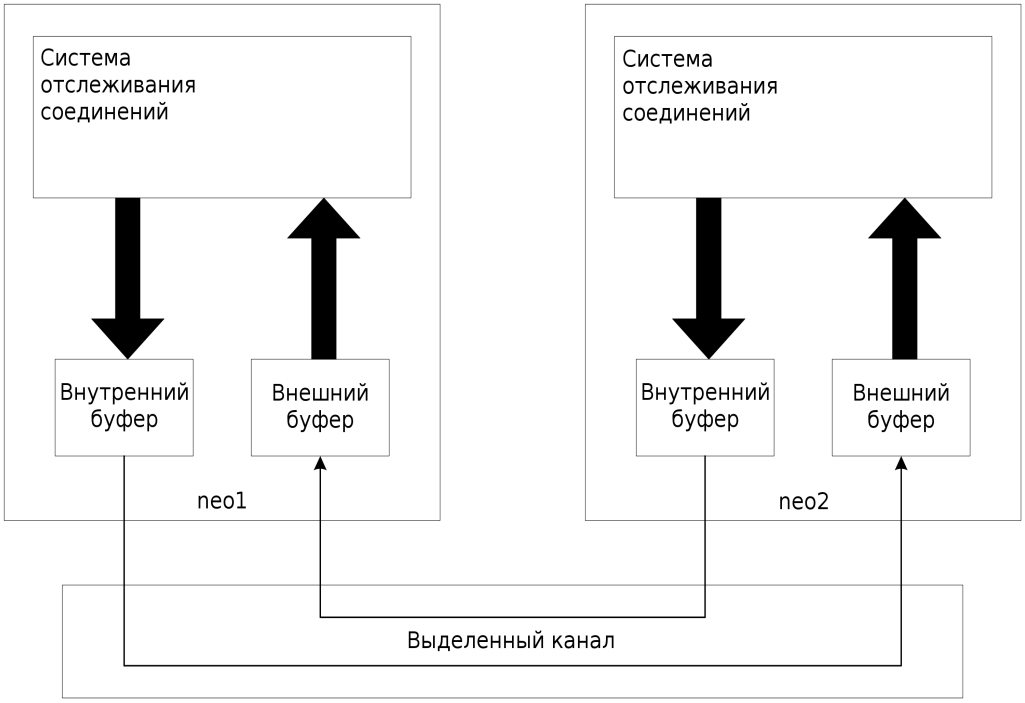
## 29.2. Обзор реализации

Система отслеживания соединений, как и вся система Netfilter, находятся в ядре ОС, в 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 Altell NEO 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

92:

*Рисунок 92 - 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.

## 29.3. 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).

## 29.4. Настройка сохранения состояния системы отслеживания соединений

### 29.4.1. 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 (вне кластера):

*Пример 29.1 - пример настройки conntrack-sync для самостоятельной работы*

| Действие | Команда |
|---|---|
| Учитывать соединения через локальный петлевой интерфейс вряд ли необходимо, поэтому добавляем связанный с ним адрес в список игнорируемых. | admin@neo# **set service conntrack-sync address-ignore ipv4 127.0.0.1**<br>[edit] |
| 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. | admin@neo# **set service conntrack-sync address-ignore ipv4 226.0.0.0/24**<br>[edit] |
| Задаём размер буфера (в байтах) для сообщений, которые **conntrackd** будет получать от системы отслеживания | admin@neo# set service conntrack-sync event-listen-queue-size 16777216 |

соединений ядра.

```
[edit]
```

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.

```
admin@neo# set service conntrack-sync interface eth2
[edit]
```

Задаём адрес назначения (идентификатор группы) для многоадресного вещания.

```
admin@neo# set service conntrack-sync mcast-group 226.0.0.50
[edit]
```

Задаём размер приёмных и передающих буферов (в байтах), использующихся в обмене информацией о соединениях с другими службами **conntrack-sync**.

```
admin@neo# set service conntrack-sync sync-queue-size 2097152
[edit]
```

Смотрим, что получилось.

```
admin@neo# 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]
```

Применяем. В процессе применения конфигурации система также запустит

```
admin@neo# commit
Starting conntrack-sync...
```

службу **conntrackd**. [edit]

При самостоятельной (вне кластера) 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.

В то же время, в кластере есть агент **conntrack-failover**, при помощи которого можно создать кластерный ресурс и указать кластерному ПО следить за его состоянием и, при необходимости, давать команду ведомой службе **conntrack-sync** загрузить содержимое своего внешнего буфера в ядро.

Создание ресурса кластера на базе **conntrack-failover** рассмотрено в разделе 28. Кластеризация в примере, описывающем построение отказоустойчивого клиента VPN.

### 29.4.2. 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 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 sync-queue-size <размер>` | Установка размера буферов для сообщений о состоянии соединений от/для других служб |

| | |
|---|---|
| | **conntrack-sync**. |
| Эксплуатационные команды | |
| `clear connection-tracking` | Очистка памяти ядра, содержащей информацию о текущих соединениях. |
| `clear conntrack-sync external-cache` | Очистка внешнего буфера и запрос актуальных данных у других систем. |
| `clear conntrack-sync 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. |
| `restart conntrack-sync` | Перезапуск службы **conntrack-sync**. |
| `show conntrack-sync external-cache` | Вывод содержимого внешнего буфера. |
| `show conntrack-sync internal-cache` | Вывод содержимого внутреннего буфера. |
| `show conntrack-sync statistics` | Вывод статистической информации о работе службы **conntrack-sync**. |
| `show conntrack-sync status` | Вывод информации о текущем состоянии службы **conntrack-sync**. |

### 29.4.3. 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.

**Оператор настройки**

```
service {
    conntrack-sync {
        address-ignore {
            версия_IP адрес
        }
    }
}
```

**Параметры**

*версия_IP*

**ipv4** или **ipv6**. Множественный узел. Версия межсетевого протокола (Internet Protocol — IP), по правилам которой приведён адрес системы или сети в следующем параметре.

*адрес*

Множественный узел. Адрес системы или сети, для которого следует игнорировать сообщения от системы отслеживания соединений, например: **192.168.1.10** (адрес системы) и **192.168.1.0/24** (адрес сети).

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Команда используется для указания адреса системы или сети, сообщения про который 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.

### 29.4.4. 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.

**Оператор настройки**

```
service {
    conntrack-sync {
        event-listen-queue-size размер
    }
}
```

**Параметры**

*размер*

Размер буфера в байтах.

**Значение по умолчанию**

**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.

### 29.4.5. service conntrack-sync interface <имя_интерфейса>

Установка интерфейса, через который будет происходить обмен информацией о состоянии соединений.

**Синтаксис**

```
set service conntrack-sync interface имя_интерфейса
delete service conntrack-sync interface
show service conntrack-sync interface
```

**Режим команды**

Режим настройки.

**Оператор настройки**

```
service {
    conntrack-sync {
        interface имя_интерфейса
    }
}
```

**Параметры**

*имя_интерфейса*

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 «сердцебиения» и 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.

## 29.4.6. 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.

**Оператор настройки**

```
service {
    conntrack-sync {
        mcast-group адрес
    }
}
```

**Параметры**

*адрес*

Адрес IPv4 назначения многоадресной («multicast») передачи, используемый для рассылки информации о соединениях.

**Значение 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.

## 29.4.7. service conntrack-sync sync-queue-size <размер>

Установка размера буферов для сообщений о 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.

**Оператор настройки**

```
service {
    conntrack-sync {
        sync-queue-size размер
    }
}
```

**Параметры**

*размер*

Размер буферов в байтах. Оба буфера (и на приём, и на передачу) будут иметь такой — одинаковый — размер.

**Значение по умолчанию**

**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.

## 29.4.8. clear connection-tracking

Очистка памяти ядра, содержащей информацию о текущих 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.

## 29.4.9. clear conntrack-sync external-cache

Очистка внешнего буфера и запрос актуальных данных у других систем.

**Синтаксис**

```
clear conntrack-sync 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.

## 29.4.10. clear conntrack-sync 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**

```
clear conntrack-sync 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.

## 29.4.11. restart conntrack-sync

Перезапуск службы **conntrack-sync**.

**Синтаксис**

```
restart conntrack-sync
```

**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.

## 29.4.12. show conntrack-sync external-cache

Вывод содержимого внешнего буфера.

**Синтаксис**

```
show conntrack-sync external-cache
```

**Режим команды**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда предназначена для отображения содержимого внешнего буфера службы **conntrack-sync** локальной системы.

**Примеры**

Ниже приведён пример такого вывода. Показано возможное содержимое внутреннего буфера удаленной системы, которое и копируется во внешний буфер службы **conntrack-sync** локальной системы, содержимое которого уже отображается командой **show conntrack-sync external-cache**.

*Пример 29.2 - Вывод команды show conntrack-sync external-cache*

```
admin@neo:~$ show conntrack-sync external-cache
Source                  Destination
          Protocol
```

```
|192.168.74.1|:138       |192.168.74.255|:138 udp [17]

|192.168.74.1|:1140      |192.168.74.128|:22
      tcp [6]

|192.168.74.1|:1145      |192.168.74.200|:22
      tcp [6]

|172.16.117.133|:55964   |10.1.0.23|:80
           tcp [6]

|10.3.0.182|:1151        |10.3.0.15|:22
           tcp [6]
```

## 29.4.13. show conntrack-sync internal-cache

Вывод содержимого внутреннего буфера.

**Синтаксис**

**show conntrack-sync internal-cache**

**Режим команды**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда предназначена для отображения содержимого внутреннего буфера службы **conntrack-sync**.

**Примеры**

Ниже приведён пример такого вывода. Показано возможное содержимое внутреннего буфера службы **conntrack-sync** в локальной системе, полученное по команде **show conntrack-sync internal-cache**.

*Пример 29.3 - Вывод команды show conntrack-sync internal-cache*

```
admin@neo:~$ show conntrack-sync internal-cache

Source                    Destination
          Protocol

|192.168.74.1|:1140      |192.168.74.128|:22
     tcp [6]
```

```
|192.168.74.1|:1145      |192.168.74.200|:22
     tcp [6]

|10.3.0.182|:1151        |10.3.0.15|:22
          tcp [6]

|172.16.117.128|         |224.0.0.18|
          unknown [112]
```

## 29.4.14. show conntrack-sync statistics

Вывод статистической информации о работе службы **conntrack-sync**.

**Синтаксис**

**show conntrack-sync statistics**

**Режим команды**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда предназначена для вывода статистических данных, относящихся к работе службы **conntrack-sync** в локальной системе.

**Примеры**

В примере ниже приведён возможный результат работы команды **show conntrack-sync statistics**.

Выходные данные разбиты на пять разделов:

- статистика для внутреннего буфера;
- статистика для внешнего буфера;
- трафик, обработанный уничтоженными соединениями, перечисленными в первом разделе;
- статистика трафика многоадресных передач, порождаемого обменом между службами **conntrack-sync** сообщениями о состоянии соединений;
- статистика отслеживания сообщений многоадресных передач, используемая для оценки надежности передачи сообщений по UDP.

*Пример 29.4 - Вывод команды show conntrack-sync statistics*

```
admin@:~$ show conntrack-sync statistics

cache internal:

current active connections:
     3

connections created:
     3477      failed:
     0

connections updated:
     12        failed:
     0

connections destroyed:
     3474      failed:
     0


cache external:

current active connections:
     4

connections created:
     11        failed:
     0

connections updated:
     8         failed:
     0

connections destroyed:
     7         failed:
     0


traffic processed:

          135219375 Bytes
     163080 Pckts


multicast traffic (active device=eth1):

     333248    Bytes sent
          327592    Bytes recv

     8515      Pckts sent
```

```
            8137      Pckts recv

        0         Error send
            0         Error recv


    message tracking:

            0         Malformed msgs
            0         Lost msgs
```

### 29.4.15. show conntrack-sync status

Вывод информации о текущем состоянии службы **conntrack-sync**.

**Синтаксис**

**show conntrack-sync status**

**Режим команды**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда предназначена для отображения информации о текущем состоянии службы **conntrack-sync**.

**Примеры**

В примере ниже приведён возможный результат работы команды **show conntrack-sync status**.

*Пример 29.5 - Вывод команды show conntrack-sync status*

```
admin@neo:~$ show conntrack-sync status
conntrack-sync status
---------------------
process id          : 2158
sync-interface      : eth2
cluster-group       :
```

# 30. ФИЛЬТРАЦИЯ ПОЧТЫ

## 30.1. Общие сведения

Altell NEO может функционировать в качестве прокси-сервера SMTP, позволяя обеспечить полную проверку почтовой корреспонденции на наличие спама и вирусов. Прокси-сервер SMTP поддерживает работу в двух режимах: в режиме прозрачного проксирования, а также в режиме проксирования для заданного сервера.

Все почтовые сообщения, перехватываемые на фильтруемом интерфейсе будут автоматически перенаправляться на адрес, который прослушивается прокси-сервером SMTP (указывается при помощи команды service smtpproxy listen-address <адрес>). После этого, в том случае если включен соответствующий режим, сообщения сканируются на наличие спама и вирусов, а затем перенаправляются либо на тот же IP-адрес, куда сообщение было направлено изначально (если используется режим прозрачного проксирования), либо на IP-адрес сервера, заданного при помощи команды service smtpproxy fixed-server address <адрес> (если используется режим проксирования для заданного сервера).

*Внимание! В качестве адреса, прослушиваемого прокси-сервером, рекомендуется указывать адрес одного из внутренних интерфейсов системы (обращенных во внутренний сегмент сети). В противном случае прокси-сервер SMTP будет осуществлять открытую ретрансляцию SMTP, то есть позволит бесконтрольно пересылать любые почтовые сообщения из внешней сети. При этом следует учитывать, что в том случае если значение для этого параметра явно не указано, прокси-сервер прослушивает все настроенные в системе адреса, в том числе адреса, настроенные на внешних интерфейсах системы!*

Режим проксирования для заданного сервера может быть использован для обеспечения защиты почтового сервера, находящегося во внутренней локальной сети, когда в записи MX для защищаемого домена указан маршрутизатор, на котором запущен прокси-сервер SMTP. В этом случае сообщения будут приходить на прокси-сервер SMTP, который будет осуществлять сканирование на наличие спама и вирусов, а затем перенаправлять сообщения на внутренний почтовый сервер.

При этом следует учитывать, что в том случае если используется шифрование передаваемой почты с использованием TLS, почтовые сообщения не могут быть просканированы. При использовании режима фильтрации для заданного сервера рекомендуется отключить возможность включения TLS (STARTTLS) на заданном сервере, для того чтобы почтовый фильтр имел возможность работы со всей почтой.

## 30.2. Антивирусная проверка

Сканирование почтовых сообщений выполняется на лету. В том случае если сообщение классифицировано как содержащее спам или вирус, сеанс SMTP прерывается. Письмо отвергается в ответ на команду DATA, то есть, при отклонении корректного письма MTA отправителя должен сгенерировать письмо о недоставке отправителю. Команды service smtpproxy lock on spam <режим> и service smtpproxy lock on virus <режим> позволяют установить режим блокировки узла, передавшего зараженное сообщение. Период блокировки устанавливается при помощи команды service smtpproxy lock duration <время>.

Тип используемого для сканирования антивирусного пакета указывается при помощи команды service smtpproxy antivirus type <средство_фильтрации>.Возможно использование пакетов антивирусного ПО ClamAV или Kaspersky AV. Они могут быть использованы как по отдельности, так и совместно. Если письмо будет классифицировано как содержащее вирусы хотя бы одним из используемых средств, оно будет отброшено. В том случае если значение для данного параметра не указано, проверка на вирусы не производится.

## 30.3. Проверка на спам

Фильтрация спама осуществляется при помощи средства Spamassassin. Режим проверки почтовых сообщений на наличие спама включается при помощи команды service smtpproxy antispam type <средство_фильтрации>.

Команда service smtpproxy antispam spamassassin spam-threshold <порог> позволяет указать пороговое значение, которое используется средством SpamAssassin при проверке писем на спам.

## 30.4. Примеры настройки

В данном разделе приведены следующие примеры:

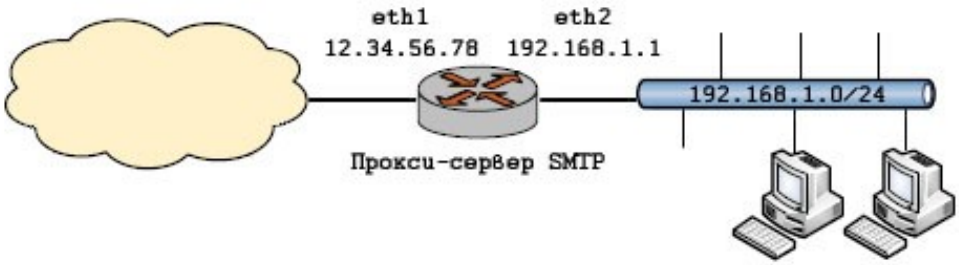
- Пример 30.1 - Настройка режима прозрачного проксирования;
- Пример 30.2 - Настройка режима проксирования для заданного сервера.

### 30.4.1. Режим прозрачного проксирования

В примере 30.1 приведен пример настройки Altell NEO в качестве прокси-сервера в прозрачном режиме. В данном примере в качестве фильтруемого интерфейса указывается интерфейс **eth2**, в качестве прослушиваемого адреса указан адрес 192.168.2.1 внутреннего интерфейса **eth2.** Интерфейсы должны быть заранее настроены.

Фильтрации подлежит весь трафик SMTP, отправляемый из локальной сети 192.168.1.0/24. При классификации сообщения как содержащего спам или вирус, все сеансы SMTP отправителя сообщения будут заблокированы на 1 час.

*Рисунок 93 - Режим прозрачного проксирования*




Для настройки режима прозрачного проксирования необходимо выполнить следующие действия в режиме настройки.

*Пример 30.1 - Настройка режима прозрачного проксирования*

| Действие | Команда |
|---|---|
| Указание интерфейса, на котором будет осуществляться фильтрация. | `admin@neo# set service smtpproxy filter-interface eth2`<br>`[edit]` |
| Указание адреса, который прослушивает | `admin@neo# set service smtpproxy` |

| | |
|---|---|
| прокси-сервер SMTP. | **listen-address 192.168.1.1**<br>[edit] |
| Включение режима сканирования сообщений на наличие спама с использованием Spamassassin. | admin@neo# **set service smtpproxy antispam type spamassassin**<br>[edit] |
| Включение режима сканирования сообщений на наличие вирусов с использованием Clam Antivirus. | admin@neo# **set service smtpproxy antivirus type clamav**<br>[edit] |
| Включение режима сканирования сообщений на наличие вирусов с использованием Kaspersky Antivirus. | admin@neo# **set service smtpproxy antivirus type kav**<br>[edit] |
| Включение режима блокировки сеансов SMTP от узла, передавшего сообщение, которое было классифицировано как спам. | admin@neo# **set service smtpproxy lock on spam true**<br>[edit] |
| Включение режима блокировки сеансов SMTP от узла, передавшего сообщение, которое было классифицировано как содержащее вирус. | admin@neo# **set service smtpproxy lock on virus true**<br>[edit] |
| Включение регистрации в системном журнале команд HELO/EHLO, а также адресов отправителя и получателя. | admin@neo# **set service smtpproxy log accepted from true**<br>[edit]<br>admin@neo# **set service smtpproxy log accepted to true**<br>[edit]<br>admin@neo# **set service smtpproxy log rejected to true**<br>[edit]<br>admin@neo# **set service smtpproxy** |

```
log rejected from true
[edit]
admin@neo# set service smtpproxy
log helo true
[edit]
```

Фиксация настройки.

```
admin@neo# commit
Restarting SMTP Gateway: smtp-
gated.
[edit]
```

Вывод настройки.

```
admin@neo# show service smtpproxy
   antispam {
       type spamassassin
   }
   antivirus {
       type clamav
       type kav
   }
   filter-interface eth2
   listen-address 192.168.1.1
   lock {
       on {
           spam true
           virus true
       }
   }
   log {
       accepted {
           from true
           to true
       }
       helo true
```

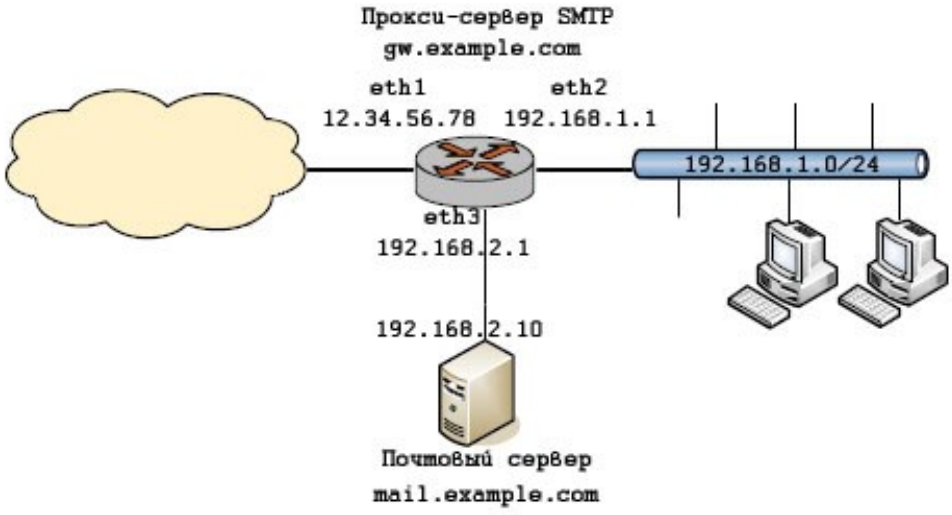
```
            rejected {
                from true
                to true
            }
        }
    [edit]
```

### 30.4.2. Режим проксирования для заданного сервера

В примере 30.2 приведена настройка режима проксирования для заданного сервера, который используется для обеспечения защиты почтового сервера mail.example.com, находящегося во внутренней локальной сети. В записи MX для защищаемого домена указано имя маршрутизатора gw.example.com, на котором запущен прокси-сервер SMTP. В настройках прокси-сервера с помощью команды service smtpproxy fixed-server address <адрес> указывается адрес защищаемого сервера 192.168.2.10. В этом случае сообщения будут приходить на прокси-сервер, который будет осуществлять сканирование на наличие спама и вирусов, а затем перенаправлять сообщения на внутренний почтовый сервер.

В качестве интерфейса, на котором фильтруются почтовые сообщения, указан интерфейс **eth1**. В качестве адреса, прослушиваемого прокси-сервером указан адрес 192.168.1.1 внутреннего интерфейса **eth2**.

*Рисунок 94 - Режим проксирования для заданного сервера*



Для настройки режима проксирования для заданного сервера необходимо выполнить следующие действия в режиме настройки.

*Пример 30.2 - Настройка режима проксирования для заданного сервера*

| Действие | Команда |
|---|---|
| Указание интерфейса, на котором будет осуществляться фильтрация. | admin@neo# **set service smtpproxy filter-interface eth1**<br>[edit] |
| Указание адреса, который прослушивает прокси-сервер SMTP. | admin@neo# **set service smtpproxy listen-address 192.168.1.1**<br>[edit] |
| Включение режима проксирования для заданного сервера и указание адреса для перенаправления сообщений. | admin@neo# **set service smtpproxy fixed-server address 192.168.2.10**<br>[edit] |
| Включение режима сканирования сообщений на наличие спама с использованием Spamassassin. | admin@neo# **set service smtpproxy antispam type spamassassin**<br>[edit] |
| Включение режима сканирования сообщений на наличие вирусов с использованием Clam Antivirus. | admin@neo# **set service smtpproxy antivirus type clamav**<br>[edit] |
| Включение режима сканирования сообщений на наличие вирусов с использованием Kaspersky Antivirus. | admin@neo# **set service smtpproxy antivirus type kav**<br>[edit] |
| Включение регистрации в системном журнале команд HELO/EHLO, а также адресов отправителя и получателя. | admin@neo# **set service smtpproxy log accepted from true**<br>[edit]<br>admin@neo# **set service smtpproxy log accepted to true**<br>[edit] |

admin@neo# **set service smtpproxy log rejected to true**
[edit]
admin@neo# **set service smtpproxy log rejected from true**
[edit]
admin@neo# **set service smtpproxy log helo true**
[edit]

Фиксация настройки.

admin@neo# **commit**
Restarting SMTP Gateway: smtp-gated.
[edit]

Вывод настройки.

admin@neo# **show service smtpproxy**

```
  antispam {
     type spamassassin
  }
  antivirus {
     type clamav
     type kav
  }
  filter-interface eth1
  fixed-server {
     address 192.168.2.10
  }
  listen-address 192.168.1.1
  log {
     accepted {
        from true
        to true
     }
     helo true
```

```
        rejected {
            from true
            to true
        }
    }
[edit]
```

## 30.5. Команды фильтрации почтовых сообщений

| Команды режима настройки | |
|---|---|
| `service smtpproxy` | Включение режима проксирования сетевого трафика протокола SMTP. |
| `service smtpproxy antispam spamassassin spam-threshold <порог>` | Указание порогового значения набранных баллов, используемого при классификации письма как спама. |
| `service smtpproxy antispam type <средство_фильтрации>` | Указание используемого средства проверки писем на спам. |
| `service smtpproxy antivirus type <средство_фильтрации>` | Указание используемого средства проверки писем на вирусы. |
| `service smtpproxy antivirus maximum-object-size <размер>` | Указание ограничения на размер проверяемых файлов. |
| `service smtpproxy filter-interface <интерфейс>` | Указание фильтруемого интерфейса. |
| `service smtpproxy fixed-server address <адрес>` | Включение режима проксирования для заданного сервера. |
| `service smtpproxy fixed-server port <порт>` | Указание используемого сетевого порта заданного сервера. |
| `service smtpproxy listen-` | Указание адреса, который прослушивается |

| | |
|---|---|
| | прокси-сервером. |
| `service smtpproxy lock duration <время>` | Указание периода времени, в течение которого будет осуществляться блокировка. |
| `service smtpproxy lock on spam <режим>` | Включение режима блокировки соединений SMTP для узлов, передавших почтовые сообщения, классифицированные как спам. |
| `service smtpproxy lock on virus <режим>` | Включение режима блокировки соединений SMTP для узлов, передавших почтовые сообщения, в которых были обнаружены вирусы. |
| `service smtpproxy log accepted from <режим>` | Включение регистрации в системном журнале адреса отправителя, в том случае если адрес был принят MTA. |
| `service smtpproxy log accepted to <режим>` | Включение регистрации в системном журнале адреса получателя, в том случае если адрес был принят MTA. |
| `service smtpproxy log helo <режим>` | Включение регистрации с системном журнале команды HELO/EHLO. |
| `service smtpproxy log rejected from` | Включение регистрации в системном журнале адреса отправителя, в том случае если адрес был отвергнут MTA. |
| `service smtpproxy log rejected to` | Включение регистрации в системном журнале адреса получателя, в том случае если адрес был отвергнут MTA. |
| `service smtpproxy port <порт>` | Указание номера сетевого порта, который прослушивается прокси-сервером. |
| Команды эксплуатационного режима | |

| | |
|---|---|
| `show smptproxy status` | Вывод статусной информации о работе прокси-сервера SMTP. |

### 30.5.1. service smtpproxy

Включение режима проксирования трафика протокола SMTP.

**Синтаксис**

```
set service smtpproxy
delete service smtpproxy
show service smtpproxy
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
    smtpproxy {
    }
}
```

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда используется для включения режима проксирования SMTP в системе Altell NEO.

Форма **set** данной команды используется для включения режима проксирования.

Форма **delete** данной команды используется для отключения режима проксирования.

Форма **show** используется для отображения настройки.

### 30.5.2. service smtpproxy antispam spamassassin spam-threshold <порог>

Указание порогового значения набранных баллов, используемого при классификации письма как спама.

**Синтаксис**

**set service smtpproxy spamassassin spam-threshold** *порог*

**delete service smtpproxy spamassassin spam-threshold**

**show service smtpproxy spamassassin spam-threshold**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
    smtpproxy {
        spamassassin {
            spam-threshold 1-1000
        }
    }
}
```

**Параметры**

*порог*

Пороговое значение набранных баллов, при достижении которого письмо классифицируется как спам. Значение должно лежать в диапазоне от 1 до 1000.

**Значение по умолчанию**

По умолчанию установлено значение равное 10 баллам.

**Указания по использованию**

Данная команда используется для указания порогового значения, используемого SpamAssassin при проверке писем на спам.

При фильтрации каждое сообщение проходит ряд проверок в соответствии с набором правил, каждое из которых определяет некоторый классификационный признак, определяющий принадлежность письма к спаму. В том случае если письмо успешно проходит проверку на соответствие правилу, ему начисляется определенное количество баллов. При прохождении полной проверки сообщения на всех правилах набора, баллы, начисляемые сообщению, суммируются. Чем выше набранная сумма баллов, тем выше вероятность того, что сообщение является спамом.

Пороговое значение определяет сумму баллов, при превышении которой сообщение классифицируется как спам. Значение по умолчанию равно 10 баллам.

Форма **set** данной команды используется для указания порогового значения, при достижении которого сообщение классифицируется как спам.

Форма **delete** данной команды используется для удаления настройки порогового значения и восстановления значения по умолчанию.

Форма **show** используется для отображения настройки порогового значения.

### 30.5.3. service smtpproxy antispam type <средство_фильтрации>

Указание используемого средства проверки почтовых сообщений на спам.

#### Синтаксис

**set service smtpproxy antispam type** *средство_фильтрации*

**delete service smtpproxy antispam type**

**show service smtpproxy antispam type**

#### Режим интерфейса

Режим настройки.

#### Ветвь конфигурации

```
service {
    smtpproxy {
        antispam {
            type текст
        }
    }
}
```

#### Параметры

*средство_фильтрации*

Множественный узел. Тип используемого средства проверки писем на спам.

Список допустимых значений:

- **spamassassin**.

#### Значение по умолчанию

По умолчанию используется **spamassassin**.

**Указания по использованию**

Данная команда используется для указания средства проверки сообщений на спам.

В настоящее время для проверки используется средство для фильтрации спама Spamassassin.

В том случае если данное значение не определено, проверка на спам не производится.

> *При этом следует учитывать, что в том случае если используется шифрование передаваемой почты с использованием TLS, почтовые сообщения не могут быть просканированы. При использовании режима фильтрации для заданного сервера рекомендуется отключить возможность включения TLS (STARTTLS) на заданном сервере, для того чтобы почтовый фильтр имел возможность работы со всей почтой.*

Форма **set** данной команды используется для указания средства проверки писем на спам.

Форма **delete** данной команды используется для удаления настройки и выключения режима проверки писем на спам.

Форма **show** используется для отображения настройки.

## 30.5.4. service smtpproxy antivirus type <средство_фильтрации>

Указание используемого средства проверки почтовых сообщений на вирусы.

**Синтаксис**

**set service smtpproxy antivirus type** *средство_фильтрации*

**delete service smtpproxy antivirus type**

**show service smtpproxy antivirus type**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
```

```
        smtpproxy {
            antivirus {
                type текст
            }
        }
}
```

**Параметры**

*средство_фильтрации*

Множественный узел. Тип используемого средства проверки почтовых сообщений на вирусы. Список допустимых значений:

**clamav**

Пакет антивирусного ПО Clam Antivirus.

**kav**

Пакет антивирусного ПО Kaspersky Antivirus.

**Значение по умолчанию**

По умолчанию используется **clamav**.

**Указания по использованию**

Данная команда используется для указания средства проверки сообщений на вирусы. Возможно использование пакетов антивирусного ПО ClamAV или Kaspersky AV. Они могут быть использованы как по отдельности, так и совместно. Если письмо будет классифицировано как содержащее вирусы хотя бы одним из используемых средств, оно будет отброшено. В том случае если значение для данного параметра не указано, проверка на вирусы не производится.

*При этом следует учитывать, что в том случае если используется шифрование передаваемой почты с использованием TLS, почтовые сообщения не могут быть просканированы. При использовании режима фильтрации для заданного сервера рекомендуется отключить возможность включения TLS (STARTTLS) на заданном сервере, для того чтобы почтовый фильтр имел возможность работы со всей*

*почтой.*

Форма **set** данной команды используется для указания средства проверки почтовых сообщений на вирусы.

Форма **delete** данной команды используется для удаления настройки и выключения режима антивирусной проверки.

Форма **show** используется для отображения настройки.

### 30.5.5. service smtpproxy antivirus maximum-object-size <размер>

Указание ограничения на размер проверяемых файлов.

**Синтаксис**

**set service smtpproxy antivirus maximum-object-size** *размер*

**delete service smtpproxy antivirus maximum-object-size**

**show service smtpproxy antivirus maximum-object-size**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
    smtpproxy {
        antivirus {
            maximum-object-size 1-128
        }
    }
}
```

**Параметры**

*размер*

Максимальный размер проверяемых файлов в Мб, письма большего размера проверяться не будут.

**Значение по умолчанию**

По умолчанию максимальный размер проверяемых файлов 10 Мб.

**Указания по использованию**

Данная команда позволяет установить ограничение на размер проверяемых

на вирусы файлов. Проверка писем, имеющих размер больше указанного, не осуществляется.

Форма **set** данной команды используется для указания максимального размера проверяемых файлов.

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

Форма **show** используется для отображения настройки.

### 30.5.6. service smtpproxy filter-interface <интерфейс>

Указание интерфейса, на котором будет осуществляться фильтрация.

```
set service smtpproxy filter-interface интерфейс
delete service smtpproxy filter-interface
show service smtpproxy filter-interface
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
    smtpproxy {
        filter-interface текст
        }
    }
}
```

**Параметры**

*интерфейс*

Обязательный. Множественный узел. Указание фильтруемого интерфейса. Интерфейс должен быть заранее определен в системе. Для того чтобы указать несколько фильтрующих интерфейсов, необходимо создать соответствующее количество узлов конфигурации.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет указать интерфейс (реальный или виртуальный),

на котором будет осуществляться фильтрация трафика SMTP.

Форма **set** данной команды используется для указания интерфейса, на котором осуществляется фильтрация.

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

Форма **show** используется для отображения настройки.

### 30.5.7. service smtpproxy fixed-server address <адрес>

Включение режима проксирования для заданного сервера.

**set service smtpproxy fixed-server address** *адрес*

**delete service smtpproxy fixed-server address**

**show service smtpproxy fixed-server address**

#### Режим интерфейса

Режим настройки.

#### Ветвь конфигурации

```
service {
    smtpproxy {
        fixed-server {
            address текст
        }
    }
}
```

#### Параметры

*адрес*

Адрес защищаемого почтового сервера. Адрес указывается в следующем формате *ip-адрес/префикс*.

#### Значение по умолчанию

Отсутствует.

#### Указания по использованию

Данная команда позволяет указать адрес почтового сервера, на который будут перенаправляться сообщения.

Прокси-сервер SMTP имеет два режима работы: режим прозрачного проксирования и режим проксирования для заданного сервера. При

использовании режима прозрачного проксирования сообщения перехватываются, проверяются, затем направляются на тот же IP-адрес, на который они были изначально направлены. При использовании режима проксирования для заданного сервера сообщения после проверки перенаправляются на указанный адрес защищаемого сервера. В том случае если значение для данного параметра явно не указано, используется режим прозрачного проксирования. При указании значения для параметра **fixed-server address** включается режим проксирования для заданного сервера. Этот режим рекомендован к использованию для обеспечения защиты почтового сервера, находящегося во внутренней локальной сети, когда в записи MX для защищаемого домена указано имя маршрутизатора. В этом случае сообщения будут приходить на прокси-сервер, который будет осуществлять проверку на вирусы и спам, а затем перенаправлять почтовые сообщения на внутренний почтовый сервер.

Форма **set** данной команды используется для указания адреса защищаемого почтового сервера, на который будут перенаправляться сообщения.

Форма **delete** данной команды используется для удаления настройки адреса защищаемого почтового сервера и отключения режима проксирования для данного сервера.

Форма **show** используется для отображения настройки.

## 30.5.8. service smtpproxy fixed-server port <порт>

Указание номера, используемого для подключения к заданному серверу.

**set service smtpproxy fixed-server port** *порт*

**delete service smtpproxy fixed-server port**

**show service smtpproxy fixed-server port**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
    smtpproxy {
        fixed-server {
```

```
                port 1-65535
            }
        }
    }
```

**Параметры**

*порт*

Номер сетевого порта, используемого для подключения к указанному серверу.

**Значение по умолчанию**

По умолчанию используется порт 25.

**Указания по использованию**

Данная команда позволяет указать номер сетевого порта, который будет использован для подключения к указанному серверу. По умолчанию используется порт 25.

Форма **set** данной команды используется для указания номера сетевого порта, используемого для подключения к указанному серверу.

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

Форма **show** используется для отображения настройки.

## 30.5.9. service smtpproxy listen-address <адрес>

Указание адреса, который прослушивается прокси-сервером SMTP.

**set service smtpproxy listen-address** *адрес*

**delete service smtpproxy listen-address**

**show service smtpproxy listen-address**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
    smtpproxy {
        listen-address текст
    }
```

}

**Параметры**

*адрес*

IP-адрес, который прослушивается прокси-сервером. Указанный адрес должен быть заранее настроен на одном из интерфейсов системы.

**Значение по умолчанию**

По умолчанию прокси-сервер прослушивает все адреса, настроенные в системе.

**Указания по использованию**

Данная команда позволяет указать адрес, который будет прослушивать прокси-сервер SMTP. Все почтовые сообщения, перехватываемые на фильтруемом интерфейсе будут автоматически перенаправляться на указанный адрес, который прослушивается прокси-сервером SMTP. После этого в том случае если включен соответствующий режим, сообщения проходят антивирусную и антиспам проверку, а затем перенаправляются либо на исходный IP-адрес (если используется режим прозрачного проксирования), либо на IP-адрес сервера, заданного в параметре **fixed-server address** (если используется режим проксирования для заданного сервера).

*Внимание! В качестве адреса, прослушиваемого прокси-сервером, рекомендуется указывать адрес одного из внутренних интерфейсов системы (обращенных во внутренний сегмент сети). В противном случае прокси-сервер SMTP будет функционировать как сервер open relay, то есть позволит бесконтрольно пересылать любые почтовые сообщения из внешней сети. При этом следует учитывать, что в том случае если значение для этого параметра явно не указано, прокси-сервер прослушивает все настроенные в системе адреса, в том числе адреса, настроенные на внешних интерфейсах системы!*

Форма **set** данной команды используется для указания адреса,

прослушиваемого прокси-сервером SMTP.

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

Форма **show** используется для отображения настройки.

### 30.5.10. service smtpproxy lock duration <время>

Указание периода времени, в течение которого будет осуществляться блокировка.

**set service smtpproxy lock duration** *время*

**delete service smtpproxy lock duration**

**show service smtpproxy lock duration**

#### Режим интерфейса

Режим настройки.

#### Ветвь конфигурации

```
service {
    smtpproxy {
        lock {
            duration 30-604800
        }
    }
}
```

#### Параметры

*время*

Период времени в секундах, в течении которого будет заблокирован IP-адрес узла, передавшего почтовое сообщение, которое было классифицировано как содержащее вирусы или спам.

#### Значение по умолчанию

По умолчанию период блокировки равен 3600 секунд.

#### Указания по использованию

Данная команда позволяет указать период времени, на который будет заблокирован IP-адрес узла, передавшего почтовое сообщение, которое было классифицировано как содержащее вирусы или спам.

В том случае если в сканируемом сообщении обнаружен вирус или спам, IP-

адрес узла, передавшего данного сообщение может быть заблокирован на указанное время. Для включения режима блокировки при обнаружении вируса используется команда service smtpproxy lock on virus <режим>, для включения режима блокировки при классификации сообщения как спама используется команда service smtpproxy lock on spam <режим>. После истечения указанного периода времени трафик SMTP от данного узла перестает блокироваться.

Форма **set** данной команды используется для указания периода блокировки.

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

Форма **show** используется для отображения настройки.

## 30.5.11. service smtpproxy lock on spam <режим>

Включение режима блокировки соединений SMTP для узлов, передавших почтовое сообщение, классифицированное как спам.

```
set service smtpproxy lock on spam [true|false]
delete service smtpproxy lock on spam
show service smtpproxy lock on spam
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
    smtpproxy {
        lock {
            on {
                spam [true|false]
            }
        }
    }
}
```

**Параметры**

*режим*

Режим блокировки соединений SMTP для узлов, передавших почтовое сообщение, классифицированное как спам. Допустимые значения:

**true**

Режим блокировки включен.

**false**

Режим блокировки выключен.

**Значение по умолчанию**

По умолчанию режим блокировки выключен.

**Указания по использованию**

Данная команда позволяет включить/отключить режим блокировки SMTP для узлов, передавших почтовое сообщение, классифицированное как спам. Прохождение трафика SMTP от заблокированного узла будет запрещено в течение времени, указанного при помощи команды **service smtpproxy lock duration <время>**.

Форма **set** данной команды используется включения/отключения режима блокировки трафика SMTP для узлов, передавших почтовое сообщение, классифицированное как спам.

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

Форма **show** используется для отображения настройки.

## 30.5.12. service smtpproxy lock on virus <режим>

Включение режима блокировки соединений SMTP для узлов, передавших почтовое сообщение, в котором были обнаружены вирусы.

```
set service smtpproxy lock on virus [true|false]
delete service smtpproxy lock on virus
show service smtpproxy lock on virus
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
    smtpproxy {
        lock {
            on {
                virus [true|false]
            }
        }
    }
}
```

**Параметры**

*режим*

Режим блокировки соединений SMTP для узлов, передавших почтовое сообщение, классифицированное как содержащее вирус. Допустимые значения:

**true**

Режим блокировки включен.

**false**

Режим блокировки выключен.

**Значение по умолчанию**

По умолчанию режим блокировки выключен.

**Указания по использованию**

Данная команда позволяет включить/отключить режим блокировки SMTP для узлов, передавших почтовое сообщение, классифицированное как содержащее вирус. Прохождение трафика SMTP от заблокированного узла будет запрещено в течение времени, указанного при помощи команды **service smtpproxy lock duration <время>**.

Форма **set** данной команды используется включения/отключения режима блокировки трафика SMTP для узлов, передавших почтовое сообщение, классифицированное как содержащее вирус.

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

Форма **show** используется для отображения настройки.

### 30.5.13. service smtpproxy log accepted from <режим>

Включение регистрации в системном журнале адреса отправителя, в том случае если адрес был принят MTA.

**set service smtpproxy log accepted from [true|false]**

**delete service smtpproxy log accepted from**

**show service smtpproxy log accepted from**

#### Режим интерфейса

Режим настройки.

#### Ветвь конфигурации

```
service {
    smtpproxy {
        log {
            accepted {
                from [true|false]
            }
        }
    }
}
```

#### Параметры

*режим*

Режим регистрации адреса отправителя, в том случае если адрес был принят MTA. Допустимые значения:

**true**

Режим регистрации включен.

**false**

Режим регистрации выключен.

#### Значение по умолчанию

По умолчанию режим регистрации выключен.

**Указания по использованию**

Данная команда позволяет включить/отключить режим регистрации адреса отправителя, в том случае если он был принят MTA.

Форма **set** данной команды используется включения/отключения режима регистрации адреса отправителя, в том случае если адрес был принят MTA.

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

Форма **show** используется для отображения настройки.

## 30.5.14. service smtpproxy log accepted to <режим>

Включение регистрации в системном журнале адреса получателя, в том случае если адрес был принят MTA.

```
set service smtpproxy log accepted to [true|false]
delete service smtpproxy log accepted to
show service smtpproxy log accepted to
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
    smtpproxy {
        log {
            accepted {
                to [true|false]
            }
        }
    }
}
```

**Параметры**

*режим*

Режим регистрации адреса получателя, если адрес был принят MTA. Допустимые значения:

**true**

Режим регистрации включен.

**false**

Режим регистрации выключен.

**Значение по умолчанию**

По умолчанию режим регистрации выключен.

**Указания по использованию**

Данная команда позволяет включить/отключить режим регистрации адреса получателя, в том случае если адрес был принят MTA.

Форма **set** данной команды используется включения/отключения режима регистрации адреса получателя, в том случае если адрес был принят MTA.

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

Форма **show** используется для отображения настройки.

## 30.5.15. service smtpproxy log helo <режим>

Включение регистрации с системном журнале команды HELO/EHLO.

**set service smtpproxy log helo [true|false]**

**delete service smtpproxy log helo**

**show service smtpproxy log helo**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
    smtpproxy {
        log {
            helo [true|false]
        }
        }
    }
}
```

**Параметры**

*режим*

Режим регистрации команды EHLO/HELO. Допустимые значения:

**true**

Режим регистрации включен.

**false**

Режим регистрации выключен.

#### Значение по умолчанию

По умолчанию режим регистрации выключен.

#### Указания по использованию

Данная команда позволяет включить/отключить режим регистрации регистрации команды EHLO/HELO.

Форма **set** данной команды используется включения/отключения режима регистрации команды EHLO/HELO.

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

Форма **show** используется для отображения настройки.

## 30.5.16. service smtpproxy log rejected from

Включение регистрации в системном журнале адреса отправителя, в том случае если адрес был отвергнут MTA.

**set service smtpproxy log rejected from [true|false]**

**delete service smtpproxy log rejected from**

**show service smtpproxy log rejected from**

#### Режим интерфейса

Режим настройки.

#### Ветвь конфигурации

```
service {
    smtpproxy {
        log {
            rejected {
                from [true|false]
            }
        }
```

```
        }
    }
```

**Параметры**

*режим*

Режим регистрации адреса отправителя, в том случае если адрес был отвергнут MTA. Допустимые значения:

**true**

Режим регистрации включен.

**false**

Режим регистрации выключен.

**Значение по умолчанию**

По умолчанию режим регистрации выключен.

**Указания по использованию**

Данная команда позволяет включить/отключить режим регистрации адреса отправителя, в том случае если он был отвергнут MTA.

Форма **set** данной команды используется включения/отключения режима регистрации адреса отправителя, в том случае если адрес был отвергнут MTA.

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

Форма **show** используется для отображения настройки.

## 30.5.17. service smtpproxy log rejected to

Включение регистрации в системном журнале адреса получателя, в том случае если адрес был отвергнут MTA.

```
set service smtpproxy log rejected to [true|false]
delete service smtpproxy log rejected to
show service smtpproxy log rejected to
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
```

```
smtpproxy {
    log {
        rejected {
            to [true|false]
        }
    }
}
}
```

**Параметры**

*режим*

Режим регистрации адреса получателя, если адрес был отвергнут MTA. Допустимые значения:

**true**

Режим регистрации включен.

**false**

Режим регистрации выключен.

**Значение по умолчанию**

По умолчанию режим регистрации выключен.

**Указания по использованию**

Данная команда позволяет включить/отключить режим регистрации адреса получателя, в том случае если адрес был отвергнут MTA.

Форма **set** данной команды используется включения/отключения режима регистрации адреса получателя, в том случае если адрес был отвергнут MTA.

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

Форма **show** используется для отображения настройки.

## 30.5.18. service smtpproxy port <порт>

Указание номера сетевого порта, который прослушивается прокси-сервером.

**set service smtpproxy port** *порт*

**delete service smtpproxy port**

**show service smtpproxy port**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
    smtpproxy {
        port 1-65535
    }
}
```

**Параметры**

*порт*

Номер сетевого порта, который прослушивается прокси-сервером SMTP. По умолчанию используется порт 9199.

**Значение по умолчанию**

По умолчанию прослушивается порт 9199.

**Указания по использованию**

Данная команда позволяет указать номер сетевого порта, который прослушивается прокси-сервером SMTP. По умолчанию прослушивается порт 9199 на всех настроенных в системе интерфейсах.

Все почтовые сообщения, перехватываемые на фильтруемом интерфейсе будут автоматически перенаправляться на указанный порт на адрес, указанный с помощью команды **service smtpproxy listen-address <адрес>**, который прослушивается прокси-сервером SMTP. После этого в том случае если включен соответствующий режим, сообщения проходят антивирусную и антиспам проверку, а затем перенаправляются либо на исходный IP-адрес (если используется режим прозрачного проксирования), либо на IP-адрес сервера, заданного в параметре **fixed-server address** (если используется режим проксирования для заданного сервера).

Форма **set** данной команды используется для указания сетевого порта, прослушиваемого прокси-сервером SMTP.

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

сетевого порта и восстановления значения, принятого по умолчанию.

Форма **show** используется для отображения настройки.

## 30.5.19. show smptproxy status

Вывод статусной информации о работе прокси-сервера SMTP.

**Синтаксис**

**show smtpproxy status**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет вывести статусную информацию о работе прокси-сервера SMTP.

**Примеры**

*Пример 30.3 - Вывод статусной информации о работе фильтра почты*

```
admin@neo:$ show smtpproxy status
version:      1.4.17
Compile date: Apr 11 2011 02:08:51
Dump time:    Thu Apr 14 15:46:51 2011
Start time:   Thu Apr 14 15:46:16 2011
Restart time: Thu Apr 14 15:46:16 2011
Last BUG:     Thu Jan  1 03:00:00 1970
Uptime:   0d 0h 0m 35s
Resource: 328/0/0/0 (maxrss/ixrss/idrss/isrss)
Children: 0/0/0 (current/max/buggy)
Found:    0/0/0/0/0 (viruses/spam/no-auth/spf/regex)
Requests: 0/0/0 (total/direct/empty)
Rejects:  0/0/0/0/0 (host/ident/lock/dnsbl/other)
```

```
Auth:     0/0 (accepted/rejected)


slot pid   state    flags time  source          target
trns   cli_rx

srv_rx    kbps ident

[edit]
```

# 31. ФИЛЬТРАЦИЯ И КЭШИРОВАНИЕ ДАННЫХ ИЗ WEB

В этом разделе описана настройка модуля (программы-сервера) веб-прокси (посредника для работы в веб) системы Altell NEO для фильтрации запросов пользователей и кэширования данных, получаемых из World Wide Web.

## 31.1. 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.

### 31.1.1. "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 Altell NEO работает в "прозрачном" режиме.

При использовании аутентификации пользователей необходимо отключить "прозрачный" режим, для этого используется команда service webproxy listen-address <ipv4_адрес> disable-transparent.

### 31.1.2. 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.

### 31.1.3. 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 Altell NEO фильтрация средствами веб-прокси выключена, все запросы пропускаются беспрепятственно.

#### *31.1.3.1. Порядок фильтрации запросов пользователей*

Фильтрация запросов пользователей производится посредником Altell NEO 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 **service webproxy url-filtering squidguard rule <номер> default-action <действие>**.

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):

1. **local-ok** - разрешает доступ к указанному адресу IP или домену;
2. **local-block** - запрещает доступ к указанному адресу IP или домену;
3. **allow-ipaddr-url** - разрешает запросы, в URL которых вместо доменного имени сайта указан IP-адрес;
4. **block-category** - запрещает доступ по адресам из указанной категории;
5. **allow-category** - разрешает доступ по адресам из указанной категории;
6. **local-block-keyword** - блокирует запросы к содержимому, URL которого содержит указанный набор символов;
7. **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).

### 31.1.4. 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

описаны ниже в этой главе.

По умолчанию в системе Altell NEO 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.*

## 31.2. Настройка веб-прокси

Настройка поведения посредника производится посредством отдачи поддерживаемых им команд через интерфейс командной строки либо через графический веб-интерфейс системы Altell NEO. Перечень поддерживаемых команд, их параметры и задаваемое ими поведение прокси рассмотрены ниже.

### 31.2.1. Примеры настройки фильтрации

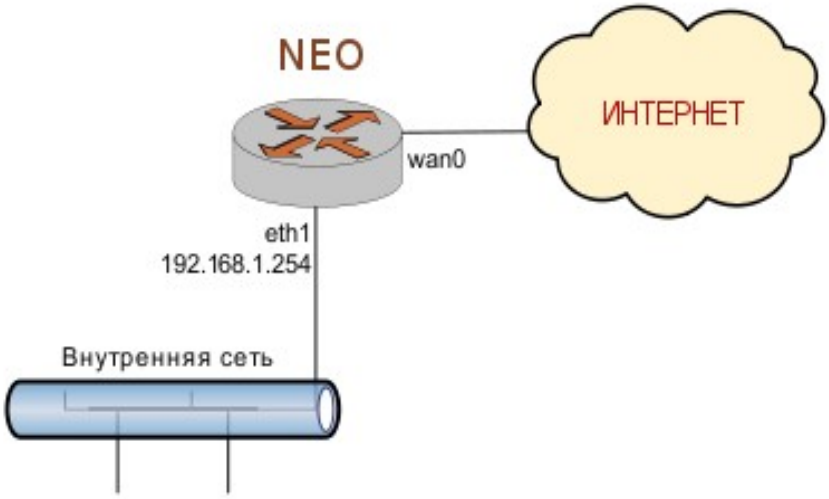
На рисунке 95 показана схема сети, на которой основаны приведённые ниже примеры. Предположим следующее:

- устройства из внутренней сети компании пользуются ресурсами Интернет через систему Altell NEO;
- фильтрация и кэширование веб-содержимого обеспечиваются веб-прокси, входящим в состав системы Altell NEO;
- 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**).

В примерах этого раздела рассмотрены следующие ситуации:

*Рисунок 95 - Схема сети для примеров*




- пример 31.1: блокировка отдельных адресов (URL);
- пример 31.2: проверка фильтрации;
- пример 31.3: фильтрация по категории данных;
- пример 31.4: фильтрация по ключевому слову;
- пример 31.5: допуск к отдельным сайтам;
- пример 31.6: перенаправление запросов пользователей;
- пример 31.7: поддержка разных групп пользователей;
- пример 31.8: учёт разных временных промежутков;
- пример 31.9: работа с "белым" списком.

#### *31.2.1.1. Блокировка отдельных адресов (URL)*

Команды примера 31.1 при помощи фильтра **local-block** явно указывают отдельные адреса (вне категорий), запросы к которым будут блокироваться.

*Пример 31.1 - Запрет доступа к отдельным адресам*

| Действие | Команда |
|---|---|
| Включение ожидания запросов на интерфейсе с адресом 192.168.1.254. | `admin@neo# set service webproxy listen-address 192.168.1.254 [edit]` |

| | |
|---|---|
| Запрет доступа к веб-сайту YouTube. | admin@neo# **set service webproxy url-filtering squidguard local-block youtube.com**<br>[edit] |
| Запрет доступа к веб-сайту Facebook. | admin@neo# **set service webproxy url-filtering squidguard local-block facebook.com**<br>[edit] |
| Применение изменений. | admin@neo# **commit**<br>[edit] |
| Просмотр текущей конфигурации веб-прокси в этом контексте. | admin@neo# **show service webproxy**<br>listen-address 192.168.1.254 {<br>}<br>url-filtering {<br>squidguard {<br>local-block youtube.com<br>local-block facebook.com<br>}<br>}<br>[edit] |

#### *31.2.1.2. 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 **show webproxy blacklist log** (запрещающие фильтры помещают адреса в так называемый "чёрный" список - blacklist).

Команда в примере 31.2 включает протоколирование запросов по адресам, закрытым фильтром **local-block** из предыдущего примера.

*Пример 31.2 - Включение протоколирования*

| Действие | Команда |
|---|---|
| Включение протоколирования всего, что перехватывается фильтром **local-block**. | admin@neo# **set service webproxy url-filtering squidguard log local-block**<br>[edit] |
| Применение изменений. | admin@neo# **commit**<br>[edit] |
| Просмотр текущей конфигурации веб-прокси в этом контексте. | admin@neo# **show service webproxy**<br>listen-address 192.168.1.254 {<br>}<br>url-filtering {<br>squidguard {<br>local-block youtube.com<br>local-block facebook.com<br>log local-block<br>}<br>}<br>[edit] |

#### *31.2.1.3. Фильтрация по категории данных*

Команды из примера 31.3 включат блокирование адресов из заранее определённых в Altell NEO категорий "реклама" (**ads**), "шпионское ПО" (**spyware**) и "азартные игры" (**gambling**).

*Пример 31.3 - Включение фильтрации по категориям адресов*

| Действие | Команда |
|---|---|
| Включение блокирования адресов из категории "реклама". | admin@neo# **set service webproxy url-filtering squidguard block-category ads**<br>[edit] |

| | |
|---|---|
| Включение блокирования адресов из категории "шпионское ПО". | admin@neo# **set service webproxy url-filtering squidguard block-category spyware**<br>[edit] |
| Включение блокирования адресов из категории "азартные игры". | admin@neo# **set service webproxy url-filtering squidguard block-category gambling**<br>[edit] |
| Применение изменений. | admin@neo# **commit**<br>[edit] |
| Просмотр текущей конфигурации веб-прокси в этом контексте. | admin@neo# **show service webproxy**<br>listen-address 192.168.1.254 {<br>}<br>url-filtering {<br>squidguard {<br>block-category ads<br>block-category spyware<br>block-category gambling<br>local-block youtube.com<br>local-block facebook.com<br>log local-block<br>}<br>}<br>[edit] |

#### *31.2.1.4. Фильтрация по ключевому слову*

Команды из примера 31.4 запрещают доступ к сайтам, адреса которых содержат указанную последовательность символов. В этом примере блокируется доступ ко всем сайтам в доменной зоне Китая (".cn").

*Пример 31.4 - Включение фильтрации по ключевому слову*

| Действие | Команда |
|---|---|
| Запрет доступа ко всем сайтам доменной зоны Китая. | admin@neo# **set service webproxy url-filtering squidguard local-block-keyword ".cn"**<br>[edit] |
| Применение изменений. | admin@neo# **commit**<br>[edit] |
| Просмотр текущей конфигурации веб-прокси в этом контексте. | admin@neo# **show service webproxy**<br>listen-address 192.168.1.254 {<br>}<br>url-filtering {<br>squidguard {<br>block-category ads<br>block-category spyware<br>block-category gambling<br>local-block youtube.com<br>local-block facebook.com<br>local-block-keyword .cn<br>log local-block<br>}<br>}<br>[edit] |

### *31.2.1.5. Допуск к отдельным сайтам*

Команды из примера 31.5 разрешают доступ к отдельным сайтам из заблокированных категорий. В этом примере открывается доступ к сайту по фиктивному адресу www.company-ads.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 31.5 - Допуск к отдельным сайтам*

| Действие | Команда |
|---|---|
| Предоставление пользователям доступа к фиктивному сайту www.company-ads.com | admin@neo# **set service webproxy url-filtering squidguard local-ok** www.company-ads.com<br>[edit] |
| Применение изменений. | admin@neo# **commit**<br>[edit] |
| Просмотр текущей конфигурации веб-прокси в этом контексте. | admin@neo# **show service webproxy**<br>listen-address 192.168.1.254 {<br>}<br>url-filtering {<br>squidguard {<br>block-category ads<br>block-category spyware<br>block-category gambling<br>local-block youtube.com<br>local-block facebook.com<br>local-block-keyword .cn<br>local-ok www.company-ads.com<br>log local-block<br>}<br>}<br>[edit] |

### *31.2.1.6. 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

31.6 указывают системе Altell NEO показывать страницу с категорией и адресом заблокированного сайта, к которому пытается обратиться пользователь.

*Пример 31.6 - Установка адреса страницы с сайта-подмены для заблокированных адресов*

| Действие | Команда |
|---|---|
| Установка адреса нужной страницы. Приведённый в примере URL вызовет обращение к скрипту squidGuard, который вернёт страницу с заблокированным адресом и причиной, по которой доступ к нему был закрыт (обратите внимание на регистр символов в URL - в рамках HTTP он имеет значение). | admin@neo# **set service webproxy url-filtering squidguard redirect-url** "http://192.168.1.254/cgi-bin/squidGuard-simple.cgi?targetclass=%t&url=%u"<br>[edit] |
| Применение изменений. | admin@neo# **commit**<br>[edit] |

Просмотр текущей конфигурации веб-прокси в этом контексте.

```
admin@neo# show service webproxy
 listen-address 192.168.1.254 {
 }
 url-filtering {
     squidguard {
          block-category ads
          block-category spyware
          block-category gambling
          local-block youtube.com
          local-block facebook.com
          local-block-keyword .cn
          local-ok www.company-
ads.com
          log local-block
          redirect-url
"http://192.168.1.254/cgi-
bin/squidGuard-simple.cgi?
targetclass=%t&url=%u"
     }
 }
[edit]
```

### *31.2.1.7. 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 31.7 подразумевается та же схема сети, что и в примере 31.1, но сейчас она рассматривается как настроенная соответственно потребностями школы, где запросы системных администраторов, учителей и учащихся рассматриваются независимо.

*Пример 31.7 - Настройка доступа в зависимости от группы*

| Действие | Команда |
|---|---|
| Очистка существующей конфигурации в отношении фильтрации запросов. | admin@neo# **delete service webproxy url-filtering**<br>[edit] |
| Применение изменений. | admin@neo# **commit**<br>[edit] |
| Возвращать в ответ на запросы к заблокированным сайтам титульную страницу сайта google.ru | admin@neo# **set service webproxy url-filtering squidguard redirect-url** “http://google.ru”<br>[edit] |
| Создание группы для администраторов (с единственным IP-адресом). | admin@neo# **set service webproxy url-filtering squidguard source-group ADMIN address 10.0.5.15**<br>[edit] |
| Создание группы для учителей (с одной подсетью). | admin@neo# **set service webproxy url-filtering squidguard source-group TEACHERS address 10.0.5.0/24**<br>[edit] |
| Создание группы для учащихся (с первой из двух подсетей). | admin@neo# **set service webproxy url-filtering squidguard source-group STUDENTS address 10.0.1.0/24**<br>[edit] |
| Создание группы для учащихся (со второй из двух подсетей). | admin@neo# **set service webproxy url-filtering squidguard source-group STUDENTS address 10.0.2.0/24**<br>[edit] |
| Создание правила для фильтрации запросов от группы ADMIN. В данном | admin@neo# **set service webproxy url-filtering squidguard rule 10** |

| | |
|---|---|
| случае ограничений нет. | **source-group ADMIN**<br>[edit] |
| Создание правила для фильтрации запросов от группы TEACHERS. | admin@neo# **set service webproxy url-filtering squidguard rule 20 source-group TEACHERS**<br>[edit] |
| Запрет доступа пользователей из группы TEACHERS к сайтам из категории “**porn**” ("сайты с порнографическим содержимым"). | admin@neo# **set service webproxy url-filtering squidguard rule 20 block-category porn**<br>[edit] |
| Запрет доступа пользователей из группы TEACHERS к сайтам из категории “**shopping**” ("покупки"). | admin@neo# **set service webproxy url-filtering squidguard rule 20 block-category shopping**<br>[edit] |
| Создание правила для фильтрации запросов от группы STUDENTS. | admin@neo# **set service webproxy url-filtering squidguard rule 30 source-group STUDENTS**<br>[edit] |
| Запрет доступа пользователей из группы STUDENTS к сайтам из категории “**adult**” ("для взрослых"). | admin@neo# **set service webproxy url-filtering squidguard rule 30 block-category adult**<br>[edit] |
| Запрет доступа пользователей из группы STUDENTS к сайтам из категории “**warez**” ("краденое/взломанное ПО"). | admin@neo# **set service webproxy url-filtering squidguard rule 30 block-category warez**<br>[edit] |
| Запрет доступа пользователей из группы STUDENTS к сайтам из категории “**drugs**” ("наркотики"). | admin@neo# **set service webproxy url-filtering squidguard rule 30 block-category drugs** |

```
[edit]
```

Запрет доступа пользователей из группы STUDENTS к сайтам из категории “**filehosting**” ("файлообмен").

```
admin@neo# set service webproxy
url-filtering squidguard rule 30
block-category filehosting
[edit]
```

Запрет доступа пользователей из группы STUDENTS к сайтам из категории “**audio-video**” ("аудио-видео содержимое").

```
admin@neo# set service webproxy
url-filtering squidguard rule 30
block-category audio-video
[edit]
```

Применение изменений.

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

Просмотр текущей конфигурации веб-прокси в этом контексте.

```
admin@neo# show service webproxy
 listen-address 192.168.1.254 {
 }
 url-filtering {
     squidguard {
          redirect-url
http://google.ru
          rule 10 {
               source-group ADMIN
          }
          rule 20 {
               block-category porn
               block-category
shopping
               source-group
TEACHERS
          }
          rule 30 {
               block-category adult
```

```
                    block-category
audio-video
                    block-category drugs
                    block-category
filehosting
                    block-category warez
                    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
               }
          }
     }
[edit]
```

#### *31.2.1.8. 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 31.8 подразумевают пример 31.7 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 (за счёт обращения значения SCHOOLHOURS при помощи символа "!"), 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 31.8 - Применение правил в определённое время суток.*

| Действие | Команда |
|---|---|
| Определение временн**о**го периода под названием SCHOOLHOURS, обозначающего рабочие (учебные) часы. | admin@neo# **set service webproxy url-filtering squidguard time-period SCHOOLHOURS days weekdays time "09:00-12:00, 13:00-16:00"**<br>[edit] |
| Уточнение правила 20 этим промежутком времени - теперь оно актуально только во время учебных часов. | admin@neo# **set service webproxy url-filtering squidguard rule 20 time-period SCHOOLHOURS**<br>[edit] |
| Создание нового правила для фильтрации запросов от группы TEACHERS ("преподаватели") во внеучебное время. | admin@neo# **set service webproxy url-filtering squidguard rule 25 source-group TEACHERS**<br>[edit] |
| Правило 25 актуально только во внеучебное время (за счёт инверсии значения SCHOOLHOURS при помощи знака "!"). | admin@neo# **set service webproxy url-filtering squidguard rule 25 time-period !SCHOOLHOURS**<br>[edit] |
| Закрытие доступа пользователей из группы TEACHERS к сайтам только из категории "**porn**". | admin@neo# **set service webproxy url-filtering squidguard rule 25 block-category porn**<br>[edit] |
| Применение изменений. | admin@neo# **commit**<br>[edit] |

Просмотр текущей конфигурации веб-прокси в этом контексте.

```
admin@neo# show service webproxy
 listen-address 192.168.1.254 {
 }
 url-filtering {
     squidguard {
          redirect-url
http://google.ru
          rule 10 {
               source-group ADMIN
          }
          rule 20 {
               block-category porn
               block-category
shopping
               source-group
TEACHERS
               time-period
SCHOOLHOURS
          }
          rule 25 {
               block-category porn
               source-group
TEACHERS
               time-period !
SCHOOLHOURS
          }
          rule 30 {
               block-category adult
               block-category
audio-video
               block-category drugs
               block-category
```

```
filehosting
                block-category warez
                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
          }
          time-period SCHOOLHOURS {
                days weekdays {
                     time “09:00-
12:00, 13:00-16:00”
                }
          }
     }
 }
[edit]
```

#### *31.2.1.9. 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 31.9 показано создание "белого" списка.

*Пример 31.9 - Определение "белого" списка.*

| Действие | Команда |
|---|---|
| Очистка существующей конфигурации. | admin@neo# **delete service webproxy url-filtering**<br>[edit] |
| Применение изменений. | admin@neo# **commit**<br>[edit] |
| Возвращать в ответ на запросы к заблокированным сайтам титульную страницу сайта google.ru. | admin@neo# **set service webproxy url-filtering squidguard redirect-url** “http://google.ru”<br>[edit] |
| Запрещение доступа ко всем сайтам в качестве действия по умолчанию (т.е. если явно не указано иное). | admin@neo# **set service webproxy url-filtering squidguard default-action block**<br>[edit] |
| Разрешение доступа к сайту “altell.ru”. | admin@neo# **set service webproxy url-filtering squidguard local-ok altell.ru**<br>[edit] |
| Разрешение доступа к сайту “yandex.ru”. | admin@neo# **set service webproxy url-filtering squidguard local-ok yandex.ru**<br>[edit] |
| Разрешение доступа к сайту “google.ru”. | admin@neo# **set service webproxy url-filtering squidguard local-ok google.ru**<br>[edit] |
| Применение изменений. | admin@neo# **commit**<br>[edit] |

Просмотр текущей конфигурации веб-прокси в этом контексте.

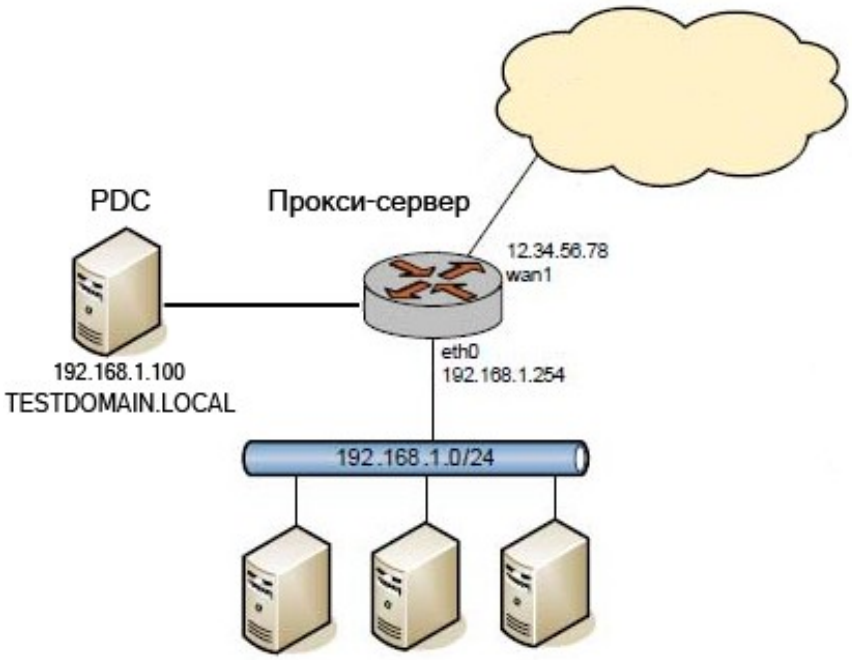
```
admin@neo# show service webproxy
 listen-address 192.168.1.254 {
 }
 url-filtering {
     squidguard {
          default-action block
          local-ok altell.ru
          local-ok yandex.ru
          local-ok google.ru
          redirect-url
http://google.ru
     }
 }
[edit]
```

#### *31.2.1.10. Настройка аутентификации пользователей на основе NTLM*

В примере 31.10 приведена настройка аутентификации пользователей прокси-сервера на основе NTLM. На рисунке 96 приведена используемая схема сети.

Для корректной работы аутентификации на основе NTLM должны быть выполнены следующие условия:

*Рисунок 96 - Аутентификация пользователей прокси на основе протокола NTLM*




- 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 neo.testdomain.local.
- PDC имеет IP-адрес 192.168.1.100.
- В базе AD создана учетная запись для прокси-сервера с правами администратора.

Для настройки аутентификации пользователей прокси на основе NTLM, необходимо выполнить следующие шаги в режиме настройки:

*Пример 31.10 - Настройка аутентификации пользователей прокси на основе NTLM*

| Действие | Команда |
|---|---|
| Отключение прозрачного режима работы прокси-сервера. | admin@neo# **set service webproxy listen-address 192.168.1.254 disable-transparent** |
| Установка аутентификации клиентов на основе NTLM. | admin@neo# **set service webproxy authorization method ntlm**<br>[edit] |
| Указание имени компьютера в домене. | admin@neo# **set service webproxy authorization ntlm name neo**<br>[edit] |
| Указание пароля для учетной записи, созданной в AD для прокси сервера. | admin@neo# **set service webproxy authorization ntlm password 123**<br>[edit] |
| Указание адреса контроллера домена. | admin@neo# **set service webproxy authorization ntlm pdc 192.168.1.100**<br>[edit] |
| Указание имени пользователя. | admin@neo# **set service webproxy authorization ntlm user proxy**<br>[edit] |
| Указание имени домена. | admin@neo# **set service webproxy** |

| | |
|---|---|
| | **authorization ntlm workgroup testdomain**<br>[edit] |
| Фиксация конфигурации. | admin@neo# **commit**<br>[edit] |

### *31.2.1.11. Настройка аутентификации пользователей на основе LDAP*

Altell NEO 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.

В примере 31.11 приведена настройка параметров подключения к серверу LDAP.

*Рисунок 97 - Аутентификация пользователей прокси на основе протокола LDAP*


*Пример 31.11 - Настройка параметров подключения к серверу LDAP*

| Действие | Команда |
|---|---|
| Указание имени привязки, используемого для подключения к серверу LDAP. | `admin@neo# set system ldap-server dn cn=neoproxy,dc=altell,dc=local [edit]` |
| Указание IP-адреса сервера LDAP. | `admin@neo# set system ldap-server host 192.168.1.100 [edit]` |
| Указание пароля для аутентификации на сервере LDAP. | `admin@neo# set system ldap-server password testpassword [edit]` |
| Указание используемого для подключения к серверу LDAP номера сетевого порта. | `admin@neo# set system ldap-server port 389 [edit]` |

| | |
|---|---|
| Указание корневого объекта каталога, начиная от которого необходимо производить поиск учетных записей пользователей. | admin@neo# **set system ldap-server userbasedn ou=Users,dc=altell,dc=local**<br>[edit] |
| Фиксация конфигурации. | admin@neo# **commit**<br>[edit] |

В примере 31.12 приведена настройка параметров прокси-сервера для включения аутентификации на основе протокола LDAP.

*Пример 31.12 - Включение аутентификации на основе LDAP в параметрах прокси-сервера*

| Действие | Команда |
|---|---|
| Указание аутентификации на основе LDAP. | admin@neo#**set service webproxy authorization method ldap**<br>[edit] |
| Отключение прозрачного режима. | admin@neo#**set service webproxy listen-address 192.168.1.254 disable-transparent**<br>[edit] |
| Фиксация конфигурации. | admin@neo# **commit**<br>[edit] |

## 31.2.2. Команды настройки фильтрации веб-содержимого и управления веб-прокси

### *31.2.2.1. Краткие описания команд*

| Команды, связанные с фильтрацией запросов | |
|---|---|
| service webproxy antivirus maximum-object-size <размер> | Антивирусная проверка будет выполняться в отношении файлов с размером не больше указанного. |

| | |
|---|---|
| `service webproxy antivirus nonscanned-send-min-size <размер>` | Указывает запускать отправку файла частями до окончания его антивирусной проверки, только если его размер превышает указанный. |
| `service webproxy antivirus nonscanned-send-percent <процент>` | Задаёт размер части файла, которую можно отправлять клиенту не дожидаясь проверки всего файла. |
| `service webproxy antivirus type <название>` | Указывает, какое антивирусное ПО использовать. |
| `service webproxy domain-block <домен>` | Запрещает доступ к указанному домену. |
| `service webproxy proxy-bypass <адрес>` | Указанные адрес или подсеть будут доступны в обход веб-прокси. |
| `service webproxy reply-block-mime <тип_mime>` | Запрещает доступ к данным веб указанного типа mime. |
| `service webproxy url-filtering disable` | Выключает фильтрацию, без потери настроек. |
| `service webproxy url-filtering squidguard` | Запрещает доступ по адресам из всех категорий. |
| `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-` | 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 содержимому, URL которого содержит указанный в ключе набор символов. |
| `service webproxy url-filtering squidguard local-block-url <адрес>` | Блокирует запросы к содержимому, URL которого совпадает с указанным. |
| `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` | 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 с указанным номером. |
| `service webproxy url-filtering squidguard rule <номер> block-category <категория>` | Запрещает доступ к веб-содержимому по адресам из указанной категории в пределах правила с указанным номером. |
| `service webproxy url-filtering squidguard rule <номер> allow-ipaddr-url` | В случае успешного применения правила с указанным номером будут разрешены запросы, в URL которых указан IP-адрес, а не доменное имя. |
| `service webproxy url-filtering squidguard rule <номер> default-action <действие>` | Задаёт действие, которое будет применяться ко всем запросам, не попавшим под имеющиеся у модуля веб-прокси правила, если правило с указанным номером будет успешно применено. |
| `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` | В случае успешного применения правила с указанным номером включает режим безопасного поиска ("Safe Search") на многих популярных поисковых машинах. |
| `service webproxy url-filtering squidguard rule <номер> local-block <адрес>` | Запрещает доступ к указанному адресу IP или URL в пределах правила с указанным номером. |
| `service webproxy url-` | Блокирует в рамках правила с указанным |

| | |
|---|---|
| | номером 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 с указанным номером. |
| `service webproxy url-filtering squidguard rule <номер> log <категория>` | Включает в пределах правила с указанным номером протоколирование запросов пользователей к адресам из указанной категории. |
| `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 адрес. |
| `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>` | 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 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 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-` | Прокси будет помещать в кэш только объекты с |

| | |
|---|---|
| | размером не меньше указанного. |
| Команды, связанные с аутентификацией пользователей | |
| `service webproxy authorization method` | Позволяет указать используемый метод аутентификации пользователей прокси. |
| `service webproxy authorization ntlm name` | Указание имени компьютера в домене. |
| `service webproxy authorization ntlm password` | Указание пароля для учетной записи пользователя, которая используется для авторизации в домене. |
| `service webproxy authorization ntlm pdc` | Указание IP-адреса или имени контроллера домена. |
| `service webproxy authorization ntlm user` | Указание имени пользователя для авторизации в домене. |
| `service webproxy authorization ntlm workgroup` | Указание имени домена. |
| Команды управления самим сервером веб-прокси и просмотра его состояния | |
| `restart webproxy` | Перезапускает процесс веб-прокси. |
| `service webproxy append-domain <домен>` | Указанное доменное имя будет присоединяться к URL, не содержащим точек. |
| `service webproxy default-port <порт>` | Задаёт порт, на котором по умолчанию программа-сервер веб-прокси будет ожидать соединений от клиентов. |
| `service webproxy disable-access-log` | Выключает протоколирование запросов по HTTP. |
| `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> port <порт>` | Задаёт отличный от значения по умолчанию номер порта для указанного адреса IPv4. |
| `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. |
| `show webproxy blacklist categories` | Показывает перечень категорий, доступ к которым закрыт ("чёрный" список категорий). |
| `show webproxy blacklist domains` | Показывает перечень доменов, доступ к которым закрыт ("чёрный" список доменов). |
| `show webproxy blacklist log` | Выводит протокол (журнал) запросов по адресам, находящимся в "чёрных" списках. |
| `show webproxy blacklist search <текст>` | Ищет в "чёрных" списках домены и/или адреса, включающие в себя указанный текст. |
| `show webproxy blacklist urls` | Показывает перечень адресов (URL), доступ к которым закрыт ("чёрный" список URL). |
| `show webproxy log` | Вывод на экран протокола (журнала) всех запросов пользователей к веб-прокси. |

#### *31.2.2.2. service webproxy antivirus maximum-object-size <размер>*

Антивирусная проверка будет выполняться в отношении файлов с размером не больше указанного.

**Синтаксис**

**set service webproxy antivirus maximum-object-size** *размер*

**delete service webproxy antivirus maximum-object-size**

**set service webproxy antivirus maximum-object-size**

**Режим команды**

Режим настройки.

**Оператор настройки**

```
service {
    webproxy {
        antivirus {
            maximum-object-size размер
        }
    }
}
```

**Параметры**

*размер*

Размер файла в мегабайтах.

**Значение по умолчанию**

По умолчанию установлено значение 30.

**Указания по использованию**

Эта команда предназначена для выключения проверки антивирусом файлов с размерами, превышающими указанный.

Форма **set** этой команды используется для задания размера файлов, отличного от значения по умолчанию.

Форма **delete** этой команды используется для возвращения параметру значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### *31.2.2.3. service webproxy antivirus nonscanned-send-min-size <размер>*

Указывает запускать отправку файла частями до окончания его антивирусной проверки, только если его размер превышает указанный.

**Синтаксис**

**set service webproxy antivirus nonscanned-send-min-size**

*размер*

**delete service webproxy antivirus nonscanned-send-min-size**

**set service webproxy antivirus nonscanned-send-min-size**

**Режим команды**

Режим настройки.

**Оператор настройки**

```
service {
    webproxy {
        antivirus {
            nonscanned-send-min-size размер
        }
    }
}
```

**Параметры**

*размер*

Размер файла в мегабайтах.

**Значение по умолчанию**

По умолчанию установлено значение 2.

**Указания по использованию**

Эта команда предназначена для управления выдачей файла частями до окончания его проверки, как это описано в разделе **service webproxy antivirus nonscanned-send-percent <процент>**. Такая выдача запускается только для файлов, размер которых превышает указанный.

Форма **set** этой команды используется для установки значения параметра, отличного от значения по умолчанию.

Форма **delete** этой команды используется для возвращения параметру значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### *31.2.2.4. service webproxy antivirus nonscanned-send-percent <процент>*

Задаёт размер части файла, которую можно отправлять клиенту не дожидаясь проверки всего файла.

**Синтаксис**

**set service webproxy antivirus nonscanned-send-percent** *размер*

**delete service webproxy antivirus nonscanned-send-percent**

**set service webproxy antivirus nonscanned-send-percent**

**Режим команды**

Режим настройки.

**Оператор настройки**

```
service {
    webproxy {
        antivirus {
            nonscanned-send-percent процент
        }
    }
}
```

**Параметры**

*процент*

Размер части файла в процентах от его полного размера.

**Значение по умолчанию**

По умолчанию установлено значение 5.

**Указания по использованию**

Эта команда предназначена для ускорения видимой реакции прокси на запросы за счёт отправки клиенту файла частями указанного размера (в процентах от полного размера), не дожидаясь результата антивирусной проверки всего файла, по которому файл может быть признан заражённым и отправка может быть прервана.

Такое поведение может вызвать проблемы из-за того, что вирусы или их части могут оказаться у клиента среди уже отправленных частей файла. С другой стороны, исполняемые файлы или архивы невозможно использовать,

если они загружены не полностью, так как в таком состоянии их целостность нарушена.

Форма **set** этой команды используется для установки значения параметра, отличного от значения по умолчанию.

Форма **delete** этой команды используется для возвращения параметру значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

#### *31.2.2.5. service webproxy antivirus type <название>*

Указывает, какое антивирусное ПО использовать.

**Синтаксис**

```
set service webproxy antivirus type название
delete service webproxy antivirus type
set service webproxy antivirus type
```

**Режим команды**

Режим настройки.

**Оператор настройки**

```
service {
    webproxy {
        antivirus {
            type название
        }
    }
}
```

**Параметры**

*название*

Название антивирусного продукта. Допустимые значения параметра:

**clamav**: антивирус ClamAV с открытым исходным кодом;

**kav**: антивирус Лаборатории Касперского.

**Значение по умолчанию**

По умолчанию используется **clamav**.

**Указания по использованию**

Эта команда предназначена для выбора антивирусного ПО.

Форма **set** этой команды используется для установки значения параметра, отличного от значения по умолчанию.

Форма **delete** этой команды используется для возвращения параметру значения по умолчанию.

Форма **show** этой команды используется для просмотра текущего состояния конфигурации в этом контексте.

### *31.2.2.6. service webproxy authorization method*

Позволяет указать используемый метод аутентификации пользователей прокси.

**Синтаксис**

**set service webproxy authorization method** [**none**|**ldap**|**ntlm**]

**delete service webproxy authorization method**

**set service webproxy authorization method**

**Режим команды**

Режим настройки.

**Оператор настройки**

```
service {
    webproxy {
        authorization {
            method [none|ldap|ntlm]
        }
    }
}
```

**Параметры**

**method**

Используемый метод аутентификации пользователей прокси. Допустимые значения:

**none**: Аутентификация пользователей не используется. Установлен по умолчанию.

**ldap**: Аутентификация на основе протокола LDAP.

**ntlm**: Аутентификация на основе протокола NTLM.

**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 service webproxy listen-address <ipv4_адрес> disable-transparent.

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.

### 31.2.3. service webproxy authorization ntlm name

Указание имени компьютера в домене.

**Синтаксис**

```
set service webproxy authorization name имя
delete service webproxy authorization name
set service webproxy authorization name
```

**Режим команды**

Режим настройки.

**Оператор настройки**

```
service {
    webproxy {
        authorization {
            name текст
```

```
        }
    }
}
```

**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 Altell NEO.

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.

### 31.2.4. service webproxy authorization ntlm password

Указание пароля для учетной записи пользователя, которая используется для авторизации в домене.

**Синтаксис**

**set service webproxy authorization password** *пароль*

**delete service webproxy authorization password**

**set service webproxy authorization password**

**Режим команды**

Режим настройки.

**Оператор настройки**

```
service {
    webproxy {
        authorization {
            password текст
```

```
            }
        }
    }
```

**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.

## 31.2.5. service webproxy authorization ntlm pdc

Указание IP-адреса или имени контроллера домена.

**Синтаксис**

**set service webproxy authorization pdc** *адрес*

**delete service webproxy authorization pdc**

**set service webproxy authorization pdc**

**Режим команды**

Режим настройки.

**Оператор настройки**

```
service {
    webproxy {
```

```
            authorization {
                pdc [ipv4-адрес|ipv6-адрес|текст]
            }
        }
    }
```

**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.

## 31.2.6. service webproxy authorization ntlm user

Указание имени пользователя для авторизации в домене.

**Синтаксис**

**set service webproxy authorization user** *имя_пользователя*

**delete service webproxy authorization user**

**set service webproxy authorization user**

**Режим команды**

Режим настройки.

**Оператор настройки**

```
service {
    webproxy {
        authorization {
```

```
                    name текст
                }
            }
        }
```

**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.

## 31.2.7. service webproxy authorization ntlm workgroup

Указание имени домена.

**Синтаксис**

**set service webproxy authorization workgroup** *имя_домена*

**delete service webproxy authorization workgroup**

**set service webproxy authorization workgroup**

**Режим команды**

Режим настройки.

**Оператор настройки**

```
service {
```

```
webproxy {
    authorization {
        workgroup текст
    }
}
}
```

**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.

### *31.2.7.1. 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.

### *31.2.7.2. service webproxy proxy-bypass <адрес>*

Указанные адрес или подсеть будут доступны в обход веб-прокси.

**Синтаксис**

```
set service webproxy proxy-bypass адрес
delete service webproxy proxy-bypass [адрес]
show service webproxy proxy-bypass
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
    webproxy {
        proxy-bypass адрес
    }
}
```

**Параметры**

*адрес*

Множественный узел. Адрес IPv4 отдельной системы или целой подсети, которые будут доступны в обход веб-прокси. Если в форме **delete** команды параметр опустить, то будет очищен весь список адресов/сетей, доступных в обход прокси.

**Значение по умолчанию**

По умолчанию этот список пуст и веб-прокси обрабатывает запросы от всех систем без исключений.

**Указания по использованию**

Эта команда предназначена для указания адресов отдельных систем или целых подсетей, запросы к которым будут проходить мимо веб-прокси когда он включён. Когда веб-прокси задействован, весь трафик на 80-ый порт систем в Интернет перенаправляется на порт устройства, на котором прокси ожидает соединений (по умолчанию 3128) и обрабатывается им.

Данная команда отключает такое перенаправление для введённых с её помощью адресов отдельных систем и целых подсетей, которые, таким образом, становятся доступными в обход прокси.

Форма **set** команды используется для задания адреса IPv4 отдельной системы или целой подсети, запросы к которым будут проходить мимо веб-прокси.

Форма **delete** команды используется для восстановления перенаправления запросов к указанной системе/подсети на модуль веб-прокси.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

### *31.2.7.3. 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** *тип_mime*

**show service webproxy reply-block-mime** *тип_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.

### *31.2.7.4. service webproxy url-filtering disable*

Просто выключает 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 общего выключения/включения фильтрации запросов пользователей, при этом настройки фильтрации не теряются.

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.

### *31.2.7.5. service webproxy url-filtering squidguard*

Закрывает доступ к адресам из всех категорий.

**Синтаксис**

```
set service webproxy url-filtering squidguard
delete service webproxy url-filtering squidguard
show service webproxy url-filtering squidguard
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
    webproxy {
        url-filtering {
            squidguard {
            }
        }
    }
}
```

**Параметры**

Отсутствуют.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Эта команда предназначена для закрытия доступа к URL из всех имеющихся категорий. Введение дополнительных узлов-потомков с URL ниже по дереву конфигурации включит блокирование этих конкретных URL.

Форма **set** команды используется для закрытия доступа к адресам (URL) из всех категорий.

Форма **delete** команды используется для разрешения доступа по заблокированным ранее при помощи формы **set** соответствующим URL.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

### *31.2.7.6. service webproxy url-filtering squidguard allow-category <категория>*

Разрешает доступ по URL 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 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 на разных устройствах категорий могут отличаться. Для просмотра перечня определённых на конкретном устройстве категорий можно воспользоваться командой **show webproxy blacklist categories**.

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.

### *31.2.7.7. 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. Для

просмотра перечня определённых на конкретном устройстве категорий можно воспользоваться командой **show webproxy blacklist categories**.

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.

### *31.2.7.8. 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 allow-
ipaddr-url
```

**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.

### *31.2.7.9. 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 [allow|block]
```

```
                    }
                }
            }
        }
```

**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.

**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.

### *31.2.7.10. 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, MSN 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.

### *31.2.7.11. 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.

### *31.2.7.12. 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 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 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.

### *31.2.7.13. 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.

### *31.2.7.14. 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.

#### *31.2.7.15. 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.

### *31.2.7.16. 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.

### *31.2.7.17. 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 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 предопределённому адресу.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

### *31.2.7.18. 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 1-1024 {
                }
            }
        }
    }
}
```

**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.

### *31.2.7.19. service webproxy url-filtering squidguard rule <номер> allow-category <категория>*

Разрешает 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 разрешением.

**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 1-1024 {
                    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 существующее правило либо для создания нового правила с таким разрешением. 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. Ознакомиться с перечнем категорий, доступных на конкретном устройстве, можно при помощи команды **show webproxy blacklist categories**.

Форма **set** используется для разрешения доступа по URL из указанной категории в рамках указанного правила, либо создаёт новое правило с указанным номером и таким разрешением.

Форма **delete** используется для закрытия доступа по URL из указанной категории в рамках указанного существующего правила.

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

### *31.2.7.20. 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 1-1024 {
                    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 **show webproxy blacklist categories**.

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.

### *31.2.7.21. service webproxy url-filtering squidguard rule <номер> allow-ipaddr-url*

Создаёт правило с указанным номером с разрешением доступа по запросам, в URL которых указан IP-адрес, а не доменное имя, либо добавляет такое разрешение в уже существующее правило с таким номером.

**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* **allow-ipaddr-url**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
    webproxy {
        url-filtering {
            squidguard {
                rule 1-1024 {
```

```
                                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.

### *31.2.7.22. service webproxy url-filtering squidguard rule <номер> default-action <действие>*

В случае успешного применения содержащего эту команду правила указанное в ней действие будет установлено как действие 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 1-1024 {
                    default-action [allow|block]
                }
            }
        }
    }
}
```

**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.

### *31.2.7.23. 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 1-1024 {
                    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.

### *31.2.7.24. service webproxy url-filtering squidguard rule <номер> enable-safe-search*

Включает режим безопасного поиска ("Safe Search") на популярных поисковых системах в рамках правила с указанным номером.

**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 1-1024 {
                    enable-safe-search
               }
          }
     }
}
```

**Параметры**

*номер*

Множественный узел. Номер правила.

**Значение по умолчанию**

Режим безопасного поиска выключен.

**Указания по использованию**

Эта команда в рамках правила с указанным номером 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, MSN 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.

### *31.2.7.25. 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 1-1024 {
                    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.

### *31.2.7.26. 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** *ключ* **local-block-keyword** *ключ*

**show service webproxy url-filtering squidguard rule** *ключ* **local-block-keyword**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
    webproxy {
        url-filtering {
            squidguard {
                rule 1-1024 {
                    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.

### *31.2.7.27. service webproxy url-filtering squidguard rule <номер> local-ok <адрес>*

Разрешает доступ к указанному адресу IP или домену.

**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 1-1024 {
                    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.

### *31.2.7.28. 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 1-1024 {
                    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.

### *31.2.7.29. 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 1-1024 {
                    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 **service webproxy url-filtering squidguard redirect-url <адрес>**.

**Указания по использованию**

Эта команда задаёт URL, содержимое по которому будет возвращено в ответ на запросы пользователей по адресам из "чёрного" списка. Если в рамках правила такой URL не задан, то будет использован глобальный URL, задаваемый при помощи команды **service webproxy url-filtering squidguard redirect-url <адрес>**.

> ***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.

### *31.2.7.30. 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 1-1024 {
                    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 **service webproxy url-filtering squidguard source-group <имя_группы>**.

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.

#### *31.2.7.31. 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 1-1024 {
                    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 при помощи команды **service webproxy url-filtering squidguard time-period <имя_промежутка>**.

Обратить смысл промежутка времени (то есть принять в рассмотрение период времени, исключающий указанный) можно при помощи символа "!".

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.

### *31.2.7.32. 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.

### *31.2.7.33. 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** *адрес*

**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.

### *31.2.7.34. 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.

### *31.2.7.35. 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, altell.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.

### *31.2.7.36. 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.

### *31.2.7.37. 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* **days** *день* **time** *время*

**delete service webproxy url-filtering squidguard time-period** *имя_промежутка* **days** *день* [*время*]

**show service webproxy url-filtering squidguard time-period** *имя_промежутка* **days** *день* [*время*]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
     webproxy {
          url-filtering {
               squidguard {
                    time-period имя_промежутка {
                         days [Mon|Tue|Wed|Thu|Fri|Sat|
Sun| weekdays|weekends|all] {

     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.

**weekdays**: указанный промежуток времени актуален по будням.

**weekends**: указанный промежуток времени актуален по выходным (не праздничным) дням.

**all**: 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").

**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.

### *31.2.7.38. 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.

### *31.2.7.39. 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.

### *31.2.7.40. 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.

### *31.2.7.41. 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** [*размер*]

**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.

### *31.2.7.42. service webproxy minimum-object-size <size>*

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 [размер]
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.

### *31.2.7.43. restart webproxy*

Перезапускает процесс веб-прокси.

**Синтаксис**

**restart webproxy**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Указания по использованию**

Эта команда предназначена для перезапуска работающего процесса веб-прокси.

**Примеры**

*Пример 31.13 - Перезапуск процесса веб-прокси.*

```
admin@neo> restart webproxy
Restarting Squid HTTP proxy: squid .......done.
2011/05/04 14:50:35| Creating Swap Directories
done.
admin@neo>
```

### *31.2.7.44. 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 "altell.ru", а запрос пользователя обращается по URL "www/abc.php", то в результате присоединения в дальнейшую обработку пойдёт URL "www.altell.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.

### *31.2.7.45. service webproxy default-port <порт>*

Задаёт порт, на котором по умолчанию программа-сервер веб-прокси будет ожидать соединений от клиентов.

**Синтаксис**

**set service webproxy default-port** *порт*

**delete service webproxy default-port**

**show service webproxy default-port**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
    webproxy {
        default-port порт
```

```
        }
    }
```

**Параметры**

*порт*

Номер порта в диапазоне от 0 до 65535.

**Значение по умолчанию**

По умолчанию прокси ожидает соединений на порте с номером 3128.

**Указания по использованию**

Эта команда предназначена для задания номера порта TCP, на котором прокси будет ожидать входящих соединений от клиентов. Если прокси будет ожидать соединений через несколько сетевых интерфейсов, то для каждого из них указанный здесь номер порта будет использоваться в качестве значения по умолчанию.

Форма **set** команды используется для установки нового (указанного в команде) номера порта по умолчанию.

Форма **delete** команды используется для восстановления значения по умолчанию (3128).

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

### *31.2.7.46. service webproxy disable-access-log*

Выключает протоколирование запросов по HTTP.

**Синтаксис**

```
set service webproxy disable-access-log
delete service webproxy disable-access-log
show service webproxy disable-access-log
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
    webproxy {
        disable-access-log
```

```
        }
    }
```

**Параметры**

Отсутствуют.

**Значение по умолчанию**

HTTP-запросы пользователей к сайтам протоколируются.

**Указания по использованию**

Эта команда предназначена для выключения протоколирования запросов ПО пользователей к сайтам по HTTP (через веб-прокси).

Форма **set** команды используется для выключения протоколирования.

Форма **delete** команды используется для восстановления поведения по умолчанию (протоколирование включено).

Форма **show** команды используется для просмотра текущего состояния конфигурации в этом контексте.

### *31.2.7.47. 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.

**Оператор настройки**

```
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.

### *31.2.7.48. 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.

**Оператор настройки**

```
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 Altell_NEO.

**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.

### *31.2.7.49. 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. IP-адрес интерфейса (по 4-ой версии протокола), 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 файрвола.

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.

### *31.2.7.50. service webproxy listen-address <ipv4_адрес> disable-transparent*

Выключает "прозрачный" режим работы для соединений, поступающих на интерфейс Altell NEO 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**

*ipv4_адрес*

IP-адрес сетевого интерфейса (по 4-ой версии протокола), 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 Altell NEO.

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.

### *31.2.7.51. service webproxy listen-address <ipv4-адрес> port <порт>*

Задаёт отличный от значения по умолчанию номер порта для указанного IPv4-адреса прокси.

**Синтаксис**

**set service webproxy listen-address** *ipv4-адрес* **port** *порт*

**delete service webproxy listen-address** *ipv4-адрес* **port**

**show service webproxy listen-address** *ipv4-адрес* **port**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
service {
    webproxy {
        listen-address ipv4-адрес {
            port порт
        }
    }
}
```

**Параметры**

*ipv4-адрес*

IP-адрес сетевого интерфейса (по 4-ой версии протокола), 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, указанное при помощи команды **service webproxy default-port <порт>**.

**Указания по использованию**

Эта команда предназначена для перенастройки прокси на ожидание соединений по другому порту, отличному от используемого по умолчанию. 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.

### *31.2.7.52. show webproxy blacklist categories*

Показывает перечень категорий, доступ к которым нежелателен ("чёрный" список категорий).

**Синтаксис**

**show webproxy 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.

**Примеры**

*Пример 31.14 - Вывод перечня категорий.*

```
admin@neo:~$ show webproxy blacklist categories
ads
aggressive
audio-video
drugs
gambling
hacking
mail
porn
proxy
redirector
spyware
suspect
```

```
violence
warez
admin@neo:~$
```

### *31.2.7.53. show webproxy blacklist domains*

Показывает перечень доменов, доступ к которым нежелателен ("чёрный" список доменов).

**Синтаксис**

**`show webproxy blacklist domains`**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Указания по использованию**

С помощью этой команды можно ознакомиться с перечнем всех известных на момент отдачи команды веб-прокси доменов из всех категорий.

**Примеры**

*Пример 31.15 - Вывод перечня доменов.*

```
admin@neo:~$ show webproxy blacklist domains
101com.com
101order.com
103bees.com
1100i.com
123banners.com
123found.com
123pagerank.com
180searchassistant.com
180solutions.com
207.net
247media.com
247realmedia.com
```

```
24pm-affiliation.com
...
```

#### 31.2.7.54. show webproxy blacklist log

Показывает протокол (журнал) запросов по адресам, находящимся в "чёрных" списках.

**Синтаксис**

**show webproxy blacklist log**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Указания по использованию**

Показать записанную в журнальный файл информацию о фактах обращения по адресам из "чёрных" списков вместе с адресом источника запроса.

**Примеры**

*Пример 31.16 - Вывод протокола запросов*

```
admin@neo:~$ show webproxy blacklist log
2008-09-03 18:12:01 [12027] Request(default/gambling/-)
http://www.goldenpalacepoker.com 10.1.0.173/- - GET
2008-09-04 10:00:44 [12988] Request(default/spyware/-)
http://www.180solutions.com 10.1.0.173/- - GET
admin@neo:~$
```

#### 31.2.7.55. show webproxy 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**

**show webproxy 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.

**Примеры**

В примере производится поиск во всех "чёрных" списках любых записей, содержащих "206.132.42".

*Пример 31.17 - Поиск адреса IP или URL по всем категориям.*

```
admin@neo:~$ show webproxy blacklist search 206.132.42
porn/domains 206.132.42.195
porn/domains 206.132.42.197
porn/domains 206.132.42.200
porn/domains 206.132.42.201
porn/domains 206.132.42.206
porn/domains 206.132.42.212
porn/domains 206.132.42.213
porn/domains 206.132.42.215
porn/domains 206.132.42.218
porn/domains 206.132.42.219
porn/domains 206.132.42.231
porn/domains 206.132.42.250
porn/domains 206.132.42.251
porn/domains 206.132.42.253
warez/domains 206.132.42.196
warez/domains 206.132.42.208
admin@neo:~$
```

### *31.2.7.56. show webproxy blacklist urls*

Показывает перечень URL, переход по которым нежелателен ("чёрный" список URL).

**Синтаксис**

**show webproxy blacklist urls**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Указания по использованию**

С помощью этой команды можно ознакомиться с перечнем всех известных на момент отдачи команды веб-прокси URL из всех категорий.

**Примеры**

*Пример 31.18 - Вывод перечня URL.*

```
admin@neo:~$ show webproxy blacklist urls
thisisarandomentrythatdoesnotexist.com/foo
thisisarandomentrythatdoesnotexist.com/foo
134.121.0.99/~dcarp
165.21.101.33/~mp3mania
194.134.35.11/mp3forever
194.134.35.12/mp3forever
194.134.35.17/mp3forever
194.145.63.33/bg-mp3
195.141.34.45/mp3millennium
195.141.34.45/mp3sweden
195.66.60.36/mhs00160
195.96.96.198/~brouns
205.188.134.217/h0tp00lman
209.202.218.12/mb/honzicek
...
```

### *31.2.7.57. show webproxy log*

Вывод на экран протокола (журнала) всех запросов пользователей к веб-прокси.

**Синтаксис**

```
show webproxy 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.

**Примеры**

*Пример 31.19 - Вывод на экран журнала информации о запросах.*

```
admin@neo:~$ show webproxy log

1220642699.568 830 172.16.117.25 TCP_MISS/200 46448 GET
http://sb.google.com/safebrowsing/update?
DIRECT/209.85.133.136 text/html

1220644499.691 1274 172.16.117.25 TCP_MISS/200 53832 GET
http://sb.google.com/safebrowsing/update?
DIRECT/209.85.133.93 text/html

1220645984.836 34 172.16.117.25 TCP_MISS/302 694 GET
http://en-us.fxfeeds.mozilla.com/en-
US/firefox/headlines.xml DIRECT/63.245.209.121 text/html

1220645984.881 31 172.16.117.25 TCP_MISS/302 736 GET
http://fxfeeds.mozilla.com/firefox/headlines.xml
DIRECT/63.245.209.121 text/html

…
```

# 32. СИСТЕМА ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

## 32.1. Общие сведения

Система обнаружения и предотвращения вторжений позволяет контролировать сетевой трафик в реальном времени с целью выявления, предотвращения или блокировки вторжений, сетевых атак и вредоносной активности.

В Altell NEO в качестве системы обнаружения и предотвращения вторжений используется Suricata IDS/IPS.

Система может функционировать в двух режимах: режиме обнаружения вторжений (IDS) и режиме предотвращения вторжений (IPS). Включение IDS для интерфейса осуществляется при помощи команды interfaces <интерфейс> ids enable. Включение режима предотвращения вторжений (IPS) на интерфейсе осуществляется при помощи команды interfaces <интерфейс> ips <направление> enable. Функционально их отличие заключается в том, что в режиме IPS сетевые атаки могут быть заблокированы в режиме реального времени.

В Altell NEO интегрирован набор правил безопасности, разрабатываемый сообществом Emergency Threats. Правила основаны на многолетнем совместном опыте экспертов в области сетевой безопасности и постоянно совершенствуются. Обновление правил происходит автоматически, для этого в Altell NEO должно быть настроено подключение к Интернет.

Правила располагаются в каталоге /etc/suricata/rules. Каждое правило содержит идентификационный номер в формате [*gid*:]*sid*, где *gid* – номер группы правил, *sid* — идентификационный номер правила. В том случае если номер группы явно не указан, он равен 1.

Правила распределены по категориям. Категория правил представляет собой набор правил, направленных на обнаружение атак схожего типа. Краткое описание используемых категорий правил:

- **emerging-activex.rules** Позволяют обнаруживать эксплойты для компонентов ActiveX.
- **emerging-attack_response.rules** Позволяют обнаружить трафик, передаваемый узлами

внутренней локальной сети, характерный для ответов после успешного проведения атаки.

- **emerging-botcc.rules** Позволяют обнаружить сетевой трафик командно-контрольных серверов бот сетей (Bot C&C).
- **emerging-chat.rules** Позволяют обнаружить сетевой трафик, относящийся к протоколам и программам для мгновенного обмена сообщениями.
- e**merging-compromised.rules** Позволяют обнаружить сетевой трафик от опасных или взломанных сетевых узлов.
- **emerging-deleted.rules** К этой категории относятся правила, которые были удалены из других категорий по различным причинам.
- **emerging-dns.rules** Позволяют обнаружить сетевые атаки, направленные на сервера DNS.
- **emerging-dos.rules** Позволяют обнаружить трафик, характерный для атак отказа в обслуживании.
- **emerging-drop.rules** Позволяют обнаружить сетевой трафик от узлов из списка Spamhaus Drop list.
- **emerging-dshield.rules** Позволяют обнаружить сетевой трафик от узлов, которые известны как источники атак, на основе списка Dshield.
- **emerging-exploit.rules** Позволяют обнаруживать сетевой трафик, характерный для программ использования уязвимостей (эксплойтов).
- **emerging-ftp.rules** Позволяют обнаруживать сетевой трафик, характерный для атак на сервисы FTP.
- **emerging-games.rules** Позволяют обнаруживать трафик, характерный для некоторых игр.
- **emerging-icmp.rules** Позволяют обнаружить трафик ICMP, характерный для проведения сетевых атак, например такой как сканирование портов.
- **emerging-icmp_info.rules** Правила относящиеся к использованию протокола ICMP, не вошедшие в категорию **emerging-icmp.rules**. Включение данной категории правил может привести к генерации системой обнаружения и предотвращения вторжений большого количества предупреждений.
- **emerging-imap.rules** Позволяют обнаружить сетевой трафик, характерный для атак на

сервисы IMAP.

- **emerging-inappropriate.rules** Позволяют обнаружить недопустимый сетевой трафик, который может противоречить политике безопасности организации.
- **emerging-malware.rules** Позволяют обнаруживать сетевой трафик, характерный для вредоносных программ.
- **emerging-misc.rules** Правила, которые не попадают ни в одну из других категорий
- **emerging-netbios.rules** Позволяют обнаруживать сетевой трафик, характерный для некоторых сетевых червей, использующих протокол NetBIOS.
- **emerging-p2p.rules** Позволяют обнаруживать сетевой трафик программ одноранговогo разделения файлов.
- **emerging-policy.rules** Позволяют обнаруживать сетевую активность, которая может противоречить политике безопасности организации (например, трафик VNC или использование анонимного доступа по протоколу FTP).
- **emerging-pop3.rules** Позволяют обнаруживать трафик, характерный для атак на сервисы POP3.
- **emerging-rbn.rules** Позволяют обнаруживать сетевой трафик от узлов сети Russian Business Network.
- **emerging-rpc.rules** Позволяют обнаружить атаки на сервисы RPC (удаленный вызов процедур).
- **emerging-scan.rules** Позволяют обнаружить сетевой трафик программ сканирования портов. Сканирование портов является надежным индикатором ненадлежащей активности.
- **emerging-shellcode.rules** Позволяют обнаружить пакеты, содержащие ассемблерный код, низкоуровневые команды, называемые также командным кодом. Эти команды являются существенной частью многих программ использования уязвимостей, таких как переполнение буфера. Перехват фрагмента командного кода зачастую служит надежным индикатором развивающейся атаки
- **emerging-smtp.rules** Позволяют обнаруживать трафик, характерный для атак на сервисы SMTP.
- **emerging-snmp.rules** Позволяют обнаружить сетевой трафик протокола SNMP.
- **emerging-sql.rules** Правила для различных программ баз данных SQL.

- **emerging-telnet.rules** Позволяют обнаружить сетевой трафик протокола Telnet в сети.
- **emerging-tftp.rules** Позволяют обнаружить сетевой трафик, характерный для атак на TFTP (trivial FTP).
- **emerging-tor.rules** Позволяют обнаружить трафик, исходящий от отправителя, использующего сеть Tor для сохранения анонимности.
- **emerging-trojan.rules** Позволяют обнаруживать трафик, характерный для троянских программ.
- **emerging-user_agents.rules** Позволяют обнаруживать атаки на пользовательские агенты.
- **emerging-virus.rules** Содержит сигнатуры некоторых распространенных вирусов. Этот список не является полным, изменяется нерегулярно и не может служить заменой антивирусного программного обеспечения.
- **emerging-voip.rules** Позволяют обнаружить сетевой трафик, характерный для атак на сервисы VoIP.
- **emerging-web_client.rules** Позволяют обнаруживать эксплойты для web-клиентов.
- **emerging-web_server.rules** Позволяют обнаруживать сетевые атаки на web-сервера.
- **emerging-web_specific_apps.rules** Позволяют обнаруживать атаки на основе инъекций sql (sql-injection attacks).
- **emerging-worm.rules** Позволяют обнаруживать сетевой трафик, характерный для сетевых червей.

Команда idps modify-rules exclude-category <категория> позволяет отключить сразу все правила, относящиеся к указанной категории.

Каждому правилу назначен приоритет в соответствии с классом атаки по частоте использования и важности. Стандартные уровни приоритетов от 1 до 3, при этом приоритет 1 является высоким, приоритет 2 — средним, приоритет 3 — низким.

*Таблица 49 - Приоритеты правил системы обнаружения и предотвращения вторжений*

| Тип | Описание | Приоритет |
|---|---|---|
| attempted-admin | Попытка получения привилегий администратора. | Высокий |
| attempted-user | Попытка получения привилегий пользователя. | Высокий |

| | | |
|---|---|---|
| shellcode-detect | Обнаружен исполняемый код. | Высокий |
| successful-admin | Получены права администратора. | Высокий |
| successful-user | Получены права пользователя. | Высокий |
| trojan-activity | Обнаружена сетевая троянская программа. | Высокий |
| unsuccessful-user | Неудачная попытка получения привилегий пользователя. | Высокий |
| web-application-attack | Атака на Web-приложение. | Высокий |
| attempted-dos | Предпринята атака отказа в обслуживании (DoS). | Средний |
| attempted-recon | Попытка несанкционированной передачи информации (утечка). | Средний |
| bad-unknown | Неизвестный трафик, который может оказаться опасным. | Средний |
| denial-of-service | Обнаружена атака отказа в обслуживании (DoS). | Средний |
| misc-attack | Прочие атаки. | Средний |
| non-standard-protocol | Зафиксировано использование нестандартного протокола. | Средний |
| rpc-portmap-decode | Обнаружен запрос RPC. | Средний |
| successful-dos | Успешная атака отказа в обслуживании (DoS). | Средний |
| successful-recon-largescale | Крупномасштабная утечка информации. | Средний |
| successful-recon-limited | Утечка информации. | Средний |
| suspicious-filename-detect | Обнаружено подозрительное имя файла. | Средний |

| | | |
|---|---|---|
| suspicious-login | Попытка входа в систему с использованием подозрительного имени. | Средний |
| system-call-detect | Обнаружен вызов системной функции. | Средний |
| unusual-client-port-connection | Клиент использует необычный порт. | Средний |
| web-application-activity | Доступ к потенциально опасному web-приложению. | Средний |
| icmp-event | Обычный пакет ICMP. | Низкий |
| misc-activity | Прочие действия. | Низкий |
| network-scan | Обнаружено сканирование сети. | Низкий |
| not-suspicious | Трафик не является подозрительным. | Низкий |
| protocol-command-decode | Обнаружена обычная команда протокола. | Низкий |
| string-detect | Обнаружена подозрительная строка. | Низкий |
| unknown | Неизвестный трафик. | Низкий |

В соответствии с данными приоритетами может быть назначено действие, которое будет выполнять система обнаружения и предотвращения вторжений в режиме реального времени при обнаружении сетевого трафика, соответствующего сигнатуре правила. Действие может быть одним из следующих:

- **alert.** Трафик разрешается и пересылается получателю. В журнал регистрации событий записывается предупреждение. Это действие установлено по умолчанию для всех правил.
- **drop**. При использовании режима IPS в том случае если устанавливается соответствие пакета правилу, для которого определено действие **drop**, анализ пакета прекращается, дальнейшее сравнение на соответствие оставшимся правилам не производится. Пакет отбрасывается, в журнал записывается предупреждение. При этом никаких сообщений с уведомлением отправителю и получателю пакета не отправляется.
- **reject**. При использовании режима IPS в том случае если устанавливается

соответствие пакета правилу, для которого определено действие **reject**, анализ пакета прекращается, дальнейшее сравнение на соответствие оставшимся правилам не производится. Пакет отбрасывается, в журнал записывается предупреждение. При этом отправителю и получателю пакета отправляется сообщение: для пакетов TCP будет отправлен пакет с флагом RST для сброса соединения TCP, для пакетов всех остальных протоколов — сообщение ICMP о недоступности.

- **sdrop**. В текущей версии Altell NEO данное действие аналогично действию **drop**.
- **pass**. В том случае если устанавливается соответствие пакета правилу, для которого определено действие **pass**, анализ пакета прекращается, дальнейшее сравнение на соответствие оставшимся правилам не производится. Пакет пересылается по назначению, предупреждение не генерируется.

Для указания действия используются следующие команды: idps actions priority-1 <действие>, idps actions priority-2 <действие>, idps actions priority-3 <действие>, idps actions other <действие>.

Так как характер трафика, анализируемого системой обнаружения и предотвращения вторжений, заранее не известен, по умолчанию используется обширная база сигнатур возможной подозрительной сетевой активности, что может привести к ложным срабатываниям. Ложное срабатывание имеет место, когда система генерирует сигнал тревоги для сетевого трафика, в действительности являющегося легитимным в данной сети. Для тех правил, которые приводят к ложным срабатываниям существует механизм создания исключений.

В случае обнаружения системой трафика, прошедшего проверку на соответствие сигнатуре правила, генерируется предупреждение, которое заносится в журнал регистрации (кроме правил для которых установлено действие **pass**). В журнал регистрации заносится подробная информация о событии, включая идентификационный номер правила. Для просмотра журнала регистрации используется эксплуатационная команда show idps log. Для вывода общих сведений об обнаруженных событиях используется команда show idps summary. При необходимости для правил могут быть созданы исключения. Например, команда idps modify-rules disable-sid <идентификатор> позволяет отключить правило на основе его идентификационного номера.

*Внимание! Особую осторожность необходимо соблюдать при настройке*

*действий **drop**, **sdrop** и **reject** при использовании режима IPS. В этом случае, при ложном срабатывании системы обнаружения и предотвращения вторжений, легитимный сетевой трафик может быть заблокирован.*

В производственных условиях первоначально рекомендуется включать систему только в режиме IDS для тестовой эксплуатации и выявления правил, приводящих к ложным срабатываниям (продолжительность тестового периода зависит от числа сетевых узлов, нагрузки и типа сетевого трафика). Перед тем, как система будет переведена в промышленный режим эксплуатации, необходимо внимательно изучить журнал регистрации событий и добавить исключения для правил, вызывающих ложные срабатывания.

При возникновении проблем с прохождением трафика разрешенных программ и протоколов, в первую очередь следует просмотреть журнал регистрации на предмет возможной неверной идентификации вторжения. В том случае если трафик был заблокирован системой обнаружения и предотвращения вторжений, следует убедиться в его легитимном поведении.

## 32.2. Примеры настройки

В данном разделе приведены следующие примеры:

- Пример 32.1- Настройка IPS на интерфейсе.
- Пример 32.2- Настройка IDS на интерфейсе.

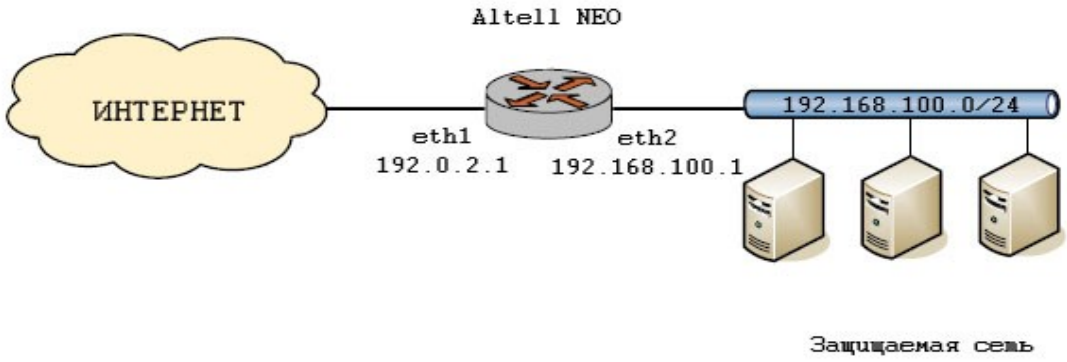
### 32.2.1. Настройка режима IPS

В этом разделе приведен пример настройки системы обнаружения и предотвращения вторжений в режиме IPS.

Подозрительный сетевой трафик, для которого будет установлено соответствие сигнатуре правила с приоритетом 1, будет заблокирован, при этом в журнал регистрации событий будет занесено соответствующее предупреждение. Для трафика, соответствующего сигнатурам правил с другими приоритетами, будет добавлено предупреждение в журнал регистрации, при этом такой трафик будет перенаправлен получателю.

Настройка осуществляется в соответствии с рисунком 98. Система обнаружения и предотвращения вторжений включается на внешнем интерфейсе Altell NEO eth1 (обращенном во внешний сегмент сети).

*Рисунок 98 - Система обнаружения и предотвращения вторжений*




Для настройки системы обнаружения и предотвращения вторжений необходимо выполнить следующие шаги в режиме настройки:

*Пример 32.1 - Настройка IPS на интерфейсе*

| Действие | Команда |
|---|---|
| Настройка параметров системы | admin@neo# **set idps**<br>[edit] |
| Указание защищаемой внутренней подсети. | admin@neo# **set idps modify-rules internal-network 192.168.100.0/24**<br>[edit] |
| Указание действия для правил с приоритетом 1. | admin@neo# **set idps actions priority-1 drop**<br>[edit] |
| Указание действия для правил с приоритетом 2. | admin@neo# **set idps actions priority-2 alert**<br>[edit] |
| Указание действия для правил с приоритетом 3. | admin@neo# **set idps actions priority-3 alert**<br>[edit] |

Фиксация конфигурации.

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

Просмотр конфигурации.

```
admin@neo# show idps
   actions {
       priority-1 drop
       priority-2 alert
       priority-3 alert
   }
   modify-rules {
       internal-network
192.168.100.0/24
   }
[edit]
```

Включение системы предотвращения вторжений для анализа входящего транзитного трафика на интерфейсе eth1.

```
admin@neo# set interfaces
ethernet eth1 ips in enable
[edit]
```

Включение системы предотвращения вторжений для анализа входящего трафика, предназначенного для самого Altell NEO, на интерфейсе eth1.

```
admin@neo# set interfaces
ethernet eth1 ips local enable
[edit]
```

Фиксация конфигурации.

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

Просмотр конфигурации.

```
admin@neo# show interfaces
ethernet eth1
   address 192.0.2.1/24
   ips {
       in {
           enable
       }
       local {
```

```
            enable
        }
    }
[edit]
```

### 32.2.2. Настройка режима IDS

При использовании режима IDS единственной мерой, принимаемой при обнаружении подозрительного трафика, соответствующего сигнатуре одного из используемых правил, является добавление предупреждения в журнал регистрации событий (в том случае если установлено действие **pass** предупреждение не формируется).

Настройка осуществляется в соответствие с рисунком 98. Для настройки и включения режима IDS на интерфейсе необходимо выполнить следующие шаги в режиме настройки:

*Пример 32.2 - Настройка IDS на интерфейсе*

| Действие | Команда |
|---|---|
| Настройка параметров системы | admin@neo# **set idps**<br>[edit] |
| Указание защищаемой внутренней подсети | admin@neo# **set idps modify-rules internal-network 192.168.100.0/24**<br>[edit] |
| Указание действия для правил с приоритетом 1. | admin@neo# **set idps actions priority-1 alert**<br>[edit] |
| Указание действия для правил с приоритетом 2. | admin@neo# **set idps actions priority-2 alert**<br>[edit] |
| Указание действия для правил с приоритетом 3. | admin@neo# **set idps actions priority-3 alert**<br>[edit] |
| Фиксация конфигурации. | admin@neo# **commit** |

```
[edit]
```

Просмотр конфигурации.

```
admin@neo# show idps
   actions {
       priority-1 alert
       priority-2 alert
       priority-3 alert
   }
   modify-rules {
       internal-network
192.168.100.0/24
   }
[edit]
```

Включение системы предотвращения вторжений на интерфейсе eth1.

```
admin@neo# set interfaces
ethernet eth1 ids enable
[edit]
```

Фиксация конфигурации.

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

Просмотр конфигурации.

```
admin@neo# show interfaces
ethernet eth1
   address 192.0.2.1/24
   ids {
          enable
   }
[edit]
```

## 32.3. Команды системы обнаружения и предотвращения вторжений

| Режим настройки | |
|---|---|
| `interfaces <интерфейс> ids` | Включение системы обнаружения вторжений |

| | |
|---|---|
| | на указанном интерфейсе. |
| `interfaces <интерфейс> ips <направление> enable` | Включение системы предотвращения вторжений на указанном интерфейсе. |
| `idps actions priority-1 <действие>` | Указание действия, которое будет применяться к пакетам, для которых было установлено соответствие правилу с приоритетом 1. |
| `idps actions priority-2 <действие>` | Указание действия, которое будет применяться к пакетам, для которых было установлено соответствие правилу с приоритетом 2. |
| `idps actions priority-3 <действие>` | Указание действия, которое будет применяться к пакетам, для которых было установлено соответствие правилу с приоритетом 3. |
| `idps actions other <действие>` | Указание действия, которое будет применяться к пакетам, для которых было установлено соответствие правилу с приоритетом отличным от 1, 2, 3. |
| `idps modify-rules disable-sid <идентификатор>` | Позволяет выборочно отключать используемые правила на основе идентификатора сигнатуры. |
| `idps modify-rules enable-sid <идентификатор>` | Позволяет выборочно включать неиспользуемые правила на основе идентификатора сигнатуры. |
| `idps modify-rules exclude-category <категория>` | Позволяет выборочно отключить категорию используемых правил. |
| `idps modify-rules internal-` | Указание защищаемой подсети. |

| Эксплуатационный режим | |
|---|---|
| `show idps log` | Вывод журнала системы обнаружения и предотвращения вторжений. |
| `show idps summary` | Вывод кратких сведений для системы обнаружения и предотвращения вторжений. |

### 32.3.1. interfaces <интерфейс> ids enable

Включение системы обнаружения вторжений на указанном интерфейсе.

**Синтаксис**

**set interfaces** *интерфейс* **ids enable**

**delete interfaces** *интерфейс* **ids**

**show interfaces** *интерфейс* **ids**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    интерфейс {
        ids enable
    }
}
```

**Параметры**

*интерфейс*

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице ниже в разделе Указания по использованию.

**Значение по умолчанию**

По умолчанию система обнаружения вторжений отключена.

**Указания по использованию**

Данная команда позволяет включить систему обнаружения вторжений на

интерфейсе.

При использовании режима IDS единственной мерой, принимаемой при обнаружении подозрительного трафика, соответствующего сигнатуре одного из используемых правил, является добавление предупреждения в журнал регистрации событий (в том случае если установлено действие **pass** предупреждение не формируется).

*Таблица 50 - Типы используемых интерфейсов*

| Тип интерфейса | Синтаксис | Параметры |
|---|---|---|
| Агрегирование каналов | `bonding` *`bondx`* | *bondx* Идентификатор интерфейса агрегированных каналов. Поддерживаются значения в диапазоне от **bond0** до **bond99**. |
| Виртуальный интерфейс агрегированных каналов | `bonding` *`bondx`* `vif` *`идентификатор_vlan`* | *bondx* Идентификатор интерфейса агрегированных каналов. Поддерживаются значения в диапазоне от **bond0** до **bond99**.<br>*идентификатор_vlan* Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 0 до 4094. |
| Сетевой мост | `bridge` *`brx`* | *brx* Имя мостовой группы. Поддерживаются значения в диапазоне от **br0** до **br999**. |
| Ethernet | `ethernet` *`ethx`* | *ethx* Имя интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**, в зависимости от доступных в системе физических интерфейсов. |
| Ethernet PPPoE | `ethernet` *`ethx`* `pppoe` *`номер`* | *ethx* Имя интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**, в зависимости от доступных в системе физических интерфейсов.<br>*номер* Имя определенного блока PPPoE. Значение должно лежать в диапазоне от 0 до 15. |
| Виртуальный интерфейс Ethernet | `ethernet` *`ethx`* `vif` *`идентификатор_vlan`* | *ethx* Имя интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**, в зависимости от доступных в системе физических интерфейсов.<br>*идентификатор_vlan* Идентификатор VLAN для |

| Тип интерфейса | Синтаксис | Параметры |
|---|---|---|
| | | виртуального интерфейса. Значение должно лежать в диапазоне от 0 до 4094. |
| Ethernet Vif PPPoE | `ethernet` *`ethx`* `vif` *`идентификатор_vlan`* `pppoe` *`номер`* | *ethx* Имя интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23**, в зависимости от доступных в системе физических интерфейсов.<br>*идентификатор_vlan* Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 0 до 4094.<br>*номер* Имя определенного блока PPPoE. Значение должно лежать в диапазоне от 0 до 15. |
| Интерфейс заглушки | `loopback` *`lo`* | *lo* Имя интерфейса заглушки. |
| Многоканальная связь | `multilink` **`mlx`** `vif 1` | *mlx* Идентификатор многоканальной связки. Можно создать до двух многоканальных связок. Значение должно лежать в диапазоне от **ml0** (“эм эль ноль”) до **ml23** (“эм эль двадцать три”).<br>**1** Идентификатор виртуального интерфейса. На текущий момент, можно создать только один виртуальный интерфейс для многоканального интерфейса, с идентификатором 1. Виртуальный интерфейс должен быть заранее определен. |
| OpenVPN | `openvpn` *`vtunx`* | *vtunx* Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun***x*, где *x* неотрицательное целое число. |
| Псевдо-Ethernet | `pseudo-ethernet` *`pethx`* | *pethx* Имя интерфейса псевдо-Ethernet. Значение должно лежать в диапазоне от **peth0** до **peth999**. |
| Последовательный PPP | `serial` *`wanx`* `ppp vif 1` | *wanx* Последовательный интерфейс: значение должно лежать в диапазоне от **wan0** до **wan23**. Интерфейс должен быть заранее определен. |

| Тип интерфейса | Синтаксис | Параметры |
|---|---|---|
| | | **1** Идентификатор виртуального интерфейса. На текущий момент, можно создать только один виртуальный интерфейс для интерфейса "точка-точка", с идентификатором **1**. Виртуальный интерфейс должен быть заранее определен. |
| Туннель | `tunnel` *`tunx`* | *tunx* Идентификатор туннельного интерфейса. Значение должно лежать в диапазоне от **tun0** до **tun23**. |

Форма **set** данной команды используется для включения системы обнаружения вторжений на указанном интерфейсе.

Форма **delete** данной команды используется для отключения системы обнаружения вторжений на интерфейсе.

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

### 32.3.2. interfaces <интерфейс> ips <направление> enable

Включение системы предотвращения вторжений на указанном интерфейсе.

**Синтаксис**

**`set interfaces`** *`интерфейс`* **`ips {in | out | local} enable`**

**`delete interfaces`** *`интерфейс`* **`ips`** [**`in`** | **`out`** | **`local`**]

**`show interfaces`** *`интерфейс`* **`ips`** [**`in`** | **`out`** | **`local`**]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
interfaces {
    интерфейс {
        ips {
            in {
                enable
            }
```

```
                    local {
                        enable
                    }
                    out {
                        enable
                    }
                }
            }
        }
```

**Параметры**

*интерфейс*

Обязательный. Тип интерфейса. Ключевые слова и аргументы, которые могут быть указаны, приведены в таблице ниже в разделе Указания по использованию.

**Значение по умолчанию**

По умолчанию система предотвращения вторжений отключена.

**Указания по использованию**

Данная команда позволяет включить систему предотвращения вторжений на интерфейсе.

По умолчанию система предотвращения вторжений отключена на всех интерфейсах.

Система предотвращения вторжений анализирует сетевой трафик, в зависимости от указанного направления:

- **in**. Если активировать систему предотвращения вторжений с использованием ключевого слова **in**, анализу будет подлежать сетевой трафик, принимаемый на указанном интерфейсе.

- **out**. Если активировать систему предотвращения вторжений с использованием ключевого слова **out**, анализу будет подлежать сетевой трафик, передаваемый с указанного интерфейса.

- **local**. Если активировать систему предотвращения вторжений с использованием ключевого слова **local**, фильтрации будет подлежать

сетевой трафик, предназначенный для самого Altell NEO.

Для каждого интерфейса можно включить систему предотвращения вторжений для анализа трафика одновременно в трех направлениях: приходящего на интерфейс (**in**), покидающего интерфейс (**out**), а также трафика предназначенного для самого Altell NEO (**local**). Для этого необходимо создать соответствующее количество узлов настройки **ips**.

> ***ВНИМАНИЕ**. Инициализация системы предотвращения вторжений при включении может потребовать некоторое количество времени, в течение которого возможна задержка в прохождении сетевого трафика, анализируемого системой. Продолжительность периода инициализации зависит от характеристик используемого устройства и может занимать от 5 до 20 минут.*

Мера к противодействию, предпринимаемая системой предотвращения вторжений при обнаружении сетевого трафика, соответствующего сигнатуре правила, зависит от действия, установленного для правил с данным приоритетом.

Форма **set** данной команды используется для включения системы предотвращения вторжений на указанном интерфейсе.

Форма **delete** данной команды используется для отключения системы предотвращения вторжений на интерфейсе.

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

### 32.3.3. idps actions priority-1 <действие>

Указание действия, применяемого к пакетам, для которых было установлено соответствие правилу с приоритетом 1.

**Синтаксис**

```
set idps actions priority-1 действие
delete idps actions priority-1 [действие]
show idps actions priority-1 [действие]
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
idps {
    actions {
        priority-1 текст
    }
}
```

**Параметры**

*действие*

Обязательный. Действие, применяемого к пакетам, для которых было установлено соответствие правилу с приоритетом 1. Допустимые значения:

- **alert.** Трафик разрешается и пересылается получателю. В журнал регистрации записывается предупреждение. Это действие установлено по умолчанию для всех правил.

- **drop**. При использовании режима IPS в том случае если устанавливается соответствие пакета правилу, для которого определено действие **drop**, анализ пакета прекращается Пакет отбрасывается, в журнал записывается предупреждение. При этом никаких сообщений с уведомлением отправителю и получателю пакета не отправляется.

- **reject**. При использовании режима IPS в том случае если устанавливается соответствие пакета правилу, для которого определено действие **reject**, анализ пакета прекращается. Пакет отбрасывается, в журнал записывается предупреждение. При этом отправителю и получателю пакета отправляется сообщение: для пакетов TCP будет отправлен пакет с флагом RST для сброса соединения TCP, для пакетов всех остальных протоколов — сообщение ICMP о недоступности.

- **sdrop**. В текущей версии Altell NEO данное действие аналогично действию **drop**.

- **pass**. В том случае если устанавливается соответствие пакета правилу, для которого определено действие **pass,** пакет пересылается по назначению, предупреждение системы не генерируется.

**Значение по умолчанию**

По умолчанию установлено значение **alert**.

**Указания по использованию**

Данная команда позволяет указать действие, применяемое к сетевому трафику, прошедшему проверку на соответствие правилу системы предотвращения вторжений с приоритетом 1.

Каждое правило системы предотвращения вторжений имеет приоритет от 1 до 3, в зависимости от степени угрозы. К приоритету 1 относят черви, вирусы, известные эксплойты, а также другие угрозы, которые гарантированно опасны, трафик которых не может быть полезным. К приоритету 2 относят вероятные DoS-атаки, использование нестандартных портов и протоколов и другой трафик, который с большой вероятностью может быть опасным. К приоритету 3 относят сканирование портов, доступ к потенциально уязвимым приложениям и другой трафик, который подозрителен, но не представляет прямой опасности (см. табл. 49).

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

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

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

## 32.3.4. idps actions priority-2 <действие>

Указание действия, которое будет применяться к пакетам, для которых было установлено соответствие правилу с приоритетом 2.

**Синтаксис**

**set idps actions priority-2** *действие*

**delete idps actions priority-2** [*действие*]

**show idps actions priority-2** [*действие*]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
idps {
    actions {
        priority-2 текст
```

```
        }
    }
```

**Параметры**

*действие*

Обязательный. Действие, применяемого к пакетам, для которых было установлено соответствие правилу с приоритетом 2. Допустимые значения:

- **alert.** Трафик разрешается и пересылается получателю. В журнал регистрации записывается предупреждение. Это действие установлено по умолчанию для всех правил.

- **drop**. При использовании режима IPS в том случае если устанавливается соответствие пакета правилу, для которого определено действие **drop**, анализ пакета прекращается Пакет отбрасывается, в журнал записывается предупреждение. При этом никаких сообщений с уведомлением отправителю и получателю пакета не отправляется.

- **reject**. При использовании режима IPS в том случае если устанавливается соответствие пакета правилу, для которого определено действие **reject**, анализ пакета прекращается. Пакет отбрасывается, в журнал записывается предупреждение. При этом отправителю и получателю пакета отправляется сообщение: для пакетов TCP будет отправлен пакет с флагом RST для сброса соединения TCP, для пакетов всех остальных протоколов — сообщение ICMP о недоступности.

- **sdrop**. В текущей версии Altell NEO данное действие аналогично действию **drop**.

- **pass**. В том случае если устанавливается соответствие пакета правилу, для которого определено действие **pass,** пакет пересылается по назначению, предупреждение системы не генерируется.

**Значение по умолчанию**

По умолчанию установлено значение **alert**.

**Указания по использованию**

Данная команда позволяет указать действие, применяемое к сетевому трафику, прошедшему проверку на соответствие правилу системы предотвращения вторжений с приоритетом 2.

Каждое правило системы предотвращения вторжений имеет приоритет от 1 до 3, в зависимости от степени угрозы. К приоритету 1 относят черви, вирусы, известные эксплойты, а также другие угрозы, которые гарантированно опасны, трафик которых не может быть полезным. К приоритету 2 относят вероятные DoS-атаки, использование нестандартных портов и протоколов и другой трафик, который с большой вероятностью может быть опасным. К приоритету 3 относят сканирование портов, доступ к потенциально уязвимым приложениям и другой трафик, который подозрителен, но не представляет прямой опасности (см. табл. 49).

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

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

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

## 32.3.5. idps actions priority-3 <действие>

Указание действия, которое будет применяться к пакетам, для которых было установлено соответствие правилу с приоритетом 3.

**Синтаксис**

**set idps actions priority-3** *действие*

**delete idps actions priority-3** [*действие*]

**show idps actions priority-3** [*действие*]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
idps {
    actions {
        priority-3 текст
    }
}
```

**Параметры**

*действие*

Обязательный. Действие, применяемого к пакетам, для которых было установлено соответствие правилу с приоритетом 3. Допустимые значения:

- **alert.** Трафик разрешается и пересылается получателю. В журнал регистрации записывается предупреждение. Это действие установлено по умолчанию для всех правил.

- **drop**. При использовании режима IPS в том случае если устанавливается соответствие пакета правилу, для которого определено действие **drop**, анализ пакета прекращается Пакет отбрасывается, в журнал записывается предупреждение. При этом никаких сообщений с уведомлением отправителю и получателю пакета не отправляется.

- **reject**. При использовании режима IPS в том случае если устанавливается соответствие пакета правилу, для которого определено действие **reject**, анализ пакета прекращается. Пакет отбрасывается, в журнал записывается предупреждение. При этом отправителю и получателю пакета отправляется сообщение: для пакетов TCP будет отправлен пакет с флагом RST для сброса соединения TCP, для пакетов всех остальных протоколов — сообщение ICMP о недоступности.

- **sdrop**. В текущей версии Altell NEO данное действие аналогично действию **drop**.

- **pass**. В том случае если устанавливается соответствие пакета правилу, для которого определено действие **pass,** пакет пересылается по назначению, предупреждение системы не генерируется.

**Значение по умолчанию**

По умолчанию установлено значение **alert**.

**Указания по использованию**

Данная команда позволяет указать действие, применяемое к сетевому трафику, прошедшему проверку на соответствие правилу системы предотвращения вторжений с приоритетом 3.

Каждое правило системы предотвращения вторжений имеет приоритет от 1 до 3, в зависимости от степени угрозы. К приоритету 1 относят черви, вирусы, известные эксплойты, а также другие угрозы, которые гарантированно опасны, трафик которых не может быть полезным. К приоритету 2 относят вероятные DoS-атаки, использование нестандартных портов и протоколов и другой трафик, который с большой вероятностью

может быть опасным. К приоритету 3 относят сканирование портов, доступ к потенциально уязвимым приложениям и другой трафик, который подозрителен, но не представляет прямой опасности (см. табл. 49).

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

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

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

### 32.3.6. idps actions other <действие>

Указание действия, которое будет применяться к пакетам, для которых было установлено соответствие правилу с приоритетом отличным от 1, 2, 3.

**Синтаксис**

**set idps actions other** *действие*

**delete idps actions other** [*действие*]

**show idps actions other** [*действие*]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
idps {
     actions {
          other текст
     }
}
```

**Параметры**

*действие*

Обязательный. Действие, применяемого к пакетам, для которых было установлено соответствие правилу с приоритетом отличным от 1, 2, 3. Допустимые значения:

- **alert.** Трафик разрешается и пересылается получателю. В журнал регистрации записывается предупреждение. Это действие установлено по умолчанию для всех правил.

- **drop**. При использовании режима IPS в том случае если устанавливается соответствие пакета правилу, для которого определено действие **drop**,

анализ пакета прекращается Пакет отбрасывается, в журнал записывается предупреждение. При этом никаких сообщений с уведомлением отправителю и получателю пакета не отправляется.

- **reject**. При использовании режима IPS в том случае если устанавливается соответствие пакета правилу, для которого определено действие **reject**, анализ пакета прекращается. Пакет отбрасывается, в журнал записывается предупреждение. При этом отправителю и получателю пакета отправляется сообщение: для пакетов TCP будет отправлен пакет с флагом RST для сброса соединения TCP, для пакетов всех остальных протоколов — сообщение ICMP о недоступности.

- **sdrop**. В текущей версии Altell NEO данное действие аналогично действию **drop**.

- **pass**. В том случае если устанавливается соответствие пакета правилу, для которого определено действие **pass,** пакет пересылается по назначению, предупреждение системы не генерируется.

**Значение по умолчанию**

По умолчанию установлено значение **alert**.

**Указания по использованию**

Данная команда позволяет указать действие, применяемое к сетевому трафику, прошедшему проверку на соответствие правилу системы предотвращения вторжений с приоритетом отличным от 1, 2, 3.

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

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

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

## 32.3.7. idps modify-rules disable-sid <идентификатор>

Позволяет выборочно отключать используемые правила системы обнаружения и предотвращения вторжений.

**Синтаксис**

```
set idps modify-rules disable-sid идентификатор
delete idps modify-rules disable-sid
show idps modify-rules disable-sid
```

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
idps {
    modify-rules {
        disable-sid текст
    }
}
```

**Параметры**

*идентификатор*

Множественный. Идентификатор правила, которое требуется выборочно отключить. Значение указывается в следующем формате: [*gid*:]*sid*, где *gid* – это идентификатор группы правил, а *sid* — идентификатор сигнатуры правила. Для того чтобы отключить несколько правил, необходимо создать соответствующее количество узлов **disable-sid**.

Идентификатор группы для всех правил в стандартном каталоге (/etc/suricata/rules) равен 1. Идентификатор в правиле указывается после ключевого слова **sid** в формате *gid-sid*, в том случае если идентификатор группы явно не указан, он предполагается равным 1.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда используется для выборочного отключения используемых правил системы обнаружения и предотвращения вторжений.

Эта команда может быть использована для отключения тех правил, из-за которых происходит большое число ложных срабатываний системы обнаружения и предотвращения вторжений.

Форма **set** данной команды используется для выборочного отключения правила.

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

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

### 32.3.8. idps modify-rules enable-sid <идентификатор>

Позволяет выборочно включать правила на основе идентификатора.

**Синтаксис**

**set idps modify-rules enable-sid** *идентификатор*

**delete idps modify-rules enable-sid**

**show idps modify-rules enable-sid**

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
idps {
    modify-rules {
        enable-sid текст
    }
}
```

**Параметры**

*идентификатор*

Множественный. Идентификатор правила, которое требуется выборочно включить. Значение указывается в следующем формате: [*gid*:]*sid*, где *gid* – это идентификатор группы правил, а *sid* — идентификатор сигнатуры правила. Для того чтобы включить несколько правил, необходимо создать соответствующее количество узлов **enable-sid**.

Идентификатор группы для всех правил в стандартном каталоге (/etc/suricata/rules) равен 1. Идентификатор в правиле указывается после ключевого слова **sid** в формате *gid-sid*, в том случае если идентификатор группы явно не указан, он предполагается равным 1.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда используется для выборочного включения правил системы обнаружения и предотвращения вторжений в стандартном каталоге (/etc/suricata/rules), которые отключены по умолчанию.

Форма **set** данной команды используется для выборочного включения

правила.

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

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

### 32.3.9. idps modify-rules exclude-category <категория>

Позволяет выборочно отключить правила, относящиеся к указанной категории.

**Синтаксис**

**set idps modify-rules exclude-category** *категория*

**delete idps modify-rules exclude-category** [*категория*]

**show idps modify-rules exclude-category** [*категория*]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
idps {
    modify-rules {
        exclude-category текст
    }
}
```

**Параметры**

*категория*

Множественный. Категория правил, которые не будут использоваться системой обнаружения и предотвращения вторжений при анализе сетевого трафика, например, **emerging-dos.rules**, **emerging-scan.rules**.

**Значение по умолчанию**

Отсутствует.

**Указания по использованию**

Данная команда позволяет выборочно отключить все правила, относящиеся к указанной категории. Правила системы обнаружения и предотвращения вторжений находятся в каталоге /etc/suricata/rules.

Форма **set** данной команды используется для выборочного отключения категории правил.

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

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

## 32.3.10. idps modify-rules internal-network <ipv4-сеть>

Позволяет указать защищаемые подсети.

**Синтаксис**

**set idps modify-rules internal-network** *ipv4-сеть*

**delete idps modify-rules internal-network** [*ipv4-сеть*]

**show idps modify-rules internal-network** [*ipv4-сеть*]

**Режим интерфейса**

Режим настройки.

**Ветвь конфигурации**

```
idps {
    modify-rules {
        internal-network ipv4-сеть
    }
}
```

**Параметры**

*ipv4-сеть*

Множественный. Адрес защищаемой сети, в формате *ip-адрес/префикс*. Для того чтобы указать несколько сетей, необходимо ввести соответствующее количество узлов конфигурации **internal-network**.

**Значение по умолчанию**

По умолчанию установлены значения 192.168.0.0/16, 10.0.0.0/8, 172.16.0.0/12.

**Указания по использованию**

Данная команда позволяет указать значение для переменной $HOME_NETWORK, которое используется системой обнаружения и предотвращения вторжений.

Переменные $HOME_NETWORK и $EXTERNAL_NETWORK являются стандартными переменными, используемыми Suricata при обработке сетевого трафика. Переменная $HOME_NETWORK определяет защищаемые подсети, переменная $EXTERNAL_NETWORK определяет

сети, из которых предположительно будут исходить атаки.

*Следует учитывать, что переменной $EXTERNAL_NETWORK присваивается значение, соответствующее всем сетям, кроме указанных в качестве значения для $HOME_NETWORK.*

Форма **set** данной команды позволяет установить значение для переменной $HOME_NETWORK.

Форма **delete** данной команды используется для удаления конфигурации и восстановления значения принятого по умолчанию.

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

## 32.3.11. show idps log

Вывод журнала системы обнаружения и предотвращения вторжений.

**Синтаксис**

**show idps log**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Указания по использованию**

Эта команда выводит на экран содержимое файла-журнала, в который заносится информация о событиях, обнаруженных системой обнаружения и предотвращения вторжений.

**Примеры**

*Пример 32.3 - Отображение журнала регистрации системы обнаружения и предотвращения вторжений*

```
admin@neo:~$ show idps log

2011-05-31 15:36:49.1306841809 {UDP} 192.0.2.2:63527 ->
192.168.100.10:39479

(shellcode-detect) Executable Code was Detected (priority
1)

[1:1390:5] GPL SHELLCODE x86 inc ebx NOOP

------------------------------------------------------------
```

```
------------------

2011-05-31 15:36:49.1306841809 {UDP} 192.0.2.2:63527 ->
192.168.100.10:39479

(shellcode-detect) Executable Code was Detected (priority
1)

[1:1390:5] GPL SHELLCODE x86 inc ebx NOOP

------------------------------------------------------------

[edit]
```

## 32.3.12. show idps summary

Вывод кратких сведений для системы обнаружения и предотвращения вторжений.

**Синтаксис**

**show idps summary**

**Режим интерфейса**

Эксплуатационный режим.

**Параметры**

Отсутствуют.

**Указания по использованию**

Эта команда выводит на экран общие сведения об обнаруженных событиях: общее число обнаруженных событий, распределение по идентификаторам сигнатур, по классам сигнатур, по приоритетам, а также по датам.

**Примеры**

*Пример 32.4 - Вывод общих сведений для системы обнаружения и предотвращения вторжений*

```
admin@neo:~$ show idps summary

admin@neo# run show idps summary

Processing log files...

Done.

============================================================

Summary of IPS events logged since Tue May 31 13:20:38
2011

============================================================
```

```
Total number of events: 5721

Breakdown by priorities:
  Priority 1: 11
  Priority 2: 24
  Priority 3: 5686

Breakdown by classes:
  bad-unknown: 8 (Potentially Bad Traffic)
  attempted-recon: 16 (Attempted Information Leak)
  shellcode-detect: 8 (Executable Code was Detected)
  web-application-attack: 3 (Web Application Attack)
  misc-activity: 5686 (Misc activity)

Breakdown by signatures:
  [1:257:9]: 2 (GPL DNS named version attempt)
  [1:366:7]: 2843 (GPL ICMP_INFO PING *NIX)
  [1:368:6]: 2843 (GPL ICMP_INFO PING BSDtype)
  [1:1390:5]: 8 (GPL SHELLCODE x86 inc ebx NOOP)
  [1:1418:11]: 2 (GPL SNMP request tcp)
  [1:2001219:18]: 6 (ET SCAN Potential SSH Scan)
  [1:2002910:4]: 2 (ET SCAN Potential VNC Scan 5800-
5820)
  [1:2002911:4]: 4 (ET SCAN Potential VNC Scan 5900-
5920)
  [1:2009358:3]: 3 (ET SCAN Nmap Scripting Engine User-
Agent Detected (Nmap Scripting Engine))
  [1:2010935:2]: 2 (ET POLICY Suspicious inbound to
MSSQL port 1433)
  [1:2010936:2]: 2 (ET POLICY Suspicious inbound to
Oracle SQL port 1521)
  [1:2010937:2]: 2 (ET POLICY Suspicious inbound to
```

```
mySQL port 3306)

    [1:2010939:2]: 2 (ET POLICY Suspicious inbound to
PostgreSQL port 5432)


  Breakdown by dates:

    2011-05-31: 5721

[edit]
```

# ПРИЛОЖЕНИЕ 1. ТИПЫ ICMP

В этом приложении перечислены типы ICMP, определенные IANA.

Организацией IANA (Internet Assigned Numbers Authority, Администрация адресного пространства Интернета) разработан стандарт сопоставления типов ICMP с набором целых чисел. В таблице 1-1 перечислены типы ICMP с кодами, определенными IANA, и их сопоставление с символьными строками, имеющимися в системе.

Таблица 1-1 Типы ICMP

| Тип ICMP | Код | Символьная строка | Описание |
|---|---|---|---|
| 0 - Echo reply | 0 | echo-reply | Эхо-ответ (понг) |
| 3 - Destination unreachable | | destination-unreachable | Получатель недостижим |
| | 0 | network-unreachable | Сеть получателя недостижима |
| | 1 | host-unreachable | Узел получателя недостижим |
| | 2 | protocol-unreachable | Протокол получателя недостижим |
| | 3 | port-unreachable | Порт получателя недостижим |
| | 4 | fragmentation-needed | Требуется фрагментация |
| | 5 | source-route-failed | Сбой маршрута отправителя |
| | 6 | network-unknown | Сеть получателя неизвестна |
| | 7 | host-unknown | Узел получателя неизвестен |
| | 9 | network-prohibited | Сеть административно запрещена |
| | 10 | host-prohibited | Узел административно запрещен |
| | 11 | TOS-network-unreachable | Сеть недостижима для TOS |
| | 12 | TOS-host-unreachable | Узел недостижим для TOS |
| | 13 | communication-prohibited | Связь административно запрещена |
| | 14 | host-precedence-violation | Запрошенный приоритет не разрешен. |
| | 15 | precedence-cutoff | Дейтаграмма отправлена с приоритетом ниже требуемого минимума. |
| 4 - Source quench | 0 | source-quench | Подавление отправителя |

| | | | |
|---|---|---|---|
| | | | (контроль перегрузки) |
| 5 - Redirect message | | redirect | Перенаправление |
| | 0 | network-redirect | Перенаправление дейтаграмм для сети |
| | 1 | host-redirect | Перенаправление дейтаграмм для узла |
| | 2 | TOS-network-redirect | Перенаправление дейтаграмм для TOS и сети |
| | 3 | TOS-host-redirect | Перенаправление дейтаграмм для TOS и узла |
| 8 - Echo request | 0 | echo-request | Эхо-запрос (пинг) |
| 9 - Router advertisement | 0 | router-advertisement | Объявление маршрутизатора |
| 10 - Router solicitation | 0 | router-solicitation | Запрос маршрутизатора |
| 11 - Time exceeded | | time-exceeded | |
| | 0 | ttl-zero-during-transit | Время жизни истекло при транзите |
| | 1 | ttl-zero-during-reassembly | Время сборки фрагментов истекло |
| 12 - Parameter problem: Bad IP header | | parameter-problem | |
| | 0 | ip-header-bad | Указатель означает ошибку |
| | 1 | required-option-missing | Отсутствует требуемый параметр |
| 13 - Timestamp | 0 | timestamp-request | Отметка времени |
| 14 - Timestamp reply | 0 | timestamp-reply | Ответ отметки времени |
| 15 - Information request | 0 | | Запрос сведений |
| 16 - Information reply | 0 | | Ответ со сведениями |
| 17 - Address | 0 | address-mask-request | Запрос маски адреса |

| | | | |
|---|---|---|---|
| mask request | | | |
| 18 - Address mask reply | 0 | address-mask-reply | Ответ с маской адреса |

# ПРИЛОЖЕНИЕ 2: ТИПЫ ICMPV6

В этом приложении перечислены типы ICMPv6, определенные IANA.

Организацией IANA (Internet Assigned Numbers Authority, Администрация адресного пространства Интернета) разработан стандарт сопоставления типов ICMPv6 с набором целых чисел. В таблице 2-1 перечислены типы ICMPv6 с кодами, определенными IANA, и их сопоставление с символьными строками, имеющимися в системе.

Таблица 2-1 Типы ICMPv6

| Тип ICMPv6 | Код | Символьная строка | Описание |
|---|---|---|---|
| 1 - Destination unreachable | | destination- unreachable | |
| | 0 | no-route | Отсутствует маршрут к получателю |
| | 1 | communication-prohibited | Связь с получателем административно запрещена |
| | 2 | | Вне области действия адреса отправителя |
| | 3 | address-unreachable | Адрес недостижим |
| | 4 | port-unreachable | Порт недостижим |
| | 5 | | Сбой политики входа/выхода на адресе отправителя |
| | 6 | | Отклонить маршрут к получателю |
| 2 - Packet too big | 0 | packet-too-big | |
| 3 - Time exceeded | | time-exceeded | |
| | 0 | ttl-zero-during-transit | Ограничение числа транзитных участков превзойдено при транзите |
| | 1 | ttl-zero-during-reassembly | Время сборки фрагментов истекло |
| 4 - Parameter problem | | parameter-problem | |
| | 0 | bad-header | Найдено ошибочное поле |

| | | | |
|---|---|---|---|
| | | | заголовка |
| | 1 | unknown-header-type | Найден неопознанный тип следующего заголовка |
| | 2 | unknown-option | Найден неопознанный параметр IPv6 |
| 128 - Echo request | 0 | echo-request (ping) | Эхо-запрос |
| 129 - Echo reply | 0 | echo-reply (pong) | Эхо-ответ |
| 133 - Router solicitation | 0 | router-solicitation | Запрос маршрутизатора |
| 134 - Router advertisement | 0 | router-advertisement | Объявление маршрутизатора |
| 135 - Neighbor solicitation | 0 | neighbor-solicitation (neighbour-solicitation) | Запрос соседа |
| 136 - Neighbor advertisement | 0 | neighbor-advertisement (neighbour-advertisement) | Объявление соседа |

# ПРИЛОЖЕНИЕ 3: ПОДДЕРЖИВАЕМЫЕ ТИПЫ ИНТЕРФЕЙСОВ

В приведенной ниже таблице показаны синтаксис и параметры для типов интерфейсов, поддерживаемых командами протоколов маршрутизации для интерфейсов.

Таблица 3-1 Поддерживаемые типы интерфейсов

| Тип интерфейса | Синтаксис | Параметры |
|---|---|---|
| Ethernet по ADSL в режиме моста | `adsl` *`adslx`* `pvc` *`идентификатор_pvc`* `bridged-ethernet` | *`adslx`*<br>Имя интерфейса DSL с инкапсуляцией Ethernet в режиме моста.<br>*`идентификатор_pvc`*<br>Идентификатор для PVC. Он может иметь формат пары *vpi/vci* или быть ключевым словом *auto*, где параметр *vpi* (Virtual Path Index, индекс виртуального пути) есть число от 0 до 255, параметр *vci* (Virtual Circuit Index, индекс виртуального контура) есть число от 0 до 65535, а *auto* есть указание системе определить параметры vpi и vci автоматически. |
| Классический IPOA по ADSL | `adsl` *`adslx`* `pvc` *`идентификатор_pvc`* `classical-ipoa` | *`adslx`*<br>Имя интерфейса DSL с классической инкапсуляцией IPoA.<br>*`идентификатор_pvc`*<br>Идентификатор для PVC. Он может иметь формат пары *vpi/vci* или быть ключевым словом **auto**, где параметр *vpi* (Virtual Path Index, индекс виртуального пути) есть число от 0 до 255, параметр *vci* (Virtual Circuit Index, индекс виртуального контура) есть число от 0 до 65535, а **auto** есть указание системе определить параметры vpi и vci автоматически. |

| | | |
|---|---|---|
| PPPoA по ADSL | `adsl` *`adslx`* `pvc` *`идентификатор_pvc`* `pppoa` *`номер`* | *`adslx`*<br>Имя интерфейса DSL с классической инкапсуляцией IPoA.<br>*`идентификатор_pvc`*<br>Идентификатор для PVC. Он может иметь формат пары *vpi/vci* или быть ключевым словом **auto**, где параметр *vpi* (Virtual Path Index, индекс виртуального пути) есть число от 0 до 255, параметр *vci* (Virtual Circuit Index, индекс виртуального контура) есть число от 0 до 65535, а **auto** есть указание системе определить параметры vpi и vci автоматически.<br>*`номер`*<br>Номер модуля PPPoA. Номер должен быть уникальным среди всех интерфейсов PPPoA. Кроме того, на PVC можно настроить только один экземпляр PPPoA. Номер модуля PPPoA выбирается из интервала от 0 до 15, так что получаются имена интерфейсов в диапазоне от **pppoa0** до **pppoa15**. |
| PPPoE по ADSL | `adsl` *`adslx`* `pvc` *`идентификатор_pvc`* `pppoe` *`номер`* | *`adslx`*<br>Имя интерфейса DSL с классической инкапсуляцией IPoA.<br>*`идентификатор_pvc`*<br>Идентификатор для PVC. Он может иметь формат пары *vpi/vci* или быть ключевым словом **auto**, где параметр *vpi* (Virtual Path Index, индекс виртуального пути) есть число от 0 до 255, параметр *vci* (Virtual Circuit Index, индекс виртуального контура) есть число от 0 до 65535, а **auto** есть указание |

| | | |
|---|---|---|
| | | системе определить параметры vpi и vci автоматически.<br>*номер*<br>Имя определенного модуля PPPoE. Значение должно лежать в диапазоне от 0 до 15. |
| Агрегирование | bonding *bondx* | *bondx*<br>Идентификатор интерфейса агрегирования. Поддерживаются значения в диапазоне от **bond0** до **bond99**. |
| Виртуальный интерфейс агрегирования | bonding *bondx* vif *идентифиактор_vlan* | *bondx*<br>Идентификатор интерфейса агрегирования. Поддерживаются значения в диапазоне от **bond0** до **bond99**.<br>*идентификатор_vlan*<br>Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 0 до 4094. |
| Мост | bridge *brx* | *brx*<br>Имя мостовой группы. Значение должно лежать в диапазоне от **br0** до **br999**. |
| Ethernet | ethernet *ethx* | *ethx*<br>Имя интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23** в зависимости от физических интерфейсов, имеющихся в системе. |
| PPPoE по Ethernet | ethernet *ethx*<br>pppoe *номер* | *ethx*<br>Имя интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23** в зависимости от физических интерфейсов, имеющихся в системе.<br>*номер* |

| | | |
|---|---|---|
| | | Имя определенного модуля PPPoE. Значение должно лежать в диапазоне от 0 до 15. |
| Виртуальный интерфейс Ethernet | `ethernet` *`ethx`* `vif` *`идентификатор_vlan`* | *`ethx`*<br>Имя интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23** в зависимости от физических интерфейсов, имеющихся в системе.<br>*`идентификатор_vlan`*<br>Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 0 до 4094. |
| PPPoE по виртуальному интерфейсу Ethernet | `ethernet` *`ethx`* `vif` *`идентификатор_vlan`* `pppoe` *`число`* | *`ethx`*<br>Имя интерфейса Ethernet. Значение должно лежать в диапазоне от **eth0** до **eth23** в зависимости от физических интерфейсов, имеющихся в системе.<br>*`vlan`*`-id`<br>Идентификатор VLAN для виртуального интерфейса. Значение должно лежать в диапазоне от 0 до 4094.<br>*`номер`*<br>Имя определенного модуля PPPoE. Значение должно лежать в диапазоне от 0 до 15. |
| Заглушка | `loopback` *`lo`* | *`lo`*<br>Имя интерфейса заглушки. |
| Многоканальный | `multilink` *`mlx`* `vif 1` | *`mlx`*<br>Идентификатор многоканальной группы. Можно создать до двух многоканальных групп. Поддерживаются значения в диапазоне от **ml0** (“мл-ноль”) до |

| | | |
|---|---|---|
| | | **ml23** (“мл-двадцать три”).<br>*1*<br>Идентификатор виртуального интерфейса. В настоящее время для многоканальных интерфейсов поддерживается только один виртуальный интерфейс, так что идентификатор должен быть равен 1. Виртуальный интерфейс к моменту выдачи команды должен быть уже определен. |
| OpenVPN | `openvpn` *`vtunx`* | *`vtunx`*<br>Идентификатор интерфейса OpenVPN. Значение должно лежать в диапазоне от **vtun0** до **vtun*x***, где ***x* —** натуральное число. |
| Псевдо-Ethernet | `pseudo-ethernet`<br>*`pethx`* | *`pethx`*<br>Имя интерфейса псевдо-Ethernet. Значение должно лежать в диапазоне от **peth0** до **peth999**. |
| Последовательный интерфейс HDLC Cisco | `serial` *`wanx`*<br>`cisco-hdlc vif 1` | *`wanx`*<br>Настраиваемый последовательный интерфейс: идентификатор из диапазона от **wan0** до **wan23**. Интерфейс к моменту выдачи команды должен быть уже определен.<br>`1`<br>Идентификатор виртуального интерфейса. В настоящее время для интерфейсов HDLC Cisco поддерживается только один виртуальный интерфейс, так что идентификатор должен быть равен 1. Виртуальный интерфейс к этому моменту должен быть уже определен. |
| Последовательный | `serial` *`wanx`* | *`wanx`* |

| | | |
|---|---|---|
| интерфейс Frame Relay | `frame-relay vif` *`dlci`* | Настраиваемый последовательный интерфейс: идентификатор из диапазона от **wan0** до **wan23**. Интерфейс к этому моменту должен быть уже определен.<br>*`dlci`*<br>Идентификатор виртуального интерфейса. В случае интерфейсов Relay interfaces это номер DLCI для инетрфейса. Значение должно лежать в диапазоне от 16 до 991. Виртуальный интерфейс к моменту выдачи команды должен быть уже определен. |
| Последовательный интерфейс PPP | `serial` *`wanx`* `ppp vif 1` | *`wanx`*<br>Настраиваемый последовательный интерфейс: идентификатор из диапазона от **wan0** до **wan23**. Интерфейс к моменту выдачи команды должен быть уже определен.<br>`1`<br>Идентификатор виртуального интерфейса. В настоящее время для интерфейсов "точка-точка" поддерживается только один виртуальный интерфейс, так что идентификатор должен быть равен 1. Виртуальный интерфейс к моменту выдачи команды должен быть уже определен. |
| Туннель | `tunnel` *`tunx`* | *`tunx`*<br>Идентификатор определяемого интерфейса туннеля. Значение должно лежать в диапазоне от **tun0** до **tun23**. |
| Беспроводной | `wireless` *`wlanx`* | *`wlanx`*<br>Идентификатор для определяемого беспроводного интерфейса. Значение должно лежать в диапазоне от **wlan0** до **wlan999**. |

| | | |
|---|---|---|
| Беспроводной модем | `wirelessmodem` *`wlmx`* | *`wlmx`*<br>Идентификатор для определяемого интерфейса беспроводного модема. Значение должно лежать в диапазоне от **wlm0** до **wlm999**. |

# ПРИЛОЖЕНИЕ 4. ЗНАЧЕНИЯ ПОЛЯ DSCP В СООТВЕТСТВИИ С ДОКУМЕНТОМ RFC 2474

| Двоичное значение | Настроенное значение | Скорость отбрасывания | Смысл |
|---|---|---|---|
| 101 110 | 46 | N/A | Expedited forwarding (EF) |
| 000 000 | 0 | N/A | Default: Best-effort traffic |
| 001 010 | 10 | Low | Assured forwarding (AF) 11 |
| 001 100 | 12 | Medium | Assured forwarding (AF) 12 |
| 001 110 | 14 | High | Assured forwarding (AF) 13 |
| 010 010 | 18 | Low | Assured forwarding (AF) 21 |
| 010 100 | 20 | Medium | Assured forwarding (AF) 22 |
| 010 110 | 22 | High | Assured forwarding (AF) 23 |
| 011 010 | 26 | Low | Assured forwarding (AF) 31 |
| 011 100 | 28 | Medium | Assured forwarding (AF) 32 |
| 011 110 | 30 | High | Assured forwarding (AF) 33 |
| 100 010 | 34 | Low | Assured forwarding (AF) 41 |
| 100 100 | 36 | Medium | Assured forwarding (AF) 42 |
| 100 110 | 38 | High | Assured forwarding (AF) 43 |

# ПРИЛОЖЕНИЕ 5: ТИПЫ ПРОТОКОЛОВ ДЛЯ ФИЛЬТРАЦИИ НА ПРИКЛАДНОМ УРОВНЕ

Поддерживается фильтрация на прикладном уровне для следующих типов протоколов:

- 100bao;
- aim;
- aimwebcontent;
- applejuice;
- ares;
- armagetron;
- battlefield1942;
- battlefield2;
- battlefield2142;
- bgp;
- biff;
- bittorrent;
- chikka;
- cimd;
- ciscovpn;
- citrix;
- counterstrike-source;
- cvs;
- dayofdefeat-source;
- dhcp;
- directconnect;
- dns;
- doom3;
- edonkey;
- fasttrack;
- finger;
- freenet;
- ftp;
- gkrellm;
- gnucleuslan;
- gnutella;
- goboogy;
- gopher;
- guildwars;
- h323;
- halflife2-deathmatch;
- hddtemp;
- hotline;
- http-rtsp;
- http;
- ident;

- imap;
- imesh;
- ipp;
- irc;
- jabber;
- kugoo;
- live365;
- liveforspeed;
- lpd;
- mohaa;
- msn-filetransfer;
- msnmessenger;
- mute;
- napster;
- nbns;
- ncp;
- netbios;
- nntp;
- ntp;
- openft;
- pcanywhere;
- poco;
- pop3;
- pplive;
- qq;
- quake-halflife;
- quake1;
- radmin;
- rdp;
- replaytv-ivs;
- rlogin;
- rtcp;
- rtp;
- rtsp;
- shoutcast;
- sip;
- skypeout;
- skypetoskype;
- smb;
- smtp;
- snmp;
- socks;
- soribada;
- soulseek;
- ssdp;

- ssh;
- ssl;
- stun;
- subspace;
- subversion;
- teamfortress2;
- teamspeak;
- telnet;
- tesla;
- tftp;
- thecircle;
- tor;
- tsp;
- unknown;
- unset;
- uucp;
- validcertssl;
- ventrilo;
- vnc;
- whois;
- worldofwarcraft;
- x11;
- xboxlive;
- xunlei;
- yahoo;
- zmaap.

# ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

| | |
|---|---|
| ABR | Area Border Router |
| ACL | access control list |
| ADSL | Asymmetric Digital Subscriber Line |
| API | Application Programming Interface |
| ARP | Address Resolution Protocol |
| AS | autonomous system |
| ASBR | Autonomous System Border Router) |
| BDR | Backup Designated Router |
| BGP | Border Gateway Protocol |
| BIOS | Basic Input Output System |
| BPDU | Bridge Protocol Data Unit |
| CA | certificate authority |
| CHAP | Challenge Handshake Authentication Protocol |
| CLI | command-line interface |
| DD | database description |
| DDNS | dynamic DNS |
| DHCP | Dynamic Host Configuration Protocol |
| DHCPv6 | Dynamic Host Configuration Protocol version 6 |
| DLCI | data-link connection identifier |
| DMI | desktop management interface |
| DMZ | demilitarized zone |
| DN | distinguished name |
| DNS | Domain Name System |
| DR | Designated Router |
| DSCP | Differentiated Services Code Point |
| DSL | Digital Subscriber Line |
| eBGP | external BGP |
| ECMP | equal-cost multipath |

| | |
|---|---|
| EGP | Exterior Gateway Protocol |
| ESP | Encapsulating Security Payload |
| FIB | Forwarding Information Base |
| FTP | File Transfer Protocol |
| GRE | Generic Routing Encapsulation |
| HDLC | High-Level Data Link Control |
| I/O | Input/Ouput |
| ICMP | Internet Control Message Protocol |
| IDS | Intrusion Detection System |
| IPS | Intrusion Prevention System |
| IEEE | Institute of Electrical and Electronics Engineers |
| IGP | Interior Gateway Protocol |
| IGP | Interior Gateway Protocol |
| IKE | Internet Key Exchange |
| IP | Internet Protocol |
| IPOA | IP over ATM |
| IPS | Intrusion Prevention System |
| IPSec | IP security |
| IPv4 | IP Version 4 |
| IPv6 | IP Version 6 |
| ISP | Internet Service Provider |
| L2TP | Layer 2 Tunneling Protocol |
| LACP | Link Aggregation Control Protocol |
| LAN | local area network |
| LDAP | Lightweight Directory Access Protocol |
| LSA | link-state advertisement |
| LSR | link-state request |
| LSU | link-state update |
| MAC | medium access control |

| | |
|---|---|
| MIB | Management Information Base |
| MLPPP | multilink PPP |
| MPLS-TE | Multi-Protocol Label Switching Traffic Engineering |
| MRRU | maximum received reconstructed unit |
| MTA | Mail Transfer Agent |
| MTU | maximum transmission unit |
| MX | Mail eXchanger |
| NAT | Network Address Translation |
| ND | Neighbor Discovery |
| NIC | network interface card |
| NSSA | not-so-stubby areas |
| NTP | Network Time Protocol |
| OSPF | Open Shortest Path First |
| OSPFv2 | OSPF Version 2 |
| OSPFv3 | OSPF Version 3 |
| PAM | Pluggable Authentication Module |
| PAP | Password Authentication Protocol |
| PAT | Port Address Translation |
| PCI | peripheral component interconnect |
| PKI | Public Key Infrastructure |
| PPP | Point-to-Point Protocol |
| PPPoA | PPP over ATM |
| PPPoE | PPP over Ethernet |
| PPTP | Point-to-Point Tunneling Protocol |
| PVC | permanent virtual circuit |
| QoS | quality of service |
| RA | router advertisement |
| RADIUS | Remote Authentication Dial-In User Service |
| RIB | Routing Information Base |

| | |
|---|---|
| RIP | Routing Information Protocol |
| RIPng | RIP next generation |
| RS | router solicitation |
| Rx | receive |
| SLAAC | Stateless address auto-configuration |
| SMTP | Simple Mail Transfer Protocol |
| SNMP | Simple Network Management Protocol |
| SONET | Synchronous Optical Network |
| SPF | Shortest Path First |
| SPT | Shortest Path Tree |
| SSH | Secure Shell |
| STP | Spanning Tree Protocol |
| TACACS+ | Terminal Access Controller Access Control System Plus |
| TCP | Transmission Control Protocol |
| ToS | Type of Service |
| Tx | transmit |
| UDP | User Datagram Protocol |
| vif | virtual interface |
| VLAN | virtual LAN |
| VPN | Virtual Private Network |
| VRRP | Virtual Router Redundancy Protocol |
| WAN | wide area network |

# ПЕРЕЧЕНЬ РИСУНКОВ

# ПЕРЕЧЕНЬ ТАБЛИЦ

# СПИСОК ПРИМЕРОВ