

Маршрутизаторы ELTEX серии ME. Руководство по настройке.

Eltex Network OS for ME5k series ver. 1.8.2

Оглавление

| | |
|--|----|
| ВВЕДЕНИЕ | 1 |
| Аннотация | 1 |
| Целевая аудитория | 1 |
| Условные обозначения | 1 |
| ОСНОВЫ РАБОТЫ С КОМАНДНОЙ СТРОКОЙ | 3 |
| Командный интерфейс и доступ к устройству | 3 |
| Режимы командного интерфейса и команды навигации | 3 |
| Работа с глобальным режимом | 4 |
| Работа с режимом конфигурирования | 5 |
| Именованье интерфейсов | 7 |
| ФУНКЦИИ УПРАВЛЕНИЯ | 10 |
| Настройка параметров системы безопасности | 10 |
| Механизм AAA | 11 |
| Настройка серверов TACACS+ и RADIUS | 12 |
| Настройка серверов SSH и telnet | 14 |
| Настройка параметров терминальных сессий | 16 |
| ИНТЕРФЕЙСЫ И АДРЕСАЦИЯ | 19 |
| Параметры, настраиваемые на интерфейсах | 19 |
| Режим маршрутизации и режим коммутации | 19 |
| Настройка IP-адресации, параметров ARP и описания интерфейса | 20 |
| Настройка MTU, режимов физического интерфейса и интервала подсчета статистики .. | 22 |
| Настройка базовых ограничителей полосы пропускания интерфейса | 23 |
| Назначение QoS-политик и классификаторов трафика на интерфейсе | 24 |
| Использование агрегирующих интерфейсов | 25 |
| Использование сабинтерфейсов | 28 |
| Команды диагностики интерфейсов | 32 |
| ПОСТОЯННЫЕ МАРШРУТЫ И СТАТИЧЕСКАЯ МАРШРУТИЗАЦИЯ | 35 |
| Типы постоянных маршрутов | 35 |
| Присоединенные маршруты | 35 |
| Локальные маршруты | 35 |
| Просмотр присоединенных и локальных маршрутов | 36 |
| Статические маршруты | 36 |
| Команды просмотра маршрутной информации | 39 |
| НАСТРОЙКА ПРОТОКОЛА OSPF | 42 |
| Принципы конфигурирования протокола OSPFv2 | 42 |
| Базовая настройка протокола OSPFv2 | 42 |
| Настройка OSPF для экземпляра VRF | 45 |
| Работа с протоколом BFD | 48 |

| | |
|--|-----|
| Редистрибуция маршрутной информации | 48 |
| Аутентификация OSPF | 50 |
| Проверка работы OSPF и диагностические команды | 51 |
| НАСТРОЙКА ПРОТОКОЛА IS-IS | 57 |
| Принципы конфигурирования протокола IS-IS | 57 |
| Базовая настройка протокола IS-IS | 57 |
| Настройка IS-IS для экземпляра VRF | 60 |
| Работа с протоколом BFD | 64 |
| Редистрибуция маршрутной информации | 64 |
| Аутентификация IS-IS | 67 |
| Проверка работы IS-IS и диагностические команды | 68 |
| НАСТРОЙКА ПРОТОКОЛА BGP | 75 |
| Принципы конфигурирования протокола BGP | 75 |
| Базовая настройка BGP-процесса | 77 |
| Фильтрация маршрутов списками префиксов (prefix-lists) | 80 |
| Фильтрация маршрутов посредством route-map | 84 |
| Internal BGP и External BGP | 88 |
| Административная дистанция протокола BGP | 89 |
| НАСТРОЙКА MPLS-КОММУТАЦИИ И ПРОТОКОЛА LDP | 91 |
| Необходимые шаги | 91 |
| Предварительная настройка IGP | 91 |
| Настройка протокола LDP | 93 |
| LDP-IGP синхронизация | 95 |
| Включение в LDP дополнительных интерфейсов (редистрибуция) | 96 |
| Проверка работы протокола LDP и диагностические команды | 97 |
| НАСТРОЙКА MPLS L3VPN | 102 |
| Необходимые шаги | 102 |
| Создание экземпляров VRF и технология VRF Lite | 102 |
| Настройка MP-BGP | 106 |
| Установка BGP-путей в качестве маршрутов экземпляра VRF | 111 |
| Процесс BGP для экземпляра VRF и редистрибуция маршрутов | 114 |
| НАСТРОЙКА MPLS L2VPN | 117 |
| Составные элементы L2VPN | 117 |
| Настройка бридж-доменов | 118 |
| Настройка кросс-коннектов | 124 |

ВВЕДЕНИЕ

Аннотация

Настоящее руководство содержит описание методов настройки функций маршрутизаторов ELTEX серии ME. В разделах руководства приведены примеры настройки функциональных блоков, полное описание всех имеющихся команд с пояснением их параметров содержится в "Справочнике команд".

Интерфейс командной строки (Command Line Interface, CLI) — интерфейс, предназначенный для управления, просмотра состояния и мониторинга устройства. Для работы потребуется любая установленная на ПК программа, поддерживающая работу по протоколу Telnet, SSH или прямое подключение через консольный порт (например, Putty/SecureCRT).

Целевая аудитория

Руководство по настройке предназначено для технического персонала, выполняющего настройку и мониторинг маршрутизаторов серии ME посредством интерфейса командной строки (CLI). Квалификация технического персонала предполагает знание основ работы стека протоколов TCP/IP и принципов построения IP/MPLS-сетей.

Условные обозначения

Таблица 1. Обозначения в примерах и описаниях команд

| Обозначения | Описание |
|------------------------------|---|
| <code>command example</code> | Моноширинным шрифтом приведены примеры ввода команд и результатов их выполнения. |
| [] | В квадратных скобках для команд указываются необязательные параметры. |
| { } | В фигурных скобках для команд указываются возможные обязательные параметры, приведенные списком. Необходимо выбрать один из параметров. |
| | Данный знак в описании команды обозначает "или". |
| < > | В угловых скобках для команд указывается имя параметра, тип и значение которого объясняются в описании. |

NOTE | Примечания содержат полезную информацию, которую необходимо учитывать при настройке устройства.

IMPORTANT | Примечания содержат важную информацию, советы или рекомендации по использованию и настройке устройства.

CAUTION

Предупреждения информируют пользователя о ситуациях, которые могут нанести вред устройству, привести к некорректной работе системы, потере данных или нарушению прохождения и обработки трафика.

ОСНОВЫ РАБОТЫ С КОМАНДНОЙ СТРОКОЙ

Командный интерфейс и доступ к устройству

Основным инструментом настройки и управления устройством является интерфейс командной строки (CLI).

Учётной записью по умолчанию является **admin** с паролем **password**. Данной учётной записью можно воспользоваться для авторизации на устройстве и получения доступа к командному интерфейсу в процессе первоначальной настройки.

IMPORTANT

Операционная система устройства имеет систему разделения привилегий пользователей. Пользователю **admin** по умолчанию назначены максимальные привилегии - уровень *p15*.

Командный интерфейс устройства поддерживает функцию автоматического дополнения команд. Эта функция активируется при нажатии клавиши табуляции <TAB>. Также интерфейс командной строки имеет функцию контекстной подсказки. На любом этапе ввода команды можно получить подсказку о следующих возможных элементах команды путём ввода вопросительного знака <?>.

Режимы командного интерфейса и команды навигации

Интерфейс командной строки имеет два основных режима — глобальный режим и режим конфигурирования. Для удобства оператора при переходе между режимами меняется приглашение командной строки.

Вид приглашения командной строки в глобальном режиме

```
0/ME5100:EOS#
```

Вид приглашения командной строки в режиме конфигурирования

```
0/ME5100:EOS(config)#
```

Таблица 2. Основные команды навигации и переходов в интерфейсе командной строки

| Команда | Режим | Действие команды |
|------------------------|--------------------------|--|
| <code>configure</code> | <code>global-view</code> | Переход из глобального режима CLI в режим конфигурирования |
| <code>exit</code> | <code>config</code> | Переход на вышестоящий уровень конфигурирования |

| Команда | Режим | Действие команды |
|--|----------------------------------|---|
| <code>logout</code> | <code>config, global-view</code> | Быстрый выход из сессии интерфейса командной строки |
| <code>do <command_sequence></code> | <code>config</code> | Выполнение команды глобального режима CLI (<code>command_sequence</code>) без выхода из режима конфигурирования |
| <code>root</code> | <code>config</code> | Выход на верхний уровень режима конфигурирования |
| <code>end</code> | <code>config</code> | Выход из любого уровня режима конфигурирования в глобальный режим |
| <code>quit</code> | <code>global-view</code> | Выход из сессии интерфейса командной строки |

Работа с глобальным режимом

В глобальном режиме интерфейса командной строки доступны команды просмотра оперативного состояния системы (`show`-команды), команды управления компонентами системы (например, `reload`, `hw-module`), запуска различных диагностических тестов и работы с образами операционной системы.

Для уменьшения объема отображаемых данных в ответ на запросы пользователя и облегчения поиска необходимой информации можно воспользоваться фильтрацией. Для фильтрации вывода команд нужно добавить в конец командной строки символ "|" и использовать одну из опций фильтрации:

- `begin` — выводить всё после строки, содержащей заданный шаблон;
- `include` — выводить все строки, содержащие заданный шаблон;
- `exclude` — выводить все строки, не содержащие заданный шаблон;
- `count` — произвести подсчёт количества строк в выводе команды.

При необходимости включить в шаблон поиска символ пробела необходимо заключить весь шаблон в двойные кавычки.

Фильтры можно стекировать, указывая несколько фильтров через символы "|".

```
0/ME5100:EOS# show running-config | begin "telnet server"
Thu Mar 23 12:03:57 2017

telnet server vrf mgmt-intf
exit

user admin
  password encrypted
  $6$zMGqwSsQnYcfDrxH$6TGyBVbqUB8s2InhRT4QA5VADoCc4zGhILDKjTxgVt7H0TBzxmbwNkpkH5kHNAU9qC
  zdQ/ZeonLI8E0rkII620
  privilege p15
exit

0/ME5100:EOS#
```

Работа с режимом конфигурирования

В режиме конфигурирования командный интерфейс системы позволяет производить настройку устройства. Переход в режим конфигурирования производится командой `configure`. В режиме конфигурирования интерфейс принимает и распознает команды настройки соответствующих разделов. Все введенные команды, в свою очередь, формируют общую конфигурацию устройства.

Командный интерфейс системы работает с двумя экземплярами конфигурации устройства:

- Текущая конфигурация (*running-config*). Текущая конфигурация — это конфигурация, которая в данный момент применена и используется на маршрутизаторе.
- Кандидат-конфигурация (*candidate-config*). Кандидат-конфигурация — это конфигурация, которая включает в себя изменения, внесенные оператором в процессе сеанса конфигурирования. Кандидат-конфигурация может быть применена в качестве текущей.

IMPORTANT

Все введенные в режиме конфигурирования команды **не применяются** по мере ввода, а заносятся в кандидат-конфигурацию (*candidate-config*).

В обычном состоянии системы кандидат-конфигурация идентична текущей. После внесения изменений в кандидат-конфигурацию её можно либо применить (скопировать в текущую), либо отменить.

Таблица 3. Основные команды работы с экземплярами конфигурации

| Команда | Режим | Действие команды |
|------------------------|--------------------|---|
| <code>configure</code> | <i>global-view</i> | Перейти из глобального режима CLI в режим конфигурирования. |

| Команда | Режим | Действие команды |
|---|--------------------|--|
| <code>show running-config</code> | <i>global-view</i> | Вывести текущую конфигурацию устройства. |
| <code>show candidate-config</code> | <i>global-view</i> | Вывести кандидат-конфигурацию устройства. |
| <code>show configuration changes</code> | <i>global-view</i> | Вывести список изменений в кандидат-конфигурации относительно текущей конфигурации устройства. |
| <code>commit</code> | <i>config</i> | Применить кандидат-конфигурацию (применить изменения, внесенные во время сеанса редактирования). |
| <code>abort</code> | <i>config</i> | Отменить изменения в кандидат-конфигурации и выйти из режима конфигурирования. При выполнении этой команды кандидат-конфигурация становится идентичной текущей (стартовой) конфигурации. |

IMPORTANT

При выполнении команды `commit` текущая конфигурация автоматически сохраняется на устройстве в качестве загрузочной. Отдельной команды сохранения конфигурации на устройстве нет.

CAUTION

Текущая версия командного интерпретатора не поддерживает несколько кандидат-конфигураций и независимое конфигурирование устройства из разных сессий. Кандидат-конфигурация в любой момент времени является единой для всего устройства. Таким образом, команды `commit` и `abort`, введенные оператором, могут повлиять на изменения, внесенные в других сессиях конфигурирования.

Пример: настройка системного имени (hostname)

```
EOS login: admin
Password:

*****
*           Welcome to ME5100           *
*****

0/ME5100:EOS# config
0/ME5100:EOS(config)# hostname Router
0/ME5100:EOS(config)# do show configuration changes
Tue Jan 18 21:37:19 2000

hostname Router
0/ME5100:EOS(config)# commit
Tue Jan 18 21:37:23 2000

Commit successfully completed in 0.031951 sec
0/ME5100:Router(config)# end
0/ME5100:Router#
```

Именованние интерфейсов

При работе маршрутизатора используются сетевые интерфейсы различного типа и назначения. Система именования позволяет однозначно адресовать интерфейсы по их функциональному назначению и местоположению в системе. Далее в таблице приведен перечень типов интерфейсов.

Таблица 4. Поддерживаемые типы интерфейсов

| Тип интерфейса | Обозначение и функционал |
|---------------------------------|---|
| Физические интерфейсы | <p>Обозначение физического интерфейса включает в себя его тип и идентификатор.</p> <p>Идентификатор имеет вид <code><UNIT>/<SLOT>/<PORT></code>, где:</p> <ul style="list-style-type: none">• <code><UNIT></code> - номер устройства в кластере устройств;• <code><SLOT></code> - номер модуля в составе устройства;• <code><PORT></code> - порядковый номер интерфейса данного типа в модуле. <p><i>Физические интерфейсы всегда присутствуют в системе.</i></p> |
| Интерфейсы Ethernet 10Гбит/с | <p><code>tengigabitethernet <UNIT>/<SLOT>/<PORT></code></p> <p>Пример обозначения: <code>'tengigabitethernet 0/0/10'</code>. Допускается использовать сокращенную форму с обязательным пробелом, например, <code>'te 0/0/10'</code>.</p> |

| Тип интерфейса | Обозначение и функционал |
|----------------------------------|--|
| Интерфейсы Ethernet 40Гбит/с | <p><code>fourtygigabitethernet <UNIT>/<SLOT>/<PORT></code></p> <p>Пример обозначения: <code>'fourtygigabitethernet 0/0/2'</code>. Допускается использовать сокращенную форму с обязательным пробелом, например, <code>'fo 0/0/2'</code>.</p> |
| Интерфейсы Ethernet 100Гбит/с | <p><code>hundredgigabitethernet <UNIT>/<SLOT>/<PORT></code></p> <p>Пример обозначения: <code>'hundredgigabitethernet 0/0/3'</code>. Допускается использовать сокращенную форму с обязательным пробелом, например, <code>'hu 0/0/3'</code>.</p> |
| Группы агрегации каналов | <p><code>bundle-ether <BUNDLE_ID></code></p> <p>Обозначение группы агрегации каналов включает в себя тип интерфейса ("bundle-ether") и порядковый номер группы. Пример обозначения: <code>'bundle-ether 8'</code>. Допускается использовать сокращенную форму с обязательным пробелом, например, <code>'bu 8'</code>.</p> <p><i>Группы агрегации каналов в системе можно создавать и удалять.</i></p> |
| Сабинтерфейсы | <p><code>bundle-ether <BUNDLE_ID>.<SUBIF_ID></code> <code>tengigabitethernet <UNIT>/<SLOT>/<PORT>.<SUBIF_ID></code> <code>fourtygigabitethernet <UNIT>/<SLOT>/<PORT>.<SUBIF_ID></code> <code>hundredgigabitethernet <UNIT>/<SLOT>/<PORT>.<SUBIF_ID></code></p> <p>Обозначение сабинтерфейса образуется из обозначения базового интерфейса и идентификатора сабинтерфейса, разделенных точкой. Для сабинтерфейсов обязательно задание типа инкапсуляции ('encapsulation'). Пример обозначения: <code>'tengigabitethernet 0/0/10.350'</code></p> <p><i>Сабинтерфейсы в системе можно создавать и удалять.</i></p> |
| Интерфейсы локальной петли | <p><code>loopback <ID></code></p> <p>Виртуальный интерфейс локальной петли. Данный тип применяется в случаях, когда требуется постоянно активный логический интерфейс. Пример обозначения: <code>'loopback 100'</code></p> <p><i>Интерфейсы локальной петли в системе можно создавать и удалять.</i></p> |

| Тип интерфейса | Обозначение и функционал |
|-----------------------|--|
| Интерфейсы управления | <p data-bbox="536 159 890 192"><code>mgmt <UNIT>/<SLOT>/<PORT></code></p> <p data-bbox="536 230 1458 387">Интерфейсы out-of-band управления - это выделенные ethernet-интерфейсы для доступа и управления маршрутизатором. В качестве <SLOT> могут выступать 'fmc0' и 'fmc1', в зависимости от аппаратной конфигурации. Примеры обозначений:</p> <ul data-bbox="560 427 1458 658" style="list-style-type: none"> <li data-bbox="560 427 991 461">• <code>'mgmt 0/fmc0/1'</code> - для ME5100; <li data-bbox="560 488 1458 562">• <code>'mgmt 0/fmc0/0'</code> и <code>'mgmt 0/fmc0/1'</code> для FMC0 в маршрутизаторе ME5000; <li data-bbox="560 589 1458 658">• <code>'mgmt 0/fmc1/0'</code> и <code>'mgmt 0/fmc1/1'</code> для FMC1 в маршрутизаторе ME5000 <p data-bbox="536 701 1374 734"><i>Интерфейсы управления всегда присутствуют в системе.</i></p> <div data-bbox="568 768 1458 987" style="border: 1px solid gray; padding: 5px;"> <p data-bbox="568 831 746 864">IMPORTANT</p> <p data-bbox="810 786 1458 987">Интерфейсы управления не предназначены для передачи транзитного трафика (не участвуют в работе data-plane) и жестко прикреплены к VRF 'mgmt-intf'.</p> </div> |

NOTE

1. Количество физических интерфейсов в системе зависит от модели маршрутизатора и установленных линейных модулей.
2. Текущая версия ПО не поддерживает кластеризацию. Номер устройства в кластере <UNIT> может принимать только значение 0.

ФУНКЦИИ УПРАВЛЕНИЯ

Настройка параметров системы безопасности

Как указывалось выше, учётной записью по умолчанию является admin с паролем password. Для локального доступа к устройству рекомендуется создать учетные записи пользователей, возможно, ограничив для них уровень привилегий.

Таблица 5. Настройка локальной учетной записи

| Команда | Назначение |
|--|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>user user_name</code> | Переход в режим конфигурации учетной записи пользователя. |
| <code>password [encrypted] password</code> | Задание пароля пользователя в открытом или зашифрованном виде. |
| <code>privilege p1-p15</code> | Задание уровня привилегий пользователя. |
| <code>exit</code> | (Опционально) Возврат в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

Пример. Настройка учетной записи пользователя.

```
user test
  password test123
  privilege p10
exit
```

Также можно задать локальный пароль для каждого уровня привилегий.

Пример.

```
enable p15
  password highest
exit
```

Таблица 6. Команда перехода на соответствующий уровень привилегий в текущей сессии

| Команда | Назначение |
|---|--|
| <code>change-privilege { p1 p2 .. p15 } [PASSWORD]</code> | Переход на соответствующий уровень привилегий. |

Пример.

```
0/ME5100:Router> change-privilege p15 highest
0/ME5100:Router#
```

NOTE | Переход на меньший уровень привилегий производится без пароля.

Механизм AAA

Для обеспечения безопасности системы используется механизм AAA (аутентификация, авторизация, учет):

- authentication (аутентификация) — сопоставление запроса существующей учётной записи в системе безопасности;
- authorization (авторизация, проверка уровня доступа) — сопоставление учётной записи в системе (прошедшей аутентификацию) и определённых полномочий;
- accounting (учёт) — учёт действий пользователя.

Таблица 7. Настройка аутентификации

| Команда | Назначение |
|--|---|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>aaa authentication { login enable } list_name</code> | Создание списка аутентификации. <ul style="list-style-type: none">• <code>login</code> — для входа в систему;• <code>enable</code> — для смены уровня привилегий. |
| <code>method { local tacacs radius }</code> | Задание метода аутентификации внутри соответствующего списка аутентификации. <ul style="list-style-type: none">• <code>local</code> — метод устанавливает локальную аутентификацию, то есть аутентификацию согласно настройкам 'enable' и 'user' в текущей конфигурации;• <code>tacacs</code> — метод устанавливает аутентификацию через сконфигурированные TACACS+-серверы;• <code>radius</code> — метод устанавливает аутентификацию через сконфигурированные RADIUS-серверы. |
| <code>exit</code> | (Опционально) Возврат в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

Таблица 8. Настройка авторизации и учета

| Команда | Назначение |
|---|---|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>aaa authorization commands tacacs</code> | Включение авторизации команд пользователя через TACACS+-сервер. |
| <code>aaa accounting commands { start-only start-stop stop-only } tacacs</code> | Включение логирования команд пользователя на TACACS+-сервере. |
| <code>aaa accounting login start-stop { tacacs radius } tacacs</code> | Включение логирования входа пользователя в систему и выхода из нее на TACACS+ или RADIUS-сервере. |
| <code>exit</code> | (Опционально) Возврат в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

Пример. Настройка аутентификации для сервиса telnet.

```
aaa authentication login TAC245
  method tacacs
  method local
exit

line telnet login authentication TAC245
```

Настройка серверов TACACS+ и RADIUS

Таблица 9. Настройка сервера TACACS+

| Команда | Назначение |
|---|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>tacacs-server host { IP_serveraddr IPv6_serveraddr} [vrf vrf_name]</code> | Задание в конфигурации сервера TACACS+ с указанным IPv4 (IPv6)-адресом в глобальной таблице маршрутизации (GRT) или внутри указанного VRF. |
| <code>password [encrypted] password</code> | Задание пароля сервера TACACS+ в открытом или зашифрованном виде. |
| <code>priority priority</code> | Задание приоритета TACACS-сервера . |
| <code>exit</code> | Возврат в режим глобальной конфигурации. |

| Команда | Назначение |
|--|--|
| <code>tacacs-server timeout secs</code> | (Опционально) Задание времени ожидания ответа от серверов TACACS+, в секундах. |
| <code>tacacs-server dscp dscp_val</code> | (Опционально) Задание значения поля DSCP, с которым будут генерироваться IP-пакеты, отправляемые на серверы TACACS+. |
| <code>commit</code> | Применение произведенных настроек. |

Пример. Настройка сервера TACACS+.

```
tacacs-server timeout 10
tacacs-server dscp 7
tacacs-server host 192.168.16.245 vrf mgmt-intf
    password encrypted 8FB1007FB51B43FED3
exit
```

Таблица 10. Настройка сервера RADIUS

| Команда | Назначение |
|---|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>radius-server host { IP_serveraddr IPv6_serveraddr} [vrf vrf_name]</code> | Задание в конфигурации сервера RADIUS с указанным IPv4 (IPv6)-адресом в глобальной таблице маршрутизации (GRT) или внутри указанного VRF. |
| <code>password [encrypted] password</code> | Задание пароля сервера RADIUS в открытом или зашифрованном виде. |
| <code>priority priority</code> | Задание приоритета RADIUS-сервера. |
| <code>source-address { IP_intf-addr IPv6_intf-addr }</code> | Задание IP (IPv6) адреса, который будет использоваться в качестве IP-адреса отправителя при отправке пакетов на RADIUS-сервер. Следует указывать адрес, принадлежащий интерфейсу маршрутизатора в соответствующем VRF. |
| <code>acct-port port</code> | (Опционально) Задание номера UDP-порта для передачи данных учета. |
| <code>auth-port port</code> | (Опционально) Задание номера порта для передачи аутентификационных данных. |
| <code>timeout secs</code> | (Опционально) Задание времени ожидания ответа от сервера RADIUS, в секундах. |

| Команда | Назначение |
|---|---|
| <code>usage type</code> | (Опционально) Выбор типа использования RADIUS-сервера. |
| <code>exit</code> | Возврат в режим глобальной конфигурации. |
| <code>timeout secs</code> | (Опционально) Задание времени ожидания ответа от серверов TACACS+, в секундах. |
| <code>radius-server dscp dscp_val</code> | (Опционально) Задание значения поля DSCP, с которым будут генерироваться IP-пакеты, отправляемые на серверы RADIUS. |
| <code>radius-server timeout secs</code> | (Опционально) Задание времени ожидания ответа от серверов RADIUS, в секундах. |
| <code>radius-server retransmit val</code> | (Опционально) Задание количества попыток обращения к RADIUS-серверу. |
| <code>commit</code> | Применение произведенных настроек. |

Пример. Настройка сервера RADIUS.

```
radius-server host 10.1.1.10 vrf test
  password radius-pass
  source-address 5.5.0.0
  timeout 10
  usage aaa
exit
```

Настройка серверов SSH и telnet

Удаленный доступ к управлению устройством осуществляется по протоколу SSH или telnet, локальный - через консольный порт. Для удаленного доступа необходимо указать в конфигурации соответствующие серверы.

Таблица 11. Настройка telnet-сервера.

| Команда | Назначение |
|------------------------|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |

| Команда | Назначение |
|---|--|
| <code>telnet server [vrf vrf_name]</code> | Создание в конфигурации Telnet-сервера и переход в режим настройки его параметров (config-telnet-server-vrf). При запуске Telnet-сервера в каком-либо VRF (либо в глобальной таблице маршрутизации) устройство начинает принимать соединения по протоколу Telnet на тех своих интерфейсах, которые включены в указанный VRF. |
| <code>dscp dscp_val</code> | (Опционально) Задание значения поля DSCP, с которым будут генерироваться IP-пакеты. |
| <code>session-limit val</code> | (Опционально) Задание максимального количества одновременно подключенных пользователей |
| <code>port val</code> | (Опционально) Задание номера порта, по которому будет принимать входящие соединения соответствующий локальный сервер. |
| <code>exit</code> | (Опционально) Возврат в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

Таблица 12. Настройка SSH-сервера.

| Команда | Назначение |
|--|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>ssh server [vrf vrf_name]</code> | Создание в конфигурации Telnet-сервера и переход в режим настройки его параметров (config-ssh-server-vrf). При запуске Telnet-сервера в каком-либо VRF (либо в глобальной таблице маршрутизации) устройство начинает принимать соединения по протоколу SSH на тех своих интерфейсах, которые включены в указанный VRF. |
| <code>dscp dscp_val</code> | (Опционально) Задание значения поля DSCP, с которым будут генерироваться IP-пакеты. |
| <code>session-limit val</code> | (Опционально) Задание максимального количества одновременно подключенных пользователей |
| <code>port val</code> | (Опционально) Задание номера порта, по которому будет принимать входящие соединения соответствующий локальный сервер. |

| Команда | Назначение |
|---------------------|--|
| <code>exit</code> | (Опционально) Возврат в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

Настройка параметров терминальных сессий

Таблица 13. Настройка Telnet-сессии.

| Команда | Назначение |
|--|---|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>line telnet enable authentication list_name</code> | Включение enable-аутентификации (аутентификации при переходе на разные уровни привилегий) подключенных по протоколу Telnet пользователей через ранее сконфигурированный список методов AAA ('aaa authentication enable'). После выполнения данной команды enable-аутентификация подключенных по протоколу Telnet пользователей будет проводиться по методам, указанным в этом списке. |
| <code>line telnet login authentication list_name</code> | Включение аутентификации входа пользователей при подключении по протоколу Telnet через ранее сконфигурированный список методов AAA ('aaa authentication login'). После выполнения данной команды аутентификация входа подключенных по протоколу Telnet пользователей будет проводиться по методам, указанным в этом списке. |
| <code>line telnet session-timeout val</code> | (Опционально) Задание периода неактивности (в минутах) для подключенных по протоколу telnet пользователей, по истечении которого сессии таких пользователей будет принудительно завершены. |
| <code>commit</code> | Применение произведенных настроек. |

Таблица 14. Настройка SSH-сессии.

| Команда | Назначение |
|------------------------|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |

| Команда | Назначение |
|---|---|
| <code>line ssh enable authentication list_name</code> | Включение enable-аутентификации (аутентификации при переходе на разные уровни привилегий) подключенных по протоколу SSH пользователей через ранее сконфигурированный список методов AAA ('aaa authentication enable'). После выполнения данной команды enable-аутентификация подключенных по протоколу SSH пользователей будет проводиться по методам, указанным в этом списке. |
| <code>line ssh login authentication list_name</code> | Включение аутентификации входа пользователей при подключении по протоколу SSH через ранее сконфигурированный список методов AAA ('aaa authentication login'). После выполнения данной команды аутентификация входа подключенных по протоколу Telnet пользователей будет проводиться по методам, указанным в этом списке. |
| <code>line ssh session-timeout val</code> | (Опционально) Задание периода неактивности (в минутах) для подключенных по протоколу SSH пользователей, по истечении которого сессии таких пользователей будет принудительно завершены. |
| <code>commit</code> | Применение произведенных настроек. |

Таблица 15. Настройка локальной консольной сессии.

| Команда | Назначение |
|---|---|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>line console enable authentication list_name</code> | Включение аутентификации входа пользователей на консольном порту устройства через ранее сконфигурированный список методов AAA ('aaa authentication login'). После выполнения данной команды аутентификация входа через консоль будет проводиться по методам, указанным в этом списке. |
| <code>line console login authentication list_name</code> | Включение аутентификации входа пользователей на консольном порту устройства через ранее сконфигурированный список методов AAA ('aaa authentication login'). После выполнения данной команды аутентификация входа через консоль будет проводиться по методам, указанным в этом списке. |

| Команда | Назначение |
|---|---|
| <code>line console session-timeout val</code> | (Опционально) Задание периода неактивности подключенного на консольном порту пользователя, по истечении которого сессия пользователя будет принудительно завершена. |
| <code>commit</code> | Применение произведенных настроек. |

Пример. Настройка Telnet-сессии.

```
line telnet login authentication TAC245
line telnet enable authentication PRI0
line telnet session-timeout 40
```

ИНТЕРФЕЙСЫ И АДРЕСАЦИЯ

Параметры, настраиваемые на интерфейсах

Синтаксис командной строки маршрутизаторов является функционально-ориентированным. Это означает, что непосредственно на интерфейсах настраивается только ограниченный список параметров, при этом протокольные настройки (например, интерфейсные настройки протокола OSPF) задаются в отдельных протокольных блоках CLI.

На интерфейсах конфигурируется:

- Строковое описание интерфейса (для всех интерфейсов);
- Назначение IP-адресов и экземпляра VRF, к которому относится интерфейс;
- Параметры работы протокола ARP (для всех интерфейсов, кроме локальной петли, loopback);
- Параметры максимального размера пакетов — MTU канального уровня и протокольные IP MTU (для физических и агрегирующих интерфейсов);
- Интервал подсчёта статистики по трафику (для всех интерфейсов, кроме локальной петли);
- Параметры базовых ограничителей полосы (для всех интерфейсов, кроме локальной петли);
- Назначение политики QoS и классификаторов входящего трафика (для всех интерфейсов, кроме локальной петли);
- Административный статус интерфейса (shutdown);
- Режимы работы интерфейсов — скорость и дуплекс (для физических интерфейсов);
- Параметры MicroBFD (только для агрегирующих интерфейсов).

Режим маршрутизации и режим коммутации

Интерфейс маршрутизатора может находиться в одном из двух режимов — в режиме маршрутизации (*layer3 forwarding*) либо коммутации (*layer2 forwarding*).

Режим маршрутизации означает, что на интерфейсе сконфигурирован IPv4/IPv6-адрес и сквозная коммутация Ethernet-кадров через него невозможна.

Режим коммутации означает, что на интерфейсе не включена IP-маршрутизация и через него может осуществляться сквозная коммутация Ethernet-кадров.

Информация о режиме содержится в выводе команды `show interfaces`:

```
0/ME5100:Router# show interfaces tengigabitethernet 0/0/1.500
Tue Jan 30 21:24:35 2018
  tengigabitethernet 0/0/1.500 is up
    Interface index is 62
    Hardware is tengigabitethernet, address is a8:f9:4b:8b:bc:21
    Encapsulation 802.1Q, VLAN tag 500
    Description is not set
    IPv4 address is 200.1.1.151/24
    No IPv6 address assigned
    Interface is bound to VRF default
    Interface is in layer3 forwarding mode
    ARP aging time is 240 minutes
    Interface MTU is 1518
    Interface IP MTU is 1500
    300 seconds input rate is 0 bit/s
    300 seconds output rate is 0 bit/s
    300 seconds input rate is 0 pps
    300 seconds output rate is 0 pps
      9793 packets input, 666441 bytes received
      893 packets output, 63423 bytes sent
```

IMPORTANT

По умолчанию интерфейсы устройства находятся в режиме коммутации. Режим маршрутизации включается автоматически при назначении IPv4/IPv6-адреса на интерфейс. Подробнее о применении режима коммутации см. раздел "L2VPN и сервисы Ethernet". Интерфейс в режиме layer2 forwarding не осуществляет никакой пересылки пакетов до тех пор, пока не будет включен в бридж-домен или кросс-коннект.

Настройка IP-адресации, параметров ARP и описания интерфейса

Для маршрутизации IP-трафика через интерфейс требуется назначить на нем IPv4/IPv6 адрес и назначить для интерфейса VRF. Если VRF на интерфейсе не сконфигурирован, то интерфейс относится к глобальной таблице маршрутизации устройства (Global Routing Table, GRT).

VRF (Virtual Routing and Forwarding instance) представляет собой виртуальный экземпляр маршрутизации, или простой виртуальный маршрутизатор. Каждый VRF имеет отдельный независимый список интерфейсов, таблицу маршрутизации и ARP-таблицу. Трафик между интерфейсами разных VRF полностью изолирован друг от друга и маршрутизируется независимо.

В случае, если разделение по VRF используется в пределах одного маршрутизатора, метод имеет название VRF lite. Организация одного VRF на нескольких связанных устройствах, как правило, обозначается как технология L3VPN (Layer3 Virtual Private Network).

Использование VRF Lite и L3VPN описано в разделе "L3VPN" данного Руководства.

Локально на интерфейсах также можно назначить параметр ARP timeout. Данный параметр задает максимальное время жизни ARP-записей на указанном интерфейсе. В течение времени жизни записей маршрутизатор периодически производит их обновление путем рассылки ARP-запросов. В случае, если удаленный хост не отвечает на ARP запросы в течение указанного таймаута, запись удаляется из таблицы.

Таблица 16. Последовательность настройки IP-адресации и VRF на интерфейсе

| Команда | Назначение |
|--|---|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>interface type num</code> | Переход в режим настройки интерфейса. |
| <code>vrf vrf_name</code> | Назначение на интерфейсе экземпляра VRF. |
| <code>ipv4 address ipv4address/prefix</code> | Назначение на интерфейсе IPv4-адреса в формате CIDR (адрес/длина префикса). |
| <code>arp aging-time minutes</code> | Задание времени жизни ARP-записей на интерфейсе. Параметр является опциональным и либо наследуется от глобальной настройки arp aging-time , либо устанавливается равным значению по умолчанию — 240 минут. |
| <code>ipv6 address ipv6address/prefix</code> | Назначение на интерфейсе IPv6-адреса. |
| <code>description descr</code> | Назначение на интерфейсе имени-описания. Описание следует заключать в кавычки в случае, если строка содержит символы пробела. |
| <code>commit</code> | Применение произведенных настроек. |

Пример: назначение адреса, описания и экземпляра VRF

```
0/ME5100:Router# configure
0/ME5100:Router(config)# interface tengigabitethernet 0/0/2
0/ME5100:Router(config-tengigabitethernet)# vrf example_vrf
0/ME5100:Router(config-tengigabitethernet)# ipv4 address 10.0.0.1/24
0/ME5100:Router(config-tengigabitethernet)# ipv6 address 2000::1/64
0/ME5100:Router(config-tengigabitethernet)# arp aging-time 10
0/ME5100:Router(config-tengigabitethernet)# description "Example interface"
0/ME5100:Router(config-tengigabitethernet)# commit
```

Пример: задание глобальной конфигурации ARP-таймаута:

```
0/ME5100:Router# configure
0/ME5100:Router(config)# arp aging-time 10
0/ME5100:Router(config)# commit
```


Настройка MTU, режимов физического интерфейса и интервала подсчета статистики

MTU (Maximum Transmission Unit) — максимальный размер передаваемых через интерфейс пакетов. Размер MTU относится к длине Ethernet-фрейма (кадра канального уровня) с учетом VLAN-тегов. Например, для IP-пакета размером в 1500 байт канальный MTU составляет 1522 байта с учетом возможного двойного тегирования.

Установленное значение MTU влияет на передачу всех Ethernet-кадров, независимо от их протокольного содержимого.

IP MTU — максимальный размер передаваемых через интерфейс IPv4/IPv6-пакетов. Значение IP MTU применяется при работе интерфейса в режиме маршрутизации (layer3 forwarding) для транзитного трафика, а также для пакетов, отправляемых самим маршрутизатором с данного интерфейса — например, сигнальным сообщениям протоколов маршрутизации.

NOTE По умолчанию на интерфейсах маршрутизатора используется MTU 1522 байта и IP MTU — 1500 байт.

IMPORTANT Значения MTU и IP MTU задаются целиком для физического интерфейса (либо агрегирующего интерфейса) и наследуются всеми его сабинтерфейсами. Задание значений MTU и IP MTU отдельно на сабинтерфейсах не поддерживается аппаратной платформой. При конфигурировании агрегирующего интерфейса (**bundle-ether**) следует задавать значения MTU на нем, эти значения будут унаследованы составляющими его физическими интерфейсами.

К режимам физического интерфейса относится скорость (speed) и дуплекс (duplex). Список поддерживаемых режимов определяется возможностями установленного в интерфейс трансивера.

NOTE По умолчанию интерфейсы устройства находятся в режиме полного автосогласования (speed auto, duplex auto).

Интервал подсчета статистики определяет время, за которое будет усредняться статистика переданных/отправленных пакетов и байт при вычислении значений текущей загрузки интерфейса.

NOTE По умолчанию интервал подсчета статистики составляет 300 секунд (5 минут). Уменьшение этого интервала позволяет увеличить точность определения "моментальной" загрузки интерфейса.

Таблица 17. Последовательность настройки MTU, режима интерфейса и интервала подсчета статистики

| Команда | Назначение |
|---|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>interface type num</code> | Переход в режим настройки интерфейса. |
| <code>mtu l2_mtu_bytes</code> | Установка канального MTU в байтах. |
| <code>ip mtu ip_mtu_bytes</code> | Установка IP MTU в байтах. |
| <code>speed { 10 100 1G 10G auto }</code> | Задание скорости физического интерфейса. |
| <code>duplex { half full auto }</code> | Задание дуплекса физического интерфейса. |
| <code>load-interval seconds</code> | Установка интервала подсчета загрузки интерфейса в секундах. |
| <code>commit</code> | Применение произведенных настроек. |

Пример: настройка MTU, режима интерфейса и интервала подсчета статистики:

```
0/ME5100:Router# configure
0/ME5100:Router(config)# interface tengigabitethernet 0/0/2
0/ME5100:Router(config-tengigabitethernet)# mtu 9122
0/ME5100:Router(config-tengigabitethernet)# ip mtu 9100
0/ME5100:Router(config-tengigabitethernet)# speed 1G
0/ME5100:Router(config-tengigabitethernet)# duplex full
0/ME5100:Router(config-tengigabitethernet)# load-interval 30
0/ME5100:Router(config-tengigabitethernet)# commit
```

Настройка базовых ограничителей полосы пропускания интерфейса

Для ограничения полосы пропускания интерфейса для входящего трафика используется команда **rate-limit input**, для исходящего трафика — **shape output**. Значение полосы пропускания задается в килобитах в секунду.

При задании полосы на физическом или агрегирующем интерфейсе данное ограничение действует на весь трафик интерфейса, включая его сабинтерфейсы.

Таблица 18. Последовательность настройки базовых ограничителей полосы

| Команда | Назначение |
|---|---|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>interface type num</code> | Переход в режим настройки интерфейса. |
| <code>rate-limit input input_rate_kbps</code> | Установка ограничения полосы для входящего трафика, в килобитах в секунду. |
| <code>shape output output_rate_kbps</code> | Установка ограничения полосы для исходящего трафика, в килобитах в секунду. |
| <code>commit</code> | Применение произведенных настроек. |

Пример: настройка ограничителей полосы для входящего и исходящего трафика:

```
0/ME5100:Router# configure
0/ME5100:Router(config)# interface tengigabitethernet 0/0/2
0/ME5100:Router(config-tengigabitethernet)# shape output 30000
0/ME5100:Router(config-tengigabitethernet)# rate-limit input 30000
0/ME5100:Router(config-tengigabitethernet)# commit
```

Назначение QoS-политик и классификаторов трафика на интерфейсе

Для работы системы обеспечения качества обслуживания (QoS, Quality of Service) требуется назначение классификаторов трафика на интерфейсе. Данные классификаторы позволяют определить принадлежность всего входящего в интерфейс трафика к сконфигурированным на устройстве классам. Назначенная на входе классификация будет использоваться при обработке QoS-политиками на выходе из интерфейсов маршрутизатора.

Таким образом, для обработки трафика согласно политик QoS требуется назначение классификаторов на входе в интерфейсы (**tc-map**) и назначение политик QoS на выходе из интерфейсов (**service-policy**).

Таблица 19. Последовательность назначения классификаторов трафика и политик QoS

| Команда | Назначение |
|---|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>interface type num</code> | Переход в режим настройки интерфейса. |
| <code>tc-map input tcmap_index</code> | Установка классификатора входящего в интерфейс трафика. <i>tcmap_index</i> — номер предварительно сконфигурированного классификатора. |
| <code>service-policy output servicepolicy_name</code> | Установка политики QoS для исходящего из интерфейса трафика. <i>servicepolicy_name</i> — имя предварительно сконфигурированной политики QoS. |
| <code>commit</code> | Применение произведенных настроек. |

Пример: назначение классификатора трафика и политики QoS:

```
0/ME5100:Router# configure
0/ME5100:Router(config)# interface tengigabitethernet 0/0/2.300
0/ME5100:Router(config-tengigabitethernet)# tc-map input 3
0/ME5100:Router(config-tengigabitethernet)# service-policy output VPN_30Mbit
0/ME5100:Router(config-tengigabitethernet)# commit
```

IMPORTANT

В текущей версии ПО назначение политик QoS возможно только на сабинтерфейсы физических и агрегирующих (bundle-ether) интерфейсов. Назначение политик QoS напрямую на физические и агрегирующие интерфейсы не поддерживается.

Более подробно описание работы подсистемы QoS см. в соответствующей главе данного Руководства.

Использование агрегирующих интерфейсов

Агрегирующие интерфейсы (группы агрегации каналов, или интерфейсы **bundle-ether**) представляют собой логические интерфейсы, каждый из которых состоит из нескольких физических. Полоса пропускания агрегирующего интерфейса равна сумме пропускных способностей составляющих его физических портов с учетом балансировки по этим портам.

При использовании агрегирующих интерфейсов следует уделять особое внимание вопросу балансировки трафика и контроля загрузки составляющих интерфейсов — только при достаточно равномерной балансировке трафика по составным портам можно получить максимально возможную пропускную способность. Возникновение же перегрузки на одном или нескольких интерфейсах-участниках агрегирующего соединения приведет к потерям трафика, хотя общая загрузка агрегирующего интерфейса может при этом не достигать максимума.

Группы агрегации также можно применять с целью организации резервирования каналов — при отказе одного из интерфейсов-участников (например, физическом обрыве соединения) трафик автоматически перераспределяется на оставшиеся активные порты.

Для создания агрегирующих интерфейсов можно применять два подхода — создание статических агрегаций либо агрегаций с использованием протокола LACP (Link Aggregation Control Protocol).

При организации интерфейсов с использованием LACP работоспособность составляющих соединений контролируется сигнальными средствами данного протокола. Агрегирующие интерфейсы с протоколом LACP рекомендуется применять в большинстве случаев, так как протокольные механизмы контроля целостности соединения гарантируют обнаружение обрывов даже в тех случаях, когда физические интерфейсы продолжают оставаться в активном состоянии.

Например, при организации стыка между двумя маршрутизаторами транспортом между ними может служить какая-либо первичная сеть, которая не отключит конечные порты тракта при его обрыве. Без использования сигнализации LACP в данном случае маршрутизаторы продолжают отсылать часть трафика в неисправный линк, что приведет к потере этого трафика.

Статические группы агрегации рекомендуется применять только при необходимости и в случаях, если соединяемые устройства соединены "спина к спине", то есть прямыми Ethernet-соединениями без участия какого-либо дополнительного транспорта. Однако даже в таком случае возможна ситуация, когда неисправность линии затронет только одно направление передачи трафика, и тогда одно из устройств не сможет обнаружить отказ и продолжит отсылать трафик в неработоспособный интерфейс.

При объединении устройств агрегирующими интерфейсами следует использовать одинаковый режим работы (статический либо LACP) с обеих сторон соединения.

Для каждого агрегирующего интерфейса можно выбрать метод балансировки трафика по составляющим портам — "hash" или "round-robin". Метод балансировки "hash" означает, что каждый отправляемый пакет будет отправляться в один из составляющих линков на основании хэш-функции от заголовков этого пакета. Данный метод позволяет направить все пакеты каждого отдельно взятого потока трафика (например, трафика между двумя определенными узлами) в один и тот же интерфейс-участник агрегации. Метод "round-robin" отправляет каждый последующий пакет в следующий по очереди составляющий линк (т.н. по пакетной балансировке), невзирая на его принадлежность к какому-либо потоку.

Метод "round-robin" позволяет максимально равномерно распределить трафик по участникам агрегирующего линка, однако, его побочным эффектом может являться переупорядочивание пакетов внутри потоков трафика — в случае, если составляющие соединения вносят разную задержку. В большинстве применений рекомендуется использовать метод балансировки "hash", предварительно сконфигурировав на устройстве метод учета полей для вычисления хэш-функции (команда **load-balancing hash-fields** глобального режима конфигурации).

Таким образом, на маршрутизаторах ME можно использовать следующие возможности настройки агрегации каналов:

1. Создавать агрегированные интерфейсы, включая в них физические порты;
2. Устанавливать метод работы агрегирующего интерфейса — статический либо с использованием LACP;
3. Выбирать режим работы LACP — "slow" или "fast";
4. Задавать режим балансировки трафика в агрегирующем интерфейсе — "hash" или "round-robin";
5. Настраивать максимальное и минимальное количество активных участников в агрегирующем интерфейсе;
6. Включать и настраивать на агрегирующем интерфейсе дополнительный метод быстрого детектирования обрыва линка — протокол MicroBFD.

Таблица 20. Последовательность создания и настройки агрегирующего интерфейса

| Команда | Назначение |
|---|---|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>lasp interface tengigabitethernet <i>num</i></code> | Добавление физического линка в агрегированный интерфейс и переход в режим настройки его параметров агрегации. |
| <code>bundle id <i>bundle_id</i></code> | Привязка физического интерфейса к указанному номеру агрегированного интерфейса системы. |
| <code>bundle mode { active passive off }</code> | Указание режима работы агрегации — LACP active, LACP passive либо статическая агрегация. Важно указывать одинаковый режим работы для всех участников одного и того же агрегированного интерфейса. |
| <code>timeout { short long }</code> | (Опционально) Выбор режима работы LACP — "slow" (long) или "fast" (short). |

| Команда | Назначение |
|--|--|
| <code>exit</code> | Возврат в режим глобальной конфигурации. Далее можно повторить перечисленные шаги, добавив требуемые интерфейсы в состав агрегированного соединения. |
| <code>lasp interface bundle-ether bundle_id</code> | Создание вспомогательного элемента — блока настройки параметров агрегации интерфейса bundle-ether и переход в режим настройки этих параметров. Команда является обязательной. |
| <code>active-links max max_links</code> | (Опционально) Указание максимально возможного количества активных участников агрегированного интерфейса. При наличии большего количества участников они будут переводиться в неактивное состояние. |
| <code>active-links min min_links</code> | (Опционально) Указание минимально требуемого количества активных участников агрегированного интерфейса. В случае, если количество активных участников опустится ниже данного значения, агрегированный интерфейс будет принудительно деактивирован. |
| <code>exit</code> | Возврат в режим глобальной конфигурации. |
| <code>interface bundle-ether bundle_id</code> | Создание в системе агрегированного интерфейса и переход в режим его настройки. |
| <code>ipv4 address ipv4address/prefix</code> | (Опционально) Задание IPv4-адреса на интерфейсе. |
| <code>commit</code> | Применение произведенных настроек. |

NOTE

Назначать физические интерфейсы в группу агрегации каналов можно либо после, либо одновременно с созданием в системе соответствующего интерфейса **bundle-ether**.

IMPORTANT

По умолчанию режим балансировки агрегированного интерфейса — "hash". Для обеспечения требуемой балансировки необходимо воспользоваться командой "**load-balancing hash-fields**" глобального режима конфигурации.

Полученный агрегированный интерфейс можно использовать в системе наравне с обычными физическими портами.

Пример: конфигурация агрегированного интерфейса, состоящего из двух физических:

```
load-balancing hash-fields mac-src
load-balancing hash-fields mac-dst
load-balancing hash-fields ip-src
load-balancing hash-fields ip-dst

lacp interface tengigabitethernet 0/0/8
  bundle id 1
  bundle mode active
exit
lacp interface tengigabitethernet 0/0/9
  bundle id 1
  bundle mode active
exit
lacp interface bundle-ether 1
  active-links min 2
exit

interface bundle-ether 1
  bfd address-family ipv4 source 11.11.11.1
  bfd address-family ipv4 destination 11.11.11.2
  bfd address-family ipv4 fast-detect
  bfd multiplier 3
  ipv4 address 11.11.11.1/24
exit
```

Использование сабинтерфейсов

Сабинтерфейсы (subinterfaces) представляют собой логические интерфейсы, являющиеся потомками физического интерфейса (либо группы агрегации каналов) и работающие с тегированным Ethernet-трафиком.

Например, на одном физическом интерфейсе можно создать три логических сабинтерфейса, первый из которых работает только с трафиком с инкапсуляцией 802.1q и помеченным тегом 100, второй - с тегом 300 и третий - с тегом 400. Под работой с трафиком в данном случае подразумевается прием соответствующего тегированного трафика и передача трафика с соответствующими тегами.

NOTE

Идентификатор сабинтерфейса (указывается через точку после номера родительского интерфейса) — число, уникальное в пределах родительского интерфейса. Идентификатор при этом может быть произвольным и не обязан соответствовать тегам, заданным для инкапсуляции. Тем не менее, для удобства рекомендуется использовать какую-либо систему соответствия между идентификаторам и используемыми тегами.

В качестве классификатора для инкапсуляции может использоваться один или два тега.

Классификатор инкапсуляции задается на сабинтерфейсе командой **encapsulation**.

IMPORTANT

Текущая версия ПО распознает в качестве VLAN-тегов только теги с TPID 0x8100.

Сабинтерфейсы могут полноценно использоваться в системе наравне с физическими и служить как для Layer3-маршрутизации, так и для Layer2-коммутации.

Сабинтерфейсы в режиме L3-маршрутизации

Сабинтерфейс, как и обычный физический интерфейс, может работать в режиме layer3 forwarding при назначении на него IPv4/IPv6-адресов.

При получении Ethernet-кадра в L3-сабинтерфейс все заголовки второго уровня, включая VLAN-теги, отбрасываются, и вложенный IP-пакет маршрутизируется согласно таблиц маршрутизации.

При передаче IP-пакета из L3-сабинтерфейса пакет инкапсулируется в Ethernet-кадр с автоматическим добавлением тех VLAN-тегов, которые заданы на сабинтерфейсе в качестве классификатора инкапсуляции.

Таблица 21. Последовательность создания и настройки L3-сабинтерфейса

| Команда | Назначение |
|---|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>interface { tengigabitethernet bundle-ether } num.subif_id</code> | Создание сабинтерфейса и переход в режим настройки его параметров. |
| <code>encapsulation outer-vid outer-vid [inner-vid inner-vid]</code> | Задание классификатора — инкапсуляции трафика на сабинтерфейсе. <i>outer-vid</i> — значение внешнего VLAN-тега. <i>inner-vid</i> — значение внутреннего VLAN-тега. |
| <code>ipv4 address ipv4address/prefix</code> | (Опционально) Задание IPv4-адреса на интерфейсе. |
| <code>ipv6 address ipv6address/prefix</code> | (Опционально) Задание IPv6-адреса на интерфейсе. |
| <code>commit</code> | Применение произведенных настроек. |

Пример L3-сабинтерфейса с одинарным VLAN-тегированием

```
interface tengigabitethernet 0/0/1.4036
  vrf example_vrf
  ipv4 address 10.10.36.1/24
  encapsulation outer-vid 4036
exit
```



```
interface tengigabitethernet 0/0/1.40000100
  vrf example_vrf
  ipv4 address 192.0.2.0/31
  encapsulation outer-vid 4000 inner-vid 100
exit
```

NOTE На L3-сабинтерфейсах игнорируется команда `rewrite ingress/egress tag`.

Сабинтерфейсы в режиме L2-коммутации

Сабинтерфейс также может работать в режиме layer2 forwarding, включаться в сервисы L2VPN (бридж-домены или кросс-коннекты) и служить для сквозной коммутации Ethernet-кадров.

При работе в режиме L2-коммутации есть важное отличие — при передаче кадров через сабинтерфейс маршрутизатор **не производит** никакой модификации VLAN-тегов. Таким образом, если требуется с принимаемых кадров снять теги, назначить на них дополнительные теги либо изменить теги, — то необходимо задать требуемое действие при помощи дополнительной команды `rewrite ingress/egress tag`.

Семейство команд `rewrite ingress/egress tag` позволяет выполнить с тегами следующие действия:

- **push** — добавить в Ethernet-кадр один или два VLAN-тега с заданным VLAN ID;
- **pop** — снять с кадра один или два VLAN-тега;
- **replace** — заменить внешний тег на заданный VLAN ID и (опционально) заменить также внутренний тег в кадре;
- **exchange** — поменять местами внешний и внутренний теги.

NOTE На одном сабинтерфейсе можно задать только одно правило '`rewrite ingress tag`' и одно правило '`rewrite egress tag`'.

Таблица 22. Последовательность создания и настройки L2-сабинтерфейса

| Команда | Назначение |
|---|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>interface { tengigabitethernet bundle-ether } num.subif_id</code> | Создание сабинтерфейса и переход в режим настройки его параметров. |
| <code>encapsulation outer-vid outer-vid [inner-vid inner-vid]</code> | Задание классификатора — инкапсуляции трафика на сабинтерфейсе. <i>outer-vid</i> — значение внешнего VLAN-тега. <i>inner-vid</i> — значение внутреннего VLAN-тега. |
| <code>commit</code> | Применение произведенных настроек. |

Таблица 23. Настройка правил '`rewrite egress tag`' на L2-сабинтерфейсе

| Команда | Назначение |
|--|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>interface { tengigabitethernet bundle-ether } num.subif_id</code> | Создание сабинтерфейса и переход в режим настройки его параметров. |
| <code>rewrite egress tag pop {one two}</code> | Снять один или два тега с передаваемого Ethernet-кадра. |
| <code>rewrite egress tag push outer-vid outer-vid [inner-vid inner-vid]</code> | Добавить один или два тега на передаваемый Ethernet-кадр. |
| <code>rewrite egress tag replace outer-vid outer-vid [inner-vid inner-vid]</code> | Заменить один (верхний) или два тега на передаваемом Ethernet-кадре. |
| <code>rewrite egress tag exchange</code> | Поменять местами внешний и внутренний теги на передаваемом Ethernet-кадре. |
| <code>commit</code> | Применение произведенных настроек. |

Таблица 24. Настройка правил 'rewrite ingress tag' на L2-сабинтерфейсе

| Команда | Назначение |
|---|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>interface { tengigabitethernet bundle-ether } num.subif_id</code> | Создание сабинтерфейса и переход в режим настройки его параметров. |
| <code>rewrite ingress tag pop {one two}</code> | Снять один или два тега с принятого Ethernet-кадра. |
| <code>rewrite ingress tag push outer-vid outer-vid [inner-vid inner-vid]</code> | Добавить один или два тега на принятый Ethernet-кадр. |
| <code>rewrite ingress tag replace outer-vid outer-vid [inner-vid inner-vid]</code> | Заменить один (верхний) или два тега на принятом Ethernet-кадре. |
| <code>rewrite ingress tag exchange</code> | Поменять местами внешний и внутренний теги на принятом Ethernet-кадре. |
| <code>commit</code> | Применение произведенных настроек. |

Утилизация сабинтерфейсов

Как на физических и агрегирующих интерфейсах, на сабинтерфейсах ведется статистика переданных и принятых пакетов. Также имеется возможность подсчета текущей загрузки интерфейса в битах в секунду. Подсчет загрузки для сабинтерфейсов включается глобальной командой `system subint-utilization`.

Таблица 25. Включение подсчета загрузки сабинтерфейсов

| Команда | Назначение |
|---|---|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>[no] system subint-utilization</code> | Включение подсчета загрузки для всех сабинтерфейсов системы. Отрицательная форма команды отключает подсчет. По умолчанию подсчет загрузки на сабинтерфейсах выключен. |
| <code>commit</code> | Применение произведенных настроек. |

Команды диагностики интерфейсов

Ниже перечислены show-команды, посредством которых можно получить различную диагностическую информацию об интерфейсах системы.

show interfaces

Команда, при указании имени и номера интерфейса, выводит детализированную информацию о состоянии интерфейса и статистику интерфейса. Без указания конкретного интерфейса выводится информация по всем интерфейсам системы.

Пример: show interfaces

```
0/ME5100:Router# show interfaces tengigabitethernet 0/0/5
Tue Feb  6 20:45:47 2018
tengigabitethernet 0/0/5 is up
  Interface index is 6
  Hardware is tengigabitethernet, address is a8:f9:4b:8b:bb:25
  Link is up for 9 hours, 1 minutes, 46 seconds
  Description: to AR1(1.1.1.1) te 0/0/5
  IPv4 address is 100.100.12.1/31
  No IPv6 address assigned
  Interface is bound to VRF default
  Interface is in layer3 forwarding mode
  ARP aging time is 240 minutes
  Interface MTU is 9192
  Interface IP MTU is 1500
  Full, 10G, link type is auto, media type is 10G-Fiber
  Flow control is rx
  300 seconds input rate is 6120 bit/s
  300 seconds output rate is 6200 bit/s
  300 seconds input unicast rate is 10 pps
  300 seconds output unicast rate is 10 pps
  300 seconds input multicast rate is 0 pps
  300 seconds output multicast rate is 0 pps
  300 seconds input broadcast rate is 0 pps
  300 seconds output broadcast rate is 0 pps
    346192 packets input, 24913496 bytes received
    6 broadcasts, 14268 multicasts
    0 input errors, 0 FCS
    0 oversize, 0 internal MAC
  350273 packets output, 25201238 bytes sent
    1 broadcasts, 14269 multicasts
    0 output errors, 0 collisions
    0 excessive collisions, 0 late collisions
    0 symbol errors, 0 carrier, 0 SQE test error
```

show ipv4 interfaces brief

Команда выводит в табличном виде информацию обо всех L3-интерфейсах системы с указанием их IPv4-адресов и VRF, к которым они отнесены.

Пример: *show ipv4 interfaces brief*

```
0/ME5100:Router# show ipv4 interfaces brief
Tue Feb  6 20:47:35 2018
Interface                IPv4 address            VRF
-----
te 0/0/5                  100.100.12.1/31        default
te 0/0/6                  100.100.24.1/31        default
te 0/0/7                  100.100.23.1/31        default
te 0/0/17.10004000        4.4.4.4/24             l3-1
te 0/0/17.10004001        1.1.1.1/24             l3-1
te 0/0/17.20004000        172.16.0.0/31          l3-1
lo 1                      2.2.2.2/32             default
lo 7991                   3.1.3.1/32             l3-1
mgmt 0/fmc0/1            172.17.0.32/24         mgmt-intf
```

show interfaces description

Команда выводит в табличном виде перечень интерфейсов с указанием их описаний (description), сконфигурованных пользователем.

show interfaces counters

Команда выводит в табличном виде перечень интерфейсов и статистику по счетчикам пакетов на них.

show interfaces status

Команда выводит в табличном виде перечень физических и агрегирующих интерфейсов и информацию о их текущих состояниях и режиме работы.

show interfaces summary

Команда выводит сводную таблицу по количеству интерфейсов/сабинтерфейсов системы и их состоянию.

Пример: *show interfaces summary*

```
0/ME5100:Router# show interfaces summary
```

```
Tue Feb 6 20:52:34 2018
```

| Interface type | Total | Up | Down | Admin down |
|------------------------|-------|----|------|------------|
| tengigabitethernet | 20 | 2 | 18 | 0 |
| tengigabitethernet-sub | 22 | 21 | 1 | 0 |
| bundle-ether | 2 | 0 | 2 | 0 |
| loopback | 1 | 1 | 0 | 0 |
| mgmt | 1 | 0 | 1 | 0 |
| ALL | 46 | 24 | 22 | 0 |

show interfaces utilization

Команда выводит в табличном виде информацию о текущей загрузке физических и агрегирующих интерфейсов.

ПОСТОЯННЫЕ МАРШРУТЫ И СТАТИЧЕСКАЯ МАРШРУТИЗАЦИЯ

В этой главе дается понятие постоянных маршрутов, описаны методы их диагностики и настройка статической маршрутизации для глобальной таблицы (GRT) и экземпляров VRF.

NOTE Основное средство диагностики таблиц маршрутизации устройства — команда `show route`.

Типы постоянных маршрутов

Постоянные маршруты — это маршруты, не зависящие от работы протоколов динамической маршрутизации и существующие в системе как результат ручной настройки.

В системе имеется три типа таких маршрутов:

- присоединенные (connected);
- локальные (local);
- статические (static).

Присоединенные маршруты

Присоединенные (connected) маршруты — это маршруты, соответствующие назначенным на IP-интерфейсы подсетям. Параметры присоединенного маршрута — это непосредственно адрес сети и интерфейс, на котором назначена данная подсеть.

Например, при назначении на интерфейсе IPv4-адреса `100.64.0.1/24` в таблицу маршрутизации будет внесено, что активен маршрут `100.64.0.0/24`, присоединенный к соответствующему интерфейсу устройства.

Присоединенные маршруты появляются в таблице маршрутизации и используются для пересылки трафика только в том случае, если соответствующий интерфейс находится в активном состоянии.

Локальные маршруты

Локальные (local) маршруты — это максимально специфичные (/32 для IPv4) маршруты, соответствующие назначенным на IP-интерфейсы устройства адресам. Параметры локального маршрута — это адрес интерфейса с маской /32 и непосредственно сам интерфейс, на котором адрес назначен.

Например, при назначении на интерфейсе IPv4-адреса `100.64.0.1/24` в таблицу маршрутизации будет внесено, что активен маршрут `100.64.0.1/32`, локальный для соответствующего интерфейса устройства.

Локальные маршруты появляются в таблице маршрутизации только в том случае, если соответствующий интерфейс находится в активном состоянии. Локальные маршруты используются в системе для внутренних нужд.

CAUTION

Следует с осторожностью применять редистрибуцию локальных маршрутов в протоколы динамической маршрутизации, так как появление таких специфичных маршрутов может привести к неочевидному выбору лучших путей в сети.

IMPORTANT

В случае, если на интерфейс назначен адрес с маской /32 (например, при использовании интерфейсов локальной петли — loopback), соответствующий маршрут будет рассматриваться системой как локальный, а не как присоединенный. Данную особенность следует учитывать при редистрибуции адресов loopback-интерфейсов.

Просмотр присоединенных и локальных маршрутов

Вывод всех имеющихся присоединенных маршрутов производится командой `show route [vrf NAME] connected`.

Вывод всех имеющихся локальных маршрутов производится командой `show route [vrf NAME] local`.

Предположим, в системе настроен IPv4-интерфейс:

```
interface tengigabitethernet 0/0/5
  load-interval 30
  description "to AR2(2.2.2.2) te 0/0/5"
  ipv4 address 100.100.12.0/31
exit
```

Тогда в таблице маршрутизации будут присутствовать следующие присоединенные (код **C**) и локальные (код **L**) маршруты:

```
C    100.100.12.0/31    is directly connected, 12h50m46s, te 0/0/5
L    100.100.12.0/32    is directly connected, 12h50m46s, te 0/0/5
```

Статические маршруты

Статические маршруты создаются в системе вручную путем задания соответствующих команд конфигурации. При создании статических маршрутов имеются обязательные и опциональные параметры.

Обязательные параметры:

- Сеть или префикс назначения в формате CIDR;
- IP-адрес следующего узла (*nexthop*).

Опциональные параметры:

- Интерфейс, через который направляется статический маршрут;
- Включение/отключение быстрого детектирования обрыва BFD;
- Метрика маршрута;
- Внутренний числовой тэг маршрута.

Настройка статических маршрутов внутри глобальной таблицы маршрутизации (GRT)

Добавление статических маршрутов в глобальной таблице производится в иерархическом виде в разделе конфигурации `router static`.

Таблица 26. Настройка статических маршрутов в GRT

| Команда | Назначение |
|---|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>router static</code> | Переход в режим конфигурации статической маршрутизации в глобальной таблице. |
| <code>address-family { ipv4 ipv6 } unicast</code> | Переход в режим настройки IP unicast-маршрутов. |
| <code>destination ip_network ip_nexthop</code> | Создание статического маршрута на подсеть <i>ip_network</i> с адресом следующего узла <i>ip_nexthop</i> и переход в режим конфигурации опциональных параметров данного маршрута. |
| <code>interface { null tengigabitethernet bundle-ether } num</code> | (Опционально) Указание интерфейса, через который будет направлен маршрут и переход в режим настройки дальнейших опциональных параметров. |
| <code>bfd fast-detect</code> | (Опционально) Включение быстрого детектирования обрыва связи до следующего узла (<i>nexthop</i>). |
| <code>metric</code> | (Опционально) Установка метрики маршрута. |
| <code>exit</code> | (Опционально) Возврат в режим настройки опциональных параметров маршрута. |
| <code>tag tag</code> | (Опционально) Указание внутреннего числового тега, который может быть впоследствии использован при фильтрации маршрута правилами редистрибуции. |
| <code>commit</code> | Применение произведенных настроек. |

Пример: настройка статического маршрута на сеть 100.70.0.0/16 через узел 4.4.4.4, интерфейс bundle-ether 1.21, с метрикой 15 и внутренним тегом 555:

```
router static
  address-family ipv4 unicast
    destination 100.70.0.0/16 4.4.4.4
    interface bundle-ether 1.21
    metric 15
  exit
  tag 555
exit
exit
exit
```

Настройка статических маршрутов внутри экземпляра VRF

Добавление статических маршрутов для экземпляра VRF производится в иерархическом виде в разделе конфигурации `router vrf`.

IMPORTANT

Для включения IP-маршрутизации в экземпляре VRF **необходимо** наличие в конфигурации как минимум пустого блока `router vrf VRF_NAME` для данного экземпляра.

Таблица 27. Настройка статических маршрутов внутри экземпляра VRF

| Команда | Назначение |
|---|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>router vrf vrf_name</code> | Включение маршрутизации в указанном экземпляре VRF и переход в режим настройки основных параметров маршрутизации для него. |
| <code>static</code> | Переход в режим конфигурации статической маршрутизации в текущем экземпляре VRF. |
| <code>address-family { ipv4 ipv6 } unicast</code> | Переход в режим настройки IP unicast-маршрутов. |
| <code>destination ip_network ip_nexthop</code> | Создание статического маршрута на подсеть <code>ip_network</code> с адресом следующего узла <code>ip_nexthop</code> и переход в режим конфигурации опциональных параметров данного маршрута. |
| <code>interface { null tengigabitethernet bundle-ether } num</code> | (Опционально) Указание интерфейса, через который будет направлен маршрут и переход в режим настройки дальнейших опциональных параметров. |
| <code>bfd fast-detect</code> | (Опционально) Включение быстрого детектирования обрыва связи до следующего узла (nexthop). |
| <code>metric</code> | (Опционально) Установка метрики маршрута. |
| <code>exit</code> | (Опционально) Возврат в режим настройки опциональных параметров маршрута. |

| Команда | Назначение |
|----------------------|---|
| <code>tag tag</code> | (Опционально) Указание внутреннего числового тега, который может быть впоследствии использован при фильтрации маршрута правилами редистрибуции. |
| <code>commit</code> | Применение произведенных настроек. |

Пример: настройка статического маршрута внутри VRF "example_vrf" на сеть 10.0.0.0/23 через узел 4.4.4.4, интерфейс tengigabitethernet 0/0/18.1, с метрикой 15 и внутренним тегом 65001:

```
router vrf example_vrf
  static
    address-family ipv4 unicast
      destination 10.0.0.0/23 4.4.4.4
        interface tengigabitethernet 0/0/18.1
          metric 15
        exit
      tag 65001
    exit
  exit
exit
exit
```

Команды просмотра маршрутной информации

show route [vrf VRF] [connected | static | local]

Данная команда выводит полный список маршрутов устройства в глобальной таблице маршрутизации либо в указанном экземпляре VRF. При указании типа маршрутов (connected/static/local) вывод фильтруется в соответствии с заданным параметром.

Пример: вывод команды `show route`

```
0/ME5100:Router# show route
Wed Feb  7 00:20:01 2018
Codes: C - connected, S - static, O - OSPF, B - BGP, L - local
       IA - OSPF inter area, EA - OSPF intra area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       LE1 - ISIS level1 external, LE2 - ISIS level2 external
       BI - BGP internal, BE - BGP external, BV - BGP vpn

L      1.1.1.1/32      is directly connected, 13h41m48s, lo 1
i L2   2.2.2.2/32      via 100.100.12.1 [116/10], 13h39m57s, te 0/0/5
i L2   3.3.3.3/32      via 100.100.13.0 [116/10], 13h41m22s, te 0/0/6
i L2   4.4.4.4/32      via 100.100.14.0 [116/10], 13h38m03s, te 0/0/7.14
i L2   5.5.5.5/32      via 100.100.13.0 [116/30], 13h41m09s, te 0/0/6
i L2   6.6.6.6/32      via 100.100.13.0 [116/20], 13h41m09s, te 0/0/6
i L2   9.9.9.9/32      via 100.100.13.0 [116/10], 13h41m22s, te 0/0/6
C      10.10.0.0/24     is directly connected, 13h41m30s, te 0/0/1.10
L      10.10.0.1/32     is directly connected, 13h41m30s, te 0/0/1.10
C      10.100.100.0/24  is directly connected, 13h41m30s, te 0/0/1.100
L      10.100.100.1/32  is directly connected, 13h41m30s, te 0/0/1.100
C      11.1.0.0/24     is directly connected, 13h41m30s, te 0/0/1.11
L      11.1.0.1/32     is directly connected, 13h41m30s, te 0/0/1.11
B BI   20.20.0.0/32     via 100.100.12.1 [200/0], 13h38m05s, te 0/0/5
B BI   22.11.0.0/24    via 100.100.12.1 [200/0], 13h38m05s, te 0/0/5
B BI   22.21.21.0/24   via 100.100.12.1 [200/0], 13h38m05s, te 0/0/5
<..>
```

NOTE

При наличии в системе большого количества маршрутов вывод полной таблицы может занимать значительное время.

show route [vrf VRF] { ipv4 | ipv6 } PREFIX

Данная команда выводит детальную информацию по конкретному префиксу в таблице маршрутизации.

Пример: вывод команды `show route ipv4 PREFIX`

```
0/ME5100:Router# show route ipv4 6.6.6.6/32
Wed Feb 7 00:24:31 2018
Routing entry for 6.6.6.6/32
  Last update: 13h45m39s
  Routing Descriptor Blocks
    100.100.13.0, via te 0/0/6
    Known via isis, distance 116, metric 20
    type isis-level2-internal, protection none, route-type remote

Entries: 1
```

IMPORTANT

В качестве аргумента команда `show route { ipv4 | ipv6 }` принимает только точный маршрут в формате CIDR, имеющийся в таблице маршрутизации. Для выполнения поиска маршрута для какого-либо IP-адреса (т.н. процесс точного поиска маршрута) следует воспользоваться командой `show l3forwarding`.

show route rib summary [detailed]

Команда выводит сводную информацию о количестве маршрутов в системе с указанием их типов/источников.

Пример: вывод команды `'show route rib summary'`:

```
0/ME5100:Router# show route rib summary
Wed Feb 7 00:27:47 2018

Route Source      Routes
-----
static            2
connected         8
local             9
ospf              0
isis              25
bgp               12
lfa               0
summary address  0
default           0
FIB installed     49
```

НАСТРОЙКА ПРОТОКОЛА OSPF

В данной главе описаны принципы настройки протокола динамической маршрутизации OSPFv2 (Open Shortest Path First, version 2).

Данный протокол принадлежит к семейству протоколов состояния соединения и относится к группе IGP (Interior Gateway Protocol).

Принципы конфигурирования протокола OSPFv2

Настройка процесса динамической маршрутизации OSPF производится в разделе конфигурации `router ospfv2`. На устройстве возможно создать только один процесс маршрутизации OSPFv2 (однако для него необходимо задать уникальное имя). Внутри данного конфигурационного блока настраивается OSPFv2 как для глобальной таблицы, так и для имеющихся на маршрутизаторе экземпляров VRF.

Дальнейшая конфигурация также производится иерархически. Внутри таблицы маршрутизации конфигурируются OSPF-зоны (area), в которые уже назначаются логические и физические интерфейсы устройства.

IMPORTANT

По умолчанию ни один из интерфейсов устройства не включен в протокол OSPF. Для запуска протокола OSPF на интерфейсе и/или сабинтерфейсе требуется явно указать этот интерфейс в конфигурации соответствующей зоны внутри процесса OSPFv2.

IMPORTANT

На интерфейсе, сконфигурированном внутри какой-либо зоны OSPF, запускается механизм протокольного обнаружения OSPF — начинается отправка HELLO-пакетов и прием таких пакетов. Исключение составляют т.н. "пассивные" интерфейсы — такие интерфейсы только включаются в состав объявлений OSPF Router links при рассылке протокольных сообщений, соседства через такие интерфейсы не устанавливаются.

Таким образом, последовательность конфигурирования протокола OSPF выглядит следующим образом:

1. Создание процесса маршрутизации.
2. Общая настройка протокола OSPF на устройстве.
3. Создание требуемых OSPF-зон внутри блока процесса маршрутизации и настройка этих зон.
4. Добавление интерфейсов в соответствующие OSPF-зоны.

Базовая настройка протокола OSPFv2

Настройка протокола производится согласно описанной выше иерархии.

Таблица 28. Базовая настройка протокола OSPFv2

| Команда | Назначение |
|---|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>router ospfv2 OSPF_NAME</code> | Создание процесса маршрутизации OSPFv2 с именем <i>OSPF_NAME</i> и переход в режим его настройки. |
| <code>router-id X.X.X.X</code> | Задание идентификатора узла сети (Router ID) в формате IPv4-адреса. |
| <code>area Y.Y.Y.Y</code> | Создание в конфигурации OSPF-зоны (area) и переход в режим её настройки. Допускается использование только dotted-нотации. Backbone-зоной является зона с номером 0.0.0.0 . |
| <code>nssa</code> | (Опционально) Указание текущей зоны в качестве OSPF NSSA ('not-so-stubby area'). |
| <code>stub</code> | (Опционально) Указание текущей зоны в качестве OSPF Stub area. |
| <code>interface { loopback tengigabitethernet bundle-ether } num</code> | Добавление соответствующего интерфейса (либо сабинтерфейса) в указанную зону OSPF и переход в режим настройки OSPF-параметров этого интерфейса. |
| <code>dead-interval { minimal SECONDS }</code> | (Опционально) Установка временного интервала — таймаута получения HELLO-пакетов от соседа, по истечении которого сосед на данном интерфейсе будет считаться потерянным. Указание параметра minimal включает режим OSPF fast hello. |
| <code>hello-interval SECONDS</code> | (Опционально) Установка интервала отправки HELLO-пакетов на текущем интерфейсе, в секундах. |
| <code>fast-hello-multiplier PACKETS</code> | (Опционально) Установка количества HELLO-пакетов, которые будут отправляться с интерфейса за секунду при работе в режиме OSPF fast hello. Принимает значения 2..20. |
| <code>metric METRIC</code> | (Опционально) Устанавливает протокольную "стоимость" (иначе — метрику) интерфейса. Принимает значения 0..65535. ВАЖНО: В текущей версии ПО все интерфейсы устройства по умолчанию имеют метрику 10. Назначение метрик на интерфейсы следует производить в соответствии с принятой на сети политикой IGP-маршрутизации. |
| <code>mtu-ignore</code> | (Опционально) С данным параметром при установлении соседств через интерфейс будет игнорироваться информация о размере MTU в объявлениях соседних маршрутизаторов. Команду следует использовать при невозможности выполнения согласованной настройки MTU на соседних маршрутизаторах. |

| Команда | Назначение |
|---|--|
| <pre>network { broadcast nbma point-to-multipoint point-to- point }</pre> | <p>(Опционально) Указание типа OSPF-подсети на интерфейсе.</p> <p>При использовании типа point-to-multipoint устройство может работать только в пассивном non-broadcast режиме — то есть устанавливать соседство по факту получения unicast HELLO-сообщений от соседей. Возможность инициации соединений к сконфигурированным соседям будет доступна в будущих релизах ПО.</p> |
| <pre>passive</pre> | <p>(Опционально) Перевод интерфейса в пассивный режим.</p> <p>В данном режиме интерфейс не отправляет и не принимает HELLO-сообщений и через интерфейс не устанавливается никаких соседств. Режим используется при необходимости анонсировать в OSPF подсеть данного интерфейса (например, для интерфейсов локальной петли loopback).</p> |
| <pre>priority ROUTER_PRIORITY</pre> | <p>(Опционально) Установка приоритета маршрутизатора для участия в выборах Designated router. Принимает значения 0..255.</p> |
| <pre>exit</pre> | <p>Возврат в режим настройки OSPF-зоны.</p> |
| <pre>exit</pre> | <p>Возврат в режим настройки OSPF-процесса.</p> |
| <pre>exit</pre> | <p>Возврат в режим глобальной конфигурации.</p> |
| <pre>commit</pre> | <p>Применение произведенных настроек.</p> |

```
router ospfv2 test
  router-id 1.1.1.1
  area 0.0.0.0
    interface tengigabitethernet 0/0/12
      network point-to-point
    exit
    interface tengigabitethernet 0/0/13
      network point-to-point
      metric 20
    exit
    interface loopback 1
      passive
    exit
  exit
  area 0.0.0.100
    stub
    interface bundle-ether 7.400
      network point-to-point
      metric 250
    exit
  exit
exit
```

Настройка OSPF для экземпляра VRF

Для запуска процесса маршрутизации OSPF внутри какого-либо экземпляра VRF необходимо сконфигурировать соответствующий блок `vrf <NAME>` внутри заранее созданного процесса маршрутизации `router ospfv2`. Процесс дальнейшей настройки OSPF внутри VRF идентичен таковому для глобальной таблицы маршрутизации.

NOTE

Процессы маршрутизации для разных VRF работают независимо друг от друга.

Таблица 29. Настройка протокола OSPFv2 для экземпляра VRF

| Команда | Назначение |
|--------------------------------------|---|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>router ospfv2 OSPF_NAME</code> | Создание процесса маршрутизации OSPFv2 с именем <code>OSPF_NAME</code> и переход в режим его настройки. |
| <code>vrf VRF_NAME</code> | Запуск процесса маршрутизации OSPFv2 в указанном VRF и переход в режим настройки этого процесса. |
| <code>router-id X.X.X.X</code> | Задание идентификатора узла сети (Router ID) в формате IPv4-адреса. |

| Команда | Назначение |
|--|--|
| <code>area Y.Y.Y.Y</code> | Создание в конфигурации OSPF-зоны (area) и переход в режим её настройки. Допускается использование только dotted-нотации. Backbone-зоной является зона с номером <code>0.0.0.0</code> . |
| <code>nssa</code> | (Опционально) Указание текущей зоны в качестве OSPF NSSA ('not-so-stubby area'). |
| <code>stub</code> | (Опционально) Указание текущей зоны в качестве OSPF Stub area. |
| <code>interface { loopback tengigabitethernet bundle-ether } num</code> | Добавление соответствующего интерфейса (либо сабинтерфейса) в указанную зону OSPF и переход в режим настройки OSPF-параметров этого интерфейса. |
| <code>dead-interval { minimal SECONDS }</code> | (Опционально) Установка временного интервала — таймаута получения HELLO-пакетов от соседа, по истечении которого сосед на данном интерфейсе будет считаться потерянным. Указание параметра <code>minimal</code> включает режим OSPF fast hello. |
| <code>hello-interval SECONDS</code> | (Опционально) Установка интервала отправки HELLO-пакетов на текущем интерфейсе, в секундах. |
| <code>fast-hello-multiplier PACKETS</code> | (Опционально) Установка количества HELLO-пакетов, которые будут отправляться с интерфейса за секунду при работе в режиме OSPF fast hello. Принимает значения 2..20. |
| <code>metric METRIC</code> | (Опционально) Устанавливает протокольную "стоимость" (иначе — метрику) интерфейса. Принимает значения 0..65535. ВАЖНО: В текущей версии ПО все интерфейсы устройства по умолчанию имеют метрику 10. Назначение метрик на интерфейсы следует производить в соответствии с принятой на сети политикой IGP-маршрутизации. |
| <code>mtu-ignore</code> | (Опционально) С данным параметром при установлении соседств через интерфейс будет игнорироваться информация о размере MTU в объявлениях соседних маршрутизаторов. Команду следует использовать при невозможности выполнения согласованной настройки MTU на соседних маршрутизаторах. |
| <code>network { broadcast nbma point-to-multipoint point-to-point }</code> | (Опционально) Указание типа OSPF-подсети на интерфейсе. |

| Команда | Назначение |
|---------------------------------------|--|
| <code>passive</code> | (Опционально) Перевод интерфейса в пассивный режим. В данном режиме интерфейс не отправляет и не принимает HELLO-сообщений и через интерфейс не устанавливается никаких соседств. Режим используется при необходимости анонсировать в OSPF подсеть данного интерфейса (например, для интерфейсов локальной петли <code>loopback</code>). |
| <code>priority ROUTER_PRIORITY</code> | (Опционально) Установка приоритета маршрутизатора для участия в выборах Designated router. Принимает значения 0..255. |
| <code>exit</code> | Возврат в режим настройки OSPF-зоны. |
| <code>exit</code> | Возврат в режим настройки OSPF-процесса внутри VRF. |
| <code>exit</code> | Возврат в режим настройки OSPF-процесса. |
| <code>exit</code> | Возврат в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

Пример. Настройка OSPFv2 для экземпляра VRF.

```
router ospfv2 test
  vrf EXAMPLE
    area 0.0.0.0
      interface tengigabitethernet 0/0/2
        mtu-ignore
        network point-to-point
      exit
      interface tengigabitethernet 0/0/3
        network point-to-point
        metric 20
      exit
      interface loopback 100
        passive
      exit
    exit
    area 0.0.0.100
      stub
      interface bundle-ether 6.400
        network point-to-point
        metric 250
      exit
    exit
  exit
exit
```

IMPORTANT

Соответствующий экземпляр VRF должен быть заранее создан в конфигурации маршрутизатора.

Работа с протоколом BFD

Протокол BFD (Bidirectional forwarding detection) служит для быстрого обнаружения отказов соединений между двумя и более соседними устройствами.

Маршрутизаторы семейства ME имеют аппаратную поддержку BFD, что позволяет максимально быстро обнаруживать обрывы соединений и производить переключение трафика на резервные маршруты.

Включение протокола BFD производится путём выполнения команды `bfd fast-detect` на соответствующем интерфейсе в конфигурационном блоке протокола OSPFv2. При этом маршрутизатор будет пытаться установить BFD-сессии с IP-адресами всех соседей, которых протокол OSPF обнаружит на интерфейсе. В случае успешного установления таких соседств статус OSPF-сессии свяжется со статусом соответствующей BFD-сессии.

Таблица 30. Настройка протокола BFD для OSPF-соседств

| Команда | Назначение |
|--|---|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>router ospfv2 OSPF_NAME</code> | Создание процесса маршрутизации OSPFv2 с именем <code>OSPF_NAME</code> и переход в режим его настройки. |
| <code>area Y.Y.Y.Y</code> | Создание в конфигурации OSPF-зоны (area) и переход в режим её настройки. |
| <code>interface { tengigabitethernet bundle-ether } num</code> | Переход в режим настройки OSPF-параметров соответствующего интерфейса. |
| <code>bfd fast-detect</code> | Включение механизма установления BFD-сессий для всех протокольных OSPF-соседей на данном интерфейсе. |
| <code>root</code> | Возврат в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

Пример. Настройка протокола BFD для OSPF-интерфейса.

```
router ospfv2 test
  router-id 1.1.1.1
  area 0.0.0.0
    interface tengigabitethernet 0/0/5
      bfd fast-detect
    exit
  exit
exit
```

Редистрибуция маршрутной информации

Механизм редистрибуции позволяет передать в OSPF маршруты из других протоколов (протоколов IGP/EIGP, статических маршрутов и т.п.).

По умолчанию маршруты, переданные в OSPF при помощи механизма редистрибуции,

имеют тип OSPF External.

Редистрибуция настраивается путём создания набора именованных правил, при помощи которых можно фильтровать маршруты, подлежащие редистрибуции, а также назначать на маршруты параметры, специфичные для OSPF. Для каждого из источников (bgp/connected/local и т.п.) можно создать несколько правил, назначив им приоритет командой `priority` — данные правила будут применяться к маршруту по очереди до первого вхождения. Правила редистрибуции имеют по умолчанию действие "разрешить" — таким образом, пустое правило автоматически производит редистрибуцию всех маршрутов из указанного источника.

Источники редистрибуции:

1. **bgp** — маршрутная таблица протокола BGP;
2. **connected** — маршруты, соответствующие подсетям, назначенным на IP-интерфейсы маршрутизатора в данном VRF (либо GRT);
3. **isis** — маршрутная таблица протокола IS-IS;
4. **local** — маршруты, являющиеся спецификами /32 для адресов, назначенных на IP-интерфейсы маршрутизатора.
5. **static** — статические маршруты.

Таблица 31. Настройка редистрибуции в OSPF маршрутной информации из других протоколов.

| Команда | Назначение |
|---|---|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>router ospfv2 OSPF_NAME</code> | Создание процесса маршрутизации OSPFv2 с именем <i>OSPF_NAME</i> и переход в режим его настройки. |
| <code>redistribution { bgp connected isis local static } RULE_NAME</code> | Создание правила редистрибуции с именем <i>RULE_NAME</i> из указанного источника (bgp/connected/isis/local/static) и переход в режим настройки этого правила. |
| <code>match prefix IPv4PREFIX/MASK</code> | Указание фильтра, используемого для данного правила. При указании такого фильтра правило будет действовать только на маршруты, строго совпадающие с заданным <i>IPv4PREFIX/MASK</i> . |
| <code>metric-type { ospf-type1-external ospf-type2-external }</code> | Назначить на маршруты, прошедшие через данное правило, метрику типа "OSPF External 1" либо "OSPF External 2". |
| <code>metric-value METRIC</code> | Установить значение OSPF-метрики для маршрутов, прошедших через данное правило. |
| <code>priority RULE_PRIORITY</code> | Установить приоритет данного правила редистрибуции. Правила редистрибуции выполняются по очереди от низкого значения приоритета к высокому и срабатывают по первому вхождению. Таким образом, маршрут, попавший, например, в первое правило, будет передан в OSPF согласно настроек этого правила и не будет обрабатываться последующими правилами. |

| Команда | Назначение |
|-----------------------------------|--|
| <code>redistribute disable</code> | Запретить редистрибуцию маршрутов, попавших в текущее правило. При выполнении данной команды текущее правило становится запрещающим. |
| <code>exit</code> | Выход из режима настройки правила редистрибуции. Далее можно настроить следующие правила — для того же самого источника, либо для других источников редистрибуции. |
| <code>root</code> | Выход в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

Пример. Настройка процесса OSPF с двумя правилами редистрибуции connected-маршрутов.

```

router ospfv2 test
  router-id 1.1.1.1
  area 0.0.0.0
    interface tengigabitethernet 0/0/5
      bfd fast-detect
    exit
    interface tengigabitethernet 0/0/7
      bfd fast-detect
    exit
    interface loopback 1
      passive
    exit
  exit
  redistribution connected CONNECT-OSPF
    priority 10
    redistribute disable
    match prefix 100.65.0.0/24
  exit
  redistribution connected CONNECT-OSPF-20
    priority 20
    metric-value 300
    metric-type ospf-type1-external
  exit
exit

```

Аутентификация OSPF

Маршрутизаторы семейства ME позволяют использовать аутентификацию OSPF-соседства.

Аутентификация настраивается поинтерфейсно, для её работы необходимо указать требуемый тип командой `'authentication-type'` и задать ключ командой `'authentication-key'`.

Таблица 32. Настройка аутентификации OSPFv2

| Команда | Назначение |
|---|---|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>router ospfv2 OSPF_NAME</code> | Переход в режим настройки процесса маршрутизации. |
| <code>area Y.Y.Y</code> | Переход в режим настройки зоны OSPF. |
| <code>interface { tengigabitethernet bundle-ether } num</code> | Переход в режим настройки параметров OSPF требуемого интерфейса. |
| <code>authentication-type { hmacsha1 hmacsha256 hmacsha384 hmacsha512 md5 none simple-password }</code> | Выбор типа OSPF-аутентификации на интерфейсе — HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512, MD5 либо простой пароль (simple-password). Задание параметра 'none' отключает аутентификацию на интерфейсе, что соответствует поведению по умолчанию. |
| <code>authentication-key { KEY_STRING encrypted KEY_ENCRYPT }</code> | Задание ключа для аутентификации в открытом (KEY_STRING) либо в зашифрованном (KEY_ENCRYPT) виде. |
| <code>exit</code> | Выход из режима интерфейсных параметров OSPF. Далее можно настроить параметры аутентификации на других требуемых интерфейсах. |
| <code>root</code> | Выход в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

Пример. Настройка OSPF-аутентификации в режиме MD5 на интерфейсе.

```
router ospfv2 test
  area 0.0.0.0
    interface tengigabitethernet 0/0/5
      authentication-key encrypted B98C224080236D
      authentication-type md5
    exit
  exit
exit
```

NOTE

Все вводимые в открытом виде ключи автоматически шифруются в текущей конфигурации и отображаются в виде `encrypted KEY_ENCRYPT`.
Ключи можно переносить в зашифрованном виде между маршрутизаторами ME с одинаковой версией ПО.

Проверка работы OSPF и диагностические команды

show route ospf

Команда выводит маршруты, имеющиеся в таблице маршрутизации, полученные из протокола OSPF.

Пример. show route ospf

```
0/ME5100:Router# show route ospf

Codes: IA - OSPF inter area, EA - OSPF intra area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

O EA   1.1.1.1/32    via 100.100.12.0 [30/2], 06h17m31s, te 0/0/5
O EA   4.4.4.4/32    via 100.100.24.0 [30/2], 06h05m51s, te 0/0/6
O E1   100.100.13.0/31 via 100.100.12.0 [110/301], 00h02m54s, te 0/0/5
O EA   100.100.14.0/31 via 100.100.12.0 [30/2], 06h10m24s, te 0/0/5

Total route count: 4
```

show ospfv2

Команда выводит общее состояние и статистику по имеющемуся процессу маршрутизации OSPFv2.

Пример. `show ospfv2`

```
0/ME5100:Router# show ospfv2

Routing Process: test, with ID 2.2.2.2
Router is not an area border router
Graceful restart: not-restarting, remaining time: 0, reason: none
OSPF traffic engineering: not supported
The maximum delay before the Routing Table is recalculated: 0
Route max equal cost paths are stored: 5
External lsa refresh interval: 1800
LSA timers (ms): 5000 min interval, 1000 min arrival, 0 hold interval, 0 max
interval
Number of new LSA originated: 118
Number of new LSA received: 85
Number of external LSA (LS type 5): 3, checksum: 0x0001E204
Number of type-11 LSAs in the external database (opaque): 0, checksum: 0x00000000
Number of LSA in LSD at checksum checked: 0
Number of updates 0 pending, 0 merged
Number errors:
    instance id: 0, bad IP header length: 0
    header length: 0, bad IP header length: 0
    no virtual link: 0, version: 0
    bad source: 0, resource errors: 0
Number of packets received have been dropped: 0

Area 0.0.0.0, up
Area can carry data traffic: false
SPF algorithm executed 19 times
Number of number of area border routers: 0, Autonomous routers: 3
Number of Translator State changes: 0
NSSA Border router state: disabled
Number of LSA (LS type-1) count: 3, checksum: 0x0000A0E7
Number of LSA with LS type-2 count: 3
Number of LSA with LS type-3 count: 0, checksum: 0x00000000
Number of LSA with LS type-4 count: 0, checksum: 0x00000000
Number of LSA with LS type-7 (NSSA) count: 0, checksum: 0x00000000
Number of LSA with LS type-10 (opaque) count: 0, checksum: 0x00000000
Number of with LS type-7 (NSSA): 0, checksum: 0x00000000
Total number of LSA: 6, checksum: 0x00016D09

Number of interfaces in this area is: 3
```

show ospfv2 database

Команда выводит содержимое OSPF LSDB для экземпляра VRF либо для глобальной таблицы маршрутизации. При указании параметра `'detailed'` будет выводиться детальное содержимое имеющихся LSA.

При указании типа LSA будут выведены только LSA соответствующего типа.

Пример. `show ospfv2 database`

```
0/ME5100:Router# show ospfv2 database

Routing Process: test, with ID 2.2.2.2

Area Link State Database:

Link ID          ADV Router      Age             Seq#            Checksum        Area
Type
-----
-----
1.1.1.1          1.1.1.1         00:14:16       0x80000034     0x00003E58     0.0.0.0
router-lsa
2.2.2.2          2.2.2.2         00:02:25       0x80000036     0x00004C27     0.0.0.0
router-lsa
4.4.4.4          4.4.4.4         00:09:45       0x80000011     0x00001668     0.0.0.0
router-lsa
100.100.12.1     2.2.2.2         00:21:42       0x80000030     0x00000B37     0.0.0.0
network-lsa
100.100.14.1     1.1.1.1         00:14:16       0x8000000D     0x00008DD1     0.0.0.0
network-lsa
100.100.24.1     2.2.2.2         00:14:23       0x8000000D     0x0000331A     0.0.0.0
network-lsa

Link State Database:

External Link States:
Link ID          ADV Router      Age             Seq#            Checksum        Type
-----
-----
100.100.12.0     1.1.1.1         00:06:50       0x80000001     0x0000ABA2     external-lsa
100.100.13.0     1.1.1.1         00:06:50       0x80000001     0x0000A0AC     external-lsa
100.100.14.0     1.1.1.1         00:06:50       0x80000001     0x000095B6     external-lsa
```

show ospfv2 neighbors

Команда выводит в табличном виде список активных OSPFv2-соседей.

При указании параметра `'detailed'` будет выводиться детальная информация по соседям.

Пример. `show ospfv2 neighbors`

```
0/ME5100:Router# show ospfv2 neighbors
```

```
Routing Process: test, with ID 2.2.2.2
```

```
Router is not an area border router
```

| Neighbor ID Address | Area ID Interface | Pri | State | BFD | Dead Time |
|------------------------|----------------------|-----|----------|--------|-----------|
| 1.1.1.1 | 0.0.0.0 | 1 | full-BDR | active | 00:00:35 |
| 100.100.12.0 | te 0/0/5 | | | | |
| 4.4.4.4 | 0.0.0.0 | 1 | full-BDR | active | 00:00:30 |
| 100.100.24.0 | te 0/0/6 | | | | |

show ospfv2 interfaces

Команда выводит состояние и статистику по интерфейсам, участвующим в процессе OSPFv2.

Пример. show ospfv2 interfaces

```
0/ME5100:Router# show ospfv2 interfaces
```

```
Routing Process: test, with ID 2.2.2.2  
Router is not an area border router
```

```
Interface Loopback 1, state: designated-router, status: up  
Area 0.0.0.0, configured metric: 1  
Changed state: 2 time, Administrative group 0  
Designated Router IP addr: 2.2.2.2  
Backup Designated Router IP addr: 0.0.0.0  
Subnet mask: 255.255.255.255  
Remote peer index: 0  
Number of LSA count: 0, checksum: 0x00000000
```

```
Interface Tengiabitethernet 0/0/5, state: designated-router, status: up  
Area 0.0.0.0, configured metric: 1  
Changed state: 2 time, Administrative group 0  
Designated Router IP addr: 100.100.12.1  
Backup Designated Router IP addr: 100.100.12.0  
Subnet mask: 255.255.255.254  
Remote peer index: 0  
Number of LSA count: 0, checksum: 0x00000000
```

```
Interface Tengiabitethernet 0/0/6, state: designated-router, status: up  
Area 0.0.0.0, configured metric: 1  
Changed state: 2 time, Administrative group 0  
Designated Router IP addr: 100.100.24.1  
Backup Designated Router IP addr: 100.100.24.0  
Subnet mask: 255.255.255.254  
Remote peer index: 0  
Number of LSA count: 0, checksum: 0x00000000
```

```
Interface Tengiabitethernet 0/0/7, state: down, status: down  
Area 0.0.0.0, configured metric: 1  
Changed state: 0 time, Administrative group 0  
Designated Router IP addr: 0.0.0.0  
Backup Designated Router IP addr: 0.0.0.0  
Subnet mask: 255.255.255.254  
Remote peer index: 0  
Number of LSA count: 0, checksum: 0x00000000
```

НАСТРОЙКА ПРОТОКОЛА IS-IS

В данной главе описаны принципы настройки протокола динамической маршрутизации IS-IS (Intermediate System to Intermediate System).

Данный протокол принадлежит к семейству протоколов состояния соединения и относится к группе IGP (Interior Gateway Protocol).

Принципы конфигурирования протокола IS-IS.

Настройка процесса динамической маршрутизации IS-IS производится в разделе конфигурации `router isis`. На устройстве возможно создать только один процесс маршрутизации IS-IS (однако для него необходимо задать уникальное имя). Внутри данного конфигурационного блока настраивается IS-IS как для глобальной таблицы, так и для имеющихся на маршрутизаторе экземпляров VRF.

Дальнейшая конфигурация также производится иерархически.

Внутри таблицы маршрутизации конфигурируются параметры IS-IS (NET, level всей системы, IS-IS hostname и т.п.), а также добавляются интерфейсы, которые будут участвовать в маршрутизации IS-IS.

IMPORTANT

По умолчанию ни один из интерфейсов устройства не включен в протокол IS-IS. Для запуска протокола IS-IS на интерфейсе и/или сабинтерфейсе требуется явно указать этот интерфейс в конфигурации процесса IS-IS.

IMPORTANT

На интерфейсе, сконфигурированном внутри процесса IS-IS, запускается механизм протокольного обнаружения IS-IS — начинается отправка пакетов IS-IS Hello и прием таких пакетов. Исключение составляют т.н. "пассивные" интерфейсы — такие интерфейсы только включаются в адресные TLV в пакетах LSP, соседства через такие интерфейсы не устанавливаются.

Последовательность конфигурирования протокола IS-IS выглядит следующим образом:

1. Создание процесса маршрутизации IS-IS.
2. Общая настройка протокола IS-IS на устройстве.
3. Добавление и настройка интерфейсов в соответствующие таблицы маршрутизации.

Базовая настройка протокола IS-IS

Настройка протокола производится согласно описанной выше иерархии.

Для базовой работоспособности системы необходимо указать параметр `'net'` (IS-IS Network Entity Title) и выбрать тип метрики (`narrow` либо `wide`) для используемых на

маршрутизаторе уровней IS. Также рекомендуется задать параметр `'host-name'` и, в случае использования только одного из уровней IS, выбрать соответствующий уровень общей настройкой `'is-level'`.

Таблица 33. Базовая настройка протокола IS-IS

| Команда | Назначение |
|---|---|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>router isis ISIS_NAME</code> | Создание процесса маршрутизации IS-IS с именем <code>ISIS_NAME</code> и переход в режим его настройки. |
| <code>net NET</code> | Задание системного IS-IS Network Entity Title (NET) в формате <code>XX.XXXX.XXXX.XXXX.XXXX.00</code> . Данный параметр уникально идентифицирует систему во всем IS-IS-домене. |
| <code>is-level { level-1 level-1-2 level-2 }</code> | (Опционально) Выбор уровня IS, в котором будет работать система. По умолчанию используется значение <code>'level-1-2'</code> . |
| <code>host-name HOSTNAME</code> | (Опционально) Задание IS-IS hostname — имени узла, которое будет указываться в соответствующих TLV служебных пакетов IS-IS. По умолчанию используется системное имя устройства (<code>'hostname'</code>). |
| <code>level { level-1 level-2 }</code> | Переход в режим настройки параметров уровня 1 или уровня 2 (для обоих уровней параметры настраиваются одинаково). |
| <code>metric-style { wide narrow both }</code> | (Опционально) Выбор режима метрики для текущего уровня IS-IS. По умолчанию используется режим <code>"both"</code> . |
| <code>set-overload-bit on-startup SECONDS</code> | (Опционально) При указании данного параметра при старте процесса IS-IS в системе будет устанавливаться флаг <code>"IS-IS overload bit"</code> на <code>SECONDS</code> секунд после запуска. |
| <code>exit</code> | Возврат в режим настройки процесса IS-IS. |
| <code>interface { loopback tengigabitethernet bundle-ether } num</code> | Добавление соответствующего интерфейса (либо сабинтерфейса) в процесс IS-IS и переход в режим настройки параметров протокола IS-IS для этого интерфейса. |
| <code>address-family { ipv4 ipv6 } unicast</code> | Включение работы IS-IS с IPv4 или IPv6 на данном интерфейсе и переход в режим конфигурирования соответствующей AFI/SAFI. Важно: в большинстве применений данная команда является обязательной — для корректного включения интерфейса в IP-маршрутизацию протокола IS-IS потребуется указать <code>ipv4 unicast</code> , <code>ipv6 unicast</code> или обе AFI/SAFI. |
| <code>exit</code> | Возврат в режим настройки интерфейса IS-IS. |

| Команда | Назначение |
|--|---|
| <code>circuit-level { level-1 level-1-2 level-2 }</code> | <p>(Опционально) Указание уровня IS, к которому относится данный интерфейс.</p> <p>Интерфейс по умолчанию работает на всех (и только на тех) уровнях, которые заданы общей настройкой '<code>is-level</code>'. Команда же '<code>circuit-level</code>' позволяет выбрать среди системных уровней тот, который требуется для конкретного интерфейса.</p> <p>Практическое применение команда имеет в том случае, когда задан '<code>is-level level-1-2</code>' — в таком случае командой '<code>circuit-level</code>' можно выбрать для интерфейса либо level-1, либо level-2.</p> <p>Интерфейсные параметры соответствующего уровня настраиваются интерфейсной командой '<code>level</code>' (см.далее).</p> |
| <code>level { level-1 level-2 }</code> | <p>Переход в режим настройки IS-IS параметров интерфейса соответствующего уровня.</p> <p>Доступные настройки в данном режиме одинаковы для обоих уровней IS, однако конфигурируются для каждого уровня отдельно.</p> |
| <code>csnp-interval SECONDS</code> | (Опционально) Задание интервала между отправками пакетов CSNP. |
| <code>hello-multiplier MULT</code> | (Опционально) Задание количества потерянных IS-IS Hello, после которых сосед на данном интерфейсе будет считаться потерянным. |
| <code>hello-timer SECONDS</code> | (Опционально) Задание интервала отправки IS-IS Hello. |
| <code>lsp-interval MSEC</code> | (Опционально) Задание интервала между отправками пакетов LSP. |
| <code>metric METRIC</code> | (Опционально) Указание протокольной метрики (стоимости) интерфейса. |
| <code>priority PRIO</code> | (Опционально) Указание приоритета устройства при выборах DR на данном интерфейсе. |
| <code>exit</code> | Возврат в режим настройки интерфейса IS-IS. |
| <code>passive</code> | <p>(Опционально) Перевод интерфейса в пассивный режим.</p> <p>В данном режиме интерфейс не отправляет и не принимает ПН-сообщений и через интерфейс не устанавливается никаких соседств. Режим используется при необходимости анонсировать в IS-IS подсеть данного интерфейса (например, для интерфейсов локальной петли <code>loopback</code>).</p> |
| <code>point-to-point</code> | <p>(Опционально) Включение на интерфейсе режима "IS-IS Point-to-point".</p> <p>В данном режиме не производятся выборы DR и не создаются псевдоноды.</p> <p>Следует следить за тем, чтобы режим интерфейса был задан одинаково для обоих концов IS-IS соединения.</p> |

| Команда | Назначение |
|-----------------------|--|
| <code>shutdown</code> | (Опционально) Отключает протокол IS-IS на указанном интерфейсе полностью. Команда имеет практическое применение в тех случаях, когда требуется временно исключить интерфейс из IS-IS, сохранив при этом всю его конфигурацию. |
| <code>exit</code> | Возврат в режим настройки процесса IS-IS. Далее можно включить в IS-IS и настроить параметры других требуемых интерфейсов. |
| <code>root</code> | Выход в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

Пример. Базовая настройка протокола IS-IS

```
router isis test
  is-level level-2
  net 49.0001.0010.0100.1001.00
  host-name Router
  level level-2
  metric-style wide
exit
interface tengigabitethernet 0/0/5
  point-to-point
  bfd fast-detect ipv4
  hello-padding disable
  address-family ipv4 unicast
  exit
exit
interface tengigabitethernet 0/0/7
  point-to-point
  bfd fast-detect ipv4
  hello-padding disable
  address-family ipv4 unicast
  exit
exit
interface loopback 1
  passive
  address-family ipv4 unicast
  exit
exit
exit
```

Настройка IS-IS для экземпляра VRF

Для запуска процесса маршрутизации IS-IS внутри какого-либо экземпляра VRF необходимо сконфигурировать соответствующий блок `vrf <NAME>` внутри заранее созданного процесса маршрутизации `router isis`. Процесс дальнейшей настройки IS-IS внутри VRF идентичен таковому для глобальной таблицы маршрутизации.

NOTE

Процессы маршрутизации для разных VRF работают независимо друг от друга.

| Команда | Назначение |
|---|---|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>router isis ISIS_NAME</code> | Создание процесса маршрутизации IS-IS с именем <i>ISIS_NAME</i> и переход в режим его настройки. |
| <code>vrf VRF_NAME</code> | Запуск процесса маршрутизации IS-IS в указанном VRF и переход в режим настройки этого процесса. |
| <code>net NET</code> | Задание системного IS-IS Network Entity Title (NET) в формате <i>XX.XXXX.XXXX.XXXX.XXXX.00</i> . Данный параметр уникально идентифицирует систему во всем IS-IS-домене. |
| <code>is-level { level-1 level-1-2 level-2 }</code> | (Опционально) Выбор уровня IS, в котором будет работать система. По умолчанию используется значение 'level-1-2'. |
| <code>host-name HOSTNAME</code> | (Опционально) Задание IS-IS hostname — имени узла, которое будет указываться в соответствующих TLV служебных пакетов IS-IS. По умолчанию используется системное имя устройства ('hostname'). |
| <code>level { level-1 level-2 }</code> | Переход в режим настройки параметров уровня 1 или уровня 2 (для обоих уровней параметры настраиваются одинаково). |
| <code>metric-style { wide narrow both }</code> | (Опционально) Выбор режима метрики для текущего уровня IS-IS. По умолчанию используется режим "both". |
| <code>set-overload-bit on-startup SECONDS</code> | (Опционально) При указании данного параметра при старте процесса IS-IS в системе будет устанавливаться флаг "IS-IS overload bit" на <i>SECONDS</i> секунд после запуска. |
| <code>exit</code> | Возврат в режим настройки процесса IS-IS. |
| <code>interface { loopback tengigabitethernet bundle-ether } num</code> | Добавление соответствующего интерфейса (либо сабинтерфейса) в процесс IS-IS и переход в режим настройки параметров протокола IS-IS для этого интерфейса. |
| <code>address-family { ipv4 ipv6 } unicast</code> | Включение работы IS-IS с IPv4 или IPv6 на данном интерфейсе и переход в режим конфигурирования соответствующей AFI/SAFI. Важно: в большинстве применений данная команда является обязательной — для корректного включения интерфейса в IP-маршрутизацию протокола IS-IS потребуется указать <code>ipv4 unicast</code> , <code>ipv6 unicast</code> или обе AFI/SAFI. |
| <code>exit</code> | Возврат в режим настройки интерфейса IS-IS. |

| Команда | Назначение |
|--|---|
| <code>circuit-level { level-1 level-1-2 level-2 }</code> | <p>(Опционально) Указание уровня IS, к которому относится данный интерфейс.</p> <p>Интерфейс по умолчанию работает на всех (и только на тех) уровнях, которые заданы общей настройкой '<code>is-level</code>'. Команда же '<code>circuit-level</code>' позволяет выбрать среди системных уровней тот, который требуется для конкретного интерфейса.</p> <p>Практическое применение команда имеет в том случае, когда задан '<code>is-level level-1-2</code>' — в таком случае командой '<code>circuit-level</code>' можно выбрать для интерфейса либо level-1, либо level-2.</p> <p>Интерфейсные параметры соответствующего уровня настраиваются интерфейсной командой '<code>level</code>' (см.далее).</p> |
| <code>level { level-1 level-2 }</code> | <p>Переход в режим настройки IS-IS параметров интерфейса соответствующего уровня.</p> <p>Доступные настройки в данном режиме одинаковы для обоих уровней IS, однако конфигурируются для каждого уровня отдельно.</p> |
| <code>csnp-interval SECONDS</code> | (Опционально) Задание интервала между отправками пакетов CSNP. |
| <code>hello-multiplier MULT</code> | (Опционально) Задание количества потерянных IS-IS Hello, после которых сосед на данном интерфейсе будет считаться потерянным. |
| <code>hello-timer SECONDS</code> | (Опционально) Задание интервала отправки IS-IS Hello. |
| <code>lsp-interval MSEC</code> | (Опционально) Задание интервала между отправками пакетов LSP. |
| <code>metric METRIC</code> | (Опционально) Указание протокольной метрики (стоимости) интерфейса. |
| <code>priority PRIO</code> | (Опционально) Указание приоритета устройства при выборах DR на данном интерфейсе. |
| <code>exit</code> | Возврат в режим настройки интерфейса IS-IS. |
| <code>passive</code> | <p>(Опционально) Перевод интерфейса в пассивный режим.</p> <p>В данном режиме интерфейс не отправляет и не принимает ПН-сообщений и через интерфейс не устанавливается никаких соседств. Режим используется при необходимости анонсировать в IS-IS подсеть данного интерфейса (например, для интерфейсов локальной петли <code>loopback</code>).</p> |
| <code>point-to-point</code> | <p>(Опционально) Включение на интерфейсе режима "IS-IS Point-to-point".</p> <p>В данном режиме не производятся выборы DR и не создаются псевдоноды.</p> <p>Следует следить за тем, чтобы режим интерфейса был задан одинаково для обоих концов IS-IS соединения.</p> |

| Команда | Назначение |
|-----------------------|--|
| <code>shutdown</code> | (Опционально) Отключает протокол IS-IS на указанном интерфейсе полностью. Команда имеет практическое применение в тех случаях, когда требуется временно исключить интерфейс из IS-IS, сохранив при этом всю его конфигурацию. |
| <code>exit</code> | Возврат в режим настройки процесса IS-IS внутри VRF. Далее можно включить в IS-IS и настроить параметры других требуемых интерфейсов. |
| <code>root</code> | Выход в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

IMPORTANT

Соответствующий экземпляр VRF должен быть заранее создан в конфигурации маршрутизатора.

Пример. Настройка IS-IS в экземпляре VRF.

```
vrf l3-1
  rd 100:31
  import route-target 100:31
  export route-target 100:31
exit

interface tengigabitethernet 0/0/17.10004000
  vrf l3-1
  description "Some example interface"
  ipv4 address 100.64.0.0/31
  encapsulation outer-vid 1000 inner-vid 4000
exit

router isis test
  vrf l3-1
  is-level level-1
  net 49.0001.0010.0100.1001.00
  host-name AR1
  level level-1
  metric-style wide
  exit
  interface tengigabitethernet 0/0/17.10004000
  point-to-point
  address-family ipv4 unicast
  exit
  exit
  exit
exit
```

Работа с протоколом BFD

Протокол BFD (Bidirectional forwarding detection) служит для быстрого обнаружения отказов соединений между двумя и более соседними устройствами.

Маршрутизаторы семейства ME имеют аппаратную поддержку BFD, что позволяет максимально быстро обнаруживать обрывы соединений и производить переключение трафика на резервные маршруты.

Включение протокола BFD производится путём выполнения команды `bfd fast-detect` на соответствующем интерфейсе в конфигурационном блоке протокола IS-IS. При этом маршрутизатор будет пытаться установить BFD-сессии с IP-адресами всех соседей, которых протокол IS-IS обнаружит на интерфейсе. В случае успешного установления таких соседств статус сессии IS-IS свяжется со статусом соответствующей BFD-сессии.

Таблица 34. Настройка протокола BFD для OSPF-соседств

| Команда | Назначение |
|--|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>router isis ISIS_NAME</code> | Создание процесса маршрутизации IS-IS с именем <code>ISIS_NAME</code> и переход в режим его настройки. |
| <code>interface { tengigabitethernet bundle-ether } num</code> | Переход в режим настройки параметров протокола IS-IS требуемого интерфейса. |
| <code>bfd fast-detect { ipv4 ipv6 }</code> | Включение механизма установления BFD-сессий для всех протокольных соседей IS-IS на данном интерфейсе. |
| <code>root</code> | Возврат в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

Пример. Включение протокола BFD на ранее сконфигурированном интерфейсе IS-IS.

```
router isis test
  interface tengigabitethernet 0/0/5
    bfd fast-detect ipv4
  exit
exit
```

Редистрибуция маршрутной информации

Механизм редистрибуции позволяет передать в IS-IS маршруты из других протоколов (протоколов IGP/EIGP, статических маршрутов и т.п.).

Редистрибуция настраивается путём создания набора именованных правил, при помощи которых можно фильтровать маршруты, подлежащие редистрибуции, а также назначать на маршруты параметры, специфичные для протокола IS-IS. Для каждого из источников (`bgp/connected/local` и т.п.) можно создать несколько правил, назначив им приоритет командой `priority` — при редистрибуции маршрута данные правила будут применяться к нему по очереди до первого срабатывания. Правила редистрибуции имеют по умолчанию

действие "разрешить"—таким образом, пустое правило автоматически производит редистрибуцию всех маршрутов из указанного источника.

Источники редистрибуции:

1. **bgp** — маршрутная таблица протокола BGP;
2. **connected** — маршруты, соответствующие подсетям, назначенным на IP-интерфейсы маршрутизатора в данном VRF (либо GRT);
3. **ospf** — маршрутная таблица протокола OSPF;
4. **local** — маршруты, являющиеся спецификами /32 для адресов, назначенных на IP-интерфейсы маршрутизатора.
5. **static** — статические маршруты.

Таблица 35. Настройка редистрибуции в IS-IS маршрутной информации из других протоколов.

| Команда | Назначение |
|--|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>router isis ISIS_NAME</code> | Переход в режим настройки процесса маршрутизации IS-IS с именем <i>ISIS_NAME</i> . |
| <code>address-family ipv4 unicast</code> | Переход в режим настройки параметров адресного семейства IPv4 unicast. |
| <code>redistribution { bgp connected ospf local static } RULE_NAME</code> | Создание правила редистрибуции с именем <i>RULE_NAME</i> из указанного источника (bgp/connected/ospf/local/static) и переход в режим настройки этого правила. |
| <code>match prefix IPv4PREFIX/MASK</code> | Указание фильтра, используемого для данного правила. При указании такого фильтра правило будет действовать только на маршруты, строго совпадающие с заданным <i>IPv4PREFIX/MASK</i> . |
| <code>metric-type { isis-level1-external isis-level1-internal isis-level2-external isis-level2-internal }</code> | Назначить на маршруты, прошедшие через данное правило, метрику соответствующего типа. |
| <code>metric-value METRIC</code> | Установить значение метрики для маршрутов, прошедших через данное правило. |
| <code>priority RULE_PRIORITY</code> | Установить приоритет данного правила редистрибуции. Правила редистрибуции выполняются по очереди от низкого значения приоритета к высокому и срабатывают по первому вхождению. Таким образом, маршрут, попавший, например, в первое правило, будет передан в IS-IS согласно настроек этого правила и не будет обрабатываться последующими правилами. |
| <code>redistribute disable</code> | Запретить редистрибуцию маршрутов, попавших в текущее правило. При выполнении данной команды текущее правило становится запрещающим. |

| Команда | Назначение |
|---------------------|--|
| <code>exit</code> | Выход из режима настройки правила редистрибуции. Далее можно настроить следующие правила — для того же самого источника, либо для других источников редистрибуции. |
| <code>root</code> | Выход в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

Пример. Настройка процесса IS-IS с двумя правилами редистрибуции connected-маршрутов.

```

router isis eltex-test
  is-level level-2
  net 49.0001.0010.0100.1001.00
  host-name Router
  level level-2
    metric-style wide
  exit
  address-family ipv4 unicast
    redistribution connected CONN-ISIS
      match prefix 100.65.0.0/24
      priority 10
      redistribute disable
    exit
    redistribution connected CONN-ISIS-20
      priority 20
      metric-value 300
      metric-type isis-level1-internal
    exit
  exit
  interface tengigabitethernet 0/0/5
    point-to-point
    bfd fast-detect ipv4
    hello-padding disable
    address-family ipv4 unicast
    exit
  exit
  interface tengigabitethernet 0/0/7
    point-to-point
    bfd fast-detect ipv4
    hello-padding disable
    address-family ipv4 unicast
    exit
  exit
  interface loopback 1
    passive
    address-family ipv4 unicast
    exit
  exit
exit

```

Аутентификация IS-IS

Маршрутизаторы семейства ME позволяют использовать аутентификацию в протоколе IS-IS.

Для протокола IS-IS поддерживается два вида аутентификации:

- Глобальная аутентификация уровня (*level*) — настраивается в разделе '*level*' блока '*router isis*';
- Аутентификация соседства — настраивается поинтерфейсно в блоке '*router isis*'.

Для использования каждого перечисленных видов необходимо указать требуемый тип командой '*authentication-type*' и задать ключ командой '*authentication-key*'.

Таблица 36. Настройка глобальной аутентификации уровня IS-IS.

| Команда | Назначение |
|---|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>router isis ISIS_NAME</code> | Переход в режим настройки процесса маршрутизации IS-IS с именем <i>ISIS_NAME</i> . |
| <code>level { level-1 level-2 }</code> | Переход в режим настройки параметров уровня 1 или уровня 2 (для обоих уровней параметры настраиваются одинаково). |
| <code>authentication-type { hmacsha1 hmacsha256 hmacsha384 hmacsha512 md5 none simple-password }</code> | Выбор типа аутентификации для выбранного уровня IS-IS — HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512, MD5 либо простой пароль (<i>simple-password</i>). Задание параметра ' <i>none</i> ' отключает аутентификацию для уровня, что соответствует поведению по умолчанию. |
| <code>authentication-key { KEY_STRING encrypted KEY_ENCRYPT }</code> | Задание ключа для аутентификации в открытом (<i>KEY_STRING</i>) либо в зашифрованном (<i>KEY_ENCRYPT</i>) виде. |
| <code>root</code> | Выход в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

Таблица 37. Настройка аутентификации соседства IS-IS.

| Команда | Назначение |
|--|--|
| <code>router isis ISIS_NAME</code> | Переход в режим настройки процесса маршрутизации IS-IS с именем <i>ISIS_NAME</i> . |
| <code>interface { tengigabitethernet bundle-ether } num</code> | Переход в режим настройки параметров протокола IS-IS требуемого интерфейса. |

| Команда | Назначение |
|---|--|
| <code>authentication-type { hmacsha1 hmacsha256 hmacsha384 hmacsha512 md5 none simple-password }</code> | Выбор типа аутентификации для соседства на текущем интерфейсе — HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512, MD5 либо простой пароль (simple-password). Задание параметра 'none' отключает аутентификацию соседства на интерфейсе, что соответствует поведению по умолчанию. |
| <code>authentication-key { KEY_STRING encrypted KEY_ENCRYPT }</code> | Задание ключа для аутентификации в открытом (KEY_STRING) либо в зашифрованном (KEY_ENCRYPT) виде. |
| <code>root</code> | Выход в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

Пример. Включение интерфейсной аутентификации IS-IS и аутентификации соседства на интерфейсе.

```
router isis test
  level level-2
    metric-style wide
    authentication-key level-password
    authentication-type hmacsha1
  exit
interface tengigabitethernet 0/0/7
  authentication-key neighbor-password
  authentication-type hmac-md5
  exit
exit
```

NOTE При несовпадении ключей/типов аутентификации соседства между двумя маршрутизаторами не будет устанавливаться соседство (аутентификация распространяется на пакеты ISIS Hello).
При несовпадении ключей/типов аутентификации уровня маршрутизаторы могут установить соседство друг с другом, однако не могут передавать друг другу маршрутную информацию (аутентификация распространяется на пакеты LSP/CSNP/PSNP).

Проверка работы IS-IS и диагностические команды

show route isis

Команда выводит маршруты, имеющиеся в таблице маршрутизации, полученные из протокола IS-IS.

Пример. show route isis

```
0/ME5100:Router# show route isis
Tue Jun 12 00:44:30 2018
Codes: i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2
       LE1 - ISIS level1 external, LE2 - ISIS level2 external

i L2  4.4.4.4/32    via 100.100.14.0 [116/10], 00h12m42s, te 0/0/7
i L2  100.100.24.0/31 via 100.100.14.0 [116/20], 00h12m42s, te 0/0/7

Total route count: 2
```

show isis

Команда выводит общее состояние и статистику по имеющемуся процессу маршрутизации IS-IS.

Пример. `show isis`

```
0/ME5100:Router# show isis

IS-IS Router eltex-test
System Id: 0010.0100.1001
IS Levels: level-2
Net: 49.0001.0010.0100.1001.00
Hostname: AR1
LSP full-suppress: external
LSP refresh-interval: 900 secs
LSP max-lifetime: 1200 secs
Area-address: 49.0001
Topologies supported by IS-IS:
  IPv4 Unicast
    level-2
      Metric style (generate/accept): wide
  Redistributed ipv4 unicast:
    none bgp redistributed
    none ospf redistributed
    none static redistributed
    Connected routes redistribution is enabled via 'CONN-ISIS' rule
    Connected routes redistribution is enabled via 'CONN-ISIS-20' rule
  Redistributed ipv6 unicast:
    none bgp redistributed
    none ospf redistributed
    none static redistributed
    none connected redistributed
  Interfaces supported by IS-IS
    Tengigabitethernet 0/0/5 is up (active in configuration)
    Tengigabitethernet 0/0/6 is down (active in configuration)
    Tengigabitethernet 0/0/7 is up (active in configuration)
    Loopback 1 is up (passive in configuration)
```

show isis database

Команда выводит содержимое базы данных IS-IS для экземпляра VRF либо для глобальной таблицы маршрутизации. При указании параметра `'detailed'` будет выводиться детальное содержимое имеющихся LSP.

Пример. show isis database.

```
0/ME5100:Router# show isis database

IS-IS Router test
  IS-IS level-2 link-state database
LSP ID                Sequence  Checksum  Lifetime (sec)  PDU length  Attributes
-----
0010.0100.1001.00-00  0x11ab   0x632d   986             66          level-2
0010.0100.1001.00-01  0x11a8   0xa71b   517             57          level-2
0010.0100.1001.00-02  0x11c9   0xd0f7   492             116         level-2
0040.0400.4004.00-00  0x11ac   0x24e6   726             66          level-2
0040.0400.4004.00-01  0x119f   0x57b1   719             64          level-2
0040.0400.4004.00-02  0x11bd   0x7848   692             116         level-2

Total LSPs: 6
```

show isis neighbors

Команда выводит в табличном виде список активных соседей протокола IS-IS.

Пример. show isis neighbors.

```
0/ME5100:Router# show isis neighbors

IS-IS Router test adjacency:
System Id      Hostname      Interface      State      Type      SNPA
Hold (sec) NSF   BFD
-----
0040.0400.4004 DR1-me5000   te 0/0/7      up        level-2
A8F9.4B8B.2031 19           true up
```

show isis interfaces

Команда выводит состояние интерфейсов, участвующих в процессе маршрутизации IS-IS.

Пример. show isis interfaces.

```
0/ME5100:Router# show isis interfaces tengigabitethernet 0/0/7

IS-IS Router eltex-test interface:

Tengigabitethernet 0/0/7
  Last up: 02w05d16h ago
  BFD Fast detect: IPv4 enabled, IPv6 disabled
  Operation state: up
  Disabled creating neighborhood on this interface: false
  Circuit 3 way: enabled
  Extended circuit id: 8
  T1 timer status: stopped
  Media Type: p2p

  IPv4 Address Family: enabled
  IPv6 Address Family: disabled

  Circuit level: level-2 (Interface circuit type is level-1-2)
  Level one:
    ID: 0010.0100.1001, ID Hostname: Router, DR ID: none, Designated Hostname: none,
  Configured metric: 10
  Level two:
    ID: 0040.0400.4004, ID Hostname: DR1-me5000, DR ID: none, Designated Hostname:
  none, Configured metric: 10
```

show isis interfaces statistics

Команда выводит детальную протокольную статистику по интерфейсам, участвующим в процессе маршрутизации IS-IS.

Пример. show isis interfaces statistics.

```
0/ME5100:Router# show isis interfaces statistics

IS-IS Router test

Interface: Tengigabitethernet 0/0/7
  Level one:
    Hello IS-IS PDUs: 0 received, 0 sent
    Hello ES-IS PDUs: 0 received, 0 sent
    Hello ES PDUs: 0 received, 0 sent
    LSP: 0 received, 0 sent
    CSNP: 0 received, 0 sent
    PSNP: 0 received, 0 sent
    Unknown packet: 0 received, 0 sent
    Discarded: 0 received
    Discarded: 0 received
    Discarded: 0 received
```

```
Discarded: 0 received
Level two:
Hello IS-IS PDUs: 215280 received, 215898 sent
Hello ES-IS PDUs: 0 received, 0 sent
Hello ES PDUs: 0 received, 0 sent
LSP: 6465 received, 7563 sent
CSNP: 169554 received, 169559 sent
PSNP: 6770 received, 6438 sent
Unknown packet: 0 received, 0 sent
Discarded: 0 received
Discarded: 0 received
Discarded: 0 received
Discarded: 0 received

Interface: Loopback 1
Level one:
Hello IS-IS PDUs: 0 received, 0 sent
Hello ES-IS PDUs: 0 received, 0 sent
Hello ES PDUs: 0 received, 0 sent
LSP: 0 received, 0 sent
CSNP: 0 received, 0 sent
PSNP: 0 received, 0 sent
Unknown packet: 0 received, 0 sent
Discarded: 0 received
Discarded: 0 received
Discarded: 0 received
Discarded: 0 received

Level two:
Hello IS-IS PDUs: 0 received, 0 sent
Hello ES-IS PDUs: 0 received, 0 sent
Hello ES PDUs: 0 received, 0 sent
LSP: 0 received, 0 sent
CSNP: 0 received, 0 sent
PSNP: 0 received, 0 sent
Unknown packet: 0 received, 0 sent
Discarded: 0 received
Discarded: 0 received
Discarded: 0 received
Discarded: 0 received
```

show isis statistics

Команда выводит общую статистику по уровням IS-IS.

Пример. show isis statistics.

```
0/ME5100:Router# show isis statistics
```

```
IS-IS Router eltex-test
```

```
Level one:
```

```
Overload state: off
```

```
Corrupted lsps: 0
```

```
Authentication mismatches: 0 failures: 0
```

```
LSP db overloaded: 0 times
```

```
Manual address dropped: 0 times
```

```
Exceed max sequence number: 0 times - exceeded
```

```
Sequence number skipped: 0 times
```

```
Zero-aged copy LSP received: 0 times
```

```
Diff PDU id received: 0 times
```

```
SPF ran at level: 0 times
```

```
Partition changes: 0
```

```
Errors: 0 lsp, 0 csnp, 0 psnp
```

```
LSP: 2 count, 0 in queue
```

```
LSP: 6 fragments rebuilt, 0 retransmitted
```

```
LSP: 9051 regenerated, 0 purges
```

```
LSP initiated: 0 locally, 0 remotely
```

```
LSP initiated: 0 due SNP, 0 originated remotely (expired)
```

```
LSP initiated: 0 originated remotely (peer restart)
```

```
Level two:
```

```
Overload state: on
```

```
Corrupted lsps: 0
```

```
Authentication mismatches: 0 failures: 0
```

```
LSP db overloaded: 1 times
```

```
Manual address dropped: 0 times
```

```
Exceed max sequence number: 0 times - exceeded
```

```
Sequence number skipped: 0 times
```

```
Zero-aged copy LSP received: 0 times
```

```
Diff PDU id received: 0 times
```

```
SPF ran at level: 3976 times
```

```
Partition changes: 0
```

```
Errors: 0 lsp, 0 csnp, 0 psnp
```

```
LSP: 6 count, 0 in queue
```

```
LSP: 23 fragments rebuilt, 6 retransmitted
```

```
LSP: 13577 regenerated, 3 purges
```

```
LSP initiated: 0 locally, 3 remotely
```

```
LSP initiated: 0 due SNP, 3 originated remotely (expired)
```

```
LSP initiated: 0 originated remotely (peer restart)
```

НАСТРОЙКА ПРОТОКОЛА BGP

В данной главе описан процесс настройки протокола динамической маршрутизации BGP (*Border Gateway Protocol*).

Принципы конфигурирования протокола BGP

Настройка BGP-процесса

Настройка процесса динамической маршрутизации BGP производится в разделе конфигурации `'router bgp <ASN>'`. На устройстве возможно создать только один процесс маршрутизации BGP и, соответственно, задать единственную локальную автономную систему. Внутри данного конфигурационного блока настраивается BGP как для глобальной таблицы маршрутизации (Global Routing Table, GRT), так и для имеющихся на маршрутизаторе экземпляров VRF.

Внутри каждой из таблиц (глобальной таблицы либо VRF) можно конфигурировать:

- Общие параметры работы протокола BGP;
- Правила редистрибуции маршрутной информации;
- Перечень протокольных соседей BGP, доступных в данном VRF либо в GRT, и параметры этих соседей.

GRT-соседи и VRF-соседи

Для создания соседа, связность с которым производится через глобальную таблицу (GRT-соседа), требуется сконфигурировать соответствующий блок внутри раздела `'router bgp <ASN>'`.

Пример. Настройка соседа в GRT.

```
router bgp 65535
  bgp router-id 1.1.1.1
  neighbor 2.2.2.2
    address-family ipv4 unicast
  exit
  remote-as 65535
  update-source 1.1.1.1
exit
```

Для создания соседа, связность с которым производится через имеющийся на устройстве VRF (VRF-соседа), требуется сконфигурировать соответствующий блок внутри подраздела `'vrf <VRF_NAME>'` раздела `'router bgp <ASN>'`.

Пример. Настройка соседа в экземпляре VRF.

```
router bgp 65535
  vrf l3-2
    bgp router-id 1.1.1.1
    neighbor 172.16.0.0
      address-family ipv4 unicast
      exit
    remote-as 65535
    update-source 1.1.1.1
  exit
exit
exit
```

IMPORTANT

В текущей версии ПО **необходимо** задавать '**router-id**' как в глобальной таблице маршрутизации, так и для каждого сконфигурированного в BGP экземпляра VRF.

Адресные семейства и их идентификаторы (AFI/SAFI)

Реализация протокола BGP на маршрутизаторах серии ME поддерживает прием, передачу и обработку путей различных типов (адресных семейств).

В текущей версии ПО реализована работа со следующими адресными семействами:

- IPv4 Unicast;
- VPNv4 Unicast;
- L2VPN VPLS.

Часть настройки протокола BGP можно производить отдельно для каждого из семейств. Кроме того, для каждого из протокольных соседей поддержка конкретных AFI/SAFI включается отдельно.

IMPORTANT

По умолчанию на протокольных соседях BGP все адресные семейства отключены. Для обмена путями соответствующих AFI/SAFI **необходимо явно включить их поддержку** командой '**address-family <AFI> <SAFI>**' в разделе конфигурации BGP-соседа.

NOTE

Для VRF-соседей поддерживается только семейство '**ipv4 unicast**'. Семейства '**vpn4 unicast**' и '**l2vpn vpls**' могут быть использованы только для GRT-соседей.

Передача параметров community

По умолчанию параметры *community* и *extended community* не передаются сконфигурированным соседям (удаляются из анонсируемых путей).

Для того, чтобы сохранять данные параметры при передаче BGP-соседу, следует применять

команды 'send-community' и 'send-community-ext'.

Пример. Включение передачи параметров *community* и *extended community* для GRT-соседа с адресом 2.2.2.2.

```
router bgp 65535
  neighbor 2.2.2.2
    send-community
    send-community-ext
  exit
exit
```

Фильтрация маршрутной информации

Для управления анонсами при их отправке и получении имеются два механизма — карты маршрутов (*route-maps*) и списки префиксов (*prefix-lists*). Предварительно сконфигурированные карты маршрутов и списки префиксов можно использовать для фильтрации как получаемых от соседа, так и отправляемых ему путей.

Списки префиксов являются простыми фильтрами, в которых при совпадении с условием фильтра проверяемый префикс либо разрешается, либо запрещается. Условием для таких фильтров является только совпадение префикса (сети/маски).

Карты маршрутов являются более сложными фильтрами, которые помимо действия "разрешить/запретить" могут также модифицировать BGP-атрибуты соответствующего пути.

IMPORTANT

Карты маршрутов и списки префиксов при одновременном использовании (в направлении входа либо выхода) не имеют приоритета друг над другом, они применяются к анонсам одновременно. Таким образом, анонс будет принят (или передан), если его "разрешили" и карта маршрутов, и список префиксов.

IMPORTANT

По умолчанию принимаемые от соседа и отправляемые ему анонсы не фильтруются. Таким образом, пустая конфигурация фильтров приведет к тому, что соседу будут отправлены все имеющиеся в соответствующем адресном семействе маршруты; также будут приняты все проанонсированные соседом пути.

Базовая настройка BGP-процесса

Для базовой работоспособности BGP-процесса необходимо создать его в конфигурации, задать *router id* для устройства и сконфигурировать соседей.

Таблица 38. Базовая настройка BGP-процесса

| Команда | Назначение |
|------------------------|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |

| Команда | Назначение |
|--|---|
| <code>router bgp ASN</code> | Создание процесса маршрутизации BGP с автономной системой с номером ASN и переход в режим его настройки. |
| <code>bgp router-id A.B.C.D</code> | Назначение локального идентификатора маршрутизатора. Рекомендуется использовать для этой цели IPv4-адрес одного из loopback-интерфейсов устройства. |
| <code>address-family ipv4 unicast</code> | (Опционально) Переход в режим настройки адресного семейства IPv4 Unicast. |
| <code>aggregate-address IPv4_PREFIX [summary-only]</code> | Создание агрегирующего маршрута. Данный маршрут будет суммировать более специфичные префиксы при их наличии. При указании параметра 'summary-only' все входящие специфичные префиксы будут подавлены (т.е. не будут анонсироваться соседям). |
| <code>exit</code> | Возврат в режим настройки параметров BGP для IPv4 Unicast. |
| <code>dampening</code> | Включение механизма подавления мерцания маршрутов. |
| <code>redistribution { connected isis local ospf static } RULE_NAME</code> | Создание правила редистрибуции и переход в режим его настройки. Подробнее см. раздел "Редистрибуция маршрутной информации". |
| <code>exit</code> | Возврат в режим настройки параметров BGP для IPv4 Unicast. |
| <code>exit</code> | Возврат в режим настройки параметров BGP. Далее можно настроить параметры других AFI/SAFI. |
| <code>neighbor A.B.C.D A:B:C:D::X</code> | Создание протокольного соседа (с IPv4- или IPv6-адресом) и переход в режим настройки его параметров. |
| <code>description "STRING"</code> | Задание текстовой строки — описания протокольного соседа. |
| <code>ebgp-multihop ttl MULTIHOPE-TTL</code> | Данная команда указывает, что данный eBGP-сосед не является непосредственно подключенным к маршрутизатору и для работы с ним на BGP-сессии соответствующим образом следует увеличить IP TTL со стандартного значения 1 до указанного MULTIHOPE-TTL. |
| <code>max-prefixes PREFIXES</code> | Устанавливает ограничение на количество получаемых от соседа префиксов. |
| <code>remote-as ASN</code> | Задаёт номер автономной системы BGP-соседа. Является обязательным параметром при создании соседа. |
| <code>send-community</code> | Включает отправку параметра <i>community</i> в отсылаемых соседу анонсах. По умолчанию параметры <i>community</i> удаляются из отправляемых анонсов. |

| Команда | Назначение |
|--|--|
| <code>send-community-ext</code> | Включает отправку параметра <i>extended community</i> в отсылаемых соседу анонсах. По умолчанию параметры <i>extended community</i> удаляются из отправляемых анонсов. Для корректной работы AFI L2VPN, VPNv4/VPNv6 отправку <i>extended community</i> необходимо включать. |
| <code>address-family { ipv4 unicast ipv6 unicast l2vpn vpls vpnv4 unicast }</code> | Включение на данном соседе указанного адресного семейства (обязательно для работы соответствующей AFI/SAFI) и переход в режим настроек данного семейства. |
| <code>next-hop-self</code> | При указании данной команды для всех отправляемых маршрутов в качестве параметра <i>next-hop</i> будет устанавливаться адрес данного маршрутизатора. |
| <code>prefix-list { in out } PREFLIST_NAME</code> | Установка фильтра префиксов для принимаемых (<i>in</i>) или отправляемых (<i>out</i>) анонсов. Соответствующий фильтр префиксов должен быть создан в конфигурации маршрутизатора. |
| <code>route-map { in out } ROUTEMAP_NAME</code> | Установка "карты маршрутов" для фильтрации, соответственно, принимаемых (<i>in</i>) или отправляемых (<i>out</i>) анонсов. Карта маршрутов с именем, соответствующим <i>ROUTEMAP_NAME</i> , должна быть создана в конфигурации маршрутизатора. |
| <code>route-reflector-client</code> | Установка текущего протокольного соседа в режим RR-клиента. Такому iBGP-соседу будут анонсироваться пути, полученные по iBGP от других маршрутизаторов сети. |
| <code>soft-reconfiguration inbound</code> | Включение возможности мягкой реконфигурации путем хранения всех полученных от соседа анонсов в промежуточной таблице. Параметр не рекомендуется к применению из-за дополнительного расхода ресурсов; в современных реализациях BGP необходимость данного функционала снижена благодаря существованию <i>route-refresh capability</i> . |
| <code>exit</code> | Возврат в режим настройки параметров протокольного соседа BGP. Далее можно сконфигурировать другие адресные семейства для указанного соседа. |
| <code>exit</code> | Возврат в режим настройки параметров BGP. Далее можно создать и настроить других протокольных соседей. |
| <code>root</code> | Выход в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

```
router bgp 65530
  address-family ipv4 unicast
    dampening
    aggregate-address 100.100.0.0/16
    exit
    aggregate-address 100.64.0.0/16
      summary-only
    exit
    redistribution connected CONN-10
      set local-preference 120
      set origin igp
    exit
  exit
  bgp router-id 4.4.4.4
  neighbor 2.2.2.2
    address-family ipv4 unicast
      route-map in Client
      route-map out FULL
    exit
    address-family l2vpn vpls
  exit
  address-family vpnv4 unicast
  exit
  remote-as 65532
  send-community
  send-community-ext
  update-source 4.4.4.4
  exit
  vrf l3-2
    address-family ipv4 unicast
      redistribution connected CONN
    exit
  exit
  bgp router-id 4.4.4.4
  neighbor 172.16.0.0
    address-family ipv4 unicast
    exit
    remote-as 65532
  exit
  exit
  exit
```

Фильтрация маршрутов списками префиксов (prefix-lists)

Списки префиксов применимы только для фильтрации маршрутной информации и не предназначены для фильтрации трафика.

Списки префиксов являются простыми фильтрами с действиями "запретить" (префикс не пройдет через фильтр) и "разрешить" (префикс пройдет через фильтр). Для их использования необходимо создать в конфигурации сам список префиксов, после чего назначить его соответствующему соседу.

Таблица 39. Настройка списка префиксов.

| Команда | Назначение |
|--|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>prefix-list PREFLIST_NAME</code> | Создание списка префиксов <i>PREFLIST_NAME</i> и переход в режим его настройки. |
| <code>seq-num SEQ-NUM</code> | Создание элемента списка префиксов с соответствующим номером и переход в режим его настройки. Номер элемента может принимать значения 1-4294967295. |
| <code>prefix { A.B.C.D/N X:X:X::X/N }</code> | Задание префикса, сравнение с которым будет производиться данным элементом списка. |
| <code>action { permit deny }</code> | <p>Действие, которое будет производиться с соответствующим префиксом, если он попал под условия данного элемента списка.</p> <p>По умолчанию установлено <code>action permit</code>.</p> |

| Команда | Назначение |
|-------------------------------|---|
| <p><code>le 1..128</code></p> | <p>Указание дополнительного условия на длину префикса (<i>less or equal</i>, "префикс короче либо равен заданного значения").</p> <p>В данном случае элемент фильтра становится нестрогим — в сочетании с заданным <code>prefix</code> он будет включать в себя все более специфичные префиксы, входящие в него и имеющие маску не длиннее заданной параметром <code>le</code>.</p> <p>Например, комбинация:</p> <pre data-bbox="639 629 1457 846">seq-num 10 prefix 100.64.0.0/16 le 24 exit</pre> <p>даст фильтр, в который попадут все префиксы, попадающие в 100.64.0.0/16 и имеющие маску от /16 до /24.</p> |
| <p><code>ge 1..128</code></p> | <p>Указание дополнительного условия на длину префикса (<i>greater or equal</i>, "префикс длиннее либо равен заданного значения").</p> <p>В данном случае элемент фильтра становится нестрогим — в сочетании с заданным <code>prefix</code> он будет включать в себя все более специфичные префиксы, входящие в него и имеющие маску не короче заданной параметром <code>ge</code>.</p> <p>Комбинация:</p> <pre data-bbox="639 1525 1457 1742">seq-num 10 prefix 100.64.0.0/16 ge 20 exit</pre> <p>даст фильтр, в который попадут все префиксы, попадающие в 100.64.0.0/16 и имеющие маску от /20 до /32.</p> |

| Команда | Назначение |
|---|---|
| <code>exit</code> | Выход из режима настройки элемента списка фильтра префиксов. Далее можно создать следующие требуемые элементы списка. |
| <code>root</code> | Возврат в режим глобальной конфигурации |
| <code>router bgp ASN</code> | Переход в режим настройки процесса BGP. |
| <code>neighbor A.B.C.D A:B:C:D::X</code> | Переход в режим настройки параметров BGP-соседа. |
| <code>address-family { ipv4 unicast ipv6 unicast vpnv4 unicast }</code> | Переход в режим настроек тех AFI/SAFI, для которых требуется применить фильтр префиксов. |
| <code>prefix-list { in out } PREFLIST_NAME</code> | Установка фильтра префиксов для принимаемых (<i>in</i>) или отправляемых (<i>out</i>) анонсов. |
| <code>root</code> | Выход в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

Пример. Настройка и назначение на соседа фильтра префиксов, который будет пропускать только маршруты, входящие в 109.171.0.0/17 с длиной маски от /20 до /24, а также единственный маршрут 82.200.0.0/17:

```

prefix-list PREF-LIST-EXAMPLE
  seq-num 10
    prefix 109.171.0.0/17
    ge 20
    le 24
  exit
  seq-num 20
    prefix 82.200.0.0/17
  exit
exit

router bgp 65535
  neighbor 100.64.28.1
    address-family ipv4 unicast
      prefix-list in PREF-LIST-EXAMPLE
    exit
  exit
exit

```

IMPORTANT

По умолчанию каждый элемент списка префиксов имеет правило "permit". По умолчанию каждый список префиксов имеет неявное запрещающее правило в конце, то есть прохождение всех префиксов запрещается.

В случае, если BGP-сосед поддерживает функционал Route Refresh, не требуется сброс сессии (либо soft-реконфигурация) при изменении маршрутных политик; эти политики будут заново применены автоматически. Проверить возможности соседа можно командой '`show bgp neighbor`':

```
0/ME5100:Router# show bgp neighbors 100.64.28.1 | i Capabilities

    Capabilities sent:  mp-ipv4-unicast route-refresh route-refresh-cisco four-
octet-as enhanced-route-refresh
    Capabilities received:  mp-ipv4-unicast route-refresh graceful-restart four-
octet-as enhanced-route-refresh
    Capabilities negotiated:  mp-ipv4-unicast route-refresh four-octet-as enhanced-
route-refresh
0/ME5100:Router#
```

Фильтрация маршрутов посредством route-map

Для осуществления одновременной фильтрации и модификации принимаемых/получаемых анонсов используются карты маршрутов (*route-maps*).

Правила работы карт маршрутов:

1. Карты состоят из нумерованных элементов (seq-num).
2. Каждый элемент может содержать условия соответствия (*match*).
3. Каждый элемент может содержать правила модификации анонса (*set*).
4. Каждый элемент должен содержать правило "разрешить" или "запретить" (*action*).
5. Фильтруемые анонсы проходят последовательно все элементы route-map, от меньшего seq-num к большему, до первого срабатывания условия соответствия *match*. При срабатывании условия соответствия к анонсу применяются сконфигурированные модификации *set* и выдается пометка "разрешить" (*permit*) или "запретить" (*deny*) в соответствии с настройкой элемента. Дальнейшая обработка анонса после этого прекращается.
6. По умолчанию в конце каждой карты маршрутов установлено неявное запрещающее правило. Таким образом, пустая route-map запретит **все** пропущенные через неё маршруты.

Общие правила настройки карт маршрутов

Таблица 40. Создание route-map.

| Команда | Назначение |
|--|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>route-map ROUTEMAP_NAME</code> | Создание карты маршрутов с именем <i>ROUTEMAP_NAME</i> и переход в режим ее настройки. |
| <code>seq-num SEQ-NUM</code> | Создание элемента карты маршрутов с соответствующим номером и переход в режим его настройки. Номер элемента может принимать значения 1-4294967295. |
| <code>set { comm-list .. community .. ext-comm-list .. extcommunity .. local-preference .. med .. nexthop .. prepend .. remove .. weight .. }</code> | <p>Назначение правила модификации анонса. Перечень параметров зависит от типа правила модификации, см. в следующих разделах.</p> <p>Для каждого элемента карты можно назначить несколько разнотипных правил модификации, несколько однотипных правил назначить невозможно (например, для одного элемента можно задать правила <code>set community</code> и <code>set remove</code>, но нельзя назначить несколько правил <code>set community</code>).</p> |
| <code>match { as-path .. comm-list .. ext-comm-list .. prefix-list .. }</code> | <p>Назначение условия соответствия анонса. Перечень параметров зависит от типа условия соответствия, см. в следующих разделах.</p> <p>Для каждого элемента карты можно назначить несколько разнотипных условий соответствия, несколько однотипных условий назначить невозможно (например, для одного элемента можно задать условия <code>match prefix-list</code> и <code>match as-path</code>, но нельзя задать несколько условий <code>match prefix-list</code>).</p> <p>При необходимости фильтрации анонсов с различными однотипными условиями <code>match</code> требуется создавать отдельные элементы карты маршрутов, по одному на каждое условие.</p> |
| <code>action { permit deny }</code> | Действие, которое будет производиться с анонсом, если он попал под условия данного элемента списка. |
| <code>exit</code> | Выход из режима настройки элемента карты маршрутов. Далее можно создать следующие требуемые элементы списка. |
| <code>root</code> | Возврат в режим глобальной конфигурации |

| Команда | Назначение |
|---------------------|------------------------------------|
| <code>commit</code> | Применение произведенных настроек. |

Пример. Настройка `route-map` с двумя элементами.

```
route-map EXAMPLE-RM
  seq-num 10
    match as-path ^65054(_[0-9]+)*_21127$
    set local-preference 80
  exit
  seq-num 20
    match prefix-list destination EXAMPLE-PRFLIST
    match as-path ^65054(_[0-9]+)*_197728$
    set remove as-path 3216
    set local-preference 150
  exit
exit
```

Правила модификации анонсов

Правила модификации анонсов задаются внутри элементов карты маршрутов посредством команды `'set'`. Виды правил модификации приведены в таблице.

Таблица 41. Виды правил модификации анонсов `'set'`.

| Команда | Назначение |
|---|---|
| <code>comm-list { add delete } COMMLIST_NAME</code> | Добавить или удалить из анонса набор <code>community</code> , заданный соответствующим правилом <code>ip-community COMMLIST_NAME</code> . |
| <code>community remove-all</code> | Удалить все <code>community</code> из анонса. |
| <code>community remove-all-and-set value { 0-4294967295 0-65535:0-65535 accept-own accept-own-nexthop blackhole gshut internet llgr-stale local-as no-advertise no-export no-llgr nopeer route-filter-translated-v4 route-filter-translated-v6 route-filter-v4 route-filter-v6 }</code> | Удалить все <code>community</code> из анонса и добавить одну новую. |
| <code>community set-specific value { 0-4294967295 0-65535:0-65535 accept-own accept-own-nexthop blackhole gshut internet llgr-stale local-as no-advertise no-export no-llgr nopeer route-filter-translated-v4 route-filter-translated-v6 route-filter-v4 route-filter-v6 }</code> | Добавить к анонсу одну новую <code>community</code> . |

| Команда | Назначение |
|--|--|
| <code>ext-comm-list { add delete } EXTCOMMLIST_NAME</code> | Добавить или удалить из анонса набор extended community, заданный соответствующим правилом <code>ip-extcommunity EXTCOMMLIST_NAME</code> . |
| <code>extcommunity remove-all</code> | Удалить все extended community из анонса. |
| <code>extcommunity remove-all-and-set { rt soo } value { AS:Nr(0-65535:0-4294967295, 0-4294967295:0-65535) IPv4:Nr(0-65535) }</code> | Удалить все extcommunity из анонса и установить указанную RT- или SOO-extcommunity. |
| <code>extcommunity set-specific { rt soo } value { AS:Nr(0-65535:0-4294967295, 0-4294967295:0-65535) IPv4:Nr(0-65535) }</code> | Добавить указанную RT- или SOO-extcommunity. |
| <code>local-preference LOCALPREF</code> | Установить соответствующее значение параметра BGP Local Preference. |
| <code>med value MED</code> | Установить соответствующее значение параметра BGP MED. |
| <code>nexthop IPv4_ADDR IPv6_ADDR</code> | Установить соответствующее значение BGP Nexthop |
| <code>prepend as-path ASN</code> <code>prepend times N</code> | Установить препенды на параметр AS-PATH, состоящие из номера автономной системы ASN, повторенные N раз. |
| <code>remove as-path ASN</code> | Удалить из AS-PATH данного анонса указанные номера автономных систем ASN. |
| <code>remove private-as</code> | Удалить из AS-PATH данного анонса все приватные номера автономных систем (RFC6996). |
| <code>weight value WEIGHT</code> | Установить параметр weight. |

Условия соответствия анонсов

Условия соответствия анонсов задаются внутри элементов карты маршрутов при помощи команды `'match'`. Виды условий соответствия приведены в таблице.

Таблица 42. Виды условий соответствия анонсов `'set'`.

| Команда | Назначение |
|--|--|
| <code>as-path AS_REGEX</code> | Проверка AS-PATH анонса на соответствие приведенному регулярному выражению <code>AS_REGEX</code> . Допустимая длина регулярного выражения — до 300 символов. |
| <code>comm-list name COMMLIST_NAME</code> | Проверка перечня community в анонсе на соответствие заданному community-фильтру (фильтр должен быть создан командой " <code>ip-community COMMLIST_NAME</code> ") |
| <code>ext-comm-list name EXTCOMMLIST_NAME</code> | Проверка перечня расширенных community в анонсе на соответствие заданному extcommunity-фильтру (фильтр должен быть создан командой " <code>ip-extcommunity EXTCOMMLIST_NAME</code> ") |
| <code>prefix-list destination PREFLIST_NAME</code> | Проверка префикса анонса на соответствие указанному фильтру префиксов. Фильтр префиксов должен быть сконфигурирован отдельно командой " <code>prefix-list PREFLIST_NAME</code> ". |
| <code>prefix-list nexthop PREFLIST_NAME</code> | Проверка параметра BGP nexthop анонса на соответствие указанному фильтру префиксов. Фильтр префиксов должен быть сконфигурирован отдельно командой " <code>prefix-list PREFLIST_NAME</code> ". |
| <code>prefix-list source PREFLIST_NAME</code> | Проверка адреса BGP-спикера, от которого получен анонс, на соответствие указанному фильтру префиксов. Фильтр префиксов должен быть сконфигурирован отдельно командой " <code>prefix-list PREFLIST_NAME</code> ". |

Internal BGP и External BGP

Согласно спецификациям протокола, BGP-сессии делятся на два типа — внутренние BGP-сессии (*Internal BGP, iBGP*) и внешние BGP-сессии (*External BGP, eBGP*).

- Внутренняя BGP-сессия — это сессия между BGP-спикерами одной автономной системы;
- Внешняя BGP-сессия — это сессия между BGP-спикерами разных автономных систем.

Маршрутизаторы серии ME определяют тип сессии автоматически, сопоставляя номер своей автономной системы с номером автономной системы соседа.

Основные отличительные особенности iBGP-сессий:

1. При анонсировании пути по такой сессии не изменяется параметр BGP nexthop;
2. Анонсы, полученные по одной iBGP-сессии, BGP-спикер объявляет только eBGP-

соседям, но не другим iBGP-соседям.

Для управления данным поведением существуют команды-директивы `'next-hop-self'` и `'route-reflector-client'`. Первая команда принудительно задает в объявляемых анонсах свой IP-адрес в качестве параметра BGP nexthop. Вторая команда включает передачу соответствующему iBGP-соседу анонсов, полученных от других iBGP-соседей.

Пример. Использование команд 'next-hop-self' и 'route-reflector-client'.

```
router bgp 65535
  neighbor 2.2.2.2
    address-family ipv4 unicast
      next-hop-self
      route-map in STANDART-CLIENT
      prefix-list out ANY
    exit
  remote-as 65535
  route-reflector-client
exit
```

Административная дистанция протокола BGP

Административная дистанция — это параметр, определяющий приоритет всех маршрутов, получаемых из соответствующего источника. Если один и тот же маршрут система получает из разных источников (например, из протокола динамической маршрутизации и из статически прописанного маршрута), то будет выбираться маршрут из источника с меньшей административной дистанцией. В указанном примере по умолчанию будет выбран статический маршрут.

Значения административной дистанции по умолчанию приведены в таблице (при принятии решения меньшее значение является лучшим):

Таблица 43. Значения административной дистанции.

| Протокол/источник | Административная дистанция | Приоритет |
|-------------------------------------|----------------------------|-----------|
| Присоединенные (connected) маршруты | 0 | 1 |
| Статические (static) маршруты | 1 | 2 |
| External BGP | 20 | 3 |
| OSPF | 110 | 4 |
| IS-IS Level-1 | 115 | 5 |
| IS-IS Level-2 | 116 | 6 |

| Протокол/источник | Административная дистанция | Приоритет |
|-------------------|----------------------------|-----------|
| Internal BGP | 120 | 7 |

Значения административной дистанции можно изменить.

Таблица 44. Настройка административной дистанции для протокола BGP.

| Команда | Назначение |
|------------------------------------|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>router admin-distance</code> | Переход в режим настройки раздела административной дистанции протоколов. |
| <code>bgp external 0..255</code> | Задание значения административной дистанции для маршрутов eBGP. |
| <code>bgp internal 0..255</code> | Задание значения административной дистанции для маршрутов iBGP. |
| <code>root</code> | Возврат в режим глобальной конфигурации |
| <code>commit</code> | Применение произведенных настроек. |

Пример. Изменение административной дистанции для eBGP.

```
router admin-distance
  bgp external 112
exit
```

NOTE

Значения административной дистанции, заданные по умолчанию, являются оптимальными. Не следует изменять их без явной необходимости.

НАСТРОЙКА MPLS-КОММУТАЦИИ И ПРОТОКОЛА LDP

В данной главе рассматриваются принципы настройки инфраструктуры MPLS (Multiprotocol Label Switching) и протокола LDP.

Необходимые шаги

Для подготовки инфраструктуры MPLS в качестве транспорта для L2VPN- и L3VPN-сервисов требуется произвести следующие действия:

1. Определить интерфейсы, которые будут использоваться для соединения с соседними MPLS-маршрутизаторами;
2. Настроить на устройстве и на соответствующих интерфейсах требуемый протокол IGP (OSPF либо IS-IS);
3. Настроить на устройстве и на соответствующих интерфейсах протокол LDP для распространения транспортных MPLS-меток.

Конечным результатом настройки является наличие транспортных меток в таблице *mpls ldp forwarding*:

Пример. Вывод `'show mpls ldp forwarding'`:

```
0/ME5100:Router# show mpls ldp forwarding
```

```
Codes:
```

```
  R = Remote LFA FRR backup
```

| Prefix | Label(s) out | Outgoing Interface | Next Hop | flags |
|------------|--------------|--------------------|--------------|-------|
| 2.2.2.2/32 | ImpNull | te 0/0/5 | 100.100.12.1 | |
| 4.4.4.4/32 | ImpNull | te 0/0/7 | 100.100.14.0 | |

```
0/ME5100:Router#
```

Предварительная настройка IGP

Настройка протоколов внутреннего шлюза IGP (IS-IS и OSPF) описана в соответствующих разделах данного руководства. В общем случае требуется провести базовую конфигурацию и включение IGP на интерфейсах к соседним маршрутизаторам.

Помимо этого, необходимо выбрать на устройстве loopback-интерфейс в глобальной таблице маршрутизации, адрес которого будет использоваться в качестве router-id для протоколов IGP и LDP, и также включить его в процесс маршрутизации IGP (желательно в пассивном режиме).

```
interface tengigabitethernet 0/0/5
  mtu 9192
  description "to AR2(2.2.2.2) te 0/0/5"
  ipv4 address 100.100.12.0/31
exit

interface tengigabitethernet 0/0/7
  mtu 9192
  description "to DR1(4.4.4.4) te 0/1/7"
  ipv4 address 100.100.14.1/31
exit

interface loopback 1
  ipv4 address 1.1.1.1/32
  description "Main loopback"
exit

router isis eltex-test
  is-level level-2
  net 49.0001.0010.0100.1001.00
  host-name Router
  level level-2
  metric-style wide
exit
interface tengigabitethernet 0/0/5
  point-to-point
  hello-padding adaptive
  ldp-igp-synchronization
  address-family ipv4 unicast
  exit
exit
interface tengigabitethernet 0/0/7
  point-to-point
  hello-padding adaptive
  address-family ipv4 unicast
  exit
exit
interface loopback 1
  passive
  address-family ipv4 unicast
  exit
exit
exit
```

В процессе настройки протокола LDP необходимо проверить наличие в таблице маршрутизации всех путей, для которых предполагается выделение транспортных меток. Транспортные метки будут выделены только для тех путей, которые имеют корректные маршруты в IGP и для которых получены соответствующие LDP Label Mapping.

Настройка протокола LDP

Для запуска и настройки протокола LDP необходимо:

1. Задать router-id для LDP (рекомендуется выбрать "основной" loopback-интерфейс и в качестве Router ID взять его адрес, команда `'mpls ldp router-id'`);
2. Включить на интерфейсах в сторону соседей процесс автообнаружения LDP (командами `'mpls ldp discovery interface'`);
3. Включить на интерфейсах в сторону соседей процесс MPLS-коммутации (командами `'mpls forwarding interface'`);
4. Включить в протокол LDP соответствующие loopback-интерфейсы устройства (командами `'mpls forwarding interface'`).

IMPORTANT

Маршрутизаторы серии ME анонсируют соседям по LDP только свои loopback-интерфейсы, включенные в LDP командой `'mpls forwarding interface'`. В случае, если дизайн сети предполагает анонс в LDP также и адресов сетей обычных интерфейсов, требуется отдельная настройка редистрибуции connected-сетей командой `'mpls ldp address-family ipv4 unicast redistribution connected'`.

Таблица 45. Базовая настройка LDP.

| Команда | Назначение |
|---|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>mpls ldp discovery interface { tengigabitethernet bundle-ether } num</code> | Добавление соответствующего интерфейса (либо сабинтерфейса) в процесс автообнаружения LDP и переход в режим настройки параметров LDP для данного интерфейса. |
| <code>bfd fast-detect</code> | (опционально) Включение протокола BFD для обнаруженных соседей на данном интерфейсе. |
| <code>shutdown</code> | (опционально) Деактивация LDP discovery на интерфейсе. |
| <code>exit</code> | Возврат в режим глобальной конфигурации. |
| <code>mpls ldp router-id IPv4_ADDR</code> | Задание Router ID для процесса LDP. |

| Команда | Назначение |
|---|--|
| <code>mpls ldp penultimate-hop-popping disable</code> | (опционально) Отключение механизма MPLS PHP (снятия транспортной метки на предпоследнем маршруте). IMPORTANT Для применения данной настройки потребуется вручную переустановить LDP-сессии с соседями. |
| <code>mpls ldp transport-address IPv4_ADDR</code> | (опционально) Задание транспортного адреса для протокола LDP. Рекомендуется явно конфигурировать данный адрес. |
| <code>mpls ldp neighbor IPv4_ADDR</code> | Создание в конфигурации targeted-сессии с указанным соседом и переход в режим настройки этой сессии. NOTE Создание targeted-сессий требуется только в случае использования L2VPN с LDP-сигнализацией, см.соответствующий раздел Руководства. |
| <code>hello-holdtime SECONDS</code> <code>holdtime-interval SECONDS</code> | (Опционально) Настройка соответствующих таймеров на targeted-сессии. |
| <code>bfd fast-detect</code> | (Опционально) Включение на данной targeted-сессии протокола BFD. |
| <code>shutdown</code> | (Опционально) Административное отключение данной targeted-сессии. |
| <code>exit</code> | Возврат в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

Таблица 46. Включение коммутации MPLS на интерфейсах.

| Команда | Назначение |
|---|---|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>mpls forwarding interface { loopback tengigabitethernet bundle-ether } num</code> | Включение MPLS-коммутации на данном интерфейсе либо сабинтерфейсе. Обязательно включение в данный список также тех loopback-интерфейсов, которые планируется анонсировать соседям по LDP. |

| Команда | Назначение |
|---------------------|------------------------------------|
| <code>commit</code> | Применение произведенных настроек. |

Пример. Настройка MPLS LDP на двух интерфейсах.

```
mpls ldp router-id 1.1.1.1
mpls ldp transport-address 1.1.1.1
mpls ldp neighbor 2.2.2.2
  bfd fast-detect
exit
mpls ldp neighbor 4.4.4.4
  bfd fast-detect
exit
mpls ldp discovery interface tengigabitethernet 0/0/5
exit
mpls ldp discovery interface tengigabitethernet 0/0/7
exit
mpls forwarding interface tengigabitethernet 0/0/5
mpls forwarding interface tengigabitethernet 0/0/7
mpls forwarding interface loopback 1
```

LDP-IGP синхронизация

Для сетей, использующих LDP, имеется вспомогательный механизм, помогающий избежать ошибочного направления трафика в неработоспособное соединение (*blackhole*). Данный механизм называется синхронизацией LDP-IGP и предназначен для использования на тех соединениях, где должны одновременно работать LDP и протоколы IGP.

Механизм и принципы его работы описаны в RFC5443 ("*LDP IGP Synchronization*").

Суть работы данного механизма заключается в том, что при отсутствии активных LDP-соседей на том интерфейсе, где они быть должны, протокол IGP (IS-IS или OSPF) автоматически увеличивает стоимость данного интерфейса с целью максимально надежно исключить его из путей прохождения трафика.

Этот механизм позволяет исключить ситуации, когда из-за ошибки в конфигурации или сбоях в работе систем трафик будет направляться в соединения, на которых продолжает работать IGP, но перестал работать LDP.

Включение данного механизма производится поинтерфейсно в конфигурационных блоках протоколов IS-IS или OSPF командой '`ldp-igp-synchronization`'.

Пример. Включение LDP-IGP синхронизации на интерфейсе протокола IS-IS:

```
router isis eltex-test
  interface tengigabitethernet 0/0/5
    ldp-igp-synchronization
  exit
exit
```

Пример. Включение LDP-IGP синхронизации на интерфейсе протокола OSPFv2:

```
router ospfv2 test
  area 0.0.0.0
  interface bundle-ether 7.400
    ldp-igp-synchronization
  exit
exit
exit
```

Включение в LDP дополнительных интерфейсов (редистрибуция)

По умолчанию протокол LDP формирует label mappings только для адресов loopback-интерфейсов системы.

В случае, если дизайн сети предполагает анонс в LDP также и адресов сетей обычных интерфейсов (а также маршрутов, полученных от BGP), требуется отдельная настройка редистрибуции connected-сетей командой `'mpls ldp address-family ipv4 unicast redistribution connected'`.

Таблица 47. Редистрибуция в LDP.

| Команда | Назначение |
|--|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>mpls ldp address-family ipv4 unicast redistribution { connected bgp } RULE_NAME</code> | Создание правила редистрибуции с именем <i>RULE_NAME</i> из указанного источника (bgp/connected) и переход в режим настройки этого правила. |
| <code>match prefix IPv4PREFIX/MASK</code> | (опционально) Указание фильтра, используемого для данного правила. При указании такого фильтра правило будет действовать только на маршруты, строго совпадающие с заданным <i>IPv4PREFIX/MASK</i> . |

| Команда | Назначение |
|--|--|
| <code>priority</code> <i>RULE_PRIORITY</i> | Установить приоритет данного правила редистрибуции. Правила редистрибуции выполняются по очереди от низкого значения приоритета к высокому и срабатывают по первому вхождению. Таким образом, маршрут, попавший, например, в первое правило, будет передан в LDP согласно настроек этого правила и не будет обрабатываться последующими правилами. |
| <code>redistribute disable</code> | Запретить редистрибуцию маршрутов, попавших в текущее правило. При выполнении данной команды текущее правило становится запрещающим. |
| <code>exit</code> | Выход из режима настройки правила редистрибуции. Далее можно настроить следующие правила — для того же самого источника, либо для других источников редистрибуции. |
| <code>root</code> | Возврат в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

Пример. Настройка редистрибуции, которая позволит LDP объявлять метки для connected-сетей всех интерфейсов, за исключением 100.100.12.0/31.

```
mpls ldp address-family ipv4 unicast redistribution connected LDP-CONN10
  priority 10
  redistribute disable
  match prefix 100.100.12.0/31
exit
mpls ldp address-family ipv4 unicast redistribution connected LDP-CONN20
  priority 20
exit
```

Проверка работы протокола LDP и диагностические команды

`show mpls ldp bindings`

Команда выводит локальные ('*local*') и удаленные ('*remote*') FEC/метки. Доступны фильтры по меткам, соседям или префиксу FEC.

Пример. show mpls ldp bindings remote

```
0/ME5100:Router# show mpls ldp bindings remote

2.2.2.2/32
  local binding: 2.2.2.2:0, label 3
  State: mapping-established, type: prefix
  Interface: Tengigabitethernet 0/0/5
2.2.2.2/32
  local binding: 4.4.4.4:0, label 821
  State: mapping-liberally-retained, type: prefix
  Interface:
2.2.2.255/32
  local binding: 2.2.2.2:0, label 3
  State: mapping-liberally-retained, type: prefix
  Interface:
4.4.4.4/32
  local binding: 2.2.2.2:0, label 426
  State: mapping-liberally-retained, type: prefix
  Interface:
4.4.4.4/32
  local binding: 4.4.4.4:0, label 3
  State: mapping-established, type: prefix
  Interface: Tengigabitethernet 0/0/7
0/ME5100:Router#
```

show mpls ldp forwarding

Команда выводит таблицу активных LSP. Доступны фильтры по nexthop и по префиксу назначения.

Пример. show mpls ldp forwarding

```
0/ME5100:Router1# show mpls ldp forwarding

Codes:
  R = Remote LFA FRR backup

Prefix          Label(s) out  Outgoing Interface  Next Hop          flags
-----
2.2.2.2/32      437           te 0/0/5            100.100.12.1
4.4.4.4/32      ImpNull       te 0/0/7            100.100.14.0
0/ME5100:Router1#
```

show mpls ldp igp sync

Вывод состояния LDP-IGP синхронизации на интерфейсах.

Пример. show mpls ldp igp sync.

```
0/ME5100:Router1# show mpls ldp igp sync
```

```
Thu Jan 24 16:35:03 2019
```

```
LDP-ISIS sync
```

| Interface | LDP state | Metric |
|-----------|-----------|---------|
| te 0/0/5 | up | normal |
| te 0/0/6 | down | maximum |

```
LDP-OSPF sync
```

```
0/ME5100:Router1#
```

show mpls ldp neighbors

Вывод перечня, состояния и статистики по LDP-соседям системы.

Пример. show mpls ldp neighbors.

```
0/ME5100:Router# show mpls ldp neighbors
```

```
Peer LDP Identifier: 2.2.2.2:0
  Current state: operational, role: passive
  TCP connection: 2.2.2.2
  Label distribution method: downstream-unsolicited
  Loop Dection for Path Vectors limits: 0
  Last state change: 01h18m37s ago
  Discontinuity time: 01h18m52s ago
  LDP 1 Protocol is using
    The negotiated KeepAlive time: 7 secs
    Configured hold time: 40 secs
    The peer's advertised keepalive hold time: 40 secs
    Currently keepalive hold use: 40 secs
    Peer reconnect time: 0 secs, recovery time: 0 secs
  Maximum allowable length for LDP PDUs: 4096 octets
  Graceful Restart support: peer is false, local is false
  Stats:
    0 unknown message count, 0 unknown tlv count
  Neighbors in current session:
    Peer address index: 2, next hop address: 2.2.2.255
    Peer address index: 1, next hop address: 2.2.2.2
    Peer address index: 4, next hop address: 100.100.24.1
    Peer address index: 3, next hop address: 100.100.12.1

Peer LDP Identifier: 4.4.4.4:0
  Current state: operational, role: passive
  TCP connection: 4.4.4.4
  Label distribution method: downstream-unsolicited
  Loop Dection for Path Vectors limits: 0
  Last state change: 01h18m35s ago
  Discontinuity time: 01h18m51s ago
  LDP 1 Protocol is using
    The negotiated KeepAlive time: 7 secs
    Configured hold time: 40 secs
    The peer's advertised keepalive hold time: 40 secs
    Currently keepalive hold use: 40 secs
    Peer reconnect time: 0 secs, recovery time: 0 secs
  Maximum allowable length for LDP PDUs: 4096 octets
  Graceful Restart support: peer is false, local is false
  Stats:
    0 unknown message count, 0 unknown tlv count
  Neighbors in current session:
    Peer address index: 2, next hop address: 100.100.14.0
    Peer address index: 3, next hop address: 100.100.24.0
    Peer address index: 1, next hop address: 4.4.4.4
```

show mpls ldp parameters

Вывод информации об имеющихся соседях и задействованных в LDP интерфейсах системы.

Пример. show mpls ldp parameters.

```
0/ME5100:Router# show mpls ldp parameters

LDP Parameters:
  Router ID: 1.1.1.1
  Transport address: 1.1.1.1
Graceful Restart:
  Status: disabled
  Reconnect Timeout: 200 sec, Forwarding State Holdtime: 200 sec

Neighbors:

Peer address: 2.2.2.2
  BFD status: enabled
  Holdtime interval: 40 sec
  Hello interval: 0 sec

Peer address: 4.4.4.4
  BFD status: enabled
  Holdtime interval: 40 sec
  Hello interval: 0 sec

Interfaces:

Interface Tengigabitethernet 0/0/5
  BFD status: disabled
  Holdtime interval: 40 sec
  Hello interval: 15 sec

Interface Tengigabitethernet 0/0/6
  BFD status: disabled
  Holdtime interval: 40 sec
  Hello interval: 15 sec

Interface Tengigabitethernet 0/0/7
  BFD status: disabled
  Holdtime interval: 40 sec
  Hello interval: 15 sec
```


НАСТРОЙКА MPLS L3VPN

В данной главе рассматриваются принципы организации и настройки виртуальных частных сетей третьего уровня (Layer 3 VPN, L3VPN), использующих в качестве транспорта технологию MPLS.

Под сервисом L3VPN здесь и далее подразумевается обособленное пространство маршрутизации (с использованием протоколов семейства IP). Такое пространство имеет собственную таблицу маршрутизации, таблицу ARP/ND и отдельный список L3-интерфейсов, включенных в него. Сервис L3VPN позволяет узлам, подключенным к его интерфейсам, передавать IP-трафик между (и только между) собой.

Необходимые шаги

Для обеспечения работы сервиса MPLS L3VPN требуется выполнить следующие действия:

1. Настроить инфраструктуру распространения транспортных меток (см. главу "Настройка MPLS-коммутации и протокола LDP"), то есть обеспечить связность с другими устройствами сети;
2. Создать и настроить на маршрутизаторе экземпляр VRF, включить в этот экземпляр требуемые интерфейсы;
3. Обеспечить передачу маршрутной информации данного экземпляра VRF к другим устройствам сети при помощи протокола MP-BGP с использованием адресного семейства VPNv4 unicast.

Конечным результатом настройки является появление связности между узлами, подключенными к VRF на различных маршрутизаторах сети (то есть объединение VRF на разных маршрутизаторах через MPLS-транспорт). При этом должна быть обеспечена передача сервисных MPLS-меток для сервиса L3VPN посредством MP-BGP и передача транспортных меток для достижения nexthop-адресов полученных BGP-маршрутов.

Создание экземпляров VRF и технология VRF Lite

Для работы сервиса L3VPN необходимо создать в конфигурации устройства экземпляр VRF и включить в него требуемые интерфейсы.

В случае, если VRF применяется только на одном маршрутизаторе, технология имеет название VRF Lite ("облегченный" VRF).

Таблица 48. Создание и настройка экземпляра VRF.

| Команда | Назначение |
|------------------------|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |

| Команда | Назначение |
|---|--|
| <code>vrf VRF_NAME</code> | Создание в конфигурации устройства экземпляра VRF с именем <code>VRF_NAME</code> и переход в режим настройки этого экземпляра. |
| <code>rd RD</code> | Задание Route Distinguisher для данного экземпляра VRF. Параметр является обязательным при создании VRF. Допустимые формы задания: <ul style="list-style-type: none"> • ASN:Nr — со значениями [0..65535]:[0..4294967295], [0..4294967295]:[0..65535]; • IPv4:Nr — со значениями A.B.C.D:[0..65535]; здесь в качестве IPv4-адреса рекомендуется применять адрес основного loopback-интерфейса маршрутизатора. |
| <code>maximum prefix MAX_ROUTES</code> | (опционально) Установка ограничения количества маршрутов внутри экземпляра VRF. |
| <code>import route-target RT_COMMUNITY_VALUE</code> | (опционально) Установка перечня значений route-target extended community, VPNv4 BGP-пути с которыми будут устанавливаться в таблицу маршрутизации экземпляра VRF (см. ниже раздел "Route-target и Route Distinguisher"). Формат задания <code>RT_COMMUNITY_VALUE</code> аналогичен формату параметра <code>RD</code> . |
| <code>export route-target RT_COMMUNITY_VALUE</code> | (опционально) Установка перечня значений route-target extended community, с которыми маршруты из данного экземпляра VRF будут анонсироваться в VPNv4 BGP (см. ниже раздел "Route-target и Route Distinguisher"). Формат задания <code>RT_COMMUNITY_VALUE</code> аналогичен формату параметра <code>RD</code> . |
| <code>description STRING</code> | (опционально) Задание строкового описания экземпляра VRF. |
| <code>root</code> | Возврат в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

NOTE

После создания и настройки экземпляра VRF можно добавлять в него интерфейсы.

Пример. Настройка экземпляра VRF с двумя интерфейсами в нём. Настройка производится на устройстве Router1.

```
vrf example
  description "Example L3VPN service"
  rd 1.1.1.1:100
  import route-target 65535:100
  export route-target 65535:100
exit

interface tengigabitethernet 0/0/17.1100
  vrf example
  description "CE interface 1 on Router1"
  ipv4 address 100.100.1.1/24
  encapsulation outer-vid 1100
exit
interface tengigabitethernet 0/0/17.1200
  vrf example
  description "CE interface 2 on Router1"
  ipv4 address 100.100.2.1/24
  encapsulation outer-vid 1200
exit
```

Пример. Диагностика созданного экземпляра — общая информация, таблица маршрутов и ARP-таблица.

```
0/ME5100:Router1# show vrf example
```

| VRF | RD | Interface |
|---------|-------------|----------------|
| example | 1.1.1.1:100 | te 0/0/17.1100 |
| example | 1.1.1.1:100 | te 0/0/17.1200 |

```
0/ME5100:Router1# show route vrf example
```

Codes: C - connected, S - static, O - OSPF, B - BGP, L - local
IA - OSPF inter area, EA - OSPF intra area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
LE1 - IS-IS level1 external, LE2 - IS-IS level2 external
BI - BGP internal, BE - BGP external, BV - BGP vpn

| | | |
|---|----------------|--|
| C | 100.100.1.0/24 | is directly connected, 00h01m12s, te 0/0/17.1100 |
| L | 100.100.1.1/32 | is directly connected, 00h01m12s, te 0/0/17.1100 |
| C | 100.100.2.0/24 | is directly connected, 00h01m12s, te 0/0/17.1200 |
| L | 100.100.2.1/32 | is directly connected, 00h01m12s, te 0/0/17.1200 |

Total route count: 4

```
0/ME5100:Router1# show arp vrf example
```

ARP aging time is 240 minutes

| IP address | Age | Hardware address | State | Interface |
|-------------|----------|-------------------|-----------|----------------|
| 100.100.1.1 | 00:00:00 | a8:f9:4b:8b:bb:b1 | Interface | te 0/0/17.1100 |
| 100.100.2.1 | 00:00:00 | a8:f9:4b:8b:bb:b1 | Interface | te 0/0/17.1200 |

```
0/ME5100:Router1#
```

В качестве иллюстрации для дальнейшей настройки приведем также пример создания такого же экземпляра VRF на другом маршрутизаторе.

Пример. Настройка экземпляра VRF с одним интерфейсом. Настройка производится на устройстве Router2.

```
interface tengigabitethernet 0/0/17.1300
  vrf example
  description "CE interface 1 on Router2"
  ipv4 address 100.100.3.1/24
  encapsulation outer-vid 1300
exit
vrf example
  description "Example L3VPN service"
  rd 2.2.2.2:100
  import route-target 65535:100
  export route-target 65535:100
exit
```

Пример. Маршруты в экземпляре VRF на Router2.

```
0/ME5100:Router2# show route vrf example
Tue Jan 29 13:35:25 2019
Codes: C - connected, S - static, O - OSPF, B - BGP, L - local
       IA - OSPF inter area, EA - OSPF intra area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       LE1 - IS-IS level1 external, LE2 - IS-IS level2 external
       BI - BGP internal, BE - BGP external, BV - BGP vpn

C       100.100.3.0/24      is directly connected, 00h01m21s, te 0/0/17.1300
L       100.100.3.1/32     is directly connected, 00h01m21s, te 0/0/17.1300

Total route count: 2
```

Настройка MP-BGP

Для передачи маршрутной информации L3VPN на другие устройства сети необходимо использовать протокол MP-BGP. Информация о маршрутах L3VPN будет объявляться BGP-соседам по сессиям с адресным семейством VPNv4 unicast.

Таким образом, на устройстве должен быть предварительно запущен и сконфигурирован процесс маршрутизации BGP, после чего можно добавлять необходимых соседей.

Таблица 49. Настройка BGP-соседа для передачи маршрутов L3VPN.

| Команда | Назначение |
|------------------------|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |

| Команда | Назначение |
|---|---|
| <code>router bgp ASN</code> | Переход в режим настройки процесса маршрутизации. |
| <code>neighbor A.B.C.D</code> | Создание протокольного соседа в глобальной таблице маршрутизации и переход в режим настройки его параметров. IMPORTANT Передача маршрутной информации L3VPN возможна только соседям в глобальной таблице маршрутизации. |
| <code>description "STRING"</code> | (опционально) Задание текстовой строки — описания протокольного соседа. |
| <code>remote-as ASN</code> | Задаёт номер автономной системы BGP-соседа. L3VPN-сессии поддерживаются только для iBGP-соседей. |
| <code>send-community</code> | Включает отправку параметра <i>community</i> в отсылаемых соседу анонсах. По умолчанию параметры <i>community</i> удаляются из отправляемых анонсов. Для корректной работы L3VPN отправку <i>extended community</i> рекомендуется включать. |
| <code>send-community-ext</code> | Включает отправку параметра <i>extended community</i> в отсылаемых соседу анонсах. По умолчанию параметры <i>extended community</i> удаляются из отправляемых анонсов. Для корректной работы L3VPN отправку <i>extended community</i> необходимо включать . |
| <code>address-family vpnv4 unicast</code> | Включение на данном соседе адресного семейства VPNv4 unicast (обязательно для работы L3VPN/IPv4) и переход в режим настроек данного семейства. Внутри семейства при необходимости можно провести соответствующую настройку политик маршрутизации для передачи/приема анонсов от текущего BGP-соседа. |
| <code>exit</code> | Возврат в режим настроек BGP-соседа. |
| <code>update-source IPv4_ADDR</code> | Задание IPv4-адреса, с которого будет производиться взаимодействие с соседом. Данный параметр рекомендуется всегда указывать для iBGP-сессий. |
| <code>root</code> | Выход в режим глобальной конфигурации. |

| Команда | Назначение |
|---------------------|------------------------------------|
| <code>commit</code> | Применение произведенных настроек. |

Пример. Настройка MP-BGP сессии между Router1 и Router2, конфигурация Router1:

```
router bgp 65535
  bgp router-id 1.1.1.1
  neighbor 2.2.2.2
    address-family vpnv4 unicast
  exit
  remote-as 65535
  send-community
  send-community-ext
  update-source 1.1.1.1
exit
```

Пример. Настройка MP-BGP сессии между Router1 и Router2, конфигурация Router2:

```
router bgp 65535
  bgp router-id 2.2.2.2
  neighbor 1.1.1.1
    address-family vpnv4 unicast
  exit
  remote-as 65535
  send-community
  send-community-ext
  update-source 2.2.2.2
exit
```

Пример. Контроль установления BGP-сессии с соответствующими AFI/SAFI:

```
0/ME5100:Router1# show bgp vpnv4 unicast summary
```

```
BGP router identifier 1.1.1.1, local AS number 12389
```

```
Graceful Restart is disabled
```

```
BGP table state: active
```

```
BGP scan interval: 120 secs
```

| Neighbor St/PfxRcd | AS | MsgRcvd | MsgSent | Up/Down |
|-----------------------|-------|---------|---------|-------------|
| ----- | | | | |
| ----- | | | | |
| 2.2.2.2 | 12389 | 54452 | 54462 | 04d22h20m 1 |

```
0/ME5100:Router1#
```

```
0/ME5100:Router2# show bgp vpnv4 unicast summary
```

```
BGP router identifier 2.2.2.2, local AS number 12389
```

```
Graceful Restart is disabled
```

```
BGP table state: active
```

```
BGP scan interval: 120 secs
```

| Neighbor St/PfxRcd | AS | MsgRcvd | MsgSent | Up/Down |
|-----------------------|-------|---------|---------|-------------|
| ----- | | | | |
| ----- | | | | |
| 1.1.1.1 | 12389 | 54469 | 54469 | 04d22h23m 2 |

```
0/ME5100:Router2#
```


Пример. Просмотр полученных по VPNv4 unicast BGP-анонсов:

```
0/ME5100:Router1# show bgp vpnv4 unicast neighbors 2.2.2.2 routes
```

```
BGP router identifier 1.1.1.1, local AS number 12389
Graceful Restart is disabled
BGP table state: active
BGP scan interval: 120 secs
```

```
Status codes: d damped, h history, > best, S stale, * active, u untracked, i
internal
```

```
Origin codes: i igp, e egp, ? incomplete
```

```
Received bgp routes from neighbor: 2.2.2.2
```

| Route LocPrf | Distinguisher Weight | IP Prefix Path | Next hop | Metric | Label | |
|-----------------|-------------------------|-------------------|----------|--------|-------|-----|
| u>i 0 | 2.2.2.2:100 ? | 100.100.3.0/24 | 2.2.2.2 | 0 | 34 | 100 |

```
Total paths: 1
```

```
0/ME5100:Router2# show bgp vpnv4 unicast neighbors 1.1.1.1 routes
```

```
BGP router identifier 2.2.2.2, local AS number 12389
Graceful Restart is disabled
BGP table state: active
BGP scan interval: 120 secs
```

```
Status codes: d damped, h history, > best, S stale, * active, u untracked, i
internal
```

```
Origin codes: i igp, e egp, ? incomplete
```

```
Received bgp routes from neighbor: 1.1.1.1
```

| Route LocPrf | Distinguisher Weight | IP Prefix Path | Next hop | Metric | Label | |
|-----------------|-------------------------|-------------------|----------|--------|-------|-----|
| u>i 0 | 1.1.1.1:100 ? | 100.100.1.0/24 | 1.1.1.1 | 0 | 67 | 100 |
| u>i 0 | 1.1.1.1:100 ? | 100.100.2.0/24 | 1.1.1.1 | 0 | 67 | 100 |

```
Total paths: 2
```

Пример. Просмотр маршрутов, установленных в таблицу маршрутизации экземпляра VRF — Router1.

```
0/ME5100:Router1# show route vrf example

Codes: C - connected, S - static, O - OSPF, B - BGP, L - local
       IA - OSPF inter area, EA - OSPF intra area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       LE1 - IS-IS level1 external, LE2 - IS-IS level2 external
       BI - BGP internal, BE - BGP external, BV - BGP vpn

C      100.100.1.0/24    is directly connected, 01h54m07s, te 0/0/17.1100
L      100.100.1.1/32   is directly connected, 01h54m07s, te 0/0/17.1100
C      100.100.2.0/24    is directly connected, 01h54m07s, te 0/0/17.1200
L      100.100.2.1/32   is directly connected, 01h54m07s, te 0/0/17.1200
B BV   100.100.3.0/24    via 2.2.2.2 [200/0], 01h09m21s

Total route count: 5
```

Пример. Просмотр маршрутов, установленных в таблицу маршрутизации экземпляра VRF — Router2.

```
0/ME5100:Router2# show route vrf example

Codes: C - connected, S - static, O - OSPF, B - BGP, L - local
       IA - OSPF inter area, EA - OSPF intra area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       LE1 - IS-IS level1 external, LE2 - IS-IS level2 external
       BI - BGP internal, BE - BGP external, BV - BGP vpn

B BV   100.100.1.0/24    via 1.1.1.1 [200/0], 01h11m03s
B BV   100.100.2.0/24    via 1.1.1.1 [200/0], 01h11m03s
C      100.100.3.0/24    is directly connected, 01h11m03s, te 0/0/17.1300
L      100.100.3.1/32   is directly connected, 01h11m03s, te 0/0/17.1300

Total route count: 4
```

Установка BGP-путей в качестве маршрутов экземпляра VRF

Различие между параметрами RT и RD

При корректной конфигурации полученные по BGP анонсы имеют параметры *Route Distinguisher (RD)* и *Route-Target (RT)*. Оба эти параметра имеют одинаковый формат, однако выполняют разные задачи.

- *RD* является частью информации MP-REACH NLRI и служит для изоляции различных плоскостей форвардинга (например, разных VRF) друг от друга.
- *RT* является расширенным community и используется конечными маршрутизаторами при импорте/экспорте маршрутов из/в VRF.

Параметр *RD* помогает разделить анонсы при передаче через транзитные BGP-спикеры к конечному маршрутизатору. Например, если в одном и том же сервисе L3VPN (т.е. в одном VRF) на промежуточный BGP-спикер придут два одинаковых маршрута с одинаковыми *RD*, то этот спикер проведет выбор лучшего среди них и анонсирует далее в сеть только лучший путь. Однако если эти маршруты будут иметь различные *RD*, то выбор лучшего среди них будет проводиться только конечными маршрутизаторами, которые на основании настроенных политик импорта *RT* проведут установку этих BGP-путей в качестве маршрутов внутри соответствующих VRF.

Дизайн услуг, при котором решение о лучшем пути принимается на конечном устройстве, является зачастую более предпочтительным, хотя и может привести к повышенному потреблению ресурсов транзитных BGP-спикеров.

Установка маршрутов внутри соответствующих VRF

В примерах ранее была приведена настройка, позволяющая получить по VPNv4-сессии анонсы маршрутов разных *RD*. В случае, если VRF на маршрутизаторах был настроен с одинаковыми политиками *import/export*, то эти анонсы будут установлены в таблицу маршрутизации соответствующих VRF.

Пример. Таблица маршрутизации VRF на маршрутизаторе Router1:

```
0/ME5100:Router1# show route vrf example

Codes: C - connected, S - static, O - OSPF, B - BGP, L - local
       IA - OSPF inter area, EA - OSPF intra area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       LE1 - IS-IS level1 external, LE2 - IS-IS level2 external
       BI - BGP internal, BE - BGP external, BV - BGP vpn

C       100.100.1.0/24      is directly connected, 02h38m30s, te 0/0/17.1100
L       100.100.1.1/32     is directly connected, 02h38m30s, te 0/0/17.1100
C       100.100.2.0/24     is directly connected, 02h38m30s, te 0/0/17.1200
L       100.100.2.1/32     is directly connected, 02h38m30s, te 0/0/17.1200
B BV    100.100.3.0/24     via 2.2.2.2 [200/0], 01h53m44s

Total route count: 5
0/ME5100:Router1#
```

Пример. Таблица маршрутизации VRF на маршрутизаторе Router2:

```
0/ME5100:Router2# show route vrf example

Codes: C - connected, S - static, O - OSPF, B - BGP, L - local
       IA - OSPF inter area, EA - OSPF intra area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       LE1 - IS-IS level1 external, LE2 - IS-IS level2 external
       BI - BGP internal, BE - BGP external, BV - BGP vpn

B BV    100.100.1.0/24     via 1.1.1.1 [200/0], 01h54m58s
B BV    100.100.2.0/24     via 1.1.1.1 [200/0], 01h54m58s
C       100.100.3.0/24     is directly connected, 01h54m58s, te 0/0/17.1300
L       100.100.3.1/32     is directly connected, 01h54m58s, te 0/0/17.1300

Total route count: 4
0/ME5100:Router2#
```

Таким образом, в данном примере маршруты были успешно установлены в таблицу маршрутизации VRF example. Обязательным условием для этого также является наличие транспортной метки до nexthop-адреса соответствующего маршрута:

Проверка наличия транспортных меток до nexthop на Router1:

```
0/ME5100:Router1# show mpls ldp forwarding | include 2.2.2.2  
  
2.2.2.2/32          ImpNull          te 0/0/5          100.100.12.1  
0/ME5100:Router1#
```

Проверка наличия транспортных меток до nexthop на Router2:

```
0/ME5100:Router2# show mpls ldp forwarding | include 1.1.1.1  
  
1.1.1.1/32          ImpNull          te 0/0/5          100.100.12.0  
0/ME5100:Router2#
```

Процесс BGP для экземпляра VRF и редистрибуция маршрутов

Процесс BGP для VRF

На маршрутизаторах семейства ME существует понятие BGP-процесса в экземпляре VRF. Это понятие включает в себя отдельную структуру в работающей операционной системе устройства, занимающую некоторые ресурсы и выполняющую определенные действия.

Действия, которые позволяет производить BGP-процесс в экземпляре VRF:

1. Установка BGP-соседств внутри экземпляра VRF. Данная возможность относится именно к соседствам внутри VRF (т.н. сессии PE-CE), но не к L3VPN-соседствам в глобальной таблице маршрутизации.
2. Гибкая настройка редистрибуции маршрутной информации из VRF в AFI VPNv4 unicast.

Запуск BGP-процесса для экземпляра VRF производится автоматически при создании конфигурационного блока `'vrf VRF_NAME'` в разделе настройки `'router bgp'`.

В примере ниже для VRF `example` отдельного BGP-процесса не запущено, а для VRF `l3-1` такой процесс запущен; кроме этого, внутри VRF `'l3-1'` сконфигурирован BGP-сосед с адресом 172.16.0.1 и редистрибуция статических и присоединенных маршрутов.

```

vrf example
  description "Example L3VPN service"
  rd 2.2.2.2:100
  import route-target 65535:100
  export route-target 65535:100
exit

vrf l3-1
  rd 65535:1
  import route-target 65535:1
  export route-target 65535:1
exit

router bgp 65535
  bgp router-id 2.2.2.2
  neighbor 1.1.1.1
    address-family ipv4 unicast
    exit
    address-family vpnv4 unicast
    exit
  remote-as 12389
  send-community
  send-community-ext
  route-reflector-client
  update-source 2.2.2.2
exit
vrf l3-1
  address-family ipv4 unicast
    redistribution static STAT
    exit
    redistribution connected CONN
    exit
  exit
  bgp router-id 2.2.2.2
  neighbor 172.16.0.1
    address-family ipv4 unicast
    exit
    remote-as 65530
  exit
exit
exit

```

IMPORTANT

В случае, если для экземпляра VRF не требуется установления BGP-соседств и настройки редистрибуции маршрутов, для экономии ресурсов маршрутизатора **не рекомендуется** запускать BGP-процессы в VRF.

Создание отдельных процессов на больших конфигурациях (сотни VRF) может привести к чрезмерному потреблению ресурсов маршрутизатора.

NOTE

Когда процесс маршрутизации BGP не запущен внутри VRF, BGP-таблица в соответствующем экземпляре также отсутствует (вывод команд `'show bgp vrf VRF_NAME'` будет пустым). Однако в таблице маршрутизации могут присутствовать маршруты с пометкой "BGP" в том случае, если их источником является AFI VPNv4 unicast.

Автоматическая редистрибуция

По умолчанию на маршрутизаторах семейства ME работает автоматическая редистрибуция присоединенных (connected-) маршрутов в AFI VPNv4 unicast и автоматическое анонсирование таких путей VPNv4-соседям. Процесс автоматической редистрибуции неотключаем.

Автоматическая редистрибуция не требует запуска отдельного BGP-процесса для соответствующего экземпляра VRF.

Возможность назначения дополнительных атрибутов BGP на автоматически анонсируемые маршруты отсутствует. Для назначения атрибутов необходимо создавать блок `'vrf VRF_NAME'` в разделе `'router bgp'` и настраивать там процесс редистрибуции соответствующих сетей с назначением нужных атрибутов.

Редистрибуция адресов loopback-интерфейсов

Отдельным случаем является задача анонсирования адресов loopback-интерфейсов, относящихся к VRF.

Данные адреса, являясь не присоединенными, а локальными, не подпадают под автоматическую редистрибуцию. В случае, если необходимо анонсировать их соседним BGP-маршрутизаторам в VPNv4 unicast, необходимо настраивать редистрибуцию вручную.

Пример настройки редистрибуции адресов loopback-интерфейсов.

```
interface loopback 7991
  ipv4 address 3.1.3.1/32
  vrf l3-1
exit

router bgp 12389
  vrf l3-1
    address-family ipv4 unicast
      redistribution local LOCAL
      match prefix 3.1.3.1/32
    exit
  exit
exit
exit
```

НАСТРОЙКА MPLS L2VPN

В данной главе рассматриваются принципы организации и настройки виртуальных частных сетей второго уровня (Layer 2 VPN, L2VPN), использующих в качестве транспорта технологию MPLS.

Сервисы L2VPN позволяют осуществить локальную коммутацию на уровне Ethernet как между несколькими интерфейсами одного устройства, так и между несколькими устройствами, соединенными MPLS-транспортом.

Составные элементы L2VPN

Интерфейс локальной коммутации (*Attachment circuit, AC*) — интерфейс либо сабинтерфейс устройства, находящийся в режиме L2-коммутации, включенный в состав бридж-домена либо кросс-коннекта и позволяющий производить сквозную коммутацию Ethernet-кадров. Любой интерфейс устройства без назначенных IP-адресов находится в режиме L2-коммутации. Интерфейс с назначенными на нем IP-адресами невозможно включить в L2VPN в качестве AC.

IMPORTANT

При приеме и передаче Ethernet-кадров через AC по умолчанию **не осуществляется** никакой модификации заголовков кадров. В первую очередь, интерфейсы локальной коммутации не производят снятия VLAN-тегов с трафика и добавления таких тегов. Если требуется произвести операции над тегами (снятие, добавление либо замену), то для этого необходимо явно сконфигурировать данную операцию на интерфейсе командой `'rewrite'`. Таким образом, трафик, попавший в бридж-домен либо кросс-коннект через интерфейс AC, по умолчанию будет коммутироваться с сохранением всех тегов.

Классификаторы, заданные на сабинтерфейсах командой `'encapsulation'`, отвечают только за отнесение входящего в родительский интерфейс трафика к данному сабинтерфейсу. Трафик, выходящий из сабинтерфейса согласно имеющейся конфигурации L2VPN-сервиса, не проверяется на предмет соответствия тегов классификатору сабинтерфейса.

Бридж-домен, как один из основных элементов L2VPN, позволяет объединить в общую L2-среду один или несколько интерфейсов локальной коммутации (AC), а также элементы сервисов EoMPLS (Ethernet over MPLS) — псевдопровода (*Pseudowire, PW*) и виртуальные экземпляры коммутации (*Virtual Forwarding Instance, VFI*).

Кросс-коннект (*point-to-point element, p2p*) также является элементом L2VPN и позволяет объединить в общую среду строго один интерфейс локальной коммутации (AC) и один псевдопровод (PW).

Выбор используемого для L2VPN-сервиса механизма (бридж-домена либо кросс-коннекта) зависит от задачи, которую требуется выполнить.

Настройка бридж-доменов

Для организации L2VPN-сервиса с использованием бридж-домена необходимо сконфигурировать на устройстве сам бридж-домен, создать требуемые AC, PW и/или VFI и включить все нужные элементы в данный бридж-домен.

Между элементами бридж-домена будет производиться коммутация Ethernet-кадров.

Правила коммутации трафика в бридж-домене

Между элементами бридж-домена осуществляется коммутация трафика на основании перечисленных правил:

1. Для каждого бридж-домена автоматически создается таблица MAC-адресов по аналогии с Ethernet-коммутаторами. Ethernet-кадры коммутируются на основании анализа MAC-адреса получателя (DST MAC).
2. Кадры с известным DST MAC будут отправляться в соответствующие AC/PW.
3. Кадры с неизвестным DST MAC, broadcast- и multicast-кадры (т.н. BUM-трафик, "Broadcast, Unknown unicast и Multicast") будут отправляться во все элементы бридж-домена, за исключением того элемента (AC либо PW), с которого вошли в бридж-домен.
4. При коммутации учитываются DST MAC в кадрах, но не учитываются VLAN-теги, имеющиеся на кадрах — таким образом, коммутация внутри бридж-домена не является "VLAN-aware".

Псевдопровода (pseudowires)

Псевдопровод — логический элемент, объединяющий экземпляры L2VPN между двумя устройствами, объединенными MPLS-транспортом и позволяющий передавать Ethernet-кадры поверх MPLS (технология носит название *Ethernet over MPLS*, *EoMPLS*). Аналогично сервисам L3VPN, для обеспечения работы псевдопроводов L2VPN необходимо наличие и работоспособность MPLS-связности между устройствами (должны быть выделены транспортные метки MPLS для достижения адреса соседнего устройства).

Для каждого псевдопровода сервиса L2VPN выделяется также сервисная MPLS-метка (назначается посредством протокола LDP для статических псевдопроводов либо средствами протокола MP-BGP для L2VPN с автообнаружением соседей).

Псевдопровода для L2VPN-сервисов создаются и настраиваются внутри конфигурационных блоков бридж-доменов и кросс-коннектов.

В глобальной конфигурации устройства при этом **необходимо** создать профиль псевдопровода ('pw-class') и сконфигурировать targeted-сессию LDP до адреса устройства, с которым создается псевдопровод (targeted-сессии не требуются при использовании BGP autodiscovery/signalling).

Таблица 50. Настройка профиля псевдопровода.

| Команда | Назначение |
|---|---|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>l2vpn pw-class CLASS_NAME</code> | Создание в конфигурации устройства профиля псевдопровода и переход в режим задания его параметров. |
| <code>encapsulation mpls signaling-type { manual pseudowire-id-fec-signaling }</code> | <p>Задание метода сигнализации для псевдопроводов, использующих данный профиль. Для использования классической сигнализации LDP следует использовать параметр <code>'pseudowire-id-fec-signaling'</code>. При использовании метода <code>'manual'</code> сервисные метки задаются вручную в конфигурации каждого псевдопровода.</p> <p>Данный параметр является обязательным.</p> |
| <code>encapsulation mpls mtu MTU_SIZE</code> | (опционально) Задание значения MTU, которое будет использоваться при сигнализации псевдопроводов. Данный параметр влияет только на процесс сигнализации и не ограничивает размер передаваемых пакетов. |
| <code>encapsulation mpls control-word { preferred non-preferred }</code> | (опционально) Задаёт значение параметра control word (предпочитаемый "preferred" либо не предпочитаемый "non-preferred") для процесса сигнализации псевдопровода. |
| <code>root</code> | Возврат в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

Пример настройки профиля псевдопровода.

```
l2vpn pw-class example-class
  encapsulation mpls control-word preferred
  encapsulation mpls signaling-type pseudowire-id-fec-signaling
exit
```

Таблица 51. Настройка targeted LDP-сессии (обязательно для псевдопроводов с LDP-сигнализацией).

| Команда | Назначение |
|------------------------|--|
| <code>configure</code> | Переход в режим глобальной конфигурации. |

| Команда | Назначение |
|--|---|
| <code>mpls ldp neighbor IPv4_ADDR</code> | Создание targeted LDP-сессии до устройства с указанным адресом. Адрес, указанный при создании сессии, должен совпадать с адресом, используемым при создании самого псевдопровода внутри соответствующего элемента L2VPN. Для успешной установки targeted-сессии должны быть предварительно установлены транспортные LSP до указанного адреса. |
| <code>bfd fast-detect</code> | (опционально) Включение механизма BFD для соответствующей targeted LDP-сессии. |
| <code>root</code> | Возврат в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

Пример настройки targeted LDP-сессии.

```
mpls ldp neighbor 2.2.2.2
  bfd fast-detect
exit
```

После выполнения данных настроек можно производить создание и конфигурирование псевдопроводов внутри соответствующих L2VPN-сервисов.

Создание бридж-домена

Таблица 52. Создание и настройка бридж-домена.

| Команда | Назначение |
|---|---|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>l2vpn bridge-domain BD_NAME</code> | Создание в конфигурации устройства бридж-домена и переход в режим его настройки. |
| <code>interface { tengigabitethernet bundle-ether } num num.subif_id</code> | Включение указанного интерфейса либо сабинтерфейса в состав бридж-домена в качестве интерфейса локальной коммутации (AC). |

| Команда | Назначение |
|--|---|
| <code>pw IPv4_PEER PW_ID</code> | Создание внутри бридж-домена псевдопровода до указанного устройства и переход в режим настройки этого псевдопровода. Параметр <i>PW_ID</i> (также применяется термин <i>VC ID</i> , <i>Virtual circuit ID</i>) служит для идентификации псевдопровода на устройствах, он используется в процессе сигнализации и назначения сервисных меток и должен быть одинаковым для одного и того же PW на обоих устройствах. |
| <code>pw-class CLASS_NAME</code> | Привязка ранее созданного в конфигурации профиля к данному псевдопроводу. Привязка профиля к псевдопроводу является обязательной. |
| <code>mpls static label local LOCAL_LABEL_VALUE</code> <code>mpls static label remote REMOTE_LABEL_VALUE</code> | (опционально) Задание локальной и удаленной сервисной MPLS-метки для данного псевдопровода. Параметры используются в случае, когда профиль псевдопровода предполагает использование ручного назначения сервисных меток ('manual'). |
| <code>backup</code> | (опционально) Переход в режим настройки запасного (backup) псевдопровода. |
| <code>pw IPv4_PEER PW_ID</code> | Создание запасного (backup) псевдопровода до указанного устройства и переход в режим настройки этого псевдопровода. Запасной псевдопровод будет использоваться в случае отказа основного. |
| <code>pw-class CLASS_NAME</code> | Привязка ранее созданного в конфигурации профиля к данному псевдопроводу. |
| <code>exit</code> | Возврат в режим конфигурации backup PW. |
| <code>exit</code> | Возврат в режим конфигурации основного PW. |
| <code>ignore encapsulation-mismatch</code> <code>ignore mtu-mismatch</code> | Установка режима игнорирования несоответствия параметров инкапсуляции (типа псевдопровода) либо значения MTU при сигнализации псевдопровода. |
| <code>exit</code> | Возврат в режим конфигурации бридж-домена. |

| Команда | Назначение |
|---|---|
| <code>transport-mode { ethernet vlan }</code> | Установка транспортного режима для всех псевдопроводов данного бридж-домена (type4/"port" и type5/"tagged" соответственно, согласно спецификации EoMPLS). Транспортный режим задается для целей сигнализации и не влияет на обработку передаваемого по псевдопроводу трафика. |
| <code>mtu MTU_SIZE</code> | Устанавливает размер MTU в байтах для всего бридж-домена. Настройка служит для целей сигнализации. |
| <code>root</code> | Возврат в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

Пример. Создание бридж-домена с тремя АС и двумя псевдопроводами (из них один — с запасным псевдопроводом)

```
l2vpn bridge-domain example-bd
  pw 2.2.2.2 400500
    pw-class example-class
      backup
        pw 4.4.4.4 400500
          pw-class example-class
        exit
      exit
    exit
  pw 3.3.3.3 400501
    pw-class example-class
  exit
  interface tengigabitethernet 0/0/15
  interface tengigabitethernet 0/0/1.400500
  interface tengigabitethernet 0/0/17.5
exit
```

В приведенном примере бридж-домен позволит осуществлять коммутацию трафика между АС `tengigabitethernet 0/0/15`, `tengigabitethernet 0/0/1.400500`, `tengigabitethernet 0/0/17.5` и двумя псевдопроводами до соседей с адресами 2.2.2.2 и 3.3.3.3. Псевдопровод до соседа 2.2.2.2 также имеет резервный PW до соседа 4.4.4.4.

Виртуальные экземпляры коммутации и разделенный горизонт для псевдопроводов

Как было указано ранее, коммутация пакетов в бридж-доме может производиться между всеми элементами, включенными в бридж-домен, то есть в направлениях АС-АС, АС-PW и PW-PW.

Однако, коммутация трафика между разными псевдопроводами одного бридж-домена может быть нежелательной в ряде случаев (в частности, при построении полносвязных топологий VPLS — в таких случаях коммутация пакетов между PW приведет к закольцовке трафика).

Для решения данной задачи используется принцип "разделенного горизонта" (*split horizon*), когда псевдопровода собираются в специальную группу (*split horizon group*), благодаря чему запрещается коммутация трафика между ними, однако остается возможность коммутации между псевдопроводом группы и интерфейсами (AC) бридж-домена.

В конфигурации устройства такие группы называются виртуальными экземплярами коммутации (*VFI, Virtual Forwarding Instance*). В каждый экземпляр можно включить произвольное количество псевдопроводов.

Таблица 53. Создание и настройка экземпляра VFI внутри бридж-домена.

| Команда | Назначение |
|--|---|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>l2vpn bridge-domain BD_NAME</code> | Переход в режим настройки бридж-домена. |
| <code>vfi VFI_NAME</code> | Создание внутри бридж-домена экземпляра VFI и переход в режим его настройки. |
| <code>pw IPv4_PEER PW_ID</code> | Создание внутри экземпляра VFI псевдопровода до указанного устройства и переход в режим настройки этого псевдопровода. Дальнейшая конфигурация псевдопровода (включая backup) аналогична настройке PW непосредственно в бридж-домене. |
| <code>root</code> | Возврат в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

Пример. Бридж-домен с тремя интерфейсами и одним экземпляром VFI.

```
l2vpn bridge-domain example-bd
  vfi VFI-A
    pw 10.10.10.214 300
      pw-class example-class
    exit
  pw 10.10.10.220 312
    pw-class example-class
  exit
exit
interface tengigabitethernet 0/0/15
interface tengigabitethernet 0/0/1.400500
interface tengigabitethernet 0/0/17.5
exit
```

NOTE В бридж-домене может быть не более одного экземпляра VFI.

Настройка кросс-коннектов

Для организации L2VPN-сервиса с использованием кросс-коннекта необходимо создать на устройстве необходимый AC, элемент конфигурации P2P, включить в данный элемент конфигурации соответствующий AC и сконфигурировать там же псевдопровод.

Между AC и PW, включенными в кросс-коннект, будет производиться коммутация Ethernet-кадров.

Основные принципы работы кросс-коннекта аналогичны принципам работы бридж-домена, отличие заключается только в количестве возможных элементов (в кросс-коннекте можно объединять только один PW и один AC), а также в отсутствии процесса изучения MAC-адресов в кросс-коннекте.

Таблица 54. Создание и настройка кросс-коннекта.

| Команда | Назначение |
|---|---|
| <code>configure</code> | Переход в режим глобальной конфигурации. |
| <code>l2vpn xconnect-group</code> <code>XCONNECT_GROUP_NAME</code> | Создание в конфигурации устройства именованной группы кросс-коннектов и переход в режим конфигурации этой группы. |
| <code>p2p P2P_NAME</code> | Создание кросс-коннекта внутри соответствующей группы и переход в режим настройки этого кросс-коннекта. |

| Команда | Назначение |
|--|---|
| <code>interface { tengigabitethernet bundle-ether } num num.subif_id</code> | Включение указанного интерфейса либо сабинтерфейса в состав кросс-коннекта в качестве интерфейса локальной коммутации (AC). |
| <code>pw IPv4_PEER PW_ID</code> | Создание внутри кросс-коннекта псевдопровода до указанного устройства и переход в режим настройки этого псевдопровода. Параметр <i>PW_ID</i> (также применяется термин <i>VC ID</i> , <i>Virtual circuit ID</i>) служит для идентификации псевдопровода на устройствах, он используется в процессе сигнализации и назначения сервисных меток и должен быть одинаковым для одного и того же PW на обоих устройствах. |
| <code>pw-class CLASS_NAME</code> | Привязка ранее созданного в конфигурации профиля к данному псевдопроводу. Привязка профиля к псевдопроводу является обязательной. |
| <code>mpls static label local LOCAL_LABEL_VALUE</code> <code>mpls static label remote REMOTE_LABEL_VALUE</code> | (опционально) Задание локальной и удаленной сервисной MPLS-метки для данного псевдопровода. Параметры используются в случае, когда профиль псевдопровода предполагает использование ручного назначения сервисных меток ('manual'). |
| <code>backup</code> | (опционально) Переход в режим настройки запасного (backup) псевдопровода. |
| <code>pw IPv4_PEER PW_ID</code> | Создание запасного (backup) псевдопровода до указанного устройства и переход в режим настройки этого псевдопровода. Запасной псевдопровод будет использоваться в случае отказа основного. |
| <code>pw-class CLASS_NAME</code> | Привязка ранее созданного в конфигурации профиля к данному псевдопроводу. |
| <code>exit</code> | Возврат в режим конфигурации backup PW. |
| <code>exit</code> | Возврат в режим конфигурации основного PW. |
| <code>ignore encapsulation-mismatch</code> <code>ignore mtu-mismatch</code> | Установка режима игнорирования несоответствия параметров инкапсуляции (типа псевдопровода) либо значения MTU при сигнализации псевдопровода. |

| Команда | Назначение |
|---|--|
| <code>exit</code> | Возврат в режим конфигурации кросс-коннекта. |
| <code>transport-mode { ethernet vlan }</code> | Установка транспортного режима псевдопровода в данном кросс-коннекта (type4/"port" и type5/"tagged" соответственно, согласно спецификации EoMPLS). Транспортный режим задается для целей сигнализации и не влияет на обработку передаваемого по псевдопроводу трафика. |
| <code>mtu MTU_SIZE</code> | Устанавливает размер MTU в байтах для данного кросс-коннекта. Настройка служит для целей сигнализации. |
| <code>root</code> | Возврат в режим глобальной конфигурации. |
| <code>commit</code> | Применение произведенных настроек. |

Пример. Настройка кросс-коннекта.

```

l2vpn xconnect-group EXAMPLE-GROUP
  p2p PW-CUSTOMER-1
    transport-mode vlan
    pw 2.2.2.2 4012
      pw-class example-class
        backup
          pw 4.4.4.4 4018
            pw-class example-class
          exit
        exit
      exit
    exit
  interface tengigabitethernet 0/0/9.2001
  exit
exit

```