Маршрутизаторы ELTEX серии ME. Руководство по настройке.

Eltex Network OS for ME routers ver. 3.12.0

Оглавление

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
`command example`	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
`configure`	*global-view*	Переход из глобального режима CLI в режим конфигурирования
`exit`	*config*	Переход на вышестоящий уровень конфигурирования

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

Пример: использование фильтров

```
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$6TGyBVbqUB8s2InhRT4QA5VADoCc4zGhILDKjTxgVt7H0TBzxmbwNkpkHSkHNAU9qC
```

```
zdQ/ZeonlI8EOrkII620
  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
`configure`	*global-view*	Перейти из глобального режима CLI в режим конфигурирования.
`show running-config`	*global-view*	Вывести текущую конфигурацию устройства.
`show candidate-config`	*global-view*	Вывести кандидат-конфигурацию устройства.
`show configuration changes`	*global-view*	Вывести список изменений в кандидат-конфигурации относительно текущей конфигурации устройства.
`commit`	*config*	Применить кандидат-конфигурацию (применить изменения, внесенные во время сеанса редактирования).

Команда	Режим	Действие команды
`abort`	*config*	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#
```

Именование 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	Обозначение физического интерфейса включает в себя его тип и идентификатор. Идентификатор имеет вид **<UNIT>/<SLOT>/<PORT>**, где: • <UNIT> - номер устройства в кластере устройств; • <SLOT> - номер модуля в составе устройства; • <PORT> - порядковый номер интерфейса данного типа в модуле. *Физические интерфейсы всегда присутствуют в системе.*
Интерфейсы Ethernet 10Гбит/с	`tengigabitethernet <UNIT>/<SLOT>/<PORT>` Пример обозначения: `'tengigabitethernet 0/0/10'`. Допускается использовать сокращенную форму с обязательным пробелом, например, `'te 0/0/10'`.
Интерфейсы Ethernet 40Гбит/с	`fourtygigabitethernet <UNIT>/<SLOT>/<PORT>` Пример обозначения: `'fourtygigabitethernet 0/0/2'`. Допускается использовать сокращенную форму с обязательным пробелом, например, `'fo 0/0/2'`.
Интерфейсы Ethernet 100Гбит/с	`hundredgigabitethernet <UNIT>/<SLOT>/<PORT>` Пример обозначения: `'hundredgigabitethernet 0/0/3'`. Допускается использовать сокращенную форму с обязательным пробелом, например, `'hu 0/0/3'`.
Группы агрегации каналов	`bundle-ether <BUNDLE_ID>` Обозначение группы агрегации каналов включает в себя тип интерфейса ("bundle-ether") и порядковый номер группы. Пример обозначения: `'bundle-ether 8'`. Допускается использовать сокращенную форму с обязательным пробелом, например, `'bu 8'`. *Группы агрегации каналов в системе можно создавать и удалять.*

Тип интерфейса	Обозначение и функционал

Сабинтерфейсы	`bundle-ether <BUNDLE_ID>.<SUBIF_ID>`
	`tengigabitethernet <UNIT>/<SLOT>/<PORT>.<SUBIF_ID>`
	`fourtygigabitethernet <UNIT>/<SLOT>/<PORT>.<SUBIF_ID>`
	`hundredgigabitethernet <UNIT>/<SLOT>/<PORT>.<SUBIF_ID>`
	
	Обозначение сабинтерфейса образуется из обозначения базового интерфейса и идентификатора сабинтерфейса, разделенных точкой. Для сабинтерфейсов обязательно задание типа инкапсуляции ('encapsulation'). Пример обозначения: `'tengigabitethernet 0/0/10.350'`
	
	Сабинтерфейсы в системе можно создавать и удалять.

Интерфейсы локальной петли	`loopback <ID>` Виртуальный интерфейс локальной петли. Данный тип применяется в случаях, когда требуется постоянно активный логический интерфейс. Пример обозначения: ‘loopback 100’ *Интерфейсы локальной петли в системе можно создавать и удалять.*
Туннельные интерфейсы	`tunnel-ip <ID>` Виртуальный интерфейс tunnel IP. Возможны режимы работы IP-IP и IP-GRE. Пример обозначения: ‘tunnel-ip 100’ *Туннельные интерфейсы в системе можно создавать и удалять.*
Интерфейсы BVI (Bridge-domain Virtual Interface)	`bvi <ID>` Виртуальный интерфейс BVI. Данный тип применяется в случаях, когда требуется добавление маршрутизирующего интерфейса в бридж-домен. Пример обозначения: ‘bvi 100’ *Интерфейсы BVI в системе можно создавать и удалять.*

Тип интерфейса	Обозначение и функционал
Интерфейсы управления	`mgmt <UNIT>/<SLOT>/<PORT>` 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: • `'mgmt 0/fmc0/1'` - для ME5100; • `'mgmt 0/fmc0/0'` и `'mgmt 0/fmc0/1'` для FMC0 в маршрутизаторе ME5000; • `'mgmt 0/fmc1/0'` и `'mgmt 0/fmc1/1'` для FMC1 в маршрутизаторе ME5000 *Интерфейсы управления всегда присутствуют в системе.* **IMPORTANT** Интерфейсы управления не предназначены для передачи транзитного трафика (не участвуют в работе data-plane) и жестко прикреплены к VRF 'mgmt-intf'.

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.

ДОСТУП К УСТРОЙСТВУ

Локальные учетные записи

Учётной записью по умолчанию является `admin` с паролем `password` и уровнем привилегий `p15`. Для локального доступа к устройству рекомендуется создать учетные записи пользователей, возможно, ограничив для них уровень привилегий. По умолчанию пользователь ограничен уровнем привилегий `p1`.

Таблица 5. Настройка локальной учетной записи

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`user` *user_name*	Переход в режим конфигурации учетной записи пользователя.
`password [encrypted]` *password*	Задание пароля пользователя в открытом или шифрованном виде.
`privilege` *p1-p15*	Задание уровня привилегий пользователя. Для различных уровней привилегий доступны следующие действия: • **p1**: только команды `ping` и `traceroute`; • **p2-p9**: команды уровня p1 плюс все show-команды, кроме `show running-config`, `show configuration`, `show users`; • **p10-p14**: команды предыдущих уровней плюс все команды уровня конфигурации, за исключением настроек подсистем безопасности; • **p15**: полный доступ к устройству.
`exit`	(Опционально) Возврат в режим глобальной конфигурации.
`commit`	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
`change-privilege { p1 | p2 | .. | p15 } [` *PASSWORD* `]`	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.

Ролевая модель управления доступом

Для более гибкой настройки прав пользователей на маршрутизаторах серии ME реализована ролевая модель управления доступом. Ролевая модель работает поверх уровней привилегий.

Роль (role) - это набор полномочий, описанных командами, доступными пользователю и необходимыми для выполнения определённых рабочих задач. Каждый пользователь может иметь одну или несколько ролей, а каждая роль может содержать от одного до множества полномочий в рамках этой роли. Роли могут быть агрегированы в группы (group). Группы и роли имеют следующие атрибуты:

- **default** - позволяет задать правило для команд по умолчанию;
- **deny** - запретить пользователю использовать команды;
- **permit** - разрешить пользователю использовать команды.

Отдельно группы имеют атрибут **role**:

- **role** - добавить роль в группу. Правило из роли начинает действовать на пользователей, которые добавлены в группу.

Пользователь может иметь роль и (или) быть участником группы. Если для группы/роли не заданы атрибуты, то права пользователей определяются их уровнем привилегий, заданным при создании учетной записи.

Настройка ролей и групп описана в разделе **"Механизм AAA"**.

Авторизация по SSH-ключу

На маршрутизаторах серии ME поддержана только **локальная** *авторизация по SSH-ключу.*

На маршрутизаторе, используемом в качестве SSH-сервера, создается локальная учетная запись пользователя с публичным RSA-ключом, сгенерированным SSH-клиентом.

Таблица 7. Настройка локальной учетной записи с RSA-ключом.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`user` *user_name*	Переход в режим конфигурации учетной записи пользователя.
`password [encrypted]` *password*	Задание пароля пользователя в открытом или шифрованном виде.
`authorized-key` *key_name*	Задание идентификатора ключа и переход в режим его конфигурации.
`description` *descr*	(Опционально) Добавить описание, облегчающее идентификацию пользователя.
`key-string` *rsa_key*	Задание публичной части RSA-ключа 1024-11870 бит. Строку ключа необходимо заключать в кавычки.
`exit`	(Опционально) Возврат в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

Пример. Создать учетную запись пользователя tester для подключения двух устройств по SSH-ключу.

```
! Обозначим в конфигурации одно устройство как den (authorized-key den), другое - как
ivan (authorized-key ivan)

user tester
  authorized-key den
    key-string "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCxDLKDlivI1f3WC28uhuUL1LdaOPsMOqbJI5nVUIllLhKmHntmRCPaIb
Lqy853Wnz/iDTFe42XOaYfpl96i1V5u7aDCHrXPdmDJRJsnbi1oa+u5uZK1Ocm37+L+OloA88JfniVJN/6zfaw
kbAamyBvAEtV1np3wiJXILnwIZX9rQ== tester_den"
  exit
  authorized-key ivan
    key-string "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQC+3gnEwRxRucf5P/EwKjyw/Bf639w2Jh/sNBl3hgjj2Xr5Vx7y5ovwqe
PvSPOJTyzX65qO8vXZx3EwVeOX/9T2GTYqzr+DSsy9SsVpzf+Lk0go3x7Vr9JMaQJvjKTMGhcwcwEWQuQNXySu
sLqQNwJD2bsOC1udT27yeNISksq3Ww== tester_ivan"
  exit
  password encrypted
$6$MttCGmTPooukMAq7$X3z8rSGtppDAJo44fu5G03a3He9T1CwEIF8OlrcjW262/Fj/m5WPW6r8/ZKIDUg2Mn
6kwUWfE3e/mE/xUPY/I1
  privilege p15
exit
```

Генерация SSH-ключа

Генерация ключа производится следующей командой:

Команда	Назначение
`key generate` { dsa | rsa | rsa1 } [`label` *label*][`modulus` *value*]	Создать ключ указанного типа, где `label` - идентификатор устройства, по умолчанию используется hostname; `modulus` - размер ключа в битах.

Пример. Создать SSH-ключ RSA длиной 1024 бит с идентификатором устройства "ME5100_mio"

```
0/ME5100:Router# key generate rsa modulus 1024 label ME5100_mio
You already have rsa keys.
Do you really want to replace them? (y/n): [n] y
Fri Nov  3 15:32:32 2023
Keys generated successfully
Elapsed time was 0.774307 sec
0/ME5100:Router#
```

Пример. Посмотреть открытую часть SSH-ключа

```
0/ME5100:Router# show ssh key
Fri Nov  3 15:31:21 2023
---------------KEY #1---------------
  Keys type:         rsa
  Keys modulus:      4096 bits
  Label:             ME5100_mio
  Creation date:     Fri Nov  3 12:06:20 GMT+7 2023
  Public key:
    ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAACAQC4ye8ouerG37BaKqhMtEfSsZMDMs8osPYfaTJ/Kb2V4EoCnkXLRfNZvc
l+rsbW1yDfiJ+x9ehy8ai2YdwQpuMA1UNSz0VD+V8Ho0md9DrUlc9+1P0Kpo+U6qoyBXYIwT2BZF/zMyo3FiOi
2P1G8kUTdq38ekzYQXA6S9NQjn4NtrgGe015kWoXMfmjEL893Zv2cbYn/ukjGrH3Z5xGny8YcxCLxijEgTtqPD
gmLhBJqaPNIr3/ek8F4/hAm41m7FxAq5UK4c6EkbvA6xVMUNt6aPonyxAcN4oLFJ1UdX4oxX25qm5T8wPiSAWP
BNhGHiTo7NnlnGcng8cwrSKbIDDPu+JNsYYLBUoERMss3kfDtxv5H5PlruXuW6+mDfwjyhZNyootY+mn6oouO2
GfmtbbvA7a9QsWdXD3vB2MgRAuRNGLI06SYxU0HKVO2YDs+I4r+MD4HU9zuRo77lH/75KjK4hXfabto5zcD4fd
7pRZA7w8OGR6GZfZDG0+Ijb0HcKIKyJ/vR+VS8dmBs16/SzSvlea9WSeKJB9/EJaBrLzy6o9bYEJpAOhjh63FS
bOsdJee9lYeoYpFi7+cx6lIOZVXaZEAah+hjPUWPBD1zg6YoblLKproAV2/xdtQB0zxtpnQgD6wwDpxUm2BuJ0
19JVzmOnOT1mKBv/f2sBeSvMoQ== ME5100_mio
```

Открытая часть ключа копируется и добавляется в конфигурацию встречного устройства как SSH-ключ для локальной учетной записи пользователя.

Удаление ключей производится следующей командой:

Команда	Назначение
`clear ssh key { all | dsa | rsa | rsa1 }`	Удалить ключ указанного типа или все ключи.

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 8. Настройка аутентификации

Команда	**Назначение**
`configure`	Переход в режим глобальной конфигурации.
`aaa authentication { login | enable }` *list_name*	Создание списка аутентификации. • `login` — для входа в систему; • `enable` — для смены уровня привилегий.
`method { ldap| local | tacacs | radius }`	Задание метода аутентификации внутри соответствующего списка аутентификации • `ldap` — метод устанавливает аутентификацию через сконфигурированные LDAP-серверы; • `local` — метод устанавливает локальную аутентификацию, то есть аутентификацию согласно настройкам 'enable' и 'user' в текущей конфигурации; • `tacacs` — метод устанавливает аутентификацию через сконфигурированные TACACS+-серверы; • `radius` — метод устанавливает аутентификацию через сконфигурированные RADIUS-серверы.
`exit`	Возврат в режим глобальной конфигурации.

Команда	Назначение
`aaa authentication retry-options { backoff-factor | backoff-threshold | lockout-period | login-grace-time | tries-before-disconnect }` *value*	(Опционально) Настройка параметров неудачных попыток аутентификации • `backoff-factor` — время в секундах между попытками аутентификации после исчерпания количества попыток, определенных значением параметра `backoff-threshold`. • `backoff-threshold` — количество неудачных попыток аутентификации до установки задержки между попытками аутентификации. • `lockout-period` — время блокировки учетной записи пользователя. Учетная запись блокируется на время или навсегда (permanent). Дополнительно можно задать интервал времени (fail-interval), в течение которого предпринимались неуспешные попытки аутентификации. Когда заданное время закончится, учетная запись будет заблокирована. • `login-grace-time` — максимальное время ожидания устройством начала ввода логина и пароля. • `tries-before-disconnect` — максимальное количество попыток аутентификации до разрыва соединения(дефолтное значение-3).
`commit`	Применение произведенных настроек.

NOTE

При удалении узла lockout-period информация о неуспешных попытках входа всех пользователей неявно удаляется.
Блокировка работает со всеми логин-листами aaa authentication login, если присутствует lockout-period.
Блокировка используется для локальных пользователей, но не распространяется на пользователя root.
Функционал применим для аутентификации через ssh/telnet/console.

Пример. Настройка аутентификации для сервиса telnet.

После пяти неуспешных попыток аутентификации в течение трех минут пользователь будет заблокирован на час.

```
aaa authentication enable telnet
  method tacacs
exit
aaa authentication login TAC245
  method tacacs
  method local
exit
aaa authentication retry-options lockout-period 360 fail-interval 3
aaa authentication retry-options tries-before-disconnect 5
```

```
line telnet login authentication TAC245
```

При попытке подключения к устройству после блокировки появится уведомление:

```
0/ME5100:Router login: tester
The account is locked due to 5 failed logins.
(360 minutes left to unlock)
Login incorrect
```

Время окончания блокировки пользователя покажет команда "show users lockout"

```
0/ME5100:Router# show users lockout
Tue Dec 30 15:25:11 2025
  User               Consecutive  Lock      Latest failure       Lockout end
                     failures     status
  ------------------ ------------ --------- -------------------- ------------
  tester             5            Locked    2025-12-30 15:24:52  2025-12-30 16:26:52
```

Таблица 9. Настройка логирования

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

Пример. Включение логирования команд пользователя, входа пользователя в систему и выхода из нее на TACACS+-сервере.

```
aaa accounting commands start-only tacacs
aaa accounting login start-stop tacacs
```

Таблица 10. Настройка авторизации

Команда	**Назначение**
`configure`	Переход в режим глобальной конфигурации.
`aaa authorization commands tacacs`	Включение авторизации команд пользователя через TACACS+-сервер.

Команда	Назначение
`aaa authorization role` *name*	Создание роли и переход в режим её конфигурации.
`default { by-privilege | deny | permit }`	Задать права доступа по умолчанию. • `by-privilege` — права доступа определяются уровнем привилегий пользователя; • `deny` — любые действия запрещены; • `permit` — любые действия разрешены;
`deny` *command*	Указать запрещенные к вводу команды.
`permit` *command*	Указать разрешенные к вводу команды.
`no-configure`	Запретить работу в режиме конфигурации.
`priority` *value*	(Опционально) Указать приоритет роли.
`exit`	Возврат в режим глобальной конфигурации.
`aaa authorization group` *name*	Создание группы и переход в режим её конфигурации.
`default { by-privilege | deny | permit }`	Задать права доступа по умолчанию.
`deny` *command*	Указать запрещенные к вводу команды.
`permit` *command*	Указать разрешенные к вводу команды.
`no-configure`	Запретить работу в режиме конфигурации.
`priority` *value*	(Опционально)Указать приоритет группы.
`role` *name*	Добавить роль в группу.
`exit`	(Опционально) Возврат в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

Пример. Настройка ролевой модели доступа.

Сконфигурированы две роли и группа. Участникам группы, учетная запись которых не привязана к роли, доступны команды из группы (permit "show clock") и команды ролей 1 и 2 (show running-config, show tech-support, show ntp status)

Настройка авторизации

```
aaa authorization group test
  default deny
  permit "show clock"
  role role-1
  role role-2
exit
aaa authorization role role-1
  default deny
  permit "show running-config"
```

```
  permit "show tech-support"
exit
aaa authorization role role-2
  default deny
  permit "show ntp status"
exit
```

Настройка пользователей

```
user u1
  role role-1
  role role-2
exit

user u2
  role role-2
exit

user user-0
  group test
exit
```

Настройка серверов TACACS+ и RADIUS

Таблица 11. Настройка сервера TACACS+

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`tacacs-server host` { *DOMAIN NAME* | *_IP_serveraddr* | *IPv6_serveraddr*} `[ vrf` *vrf_name* `]`	Задание в конфигурации сервера TACACS+ с указанным IPv4 (IPv6)-адресом или доменным именем в глобальной таблице маршрутизации (GRT) или внутри указанного VRF.
`password [encrypted]` *password*	Задание пароля сервера TACACS+ в открытом или шифрованном виде.
`priority` *priority*	Задание приоритета TACACS-сервера.
`exit`	Возврат в режим глобальной конфигурации.
`tacacs-server timeout` *secs*	(Опционально) Задание времени ожидания ответа от серверов TACACS+, в секундах.
`tacacs-server dscp` *dscp_val*	(Опционально) Задание значения поля DSCP, с которым будут генерироваться IP-пакеты, отправляемые на серверы TACACS+.
`commit`	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 12. Настройка сервера RADIUS

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`radius-server host` { *DOMAIN NAME* | *_IP_serveraddr* | *IPv6_serveraddr*} `[ vrf` *vrf_name* `]`	Задание в конфигурации сервера RADIUS с указанным IPv4 (IPv6)-адресом или доменным именем в глобальной таблице маршрутизации (GRT) или внутри указанного VRF.
`password [encrypted]` *password*	Задание пароля сервера RADIUS в открытом или шифрованном виде.
`priority` *priority*	Задание приоритета RADIUS-сервера.
`source-address` { *IP_intf-addr* | *IPv6_intf-addr*}	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.
`acct-port` *port*	(Опционально) Задание номера UDP-порта для передачи данных учета.
`auth-port` *port*	(Опционально) Задание номера порта для передачи аутентификационных данных.
`timeout` *secs*	(Опционально) Задание времени ожидания ответа от сервера RADIUS, в секундах.
`exit`	Возврат в режим глобальной конфигурации.
`timeout` *secs*	(Опционально) Задание времени ожидания ответа от серверов TACACS+, в секундах.
`radius-server dscp` *dscp_val*	(Опционально) Задание значения поля DSCP, с которым будут генерироваться IP-пакеты, отправляемые на серверы RADIUS.
`radius-server timeout` *secs*	(Опционально) Задание времени ожидания ответа от серверов RADIUS, в секундах.
`radius-server retransmit` *val*	(Опционально) Задание количества попыток обращения к RADIUS-серверу.
`commit`	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
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 13. Настройка telnet-сервера.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`telnet server [ vrf` *vrf_name* `]`	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.
`dscp` *dscp_val*	(Опционально) Задание значения поля DSCP, с которым будут генерироваться IP-пакеты.
`session-limit` *val*	(Опционально) Задание максимального количества одновременно подключенных пользователей
`port` *val*	(Опционально) Задание номера порта, по которому будет принимать входящие соединения соответствующий локальный сервер.
`exit`	(Опционально) Возврат в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

Маршрутизаторы серии ME поддерживают протокол SSH версий 1 и 2. По умолчанию используется протокол SSHv2

Таблица 14. Настройка SSH-сервера.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.

Команда	Назначение
`ssh server [ vrf` *vrf_name* `]`	Создание в конфигурации SSH-сервера и переход в режим настройки его параметров (config-ssh-server-vrf). При запуске SSH-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.
`version-1`	(Не рекомендуется) Включение поддержки SSHv1.
`dscp` *dscp_val*	(Опционально) Задание значения поля DSCP, с которым будут генерироваться IP-пакеты.
`session-limit` *val*	(Опционально) Задание максимального количества одновременно подключенных пользователей
`hostname-lookup`	(Опционально) Включить разрешение DNS-имен
`paranoid disable`	(Опционально) Разрешить использование устаревших алгоритмов шифрования.
`port` *val*	(Опционально) Задание номера порта, по которому будет принимать входящие соединения соответствующий локальный сервер.
`exit`	(Опционально) Возврат в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

Настройка параметров терминальных сессий

Таблица 15. Настройка Telnet-сессий.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`line telnet enable authentication` *list_name*	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.
`line telnet login authentication` *list_name*	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.

Команда	Назначение
`line telnet session-timeout` *val*	(Опционально) Задание периода неактивности пользователя (в минутах), открывшего telnet-сессию, по истечении которого сессия будет принудительно завершена.
`commit`	Применение произведенных настроек.

Таблица 16. Настройка SSH-сессии.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`line ssh enable authentication` *list_name*	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.
`line ssh login authentication` *list_name*	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.
`line ssh session-timeout` *val*	(Опционально) Задание периода неактивности пользователя (в минутах), открывшего SSH-сессию, по истечении которого сессия будет принудительно завершена.
`commit`	Применение произведенных настроек.

Таблица 17. Настройка локальной консольной сессии.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`line console enable authentication` *list_name*	Включение enable-аутентификации (аутентификации при переходе на разные уровни привилегий) пользователей на консольном порту устройства через ранее сконфигурированный список методов AAA (*aaa authentication enable*). После выполнения данной команды enable-аутентификация будет проводиться по методам, указанным в этом списке.

Команда	Назначение
`line console login authentication` *list_name*	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.
`line console session-timeout` *val*	(Опционально) Задание периода неактивности подключенного на консольном порту пользователя, по истечении которого сессия пользователя будет принудительно завершена.
`line console baudrate` *val*	(Опционально) Задание скорости консольного порта. Значение по умолчанию — 115200 бит/с.
`commit`	Применение произведенных настроек.

Пример. Настройка Telnet-сессии.

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

ФУНКЦИИ УПРАВЛЕНИЯ

Установка системного времени

Системное время можно установить двумя способами:

- Вручную;
- С помощью протокола NTP.

При настройке вручную в устройстве устанавливается время и дата, но отсутствует возможность проверить точность времени. Протокол NTP определяется спецификацией RFC1305 и предоставляет устройствам в сети механизм получения точного времени от NTP-сервера. При использовании протокола NTP все устройства синхронизируются и поддерживают точное время.

Таблица 18. Установка системного времени вручную.

Команда	Назначение
`clock set` *HH:MM:SS DAY MONTH YEAR*	Установка времени и даты в программных часах системы, в формате: часы:минуты:секунды день месяц год
`clock read-calendar`	Синхронизация программных часов системы и аппаратных часов.
`clock update-calendar`	Установка в аппаратные часы устройства времени и даты программных часов.

Пример. Установка системного времени вручную.

```
0/ME5100:Router# clock set 12:21:15 21 march 2019
```

Таблица 19. Установка системного времени посредством протокола NTP.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`clock timezone gmt` *+/-12*	Установка часовой зоны
`ntp [ vrf` *vrf_name* `]`	Создание в конфигурации NTP-сервера и переход в режим настройки его параметров (config-ntp-vrf). При запуске NTP-сервера в каком-либо VRF (либо в глобальной таблице маршрутизации) устройство начинает работать с NTP-серверами на тех своих интерфейсах, которые включены в указанный VRF.
`broadcast-client`	Разрешение получения широковещательных пакетов. Стандартно равноправные NTP-серверы отправляют и принимают одноадресные пакеты. В случае, если несколько NTP-серверов расположены в общей сети, вместо одноадресных пакетов могут использоваться многоадресные.

Команда	Назначение
`source-address` { *IP_intf-addr* | *IPv6_intf-addr*}	Задание IP (IPv6) адреса, который будет использоваться в качестве IP-адреса отправителя. Следует указывать адрес, принадлежащий интерфейсу маршрутизатора в соответствующем VRF.
`peer` { *IP_intf-addr* | *IPv6_intf-addr* }	Задание IP (IPv6) адреса удаленного NTP-сервера. NTP-сервер на маршрутизаторе работает в режиме двусторонней активности с удаленным NTP-сервером, указанным в команде. В случае потери связи одного из партнеров с вышестоящим NTP-сервером, он сможет синхронизировать время по серверу-партнеру.
`authenticate`	(Опционально) Ограничение доступа к NTP-службе с помощью аутентификации.
`authentication-key` *key-number*	Переход в режим конфигурирования ключа аутентификации (config-authentication-key).
`md5 [encrypted]` *password*	Задание пароля в открытом или шифрованном виде.
`trusted-key` *key-number*	Указание ключа, по которому следует проводить аутентификацию.
`exit`	Возврат в режим конфигурации NTP-сервера.
`server` { *IP_intf-addr* | *IPv6_intf-addr* }	Задание IP (IPv6) адреса NTP-сервера и переход в командный режим config-ntp-vrf-server-ipv4. Маршрутизатор работает с указанным NTP-сервером в режиме односторонней активности. В данном режиме локальные часы маршрутизатора могут синхронизироваться с удаленным NTP сервером.
`maxpoll` *value*	Задание максимального значения интервала времени между отправкой сообщений NTP-серверу. Параметр команды используется как показатель степени двойки при вычислении длительности интервала в секундах. Сам интервал вычисляется путем возведения двойки в степень, заданную параметром команды. Принимает значения 4..17.
`minpoll` *value*	Задание минимального значения интервала опроса. Параметр команды используется как показатель степени двойки при вычислении длительности интервала в секундах. Сам интервал вычисляется путем возведения двойки в степень, заданную параметром команды. Принимает значения 4..17.
`version` { *NTPv1* | *NTPv2* | *NTPv3* | *NTPv4* }	Указание версии NTP-сервера.
`prefer`	Выбор текущего NTP-сервера как предпочтительного. При прочих равных условиях данный NTP-сервер будет выбран для синхронизации среди всех рабочих NTP-серверов.

Команда	Назначение
`key` *key-number*	Указание ранее созданного ключа, используемого для аутентификации на NTP-сервере.
`commit`	Применение произведенных настроек.

Пример. Установка часовой зоны и настройка NTP-серверов.

```
clock timezone gmt 7

ntp
  server 10.115.0.5
    key 4
  exit
  authentication-key 4
    md5 encrypted 99B1063CE15E
  exit
  authenticate
  trusted-key 4
exit
ntp vrf mng
  server 192.168.16.113
  exit
  server 192.168.16.245
    prefer
    minpoll 4
  exit
exit
```

Диагностические команды системного времени

show clock detail

Команда выводит информацию о дате, времени и часовой зоне.

Пример: show clock detail

```
0/ME5100:Router# show clock detail
Fri Aug 22 15:22:58 2025
Timezone: GMT7
```

show ntp status

Команда выводит информацию о статусе NTP-сервера

Пример: show ntp status

```
0/ME5100:Router# show ntp status
```

```
Fri Aug 22 15:18:05 2025

  Clock is synchronized (associd=0 status=0614 leap_none, sync_ntp, 1 event,
freq_mode)
  System peer:        192.168.16.245:123
  System peer mode:   client
  Leap indicator:     00
  Stratum:            3
  Log2 precision:     -20
  Root delay:         24.923 msec
  Root dispersion:    36.102
  Reference ID:       192.168.16.245
  Reference time:     ec52a63a.f8cb4be1  Fri, Aug 22 2025 15:18:02.971
  System jitter:      0.000000
  Clock jitter:       0.790 msec
  Clock wander:       0.000 msec
  Broadcast delay:    -50.000 msec
  Symm. auth. delay:  0.000 msec
  VRF:                mng
```

show ntp associations

Команда выводит информацию о синхронизации с вышестоящими серверами

Пример: show ntp associations

```
0/ME5100:Router# show ntp associations
Fri Aug 22 14:33:22 2025

 Fri Aug 22 15:22:30 2025

  remote               refid             st   t    when  poll   reach   delay
offset    jitter     auth        vrf
  -------------------- ----------------- ---- ---- ----- ------ ------- --------
--------- ---------- ----------- ---------------------------------
  *192.168.16.245      91.206.16.3        2   u       3    16     17      0.110
+2.083   +0.849    none        mng
   192.168.16.113      .INIT.            16   u       -    64      0      0.000
+0.000   +0.000    none        mng
   10.115.0.5          .INIT.            16   u       -    64      0      0.000
+0.000   +0.000     bad        default-ns
```

Резервное копирование конфигурации

Резервное копирование конфигурации сетевых устройств – одна из обязательных мер по сокращению времени простоя сети. Резервные копии конфигурации помогут быстро восстановить сеть как в случае физического выхода устройств из строя, так и при сбоях, вызванных ошибками администраторов сети.

Таблица 20. Настройка резервирования конфигурации.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`backup to` *URL*	Создание элемента резервирования конфигурации и переход в режим настройки этого элемента (config-backup-to). Идентификатором элемента является URL, указанный в данной команде. После создания элемента резервирования полная конфигурация устройства будет выгружаться по указанному URL периодически либо после применения конфигурации — в зависимости от настройки элемента. Допустимо создание нескольких элементов.
`daily` HH:MM:SS	Установка времени (в 24-часовом формате) ежедневной выгрузки файла конфигурации.
`interval` *value*	Задание значения интервала (в минутах, принимает значения от 1 до 43200), через который будет производиться периодическая выгрузка файла конфигурации.
`memory-limit` *value*	Задание ограничения на общий объем, занимаемый бэкапами (в мегабайтах, принимает значения от 0 до 300) для устройства.
`post-commit`	Включение выгрузки файла конфигурации после каждого выполнения операции commit.
`pre-commit`	Включение выгрузки файла конфигурации перед каждым выполнением операции commit. Команда применяется в режиме настройки элемента резервирования конфигурации "backup to".
`password [encrypted]` *password*	Задание пароля пользователя, который будет использован при операциях выгрузки файла конфигурации на удаленный сервер в открытом или шифрованном виде.
`vrf` *vrf_name*	Имя экземпляра VRF, в котором будет осуществляться связь с указанным URL.
`source-address` { *IP_intf-addr* | *IPv6_intf-addr*}	Задание IP (IPv6) адреса, который будет использоваться в качестве IP-адреса отправителя при операциях выгрузки файла конфигурации на удаленный сервер. Следует указывать адрес, принадлежащий интерфейсу маршрутизатора в соответствующем VRF.
`commit`	Применение произведенных настроек.

Пример: настройка ежедневного сохранения файла конфигурации на удаленном сервере.

```
backup to tftp://192.168.16.119/ME5100/
  daily 24:00:00
  vrf mng
exit
```

Пример: настройка автосохранения файла конфигурации на устройстве после каждого выполнения операции commit.

```
backup to fs://backups
  post-commit
  memory-limit 250
exit
```

Сохраненные файлы конфигурации на устройстве можно посмотреть с помощью следующей команды:

show configuration backup

Пример: show configuration backup

```
0/ME5100:Router# show configuration backup
Wed Apr  3 17:01:06 2019
  ID                Date                      Stage
  ----------------- ------------------------- -------------------------
  0                 20190403_165328           post_commit
  1                 20190403_133440           post_commit
  2                 20190403_133322           post_commit
  3                 20190403_121717           post_commit
  4                 20190403_121708           post_commit
  5                 20190403_121638           post_commit
```

В случае сбоя или некорректных действий персонала по изменению конфигурации существует возможность быстрого возврата к предыдущей рабочей конфигурации.

Пример: откат конфигурации к предыдущей версии

```
0/ME5100:Router#commit backup 1_
```

Удаление конфигурации и возврат к заводским настройкам

При полной потере управления устройством существует возможность вернуться к заводским настройкам. Для этого необходимо:

на ME5100/ME5200

- Отключить питание;
- Включить питание при нажатой кнопке F (находится на передней панели). Удерживать кнопку в таком положении необходимо до начала мигания индикатора "RUN";
- Перезагрузить устройство по питанию.

на ME5000

- Отключить питание;
- Включить питание при нажатой кнопке F на плате FMC, которая в данный момент является мастером. Удерживать кнопку в таком положении необходимо до начала мигания индикатора "STATUS";
- Перезагрузить устройство по питанию.

Управление подсистемой SYSLOG

Syslog (системный журнал) — стандарт отправки и регистрации сообщений о происходящих в системе событиях, то есть создания событийных журналов, использующийся в сетях, работающих по протоколу IP. Фильтром заносимых в журнал сообщений является минимальная степень важности (severity) событий. Все системные события, имеющие важность равную или более высокую, чем заданная, подлежат записи в журнал событий устройства.

Согласно RFC3164, имеются следующие стандартные значения степеней важности:

Numerical Code	Severity
`0`	Emergency: system is unusable
`1`	Alert: action must be taken immediately
`2`	Critical: critical conditions
`3`	Error: error conditions
`4`	Warning: warning conditions
`5`	Notice: normal but significant condition
`6`	Informational: informational messages
`7`	Debug: debug-level messages

Таблица 21. Очистка системного журнала.

Команда	Назначение
`clear logging`	Очистить локальный журнал устройства.
`clear logging persistent [file file_name]`	Очистить файлы, сохраненные на диске устройства.

Таблица 22. Настройка системного журнала.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`logging buffered severity` *severity*	Задать минимальную степень важности (severity) сообщений, сохраняемых в локальном журнале устройства. Заданная степень важности используется в качестве фильтра — все системные события, имеющие важность равную или более высокую, чем заданная, подлежат записи в журнал событий устройства.

Команда	Назначение
`logging size` *file_size*	Задать максимальный размер файлов журнала, используемых системой журналирования устройства в процессе ротации. При достижении файлом заданного размера он подлежит ротации, при этом старый файл удаляется. Размер файла по умолчанию 10000 KiB.
`logging rotate` *file_count*	Задать количество файлов, используемых системой журналирования устройства в процессе ротации файлов журнала. Количество файлов журнала может принимать значения от 1 до 1000. **NOTE** Команду рекомендуется использовать совместно с logging buffered size. На системах, находящихся в эксплуатации, не следует задавать значения более 10; вместо этого рекомендуется использование удаленных серверов журналирования.
`logging crash-info rotate` *file_count*	Задать максимальное количество файлов, содержащих автоматический отчет о критических сбоях устройства. При превышении этого количества производится ротация файлов. Количество файлов может принимать значения от 1 до 50.
`logging cli-commands disable`	Отключить учет введенных пользователями команд в системе журналирования событий. По умолчанию режим логирования команд включен.
`logging netconf-ssh disable`	Отключить учет введенных пользователями по сессии "netconf over ssh" команд в системе журналирования событий. По умолчанию режим логирования команд включен.
`logging console` *severity*	Задать минимальную степень важности (severity) сообщений, выводимых на аппаратную консоль устройства.
`logging monitor` *severity*	Задать минимальную степень важности (severity) сообщений, которые будут отображаться в сессиях удаленного управления устройством (Telnet/SSH).
`logging control-plane internal`	Включить журналирование внутренних трассировок основного протокольного процесса и перейти в режим конфигурирования.
`limit` *file_size*	Задать максимальный размер архива.
`exit`	Выйти из режима конфигурирования.
`logging control-plane problem-detection`	Включить журналирование трассировок ошибок основного протокольного процесса и перейти в режим конфигурирования.
`limit` *file_size*	Задать максимальный размер архива.
`exit`	Выйти из режима конфигурирования.

Команда	Назначение
`logging control-plane signal`	Включить журналирование сигнальных трассировок основного протокольного процесса и перейти в режим конфигурирования.
`limit` *file_size*	Задать максимальный размер архива.
`exit`	Выйти из режима конфигурирования.
`logging persistent`	Включить режим журналирования на диске устройства и перейти в режим настройки его параметров.
`file` *file_name*	Указать имя файла журналирования и перейти в режим настройки параметров.
`severity` *severity*	Задать минимальную степень важности (severity) сообщений, отправляемых в файл.
`match` { `regex` *regular-expression* | `string` *string* | `subsystem` *subsystem* }	Задать условие, при соответствии которому сообщение будет отправлено в файл. • regex - содержит заданное регулярное выражение; • string - содержит заданную строку; • subsystem - сообщение указанной подсистемы.
`exit`	Выйти из режима настройки параметров записи файла.
`exit`	Выйти из режима logging persistent.
`logging host { IP_intf-addr | IPv6_intf-addr } [ vrf` *vrf_name* `]`	Включить отправку SYSLOG-сообщений на сервер удаленного журналирования и перейти в режим настройки параметров этого сервера (config-logging-host). В конфигурации устройства можно задавать несколько серверов удаленного журналирования.
`description` *name*	Задать имя хоста.
`severity` *severity*	Задать минимальную степень важности (severity) сообщений, отправляемых на удаленный сервер журналирования.
`match` { `regex` *regular-expression* | `string` *string* | `subsystem` *subsystem* }	Задать условие, при соответствии которому сообщение будет отправлено на удаленный сервер журналирования. • regex - содержит заданное регулярное выражение; • string - содержит заданную строку; • subsystem - сообщение указанной подсистемы.
`tcp` *port*	Установить режим работы по протоколу TCP для текущего удаленного сервера журналирования и задать номер используемого порта.
`udp` *port*	Установить режим работы по протоколу udp для текущего удаленного сервера журналирования и задать номер используемого порта.

Команда	Назначение
`commit`	Применение произведенных настроек.

Пример: настройка журналирования на удаленном сервере и записи в файл сообщений подсистемы if-mgr.

```
logging console debug
logging host 192.168.17.18 vrf mgmt-intf
  description "ME EMS 17-18"
exit
logging monitor notice
logging persistent
  file int
    match subsystem if-mgr
    exit
  exit
exit
logging rotate 15
logging size 100
```

Протокол управления сетью (SNMP)

SNMP (Simple Network Management Protocol — простой протокол сетевого управления) — стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур UDP/TCP. Протокол обычно используется в системах сетевого управления для контроля подключенных к сети устройств на предмет условий, которые требуют внимания администратора.

Маршрутизаторы серии ME поддерживают протокол версий SNMPv1, SNMPv2, SNMPv3.

Таблица 23. Настройка протокола SNMP.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`snmp server sysLocation` *descr*	Задание опциональных параметров SNMP-сервера. Добавить информацию о месте установки устройства или любую информацию для идентификации устройства в сети.
`snmp server sysContact` *descr*	Добавить информацию о контактах или любую информацию для администратора сети.
`snmp server trapMode {extended | standart}`	Отправлять стандартные (по умолчанию) или расширенные (резолвится if-index интерфейса в текстовое имя) SNMP-уведомления.
`snmp server dscp` *value*	Задание значения поля DSCP, с которым будут генерироваться IP-пакеты.

Команда	Назначение
`snmp server client-list` *name*	Создание списка хостов, которым разрешен доступ к SNMP-серверу и переход в режим его настройки (config-snmp-server-client-list).
`prefix` {*ipv4address* | *iv6address*}	Указание адреса хоста.
`range` {*ipv4address range* | *iv6address range*}	Указание диапазона адресов хостов.
`exit`	Возврат в режим глобальной конфигурации.
`snmp server view` *name*	(Опционально) Создание списка отображаемых идентификаторов объектов (OID) и переход в режим его настройки. Ответом на SNMP-запрос клиента будут только разрешенные администратором объекты, что позволяет повысить безопасность сети.
`oid-tree {excluded | excluded} oid` *oid*	Переход к описанию разрешенных/запрещенных для опроса объектов. OID задается в точечной нотации.
`exit`	Возврат в режим глобальной конфигурации.
`snmp server [ vrf vrf_name]`	Переход в режим настройки параметров SNMP-сервера (config-snmp-server-vrf). При запуске SNMP-сервера в каком-либо VRF (либо в глобальной таблице маршрутизации) устройство начинает принимать соединения по протоколу SNMP на тех своих интерфейсах, которые включены в указанный VRF.
`community label` *name*	Добавить краткое описание группы доступа. Переход в режим настройки параметров группы доступа. Имя группы доступа (community) отображается в конфигурации маршрутизатора в шифрованном виде. Если групп больше, чем одна, добавление краткого описания (community label) облегчает администратору сети идентификацию community.
`community-name {encrypted encrypted name | name}`	Задание имени группы доступа в открытом или шифрованном виде.
`address` {*ipv4address* | *iv6address*}	Указание адреса хоста для обращения к community
`rights` { ro | rw_}	Задание прав доступа. • `ro` — только чтение; • `rw` — чтение и запись.
`version {any|v1|v2c}`	Указание модели безопасности.
`view` *name*	Указание списка отображаемых объектов для этого community
`exit`	(Опционально) Возврат в режим настройки SNMP-сервера.

Команда	Назначение
`host {ipv4 address ipv4address | ipv6 address ipv4address| hostname}`	Указание адреса хоста, на который будут отправляться SNMP-уведомления и переход в режим их настройки.
`community` {encrypted *encrypted name* | *name*}	Задание имени группы доступа в открытом или шифрованном виде.
`port` *value*	(Опционально) Указание порта для приема SNMP-уведомлений на удаленном сервере (по умолчанию-162).
`user` *name*	Переход в режим конфигурации учетной записи пользователя SNMPv3
`authentication access {auth | priv}`	Выбор режима безопасности пользователя. • `auth` — только аутентификация; • `priv` — аутентификация и шифрование данных.
`authentication algorithm {sha1 | md5}`	Выбор алгоритма шифрования.
`authentication key {encrypted value | value}`	Задание ключа аутентификации в открытом или шифрованном виде.
`authentication access {auth | priv}`	Выбор режима безопасности пользователя. • `auth` — только аутентификация; • `priv` — аутентификация и шифрование данных.
`privacy algorithm` {aes128 | des}	Выбор алгоритма шифрования для priv-режима безопасности пользователя.
`privacy key` {encrypted *value* | *value*}	Задание ключа аутентификации для priv-режима безопасности пользователя в открытом или шифрованном виде.
`rights` { ro | rw_}	Задание прав доступа пользователя. • `ro` — только чтение; • `rw` — чтение и запись.
`commit`	Применение произведенных настроек.

Пример: настройка SNMPv2 сервера в GRT

```
snmp server vrf default
  community label public
    community-name encrypted 8CA10161B90C
    rights rw
  exit
  host 192.168.13.1
    community encrypted 8CA10161B90C
  exit
exit
```

Пример: настройка учетной записи пользователя SNMPv3

```
user tester
    authentication access auth
    authentication algorithm sha1
    authentication key encrypted CDE65039E5591FA3
    rights rw
  exit
```

Пример: Создание списка отображаемых идентификаторов объектов

```
snmp server view entPhysicalContainedIn
  oid-tree included
    oid 1.3.6.1.2.1.1
  exit
  oid-tree excluded
    oid 1.3.6.1.2.1.1.9
  exit
exit
```

Связки ключей (KEY-CHAIN)

Key chain - функционал, позволяющий создать общую для всех протоколов маршрутизации базу ключей аутентификации. Для каждого ключа указывается период времени его использования и метод аутентификации.

Аутентификация посредством key chain реализована для протоколов OSPFv2, OSPFv3, IS-IS. Если для аутентификации используется key chain, то нижеперечисленные узлы конфигурации протоколов маршрутизации игнорируются:

- authentication-id
- authentication-key
- authentication-type

Выбор ключей из key chain для аутентификации происходит следующим образом:

для входящего пакета OSPFv2/3

- ищется ключ с таким же идентификатором (ID), как и в полученном Hello-пакете;

для входящего пакета IS-IS

- для общей криптографической аутентификации (SHA1,256,384,512) аналогично OSPFv2/3;
- для HMAC-MD5 и Simple-password перебираются ключи, хранящиеся в соответствующем key chain, до тех пор пока, не найден такой же ключ как в полученном Hello-пакете. Связано это с тем, что в пакете не содержится ID ключа, с помощью которого был вычислен digest;

для исходящих пакетов протоколов OSPFv2, OSPFv3, IS-IS

- выбирается ключ с максимальным временем жизни. Если имеется несколько ключей с одинаковым lifetime, то применяется ключ с наибольшим ID.

Настройка key chain

Таблица 24. Последовательность настройки key chain

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`key-chain` *name*	Переход в режим конфигурирования key-chain.
`key` *key-id*	Задание идентификационного номера ключа и переход в режим его настройки.
`authentication-key [encrypted]` *key*	Задание ключа в открытом или шифрованном виде.
`authentication-type {hmac-md5 | hmacsha1 | hmacsha256 | hmacsha384 | hmacsha512 | simple-password}`	Выбор алгоритма аутентификации.
`accept-lifetime`	Переход в режим настройки периода времени использования ключа для приема входящих пакетов.
`start-time` *value*	Обязательный параметр! Задание времени начала действия ключа в формате YYYY.MM.DD-hh:mm:ss.
`duration` *value*	Задание времени действия ключа в секундах. Если параметр не задан, то ключ действует бесконечно.
`end-date-time` *value*	Задание окончания времени действия ключа в формате YYYY.MM.DD-hh:mm:ss. Если параметр не задан, то ключ действует бесконечно.
`exit`	Возврат в режим конфигурации ключа.
`send-lifetime`	Переход в режим настройки периода времени использования ключа для отправки исходящих пакетов.
`start-time` *value*	Обязательный параметр! Задание времени начала действия ключа в формате YYYY.MM.DD-hh:mm:ss.
`duration` *value*	Задание времени действия ключа в секундах. Если параметр не задан, то ключ действует бесконечно. При задании окончания времени действия ключа параметр "duration" игнорируется.
`end-date-time` *value*	Задание окончания времени действия ключа в формате YYYY.MM.DD-hh:mm:ss. Если параметр не задан, то ключ действует бесконечно.
`exit`	Возврат в режим конфигурации ключа.
`exit`	Возврат в режим конфигурации key-chain.
`exit`	Возврат в режим глобальной конфигурации.

Команда	Назначение
`commit`	Применение произведенных настроек.

Пример: конфигурация key-chain.

```
key-chain primero
  key 10
    accept-lifetime
      end-date-time 2022.09.01-00:00:00
      start-time 2022.08.01-00:00:00
    exit
    authentication-key encrypted 8CB1117FBF
    authentication-type simple-password
    send-lifetime
      end-date-time 2022.09.01-00:00:00
      start-time 2022.08.01-00:00:00
    exit
  exit
  key 20
    accept-lifetime
      start-time 2022.08.02-12:12:45
    exit
    authentication-key encrypted 8CA60A60B1
    authentication-type hmacsha1
    send-lifetime
      start-time 2022.08.02-12:12:45
    exit
  exit
  key 30
    accept-lifetime
      duration 30000
      start-time 2022.08.02-20:00:00
    exit
    authentication-key encrypted 9EB5116FB9
    authentication-type hmac-md5
    send-lifetime
      duration 30000
      start-time 2022.08.02-20:00:00
    exit
  exit
exit
```

Команды диагностики

Ниже перечислены show-команды, посредством которых можно получить информацию о валидности ключей в текущий момент времени.

show key-chain

Команда выводит статистику по всем key-chain'ам системы

Пример: show key-chain

```
0/ME5100# show key-chain
Thu Aug  4 15:52:31 2022
  Key-chain name : dos

    Number of keys         : 2
      Active send key-id   : none
      Active accept key-id : 1, 2

  Key-chain name : primero

    Number of keys         : 2
      Active send key-id   : 10, 20
      Active accept key-id : 10, 20

  Key-chain name : tres

    Number of keys         : 2
      Active send key-id   : 30, 40
      Active accept key-id : 30, 40

  Key-chain name : uno

    Number of keys         : 1
      Active send key-id   : 10
      Active accept key-id : 10
```

show key-chain detailed

Команда выводит детализированную статистику всем key-chain'ам системы

Пример: show key-chain detailed

```
0/ME5100# show key-chain primero detailed - статистика по выбранному key-chain
Thu Aug  4 15:57:47 2022
  Key-chain name : primero

    Number of keys         : 2
      Active send key-id   : 10, 20
      Active accept key-id : 10, 20

    Key ID                : 10
      Key password        : 8CB1117FBF
      Send   key validity : 2022.08.01-00:00:00 to 2022.09.01-00:00:00
      Accept key validity : 2022.08.01-00:00:00 to 2022.09.01-00:00:00
```

```
Key ID                : 20
  Key password        : 8CA60A60B1
  Send   key validity : 2022.08.02-12:12:45 to infinite
  Accept key validity : 2022.08.02-12:12:45 to infinite
```

ОБНОВЛЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Данный раздел содержит инструкции по обновлению программного обеспечения маршрутизаторов ЭЛТЕКС серии ME.

Подготовка

Для проведения обновления программного обеспечения необходимы следующие программы:

- Программа терминалов (TeraTerm, PuTTY, SecureCRT и аналоги);
- Программа TFTP-сервера, установленная на рабочей станции или удаленном сервере.

При обновлении ПО непосредственно с рабочей станции требуется:

1. Подключиться консольным кабелем к порту Console маршрутизатора;
2. Соединить Ethernet-порт рабочей станции с интерфейсом OOB маршрутизатора;
3. Запустить терминальную программу;
4. Настроить следующие параметры COM-порта рабочей станции: скорость передачи 115200 бод, формат данных 8 бит, без паритета, 1 бит стоповый, без управления потоком (115200-8N1);
5. Запустить на рабочей станции программу TFTP-сервера, в папку-корень сервера скопировать файл образа ПО маршрутизатора, имя вида `firmware_2.10.1.xxxR.me5100`;
6. Включить маршрутизатор, при помощи терминальной программы дождаться загрузки и приглашения `'login:'`;
7. Авторизоваться на маршрутизаторе, используя стандартные учётные данные `admin/password`;
8. Настроить на рабочей станции IP-адрес, например, `192.168.0.1/24`;
9. Настроить на OOB-порту маршрутизатора IP-адрес из той же подсети - например, `192.168.0.10/24`:

Пример

```
0/ME5100:EOS# config
0/ME5100:EOS(config)# interface mgmt 0/fmc0/1
0/ME5100:EOS(config-mgmt)# ipv4 address 192.168.0.10/23
0/ME5100:EOS(config-mgmt)# commit
Commit successfully completed in 3.246298 sec
0/ME5100:EOS(config-mgmt)# end
0/ME5100:EOS# show running-config interface mgmt 0/fmc0/1
interface mgmt 0/fmc0/1
  vrf mgmt-intf
  ipv4 address 192.168.0.10/23
```

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

При обновлении уже настроенного маршрутизатора данные шаги можно опустить, основным требованием является наличие сетевой связности между маршрутизатором и TFTP-сервером.

Перед выполнением дальнейших шагов нужно выполнить команду `show firmware`, статусы образов должны быть аналогичны следующему выводу:

Пример

```
0/ME5100:EOS# show firmware

  Unit              Image  Running  Boot          Version               Date
  ----------------- ------ -------- ------------- ---------------------
-----------------------
  0/ME5100          0      Yes      *             2.11.0.35R            26-Sep-2022
04:22:16
  0/ME5100          1      No                     2.11.0.1T             08-Aug-2022
04:50:02
0/ME5100:EOS#
```

Загрузка файла с образом программного обеспечения

Необходимо загрузить файл образа программного обеспечения с удаленного сервера в альтернативный раздел программного обеспечения маршрутизатора командой `copy`.

Для загрузки поддерживаются различные протоколы передачи (их перечень доступен в контекстной подсказке команды copy).

Пример для загрузки по TFTP

```
0/ME5100:EOS# copy tftp://192.168.0.1/firmware_3.0.0.177R.me5100 fs://firmware vrf
mgmt-intf

Downloading image file:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! OK
Verifying firmware image compatibility: ! OK
Firmware image MD5 checksum: 2703f324f7ed6dbcf0f1385b37776e44
Preparing partition: !! OK
Extracting firmware image:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! OK
Writing firmware image: !! OK
Firmware has been copied and installed successfully
0/ME5100:EOS#
```

NOTE При выполнении операции копирования все остальные сеансы работы с устройством блокируются и возможность открытия новых подключений к устройству становится временно недоступной (с выводом сообщения *"Netconf server doesn’t respond"*). Это является нормальным поведением.

Далее следует проверить, что загруженный образ помещен в альтернативный раздел:

```
0/ME5100:EOS# show firmware

  Unit              Image  Running  Boot          Version                Date
  ----------------- ------ -------- ------------- ---------------------
-----------------------
  0/ME5100          0      Yes      *             2.11.0.35R             26-Sep-2022
04:22:16
  0/ME5100          1      No                     3.0.0.177R             23-Nov-2022
00:04:21
0/ME5100:EOS#
```

Выбор альтернативного раздела в качестве загрузочного и перезагрузка

При помощи команды `firmware select alternate` установить альтернативный раздел в качестве загрузочного и убедиться в результате командой `show firmware`:

Пример

```
0/ME5100:EOS# firmware select alternate
0/ME5100:EOS# show firmware

  Unit              Image  Running  Boot          Version                Date
  ----------------- ------ -------- ------------- ---------------------
-----------------------
  0/ME5100          0      No       MIGRATE CUR*  3.10.0.771T            28-Jul-2025
16:34:43
  0/ME5100          1      Yes      FALLBACK      3.10.0.773T            29-Jul-2025
21:27:55
0/ME5100:EOS#
```

В случае, если производится обновление на ПО с более старой мажорной версией (откат), может понадобиться сохранение конфигурации старого образа. Это можно сделать, добавив параметр `keep-config`:

Пример

```
0/ME5100:EOS# firmware select alternate keep-config
0/ME5100:EOS#show firmware

  Unit              Image  Running  Boot          Version               Date
  ----------------- ------ -------- ------------ ---------------------
-----------------------
  0/ME5100          0      No       KEEP ALT*     3.10.0.771T           28-Jul-2025
16:34:43
  0/ME5100          1      Yes      FALLBACK      3.10.0.773T           29-Jul-2025
21:27:55
0/ME5100:EOS#
```

Перезагрузить маршрутизатор командой `reload system`, подтвердив действие нажатием клавиши `y`:

```
0/ME5100:EOS# reload system
Do you really want to reload system? (y/n): [n] y
```

Запуск маршрутизаторы и подтверждение новой версии

После успешного запуска маршрутизатора на новой версии программного обеспечения следует снова авторизоваться на нем с необходимыми учетными данными и получить таким образом доступ к командной строке устройства.

При авторизации будет выведено предупреждающее сообщение, что текущая версия ПО находится в режиме однократного запуска ('CONFIRMING') и для использования этой версии для последующих запусков устройства необходимо выполнить команду `firmware confirm`.

Пример

```
**********************************************
*****     System successfully started     *****
**********************************************

version 3.0.0.177R
EOS login: admin
Password:

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

Warning:
    Firmware upgrade is in progress (consult 'show firmware' for details).
    To finalize upgrade type 'firmware confirm'. Otherwise previous version
```

```
    will be used next time.
0/ME5100:EOS#
```

При помощи команды `show firmware` проверить состояние версий на активном и альтернативном разделах ПО:

```
0/ME5100:EOS# show firmware

  Unit              Image  Running  Boot          Version               Date
  ----------------- ------ -------- ------------- --------------------
----------------------
  0/ME5100          0      No       FALLBACK*     2.11.0.35R            26-Sep-2022
04:22:16
  0/ME5100          1      Yes      CONFIRMING    3.0.0.177R            23-Nov-2022
00:04:21
0/ME5100:EOS#
```

Новая версия должна находиться в статусе Running/CONFIRMING (в предыдущих версиях ПО статус обозначался как Running/TESTING). В маршрутизаторе предусмотрена система отката версии — при перезагрузке устройства из текущего состояния оно загрузится с предыдущего образа, находящегося в статусе FALLBACK. В случае, если текущая версия работает удовлетворительно, следует подтвердить ее использование командой `firmware confirm` и проверить результат командой `show firmware`.

Пример

```
0/ME5100:EOS# firmware confirm
0/ME5100:EOS# show firmware

  Unit              Image  Running  Boot          Version               Date
  ----------------- ------ -------- ------------- --------------------
----------------------
  0/ME5100          0      No                     2.11.0.35R            26-Sep-2022
04:22:16
  0/ME5100          1      Yes      *             3.0.0.177R            23-Nov-2022
00:04:21
0/ME5100:EOS#
```

При необходимости возврата к предыдущей версии следует перезагрузить маршрутизатор **до выполнения** `firmware confirm`. Обратите внимание, что обратное переключение на предыдущую версию в случае необходимости можно осуществить командой `firmware select alternate` аналогично описанному в начале инструкции методу, однако в этом случае может быть утеряна часть конфигурации устройства из-за перехода на более старую версию. Сохранность конфигурации при таком переключении версии "вниз" следует проконтролировать отдельно, выгрузив предварительно текстовую конфигурацию на внешний сервер командой `copy`.

Обновление загрузчиков X-Loader, U-Boot и микрокода FPGA

Обновление загрузчиков производится из командного режима с использованием протокола передачи файлов, к примеру tftp.

IMPORTANT	Необходимо обеспечить бесперебойное питание устройства во время обновления загрузчиков. Отключение устройства во время записи загрузчиков может привести к его полной неработоспособности.

Для обновления начального загрузчика X-Loader необходимо на tftp-сервере разместить файл *<VERSION>-me5100-xload.sec.img*, после чего скопировать его на устройство с использованием команды *copy*.

Пример

```
0/ME5100:EOS# copy tftp://192.168.0.1/3.0.0.177R-me5100-xload.sec.img fs://x-loader
vrf mgmt-intf

!!!
X-loader has been copied and updated successfully
0/ME5100:EOS#
```

IMPORTANT	Необходимо контролировать сообщения устройства при обновлении загрузчика X-loader. Если вместо сообщения "X-loader has been copied and updated successfully" устройство отвечает ошибкой вида "Error: failed to check image header", то для обновления следует воспользоваться образом загрузчика без модификатора .sec. (например, 2.10.1.5R-me5100-xload.img), аналогично проконтролировав наличие сообщения об успешном обновлении. В случае, если обновление загрузчика все-таки не происходит, необходимо остановить процесс обновления и обратиться в службу технической поддержки производителя.

Для обновления загрузчика U-Boot необходимо на tftp сервере разместить файл *<VERSION>-me5100-u-boot.sec.img*, после чего скопировать его на устройство с использованием команды *copy*.

Пример

```
0/ME5100:EOS# copy tftp://192.168.0.1/3.0.0.177R-me5100-u-boot.sec.img fs://u-boot vrf
mgmt-intf

!!!!!!!!!!!!
U-boot has been copied and updated successfully
0/ME5100:EOS#
```

Для обновления прошивки FPGA необходимо на tftp сервере разместить файл *FPGA_ME5100_v<VERSION>.img* (либо *ME5100_and_ME5100_revX_FPGA_EP3C5_v7.img*), после чего скопировать его на устройство с использованием команды *copy*.

Пример

```
0/ME5100:EOS# copy tftp://192.168.0.1/ME5100_and_ME5100_revX_FPGA_EP3C5_v7.img
fs://fpga vrf mgmt-intf
!!!!
FPGA has been copied and updated successfully
0/ME5100:EOS#
```

Удостовериться, что версии загрузчиков xloader и u-boot совпадают (в противном случае могут возникнуть проблемы с запуском устройства):

Пример

```
0/ME5100:EOS# show system versions

  ME5100
    Firmware: 3.0.0.177R (23-Nov-2022 00:04:21)
    X-Loader version: 3.0.0.177R (23-Nov-2022 06:14:21)
    U-boot version:   3.0.0.177R (23-Nov-2022 06:14:14)
    FPGA version:     0x07

0/ME5100:EOS#
```

Для вступления изменений в силу необходимо перезагрузить устройство с использованием команды *reload system*.

НАСТРОЙКА ЗАЩИТЫ CONTROL-PLANE

Control-plane (плоскость управления) в программной архитектуре маршрутизатора отвечает за работу различных протоколов и обработку служебного трафика. Все пакеты плоскости управления (control-plane) обрабатываются непосредственно центральным процессором (CPU) маршрутизатора. Настройка фильтров control-plane позволяет администратору устанавливать правила обработки входящих пакетов для защиты от сетевых атак и несанкционированного доступа.

В данной главе рассматриваются принципы настройки защиты уровня control-plane.

Основные принципы

1. По умолчанию (при отсутствии в конфигурации блока защиты control-plane) все входящие соединения к устройству разрешены. Соответственно, при запуске какого-либо сервиса (например, telnet-server) к нему смогут подключаться все хосты, которые имеют связность с устройством.
2. Конфигурирование защиты control-plane делится на два логических блока — защита сервисов, которые работают в Global Routing Table либо в сервисных VRF устройства (`control-plane inband`) и защита сервисов, работающих на Out-of-band интерфейсах (`control-plane out-of-band`).
3. Внутри каждого из блоков *in-band/out-of-band* конфигурируется набор правил, которые действуют на **входящие** сетевые соединения к устройству. Правила могут применяться как ко всем интерфейсам данного VRF (ключ `interface all`), либо к отдельным указанным. Для правил фильтрации не требуется указание VRF (правила будут автоматически работать в том VRF, к которому относится интерфейс).
4. Правила фильтрации действуют только на Layer3-интерфейсы устройства и при этом не действуют на транзитный трафик маршрутизатора.
5. Важно! Для каждого правила защиты control-plane действием по умолчанию является "запретить все остальные входящие соединения".

Настройка базовых правил защиты

Таблица 25. Последовательность настройки control-plane для интерфейса out-of-band управления и inband интерфейсов в GRT или сервисных VRF.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`control-plane` {*out-of-band*|*inband*} `interface mgmt` {*num*| all}	Переход в режим настройки фильтров control-plane интерфейса out-of-band управления или inband интерфейсов в GRT или сервисных VRF.

Команда	Назначение
`policy { drop | reject }`	Выбор действия при получении пакета, подпадающего под запрещающее правило: * `reject` - ответить сообщением ICMP Port unreachable (по умолчанию); * `drop` - отбросить (рекомендуется).
`allow` *protocol*	Указать протокол из перечисленных ниже. Входящие соединения (пакеты) указанных протоколов будут приниматься и обрабатываться маршрутизатором, остальные - отбрасываться. • `all` -- входящие пакеты всех протоколов; • `bfd` ; • `dhcp` ; • `dhcpv6` ; • `ftp` ; • `http` ; • `ftp` ; • `icmp` — с указанием типа icmp-сообщения; • `icmpv6` — с указанием типа icmp-сообщения; • `igmp` ; • `ldp` ; • `netconf` ; • `ntp` ; • `ospf` ; • `pim` ; • `rsvp` ; • `snmp` ; • `ssh` ; • `tcp` — tcp с указанием номера порта; • `telnet` ; • `tftp` ; • `udp` — udp с указанием номера порта. • `vrrp` ;
`any`	Принимать пакеты (соединения) от всех source-адресов для указанного протокола.
`peer-list` *PEER-LIST_NAME*	Перейти в режим настройки фильтрации сетевых соединений (пакетов) и пира.

Команда	Назначение
`peer` *PEER_NAME* { *source* | *destination*}	Перейти в режим явного указания source и destination-адресов.
`address` { *ipv4address* | *ipv4address/mask* | *ipv6address* | *ipv6address/mask* }	Указать IPv4 либо IPv6-адрес, пакеты от которого будут приниматься маршрутизатором.
`address-range` { *ipv4address-ipv4address* | *ipv6address-ipv6address* }	Указать диапазон IPv4- либо IPv6-адресов, пакеты от которого будут приниматься маршрутизатором.
`commit`	Применение произведенных настроек.

Пример. Настройка control-plane для интерфейса out-of-band управления — разрешить соединения по протоколу ssh с диапазоном адресов отправителей 172.168.16.1-172.168.20.0, а также фильтроваться будет tcp трафик с адресами отправителей 172.1.0.0/16.

```
control-plane out-of-band interface mgmt 0/fmc0/1
  allow ssh
    peer-list mgmt-network
      peer main
        source
          address-range 172.168.16.1-172.168.20.0
        exit
      exit
    exit
  exit
  allow tcp 777
    peer-list mgmt-network_ssh
      peer tcp
        source
          address 172.1.0.0/16
        exit
      exit
    exit
  exit
  policy drop
exit
```

IMPORTANT

Некорректная настройка control-plane может привести к потере удаленного управления маршрутизатором и частичной либо полной неработоспособности соответствующих сетевых сервисов.

Пример. Настройка защиты control-plane для интерфейсов inband — настройка фильтров для саб-интерфейса te0/0/7.3501, где фильтруются пакеты протокола LDP с адресом отправителя 7.7.7.7 и адресом адресата 99.99.99.99. Также фильтруются пакеты протокола ospfv2, где пакеты принимаются только от отправителей с адресом 177.1.1.1-178.2.4.1.

```
control-plane inband interface tengigabitethernet 0/0/7.3501
  allow ldp
    peer-list ldp_neighbor
      peer one
        destination
          address 99.99.99.99
        exit
        source
          address 7.7.7.7
        exit
      exit
    exit
  exit
  allow ospf
    peer-list ospf_neighbors
      peer first
        source
          address-range 177.1.1.1-178.2.4.1
        exit
      exit
    exit
  exit
exit
```

Настройка расширенных правил

Правила фильтрации control-plane также можно конфигурировать с учетом дополнительных параметров — фрагментации, типов сообщений ICMP, IPv4 опций, IPv6 extension headers, TTL, а также с ограничением потока данных и количества соединений.

Настройка фильтров Control-plane для фрагментированных и нефрагментированных IPv4-пакетов

Функционал Control-plane позволяет создавать правила фильтрации для фрагментированных и нефрагментированных IPv4-пакетов.

Чтобы отбросить фрагментированные пакеты, необходимо воспользоваться настройкой fragmentation-ipv4 negation. Таким образом маршрутизатор серии ME будет обрабатывать только нефрагментированные пакеты.

Для активации фильтра, что будет отбрасывать нефрагментированные пакеты — требуется применить настройку fragmentation-ipv4.

Пример. Настройка защиты control-plane для защиты от фрагментированных пакетов — Настройка правил на интерфейсе te0/0/15, где приниматься будут только нефрагментированные пакеты протокола snmp и адресом отправителя будет 172.1.2.1.

```
control-plane inband interface tengigabitethernet 0/0/15
  allow snmp
    peer-list snmp_users
      fragmentation-ipv4
      peer firstone
        source
          address 172.1.2.1
        exit
      exit
    exit
  exit
exit
```

Настройка фильтров на основе типов сообщений протокола ICMP

Правила Control-plane позволяют фильтровать соединения (пакеты) на основе типов сообщений протокола ICMP, в том числе на основе параметра code.

Устройства серии ME имеют следующие возможности фильтрации на основе типов сообщений протокола ICMP:

- *address-mask-reply* — Address mask reply type
- *address-mask-request* — Address mask request type
- *all* — All ICMP message types
- *destination-unreachable* — Destination unreachable type
- *echo* — Echo type
- *echo-reply* — Echo reply type
- *information-reply* — Information reply type
- *information-request* — Information request type
- *parameter-problem* — Parameter problem type
- *redirect* — Redirect type
- *source-quench* — Source quench type
- *time-exceeded* — Time exceeded type
- *timestamp-reply* — Timestamp reply type
- *timestamp-request* — Timestamp request type

Для каждого типа сообщений возможно также задать и код типа с помощью команды *code*.

Пример. Настройка фильтра Control-plane на основе типов сообщений протокола ICMP — пакеты протокола ICMP на всех интерфейсах управления будут отбрасываться все, кроме пакетов с типом 0(echo reply) и 8(echo). Диапазон адресов отправителей 172.1.1.1-173.2.1.1

```
control-plane out-of-band interface mgmt all
  allow icmp
    peer-list all_users
      icmp-type echo-reply
      exit
      icmp-type echo
      exit
      peer enough
        source
          address-range 172.1.1.1-173.2.1.1
        exit
      exit
    exit
  exit
exit
```

Настройка фильтров Control-plane на основе IPv4 options

Реализация функционала Control plane представляет возможность фильтровать трафик по полю options в заголовке пакета.

Маршрутизаторы серии ME имеют возможность фильтровать все существующие IPv4 option, а именно:

- *lsr* — Loose Source Route Option
- *mtup* — MTU Probe Option
- *mtur* — MTU Reply Option
- *no-op* — No Operation Option
- *rec-route* — Record Route Option
- *router-alert* — Router Alert Option
- *secur* — Basic Security Option
- *ssr* — Time Stamp Option
- *timestamp* — Strict Source Routing Option
- *traceroute* — Trace Route Option

Аргумент *any-specified* позволяет смягчить условия фильтра. Если в конфигурации установлено какое-либо значение option, то совместно с аргументом any-specified будем пропускать пакет, где в поле options находится установленное нами значение или(и) любое другое значение option. Например: если имеем в конфигурации настройку *option rec-route* и *any-specified*, то будут приниматься пакеты, где в поле option присутствует значение Record Route и(или) любое другое значение option.

Пример. Настройка фильтра, предназначенного для отбрасывания пакетов по значению IPv4 option — настройка правил на интерфейсе te0/0/7, где отбрасываются пакеты протокола udp с любым портом, которые не имеют в поле header опций Loose Source Route Option и Record Route Option. Адрес отправителя 172.5.1.44.

```
control-plane inband interface tengigabitethernet 0/0/7
  allow udp all
    peer-list udp_traffic
      ipv4-options try
        option lsr
        option rec-route
      exit
      peer first
        source
          address 172.5.1.44
        exit
      exit
    exit
  exit
exit
```

Настройка фильтров Control-plane для фрагментированных и нефрагментированных IPv6-пакетов

Функционал Control-plane позволяет создавать правила фильтрации для фрагментированных и нефрагментированных IPv6-пакетов.

Перейти к настройке управления фрагментированными и нефрагментированными пакетами возможно с помощью настройки fragmentation-ipv6 *NAME*.

Маршрутизаторы серии ME имеют возможность фильтровать ipv6 фрагментированные пакеты по следующим типам фрагментации:

- *ipv6-first* — first fragment
- *ipv6-id* — ID in range
- *ipv6-last* — last fragment
- *ipv6-more* — not last fragment
- *ipv6-res* — reserve fields are zero

При использовании аргумента *ipv6-id* необходимо задать диапазон фрагментированных пакетов, а именно с помощью настройки *ipv6-id-range* {first /| last}.

Аргумент negation применяется лишь при указании фильтрации по типу *ipv6-id-range*.

Пример. Настройка фильтра, предназначенного для отбрасывания фрагментированных пакетов — настройка правил на интерфейсе te0/0/1, где отбрасываются фрагментированные IPv6-пакеты, кроме последних 10 фрагментов. Адрес отправителя 2008:192:199:114::56

```
control-plane inband interface tengigabitethernet 0/0/1
  allow udp all
    peer-list udp_trx
      fragmentation-ipv6 fragIPv6
        ipv6-id-range
          last 10
        exit
        type ipv6-id
      exit
      peer user_first
        source
          address 2008:192:199:114::56
        exit
      exit
    exit
  exit
exit
```

Настройка фильтров Control-plane на основе IPv6 extension headers

Реализация функционала Control plane представляет возможность фильтровать по полю extension Header в header IPv6-пакета.

Маршрутизаторы серии ME имеют возможность фильтровать все IPv6 extension header, а именно:

- *auth* — Authentication header
- *dst* — Destination Options header
- *esp* — Encapsulating Security Payload header
- *frag* — Fragment header
- *hop* — Hop-by-hop Options header
- *none* — No next header
- *prot* — Protocol header
- *route* — Time Stamp Option
- *timestamp* — Protocol header

Аргумент any-specified позволяет смягчить условия фильтра. Если в конфигурации установлено какое-либо значение option, то совместно с аргументом any-specified будем пропускать пакет, где в поле extension header находится установленное нами значение или(и) любое другое значение option. Например: если имеем в конфигурации настройку option esp и any-specified, то будут приниматься пакеты, где в поле extension header присутствует значение Encapsulating Security Payload и(или) любое другое значение option.

Аргумент *negation* позволяет отбрасывать сообщения с extension headers кроме тех, что задали в конфигурации.

Пример. Настройка фильтра, предназначенного для отбрасывания пакетов по значению ipv6 extension header — настройка правил на саб-интерфейсе te0/0/7.4000, где отбрасываются пакеты протокола http, которые имеют в поле extension header опцию Hop-by-hop Options header. Адрес отправителя и адресата любой.

```
control-plane inband interface tengigabitethernet 0/0/7.4000
  allow http
    any
      ipv6-options 1
        negation
        option hop
      exit
    exit
  exit
exit
```

Настройка фильтров Control-plane на основе ограничения скорости потока данных и количества соединений

Функционал rate-hashlimit позволяет использовать следующие инструменты для фильтрации скорости потока данных:

- *burst* — пиковый объем трафика
- *expire* — в течение какого времени фильтр будет находиться в таблице правил
- *hashlimit-value* — объем информации фильтрации
- *mode* {destination-ip | destination-port | source-ip | source-port} — режим хэширования
- *period* {day | hour | minute | second}-- единица измерения времени для расчёта скорости потока данных
- *type* {above | up-to} — тип ограничения скорости потока данных

NOTE	burst изменяется в байтах, если hashlimit-rate измеряется в байтах/килобайтах/мегабайтах в единицу времени.

Для ограничения количества соединений необходимо использовать команду *connection-rate* {per-second | per-minute}.

NOTE	Настройка *connection-rate* используется только для следующих протоколов: dhcp, dhcpv6, igmp, ldp, ospf, pim, rsvp, ssh, tcp, telnet, udp, vrrp.

Пример. Настройка фильтра на основе ограничения скорости потока данных — пакеты протокола tcp с портом 145 на интерфейсе twe0/0/4 будут обрабатываться маршрутизатором со скоростью не более чем 100 мегабайт в секунду со значением burst равным 104915200 байт. В течение минуты возможно открыть лишь 10 tcp-сессий. Адрес отправителя 171.1.2.1 и адрес получателя 171.1.7.1

```
control-plane inband interface twentyfivegigabitethernet 0/0/4
  allow tcp 145
    peer-list tcp_traffic_banned
      peer userLast
        connection-rate per-minute 10
        destination
          address 171.1.7.1
        exit
        source
          address 171.1.2.1
        exit
      exit
      rate-hashlimit max
        burst 104915200
        hashlimit-value 100
        period second
        unit mbyte
      exit
    exit
  exit
exit
```

Настройка фильтров Control-plane на основе времени жизни пакета TTL

Правила Control-plane позволяют фильтровать соединения (пакеты) на основе времени жизни пакетов TTL.

Устройства серии ME имеют следующие возможности фильтрации на основе TTL:

- *ttl eq* — TTL пакета равно значению
- *ttl greater* — TTL пакета больше значения
- *ttl less* — TTL пакета меньше значения
- *ttl neq* — TTL пакета не равно значению

Пример. Настройка фильтра на основе времени жизни пакета TTL — пакеты протокола tftp на всех интерфейсах управления с адресами отправителей 192.168.1.0/24 будут отбрасываться, если не попадают в диапазон TTL 240-250

```
control-plane out-of-band interface mgmt all
  allow tftp
    peer-list upload
      peer oob_tftp
```

```
        source
          address 192.168.1.0/24
        exit
      exit
      ttl less 250
      ttl greater 240
    exit
  exit
exit
```

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 (либо включение IP unnumbered) и экземпляра VRF, к которому относится интерфейс;
- Параметры работы протокола ARP (для всех интерфейсов, кроме локальной петли, туннельных и bvi-интерфейсов) и режима ARP proxy;
- Включение и отключение отправки сообщений ICMP unreachable и ICMP redirect;
- Параметры максимального размера пакетов — MTU канального уровня и протокольные IP MTU (для физических, агрегирующих интерфейсов и сабинтерфейсов);
- Интервал подсчёта статистики по трафику (для всех интерфейсов, кроме локальной петли и bvi-интерфейсов);
- Параметры базовых ограничителей полосы (для всех интерфейсов, кроме локальной петли, туннельных и bvi-интерфейсов);
- Назначение политики QoS и классификаторов входящего трафика (для всех интерфейсов, кроме локальной петли, туннельных и bvi-интерфейсов);
- 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`:

Пример: интерфейс в режиме layer3 forwarding

```
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 интерфейсе. 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, описания интерфейса и режима отправки сообщений ICMP unreachables/redirects

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 26. Последовательность настройки IP-адресации и VRF на интерфейсе

Команда	**Назначение**
`configure`	Переход в режим глобальной конфигурации.
`interface` *type num*	Переход в режим настройки интерфейса.
`vrf` *vrf_name*	Назначение на интерфейсе экземпляра VRF.
`ipv4 address` *ipv4address/prefix*	Назначение на интерфейсе IPv4-адреса в формате CIDR (адрес/длина префикса).
`arp aging-time` *minutes*	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.
`ipv6 address` *ipv6address/prefix*	Назначение на интерфейсе IPv6-адреса.
`description` *descr*	Назначение на интерфейсе имени-описания. Описание следует заключать в кавычки в случае, если строка содержит символы пробела.
`ipv4 unreachables disable`	(Опционально) Запретить формирование пакетов ICMP unreachable при недоступности IPv4-хоста.
`ipv6 unreachables disable`	(Опционально) Запретить формирование пакетов ICMP unreachable при недоступности IPv6-хоста.
`ipv4 redirects disable`	(Опционально) Запрет формирования уведомлений хосту о том, что нужный ему адрес назначения теперь доступен через другой шлюз (ICMP redirects). IMPORTANT: Ввиду архитектурных особенностей устройства отправка ICMP redirect в ряде случаев не производится — в частности, при маршрутизации пакета коммутационным чипом устройства без перехвата на центральный процессор.

Команда	Назначение
`ipv6 redirects disable`	(Опционально) Запрет формирования уведомлений хосту о том, что нужный ему адрес назначения теперь доступен через другой шлюз (ICMP redirects). IMPORTANT: Ввиду архитектурных особенностей устройства отправка ICMP redirect в ряде случаев не производится — в частности, при маршрутизации пакета коммутационным чипом устройства без перехвата на центральный процессор.
`commit`	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 IP unnumbered

Данный функционал позволяет включить режим маршрутизации на интерфейсе без назначения ему IPv4/IPv6-адреса, путем заимствования IPv4/IPv6-адреса, уже настроенного на одном из интерфейсов маршрутизатора. Необходимо помнить, что unnumbered-интерфейс заимствует свой адрес у запущенного и работающего интерфейса, поэтому рекомендуется указывать в качестве источника IPv4/IPv6-адреса Loopback-интерфейс.

Если на интерфейсе используется IP unnumbered, то на нем не могут быть назначены адреса командами *"ipv4 address/ipv6 address"*.

Таблица 27. Последовательность настройки IP unnumbered на интерфейсе

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`interface` *type num*	Переход в режим настройки интерфейса.
`vrf` *vrf_name*	Назначение на интерфейсе экземпляра VRF.

Команда	Назначение
`ipv4 unnumbered` *type num*	Включение IP unnumbered на интерфейсе и задание интерфейса-источника IPv4-адреса.
`ipv6 unnumbered` *type num*	Включение IP unnumbered на интерфейсе и задание интерфейса-источника IPv6-адреса.
`arp aging-time` *minutes*	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.
`arp proxy`	Включение proxy ARP.
`description` *descr*	Назначение на интерфейсе имени-описания. Описание следует заключать в кавычки в случае, если строка содержит символы пробела.
`commit`	Применение произведенных настроек.

Последовательность настройки функционала IP unnumbered

1. Создать Loopback-интерфейс, назначить на нем IPv4/IPv6 адрес.
2. Создать сабинтерфейс.
3. Включить на сабинтерфейсе ip unnumbered и указать интерфейс, IP-адрес которого будет использоваться в качестве Source в IP-пакетах (лучше использовать Loopback)
4. Прописать статический маршрут до клиентского хоста, указав в качестве шлюза созданный сабинтерфейс.
5. Если нужна связность между клиентскими хостами, то на сабинтерфейсах необходимо включить режим proxy ARP.

Пример:

В VRF "client" нужно выделить IP-адреса трем клиентам. Первый клиент доступен через интерфейс te 0/0/1.101, второй-через te 0/0/1.102, третий-через te 0/0/1.103. Между первым и третьим хостом должна быть связность.

Создаем Loopback-интерфейс, назначаем на нем IPv4 адрес из сети, выделенной для клиентских подключений, назначаем VRF.

```
0/ME5100:Router# configure
0/ME5100:Router(config)# interface loopback 100
0/ME5100:Router(config-loopback)# description "office"
0/ME5100:Router(config-loopback)# vrf client
0/ME5100:Router(config-loopback)# ipv4 address 100.1.1.1/24
0/ME5100:Router(config-loopback)# exit
```

Создаем сабинтерфейсы в том же VRF, что и Loopback, на первом и третьем включаем proxy ARP.

```
0/ME5100:Router(config)#
0/ME5100:Router(config)# interface te 0/0/1.101
0/ME5100:Router(config-tengigabitethernet-sub)# description "office-1"
0/ME5100:Router(config-tengigabitethernet-sub)# encapsulation outer-vid 101
0/ME5100:Router(config-tengigabitethernet-sub)# ipv4 unnumbered loopback 100
0/ME5100:Router(config-tengigabitethernet-sub)# arp proxy
0/ME5100:Router(config-tengigabitethernet-sub)# exit
```

```
0/ME5100:Router(config)#
0/ME5100:Router(config)# interface te 0/0/1.102
0/ME5100:Router(config-tengigabitethernet-sub)# description "office-2"
0/ME5100:Router(config-tengigabitethernet-sub)# encapsulation outer-vid 102
0/ME5100:Router(config-tengigabitethernet-sub)# ipv4 unnumbered loopback 100
0/ME5100:Router(config-tengigabitethernet-sub)# exit
```

```
0/ME5100:Router(config)#
0/ME5100:Router(config)# interface te 0/0/1.103
0/ME5100:Router(config-tengigabitethernet-sub)# description "office-1"
0/ME5100:Router(config-tengigabitethernet-sub)# encapsulation outer-vid 103
0/ME5100:Router(config-tengigabitethernet-sub)# ipv4 unnumbered loopback 100
0/ME5100:Router(config-tengigabitethernet-sub)# arp proxy
0/ME5100:Router(config-tengigabitethernet-sub)# exit
```

Прописываем статические маршруты

```
0/ME5100:Router(config)#
0/ME5100:Router(config)# router static vrf client
0/ME5100:Router(config-vrf)# address-family ipv4 unicast
0/ME5100:Router(config-unicast)# destination 100.1.1.101/32 0.0.0.0 interface te
0/0/1.101
0/ME5100:Router(config-tengigabitethernet-sub)# exit
0/ME5100:Router(config-unicast)# destination 100.1.1.102/32 0.0.0.0 interface te
0/0/1.102
0/ME5100:Router(config-tengigabitethernet-sub)# exit
0/ME5100:Router(config-unicast)# destination 100.1.1.103/32 0.0.0.0 interface te
0/0/1.103
0/ME5100:Router(config-tengigabitethernet-sub)# exit
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. 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). Для интерфейсов 40G и 100G поддержана технология коррекции ошибок (Forward Error Correction — FEC). 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 28. **Последовательность настройки MTU, режима интерфейса и интервала подсчета статистики**

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`interface` *type num*	Переход в режим настройки интерфейса.
`mtu` *l2_mtu_bytes*	Установка канального MTU в байтах.
`ip mtu` *ip_mtu_bytes*	Установка IP MTU в байтах.
`speed` { 10 | 100 | 1G | 10G | 40G | 100G | auto }	Задание скорости физического интерфейса.
`duplex` { half | full | auto }	Задание дуплекса физического интерфейса.
`fec` { auto | cl74 | cl91 | off }	Задание режима коррекции ошибок (FEC) для интерфейсов hundredgigabitethernet и fortygigabitethernet, где: **auto** - режим автоопределения FEC (дефолтный режим для 100G-интерфейсов); **cl74** - помехоустойчивое кодирование включено по cl74 (R-FEC); **cl91** - помехоустойчивое кодирование включено по cl91 (RS-FEC); **off** - режим помехоустойчивого кодирования отключен (дефолтный режим для 40G-интерфейсов).
`load-interval` *seconds*	Установка интервала подсчета загрузки интерфейса в секундах.
`commit`	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 29. **Последовательность настройки базовых ограничителей полосы**

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`interface` *type num*	Переход в режим настройки интерфейса.
`rate-limit input` *input_rate_kbps*	Установка ограничения полосы для входящего трафика, в килобитах в секунду.
`shape output` *output_rate_kbps*	Установка ограничения полосы для исходящего трафика, в килобитах в секунду.
`commit`	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 30. **Последовательность назначения классификаторов трафика и политик QoS**

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`interface` *type num*	Переход в режим настройки интерфейса.
`tc-map input` *tcmap_index*	Установка классификатора входящего в интерфейс трафика. *tcmap_index* — номер предварительно сконфигурированного классификатора.
`service-policy output` *servicepolicy_name*	Установка политики QoS для исходящего из интерфейса трафика. *servicepolicy_name* — имя предварительно сконфигурированной политики QoS.
`commit`	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
```

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 продолжат 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 определенным узлами) в один и тот же интерфейс-участник агрегации. Метод "round-robin" отправляет каждый последующий пакет в следующий по очереди составляющий линк (т.н. попакетная балансировка), 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 МЕ 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 31. **Последовательность создания и настройки агрегирующего интерфейса**

Команда	**Назначение**
`configure`	Переход в режим глобальной конфигурации.
`lacp interface tengigabitethernet` *num*	Добавление физического линка в агрегированный интерфейс и переход в режим настройки его параметров агрегации.

Команда	Назначение
`bundle id` *bundle_id*	Привязка физического интерфейса к указанному номеру агрегированного интерфейса системы.
`bundle mode { active | passive | off }`	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.
`timeout { short | long }`	(Опционально) Выбор режима работы LACP — "slow" (**long**) или "fast" (**short**).
`exit`	Возврат в режим глобальной конфигурации. Далее можно повторить перечисленные шаги, добавив требуемые интерфейсы в состав агрегированного соединения.
`lacp interface bundle-ether` *bundle_id*	Создание вспомогательного элемента — блока настройки параметров агрегации интерфейса **bundle-ether** и переход в режим настройки этих параметров. Команда является обязательной.
`active-links max` *max_links*	(Опционально) Указание максимально возможного количества активных участников агрегированного интерфейса. При наличии большего количества участников они будут переводиться в неактивное состояние.
`active-links min` *min_links*	(Опционально) Указание минимально требуемого количества активных участников агрегированного интерфейса. В случае, если количество активных участников опустится ниже данного значения, агрегированный интерфейс будет принудительно деактивирован.
`exit`	Возврат в режим глобальной конфигурации.
`interface bundle-ether` *bundle_id*	Создание в системе агрегированного интерфейса и переход в режим его настройки.
`ipv4 address` *ipv4address/prefix*	(Опционально) Задание IPv4-адреса на интерфейсе.
`commit`	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 local-address 11.11.11.1
  bfd address-family ipv4 neighbor 11.11.11.2
  bfd multiplier 5
  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. Всего на одном физическом интерфейсе можно создать до 4000 сабинтерфейсов. Максимальное количество сабинтерфейсов в системе зависит от модели маршрутизатора и указано в соответствующем техническом описании.

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	До версии ПО 2.0.1 включительно в качестве VLAN-тегов распознавались только теги с TPID 0x8100. Начиная с версии 2.2.0, на каждом из физических интерфейсов можно указать TPID для внешних и внутренних тегов при помощи команды **"encapsulation-map outer-type { 8100 | 88a8 | 9100 } [inner-type { 8100 | 88a8 | 9100 }]"**. Данная настройка будет применяться для **всех** сабинтерфейсов соответствующего физического интерфейса. По умолчанию применяется TPID 0x8100/0x8100.

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 икапсулируется в Ethernet-кадр с автоматическим добавлением тех VLAN-тегов, которые заданы на сабинтерфейсе в качестве классификатора инкапсуляции.

Таблица 32. **Последовательность создания и настройки L3-сабинтерфейса**

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

Пример L3-сабинтерфейса с двойным VLAN-тегированием

```
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 33. Последовательность создания и настройки L2-сабинтерфейса

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.

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

*Таблица 34. Настройка правил '**rewrite egress tag**' на L2-сабинтерфейсе*

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

*Таблица 35. Настройка правил '**rewrite ingress tag**' на L2-сабинтерфейсе*

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`interface { tengigabitethernet | bundle-ether }` *num.subif_id*	Создание сабинтерфейса и переход в режим настройки его параметров.
`rewrite ingress tag pop {one | two}`	Снять один или два тега с принятого Ethernet-кадра.
`rewrite ingress tag push outer-vid` *outer-vid* `[inner-vid` *inner-vid* `]`	Добавить один или два тега на принятый Ethernet-кадр.
`rewrite inress tag replace outer-vid` *outer-vid* `[inner-vid` *inner-vid* `]`	Заменить один (верхний) или два тега на принятом Ethernet-кадре.
`rewrite ingress tag exchange`	Поменять местами внешний и внутренний теги на принятом Ethernet-кадре.
`commit`	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 36. Включение подсчета загрузки сабинтерфейсов

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`[no] system subint-utilization`	Включение подсчета загрузки для всех сабинтерфейсов системы. Отрицательная форма команды отключает подсчет. По умолчанию подсчет загрузки на сабинтерфейсах выключен.
`commit`	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, состояния и VRF, к которым они отнесены.

Пример: show ipv4 interfaces brief

```
0/ME5100:Router# show ipv4 interfaces brief
Wed Dec 15 15:43:49 2021
  Interface             IPv4 address        State                VRF
  --------------------- ------------------- -------------------- ----
  te 0/0/5              100.100.12.1/31     Up                   default
  te 0/0/6              100.100.24.1/31     LowLayerDwn          default
  te 0/0/7              100.100.23.1/31     LowLayerDwn          default
  te 0/0/17.10004000    4.4.4.4/24          LowLayerDwn          l3-1
  te 0/0/17.10004001    1.1.1.1/24          Up                   l3-1
  te 0/0/17.20004000    172.16.0.0/31       Up                   l3-1
  lo 1                  2.2.2.2/32          Up                   default
  lo 7991               3.1.3.1/32          Up                   l3-1
  mgmt0/fmc0/1          172.17.0.32/24      Up                   mgmt-intf
```

show interfaces description

Команда выводит в табличном виде перечень интерфейсов с указанием их описаний (description), сконфигурированных 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 об их текущих состояниях и режиме работы.

show interfaces summary

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

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.

Настройка протокола VRRP

VRRP (Virtual Router Redundancy Protocol) — сетевой протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию.

Увеличение доступности достигается путём объединения группы маршрутизаторов в один виртуальный маршрутизатор и назначения им общего IP-адреса, который и будет использоваться как шлюз по умолчанию для устройств сети. Фактически, виртуальный маршрутизатор — это группа интерфейсов маршрутизаторов, которые находятся в одной сети, и разделяют Virtual Router Identifier (VRID) и виртуальный IP-адрес (VIP). Один маршрутизатор может состоять в нескольких группах, каждая из которых должна иметь свою уникальную пару VIP/VRID. Пара VIP/VRID должна быть одинаковой на всех маршрутизаторах одной сети.

VRRP имеет две версии: VRRPv2 и VRRPv3. VRRPv2 применим только к сетям, использующим протокол IPv4. VRRPv3, в свою очередь, работает как с IPv4, так и с IPv6. На маршрутизаторах серии ME поддержаны обе версии.

VRRP Master — VRRP-маршрутизатор, который отвечает за отправку пакетов на IP-адрес, ассоциированный с виртуальным маршрутизатором, и за ответы на ARP-запросы, отправленные на этот адрес. Если владелец IP-адреса доступен, то он всегда становится мастером.

VRRP Backup — это группа маршрутизаторов, которые находятся в режиме ожидания и

готовы взять на себя роль мастера, как только текущий VRRP Master станет недоступным.

VRRP-маршрутизатор может находиться в одном из трех состояний: Initialize, Backup, Master. Эти состояния маршрутизатор последовательно меняет.

В состоянии "Initialize" маршрутизатор ожидает начала работы. Если этот маршрутизатор является владельцем VIP адреса, то есть IP-адрес интерфейса такой же как и виртуальный IP-адрес (приоритет равен 255), то маршрутизатор отправляет сообщения о том, что он становится мастером. Он также отправляет Gratuitous ARP-запрос, в котором MAC-адрес источника равен адресу виртуального маршрутизатора. Затем он переходит в состояние "Master". Если маршрутизатор не является владельцем VIP, то он переходит в состояние Backup.

Мастер постоянно рассылает сообщения на широковещательный адрес 224.0.0.18 для IPv4 и FF02:0:0:0:0:0:0:12 для IPv6, чтобы сообщить Backup-маршрутизаторам, что он работает. Мастер отправляет сообщения с интервалом (advertise interval), равным по умолчанию одной секунде для VRRPv2 и одной миллисекунде для VRRPv3. При этом в качестве MAC адреса отправителя используется адрес группы 00:00:5E:00:01:xx, где xx — VRID в шестнадцатеричном формате.

Если Backup-маршрутизатор не получает сообщения в течение трех advertise interval'ов, то он отправляет VRRP-сообщение о том, что собирается стать мастером. Затем отправляет широковещательное VRRP-сообщение, в котором MAC-адрес источника равен адресу этого виртуального маршрутизатора. В данном сообщении маршрутизатор указывает свой приоритет.

Новым мастером становится маршрутизатор с наибольшим приоритетом. При одинаковых значениях приоритета у нескольких Backup-маршрутизаторов мастером становится маршрутизатор с наибольшим собственным IP-адресом.

Таблица 37. Создание и настройка роутера VRRP

Команда	**Назначение**
`configure`	Переход в режим глобальной конфигурации.
`router vrrp`	Создание виртуального маршрутизатора и переход в режим его конфигурации.
`gratuitous-arp refresh VALUE`	(Опционально) Задание интервала в секундах, с которым VRRP-маршрутизатор, находящийся в состоянии "master" отправляет gratuitous ARP-сообщения. По умолчанию gratuitous ARP-сообщения отправляются только один раз, в момент перехода в состояние "master".
`gratuitous-arp refresh-repeat VALUE`	(Опционально) Задание числа gratuitous ARP-сообщений, отправляемых VRRP-маршрутизатором при переходе в состояние "master". Дефолтное значение-2.
`interface TYPE NUM`	Включение протокола VRRP на L3-интерфейсе и переход в режим его конфигурации.

Команда	Назначение
`address-family ipv4 vrrp VRRP-ID`	Задание идентификатора группы (VRID) интерфейса для работы с IPv4 и переход в режим ее конфигурации.
`description STRING`	(Опционально) Назначение имени-описания для VRRP-группы. Описание следует заключать в кавычки в случае, если строка содержит символы пробела.
`priority VALUE`	Задание приоритета локального маршрутизатора для VRRP-группы в диапазоне 1-254. Значение по умолчанию-100.
`timers advertise VALUE`	(Опционально) Задание временного интервала (в секундах) между отправкой мастером VRRP-сообщений. Дефолтное значение - 1. На всех маршрутизаторах VRRP должны быть одинаковые значения timers advertise.
`preempt disable`	Включение запрета перехвата роли мастера. Backup-маршрутизатор с более высоким приоритетом не будет пытаться перехватывать роль мастера у текущего Master-маршрутизатора с более низким приоритетом. Исключение из этого правила — VRRP-маршрутизатор всегда будет становиться мастером, если он владелец IP-адреса, который присвоен виртуальному маршрутизатору независимо от этого флага (приоритет 255)
`preempt delay VALUE`	Указание времени в секундах, которое Backup-маршрутизатор будет ждать, прежде чем объявить себя мастером, взять под контроль виртуальный IP-адрес и начать маршрутизацию пакетов. Дефолтное значение-0.
`virtual-ip IPv4_ADDRESS`	Указание виртуального IPv4-адреса.
`source-ip IPv4_ADDRESS`	Указание собственного IPv4-адреса интерфейса.
`version { 2 | 3 }`	(Опционально, только для IPv4) Выбор версии протокола VRRP. Версия 3 не имеет обратной совместимости с версией 2.
`shutdown`	(Опционально) Административное отключение протокола VRRP на L3-интерфейсе.
`root`	Возврат в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

Настройка VRRP для IPv6 в целом производится аналогично, но отличается задание параметров `virtual-ip` и `source-ip`.

Таблица 38. В режиме конфигурации протокола VRRP на L3-интерфейсе IPv6

Команда	Назначение
`interface TYPE NUM`	Включение протокола VRRP на L3-интерфейсе и переход в режим его конфигурации.
`address-family ipv6 vrrp VRRP-ID`	Задание идентификатора группы (VRID) интерфейса для работы с IPv6 и переход в режим ее конфигурации.
`virtual-ip global IPv6_ADDRESS`	Указание виртуального глобального IPv6-адреса.
`virtual-ip link-local { IPv6_ADDRESS | autoconfig }`	Указание виртуального локального IPv6-адреса вручную либо при помощи автоконфигурирования. По умолчанию применяется значение `'autoconfig'`.
`source-ip IPv6_ADDRESS`	Указание собственного локального IPv6-адреса

Пример конфигурации роутера VRRP для IPv4 и IPv6

```
router vrrp
  interface tengigabitethernet 0/0/1.67
    address-family ipv4
      vrrp 67
        priority 200
        source-ip 67.1.1.151
        virtual-ip 67.1.1.5
      exit
    exit
    address-family ipv6
      vrrp 66
        source-ip fe80::aaf9:4bff:fe8b:bc21
        virtual-ip global 2001:67::15
        virtual-ip link-local fe80::200:5eff:fe00:242
      exit
    exit
  exit
exit
```

Диагностические команды

show vrrp

Команда выводит информацию о состоянии VRRP-маршрутизаторов.

Пример. show vrrp

```
0/ME5100:Router# show vrrp
Fri Nov  1 16:13:20 2024
  Interface               VRRP ID   Priority  Virtual IP                    State
Role
  ----------------------- --------- --------- ------------------------------
-------------------- --------------------
  te0/0/1.67              67        200       67.1.1.5                      running
```

```
master
  te0/0/1.67              66        100       fe80::200:5eff:fe00:242         running
master
```

show vrrp statistics

Команда выводит информацию об отправленных и принятых пакетах VRRP-групп.

Пример. show vrrp statistics

```
0/ME5100:Router# show vrrp statistics
Fri Nov  1 16:13:49 2024
  te0/0/1.67:
    Address-family: IPv4
      VRID: 67
        Become master:          1
        Release master:         0
        Advertise send:         16715
        Advertise receive:      1
        Priority zero send:     0
        Priority zero receive:  0
        Errors:
          Packet length errors:                0
          IP TTL errors:                       0
          Invalid type errors:                 0
          Address list errors:                 0
          Advertise interval errors:           0
          Router version errors:               0
          Authentication failures errors:      0
          Invalid auth type errors:            0
          Authentication type mismatch errors:  0
    Address-family: IPv6
      VRID: 66
        Become master:          1
        Release master:         0
        Advertise send:         16715
        Advertise receive:      2
        Priority zero send:     0
        Priority zero receive:  0
        Errors:
          Packet length errors:                0
          IP TTL errors:                       0
          Invalid type errors:                 0
          Address list errors:                 0
          Advertise interval errors:           0
          Router version errors:               0
          Authentication failures errors:      0
          Invalid auth type errors:            0
          Authentication type mismatch errors:  0
```

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 39. Настройка статических маршрутов в GRT

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`router static`	Переход в режим конфигурации статической маршрутизации в глобальной таблице.
`address-family { ipv4 | ipv6 } unicast`	Переход в режим настройки IP unicast-маршрутов.
`destination` *ip_network ip_nexthop*	Создание статического маршрута на подсеть *ip_network* с адресом следующего узла *ip_nexthop* и переход в режим конфигурации опциональных параметров данного маршрута.
`description` *descr*	Назначение маршруту имени-описания. Описание следует заключать в кавычки в случае, если строка содержит символы пробела.
`interface { null | tengigabitethernet | bundle-ether | fortygigabitethernet | hundredgigabitethernet | tunnel-ip | tunnel-rsvp | mgmt | twentyfivegigabitethernet}` *num*	(Опционально) Указание интерфейса, через который будет направлен маршрут и переход в режим настройки дальнейших опциональных параметров.
`bfd fast-detect`	(Опционально) Включение быстрого детектирования обрыва связи до следующего узла (nexthop). **Не применяется для tunnel-ip-, tunnel-rsvp-, mgmt-интерфейсов.**
`metric`	(Опционально) Установка метрики маршрута.
`exit`	(Опционально) Возврат в режим настройки опциональных параметров маршрута.

Команда	Назначение
`tag` *tag*	(Опционально) Указание внутреннего числового тега, который может быть впоследствии использован при фильтрации маршрута правилами редистрибуции.
`commit`	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
      description "the way to the unknown"
      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 40. Настройка статических маршрутов внутри экземпляра VRF

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`router vrf` *vrf_name*	Включение маршрутизации в указанном экземпляре VRF и переход в режим настройки основных параметров маршрутизации для него.
`static`	Переход в режим конфигурации статической маршрутизации в текущем экземпляре VRF.
`address-family { ipv4 | ipv6 } unicast`	Переход в режим настройки IP unicast-маршрутов.
`destination` *ip_network ip_nexthop*	Создание статического маршрута на подсеть *ip_network* с адресом следующего узла *ip_nexthop* и переход в режим конфигурации опциональных параметров данного маршрута.

Команда	Назначение
`description` *descr*	Назначение маршруту имени-описания. Описание следует заключать в кавычки в случае, если строка содержит символы пробела.
`interface { null | tengigabitethernet | bundle-ether | fortygigabitethernet | hundredgigabitethernet | tunnel-ip | tunnel-rsvp | mgmt | twentyfivegigabitethernet}` *num*	(Опционально) Указание интерфейса, через который будет направлен маршрут и переход в режим настройки дальнейших опциональных параметров.
`bfd fast-detect`	(Опционально) Включение быстрого детектирования обрыва связи до следующего узла (nexthop). **Не применяется для tunnel-ip-, tunnel-rsvp-, mgmt-интерфейсов.**
`metric`	(Опционально) Установка метрики маршрута.
`exit`	(Опционально) Возврат в режим настройки опциональных параметров маршрута.
`tag` *tag*	(Опционально) Указание внутреннего числового тега, который может быть впоследствии использован при фильтрации маршрута правилами редистрибуции.
`commit`	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
Thu May 29 11:21:53 2025

  Route Source       IPv4 Routes    IPv6 Routes
  ----------------   -------------- --------------
  static             0              1
  connected          153            8
  local              155            10
  ospf               5              4
  isis               1              0
  bgp                0              0
  rip                0              1
  lfa                0              0
  summary address    0              0
  default origin     0              0
  FIB installed      310            21
```

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`. Внутри данного конфигурационного блока настраивается OSPFv2 как для глобальной таблицы, так и для имеющихся на маршрутизаторе экземпляров VRF.

На устройстве возможно создать до 16 процессов маршрутизации OSPF.

Дальнейшая конфигурация блока `router ospfv2` 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.

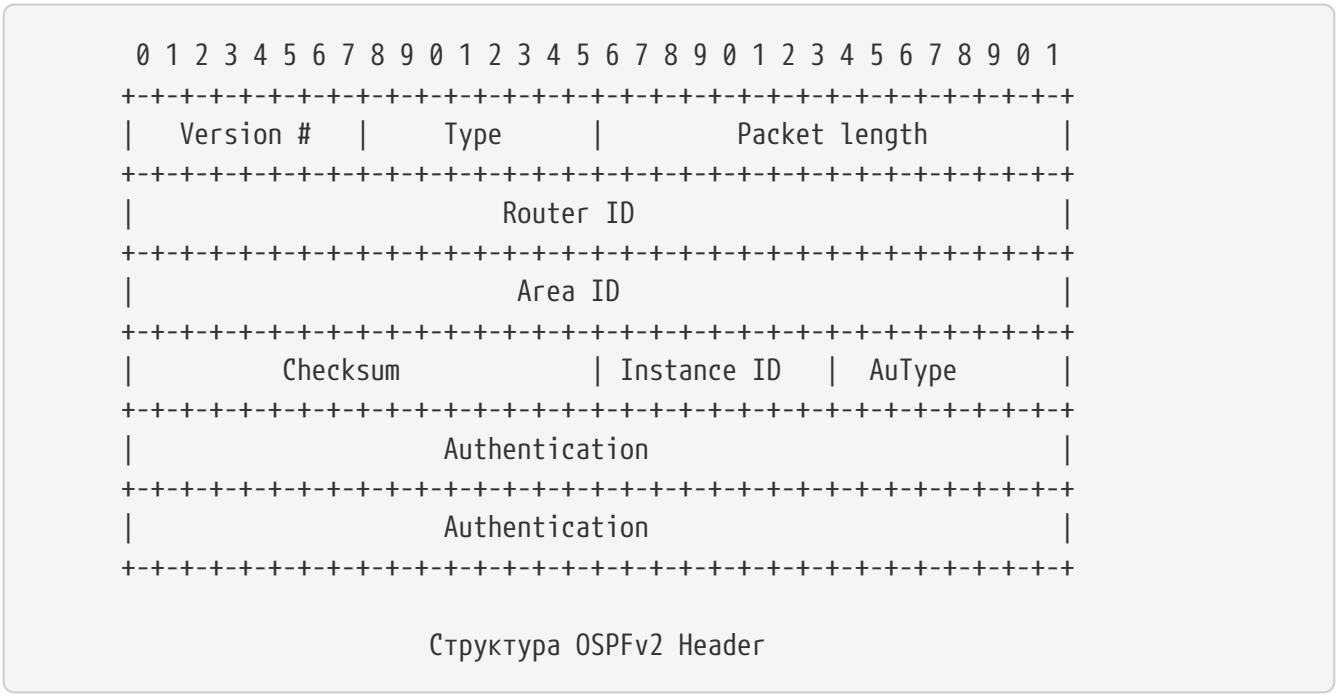
Таким образом, последовательность конфигурирования протокола OSPF выглядит следующим образом:

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.

Поддержка Instance ID

На маршрутизаторах семейства ME реализован механизм поддержки нескольких

экземпляров протокола, работающих на одном интерфейсе, описанный в RFC 6549. Этот документ расширяет RFC 2328 механизмом дифференциации пакетов для различных экземпляров, отправляемых и получаемых на одном и том же интерфейсе.
Для поддержки этой возможности, измененный формат заголовка пакета с полем "Authentication Type" разделяется на поле "Instance ID" и поле "AuType".



Структура OSPFv2 Header

Все поля, за исключением поля идентификатора экземпляра OSPFv2 (Instance ID), определены в RFC 2328. Для Instance ID выделяются первые 8 бит поля "AuType", тем самым поле "AuType" уменьшается до 8 бит без изменений в значении.

Instance ID позволяет использовать несколько экземпляров OSPFv2 на одном интерфейсе. Каждому экземпляру протокола на маршрутизаторе присваивается отдельный идентификатор экземпляра OSPFv2.

В заголовке OSPFv2-пакета устанавливается идентификатор экземпляра OSPFv2 интерфейса (Instance ID). Instance ID используется для упрощения демультиплексирования пакета и связывания его с правильным экземпляром OSPFv2. Полученные пакеты с Instance ID, не равным ни одному из настроенных Instance ID экземпляров OSPFv2 на принимающем интерфейсе, отбрасываются.

Определены следующие идентификаторы экземпляров OSPFv2:

- 0 - базовый экземпляр IPv4 - это экземпляр маршрутизации IPv4 по умолчанию, соответствующий одноадресной маршрутизации IPv4 по умолчанию и таблице маршрутизации IPv4 оператора. Использование этого идентификатора экземпляра обеспечивает обратную совместимость с базовой спецификацией OSPF;
- 1 - базовый экземпляр многоадресной рассылки IPv4 - этот экземпляр IPv4 соответствует отдельной таблице маршрутизации IPv4, используемой для проверки пересылки обратного пути (RPF), выполняемой для многоадресного трафика IPv4 (multicast traffic);
- 2 - управление in-band;

- 3-127 - частное использование, определяемое администратором локальной сети.

Поскольку поле заголовка "AuType" OSPFv2 было уменьшено с 2 октетов до 1 октета, маршрутизаторы, не поддерживающие RFC 6549, не смогут выполнить аутентификацию пакетов для любого экземпляра, кроме экземпляра по умолчанию (то есть базового экземпляра IPv4 Unicast, с Instance ID равным нулю).

Базовая настройка протокола OSPFv2

Настройка протокола производится согласно описанной выше иерархии.

Таблица 41. Базовая настройка протокола OSPFv2

Команда	**Назначение**
`configure`	Переход в режим глобальной конфигурации.
`router ospfv2` *OSPF_NAME*	Создание процесса маршрутизации OSPFv2 с именем *OSPF_NAME* и переход в режим его настройки.
`router-id` *X.X.X.X*	Задание идентификатора узла сети (Router ID) в формате IPv4-адреса.
`instance-id` *instance-id*	(Опционально) Указание идентификатора экземпляра процесса OSPF (Instance ID). Принимает значения 0..127. По умолчанию значение Instance ID равно нулю.
`area` *Y.Y.Y.Y*	Создание в конфигурации OSPF-зоны (area) и переход в режим её настройки. Backbone-зоной является зона с номером `0.0.0.0`.
`nssa`	(Опционально) Указание текущей зоны в качестве OSPF NSSA ('not-so-stubby area').
`stub`	(Опционально) Указание текущей зоны в качестве OSPF Stub area.
`interface { bundle-ether | bvi | fortygigabitethernet | gigabitethernet | hundredgigabitethernet | loopback | tengigabitethernet | tunnel-ip | twentyfivegigabitethernet }` *num*	Добавление соответствующего интерфейса (либо сабинтерфейса) в указанную зону OSPF и переход в режим настройки OSPF-параметров этого интерфейса.
`dead-interval { minimal |` *SECONDS* `}`	(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.
`hello-interval` *SECONDS*	(Опционально) Установка интервала отправки HELLO-пакетов на текущем интерфейсе, в секундах.

Команда	Назначение
`fast-hello-multiplier` *PACKETS*	(Опционально) Установка количества HELLO-пакетов, которые будут отправляться с интерфейса за секунду при работе в режиме OSPF fast hello. Принимает значения 2..20.
`metric` *METRIC*	(Опционально) Устанавливает протокольную "стоимость" (иначе — метрику) интерфейса. Принимает значения 0..65535. **IMPORTANT** 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.
`vlan-pcp` *value*	(Опционально) Устанавливает значение приоритета L2 CoS (p-bit) в отправляемых с интерфейса пакетах протокола OSPF. Принимает значения 0..7.
`mtu-ignore`	(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.
`network { broadcast | nbma | point-to-multipoint | point-to-point }`	(Опционально) Указание типа OSPF-подсети на интерфейсе. Значение по умолчанию "broadcast". 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.
`passive`	(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 `loopback`).

Команда	Назначение
`priority` *ROUTER_PRIORITY*	(Опционально) Установка приоритета маршрутизатора для участия в выборах Designated router. Принимает значения 0..255.
`exit`	Возврат в режим настройки OSPF-зоны.
`exit`	Возврат в режим настройки OSPF-процесса.
`exit`	Возврат в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

Пример. Базовая настройка протокола OSPFv2

```
router ospfv2 test
  area 0.0.0.0
    interface loopback 1
      passive
    exit
    interface tengigabitethernet 0/0/12
      network point-to-point
    exit
    interface tengigabitethernet 0/0/13
      metric 20
      network point-to-point
    exit
  exit
  area 0.0.0.100
    interface bundle-ether 7.400
      metric 250
      network point-to-point
    exit
    stub
  exit
  router-id 1.1.1.1
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 42. Настройка протокола OSPFv2 для экземпляра VRF

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`router ospfv2` *OSPF_NAME*	Создание процесса маршрутизации OSPFv2 с именем *OSPF_NAME* и переход в режим его настройки.
`vrf` *VRF_NAME*	Запуск процесса маршрутизации OSPFv2 в указанном VRF и переход в режим настройки этого процесса.
`router-id` *X.X.X.X*	Задание идентификатора узла сети (Router ID) в формате IPv4-адреса.
`area` *Y.Y.Y.Y*	Создание в конфигурации OSPF-зоны (area) и переход в режим её настройки. Backbone-зоной является зона с номером `0.0.0.0`.
`nssa`	(Опционально) Указание текущей зоны в качестве OSPF NSSA ('not-so-stubby area').
`stub`	(Опционально) Указание текущей зоны в качестве OSPF Stub area.
`interface { bundle-ether | bvi | fortygigabitethernet | gigabitethernet | hundredgigabitethernet | loopback | tengigabitethernet | tunnel-ip | twentyfivegigabitethernet }` *num*	Добавление соответствующего интерфейса (либо сабинтерфейса) в указанную зону OSPF и переход в режим настройки OSPF-параметров этого интерфейса.
`dead-interval { minimal |` *SECONDS* `}`	(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.
`hello-interval` *SECONDS*	(Опционально) Установка интервала отправки HELLO-пакетов на текущем интерфейсе, в секундах.
`fast-hello-multiplier` *PACKETS*	(Опционально) Установка количества HELLO-пакетов, которые будут отправляться с интерфейса за секунду при работе в режиме OSPF fast hello. Принимает значения 2..20.
`metric` *METRIC*	(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.

Команда	Назначение
`mtu-ignore`	(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.
`network { broadcast | nbma | point-to-multipoint | point-to-point }`	(Опционально) Указание типа OSPF-подсети на интерфейсе. Значение по умолчанию "broadcast".
`passive`	(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 `loopback`).
`priority` *ROUTER_PRIORITY*	(Опционально) Установка приоритета маршрутизатора для участия в выборах Designated router. Принимает значения 0..255.
`exit`	Возврат в режим настройки OSPF-зоны.
`exit`	Возврат в режим настройки OSPF-процесса внутри VRF.
`exit`	Возврат в режим настройки OSPF-процесса.
`exit`	Возврат в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

Пример. Настройка OSPFv2 для экземпляра VRF.

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

```
      interface bundle-ether 6.400
        metric 250
        network point-to-point
      exit
      stub
    exit
    router-id 1.1.1.1
  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 43. Настройка протокола BFD для OSPF-соседств

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

Пример. Настройка протокола BFD для OSPF-интерфейса.

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

Редистрибуция маршрутной информации

Механизм редистрибуции позволяет передать в OSPF маршруты из других протоколов (IGP/EGP, 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. **rip** — маршрутная таблица протокола RIP;
6. **static** — статические маршруты.

Таблица 44. Настройка редистрибуции в OSPF маршрутной информации из других протоколов.

Команда	**Назначение**
`configure`	Переход в режим глобальной конфигурации.
`router ospfv2` *OSPF_NAME*	Создание процесса маршрутизации OSPFv2 с именем *OSPF_NAME* и переход в режим его настройки.

Команда	Назначение
`redistribution { bgp | connected | isis | local | rip | static }` *RULE_NAME*	Создание правила редистрибуции с именем *RULE_NAME* из указанного источника (bgp/connected/isis/local/rip/static) и переход в режим настройки этого правила.
`match prefix` *IPv4PREFIX/MASK*	Указание фильтра, используемого для данного правила. При указании такого фильтра правило будет действовать только на маршруты, строго совпадающие с заданным *IPv4PREFIX/MASK*.
`metric-type { ospf-type1-external | ospf-type2-external}`	Назначить на маршруты, прошедшие через данное правило, метрику типа "OSPF External 1" либо "OSPF External 2".
`metric-value` *METRIC*	Установить значение OSPF-метрики для маршрутов, прошедших через данное правило.
`priority` *RULE_PRIORITY*	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.
`redistribute disable`	Запретить редистрибуцию маршрутов, попавших в текущее правило. При выполнении данной команды текущее правило становится запрещающим.
`exit`	Выход из режима настройки правила редистрибуции. Далее можно настроить следующие правила — для того же самого источника, либо для других источников редистрибуции.
`root`	Выход в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

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

```
router ospfv2 test
  area 0.0.0.0
    interface loopback 1
      passive
    exit
    interface tengigabitethernet 0/0/5
      bfd fast-detect
    exit
    interface tengigabitethernet 0/0/7
      bfd fast-detect
    exit
  exit
```

```
  redistribution connected CONNECT-OSPF
    match prefix 100.65.0.0/24
    priority 10
    redistribute disable
  exit
  redistribution connected CONNECT-OSPF-20
    metric-type ospf-type1-external
    metric-value 300
    priority 20
  exit
  router-id 1.1.1.1
exit
```

Multi-area link

Протокол динамической маршрутизации OSPF может работать с одной зоной (single area) или с многими (multi area). С ростом сети, работающей в одной зоне, лавинообразно увеличивается таблица маршрутизации, база данных линков LSDB, время выполнения алгоритма построения дерева и поиска маршрутов. Кроме того, любое изменение в сети (например, если где-то на удалённом участке линк то появляется, то пропадает), приводит к полному перерасчёту OSPF на всех маршрутизаторах, что увеличивает нагрузку на процессор. Сегментирование сети на зоны решает эти проблемы.

Однако, может возникать необходимость пересылать трафик между маршрутизаторами зоны, отличной от area 0, используя высокоскоростной канал между двумя граничными маршрутизаторами зоны (ABR).

Пример топологии

```
                R1-------Backbone------R2
                 |                      |
               Area 1                 Area 1
                 |                      |
                R3--------Area 1--------R4
```

Линк между R1 и R2 является высокоскоростным, и желательно пересылать трафик area 1 между R1 и R2 по нему. Однако, поскольку путь внутри зоны предпочтительнее, R1 всегда будет направлять трафик к R4 через area 1 по каналам с более низкой скоростью и пересылать трафик через R3 к сетям area 1, подключенным к R2.

RFC 5185 предлагает изящное решение - сконфигурировать multi-area линк (на примере выше - между маршрутизаторами R1 и R2), относящийся как к area 0, так и area 1.

Таблица 45. Настройка multi-area линка

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.

Команда	Назначение
`router ospfv2` *OSPF_NAME*	Создание процесса маршрутизации OSPFv2 с именем *OSPF_NAME* и переход в режим его настройки.
`router-id` *X.X.X.X*	Задание идентификатора узла сети (Router ID) в формате IPv4-адреса.
`area` *0.0.0.0*	Создание в конфигурации OSPF Backbone-зоны(area) и переход в режим её настройки. Backbone-зоной является зона с номером `0.0.0.0`.
`interface { bundle-ether | bvi | fortygigabitethernet | gigabitethernet | hundredgigabitethernet | loopback | tengigabitethernet | tunnel-ip | twentyfivegigabitethernet }` *num*	Добавление соответствующего интерфейса (либо сабинтерфейса) в указанную зону OSPF и переход в режим настройки OSPF-параметров этого интерфейса.
`exit`	Выход из режима интерфейсных параметров OSPF.
`exit`	Выход в режим конфигурации процесса OSPF.
`area` *Y.Y.Y.Y*	Создание в конфигурации OSPF-зоны (area) и переход в режим её настройки.
`multi-area-interface { tengigabitethernet | bundle-ether | fortygigabitethernet | hundredgigabitethernet | tunnel-ip }` *num*	Добавление сконфигурированного ранее интерфейса backbone-зоны к настраиваемой зоне.
`neighbor` *ipv4address*	(Опционально) Указание IP-адреса соседа. **Нейбор указывается, если тип OSPF-подсети на интерфейсе отличен от `point-to-point`.**
`commit`	Применение произведенных настроек.

Пример. Настройка multi-area линка.

```
router ospfv2 1
    area 0.0.0.0
      interface loopback 5
        passive
      exit
      interface tengigabitethernet 0/0/1.2
      exit
    exit
    area 0.0.0.2
      interface loopback 2
        passive
      exit
      multi-area-interface tengigabitethernet 0/0/1.2
        neighbor 100.2.2.150
      exit
    exit
```

```
    router-id 5.5.5.31
  exit
exit
```

Убедиться в работоспособности multi-area линка можно с помощью show-команд.

В приведенных примерах интерфейс te0/0/1.2 принадлежит area 0 и area 2.

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

  Routing Process: 1, ID 5.5.5.31
    Router is an area border router

  Neighbor ID      Area ID       Pri  State            BFD        Dead Time  Last
state change  Address          Interface
  ---------------- ------------- ---- ---------------- ---------- ----------
----------------- ---------------- ----------
  5.5.2.30         0.0.0.0       1    full-BDR         active     00:00:35   02d03h29m
100.2.2.150      te0/0/1.2
  5.5.2.30         0.0.0.2       --   full             --         00:00:34   02d03h29m
100.2.2.150      MA te0/0/1.2
```

```
0/ME5100:Router## show  ospfv2 neighbors  detailed
Wed Oct 25 16:49:34 2023
  Routing Process: 1, ID 5.5.5.31
    Router is an area border router

      Interface Loopback2, state: loopback, status: up Area 0.0.0.2

      Interface Loopback5, state: loopback, status: up Area 0.0.0.0

      Interface Tengigabitethernet0/0/1.2, state: designated-router, status: up Area
0.0.0.0

        Neighbor: 100.2.2.150, router-id: 5.5.2.30, permanence: dynamic
          State: full, relationship has changed 5 time(s)
          Priority: 1, oper-status: up
          Router state of this neighbor: backup-designated-router
          Retransmission queue length: 0
          Hellos is not suppressed
          LSAs awaiting a response: 0
          Dead time: 00:00:30
          Last state change: 02d03h32m ago
          Restart helper status: not-helping, time-remaining: 0 seconds, exit reason:
none
          Local OSPF interface address: 100.2.2.151, Interface Index: 366
          BFD status: active

      Multi Area Interface Tengigabitethernet0/0/1.2, state: point-to-point, status:
```

```
up, Area 0.0.0.2

        Neighbor: 100.2.2.150, router-id: 5.5.2.30
          State: full, relationship has changed 12 time(s)
          Retransmission queue length: 0
          LSAs awaiting a response: 0
          Dead time: 00:00:30
          Last state change: 02d03h32m ago
          Restart helper status: not-helping, time-remaining: 0 seconds, exit reason:
none
          Local OSPF interface address: 100.2.2.151, Interface Index: 366
          Session authentication: disabled
```

Аутентификация OSPF

Маршрутизаторы семейства ME позволяют использовать аутентификацию OSPF-соседства.

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

Также для настройки аутентификации можно воспользоваться командой `'authentication-key-chain'`. При использовании этой команды узлы конфигурации, заданные командами `'authentication-key'`, `'authentication-id '`, `'authentication-type'`, игнорируются.

Также для настройки аутентификации можно воспользоваться командой `'authentication-key-chain'`. При использовании этой команды узлы конфигурации, заданные командами `'authentication-key'`, `'authentication-id '`, `'authentication-type'`, игнорируются.

Таблица 46. Настройка аутентификации OSPFv2

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`router ospfv2` *OSPF_NAME*	Переход в режим настройки процесса маршрутизации.
`area` *Y.Y.Y.Y*	Переход в режим настройки зоны OSPF.
`interface { bundle-ether | bvi | fortygigabitethernet | gigabitethernet | hundredgigabitethernet | loopback | tengigabitethernet | tunnel-ip | twentyfivegigabitethernet }` *num*	Переход в режим настройки параметров OSPF требуемого интерфейса.
`authentication-type { hmacsha1 | hmacsha256 | hmacsha384 | hmacsha512 | md5 | none | simple-password }`	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.

Команда	Назначение
`authentication-key { KEY_STRING | encrypted KEY_ENCRYPT }`	Задание ключа для аутентификации в открытом (*KEY_STRING*) либо в зашифрованном (*KEY_ENCRYPT*) виде.
`authentication-id authentication-id`	Задание идентификатора ключа. Дефолтное значение - 1. При выборе типа аутентификации *simple-password* параметр `authentication-id` игнорируется.
`exit`	Выход из режима интерфейсных параметров OSPF. Далее можно настроить параметры аутентификации на других требуемых интерфейсах.
`root`	Выход в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

Таблица 47. С использованием key-chain.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`router ospfv2 OSPF_NAME`	Переход в режим настройки процесса маршрутизации.
`area Y.Y.Y.Y`	Переход в режим настройки зоны OSPF.
`interface { bundle-ether | bvi | fortygigabitethernet | gigabitethernet | hundredgigabitethernet | loopback | tengigabitethernet | tunnel-ip | twentyfivegigabitethernet } num`	Переход в режим настройки параметров OSPF требуемого интерфейса.
`authentication-key-chain KEY_CHAIN_NAME`	Указание имени списка ключей (`key-chain`), который будет использоваться для аутентификации.
`root`	Выход в режим глобальной конфигурации.
`commit`	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
```

Пример. Настройка OSPF-аутентификации с использованием ключа.

```
router ospfv2 test
```

```
  area 0.0.0.0
    interface tengigabitethernet 0/0/5
      authentication-key-chain new
    exit
  exit
exit
```

IMPORTANT	Список ключей (`key-chain`) должен быть заранее создан в конфигурации маршрутизатора.

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 всем процессам 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 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
```

Для просмотра информации об отдельном OSPF процессе в show-команде необходимо указать имя процесса.

show ospfv2 instance new

Команда выводит общее состояние и статистику по процессу маршрутизации OSPFv2 с именем "new".

Пример. show ospfv2 instance new

```
0/ME5100:Router# show ospfv2 instance new
```

```
Fri Mar  1 14:55:55 2024
  Routing process: new, ID 5.5.5.31
    Instance ID: 5
    Router is not an area border router
    Graceful restart: not-restarting, remaining time: 0, reason: none
    OSPF traffic engineering: disabled
    Traffic engineering disabled, router ID: 200.151.1.1
    The maximum delay before the Routing Table is recalculated: 5000
    Route max equal cost paths are stored: 5
    External LSA refresh interval: 1800 secs
    Full SPF calculation: 00h10m46s ago
    LSA timers:
      Minimum time between originations: 5000 msec
      Minimum time between receptions: 1000 msec
      Time to increase minimum originations interval: 0 msec
      Maximum time to delay originations: 0 msec
    Number of new LSA originated: 6
    Number of new LSA received: 21
    Number of AS-External LSA (type 5): 19, checksum: 0x000a54a4
    Number of AS-Opaque LSA  (type 11): 0, checksum: 0x00000000
    Number of LSA in LSDB at checksum check: 0
    Number of updates: 0 pending, 0 merged
    Errors count:
      Header length errors:            0
      Header errors:                   0
      No interface for virtual link:   0
      Version field is invalid:        0
      Invalid or unrecognized address: 0
      Resource errors:                 0
    Packets dropped by unknown reason: 0

      Area 0.0.0.0, up
        Area can carry data traffic: false
        SPF algorithm executed, times: 6
        Number of area border routers: 0, autonomous routers: 2
        Number of translator state changes: 0
        NSSA Border router state: disabled
        Number of LSA type-1: 2, checksum: 0x00014612
        Number of LSA type-2: 0, checksum: 0x00000000
        Number of LSA type-3: 0, checksum: 0x00000000
        Number of LSA type-4: 0, checksum: 0x00000000
        Number of LSA type-7: 0, checksum: 0x00000000
        Number of LSA type-10: 0, checksum: 0x00000000
        Total count of LSAs: 2, checksum: 0x00014612
        Number of interfaces in this area: 2
```

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      Area ID          Pri    State            BFD          Dead Time
Address          Interface
  ---------------- ---------------- ------ ---------------- ------------ ----------
---------------- ----------
  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 [detailed]

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

Пример. show ospfv2 interfaces detailed

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

  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 Tengigabitethernet 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 Tengigabitethernet 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 Tengigabitethernet 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
```

Вышеприведенные команды отображают информацию о всех процессах OSPF, настроенных глобально (в GRT).
Для просмотра информации о процессах в VRF в show-команде необходимо указать имя VRF. При выборе VRF *all* будет выводиться запрошенная информация по всем VRF.

show route vrf test ospf

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

Пример. show route vrf test ospf

```
0/ME5100:Router# AR31-17-151# show route vrf test ospf

Tue Feb 20 15:09:50 2024
  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 E2   2.2.2.0/24    via 100.101.31.2 [110/0], 00h00m20s, te0/0/1.3
  O EA   5.5.0.30/32    via 100.101.31.2 [30/2], 00h00m20s, te0/0/1.3
  O E2   13.13.13.0/24    via 100.101.31.2 [110/0], 00h00m20s, te0/0/1.3
  O E2   28.1.1.0/24    via 100.101.31.2 [110/0], 00h00m20s, te0/0/1.3
```

Дополнительная диагностика

Unexpected non-zero DR

Сообщение "Unexpected non-zero DR" отображается при получении пакета с ненулевым значением в поле DR.

Пример.

На двух маршрутизаторах настроен протокол OSPFv2, на одной стороне настроен broadcast на интерфейсе, на другой стороне point-to-point.

Пример конфигурации R1

```
0/ME5100:R1# show running-config router ospfv2
router ospfv2 1
  area 0.0.0.0
```

```
    interface tengigabitethernet 0/0/4
    exit
  exit
  router-id 1.1.1.1
exit
0/ME5100:R1#
```

Пример конфигурации R2

```
0/ME5100:R2# show running-config router ospfv2
router ospfv2 1
  area 0.0.0.0
    interface tengigabitethernet 0/0/4
      network point-to-point
    exit
  exit
  router-id 2.2.2.2
exit
0/ME5100:R1#
```

При такой конфигурации на R2 будут сообщения вида:

```
0/ME5100:R2# 2025-09-23T10:07:53+07:00 %OSPF_V2-I-ADJCHANGE: Unexpected non-zero DR
192.168.3.2 in hello packet from interface te0/0/4
0/ME5100:R2# 2025-09-23T10:08:13+07:00 %OSPF_V2-I-ADJCHANGE: Unexpected non-zero DR
192.168.3.2 in hello packet from interface te0/0/4
```

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`. Внутри данного конфигурационного блока настраивается IS-IS как для глобальной таблицы, так и для имеющихся на маршрутизаторе экземпляров VRF.

На устройстве возможно создать до 16 процессов маршрутизации IS-IS.

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

Таблица 48. Базовая настройка протокола IS-IS

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`router isis` *ISIS_NAME*	Создание процесса маршрутизации IS-IS с именем *ISIS_NAME* и переход в режим его настройки.
`net` *NET*	Задание системного IS-IS Network Entity Title (NET) в формате XX.XXXX.XXXX.XXXX.XXXX.00. Данный параметр уникально идентифицирует систему во всем IS-IS-домене.
`is-level { level-1 | level-1-2 | level-2 }`	(Опционально) Выбор уровня IS, в котором будет работать система. По умолчанию используется значение 'level-1-2'.
`host-name` *HOSTNAME*	(Опционально) Задание IS-IS hostname — имени узла, которое будет указываться в соответствующих TLV служебных пакетов IS-IS. По умолчанию используется системное имя устройства (`'hostname'`).
`set-overload-bit full-db disable`	(Опционально) Не устанавливать флаг "IS-IS overload bit", когда маршрутизатор перегружен. По умолчанию overload bit устанавливается в LSP для оповещения соседей о том, что маршрутизатор не может использоваться для передачи транзитного трафика. **IMPORTANT** флаг "IS-IS overload bit" не снимается автоматически при исчезновении перегрузки. Снять его можно командой `"clear isis overload"`.
`level { level-1 | level-2 }`	Переход в режим настройки параметров уровня 1 или уровня 2 (для обоих уровней параметры настраиваются одинаково).
`metric-style { wide | both }`	(Опционально) Выбор типа метрики для текущего уровня IS-IS. По умолчанию для маршрутов IPv4 используется режим "both", смешанный, метрики как "narrow", так и "wide". При этом, при получении internal/external-маршрутов с метрикой "narrow" маршрутизатор приводит internal/external-маршруты с метрикой "narrow" к маршрутам без признака internal/external, но с метрикой "wide" и передаёт их в SPF.
`set-overload-bit on-startup` *SECONDS*	(Опционально) При указании данного параметра при старте процесса IS-IS в системе будет устанавливаться флаг "IS-IS overload bit" на *SECONDS* секунд после запуска.
`set-overload-bit persist`	(Опционально) При указании данного параметра флаг "IS-IS overload bit" будет установлен в системе постоянно.
`exit`	Возврат в режим настройки процесса IS-IS.

Команда	Назначение
`interface { loopback | tengigabitethernet | bundle-ether | fortygigabitethernet | hundredgigabitethernet | tunnel-ip | twentyfivegigabitethernet }` *num*	Добавление соответствующего интерфейса (либо сабинтерфейса) в процесс IS-IS и переход в режим настройки параметров протокола IS-IS для этого интерфейса.
`address-family { ipv4 | ipv6 } unicast`	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 `ipv4 unicast`, `ipv6 unicast` или обе AFI/SAFI.
`exit`	Возврат в режим настройки интерфейса IS-IS.
`circuit-level { level-1 | level-1-2 | level-2 }`	(Опционально) Указание уровня IS, к которому относится данный интерфейс. Интерфейс по умолчанию работает на всех (и только на тех) уровнях, которые заданы общей настройкой `'is-level'`. Команда же `'circuit-level'` позволяет выбрать среди системных уровней тот, который требуется для конкретного интерфейса. Практическое применение команда имеет в том случае, когда задан `'is-level level-1-2'` — в таком случае командой `'circuit-level'` можно выбрать для интерфейса либо level-1, либо level-2. Интерфейсные параметры соответствующего уровня настраиваются интерфейсной командой `'level'` (см. далее).
`level { level-1 | level-2 }`	Переход в режим настройки IS-IS параметров интерфейса соответствующего уровня. Доступные настройки в данном режиме одинаковы для обоих уровней IS, однако конфигурируются для каждого уровня отдельно.
`csnp-interval` *SECONDS*	(Опционально) Задание интервала между отправками пакетов CSNP.
`hello-multiplier` *MULT*	(Опционально) Задание количества потерянных IS-IS Hello, после которых сосед на данном интерфейсе будет считаться потерянным.
`hello-timer` *SECONDS*	(Опционально) Задание интервала отправки IS-IS Hello.
`lsp-interval` *MSEC*	(Опционально) Задание интервала между отправками пакетов LSP.
`metric` *METRIC*	(Опционально) Указание протокольной метрики (стоимости) интерфейса.

Команда	Назначение
`priority` *PRIO*	(Опционально) Указание приоритета устройства при выборах DR на данном интерфейсе.
`exit`	Возврат в режим настройки интерфейса IS-IS.
`passive`	(Опционально) Перевод интерфейса в пассивный режим. В данном режиме интерфейс не отправляет и не принимает IIH-сообщений и через интерфейс не устанавливается никаких соседств. Режим используется при необходимости анонсировать в IS-IS подсеть данного интерфейса (например, для интерфейсов локальной петли `loopback`).
`point-to-point`	(Опционально) Включение на интерфейсе режима "IS-IS Point-to-point". В данном режиме не производятся выборы DR и не создаются псевдоноды. Следует следить за тем, чтобы режим интерфейса был задан одинаково для обоих концов IS-IS соединения.
`shutdown`	(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.
`exit`	Возврат в режим настройки процесса IS-IS. Далее можно включить в IS-IS и настроить параметры других требуемых интерфейсов.
`root`	Выход в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

Пример. Базовая настройка протокола IS-IS

```
router isis test
  interface loopback 1
    address-family ipv4 unicast
    exit
    passive
  exit
  interface tengigabitethernet 0/0/5
    address-family ipv4 unicast
      bfd fast-detect
    exit
    hello-padding disable
    point-to-point
  exit
  interface tengigabitethernet 0/0/7
    address-family ipv4 unicast
      bfd fast-detect
    exit
```

```
    hello-padding disable
    point-to-point
  exit
  host-name Router
  ipv4-te-level level-2
  level level-2
    metric-style wide
  exit
  net 49.0001.0010.0100.1001.00
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
`configure`	Переход в режим глобальной конфигурации.
`router isis` *ISIS_NAME*	Создание процесса маршрутизации IS-IS с именем *ISIS_NAME* и переход в режим его настройки.
`vrf` *VRF_NAME*	Запуск процесса маршрутизации IS-IS в указанном VRF и переход в режим настройки этого процесса.
`net` *NET*	Задание системного IS-IS Network Entity Title (NET) в формате XX.XXXX.XXXX.XXXX.XXXX.00. Данный параметр уникально идентифицирует систему во всем IS-IS-домене.
`is-level { level-1 | level-1-2 | level-2 }`	(Опционально) Выбор уровня IS, в котором будет работать система. По умолчанию используется значение 'level-1-2'.
`host-name` *HOSTNAME*	(Опционально) Задание IS-IS hostname — имени узла, которое будет указываться в соответствующих TLV служебных пакетов IS-IS. По умолчанию используется системное имя устройства (`'hostname'`).
`level { level-1 | level-2 }`	Переход в режим настройки параметров уровня 1 или уровня 2 (для обоих уровней параметры настраиваются одинаково).
`metric-style { wide | narrow | both }`	(Опционально) Выбор режима метрики для текущего уровня IS-IS. По умолчанию используется режим "both".

Команда	Назначение
`set-overload-bit on-startup` *SECONDS*	(Опционально) При указании данного параметра при старте процесса IS-IS в системе будет устанавливаться флаг "IS-IS overload bit" на *SECONDS* секунд после запуска.
`exit`	Возврат в режим настройки процесса IS-IS.
`interface { loopback | tengigabitethernet | bundle-ether | fortygigabitethernet | hundredgigabitethernet | tunnel-ip | twentyfivegigabitethernet }` *num*	Добавление соответствующего интерфейса (либо сабинтерфейса) в процесс IS-IS и переход в режим настройки параметров протокола IS-IS для этого интерфейса.
`address-family { ipv4 | ipv6 } unicast`	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 `ipv4 unicast`, `ipv6 unicast` или обе AFI/SAFI.
`exit`	Возврат в режим настройки интерфейса IS-IS.
`circuit-level { level-1 | level-1-2 | level-2 }`	(Опционально) Указание уровня IS, к которому относится данный интерфейс. Интерфейс по умолчанию работает на всех (и только на тех) уровнях, которые заданы общей настройкой `'is-level'`. Команда же `'circuit-level'` позволяет выбрать среди системных уровней тот, который требуется для конкретного интерфейса. Практическое применение команда имеет в том случае, когда задан `'is-level level-1-2'` — в таком случае командой `'circuit-level'` можно выбрать для интерфейса либо level-1, либо level-2. Интерфейсные параметры соответствующего уровня настраиваются интерфейсной командой `'level'` (см. далее).
`level { level-1 | level-2 }`	Переход в режим настройки IS-IS параметров интерфейса соответствующего уровня. Доступные настройки в данном режиме одинаковы для обоих уровней IS, однако конфигурируются для каждого уровня отдельно.
`csnp-interval` *SECONDS*	(Опционально) Задание интервала между отправками пакетов CSNP.
`hello-multiplier` *MULT*	(Опционально) Задание количества потерянных IS-IS Hello, после которых сосед на данном интерфейсе будет считаться потерянным.

Команда	Назначение
`hello-timer` *SECONDS*	(Опционально) Задание интервала отправки IS-IS Hello.
`lsp-interval` *MSEC*	(Опционально) Задание интервала между отправками пакетов LSP.
`metric` *METRIC*	(Опционально) Указание протокольной метрики (стоимости) интерфейса.
`priority` *PRIO*	(Опционально) Указание приоритета устройства при выборах DR на данном интерфейсе.
`exit`	Возврат в режим настройки интерфейса IS-IS.
`passive`	(Опционально) Перевод интерфейса в пассивный режим. В данном режиме интерфейс не отправляет и не принимает IIH-сообщений и через интерфейс не устанавливается никаких соседств. Режим используется при необходимости анонсировать в IS-IS подсеть данного интерфейса (например, для интерфейсов локальной петли `loopback`).
`point-to-point`	(Опционально) Включение на интерфейсе режима "IS-IS Point-to-point". В данном режиме не производятся выборы DR и не создаются псевдоноды. Следует следить за тем, чтобы режим интерфейса был задан одинаково для обоих концов IS-IS соединения.
`shutdown`	(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.
`exit`	Возврат в режим настройки процесса IS-IS внутри VRF. Далее можно включить в IS-IS и настроить параметры других требуемых интерфейсов.
`root`	Выход в режим глобальной конфигурации.
`commit`	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
    interface tengigabitethernet 0/0/17.10004000789
      address-family ipv4 unicast
        bfd fast-detect
      exit
      hello-padding disable
      point-to-point
    exit
    host-name AR1
    is-level level-1
    level level-1
      metric-style wide
    exit
    net 49.0001.0010.0100.1001.00
  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 49. Настройка протокола BFD для IS-IS-соседств

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`router isis` *ISIS_NAME*	Создание процесса маршрутизации IS-IS с именем *ISIS_NAME* и переход в режим его настройки.

Команда	Назначение
`interface { tengigabitethernet | bundle-ether | fortygigabitethernet | hundredgigabitethernet | twentyfivegigabitethernet }` *num*	Переход в режим настройки параметров протокола IS-IS требуемого интерфейса.
`address-family { ipv4 | ipv6 } unicast`	Включение работы IS-IS с IPv4 или IPv6 на данном интерфейсе и переход в режим конфигурирования соответствующей AFI/SAFI.
`bfd fast-detect { ipv4 | ipv6 }`	Включение механизма установления BFD-сессий для всех протокольных соседей IS-IS на данном интерфейсе.
`root`	Возврат в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

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

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

Редистрибуция маршрутной информации

Механизм редистрибуции позволяет передать в IS-IS маршруты из других протоколов (IGP/EGP, 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. **rip** — маршрутная таблица протокола RIP;
6. **static** — статические маршруты.

Таблица 50. Настройка редистрибуции в IS-IS маршрутной информации из других протоколов.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`router isis` *ISIS_NAME*	Переход в режим настройки процесса маршрутизации IS-IS с именем *ISIS_NAME*.
`address-family ipv4 unicast`	Переход в режим настройки параметров адресного семейства IPv4 unicast.
`redistribution { bgp | connected | ospf | local | rip | static }` *RULE_NAME*	Создание правила редистрибуции с именем *RULE_NAME* из указанного источника (bgp/connected/ospf/local/rip/static) и переход в режим настройки этого правила.
`match prefix` *IPv4PREFIX/MASK*	Указание фильтра, используемого для данного правила. При указании такого фильтра правило будет действовать только на маршруты, строго совпадающие с заданным *IPv4PREFIX/MASK*.
`metric-type { isis-level1-external | isis-level1-internal | isis-level2-external | isis-level2-internal }`	Назначить на маршруты, прошедшие через данное правило, метрику соответствующего типа.
`metric-value` *METRIC*	Установить значение метрики для маршрутов, прошедших через данное правило.
`priority` *RULE_PRIORITY*	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.
`redistribute disable`	Запретить редистрибуцию маршрутов, попавших в текущее правило. При выполнении данной команды текущее правило становится запрещающим.
`exit`	Выход из режима настройки правила редистрибуции. Далее можно настроить следующие правила — для того же самого источника, либо для других источников редистрибуции.
`root`	Выход в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

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

```
router isis eltex-test
  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
      metric-type isis-level1-internal
      metric-value 300
      priority 20
    exit
  exit
  interface loopback 1
    address-family ipv4 unicast
    exit
    passive
  exit
  interface tengigabitethernet 0/0/5
    address-family ipv4 unicast
      bfd fast-detect
    exit
    hello-padding disable
    point-to-point
  exit
  interface tengigabitethernet 0/0/7
    address-family ipv4 unicast
      bfd fast-detect
    exit
    hello-padding disable
    point-to-point
  exit
  host-name Router
  ipv4-te-level level-2
  level level-2
    metric-style wide
  exit
  net 49.0001.0010.0100.1001.00
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 из перечисленных видов необходимо указать требуемый тип командой 'authentication-type', задать ключ командой 'authentication-key' и идентификатор ключа командой 'authentication-id '.

Также для настройки аутентификации можно воспользоваться командой 'authentication-key-chain'. При использовании этой команды узлы конфигурации, заданные командами 'authentication-key', 'authentication-id ', 'authentication-type', игнорируются.

Таблица 51. Настройка глобальной аутентификации уровня IS-IS.

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

Таблица 52. С использованием key-chain.

`configure`	**Переход в режим глобальной конфигурации.**
`router isis` *ISIS_NAME*	Переход в режим настройки процесса маршрутизации IS-IS с именем *ISIS_NAME*.
`level { level-1 | level-2 }`	Переход в режим настройки параметров уровня 1 или уровня 2 (для обоих уровней параметры настраиваются одинаково).
`authentication-key-chain` *KEY_CHAIN_NAME*	Указание имени списка ключей (key-chain), который будет использоваться для аутентификации.
`root`	Выход в режим глобальной конфигурации.

`configure`	**Переход в режим глобальной конфигурации.**
`commit`	Применение произведенных настроек.

Таблица 53. Настройка аутентификации соседства IS-IS.

Команда	Назначение
`router isis` *ISIS_NAME*	Переход в режим настройки процесса маршрутизации IS-IS с именем *ISIS_NAME*.
`interface { loopback | tengigabitethernet | bundle-ether | fortygigabitethernet | hundredgigabitethernet | tunnel-ip | twentyfivegigabitethernet }` *num*	Переход в режим настройки параметров протокола IS-IS требуемого интерфейса.
`authentication-type { hmacsha1 | hmacsha256 | hmacsha384 | hmacsha512 | md5 | none | simple-password }`	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.
`authentication-key {` *KEY_STRING* | `encrypted` *KEY_ENCRYPT* `}`	Задание ключа для аутентификации в открытом (*KEY_STRING*) либо в зашифрованном (*KEY_ENCRYPT*) виде.
`authentication-id` *num*	Задание идентификатора ключа.
`root`	Выход в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

Таблица 54. С использованием key-chain.

Команда	Назначение
`router isis` *ISIS_NAME*	Переход в режим настройки процесса маршрутизации IS-IS с именем *ISIS_NAME*.
`interface { tengigabitethernet | bundle-ether }` *num*	Переход в режим настройки параметров протокола IS-IS требуемого интерфейса.
`authentication-key-chain` *KEY_CHAIN_NAME*	Указание имени списка ключей (key-chain), который будет использоваться для аутентификации.
`root`	Выход в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

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

```
router isis test
  level level-2
    metric-style wide
```

```
    authentication-type hmacsha1
    authentication-key 3
  exit
  interface tengigabitethernet 0/0/7
    authentication-key-chain test
  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/ME5100S:C_ME5100S_410_2-19# show isis
Tue Feb 10 09:03:03 2026
  IS-IS Router 1
    System Id: 1720.1612.7005
    IS Levels: level-2
```

```
    Net: 49.0001.1720.1612.7005.00
    Hostname: C_ME5100S_410_2-19
    LSP full-suppress: external
    LSP refresh-interval: 900 secs
    LSP max-lifetime: 1200 secs
    Area-address: 49.0001
    Tx packets PCP fields: 7
    Graceful-restart: Enable
      Adjacency wait: 10 secs
      Helper mode: Enable
    Topologies supported by IS-IS:
      IPv4 Unicast, IPv6 Unicast
        level-2
          Metric style (generate/accept): wide, lsp-max-size: 1492
      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
        none local redistributed
      Redistributed ipv6 unicast:
        none bgp redistributed
        none ospf redistributed
        none static redistributed
        none connected redistributed
        none local redistributed
      Interfaces supported by IS-IS
        Loopback0 is up (passive in configuration)
        Tengigabitethernet0/0/1.30 is up (active in configuration)
        Tengigabitethernet0/0/1.31 is up (active in configuration)
        Tengigabitethernet0/0/1.3986 is up (active in configuration)
        Tengigabitethernet0/0/1.3987 is up (active in configuration)
        Tengigabitethernet0/0/1.50 is up (active in configuration)
        Tengigabitethernet0/0/1.51 is up (active in configuration)
      Traffic Engineering:
        Level-1: ipv4 disabled, ipv6 disabled
        Level-2: ipv4 enabled, ipv6 disabled
        Router: ipv4 172.16.127.5, ipv6
0/ME5100S:C_ME5100S_410_2-19#
```

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  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 AR31-17-151 adjacency:
  System Id        Interface             State     Type          SNPA            Hold
(sec)  NSF    BFD   Hostname
  ---------------- --------------------- --------- ------------- ---------------
----------- ------ ----- ---------
  0050.0500.0032   te0/0/1.12            up        level-1       0013.8083.3671  27
true   none  AR32-17.32
```

show isis interfaces

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

Пример. show isis interfaces.

```
0/ME5100:Router# show isis int te0/0/1.6 detailed
Fri May 30 11:44:03 2025
  IS-IS Router AR31-17-151 interface:

  Tengigabitethernet0/0/1.6, circuit id: 54
    Last up: 17h31m26s ago
    BFD Fast detect: IPv4 disabled, IPv6 disabled
    Operation state: up
    Disabled creating neighborhood on this interface: false
    Hello padding: enabled
    Circuit 3 way: enabled
    LDP-IGP synchronization: disabled
    T1 timer status: stopped
    Media Type: p2p
```

```
  Used PDU: 1500
  Administrative tag: 0
  IPv4 Address Family: enabled
  IPv6 Address Family: disabled
  Circuit level: level-2
                                 Level-1           Level-2
  ID                             0050.0500.0031    0050.0500.0032
  Hostname                       none              AR32-17.32
  Priority                       64                64
  Metric                         10                10
  Key-chain                      none              none
  Authentication                 none              none
  Hello Multiplier               3                 3
  Hello Timer, sec               9                 9
  Minimum arrival interval, msec 0                 0
  CSNP retransmit interval, sec  10                10
  LSP retransmit interval, sec   10                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: Tengigabitethernet0/0/3.4094
                           Level-1                Level-2
                      Received    Sent        Received    Sent
     Hello IS-IS PDUs  1479        4422        1471        4416
     Hello ES-IS PDUs  0           0           0           0
     Hello ES PDUs     0           0           0           0
     LSP               47          96          50          100
     CSNP              1           1161        1           1161
     PSNP              2           0           2           1
     Unknown packet    0           0           0           0
     Discarded IIH     0           0           0           0
     Discarded LSP     0           0           0           0
     Discarded CSNP    0           0           0           0
     Discarded PSNP    0           0           0           0
```

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, labeled, multicast, mvpn, flowspec);
- IPv6 (unicast, labeled, multicast, mvpn, flowspec);
- VPNv4 (unicast, flowspec);
- VPNv6 (unicast, flowspec);
- L2VPN (VPLS, EVPN).

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 поддерживаются семейства `'ipv4 (unicast, labeled, mvpn)'` и `'ipv6 (unicast, labeled, mvpn)'`. Остальные семейства 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 55. Базовая настройка BGP-процесса

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.

Команда	Назначение
`router bgp` *ASN*	Создание процесса маршрутизации BGP с автономной системой с номером *ASN* и переход в режим его настройки.
`bgp router-id` *A.B.C.D*	Назначение локального идентификатора маршрутизатора. Рекомендуется использовать для этой цели IPv4-адрес одного из loopback-интерфейсов устройства.
`address-family ipv4 unicast`	(Опционально) Переход в режим настройки адресного семейства IPv4 Unicast.
`aggregate-address` *IPv4_PREFIX* `[ summary-only ]`	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).
`exit`	Возврат в режим настройки параметров BGP для IPv4 Unicast.
`dampening`	Включение механизма подавления мерцания маршрутов.
`redistribution { bgp-labeled | connected | isis | local | ospf | rip | static }` *RULE_NAME*	Создание правила редистрибуции и переход в режим его настройки. Подробнее см. раздел "Редистрибуция маршрутной информации".
`exit`	Возврат в режим настройки параметров BGP для IPv4 Unicast.
`exit`	Возврат в режим настройки параметров BGP. Далее можно настроить параметры других AFI/SAFI.
`neighbor` *A.B.C.D* `|` *A:B:C:D::X*	Создание протокольного соседа (с IPv4- или IPv6-адресом) и переход в режим настройки его параметров.
`description` *"STRING"*	Задание текстовой строки — описания протокольного соседа.
`ebgp-multihop ttl` *MULTIHOP-TTL*	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 *MULTIHOP-TTL*.
`max-prefixes` *PREFIXES*	Устанавливает ограничение на количество получаемых от соседа префиксов.
`remote-as` *ASN*	Задает номер автономной системы BGP-соседа. Является обязательным параметром при создании соседа.

Команда	Назначение
`send-community`	Включает отправку параметра *community* в отсылаемых соседу анонсах. По умолчанию параметры *community* удаляются из отправляемых анонсов.
`send-community-ext`	Включает отправку параметра *extended community* в отсылаемых соседу анонсах. По умолчанию параметры *extended community* удаляются из отправляемых анонсов. Для корректной работы AFI L2VPN, VPNv4/VPNv6 отправку *extended community* необходимо включать.
`address-family { ipv4 { unicast | flowspec | labeled | multicast | mvpn } | ipv6 { unicast | flowspec | labeled } | l2vpn { vpls | evpn } | vpnv4 { unicast | flowspec } | vpnv6 { unicast | flowspec } }`	Включение на данном соседе указанного адресного семейства (**обязательно для работы соответствующей AFI/SAFI**) и переход в режим настроек данного семейства.
`next-hop-self`	При указании данной команды для всех отправляемых маршрутов в качестве параметра *next-hop* будет устанавливаться адрес данного маршрутизатора.
`prefix-list { in | out }` *PREFLIST_NAME*	Установка фильтра префиксов для принимаемых (*in*) или отправляемых (*out*) анонсов. Соответствующий фильтр префиксов должен быть создан в конфигурации маршрутизатора.
`route-map { in | out }` *ROUTEMAP_NAME*	Установка "карты маршрутов" для фильтрации, соответственно, принимаемых (*in*) или отправляемых (*out*) анонсов. Карта маршрутов с именем, соответствующим *ROUTEMAP_NAME*, должна быть создана в конфигурации маршрутизатора.
`route-reflector-client`	Установка текущего протокольного соседа в режим RR-клиента. Такому iBGP-соседу будут анонсироваться пути, полученные по iBGP от других маршрутизаторов сети.
`soft-reconfiguration`	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 route-refresh capability.
`exit`	Возврат в режим настройки параметров протокольного соседа BGP. Далее можно сконфигурировать другие адресные семейства для указанного соседа.
`exit`	Возврат в режим настройки параметров BGP. Далее можно создать и настроить других протокольных соседей.
`root`	Выход в режим глобальной конфигурации.

Команда	Назначение
`commit`	Применение произведенных настроек.

Пример. Базовая настройка протокола BGP.

```
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 56. Настройка списка префиксов.

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

Команда	Назначение

`le` *1..128*	Указание дополнительного условия на длину префикса (*less or equal*, "префикс короче либо равен заданного значения").
	
	В данном случае элемент фильтра становится нестрогим — в сочетании с заданным `prefix` он будет включать в себя все более специфичные префиксы, входящие в него и имеющие маску не длиннее заданной параметром `le`.
	
	Например, комбинация:
	
	`seq-num 10`
	`  prefix 100.64.0.0/16`
	`  le 24`
	`exit`
	
	даст фильтр, в который попадут все префиксы, попадающие в 100.64.0.0/16 и имеющие маску от /16 до /24.

`ge` *1..128*	Указание дополнительного условия на длину префикса (*greater or equal*, "префикс длиннее либо равен заданного значения").
	
	В данном случае элемент фильтра становится нестрогим — в сочетании с заданным `prefix` он будет включать в себя все более специфичные префиксы, входящие в него и имеющие маску не короче заданной параметром `ge`.
	
	Комбинация:
	
	`seq-num 10`
	`  prefix 100.64.0.0/16`
	`  ge 20`
	`exit`
	
	даст фильтр, в который попадут все префиксы, попадающие в 100.64.0.0/16 и имеющие маску от /20 до /32.

`exit`	Выход из режима настройки элемента списка фильтра префиксов. Далее можно создать следующие требуемые элементы списка.
`root`	Возврат в режим глобальной конфигурации

Команда	Назначение
`router bgp` *ASN*	Переход в режим настройки процесса BGP.
`neighbor` *A.B.C.D* | *A:B:C:D::X*	Переход в режим настройки параметров BGP-соседа.
`address-family { ipv4 unicast | ipv6 unicast | vpnv4 unicast | vpnv6 unicast }`	Переход в режим настроек тех AFI/SAFI, для которых требуется применить фильтр префиксов.
`prefix-list { in | out }` *PREFLIST_NAME*	Установка фильтра префиксов для принимаемых (*in*) или отправляемых (*out*) анонсов.
`root`	Выход в режим глобальной конфигурации.
`commit`	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/отправляемых 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 57. Создание route-map.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`route-map` *ROUTEMAP_NAME*	Создание карты маршрутов с именем *ROUTEMAP_NAME* и переход в режим ее настройки.
`seq-num` *SEQ-NUM*	Создание элемента карты маршрутов с соответствующим номером и переход в режим его настройки. Номер элемента может принимать значения 1-4294967295.

Команда	Назначение
`set { comm-list .. | community .. | ext-comm-list .. | extcommunity .. | local-preference .. | med .. | nexthop .. | prepend .. | remove .. | weight .. }`	Назначение правила модификации анонса. Перечень параметров зависит от типа правила модификации, см. в следующих разделах. Для каждого элемента карты можно назначить несколько разнотипных правил модификации, несколько однотипных правил назначить невозможно (например, для одного элемента можно задать правила `set community` и `set remove`, но нельзя назначить несколько правил `set community`).
`match { as-path .. | comm-list .. | ext-comm-list .. | prefix-list .. }`	Назначение условия соответствия анонса. Перечень параметров зависит от типа условия соответствия, см. в следующих разделах. Для каждого элемента карты можно назначить несколько разнотипных условий соответствия, несколько однотипных условий назначить невозможно (например, для одного элемента можно задать условия `match prefix-list` и `match as-path`, но нельзя задать несколько условий `match prefix-list`). При необходимости фильтрации анонсов с различными однотипными условиями `match` требуется создавать отдельные элементы карты маршрутов, по одному на каждое условие.
`action { permit | deny }`	Действие, которое будет производиться с анонсом, если он попал под условия данного элемента списка.
`exit`	Выход из режима настройки элемента карты маршрутов. Далее можно создать следующие требуемые элементы списка.
`root`	Возврат в режим глобальной конфигурации
`commit`	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 58. Виды правил модификации анонсов `'set'`.

Команда	Назначение
`comm-list { add | delete }` *COMMLIST_NAME*	Добавить или удалить из анонса набор community, заданный соответствующим правилом `community-list` *COMMLIST_NAME*.
`community remove-all`	Удалить все community из анонса.
`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 }`	Удалить все community из анонса и добавить одну новую.
`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 }`	Добавить к анонсу одну новую community.
`ext-comm-list { add | delete }` *EXTCOMMLIST_NAME*	Добавить или удалить из анонса набор extended community, заданный соответствующим правилом `extcommunity-list` *EXTCOMMLIST_NAME*.
`extcommunity remove-all`	Удалить все extended community из анонса.
`extcommunity remove-all-and-set { rt | soo } value {` *AS:Nr(0-65535:0-4294967295, 0-4294967295:0-65535) | IPv4:Nr(0-65535)* `}`	Удалить все extcommunity из анонса и установить указанную RT- или SOO-extcommunity.
`extcommunity set-specific { rt | soo } value {` *AS:Nr(0-65535:0-4294967295, 0-4294967295:0-65535) | IPv4:Nr(0-65535)* `}`	Добавить указанную RT- или SOO-extcommunity.
`local-preference` *LOCALPREF*	Установить соответствующее значение параметра BGP Local Preference.

Команда	Назначение
`med value` *MED*	Установить соответствующее значение параметра BGP MED.
`nexthop` *IPv4_ADDR* | *IPv6_ADDR*	Установить соответствующее значение BGP Nexthop
`prepend as-path` *ASN* `prepend times` *N*	Установить препенды на параметр AS-PATH, состоящие из номера автономной системы *ASN*, повторенные *N* раз.
`remove as-path` *ASN*	Удалить из AS-PATH данного анонса указанные номера автономных систем *ASN*.
`remove private-as`	Удалить из AS-PATH данного анонса все приватные номера автономных систем (RFC6996).
`weight value` *WEIGHT*	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 59. Виды условий соответствия анонсов `'set'`.

Команда	Назначение
`as-path` *AS_REGEXP*	Проверка AS-PATH анонса на соответствие приведенному регулярному выражению *AS_REGEXP*. Допустимая длина регулярного выражения — до 300 символов.
`comm-list name` *COMMLIST_NAME*	Проверка перечня community в анонсе на соответствие заданному community-фильтру (фильтр должен быть создан командой "`community-list` *COMMLIST_NAME*")
`ext-comm-list name` *EXTCOMMLIST_NAME*	Проверка перечня расширенных community в анонсе на соответствие заданному extcommunity-фильтру (фильтр должен быть создан командой "`extcommunity-list` *EXTCOMMLIST_NAME*")
`prefix-list destination` *PREFLIST_NAME*	Проверка префикса анонса на соответствие указанному фильтру префиксов. Фильтр префиксов должен быть сконфигурирован отдельно командой "`prefix-list` *PREFLIST_NAME*".
`prefix-list nexthop` *PREFLIST_NAME*	Проверка параметра BGP nexthop анонса на соответствие указанному фильтру префиксов. Фильтр префиксов должен быть сконфигурирован отдельно командой "`prefix-list` *PREFLIST_NAME*".

Команда	Назначение
`prefix-list source` *PREFLIST_NAME*	Проверка адреса BGP-спикера, от которого получен анонс, на соответствие указанному фильтру префиксов. Фильтр префиксов должен быть сконфигурирован отдельно командой "`prefix-list` *PREFLIST_NAME*".

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 60. Значения административной дистанции.

Протокол/источник	**Административная дистанция**	**Приоритет**
Присоединенные (connected) маршруты	0	1
Статические (static) маршруты	1	2
Tunnel endpoint	2	3
BGP-LU external	19	4
External BGP	20	5
OSPF inter/intra-area	30	6
OSPF external	110	7
IS-IS level1 internal	115	8
IS-IS level2 internal	116	9
IS-IS level1 external	117	10
IS-IS level2 external	118	11
RIP	120	12
BGP-LU internal	199	13
Internal BGP	200	14
BGP aggregate	200	15

Значения административной дистанции можно изменить.

Таблица 61. Настройка административной дистанции для протокола BGP.

Команда	**Назначение**
`configure`	Переход в режим глобальной конфигурации.
`router admin-distance`	Переход в режим настройки раздела административной дистанции протоколов.
`bgp external` *0..255*	Задание значения административной дистанции для маршрутов eBGP.
`bgp internal` *0..255*	Задание значения административной дистанции для маршрутов iBGP.
`root`	Возврат в режим глобальной конфигурации
`commit`	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).

Подготовка конфигурации IGP на примере протокола IS-IS:

```
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 test
  interface loopback 1
    address-family ipv4 unicast
    exit
    passive
  exit
  interface tengigabitethernet 0/0/5
    address-family ipv4 unicast
      bfd fast-detect
    exit
    hello-padding disable
    ldp-igp-synchronization
    point-to-point
  exit
  interface tengigabitethernet 0/0/7
    address-family ipv4 unicast
      bfd fast-detect
    exit
    hello-padding adaptive
    point-to-point
  exit
  host-name Router
  ipv4-te-level level-2
  level level-2
    metric-style wide
  exit
  net 49.0001.0010.0100.1001.00
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 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 62. Базовая настройка LDP.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`mpls`	Переход в режим настройки параметров и протоколов MPLS.
`router-id` *IPv4_ADDR*	Задание Router ID для процесса LDP.
`penultimate-hop-popping disable`	(опционально) Отключение механизма MPLS PHP (снятия транспортной метки на предпоследнем маршруте). **IMPORTANT** Для применения данной настройки потребуется вручную переустановить LDP-сессии с соседями.
`transport-address` *IPv4_ADDR*	(опционально) Задание транспортного адреса для протокола LDP. Рекомендуется явно задавать данный адрес.
`ldp`	Переход в режим настройки протокола LDP.

Команда	Назначение
`discovery interface { tengigabitethernet | bundle-ether | fortygigabitethernet | hundredgigabitethernet }` *num*	Добавление соответствующего интерфейса (либо сабинтерфейса) в процесс автообнаружения LDP и переход в режим настройки параметров LDP для данного интерфейса.
`bfd fast-detect`	(опционально) Включение протокола BFD для обнаруженных соседей на данном интерфейсе.
`shutdown`	(опционально) Деактивация LDP discovery на интерфейсе.
`exit`	Возврат в режим настройки протокола LDP.
`neighbor` *IPv4_ADDR*	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.
`hello-holdtime` *SECONDS* `holdtime-interval` *SECONDS*	(Опционально) Настройка соответствующих таймеров на targeted-сессии.
`bfd fast-detect`	(Опционально) Включение на данной targeted-сессии протокола BFD.
`shutdown`	(Опционально) Административное отключение данной targeted-сессии.
`root`	Возврат в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

Таблица 63. Включение коммутации MPLS на интерфейсах.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`mpls`	Переход в режим настройки параметров и протоколов MPLS.
`forwarding`	Переход в режим настройки параметров MPLS-коммутации на устройстве.
`interface { loopback | tengigabitethernet | bundle-ether }` *num*	Включение MPLS-коммутации на данном интерфейсе либо сабинтерфейсе. Обязательно включение в данный список также тех loopback-интерфейсов, которые планируется анонсировать соседям по LDP.
`commit`	Применение произведенных настроек.

Пример. Настройка MPLS LDP на двух интерфейсах.

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

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-соседств 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 64. Редистрибуция в LDP.

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

Команда	Назначение
`redistribute disable`	Запретить редистрибуцию маршрутов, попавших в текущее правило. При выполнении данной команды текущее правило становится запрещающим.
`exit`	Выход из режима настройки правила редистрибуции. Далее можно настроить следующие правила — для того же самого источника, либо для других источников редистрибуции.
`root`	Возврат в режим глобальной конфигурации.
`commit`	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
    address-family ipv4 unicast redistribution connected LDP-CONN20
      priority 20
    exit
  exit
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

  Prefix                Peer ID                   Label       State
Type        Interface
  --------------------- ------------------------- -----------
---------------------------- ---------- ----------
  10.0.0.26/32          10.0.0.134:0              312         mapping-liberally-
retained   prefix
  10.0.0.30/32          10.0.0.134:0              58          mapping-established
```

```
prefix      bu1.4033
  10.0.0.111/32         10.0.0.111:0              69          mapping-established
prefix      bu1.4010
  10.0.0.111/32         10.0.0.134:0              308         mapping-liberally-
retained   prefix
  10.0.0.134/32         10.0.0.111:0              229         mapping-liberally-
retained   prefix
  10.0.0.134/32         10.0.0.134:0              59          mapping-established
prefix      bu1.4033
  46.0.0.0/24           10.0.0.111:0              70          mapping-established
prefix      bu1.4010
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

  LDP-OSPF sync

  Interface               LDP state  Metric    Hold-time duration  Hold-time left
  ----------------------- ---------- --------- ------------------- ---------------
  te0/0/5                 up         normal    0                   0

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 detail

  LDPv1 peer: 1.0.0.1:0
    Current state: operational, role: active
    TCP connection: 1.0.0.1, MD5 off
    Label distribution method: downstream-unsolicited
    Session uptime: 03h46m06s
    Keepalive interval: 7 secs
    Session holdtime: 40 secs (own 40 secs, peer 40 secs)
    Next keepalive in: 4 secs, session expires in: 37 secs
    Established adjacencies:
      link, bu1, holdtime: 14 secs, bfd: none (not-required)
      targeted, with 1.0.0.1, holdtime: 34 secs, bfd: none (not-required)
    Negotiated maximum PDUs length: 4096 octets
    Graceful Restart support: peer is false, local is false
    Peer reconnect time: 0 secs, recovery time: 0 secs
    Addresses bound to session:
      1.0.0.1
      192.168.55.2
      192.168.55.5
      192.168.55.17
    Labels received from neighbor:
      3, type: prefix, installed: yes, bu1
      27, type: prefix, installed: no
    Stats:
      0 unknown message count, 0 unknown tlv count

  LDPv1 peer: 1.0.0.2:0
    Current state: operational, role: active
    TCP connection: 1.0.0.2, MD5 off
    Label distribution method: downstream-unsolicited
    Session uptime: 03h46m47s
    Keepalive interval: 7 secs
    Session holdtime: 40 secs (own 40 secs, peer 40 secs)
    Next keepalive in: 4 secs, session expires in: 37 secs
    Established adjacencies:
      link, bu2, holdtime: 10 secs, bfd: none (not-required)
    Negotiated maximum PDUs length: 4096 octets
    Graceful Restart support: peer is false, local is false
    Peer reconnect time: 0 secs, recovery time: 0 secs
    Addresses bound to session:
      1.0.0.2
      192.168.55.6
      192.168.55.13
      192.168.55.22
```

```
    Labels received from neighbor:
      35, type: prefix, installed: no
      3, type: prefix, installed: yes, bu2
    Stats:
      0 unknown message count, 0 unknown tlv count
```

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 65. Создание и настройка экземпляра VRF.

Команда	**Назначение**
`configure`	Переход в режим глобальной конфигурации.
`vrf` *VRF_NAME*	Создание в конфигурации устройства экземпляра VRF с именем *VRF_NAME* и переход в режим настройки этого экземпляра.

Команда	Назначение
`rd` *RD*	Задание Route Distinguisher для данного экземпляра VRF. Параметр является обязательным при создании VRF. Допустимые формы задания: • **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.
`maximum prefix` *MAX_ROUTES*	(опционально) Установка ограничения количества маршрутов внутри экземпляра VRF.
`import route-target` *RT_COMMUNITY_VALUE*	(опционально) Установка перечня значений route-target extended community, VPNv4 BGP-пути с которыми будут устанавливаться в таблицу маршрутизации экземпляра VRF (см. ниже раздел "Различие между параметрами RT и RD"). Формат задания *RT_COMMUNITY_VALUE* аналогичен формату параметра *RD*.
`export route-target` *RT_COMMUNITY_VALUE*	(опционально) Установка перечня значений route-target extended community, с которыми маршруты из данного экземпляра VRF будут анонсироваться в VPNv4 BGP (см. ниже раздел "Различие между параметрами RT и RD"). Формат задания *RT_COMMUNITY_VALUE* аналогичен формату параметра *RD*.
`description` *STRING*	(опционально) Задание строкового описания экземпляра VRF.
`root`	Возврат в режим глобальной конфигурации.
`commit`	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

  Route distinguisher: 1.1.1.1:100
  Description:         Example L3VPN service
  Import from route-target:
    65535:100
  Export to route-target:
    65535:100
  Interfaces:
    Tengigabitethernet0/0/17.1100
    Tengigabitethernet0/0/17.1200
  Total entries:    2

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,
      BL - BGP labeled, R - RIP


  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       VRF
Interface
  ---------------- ----------- ------------------ ----------- ----------------
----------
  100.100.1.1      00:00:00    a8:f9:4b:8b:bb:b1  Interface   example          te
0/0/17.1100
  100.100.2.1      00:00:00    a8:f9:4b:8b:bb:b1  Interface   example          te
0/0/17.1200

  Total entries: 2
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,
      BL - BGP labeled


  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-соседям 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 66. Настройка BGP-соседа для передачи маршрутов L3VPN.

Команда	**Назначение**
`configure`	Переход в режим глобальной конфигурации.
`router bgp` *ASN*	Переход в режим настройки процесса маршрутизации.
`neighbor` *A.B.C.D*	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.
`description` *"STRING"*	(опционально) Задание текстовой строки — описания протокольного соседа.
`remote-as` *ASN*	Задает номер автономной системы BGP-соседа. L3VPN-сессии поддерживаются только для iBGP-соседей.
`send-community`	Включает отправку параметра *community* в отсылаемых соседу анонсах. По умолчанию параметры *community* удаляются из отправляемых анонсов. Для корректной работы L3VPN отправку *extended community* рекомендуется включать.
`send-community-ext`	Включает отправку параметра *extended community* в отсылаемых соседу анонсах. По умолчанию параметры *extended community* удаляются из отправляемых анонсов. Для корректной работы L3VPN отправку *extended community* **необходимо включать**.
`address-family vpnv4 unicast`	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.

Команда	Назначение
`exit`	Возврат в режим настроек BGP-соседа.
`update-source` *IPv4_ADDR*	Задание IPv4-адреса, с которого будет производиться взаимодействие с соседом. Данный параметр рекомендуется всегда указывать для iBGP-сессий.
`root`	Выход в режим глобальной конфигурации.
`commit`	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                  AS          MsgRcvd       MsgSent       Up/Down
St/PfxRcd
  ------------------------- ----------- ------------- ------------- ----------
-------------
  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                   AS          MsgRcvd       MsgSent       Up/Down
St/PfxRcd
  -------------------------- ----------- ------------- ------------- ----------
-------------
  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 Distinguisher        IP Prefix             Next hop         Metric  Rcvd/Lcl
label  LocPrf  Weight  Path
  -------------------------- --------------------- ---------------- -------
-------------- ------- ------- -----
  u>i  2.2.2.2:100           100.100.3.0/24        2.2.2.2          0       34/-
100     0       ?

  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 Distinguisher   IP Prefix             Next hop         Metric  Rcvd/Lcl label
LocPrf  Weight  Path
  --------------------- --------------------- ---------------- ------- ---------------
------- ------- -----
  u>i  1.1.1.1:100      100.100.1.0/24        1.1.1.1          0       67/-
100     0       ?
  u>i  1.1.1.1:100      100.100.2.0/24        1.1.1.1          0       67/-
100     0       ?

  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,
      BL - BGP labeled, R - RIP


  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,
      BL - BGP labeled, R - RIP
```

```
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 внутрь 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 внутрь 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,
      BL - BGP labeled, R - RIP


  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,
      BL - BGP labeled, R - RIP


  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 в BGP-таблицу соответствующего VRF.

Запуск BGP-процесса для экземпляра VRF производится автоматически при создании конфигурационного блока `'vrf VRF_NAME'` в разделе настройки `'router bgp'` и создании в нем как минимум одного соседа.

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	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 VRF могут присутствовать маршруты с пометкой "BGP" в том случае, если их источником является AFI VPNv4/VPNv6 unicast.

Автоматическая редистрибуция

По умолчанию на маршрутизаторах семейства ME работает автоматическая редистрибуция всех имеющихся в VRF маршрутов (за исключением local-маршрутов) в AFI VPNv4/VPNv6 unicast и автоматическое анонсирование таких путей VPNv4- и VPNv6-соседям. Процесс автоматический редистрибуции неотключаем.

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

Для назначения дополнительных атрибутов BGP на маршруты, попадающие в пространство VPNv4, необходимо создавать блок правил `'redistribution'` в разделе `'router bgp <ASN> address-family vpnv4 unicast'` и настраивать там процесс редистрибуции соответствующих сетей с назначением нужных атрибутов и с опциональным указанием VRF-источника (правило `'match vrf <VRF_NAME>'`) либо списка VRF-источников (правило `'match vrf-list <LIST_NAME>'`).

В примере ниже описана настройка ограничения автоматической редистрибуции connected-маршрутов из VRF 'VRFTEST' в L3VPN. Здесь для VRF будет разрешена редистрибуция маршрутов в l3vpn при условии их соответствия префикс-листу TESTVRF-PRFLST (запись "ALLOW-TESTVRF-PREFIXES" с приоритетом 10); для остальных маршрутов редистрибуция в L3VPN запрещается записью "ANNOUNCE-NONE" с приоритетом 99.

Пример настройки ограничения автоматической редистрибуции connected-маршрутов

```
prefix-list TESTVRF-PRFLST
  seq-num 10
    prefix 10.2.2.0/24
  exit
  seq-num 20
    prefix 10.9.1.0/24
  exit
exit
router bgp 65535
  address-family vpnv4 unicast
    redistribution connected ALLOW-TESTVRF-PREFIXES
      match prefix-list destination TESTVRF-PRFLST
      match vrf TESTVRF
      priority 10
    exit
    redistribution connected ANNOUNCE-NONE
      match vrf TESTVRF
      priority 99
      redistribute disable
    exit
  exit
exit
```

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.

В примере ниже включается редистрибуция адреса интерфейса `lo7991`, относящегося к `vrf l3-1`, в адресное пространство vpnv4 unicast для дальнейшего анонсирования его в l3vpn. После данного ручного правила срабатывает разрешающее правило автоматической

редистрибуции всех остальных маршрутов.

Пример настройки редистрибуции адресов loopback-интерфейсов.

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

router bgp 65535
  address-family vpnv4 unicast
    redistribution local LOCAL
      match prefix 3.1.3.1/32
      match vrf l3-1
    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 брижд-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).

Маршрутизируемый интерфейс (routed interface) является опциональным элементом бридж-домена. Его роль выполняет ранее созданный BVi-интерфейс. Он позволяет выполнять обмен трафиком между системными процессами (ICMP, маршрутизируемые процессы, такие как PIM, IGMP — функциональность расширяется) и между локальными интерфейсами и/или псевдопроводами.

IMPORTANT	При использовании маршрутизируемого интерфейса в бридж-домене вместе с сабинтерфейсами, на последних требуется использовать команду `'rewrite'` для снятия (операция `'pop'`) всех меток при передаче трафика в бридж-домен и их обратном навешивании (операция `'push'`) при передаче трафика в AC.
IMPORTANT	Использование маршрутизируемого интерфейса вместе с сабинтерфейсами одного физического интерфейса требует наличие глобальной настройки `'system hw-extended-resources-mode'` и невозможно на линейных картах LC18XGE для ME5000 и на устройствах ME5100 / ME5100S / ME5100rev.X

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 67. Настройка профиля псевдопровода.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`l2vpn pw-class` *CLASS_NAME*	Создание в конфигурации устройства профиля псевдопровода и переход в режим задания его параметров.
`encapsulation mpls signaling-type { manual | pseudowire-id-fec-signaling }`	Задание метода сигнализации для псевдопроводов, использующих данный профиль. Для использования классической сигнализации LDP следует использовать параметр `'pseudowire-id-fec-signaling'`. При использовании метода `'manual'` сервисные метки задаются вручную в конфигурации каждого псевдопровода. Данный параметр является обязательным.
`encapsulation mpls mtu` *MTU_SIZE*	(опционально) Задание значения MTU, которое будет использоваться при сигнализации псевдопроводов. Данный параметр влияет только на процесс сигнализации и не ограничивает размер передаваемых пакетов.
`encapsulation mpls control-word { preferred | non-preferred }`	(опционально) Задает значение параметра control word (предпочитаемый "preferred" либо не предпочитаемый "non-preferred") для процесса сигнализации псевдопровода.
`root`	Возврат в режим глобальной конфигурации.
`commit`	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 68. Настройка targeted LDP-сессии (обязательно для псевдопроводов с LDP-сигнализацией).

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`mpls ldp neighbor` *IPv4_ADDR*	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.
`bfd fast-detect`	(опционально) Включение механизма BFD для соответствующей targeted LDP-сессии.
`root`	Возврат в режим глобальной конфигурации.
`commit`	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 69. Создание и настройка бридж-домена.

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

Команда	Назначение
`pw` *IPv4_PEER PW_ID*	Создание внутри бридж-домена псевдопровода до указанного устройства и переход в режим настройки этого псевдопровода. Параметр *PW_ID* (также применяется термин *VC ID*, *Virtual circuit ID*) 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.
`pw-class` *CLASS_NAME*	Привязка ранее созданного в конфигурации профиля к данному псевдопроводу. Привязка профиля к псевдопроводу является обязательной.
`mpls static label local` *LOCAL_LABEL_VALUE* `mpls static label remote` *REMOTE_LABEL_VALUE*	(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'`).
`backup`	(опционально) Переход в режим настройки запасного (backup) псевдопровода.
`pw` *IPv4_PEER PW_ID*	Создание запасного (backup) псевдопровода до указанного устройства и переход в режим настройки этого псевдопровода. Запасной псевдопровод будет использоваться в случае отказа основного.
`pw-class` *CLASS_NAME*	Привязка ранее созданного в конфигурации профиля к данному псевдопроводу.
`exit`	Возврат в режим конфигурации backup PW.
`exit`	Возврат в режим конфигурации основного PW.
`ignore encapsulation-mismatch` `ignore mtu-mismatch`	Установка режима игнорирования несоответствия параметров инкапсуляции (типа псевдопровода) либо значения MTU при сигнализации псевдопровода.
`exit`	Возврат в режим конфигурации бридж-домена.
`routed interface bvi PW_ID`	Добавление маршрутизируемого интерфейса.
`transport-mode { ethernet | vlan }`	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.

Команда	Назначение
`mtu` *MTU_SIZE*	Устанавливает размер MTU в байтах для всего бридж-домена. Настройка служит для целей сигнализации.
`root`	Возврат в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

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

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

В приведенном примере бридж-домен позволит осуществлять коммутацию трафика между AC *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-домене может производиться между всеми элементами, включенными в бридж-домен, то есть в направлениях AC-AC, AC-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 70. Создание и настройка экземпляра VFI внутри бридж-домена.

Команда	**Назначение**
`configure`	Переход в режим глобальной конфигурации.
`l2vpn bridge-group default bridge-domain` *BD_NAME*	Переход в режим настройки бридж-домена.
`vfi` *VFI_NAME*	Создание внутри бридж-домена экземпляра VFI и переход в режим его настройки.
`pw` *IPv4_PEER PW_ID*	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.
`root`	Возврат в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

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

```
l2vpn
  bridge-domain example-bd
    interface tengigabitethernet 0/0/15
    exit
    interface tengigabitethernet 0/0/1.400500
    exit
    interface tengigabitethernet 0/0/17.5
    exit
    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
  exit
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 71. Создание и настройка кросс-коннекта.

Команда	**Назначение**
`configure`	Переход в режим глобальной конфигурации.
`l2vpn xconnect-group` *XCONNECT_GROUP_NAME*	Создание в конфигурации устройства именованной группы кросс-коннектов и переход в режим конфигурации этой группы.
`p2p` *P2P_NAME*	Создание кросс-коннекта внутри соответствующей группы и переход в режим настройки этого кросс-коннекта.
`interface { tengigabitethernet | bundle-ether | fortygigabitethernet | hundredgigabitethernet}` *num | num.subif_id*	Включение указанного интерфейса либо сабинтерфейса в состав кросс-коннекта в качестве интерфейса локальной коммутации (AC).
`pw` *IPv4_PEER PW_ID*	Создание внутри кросс-коннекта псевдопровода до указанного устройства и переход в режим настройки этого псевдопровода. Параметр *PW_ID* (также применяется термин *VC ID*, *Virtual circuit ID*) 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.
`pw-class` *CLASS_NAME*	Привязка ранее созданного в конфигурации профиля к данному псевдопроводу. Привязка профиля к псевдопроводу является обязательной.

Команда	Назначение
`mpls static label local` *LOCAL_LABEL_VALUE* `mpls static label remote` *REMOTE_LABEL_VALUE*	(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'`).
`backup`	(опционально) Переход в режим настройки запасного (backup) псевдопровода.
`pw` *IPv4_PEER PW_ID*	Создание запасного (backup) псевдопровода до указанного устройства и переход в режим настройки этого псевдопровода. Запасной псевдопровод будет использоваться в случае отказа основного.
`pw-class` *CLASS_NAME*	Привязка ранее созданного в конфигурации профиля к данному псевдопроводу.
`exit`	Возврат в режим конфигурации backup PW.
`exit`	Возврат в режим конфигурации основного PW.
`ignore encapsulation-mismatch` `ignore mtu-mismatch`	Установка режима игнорирования несоответствия параметров инкапсуляции (типа псевдопровода) либо значения MTU при сигнализации псевдопровода.
`exit`	Возврат в режим конфигурации кросс-коннекта.
`transport-mode { ethernet | vlan }`	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.
`mtu` *MTU_SIZE*	Устанавливает размер MTU в байтах для данного кросс-коннекта. Настройка служит для целей сигнализации.
`root`	Возврат в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

Пример. Настройка кросс-коннекта.

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

```
      exit
      transport-mode vlan
    exit
  exit
exit
```

НАСТРОЙКА MPLS TRAFFIC ENGINEERING

В данной главе рассматриваются принципы организации и настройки функционала MPLS Traffic Engineering.

Для начала определим некоторые термины, которые будут использованы в описании процедур конфигурации:

- **LSP** — Label Switched Path. Однонаправленный путь, по которому коммутируются пакеты;
- **TE-туннель** — виртуальный однонаправленный интерфейс, который имеет один или несколько LSP;
- **IGP** — семейство протоколов динамической маршрутизации на базе принципов Link-state;
- **LSR** — Labeled Switching Router. Маршрутизатор, коммутирующий по меткам;
- **Ingress LSR** — он же Head-End Router. Маршрутизатор, с которого стартует LSP;
- **Egress LSR** — он же Tail-End Router. Маршрутизатор, на котором терминируется LSP;
- **RSVP** — протокол, используемый функционалом MPLS TE для распространения меток и сигнализации LSP;
- **CSPF** — расширенный алгоритм выбора лучшего пути. Умеет, как и OSPF, строить кратчайшие пути на основе топологической базы данных, но при этом учитывать ограничения, накладываемые требованиями к TE-туннелям.

Необходимые шаги для настройки MPLS TE

На маршрутизаторах Eltex серии ME для обеспечения работы функционала MPLS Traffic Engineering требуется выполнить следующие действия:

1. Настроить инфраструктуру распространения транспортных меток и служебных RSVP сообщений, то есть обеспечить IP-связность с другими устройствами сети;
2. Активировать расширения Traffic Engineering для ВСЕХ ИСПОЛЬЗУЕМЫХ протоколов IGP;
3. Активировать протокол RSVP на интерфейсах маршрутизаторов для приема и отправки служебных сообщений;
4. Настроить MPLS TE-туннель;
5. Активировать механизм CSPF.

Конечным результатом настройки является работоспособный TE-туннель, который является транспортом для L2/L3VPN-сервисов.

Настройка инфраструктуры распространения транспортных меток

В первую очередь, для распространения меток необходимо обеспечить IP-связность между loopback-интерфейсами маршрутизаторов, чтобы протокол RSVP мог отправлять и получать служебные сообщения. Для этого необходимо активировать протокол IP на интерфейсах LSR-а и активировать работу IGP протокола (ISIS или OSPFv2) для обмена маршрутной информацией. После того как в сети появилась IP-связность между loopback-интерфейсами LSR-ов, можно считать, что инфраструктура для распространения меток создана.

Включение коммутации MPLS-пакетов на интерфейсах

Таблица 72. Включение MPLS коммутации на интерфейсах LSR.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`mpls`	Переход в режим конфигурации сервисов mpls.
`forwarding`	Переход в режим конфигурации MPLS forwarding.
`interface` <*type*> <*unit*>/<*dev*>/<*port*>.<*sub*>	Включение на интерфейсе функционала коммутации labled IP пакетов.
`root`	Возврат в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

Пример. Включение коммутации MPLS-пакетов на интерфейсах

```
mpls
  forwarding
    interface loopback 1
    interface tengigabitethernet 0/0/17.353
    interface tengigabitethernet 0/0/18.200
    interface tengigabitethernet 0/0/20
  exit
exit
```

NOTE

В данном примере видно, что в конфигурации присутствует интерфейс loopback 1, при этом пакеты через данный интерфейс не передаются. Однако, команда 'mpls forwarding interface loopback N' выполняет важную функцию — на маршрутизаторах серии ME метки генерируются только для тех connected-префиксов, интерфейсы которых добавлены в раздел 'mpls forwarding'. Если необходимо, чтобы Egress LSP получали соответствующие MPLS метки, нужно добавлять loopback интерфейс с IP-адресом, равным LSR-ID в раздел 'mpls forwarding'.

Активация поддержки TE в IGP протоколе

Наличия IP-связности между loopback-интерфейсами недостаточно для работы функционала Traffic Engineering. Необходимо, чтобы протокол IGP распространил дополнительную информацию об интерфейсах маршрутизаторов (например: max-resv-band, available-resv-band, admin-group, te-metric). Эта дополнительная информация позволит маршрутизаторам сети рассчитать LSP с учетом ограничений, накладываемых на LSP конфигурацией TE-туннеля.

Таблица 73. Активация поддержки Traffic Engineering в протоколе OSPF.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`router ospfv2` *NAME*	Создание в конфигурации OSPFv2 процесса с именем *NAME* и переход в режим его настройки.
`te-router-id` *A.B.C.D*	В режиме конфигурации процесса OSPFv2 необходимо указать IPv4-адрес, используемый в качестве LSR-id.
`area` *A.B.C.D*	Создание в конфигурации OSPFv2 процесса области с номером *A.B.C.D*. Параметр является обязательным при создании области. Допустимые формы задания: • **A.B.C.D** — со значениями [0..255] в каждом октете; • **Number** — со значением [0..4294967295];
`interface` <*type*> <*unit*>/<*dev*>/<*port*>.<*sub*>	Переход в режим конфигурации параметров OSPF интерфейса.
`te-support`	Активирует поддержку функционала MPLS TE на OSPF-интерфейсе. После активации интерфейс будет способен обрабатывать т.н. Opaque LSA, в которых и передается информация, необходимая для топологической базы данных (TEDB).
`commit`	Применение произведенных настроек.

NOTE Таким образом, для активации функционала MPLS TE в протоколе OSPF необходимо указать параметр 'te-router-id' и включить 'te-support' на тех интерфейсах, через которые будет идти обмен OSPF LSA.

Пример. Активация MPLS TE в протоколе OSPFv2.

```
router ospfv2 BackBone_Region1
  area 0.0.0.0
    interface loopback 1
    exit
    interface tengigabitethernet 0/0/17.353
      te-support
```

```
    exit
    interface tengigabitethernet 0/0/18.200
      te-support
    exit
    interface tengigabitethernet 0/0/20.350
      te-support
    exit
  exit
  te-router-id 3.3.3.3
exit
```

Таблица 74. Активация поддержки Traffic Engineering в протоколе IS-IS.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`router isis` *NAME*	Создание в конфигурации IS-IS процесса с именем *NAME* и переход в режим его настройки.
`te-router-id` *A.B.C.D*	Команда определяет параметр 'te-router-id' для процесса IS-IS.
`ipv4-te-level` *level-N*	Команда определяет, какой тип — 'level-1' или 'level-2' — используется при работе функционала Traffic Engineering. Допустимые формы задания: • **level-1** — IS-IS маршрутизатор является level-1 устройством; • **level-2** — IS-IS маршрутизатор является level-2 устройством;
`interface` <*type*> <*unit*>/<*dev*>/<*port*>.<*sub*>	Переход в режим конфигурации параметров ISIS интерфейса.
`address-family ipv4 unicast`	Команда активирует протокол IS-IS в режиме Integrated. Допустимые формы задания: • **ipv4 unicast** — IS-IS работает на интерфейсе для маршрутизации IPv4 пакетов; • **ipv6 unicast** — IS-IS работает на интерфейсе для маршрутизации IPv6 пакетов.
`commit`	Применение произведенных настроек.

NOTE Таким образом, для активации функционала MPLS TE в протоколе IS-IS необходимо указать параметр 'ipv4-te-level' и 'te-router-id'.

Пример. Активация MPLS TE в протоколе IS-IS.

```
router isis BackBone_Region1
  interface loopback 1
    address-family ipv4 unicast
    exit
    passive
  exit
  interface tengigabitethernet 0/0/17.353
    address-family ipv4 unicast
    exit
    level level-2
      metric 5
    exit
  exit
  host-name Router1
  ipv4-te-level level-2
  is-level level-2
  net 49.0000.0100.0001.9004.00
  te-router-id 10.0.19.4
exit
```

Активация протокола RSVP на интерфейсах

Для работы функционала Traffic Engineering необходима также работа протокола RSVP во всем IGP-домене. Для этого на каждом маршрутизаторе в IGP-домене необходимо включить протокол RSVP на интерфейсах, участвующих в пересылке MPLS-трафика.

Таблица 75. Активация поддержки Traffic Engineering в протоколе IS-IS.

Команда	**Назначение**
`configure`	Переход в режим глобальной конфигурации.
`mpls`	Переход в режим конфигурации протокола MPLS
`rsvp`	Глобальное включение протокола RSVP и переход в режим его конфигурации.
`interface` <*type*> <*unit*>/<*dev*>/<*port*>.<*sub*>	Включение протокола RSVP на интерфейсе и переход в режим конфигурации параметров протокола RSVP.
`maximum-reservable-bandwidth` *BANDW*	(Опционально) Определение одного из возможных атрибутов интерфейса — max-resv-band, который будет распространен по топологическим базам (TEDB) всех маршрутизаторов IGP домена с включенными расширениями для MPLS TE.
`hellos hello-interval` *MILLISEC*	(Опционально) Включение функции rsvp-hello на интерфейсе N — интервал отправки в миллисекундах.
`commit`	Применение произведенных настроек.

Пример. Включение протокола RSVP.

```
mpls
  rsvp
    interface tengigabitethernet 0/0/17.353
      hellos hello-interval 2000
      maximum-reservable-bandwidth 200000
    exit
    interface tengigabitethernet 0/0/18.200
      hellos hello-interval 2000
      maximum-reservable-bandwidth 102400
    exit
exit
```

Создание MPLS TE туннеля

После подготовки инфраструктуры, активации протокольных расширений IGP для поддержки MPLS TE и развертывания RSVP на маршрутизаторах IGP-домена можно приступать к настройке TE-туннелей.

Таблица 76. Для конфигурации TE-туннеля необходимо:

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`mpls`	Переход в режим конфигурации протокола mpls.
`rsvp`	Глобальное включение протокола RSVP и переход в режим его конфигурации.
`tunnel` *Name*	Создание туннеля с именем *Name* и переход в режим его конфигурации.
`bandwidth` *BW*	(Опционально) Команда выполняется в режиме конфигурации туннеля и определяет требование резервирования полосы пропускания для LSP-туннеля.
`source` *A.B.C.D*	Команда указывает IPv4-адрес, принадлежащий одному из loopback-интерфейсов Ingress LSR-a. Рекомендовано использовать Source IPv4, равный LSR-ID Ingress LSR.
`destination` *A.B.C.D*	Команда указывает IPv4-адрес, принадлежащий одному из loopback-интерфейсов Egress LSR-a. Рекомендовано использовать Destination IPv4, равный LSR-ID Egress LSR.
`tunnel-lsp` *Name*	Команда указывает имя RSVP LSP, которое будет использоваться при построении RSVP LSP и переключает в режим его конфигурации.

Команда	Назначение
`path-computation explicit { partial | path }` *Name*	Команда определяет способ вычисления пути прохождения RSVP LSP. Допустимые формы задания: • **partial** — на Ingress LSR RSVP LSP будет пытаться строиться, даже если CSPF не может рассчитать все hop-by-hop от source до destination (предполагается запуск CSPF на Transit LSR); • **path** — на Ingress LSR протокол CSPF будет вычислять все Transit LSR hop-by-hop от source до destination и только потом сигнализировать RSVP LSP. **NOTE** Без указания данной команды RSVP LSP будет строиться в полностью автоматическом режиме (dynamic).
`commit`	Применение произведенных настроек.

Пример. Настройка MPLS TE туннеля с именем "41".

```
mpls
  rsvp
    interface tengigabitethernet 0/0/17.353
      hellos hello-interval 2000
      maximum-reservable-bandwidth 200000
    exit
    interface tengigabitethernet 0/0/18.200
      hellos hello-interval 2000
      maximum-reservable-bandwidth 102400
    exit
    explicit-path not_over_ne5k
      explicit-route-object 0
        exclude
        ip-prefix 10.0.19.3
        loose
      exit
    exit
    tunnel 41
      bandwidth 1000
      destination 10.0.19.1
      source 10.0.19.4
      tunnel-lsp lsp1
        path-computation explicit path not_over_ne5k
      exit
    exit
  exit
exit
```

Конфигурация TE-туннеля 41 в примере выше определяет, что при расчете RSVP LSP накладываются следующие ограничения:

- Проходить RSVP LSP должен только через те интерфейсы, в которых есть возможность зарезервировать 1Mbps;
- RSVP LSP не должен проходить через LSR с IP-адресом 10.0.19.3 (директива *'exclude ip-prefix'*).

Настройка условий и ограничений для RSVP TE туннеля

Одной из ключевых возможностей функционала MPLS TE является установка различных ограничений и условий для построения TE-туннелей. При конфигурировании TE-туннеля у пользователя есть возможность указать определенные ограничения в зависимости от потребностей в передаче сервисного трафика — например, передавать трафик только через те интерфейсы, на которых есть возможность зарезервировать полосу пропускания в N Mbps; или/и запрет на передачу трафика через интерфейс с IP адресом A.B.C.D; или/и разрешение прохождения трафика через интерфейсы, которые принадлежат региону 'T' или региону 'N', но запрет передачи через интерфейсы, которые включены в радио-релейную трансмиссию.

Как работают ограничения:

1. Каждый LSR должен иметь топологическую базу сети, в которой должна присутствовать дополнительная информация по сравнению с традиционной LSDB;
2. Для того чтобы выполнился первый пункт, необходимо прописать дополнительные атрибуты интерфейсам (max-resv-band/link attribute/te metric) на интерфейсах LSR в IGP домене;
3. Для того чтобы выполнился первый пункт, также необходимо, чтобы дополнительные атрибуты распространились по топологическим базам данных (TEDB) всех LSR в IGP домене — для этого нужно включить поддержку MPLS TE в протоколе IGP;
4. После того как все LSR получили идентичную топологическую базу о сети, на устройствах запускается алгоритм CSPF (Constraint Shortest Path First). Он вычисляет кратчайший путь от Ingress LSR до Egress LSR, который удовлетворяет набору ограничений, прописанных в настройках TE туннеля. Если такой путь вычислить удалось, то результатом работы CSPF будет список узлов, через которые необходимо проложить RSVP LSP для TE-туннеля. Этот список называется Explicit Route Object (ERO);
5. На основании ERO протокол RSVP начнет попытки установить RSVP LSP.

Настройка ограничений: резервирование полосы пропускания для RSVP LSP.

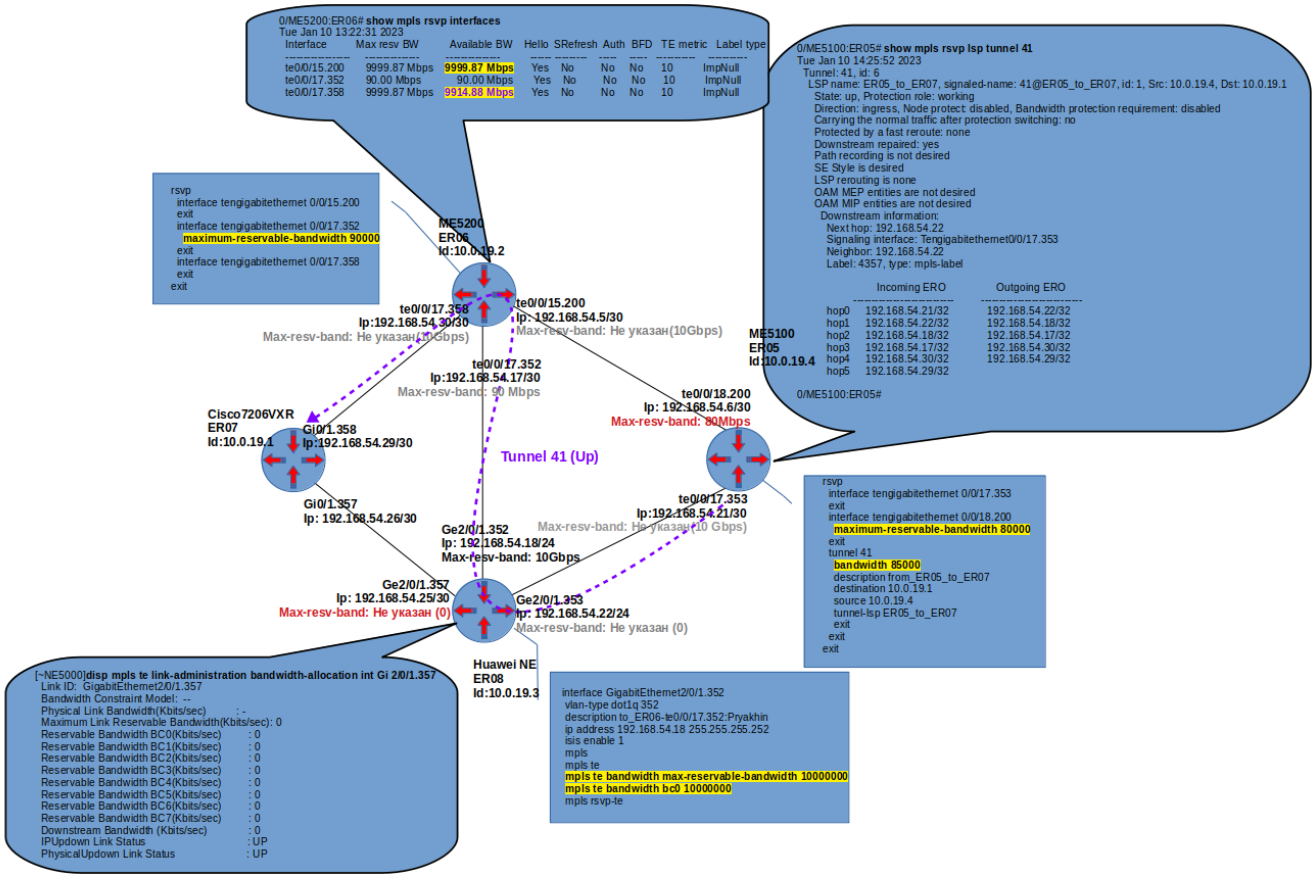


Figure 1. Конфигурация TE-туннеля с требованием резервирования полосы пропускания 85 Mbps.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`rsvp`	Переход в режим настройки протокола RSVP.
`interface te0/0/17.353`	Включение протокола RSVP на интерфейсе te0/0/17.353. **IMPORTANT** Обратите внимание, что атрибут max-resv-band не указан на исходящем интерфейсе te0/0/17.353.
`interface te0/0/18.200`	Включение протокола RSVP на интерфейсе te0/0/18.200.
`maximum-reservable-bandwidth 80000`	В режиме конфигурации RSVP параметров интерфейса te0/0/18.200 задана максимально возможная для резервирования полоса пропускания - 80Mbps.
`exit`	Возврат в режим конфигурации RSVP протокола.
`tunnel 41`	Создание MPLS TE туннеля с именем 41 и переход в режим его конфигурации.
`bandwidth 85000`	Требование резервирования полосы пропускания 85 Mbps на исходящих интерфейсах в IGP домене для LSP TE-туннеля.
`description from_ER05_to_ER07`	Текстовое описание TE-туннеля. Команда не имеет функционального значения, но помогает в анализе конфигурации.

Команда	Назначение
`destination 10.0.19.1`	Определение IPv4 адреса Egress-LSR-а — маршрутизатора, где будет терминироваться TE-туннель.
`source 10.0.19.4`	Определение IPv4 адреса Ingress LSR-а — интерфейса, с которого будет стартовать TE-туннель.
`tunnel-lsp ER05_to_ER07`	Указание имени RSVP LSP TE-туннеля (оно сигнализируется протоколом RSVP) и переход в режим его конфигурации. Далее в режиме конфигурации tunnel-lsp можно указать способ вычисления пути, указать ему backup роль, привязать admin-группы. Поскольку расчёт пути будет динамическим и это действие по умолчанию, ничего конфигурировать в этом режиме не будем.
`exit`	Возврат в режим настроек TE-туннеля.
`exit`	Возврат в режим настроек протокола RSVP.
`root`	Выход в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

NOTE

Обратите внимание на то, как построился LSP TE-туннеля 41. Если считать, что все линки имеют одинаковую TE-метрику, то кратчайшими путями будут:
- ER05→ER06→ER07
- ER05→ER08-ER07

Однако LSP построился по пути, изображенному пунктиром на рисунке 1. Причина в параметре **max-resv-band**, прописанном на интерфейсах маршрутизаторов схемы, и требуемой полосе резервирования для TE-туннеля. Следует обратить внимание, что у разных вендоров значение **max-resv-band** по умолчанию может быть разное. Например, у маршрутизаторов Cisco и Huawei, используемых в вышеописанном примере, **max-resv-band** интерфейса по умолчанию равен нулю. У маршрутизаторов Juniper **max-resv-band** равен физической полосе пропускания интерфейса. На маршрутизаторах Eltex ME max-resv-band по умолчанию равен физической полосе пропускания интерфейса.

Настройка ограничений: explicit path

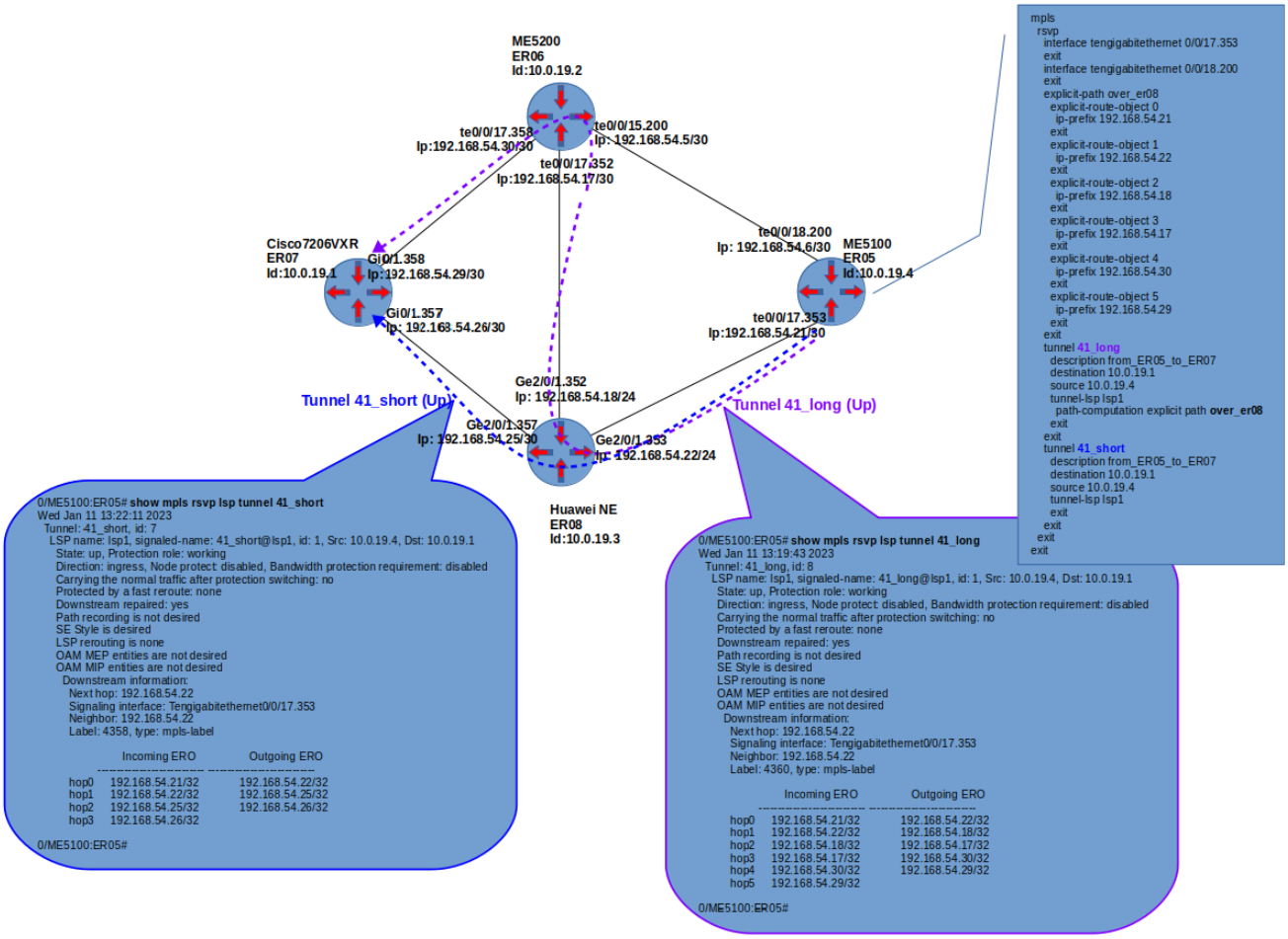


Figure 2. Конфигурация TE-туннеля с ограничением в виде explicit path.

В данном примере рассмотрим другой тип ограничений — explicit-path. Предположим, что необходимо явно указать все хопы, через которые должен пройти RSVP LSP. Для этого в примере создается explicit-path **over_er08**, в котором указаны ipv4 адреса всех интерфейсов, через которые должен пройти LSP. В режиме конфигурации tunnel-lsp TE-туннеля **41_short** используется метод **path-computation dynamic** (это действие по умолчанию, и поэтому команда не отображается в конфигурации).

Таким образом, LSP для TE-туннеля **41_short** механизм CSPF построит без учёта каких-либо ограничений самым оптимальным путём (см синий пунктир на схеме 2). В режиме конфигурации tunnel-lsp TE-туннеля **41_long** применяем сконфигурированный explicit-path **over_er08**, который определяет путь, отображенный фиолетовым пунктиром на схеме 2.

На практике указывать все hop-ы в конфигурации explicit-path избыточно и негибко, поэтому обычно указывают только ipv4 адреса loopback интерфейсов маршрутизаторов, через которые обязательно должен пройти LSP, снабжая их атрибутом 'loose' вместо 'strict'.

Пример конфигурации, показывающий различия в построении двух RSVP LSP (TE-туннель **41_short** *строит свой LSP без ограничений, а TE-туннель* **41_long** *строит свой LSP с учётом ограничений, которые накладывает explicit-path* **over_er08***):*

```
mpls
  rsvp
    interface tengigabitethernet 0/0/17.353
    exit
```

```
    interface tengigabitethernet 0/0/18.200
    exit
    explicit-path over_er08
      explicit-route-object 0
        ip-prefix 192.168.54.21
      exit
      explicit-route-object 1
        ip-prefix 192.168.54.22
      exit
      explicit-route-object 2
        ip-prefix 192.168.54.18
      exit
      explicit-route-object 3
        ip-prefix 192.168.54.17
      exit
      explicit-route-object 4
        ip-prefix 192.168.54.30
      exit
      explicit-route-object 5
        ip-prefix 192.168.54.29
      exit
    exit
    tunnel 41_long
      description from_ER05_to_ER07
      destination 10.0.19.1
      source 10.0.19.4
      tunnel-lsp lsp1
        path-computation explicit partial path over_er08
      exit
    exit
    tunnel 41_short
      description from_ER05_to_ER07
      destination 10.0.19.1
      source 10.0.19.4
      tunnel-lsp lsp1
      exit
    exit
  exit
exit
```

Посмотреть, через какие hop-ы построился RSVP LSP, можно командой:

```
0/ME5100:ER05# show mpls rsvp lsps tunnel 41_short
Wed Jan 11 15:36:30 2023
  Tunnel: 41_short, id: 7
    LSP name: lsp1, signaled-name: 41_short@lsp1, id: 1, Source: 10.0.19.4,
Destination: 10.0.19.1
      State: up, Protection role: working
      Direction: ingress, Node protect: disabled, Bandwidth protection requirement:
disabled
```

```
      Carrying the normal traffic after protection switching: no
      Protected by a fast reroute: none
      Downstream repaired: yes
      Path recording is not desired
      SE Style is desired
      LSP rerouting is none
      OAM MEP entities are not desired
      OAM MIP entities are not desired
        Downstream information:
          Next hop: 192.168.54.22
          Signaling interface: Tengigabitethernet0/0/17.353
          Neighbor: 192.168.54.22
          Label: 4358, type: mpls-label

                          Incoming ERO                 Outgoing ERO
                  ---------------------------- ----------------------------
          hop0     192.168.54.21/32             192.168.54.22/32
          hop1     192.168.54.22/32             192.168.54.25/32
          hop2     192.168.54.25/32             192.168.54.26/32
          hop3     192.168.54.26/32

0/ME5100:ER05# show mpls rsvp lsps tunnel 41_long
Wed Jan 11 15:36:35 2023
  Tunnel: 41_long, id: 8
    LSP name: lsp1, signaled-name: 41_long@lsp1, id: 1, Source: 10.0.19.4,
Destination: 10.0.19.1
      State: up, Protection role: working
      Direction: ingress, Node protect: disabled, Bandwidth protection requirement:
disabled
      Carrying the normal traffic after protection switching: no
      Protected by a fast reroute: none
      Downstream repaired: yes
      Path recording is not desired
      SE Style is desired
      LSP rerouting is none
      OAM MEP entities are not desired
      OAM MIP entities are not desired
        Downstream information:
          Next hop: 192.168.54.22
          Signaling interface: Tengigabitethernet0/0/17.353
          Neighbor: 192.168.54.22
          Label: 4361, type: mpls-label

                          Incoming ERO                 Outgoing ERO
                  ---------------------------- ----------------------------
          hop0     192.168.54.21/32             192.168.54.22/32
          hop1     192.168.54.22/32             192.168.54.18/32
          hop2     192.168.54.18/32             192.168.54.17/32
          hop3     192.168.54.17/32             192.168.54.30/32
          hop4     192.168.54.30/32             192.168.54.29/32
          hop5     192.168.54.29/32
```

```
0/ME5100:ER05#
```

Далее приведем пример про explicit-path с опцией loose. Для того, чтобы не перечислять в жесткой очередности режима strict все ipv4-адреса в explicit-path, используем explicit-path **over_er08_new**.

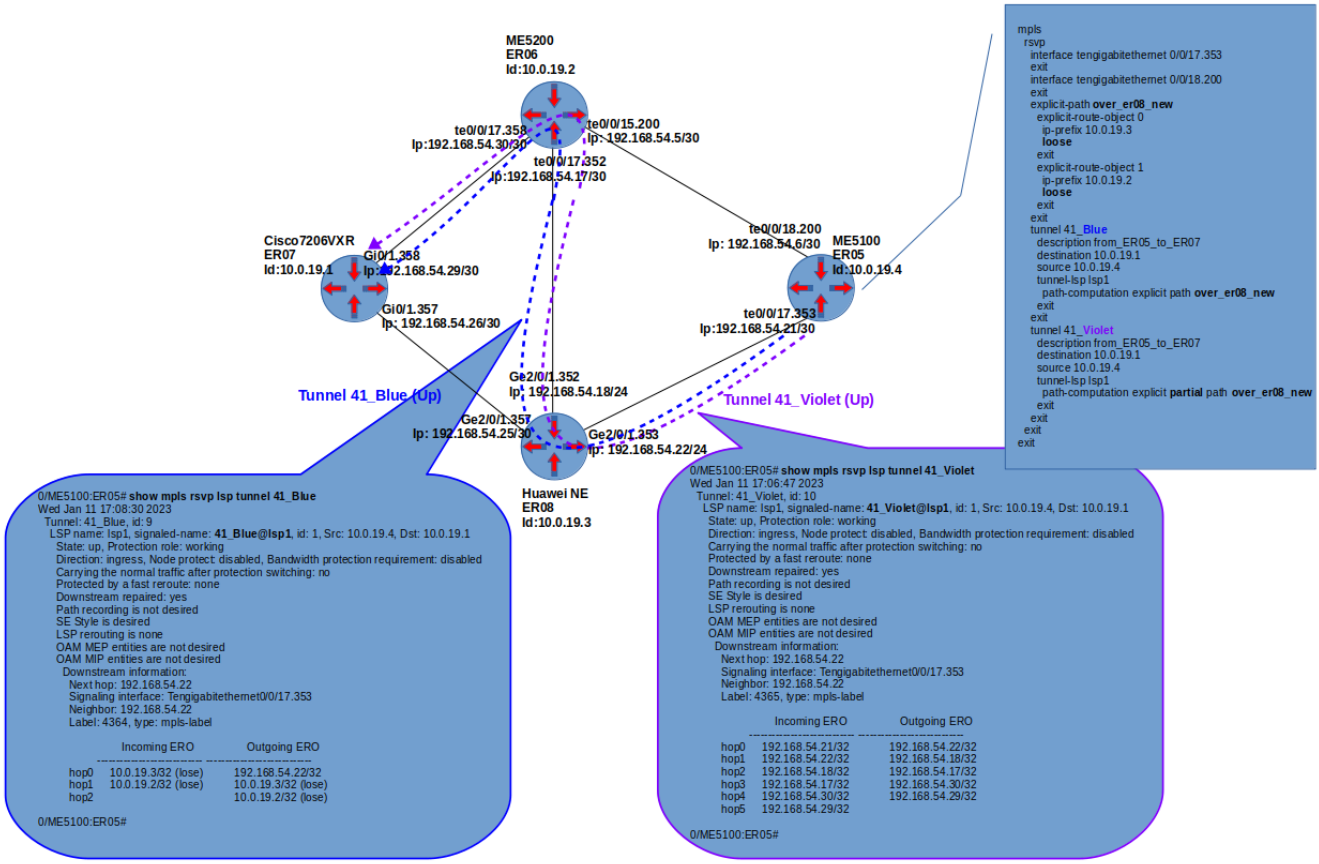


Figure 3. Конфигурация TE-туннелей с explicit path и опциями loose и partial.

Обратите внимание, что TE-туннель **41_Violet** в своей конфигурации имеет опцию **partial**, а TE-туннель **41_Blue** — нет. Explicit-path они оба используют один и тот же - **over_er08_new**. Построились оба LSP по одинаковому пути, но в выводе команды **show mpls rsvp lsps tunnel Имя_туннеля** объекты ERO отображаются по-разному. Опция **partial**, при использовании path-computation explicit, даёт указание протоколу CSPF рассчитать все промежуточные узлы от Ingress-LSR до Egress-LSR. Таким образом ingress LSR с этой опцией будет преобразовывать сконфигурированный нами explicit-path **over_er08_new** с двумя loose Explicit-Route объектами в последовательность из пяти strict Explicit-Route объектов (см. блок "Outgoing ERO" в выводе команды show mpls rsvp lsps tunnel <Имя_туннеля>).

Если не использовать опцию **partial**, то Ingress LSR рассчитает промежуточные Explicit-Route объекты только до первого узла, указанного как loose, и будет "полагать", что указанный как loose следующий маршрутизатор при обработке PATH-сообщения, запустит свой CSPF и добавит последующие недостающие strict ERO.

Настройка ограничений: Affinity/Admin Group

Сначала дадим определение понятий которыми будем оперировать далее:

- **Признак** - абстрактное условие принадлежности интерфейса к определенному классу. Например, признак принадлежности к условному "цвету", либо признак принадлежности к определённому типу передающей среды (радиорелейная среда, оптоволокно, медная витая пара и т.д.), либо признак правообладания линией связи (собственная, аренда у ISP1, аренда у ISP2 и т.д). Признаков можно придумать множество и они определяются экспертами на этапе планирования дизайна сети и модифицируются на этапе эксплуатации сети;
- **Admin-Group** - 32-битный вектор, в котором каждый отдельный бит (или их комбинация) определяет тот или иной признак (согласно дизайн-проекту на сеть, HLD/LLD), применяется на интерфейс и распространяется внутри IGP-домена протоколом маршрутизации (IS-IS/OSPF).
- **Affinity** - 32-битный вектор, назначаемый RSVP LSP TE-туннеля и определяющий, какие интерфейсы будут "родственны" для конкретного RSVP LSP, а какие нет.
- **Mask** - 32-битный параметр, который определяет, какие биты между **Admin Group** и **Affinity** подлежат проверке на совпадение (назовём это элементом родства), а какие — не анализируются. "Единица" в маске определяет что соответствующие битовые позиции в **Admin Group** и **Affinity** должны совпадать, "ноль" в маске определяет, что соответствующие битовые позиции в **Admin Group** и **Affinity** не анализируются и могут быть любыми.

Существуют две концепции применения **Affinity/Admin Group** на практике. Назовём их **Лаконичная** и **Интуитивная**.

Лаконичная — требует записи всех трёх параметров в шестнадцатеричном виде. **Admin Group** применяется на линки (по умолчанию AG = 0x0), **Affinity** и **Mask** - на RSVP LSP TE-туннеля. После этого CSPF может исключить из рассмотрения те линки, которые будут не родственны TE-туннелю. Глубину проверки родства определяет параметр **Mask** (по умолчанию Mask = 0x0).

Интуитивная — требует кодировать признаки отдельными битами, а не их комбинациями, в результате чего возникает взаимно-однозначное соответствие **Признак - Битовая позиция**, которую можно отразить в конфигурации. Такое соответствие упрощает понимание, какие биты какие признаки кодируют, но ценой этого является неэффективное использование 32-битного пространства значений Affinity. Например, необходимо закодировать пять "цветов". Если использовать **Лаконичную** концепцию, то понадобится только 3 бита, которыми можно закодировать 5 цветов, и ещё 3 оставить в резерве на случай расширения потребностей. Если использовать **Интуитивную** концепцию, то понадобятся все 5 бит — это неэкономно, но легко читается оператором. Вместо параметра Mask вводится три интуитивно понятные подгруппы соответствия:

- **include-all** — все признаки, указанные в affinity, должны присутствовать в параметре **Admin Group** интерфейса ("если Интерфейс-Паша и Туннель-Саша имеют одинаковые признаки: цвет глаз, форму носа и ушей, то они признаются родственными друг другу");
- **include-any** — хотя бы один признак из этой подгруппы, указанный в **Affinity**, должен совпадать с **Admin Group** интерфейса ("если Интерфейс-Паша и Туннель-Саша имеют одинаковый рост или вес, то признаются троюродными братьями");
- **exclude** — признаки, указанные в этой подгруппе в **Affinity**, должны отсутствовать в

параметре **Admin Group** интерфейса ("если Туннель-Саша имеет признак болельщика ФК ЦСКА и внесен в соответствующую группу, то Интерфейс-Паша не должен болеть за ФК ЦСКА, и тогда они снова являются родными друг другу").

RFC 3209 определяет последовательность проверок признаков, указанных в разных группах (так как для одного RSVP LSP можно указать признаки в разных подгруппах) Таких проверки три:

1. `(admin-group & exclude-any) == 0` — проверка, что никакие атрибуты, указанные в exclude-group, не установлены на интерфейсе;
2. `(include-any == 0) | ((admin-group & include-any) != 0)` — проверка, что include-any признаки у RSVP LSP не установлены либо на линке указан хоть один из установленных в группе include-any признаков;
3. `(include-all == 0) | (((admin-group & include-all) ^ include-all) == 0)` — проверка, что include-all признаки у RSVP LSP не установлены либо на линке установлены все признаки из группы include-all у RSVP LSP туннеля

Если все три теста успешны, то такой линк признаётся родственным туннелю и допускается к расчёту оптимального пути протоколом CSPF.

Перейдём к практическому примеру:

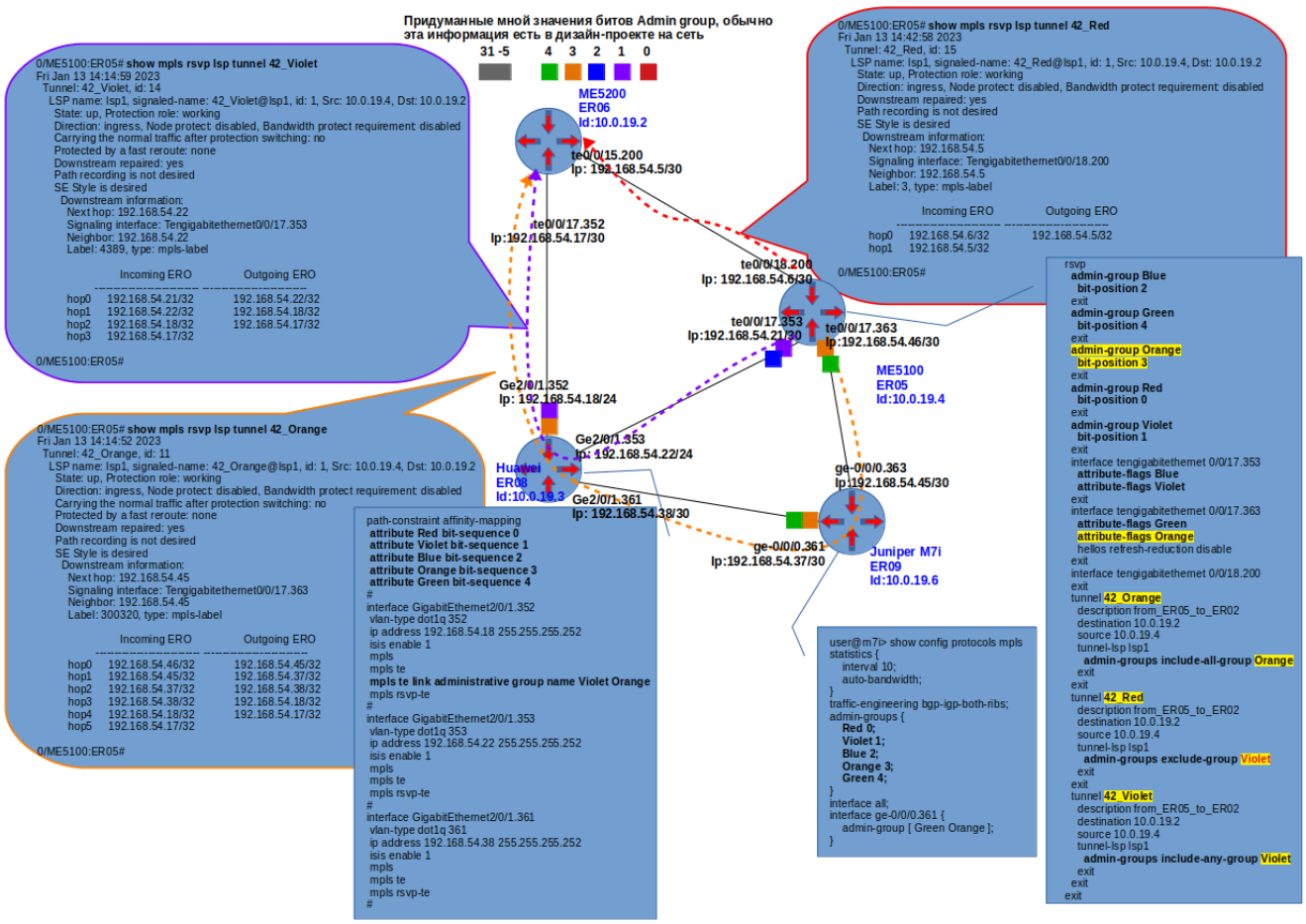


Figure 4. Конфигурация TE-туннеля с ограничением в виде Admin-Group.

На рисунке выше видно:

- RSVP LSP **42_Orange@lsp1** построился единственно возможным путем — через линки, на которых имеется признак "Orange" (оранжевая пунктирная линия);
- RSVP LSP **42_Violet@lsp1** построился единственно возможным путем — через линки, на которых имеется признак "Violet" (фиолетовая пунктирная линия);
- RSVP LSP **42_Red@lsp1** построился единственно возможным путем — через линки, на которых отсутствует признак "Violet" (красная пунктирная линия).

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`mpls rsvp`	Переход в режим настройки протокола RSVP.
`admin-group Red bit-position 0`	Назначаем битам 0 1 2 3 4 соответствие условным признакам **Red**, **Violet**, **Blue**, **Orange**, **Green** согласно дизайну сети.
`admin-group Violet bit-position 1`	
`admin-group Blue bit-position 2`	
`admin-group Orange bit-position 3`	
`admin-group Green bit-position 4`	
`interface te0/0/17.353`	Включение протокола RSVP на интерфейсе и переход в режим его конфигурации
`attribute-flags Blue`	В режиме конфигурации RSVP-параметров интерфейса te0/0/17.353 присваиваем ему признаки **Blue**, **Violet**.
`attribute-flags Violet`	
`exit`	Возврат в режим конфигурации RSVP протокола.
`interface te0/0/17.363`	Включение протокола RSVP на интерфейсе te0/0/17.363 и переход в режим его конфигурации.
`attribute-flags Green`	В режиме конфигурации RSVP-параметров интерфейса te0/0/17.363 присваиваем ему признаки **Green**, **Orange**.
`attribute-flags Orange`	
`exit`	Возврат в режим конфигурации RSVP протокола.
`tunnel 42_Orange`	Создаём 3 MPLS TE туннеля с именами 42_Orange, 42_Red, 42_Violet и настраиваем их на использование Admin-Groups с различными вариантами **include-all-group**, **include-any-group**, **exclude-group** (далее повторяющиеся команды опустим).
`tunnel 42_Red`	
`tunnel 42_Violet`	
`destination 10.0.19.2`	Определение IPv4-адреса Egress-LSR-а — маршрутизатора, где будет терминироваться TE-туннель.
`source 10.0.19.4`	Определение IPv4-адреса с Ingress LSR-а — интерфейса, с которого будет строиться TE-туннель.
`tunnel-lsp lsp1`	Создаем у TE-туннеля LSP с именем **lsp1** и переходим в режим его конфигурирования.

Команда	Назначение
`admin-groups include-all-group Orange`	Для RSVP LSP **42_Orange@lsp1** применяем ограничение через битовый вектор "соответствие всем признакам". Процесс CSPF будет использовать для расчёта только те линки, которые будут иметь все битовые признаки, указанные в команде. В данном примере обязательный признак на интерфейсах один - **Orange**.
`admin-groups exclude-group Violet`	Для RSVP LSP **42_Red@lsp1** применяем ограничение через битовый вектор "exclude-group". Процесс CSPF будет использовать для расчёта только те линки, которые НЕ будут иметь битовые признаки, указанные в команде. В данном примере признак один — "цвет" Violet. RSVP LSP **42_Red@lsp1** должен построиться, избегая интерфейсов с признаком **Violet**.
`admin-groups include-any-group Violet`	Для RSVP LSP **42_Violet@lsp1** применяем ограничение через битовый вектор "соответствие хотя бы одному признаку". Процесс CSPF будет использовать для расчёта только те линки, которые будут иметь хотя бы один из перечисленных в команде битовых признаков. В данном примере желаемый признак на интерфейсах один — **Violet**.
`exit`	Возврат в режим настроек TE-туннеля.
`exit`	Возврат в режим настроек протокола RSVP.
`root`	Выход в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

NOTE

Посмотреть топологическую базу данных (TEDB) можно командой *"show mpls te topology"*. В ней для каждого интерфейса IGP-домена есть параметр "Color/Resource class" — это представление "Link Attribute" (он же "Admin Group") в шестнадцатеричном формате.

Способы перенаправления сервисного трафика в TE-туннель

После того как LSP TE-туннеля успешно построился протоколом RSVP, сервисный трафик в него автоматически передаваться по-прежнему не будет. Для того чтобы перенаправить трафик в RSVP LSP, необходимо выполнить дополнительные действия.

Рассмотрим различные варианты направления трафика в TE-туннель:

- **IGP shortcut** — это способ представить TE-туннель как интерфейс с включенным IGP-протоколом и назначенной метрикой, при этом информация о данном интерфейсе не анонсируется в IGP домен; следовательно, другие маршрутизаторы не знают о его существовании и не могут переправить трафик через TE-туннель;

- **Static route** — этот способ позволяет, используя статическую маршрутизацию, перенаправить трафик на подсеть из глобальной таблицы маршрутизации (GRT) в TE-туннель.
- **L3VPN Forwarding** — для того, чтобы RSVP LSP рассматривался маршрутизатором как возможный интерфейс для доставки трафика к nexthop'у маршрута в VRF, необходимо выполнить команду 'l3vpn' в режиме конфигурации протокола RSVP;
- **L2VPN switching** — для того, чтобы сервисный трафик из xconnect или bridge-domain мог быть передан через RSVP LSP, необходимо в конфигурации PW L2VPN-сервиса указать команду *"transport rsvp tunnel NAME"*.

Рассмотрим эти способы более детально.

Форвардинг IP-трафика GRT (глобальной таблицы маршрутизации) через TE-туннель методом IGP shortcut

На маршрутизаторах серии ME использование метода IGP shortcut позволяет перенаправить в TE-туннель трафик из GRT, но не затрагивает трафик из L2- или L3VPN-сервисов.

Задача: Необходимо обеспечить IP связность между CE1 и CE2 в GRT.

Топология:

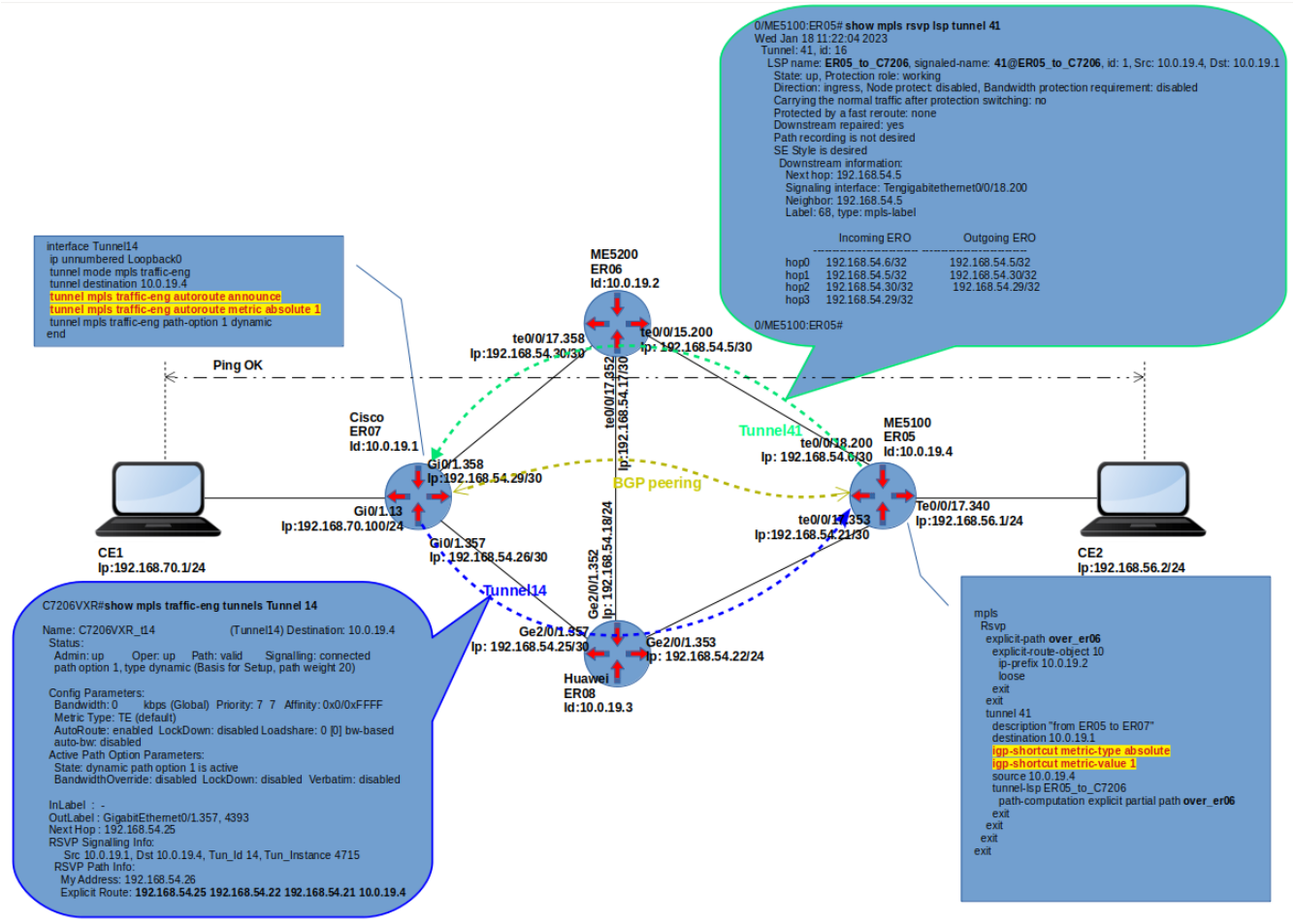


Figure 5. Передача трафика из GRT через TE-туннель

На промежуточных P-маршрутизаторах (ER06 и ER08) нет маршрутной информации о сетях 192.168.70.0/24 и 192.168.56.0/24. Информация о них распространяется по протоколу BGP между PE-маршрутизаторами; следовательно, для обеспечения связности PE-маршрутизаторы должны инкапсулировать этот трафик в TE-туннели, построенные между ними.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`mpls`	Переход в режим конфигурации функционала MPLS.
`rsvp`	Переход в режим настройки протокола RSVP.
`interface te0/0/17.353`	Включение протокола RSVP на интерфейсе te0/0/17.353.
`interface te0/0/18.200`	Включение протокола RSVP на интерфейсе te0/0/18.200.
`exit`	Возврат в режим конфигурации протокола RSVP.
`tunnel 41`	Создаем TE-туннель с именем 41 и переходим в режим его конфигурации.
`description from ER05 to ER07`	Текстовое описание TE-туннеля для облегчения понимания конфигурации.
`destination 10.0.19.1`	Команда указывает на LSR-ID Egress-маршрутизатора. В нашем примере это ER07.
`igp-shortcut metric-type absolute`	Команда включает функционал igp-shorcut и определяет тип метрики — absolute.
`igp-shortcut metric-value 1`	Команда определяет значение IGP-метрики для TE-туннеля, равной '1'.
`source 10.0.19.4`	Команда устанавливает LSR-ID Ingress-маршрутизатора в качестве источника TE-туннеля.
`tunnel-lsp ER05_to_C7206`	Создаем RSVP LSP с сигнальным именем 'ER05_to_C7206' и переходим в режим его конфигурирования.
`path-computation explicit partial path over_er06`	Команда накладывает ограничение на построение LSP, он должен проходить через hop-ы, указанные в конфигурации explicit-path 'over_er06'.
`commit`	Применение произведенных настроек.

IMPORTANT

После того как TE-туннель сконфигурирован способом, описанным выше, он все еще не может быть использован для доставки трафика до узла 10.0.19.1, даже если его метрика равна 1, а у альтернативного IGP маршрута метрика 25. **Из-за архитектурных особенностей маршрутизаторов серии ME необходимо включить функционал ECMP через команду режима глобальной конфигурации 'router equal-cost'**.

Пример. Детальная конфигурация протокола RSVP для форвардинга трафика из GRT через TE-туннель 41:

```
  rsvp
    interface tengigabitethernet 0/0/17.353
    exit
    interface tengigabitethernet 0/0/18.200
    exit
    explicit-path over_er06
      explicit-route-object 10
        ip-prefix 10.0.19.2
        loose
      exit
    exit
    tunnel 41
      description "from ER05 to ER07"
      destination 10.0.19.1
      igp-shortcut metric-type absolute
      igp-shortcut metric-value 1
      source 10.0.19.4
      tunnel-lsp ER05_to_C7206
        path-computation explicit partial path over_er06
      exit
    exit
  exit

router equal-cost
```

Маршрут на C7206 (ER07)	**Маршрут на ME5100 (ER05)**
C7206VXR#show ip route **192.168.56.2** Routing entry for **192.168.56.0/24** Known via "static", distance 1, metric 0 (connected) Routing Descriptor Blocks: * directly connected, via **Tunnel14** Route metric is 0, traffic share count is 1 C7206VXR#	0/ME5100:ER05# show route **192.168.70.100** Wed Jan 18 12:20:36 2023 Routing entry for **192.168.70.0/24** Last update: 02h53m37s Routing Descriptor Blocks 192.168.54.5, via **tu41@ER05_to_C7206** Known via bgp, distance 200, metric 0 type bgp-internal, protection none, route-type remote Entries: 1 0/ME5100:ER05#

Форвардинг IP-трафика GRT (глобальной таблицы маршрутизации) через TE-туннель с помощью статического маршрута

На маршрутизаторах серии ME использование данного метода позволяет перенаправлять трафик из GRT, но не затрагивает трафик L2- или L3VPN-сервисов.

Задача: Необходимо обеспечить IP связность между CE1 и CE2 в GRT
Топология:

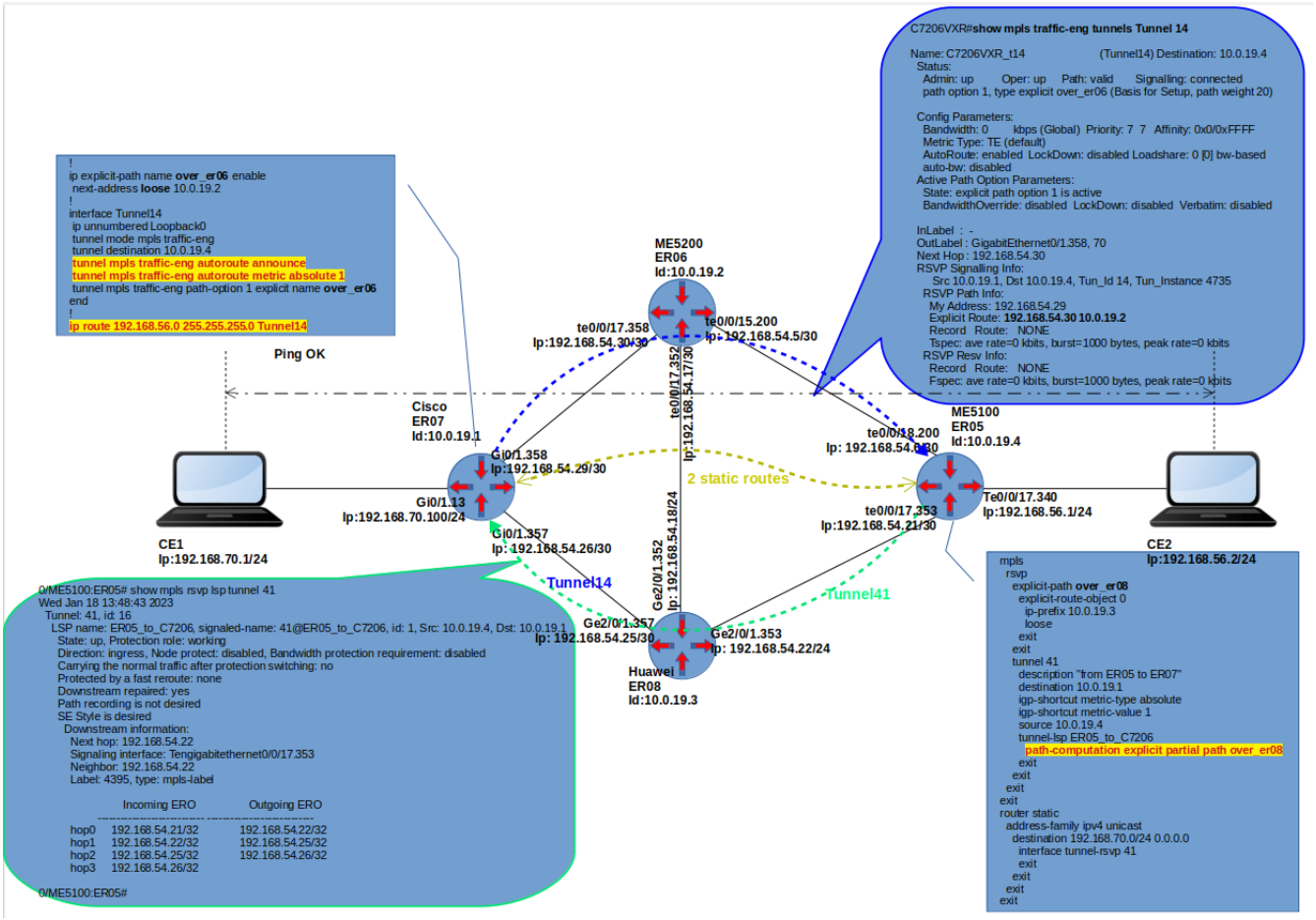


Figure 6. Передача трафика из GRT через TE-туннель с помощью статического маршрута

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`rsvp`	Переход в режим настройки протокола RSVP.
`tunnel 41`	Создаем TE-туннель с именем 41 и переходим в режим его конфигурации.
`description from_ER05_to_ER07`	Текстовое описание TE-туннеля для облегчения понимания конфигурации.
`destination 10.0.19.1`	Команда указывает на LSR-ID Egress маршрутизатора. В нашем примере это ER07.
`forwarding-adjacency`	Команда устанавливает атрибут возможности передачи сервисного трафика через RSVP LSP TE-туннеля. **IMPORTANT** Данная команда обязательна для активации возможности передачи трафика через TE-туннель. Без неё форвардинг сервисного трафика через TE-туннель невозможен.

Команда	Назначение
`routing-adjacency`	Команда устанавливает признак TE-туннеля как интерфейса, через который можно получать маршрутную информацию. **IMPORTANT** Данная команда обязательна для активации возможности передачи трафика через TE-туннели. Без неё статический маршрут, использующий TE-туннель как исходящий интерфейс, не будет инсталлирован в таблицу маршрутизации.
`source 10.0.19.4`	Команда указывает LSR-ID Ingress маршрутизатора в качестве источника TE-туннеля.
`tunnel-lsp ER05_to_C7206`	Создаем RSVP LSP с сигнальным именем 'ER05_to_C7206' и переходим в режим его конфигурирования.
`path-computation explicit partial path over_er08`	Команда накладывает ограничение в виде использования explicit-path с именем 'over_er08'.
`commit`	Применение произведенных настроек.

Таблица 77. Пример конфигурации статического маршрута через TE-туннель:

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`router static`	Переходим в режим конфигурации статических маршрутов.
`address-family ipv4 unicast`	Определяем тип address-family и переходим в режим конфигурации дополнительных параметров.
`destination 192.168.70.0/24 0.0.0.0`	Команда указывает сеть назначения для маршрута **IMPORTANT** Адрес шлюза необходимо указать равным 0.0.0.0 в случае использования TE-туннеля как исходящего интерфейса.
`interface tunnel-rsvp 41`	Команда определяет использование TE-туннеля как исходящего интерфейса в статическом маршруте.
`commit`	Применение произведенных настроек.

Пример. Детальная конфигурация протокола RSVP для форвардинга трафика из GRT через TE-туннель 41:

```
mpls
  rsvp
```

```
    interface tengigabitethernet 0/0/17.353
    exit
    interface tengigabitethernet 0/0/18.200
    exit
    explicit-path over_er08
      explicit-route-object 0
        ip-prefix 10.0.19.3
        loose
      exit
    exit
    tunnel 41
      description "from ER05 to ER07"
      destination 10.0.19.1
      forwarding-adjacency
      igp-shortcut metric-type absolute
      igp-shortcut metric-value 1
      routing-adjacency
      source 10.0.19.4
      tunnel-lsp ER05_to_C7206
        path-computation explicit partial path over_er08
      exit
    exit
  exit
exit
router static
  address-family ipv4 unicast
    destination 192.168.70.0/24 0.0.0.0
      interface tunnel-rsvp 41
      exit
    exit
  exit
exit
```

Пример. Таблица маршрутизации:

Cisco 7206 (ER07)	Eltex ME5100 (ER05)
C7206VXR#show ip route 192.168.56.2 Routing entry for 192.168.56.0/24 Known via "static", distance 1, metric 0 (connected) Routing Descriptor Blocks: * directly connected, via **Tunnel14** Route metric is 0, traffic share count is 1	0/ME5100:ER05# show route 192.168.70.1 Routing entry for 192.168.70.0/24 Last update: N/A Routing Descriptor Blocks 192.168.54.22, via **tu41@ER05_to_C7206** Known via static, distance 1, metric 1 type static, protection none, route-type remote Entries: 1

Пример. Обмен ICMP-пакетами

```
C7206VXR#traceroute 192.168.56.2 source 192.168.70.100
Type escape sequence to abort.
Tracing the route to 192.168.56.2
```

```
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.54.30 [MPLS: Label 70 Exp 0] 4 msec 0 msec 0 msec
  2 192.168.54.6 0 msec 0 msec 0 msec
  3 192.168.56.2 4 msec 0 msec 4 msec
C7206VXR#

0/ME5100:ER05# traceroute 192.168.70.1 source 192.168.56.1
Mon Oct  7 16:45:52 2019
Traceroute to 192.168.70.1 (192.168.70.1), 30 hops max, 60 byte packets
 1  192.168.70.1 (192.168.70.1)  0.323 ms  0.312 ms  0.304 ms
0/ME5100:ER05#
```

Форвардинг L3VPN-трафика через TE-туннель

На маршрутизаторах серии ME использование данного метода позволяет перенаправить трафик L3VPN-сервисов в TE-туннель.

Задача: Необходимо обеспечить IP-связность между CE1 и CE2 в VRF 'TEST1'
Топология:

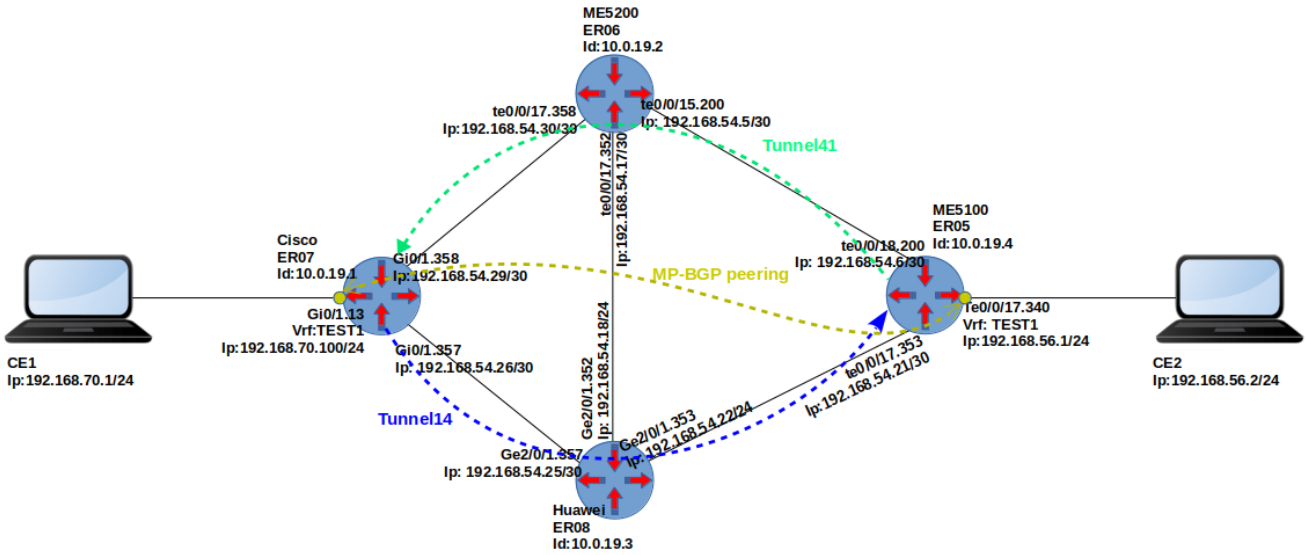


Figure 7. Передача сервисного трафика из VRF TEST1 через TE-туннель.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`rsvp`	Переход в режим настройки протокола RSVP.
`interface te0/0/17.353`	Включение протокола RSVP на интерфейсе te0/0/17.353.
`interface te0/0/18.200`	Включение протокола RSVP на интерфейсе te0/0/18.200.
`exit`	Возврат в режим конфигурации RSVP протокола.

Команда	Назначение
`l3vpn`	Включение режима передачи L3VPN трафика через TE-туннели. **IMPORTANT** Данная команда обязательна для активации возможности передачи трафика через TE-туннели. Команда работает для трафика всех VRF, созданных на данном маршрутизаторе. При наличии RSVP LSP до конкретного nexthop'a, L3VPN маршрут с таким nexthop'ом будет использовать LSP для отправки сервисного трафика.
`tunnel 41`	Создаем TE-туннель с именем 41 и переходим в режим его конфигурации.
`description "from ER05 to ER07"`	Текстовое описание TE-туннеля для облегчения понимания конфигурации.
`destination 10.0.19.1`	Команда указывает на LSR-ID Egress маршрутизатора. В нашем примере это ER07.
`forwarding-adjacency`	Команда устанавливает атрибут возможности передачи сервисного трафика через RSVP LSP TE-туннеля. **IMPORTANT** Данная команда обязательна для активации возможности передачи трафика через TE-туннели. Без неё BGP vpnv4 маршруты, изученные от удалённых PE-маршрутизаторов, не будут инсталлированы в таблицу маршрутизации VRF, так как работоспособного транспортного LSP до next-hop-ов, изученных маршрутов не будет (несмотря на то, что TE-туннель в состоянии UP). Команда 'routing-adjacency' в данном сценарии не нужна.
`source 10.0.19.4`	Команда устанавливает LSR-ID Ingress-маршрутизатора в качестве источника TE-туннеля.
`tunnel-lsp ER05_to_C7206`	Создаем RSVP LSP с сигнальным именем 'ER05_to_C7206' и переходим в режим его конфигурирования.
`path-computation explicit partial path over_er06`	Команда накладывает ограничение на построение LSP — он должен проходить через маршрутизатор ER06.

Команда	Назначение
commit	Применение произведенных настроек.

Пример. Детальная конфигурация протокола RSVP для форвардинга трафика из VRF 'Test1' через TE-туннель:

```
mpls
 rsvp
    interface tengigabitethernet 0/0/17.353
    exit
    interface tengigabitethernet 0/0/18.200
    exit
    explicit-path over_er06
      explicit-route-object 10
        ip-prefix 10.0.19.2
        loose
      exit
    exit
    l3vpn
    tunnel 41
      description "from ER05 to ER07"
      destination 10.0.19.1
      forwarding-adjacency
      source 10.0.19.4
      tunnel-lsp ER05_to_C7206
        path-computation explicit partial path over_er06
      exit
    exit
  exit
exit
```

Пример. Просмотр таблицы маршрутизации VRF 'TEST1':

```
0/ME5100:ER05# show route vrf TEST1
Wed Jan 18 18:53:42 2023
  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,
      BL - BGP labeled, R - RIP


  C      192.168.56.0/24     is directly connected, 00h17m29s, te0/0/17.340
  L      192.168.56.1/32     is directly connected, 00h17m29s, te0/0/17.340
  B BV   192.168.70.0/24    via 10.0.19.1 [200/0], 00h08m58s

  Total entries: 3
```

```
0/ME5100:ER05# show l3forwarding vrf TEST1
Wed Jan 18 18:54:32 2023
  Prefix                    Nexthop                   Outgoing label     Interface
  ------------------------ ------------------------ ------------------ ----------
  192.168.56.0/24           attached                     --/--          te0/0/17.340
  192.168.56.1/32           receive                      --/--          te0/0/17.340
  192.168.70.0/24           192.168.54.5                 73/43          te0/0/18.200
0/ME5100:ER05# ping 192.168.70.1 source 192.168.56.1 vrf TEST1
Wed Jan 18 18:54:32 2023

Sending 4, 56-byte ICMP Echos to 192.168.70.1,
request send interval is 0.100 seconds,
response wait timeout is 2.000 seconds:
!!!!

Success rate is 100 percent (4/4), round-trip min/avg/max = 0.282/0.303/0.314 ms
0/ME5100:ER05#
```

Форвардинг L2VPN-трафика через TE-туннель

На маршрутизаторах серии ME использование данного метода позволяет перенаправить трафик L2VPN-сервисов в TE-туннель.

Задача: Необходимо обеспечить IP связность между CE1 и CE2 через VPLS сервис 'BD-TEST'
Топология:

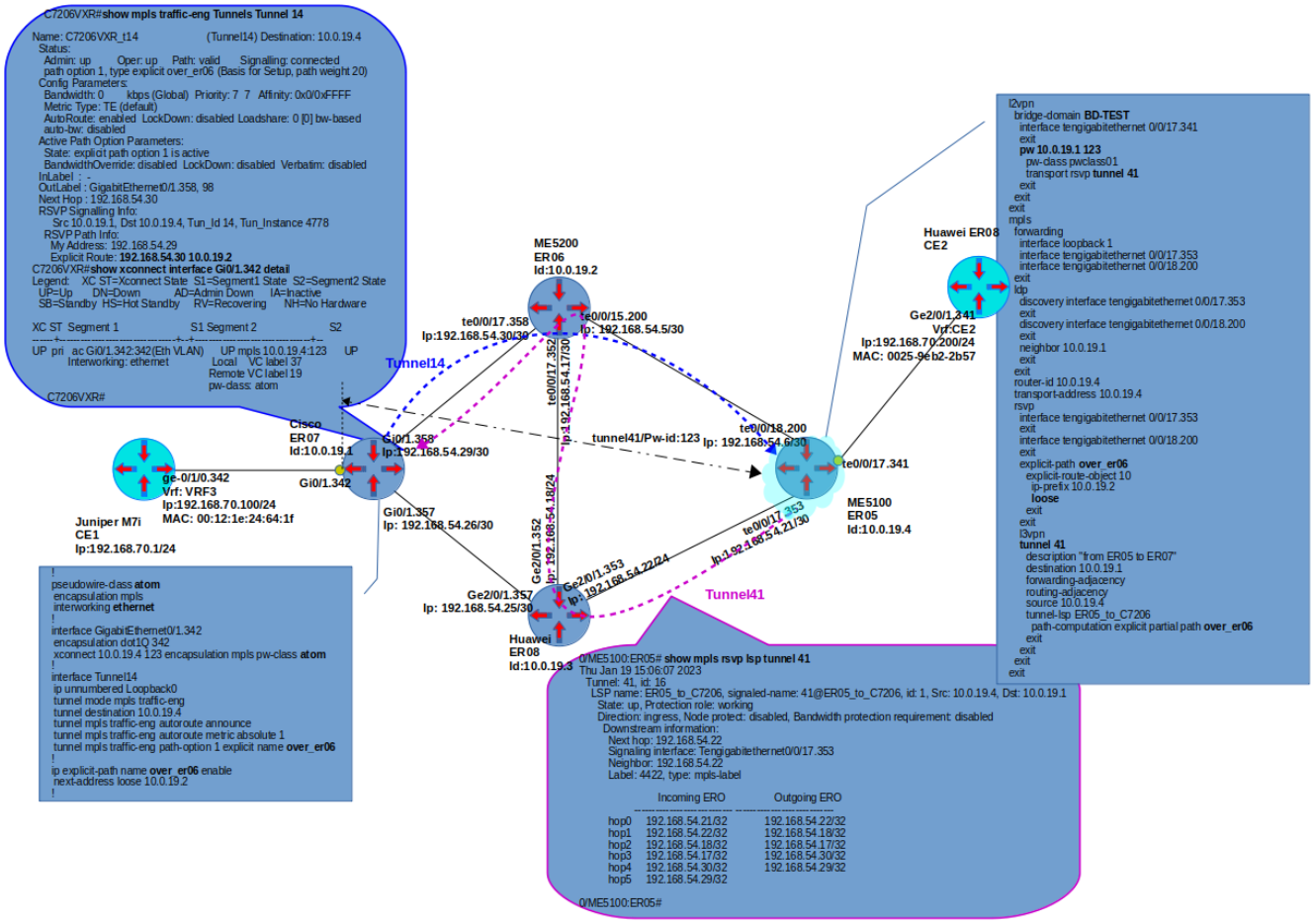


Figure 8. Передача сервисного трафика через L2VPN и TE-туннель.

Создание бридж-домена VPLS, псевдопровода и pw-class'а для псевдопровода:

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`l2vpn pw-class pwclass01`	Создаем pw-class с именем 'pwclass01' и переходим в режим его конфигурирования.
`encapsulation mpls signaling-type pseudowire-id-fec-signaling`	Указываем набор параметров, необходимых для сигнализации PW.
`root`	Возврат в режим глобальной конфигурации.
`l2vpn bridge-group default bridge-domain BD-TEST`	Создаём VPLS сервис с именем 'BD-TEST' и переходим в режим его конфигурирования.
`interface te0/0/17.341`	Указываем интерфейс как AC-интерфейс в VPLS сервисе.
`exit`	Возврат в режим конфигурации VPLS *BD-TEST*.
`pw 10.0.19.1 123`	Создаем VC интерфейс для обмена метками с ER07 и организации PW-канала для передачи сервисного трафика, а также переходим в режим его конфигурирования.
`pw-class pwclass01`	Указываем использовать при построении PW параметры из 'pwclass01', который мы создали ранее.

Команда	Назначение
`transport rsvp tunnel 41`	Указываем использовать TE-туннель *41* в качестве транспортного для этого бридж-домена (экземпляра VPLS).
`commit`	Применение произведенных настроек.
`root`	Возврат в режим глобальной конфигурации.

Создание targeted LDP-сессии до соседнего PE:

Команда	Назначение
`mpls`	Переход в режим конфигурации функционала MPLS.
`ldp`	Переход в режим конфигурации протокола LDP.
`neighbor 10.0.19.1`	Создаем remote LDP соседа '10.0.19.1' (ER07) и переходим в режим его конфигурации.
`exit`	Выходим из режима конфигурации LDP соседа.
`exit`	Выходим из режима конфигурации протокола LDP.
`transport-address 10.0.19.4`	Указываем в качестве source IP для установления LDP соседств собственный LSR-ID.
`commit`	Применение произведенных настроек.
`root`	Возврат в режим Global Config

Создание TE-туннеля с именем 41:

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`rsvp`	Переход в режим настройки протокола RSVP.
`interface te0/0/17.353`	Включение протокола RSVP на интерфейсе te0/0/17.353.
`interface te0/0/18.200`	Включение протокола RSVP на интерфейсе te0/0/18.200.
`exit`	Возврат в режим конфигурации RSVP протокола.
`tunnel 41`	Создаем TE-туннель с именем 41 и переходим в режим его конфигурации.
`description from ER05 to ER07`	Текстовое описание TE-туннеля для облегчения понимания конфигурации.
`destination 10.0.19.1`	Команда указывает на LSR-ID Egress маршрутизатора. В нашем примере это ER07.

Команда	Назначение
`forwarding-adjacency`	Команда устанавливает атрибут возможности передачи сервисного трафика через RSVP LSP TE-туннеля. **IMPORTANT** Данная команда обязательна для включения возможности передачи трафика через TE-туннели. Обратите внимание, что команда 'routing-adjacency' в данном сценарии не нужна.
`source 10.0.19.4`	Команда устанавливает LSR-ID Ingress-маршрутизатора в качестве источника TE-туннеля.
`tunnel-lsp ER05_to_C7206`	Создаем RSVP LSP с сигнальным именем 'ER05_to_C7206' и переходим в режим его конфигурирования.
`path-computation explicit partial path over_er06`	Команда накладывает ограничение на построение LSP, он должен проходить через маршрутизатор ER06.
`commit`	Применение произведенных настроек.
`root`	Возврат в режим Global Config

Последний момент — конфигурация AC-интерфейса в L2VPN-сервисе:

Команда	Назначение
`interface te0/0/17.341`	Создание сабинтерфейса и переход в режим его конфигурации
`encapsulation outer-vid 341`	Указываем внешний (он же единственный в данном примере) vlan-тэг с ID=341.
`rewrite egress tag push outer-vid 341`	Команда добавляет vlan-тэг с ID 341 к исходящим фреймам саб-интерфейса.
`rewrite ingress tag pop one`	Команда удаляет внешний vlan-тэг у всех входящих на саб-интерфейс ethernet-фреймов.
`commit`	Применение произведенных настроек.
`root`	Возврат в режим Global Config

IMPORTANT

Зачем нужны команды push и pop? Это необходимо делать по двум причинам. Во-первых, ER07 в тесте — это маршрутизатор Cisco, который удаляет VLAN-тэг у ethernet-фрейма, прежде чем отправить его через псевдопровод. Маршрутизаторы серии ME по умолчанию **не производят преобразований** с ethernet-фреймами, пришедшими с AC или VC каналов (кадры уходят с тем же тегами, с какими пришли). Во-вторых, VLAN ID у AC-интерфейсов разные (342 со стороны ER07, 341 со стороны ER05). В этом случае, даже если PW поднять между маршрутизаторами ELTEX ME, push и pop операции с тэгами

> необходимы, чтобы нивелировать разницу VLAN ID.

Пример. Необходимая конфигурация на маршрутизаторе ER05 в описанном сценарии:

```
interface tengigabitethernet 0/0/17.341
  encapsulation outer-vid 341
  rewrite egress tag push outer-vid 341
  rewrite ingress tag pop one
exit
mpls
  forwarding
    interface loopback 1
    interface tengigabitethernet 0/0/17.353
    interface tengigabitethernet 0/0/18.200
  exit
  ldp
    discovery interface tengigabitethernet 0/0/17.353
    exit
    discovery interface tengigabitethernet 0/0/18.200
    exit
    neighbor 10.0.19.1
    exit
  exit
  router-id 10.0.19.4
  transport-address 10.0.19.4
  rsvp
    interface tengigabitethernet 0/0/17.353
    exit
    interface tengigabitethernet 0/0/18.200
    exit
    explicit-path over_er06
      explicit-route-object 10
        ip-prefix 10.0.19.2
        loose
      exit
    exit
    l3vpn
    tunnel 41
      description "from ER05 to ER07"
      destination 10.0.19.1
      forwarding-adjacency
      routing-adjacency
      source 10.0.19.4
      tunnel-lsp ER05_to_C7206
        path-computation explicit partial path over_er06
      exit
    exit
  exit
exit
0/ME5100:ER05#
```

Пример. Просмотр статуса VPLS-сервиса.

```
0/ME5100:ER05# show l2vpn bridge-domain bd-name BD-TEST
Thu Jan 19 17:14:25 2023
  MM  -- mtu mismatch            Up -- up              GUp -- going up
  CM  -- control-word mismatch   Dn -- down            GDn -- going down
  OL  -- no outgoing label       ST -- standby         Lld -- lower layer down
  BK  -- backup connection       Fl -- failed          Drm -- dormant
  SP  -- static pseudowire       SW -- switchover

  Bridge group: default
    Bridge domain: BD-TEST, state: up
      MAC learning: enabled
      Local switching: enabled
      Flood replication point: ingress
      Flooding Multicast: all
        Unknown unicast: enabled
      MAC aging time: 300 s, MAC limit: 4000, Action: all, MTU: 1500
      Oper-status: up
      ACs: 1 (1 up)
      PWs: 1 (1 up)
      Routed interface: none

      List of ACs:

        AC: Tengigabitethernet0/0/17.341
          AC binding status: up, Interface oper state: up

      List of PWs:

        PW: Neighbor 10.0.19.1, pw-id 123, admin Up, oper Up
        Status codes:
          PW class: pwclass01, type: ethernet, signaling: pseudowire-id-fec-signaling
          PSN type: mpls, encapsulation: MPLS, control word: control-word-not-present
          Redundancy state active
          Vpn index: 1, type: ls
          Created: 2023-01-19 13:31:07, last state change: 02h20m40s ago

                                              Local                     Remote
          Label                               19                        37
          Group ID                            0                         0
          MTU                                 1500                      1500
          Forwarding                          true                      true
          Customer-facing (ingress) recv fault    false                 false
          Customer-facing (egress) send fault     false                 false
          Local PSN-facing (ingress) recv fault   false                 false
          Local PSN-facing (egress) send fault    false                 false
          Switchover                          false                     false
          Interface description string rcv: none
          Remote capabilities:
            VC status can be signaled: true
```

```
            VCCV ID can be signaled  : true
          Remote node capability:
            Manually set PW: false
            Protocol has not yet finished cap. determination: false
            Signaling the pseudowire: true
            Sending the pseudowire: false

      List of VFIs:

      List of Autodiscovery PWs:

0/ME5100:ER05#
```

Пример. Просмотр изученных MAC-адресов в VPLS-сервисе

```
0/ME5100:ER05# show l2vpn mac-table bridge-domain BD-TEST
Thu Jan 19 17:15:18 2023
  MAC address        Type     Learned from        LC/location     Bridge-domain name
  ------------------ -------- ------------------  ------------    ------------------
  00:12:1e:24:64:1f  Dynamic  pw 10.0.19.1 123    0/0             BD-TEST
  00:25:9e:b2:2b:57  Dynamic  te0/0/17.341        0/0             BD-TEST

  Total entries: 2
0/ME5100:ER05#
```

Настройка MPLS TE Autobandwidth

В подразделе "Резервирование полосы пропускания для RSVP LSP" мы уже настраивали TE-туннели так, чтобы для их RSVP LSP резервировалась полоса пропускания на исходящих интерфейсах, через которые они проходят. Однако, такое требование полосы статично зависит от конфигурации TE-туннеля. Учитывая тот факт, что резервирование полосы пропускания осуществляется в Control-Plane и никак не влияет на Forwarding-Plane, становится очевидно, что реальный пользовательский трафик в определенный момент времени может очень сильно отличаться от той полосы пропускания TE-туннеля, которая была указана в конфигурации устройства. В результате этого такое "слепое" резервирование ресурсов перестает адекватно отражать реальную картину требований к ресурсам, предоставляемым сетью для трафика соответствующих туннелей.

Для выхода из этой ситуации была разработана технология автоматической коррекции полосы пропускания (RSVP-TE Autobandwidth), суть которой в периодическом измерении загруженности TE-туннеля и последующих попытках сигнализировать уже измеренную (актуальную или требуемую) полосу пропускания.

Технология RSVP-TE Autobandwidth не является универсальной; на одних профилях трафика она работает хорошо, а на других — менее оптимально. Тем не менее она получила широкое распространение на практике, так как статическое резервирование полосы пропускания не является достаточно гибким методом.

Сначала дадим определение понятий, которыми будем оперировать далее:

- **Make Before Break** — основополагающий принцип работы RSVP-TE. "Прежде чем разрушить старый LSP, построй новый". Этот принцип реализуется в таких сценариях, как MPLS TE Fast Reroute, MPLS TE Soft Preemption, а также MPLS TE Autobandwidth, о котором и пойдёт речь.
- **Adjust interval** — временной интервал, по истечении которого принимается решение о сигнализации нового LSP для RSVP-TE туннеля с актуальными требованиями к резервированию полосы пропускания.
- **Sample interval** — временной интервал, по истечении которого Ingress LSR производит измерение текущего значения скорости, передаваемого через RSVP-TE туннель трафика. Неконфигурируемый параметр, равный 60 секунд.
- **Requested bandwidth** — величина полосы пропускания, которую измерил Ingrss LSR за **Adjust** интервал и указал как желаемую для резерва полосу пропускания для "нового"" RSVP LSP.
- **Signaled bandwidth** — величина полосы пропускания, которую удалось успешно просигнализировать от Ingress LSR (Head-End) до Egress LSR (Tail-End) для текущего LSP рассматриваемого RSVP-TE туннеля.
- **Adjust-threshold** — порог срабатывания автоматической коррекции полосы пропускания. Определяет степень абсолютного (Kbit/s, Mbit/s, Gbit/s) или относительного (%) отличия Requested bandwidth от Signaled bandwidth, при котором происходит сигнализация нового LSP для RSVP-TE туннеля с уже актуализированными требованиями к резервированию полосы пропускания.
- **Maximum bandwith** — максимальное значение полосы пропускания, которое разрешено просигнализировано для LSP RSVP-TE туннеля.
- **Minimum bandwith** — минимальное значение полосы пропускания, которое разрешено просигнализировано для LSP RSVP-TE туннеля.

Если по всему пути следования RSVP LSP на исходящих интерфейсах маршрутизаторов есть достаточное кол-во свободной полосы пропускания, то *Requested* и *Signaled bandwidth* будут равны. Если требуемой полосы пропускания на каких-то интерфейсах не окажется, то *Requested* и *Signaled* будут различаться. Принцип *"Make Before Break"* определяет, что старый LSP с *Signaled*-полосой входящий (Ingress) LSR не демонтирует до тех пор, пока успешно не построится новый LSP с *Requested*-полосой. В этом случае *Requested* и *Signaled* будут различаться. Если новый LSP будет успешно построен, то затем старый LSP будет демонтирован и параметры *Signaled* и *Requested* станут одинаковыми.

Покажем конфигурацию MPLS TE Autobandwidth на конкретном примере:

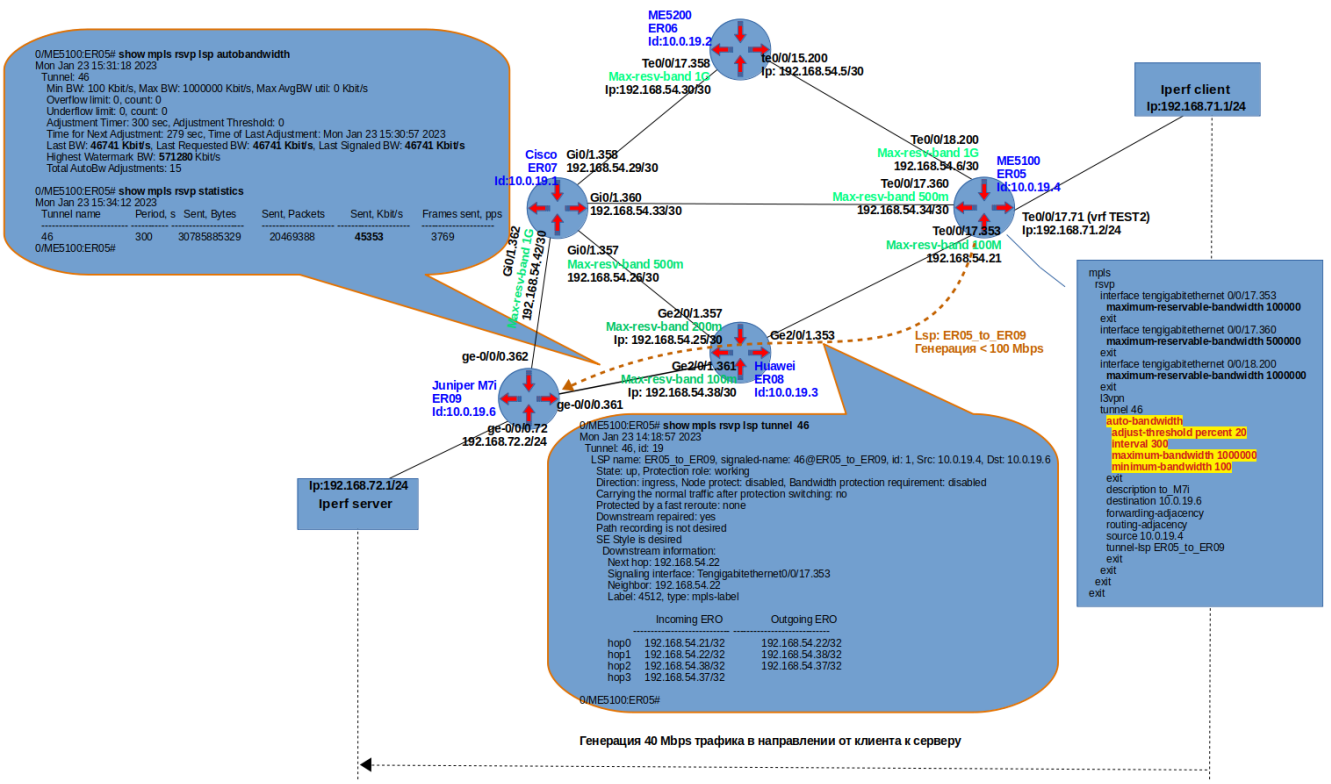


Figure 9. Начальное положение RSVP LSP 46@ER05_to_ER09 при генерации трафика до 100 Mbps.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`mpls rsvp`	Переход в режим настройки протокола RSVP.
`interface te0/0/17.353`	Включение протокола RSVP на интерфейсе te0/0/17.353.
`maximum-reservable-bandwidth 100000`	В режиме конфигурации RSVP параметров интерфейса, устанавливаем максимально возможную для резервирования полосу пропускания (в килобитах в секунду) - 100 Mbps
`exit`	Возврат в режим конфигурации RSVP протокола.
`interface te0/0/17.360`	Включение протокола RSVP на интерфейсе te0/0/17.360.
`maximum-reservable-bandwidth 500000`	В режиме конфигурации RSVP параметров интерфейса, устанавливаем максимально возможную для резервирования полосу пропускания - 500 Mbps
`exit`	Возврат в режим конфигурации RSVP протокола.
`interface te0/0/18.200`	Включение протокола RSVP на интерфейсе te0/0/18.200.
`maximum-reservable-bandwidth 1000000`	В режиме конфигурации RSVP параметров интерфейса, устанавливаем максимально возможную для резервирования полосу пропускания - 1 Gbps
`exit`	Возврат в режим конфигурации RSVP протокола.
`tunnel 46`	Создаем TE-туннель с именем 46 и переходим в режим его конфигурации.

Команда	Назначение
`auto-bandwidth`	Активируем функционал autobandwidth на данном TE-туннеле
`adjust-threshold percent 20`	Указываем относительный порог срабатывания триггера сигнализации нового резерва полосы пропускания в виде 20%
`interval 300`	Указываем Adjust интервал в виде 300 секунд, в течение которого каждые 60 секунд будет проводиться измерение (сэмплирование) передаваемого через TE-туннель трафика
`maximum-bandwidth 1000000`	Указываем максимальное значение резервируемой полосы пропускания которую может запросить TE-туннель - 1Gbps
`minimum-bandwidth 100`	Указываем минимальное значение резервируемой полосы пропускания которую может запросить TE-туннель - 100 kbps
`exit`	Возврат в режим конфигурации TE-туннеля.
`description to_M7i`	Текстовое описание TE-туннеля для облегчения понимания конфигурации.
`destination 10.0.19.6`	Команда указывает на LSR-ID Egress маршрутизатора. В нашем примере это ER09 (Juniper M7i).
`forwarding-adjacency`	Команда устанавливает атрибут возможности передачи сервисного трафика через RSVP LSP TE-туннеля. **IMPORTANT** Данная команда обязательна для включения возможности передачи трафика через TE-туннели.
`routing-adjacency`	Команда устанавливает признак TE-туннеля как интерфейса, через который можно получать маршрутную информацию.
`source 10.0.19.4`	Команда устанавливает LSR-ID Ingress-маршрутизатора в качестве источника TE-туннеля.
`tunnel-lsp ER05_to_ER09`	Создаем RSVP LSP с сигнальным именем 'ER05_to_ER09' и переходим в режим его конфигурирования. **IMPORTANT** Поскольку использовать какие-то настройки, отличные от настроек по умолчанию, мы в данном случае не будем, то никаких дополнительных команд в режиме конфигурации tunnel-lsp более не требуется.

Команда	Назначение
`root`	Возврат в режим Global Config
`system tunnel-statistic`	Включаем сбор статистики на TE-туннелях **IMPORTANT** Команда отрицательно влияет на сбор статистики через service-policy output <policy-map name> statistics.
`system tunnel-utilization`	Включаем отображение загрузки TE-туннелей трафиком
`commit`	Применение произведенных настроек.

Из конфигурации TE-туннеля 46 видно, что для него активирован функционал autobandwidth со следующими параметрами:

- **interval 300** — *Adjust*-интервал 300 секунд. В течение этого времени Ingress LSR будет каждые 60 секунд (*Sample interval*) измерять трафик, проходящий через TE-туннель 46 и сохранять максимальное значение из измеренных за интервал.
- **adjust-threshold percent 20** — порог срабатывания 20% от успешно сигнализированной полосы пропускания. Т.е. если на текущем *Adjust*-интервале максимальное из измеренных значений трафика будет отличаться от успешно сигнализированной полосы пропускания на 20%, то будет предпринята попытка просигнализировать новую полосу пропускания для TE-туннеля;
- **maximum-bandwidth 1000000** — максимальное значение резервируемой полосы пропускания, которую может запросить TE-туннель — 1Gbps;
- **minimum-bandwidth 100** — минимальное значение полосы пропускания, которую может запросить TE-туннель — 100kbps.

Что произойдёт, если передаваемый через данный TE-туннель трафик увеличится с 45 Mbps до 150 Mbps? Ingress LSR детектирует этот факт и по истечении *Adjust*-интервала будет выполнена попытка построить новый RSVP LSP для TE-туннеля 46, но уже с удовлетворением резерва для полосы пропускания 150 Mbps. Если посмотреть на рисунок, приведённый ниже, то видно, что интерфейс te0/0/17.353 (на ER05) не сможет удовлетворить такому требованию, поскольку на нем *max-resv-band* равен только 100 Mbps. В результате этого процесс CSPF на ER05 исключит из поиска оптимального пути для нового RSVP LSP этот интерфейс. Ниже приведен пример того, как перестроится RSVP LSP на лабораторном стенде при таком увеличении трафика.

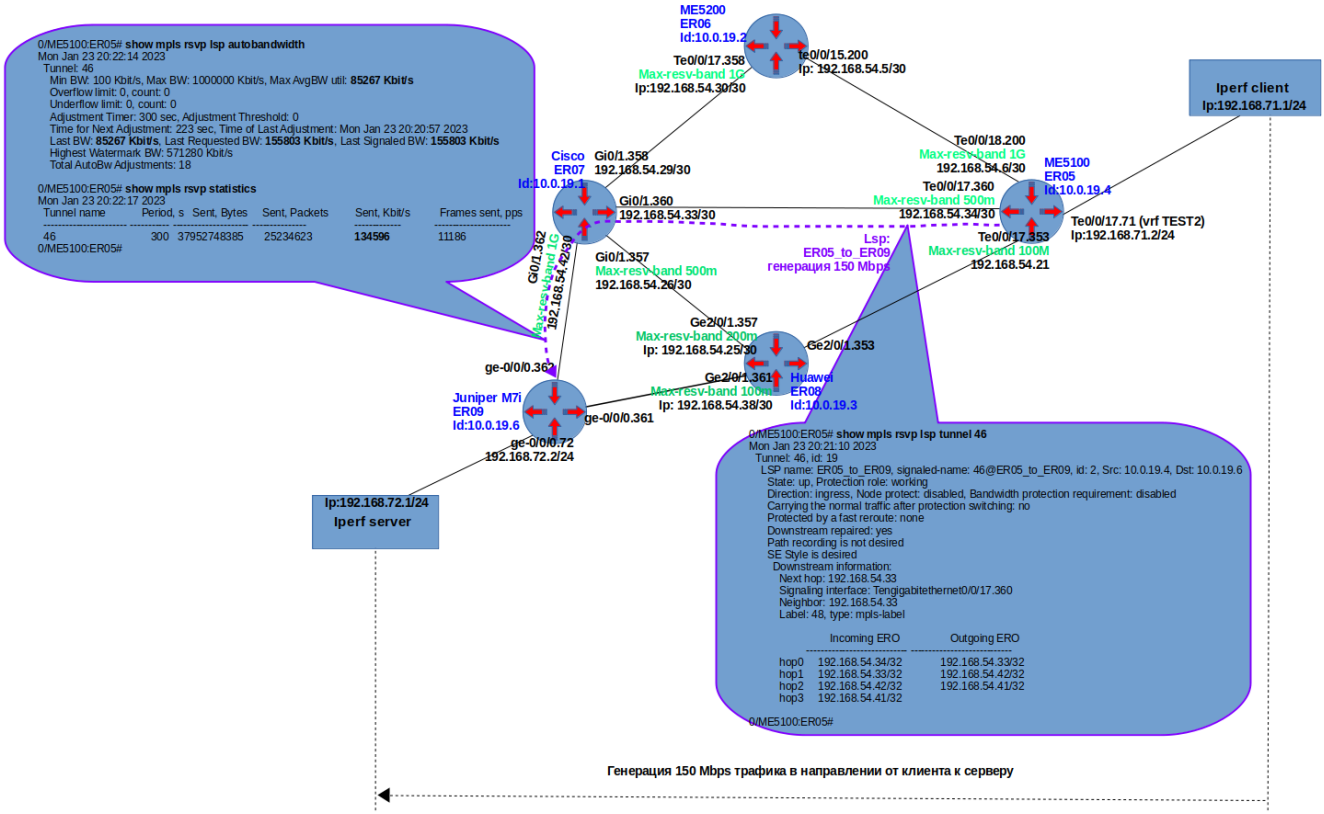


Figure 10. Как построится RSVP LSP 46@ER05_to_ER09 при генерации трафика 150 Mbps.

Пример. Нескольких команд полезных при анализе работы Autobandwidth

```
0/ME5100:ER05# show mpls rsvp lsps autobandwidth
Mon Jan 23 20:22:14 2023
  Tunnel: 46
    Min BW: 100 Kbit/s, Max BW: 1000000 Kbit/s, Max AvgBW util: 85267 Kbit/s
    Overflow limit: 0, count: 0
    Underflow limit: 0, count: 0
    Adjustment Timer: 300 sec, Adjustment Threshold: 0
    Time for Next Adjustment: 223 sec, Time of Last Adjustment: Mon Jan 23 20:20:57
2023
    Last BW: 85267 Kbit/s, Last Requested BW: 155803 Kbit/s, Last Signaled BW: 155803
Kbit/s
    Highest Watermark BW: 571280 Kbit/s
    Total AutoBw Adjustments: 18

0/ME5100:ER05#
```

Пояснения некоторым параметрам в выводе команды **show mpls rsvp lsps autobandwidth**:

- **Min BW** — минимальная полоса пропускания, которую может попытаться зарезервировать туннель;
- **Max BW** — максимальная полоса пропускания, которую может попытаться зарезервировать туннель;
- **Max AvgBW util** — максимальное значение передаваемого трафика за текущий *Adjustment interval*, будет использовано по истечению *Adjustment Timer* и сброшено в 0;

- **Overflow limit** — отключен, так как равен нулю;
- **Underflow limit** — отключен, так как равен нулю;
- **Adjustment Timer** — временной интервал, в течение которого будет приниматься решение о сигнализации RSVP LSP с новыми требованиями по резервированию полосы пропускания;
- **Adjustment Threshold** — значение, на которое должен отличаться измеренный трафик, передаваемый через TE-туннель, от успешно сигнализированной полосы пропускания, чтобы инициировать сигнализацию с новым значением резерва;
- **Time for Next Adjustment** — оставшееся время до истечения *Adjust*-интервала;
- **Time of Last Adjustment** — дата, когда происходило успешное изменение резервируемой полосы пропускания для туннеля;
- **Last BW** — последнее измеренное значение трафика через TE-туннель. Трафик измеряется через неконфигурируемые *Sampling*-интервалы. На маршрутизаторах ME они равны 60 секундам;
- **Last Requested BW** — последняя запрошенная полоса пропускания для TE-туннеля;
- **Last Signaled BW** — последняя успешно сигнализированная полоса пропускания для TE-туннеля. Если этот параметр равен *Last Requested BW*, значит ресурсов по полосе пропускания у сети хватило для TE-туннеля;
- **Highest Watermark BW** — максимальный трафик, измеренный за все время существования туннеля (с момента конфигурации autobandwidth на нем);
- **Total AutoBw Adjustments** — кол-во срабатываний технологии autobandwidth на TE-туннеле (с момента конфигурации autobandwidth на нем).

```
0/ME5100:ER05# show mpls rsvp statistics
Mon Jan 23 20:22:17 2023
  Tunnel name  Period, s   Sent, Bytes   Sent, Packets   Sent, Kbit/s  Frames sent,pps
  ------------ ---------- ------------- --------------- ------------- --------------
  46            300         37952748385   25234623        134596        11186
0/ME5100:ER05# show mpls rsvp interfaces
Mon Jan 23 20:26:19 2023
  Interface      Max resv BW     Available BW    Hello  SRefresh  Auth  BFD  TE metric
  -------------- ------------ --------------- ------ --------- ----- ----- -----------
  te0/0/17.353   100.00 Mbps     100.00 Mbps     Yes    No        No    No    5
  te0/0/17.360   500.00 Mbps     344.19 Mbps     Yes    No        No    No    10
  te0/0/18.200   1000.00 Mbps    1000.00 Mbps    Yes    No        No    No    10

0/ME5100:ER05#
```

Рассмотрим изменения, вызванные увеличением передаваемого трафика через TE-туннель 46 с 150 Mbps до 550 Mbps. Ingress LSR детектирует этот факт и по истечении *Adjust* -интервала будет выполнена попытка построить новый RSVP LSP, но уже с удовлетворением резерва полосы пропускания 550 Mbps. Если посмотреть на рисунок, приведённый выше, то видно, что единственный вариант для ER05 построить RSVP LSP, удовлетворяющий требованию резерва в 550 Mbps — это использовать интерфейс te0/0/18.200. Ниже приведен

пример того, как перестроится RSVP LSP на лабораторном стенде при увеличении трафика до 550 Mbps.

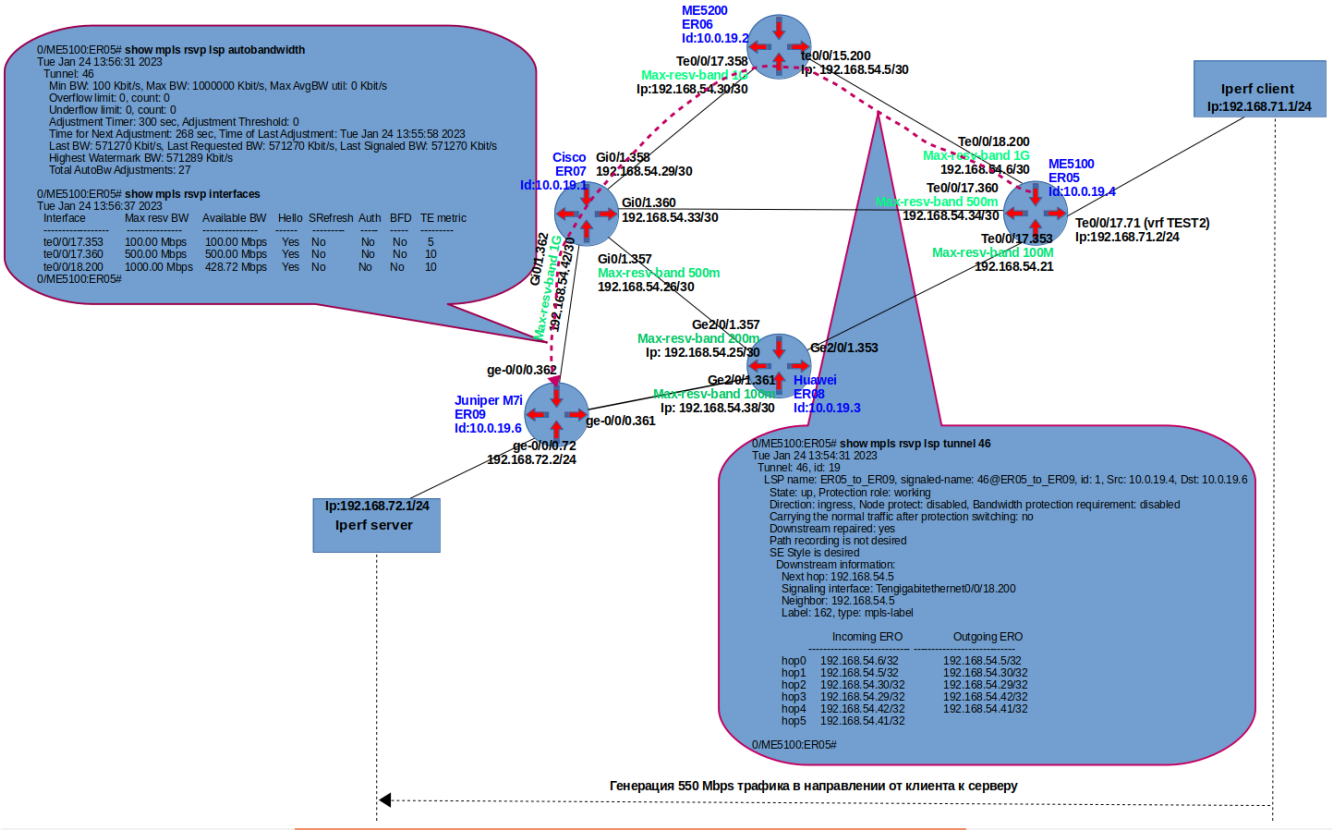


Figure 11. Как построится RSVP LSP 46@ER05_to_ER09 при генерации трафика 550 Mbps.

Overflow- и *Underflow*-лимиты и зачем они нужны.

На лабораторном стенде, который был использован в качестве демонстрации работы Autobandwidth, можно установить минимально возможный *Adjust*-интервал в 300 секунд, и тогда может показаться, что это обеспечит достаточно оперативное реагирование на изменения передаваемого трафика. На реальной сети такое значение будет вызывать слишком частые перестроения RSVP LSP, которые приведут к излишней нагрузке на устройства сети. Конкретные значения *Adjust*-интервала выбираются специалистами по дизайну сетей после её детального анализа. Обычно это значение выбирается значительно большим, чем 300 секунд, и в этом случае при определённых профилях трафика срабатывания функционала autobandwidth будут регулярно запаздывать и не соответствовать актуальному трафику.

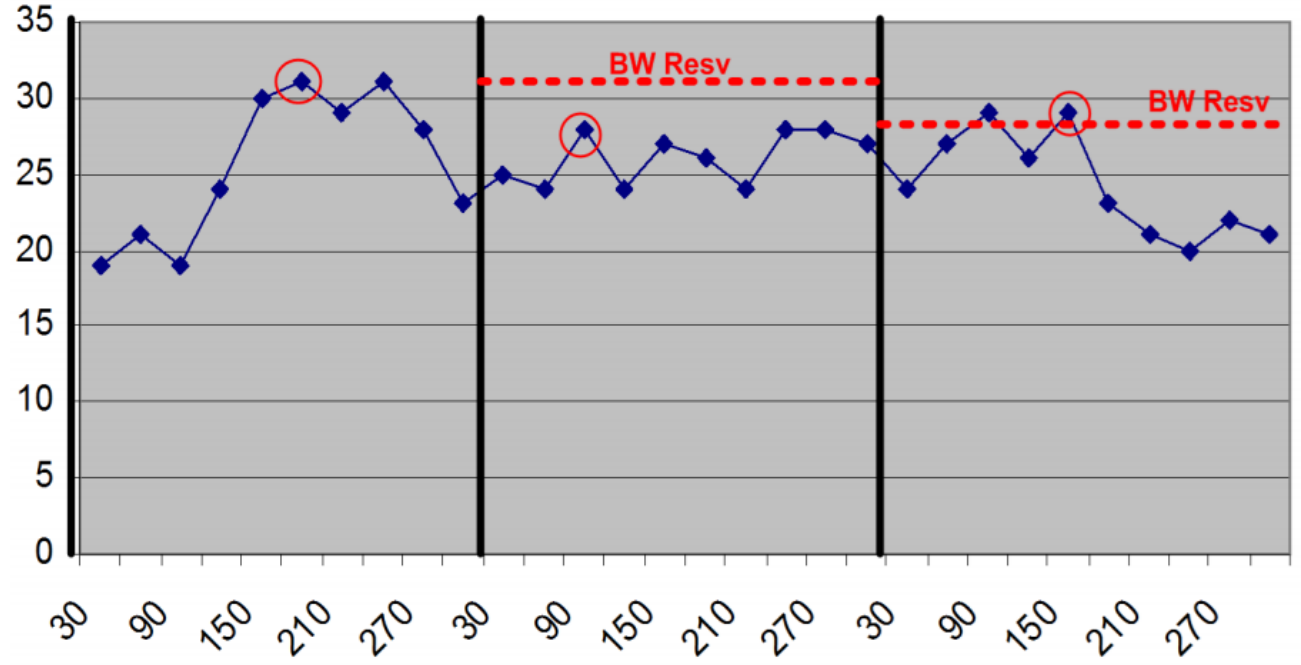


Figure 12. Пример профиля трафика и Adjust интервала в 300 секунд когда функционал работает хорошо.

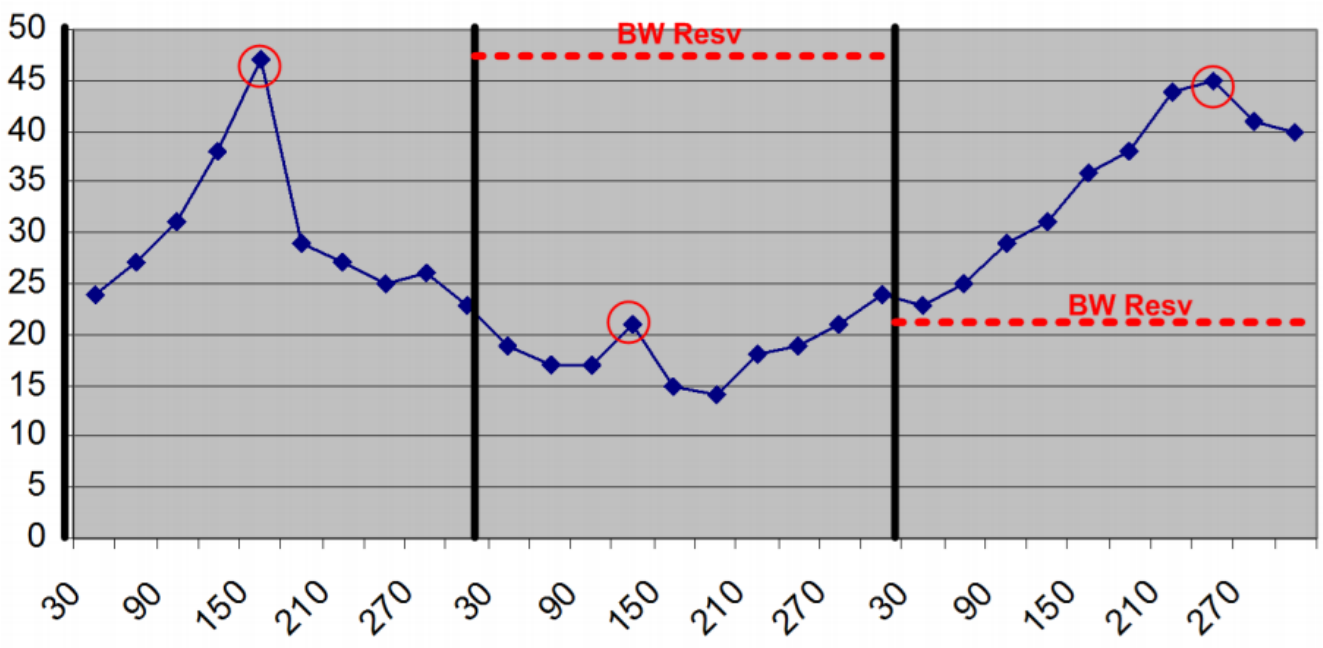


Figure 13. Пример профиля трафика и Adjust интервала в 300 секунд когда функционал работает плохо.

Как видно из Рисунка выше, профиль трафика может быть таким, что максимальное из измеренных значений на предыдущем *Adjust*-интервале плохо соответствует значениям трафика на следующем *Adjust*-интервале, в результате чего резервирование ресурсов будет неадекватным.

Для уменьшения влияния этого эффекта можно активировать дополнительные условия, при которых *Adjust*-интервал считается истекшим:

- **overflow limit N** — где N - это число следующих подряд sample-измерений трафика, значения каждого из которых превышает значение Signalled bandwidth на величину adjust threshold, необходимое для обнуления таймера Adjust-interval и досрочного

запуска механизма сигнализации нового LSP с актуализированными требованиями к резервированию полосы пропускания;

- **underflow limit N** — где N - это число следующих подряд sample-измерений трафика, значения каждого из которых меньше значения Signalled bandwidth на величину adjust threshold, необходимое для обнуления таймера Adjust-interval и досрочного запуска механизма сигнализации нового LSP с актуализированными требованиями к резервированию полосы пропускания.

Таким образом, механизм использования *overflow*- и *underflow*-лимитов позволяет сделать подстройку полосы пропускания на туннеле более точной с сохранением достаточно больших значений *Adjust*-интервала.

НАСТРОЙКА EVPN

В данной главе рассматриваются принципы организации и настройки виртуальных частных сетей второго уровня (Layer 2 VPN, L2VPN), использующих EVPN в качестве способа распространения маршрутной информации.

IMPORTANT	Определения и базовая настройка сервисов L2VPN рассмотрены в главе "НАСТРОЙКА MPLS L2VPN". Определения и настройка протокола BGP рассмотрены в главе "НАСТРОЙКА ПРОТОКОЛА BGP".

Составные элементы EVPN

- **Экземпляр EVPN** (*EVPN instance*) — уникальная сущность в конфигурации устройства для использования в связке с бридж-доменом. Определяет, с какими Route-target будут распространяться и приниматься маршруты (import/export) для последующей установки в данном бридж-домене. Также предполагается настройка route distinguisher и типа транспорта — MPLS или VXLAN.
- **Маршруты EVPN** — маршрутная информация BGP, распространяющаяся с AFI/SAFI 25/70;
- **EVPN бридж-домен** — бридж-домен типа EVPN-MPLS или EVPN-VXLAN.

Настройка бридж-доменов

Для организации L2VPN-сервиса с использованием бридж-домена с типом EVPN или VXLAN необходимо настроить на устройстве сам бридж-домен, создать требуемые AC, и добавить требуемый экземпляр EVPN. В случае использования VXLAN-туннеля необходимо добавить номер VNI в бридж-домен.

Таким образом, настройка выполняется в три этапа:

- Создание и настройка экземпляра EVPN;
- Создание и привязка бридж-домена к экземпляру EVPN, назначение VNI в случае использования VXLAN;
- Настройка протокола BGP для работы с EVPN.

Таблица 78. Порядок настройки экземпляра EVPN.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`evpn`	Переход в режим конфигурации EVPN.
`vxlan source-ip` *IPv4*	Настройка адреса источника для поднятия VXLAN-туннеля, в случае, если экземпляр EVPN имеет VXLAN-инкапсуляцию.

Команда	Назначение
`instance` *NAME*	Создание экземпляра EVPN и переход в режим его настройки.
`mpls`	Задание типа инкапсуляции MPLS для бриджей типа EVPN-MPLS.
`vxlan`	Задание типа инкапсуляции VXLAN для бриджей типа EVPN-VXLAN.
`rd` *RD*	Задание route distinguisher, если он должен отличаться от автоматически назначенного (вида "{router-id-ip}:0").
`import route-target` *RT*	Разрешить импортировать маршруты указанного route-target в данный экземпляр EVPN.
`export route-target` *RT*	Разрешить экспортировать маршруты указанного route-target из данного экземпляра EVPN.
`exit`	Возврат в режим настройки экземпляра EVPN.
`static-type2-routes` {`static-mac-ip` *MAC IP INTF* | `static-mac` *MAC INTF* }	Создание статического маршрута типа mac-ip-interface или mac-interface.
`exit`	Возврат в режим настройки экземпляра EVPN.
`commit`	Применение произведенных настроек.

Таблица 79. Порядок настройки бридж-домена.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`l2vpn`	Переход в режим настройки l2vpn.
`bridge-domain` *NAME*	Создание бридж-домена и переход в режим его настройки.
`interface` *NAME*	Добавление интерфейса локальной коммутации (AC).
`exit`	Возврат в режим настройки бридж-домена.
`evi` *NAME*	Привязка экземпляра EVPN к данному бридж-домену.
`vxlan-config` *NAME*	Переход в режим настройки VXLAN (для типа EVPN-VXLAN).
`vni` *ID*	Задание VXLAN Network Identifier (для типа EVPN-VXLAN).
`commit`	Применение произведенных настроек.

Пример настройки бридж-домена типа evpn-mpls.

```
evpn
  instance test
    export route-target 5:5
```

```
    import route-target 5:5
    mpls
  exit
exit

l2vpn
  bridge-domain test_evpn
    interface tengigabitethernet 0/8/4.2000
    exit
    evi test
  exit
exit

router bgp 65534
  bgp router-id 10.0.0.26
  neighbor 10.0.0.134
    address-family l2vpn evpn
    exit
    remote-as 65534
    send-community-ext
  exit
exit
```

Пример настройки бридж-домена типа evpn-vxlan.

```
evpn
  instance test
    export route-target 5:5
    import route-target 5:5
    vxlan
  exit
  vxlan source-ip 10.0.1.26
exit

l2vpn
  bridge-domain test_evpn
    interface tengigabitethernet 0/8/4.2000
    exit
    evi test
    vxlan-config
      vni 1
    exit
  exit
exit

router bgp 65534
  bgp router-id 10.0.0.26
  neighbor 10.0.0.134
    address-family l2vpn evpn
    exit
```

```
    remote-as 65534
    send-community-ext
  exit
exit
```

Проверка работы EVPN

show evpn

Команда выводит краткую информацию об экземпляре EVPN

Пример. show evpn

```
0/FMC0:example_router01# show evpn instance test

  EVPN instance: test, evi: 1073741824
    Oper-status: up, reason: none
    RD: 10.0.0.26:0, AUTO RT: none (none)
    RT:
      5:5 (both)
    Bridge-domain:
      Oper-status: up, reason: none
      MAC aging-time: 300, limit: 4000
      VXLAN network identifier: none
      Interfaces:
        Tengigabitethernet0/8/4.2000 Oper-status: up, reason: none
```

show bgp l2vpn evpn

Команда выводит полученные и анонсируемые маршруты EVPN

Пример. show bgp l2vpn evpn

```
0/FMC0:example_router01# show bgp l2vpn evpn
  BGP router identifier 10.0.0.26, local AS number 65534
  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

  Network                  Next hop         Metric  LocPrf  Weight  Path
  ------------------------ ---------------- ------- ------- ------- -----
  u>   [2][10.0.0.26:0][00:00:00:00:00:00:00:00:00:00][0][00:e1:a7:d0:06:40][50]
                                            0       100     0       ?
  u>i  [2][10.0.0.134:0][00:00:00:00:00:00:00:00:00:00][0][00:e8:67:d0:06:40][43]
                           10.0.0.134       0       100     0       ?
```

```
  u>   [3][10.0.0.26:0][0][10.0.0.26]
                                       0       100     0       ?
  u>i  [3][10.0.0.134:0][0][10.0.0.134]
                          10.0.0.134       0       100     0       ?

  Total entries: 4
```

show l2vpn mac-table all

Команда отобразит изученные MAC-адреса в бридже.

Пример. show l2vpn mac-table all

```
0/FMC0:example_router01# show l2vpn mac-table all
  MAC address        Type     Learned from                              Bridge-domain
name
  ------------------ -------- ----------------------------------------
------------------
  00:e1:a7:d0:06:40  Dynamic  te0/8/4.2000                              test_evpn
  00:e8:67:d0:06:40  Evpn     evi 10.0.0.134 label 43                   test_evpn
```

show evpn mac-ip-table

Команда отобразит текущие маршруты по каждому экземпляру EVPN

Пример. show evpn mac-ip-table

```
0/FMC0:example_router01# show evpn mac-ip-table

  EVPN instance: test, evi: 1073741824
  IP address                          MAC address        Ethernet tag  ESI
  ----------------------------------- ------------------ ------------ ----
  200.0.0.135                         00:00:00:11:11:11  0
00:00:00:00:00:00:00:00:00:00
                                      00:e1:a7:d0:06:40  0
00:00:00:00:00:00:00:00:00:00
                                      00:e8:67:d0:06:40  0
00:00:00:00:00:00:00:00:00:00
```

show evpn vxlan-tunnel

Команда отобразит установленные VXLAN-туннели

Пример. show evpn vxlan-tunnel

```
0/FMC0:example_router01# show evpn vxlan-tunnel
  Source               Peer                       VNI         Oper Status  EVI
VRF
  -------------------- -------------------------- ----------- ------------
```

```
-------------------------- ----
  10.0.1.26             10.0.1.134               1:1         up           test
(1073741824)
```

МНОГОАДРЕСНАЯ РАССЫЛКА ТРАФИКА (MULTICAST)

В главе рассматриваются протоколы, позволяющие Устройству принимать, обрабатывать и пропускать multicast-трафик, а также схемы применения. Устройство поддерживает протоколы IGMP, PIM и MSDP.

Адресные листы для multicast-протоколов

Адресные листы подобны access-листам; используются для указания действия по отношению к каждому элементу списка, созданного на основе определенного признака и порядкового номера элемента в списке. Признаки, на основе которых формируются эти списки, привязаны к определённым командам multicast-протоколов. Для списка `address-list` признаком является пересечение подсети с адресом группы. Для списка `group-list` признаком является пересечение подсети с адресом группы или в подсети с адресом запрашиваемого источника.

Настройка address-list

Таблица 80. Порядок настройки address-list

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`multicast address-list WORD`	Создание списка адресов с именем WORD и переход в режим его настройки.
`seq-num 1`	Создание элемента в списке и переход в режим его настройки. Для списка обязательно наличие хотя бы одного элемента.
`match address PREFIX`	Указание префикса, для которого применяется данное правило. Отсутствие префикса в элементе означает совпадение по любому адресу.
`action permit|deny`	Указание типа действия: отклонить или подтвердить. По умолчанию: `permit`.
`exit`	Возврат в режим конфигурации `multicast address-list`.
`commit`	Применение произведенных настроек.

Пример настройки address-list

```
multicast address-list no-239
  seq-num 1
    match address 224.0.0.0/4
  exit
  seq-num 2
    match address 239.0.0.0/16
```

```
    action deny
  exit
exit
```

Проверка применённых списков адресов:

show multicast address-list

Вывод сконфигурированных списков адресов. Пример:

```
0/ME5100:Router# show multicast address-list
  address-list cde
    1 permit 232.0.0.0/8
    2 permit 239.0.0.0/8

  address-list test
    1 permit 232.1.1.1/32
```

Настройка group-list

Таблица 81. Порядок настройки group-list

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`multicast address-list WORD`	Создание списка адресов с именем WORD и переход в режим его настройки.
`seq-num 1`	Создание элемента в списке и переход в режим его настройки. Для списка обязательно наличие хотя бы одного элемента.
`match group PREFIX/MASK |ADDRLIST`	Указание префикса группы, для которого применяется данное правило. Отсутствие префикса в элементе означает совпадение по любому адресу. Разрешено указание имени address-list в качестве признака.
`match source PREFIX/MASK |ADDRLIST`	Указание префикса источника, для которого применяется данное правило. Отсутствие префикса в элементе означает совпадение по любому адресу. Разрешено указание имени address-list в качестве признака.
`action permit|deny`	Указание типа действия: отклонить или подтвердить. По умолчанию: `permit`.
`exit`	Возврат в режим конфигурации `multicast group-list`.
`commit`	Применение произведенных настроек.

Пример настройки group-list

```
multicast group-list s101
  seq-num 1
    match group 225.54.205.0/24
    match source 46.61.193.86/32
  exit
  seq-num 2
    match group 224.0.0.0/4
    match source 46.61.193.0/24
    action deny
  exit
exit
```

Проверка применённых списков адресов:

show multicast group-list

Вывод сконфигурированных списков групп. Пример:

```
0/ME5100:Router# show multicast group-list
  group-list cde
    1 permit group cde

  group-list s101
    1 permit source 46.61.193.101/32
    2 deny source 46.61.193.102/32
```

Протокол IGMP

Протокол служит для составления соответствия интерфейсов-получателей multicast-трафика ("подписчиков") и групп (или группа-источник), на которые интерфейс подписан. Информация, при наличии надлежаще настроенного PIM-процесса, переносится в PIM-топологию в виде (S,G) или (*,G)-записей. Настройка протокола выполняется в секции `router igmp`. Реализация протоколов выполнена в соответствии с RFC 2236 и RFC 3376.

Существует ряд функциональных особенностей:

- Нет поддержки проксирования IGMP-запросов;
- Реализован функционал IGMP Querier: поддержан обмен сообщениями между несколькими Querier в широковещательном сегменте и обмен сообщениями с получателями трафика. Работа в нескольких режимах одновременно (v2-v3) не поддержана.

Порядок настройки IGMP

1. Выполнить предварительную настройку;

2. При необходимости, изменить протокольные настройки на интерфейсах, выставленные по умолчанию;
3. При необходимости, добавить обработку ssm.

Предварительная настройка IGMP

Работа IGMP возможна только на L3-интерфейсах. Таким образом, на интерфейсах, выбранных для работы в качестве IGMP-Querier, необходимо задать ip-адрес:

```
interface tengigabitethernet 0/0/7.10
  description "Multicast receivers 1"
  ipv4 address 192.168.10.1/24
exit
interface tengigabitethernet 0/0/7.400
  description "Multicast receivers 2"
  ipv4 address 192.168.100.1/24
exit
```

Настройка протокола IGMP

Таблица 82. Порядок настройки IGMP

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`router igmp`	Создание IGMP процесса и переход в режим его настройки.
`vrf WORD`	(Опционально) Запуск IGMP-процесса в указанном VRF и переход в режим настройки этого процесса. Нижеследующие команды применимы для процесса внутри global table и внутри специфичного vrf.
`ssm addresses NAME`	(Опционально) Переопределение списка адресов *NAME*, считающегося SSM-диапазоном.
`ssm mapping source SRCADDR`	(Опционально) Перейти в режим настройки диапазона групп, для которого будет добавлен адреса источника *SRCADDR*.
`address-list GROUPADDR`	(Опционально) Указание диапазона групп, для которого будет добавлен адреса источника *SRCADDR*
`exit`	Возврат в режим конфигурации `router igmp`.
`interface TYPE NUM`	Включение Querier на соответствующем (саб)интерфейсе в процесс и переход в режим настройки параметров LDP для данного интерфейса.
`version NUM`	(Опционально) Указание, с какой версией выполнять отправку сообщений QUERY и обрабатывать сообщения REPORT.

`filter groups NAME`	(Опционально) Применение списка фильтрации *NAME*.
`groups-limit NUM`	(Опционально) Установка максимального количества уникальных адресов групп из всех IGMP-записей, по исчерпанию которых новые записи создаваться не будут. По умолчанию: 0, не задано.
`sources-limit NUM`	(Опционально) Установка максимального количества уникальных адресов источников из всех IGMP-записей, по исчерпанию которых, новые записи создаваться не будут. По умолчанию: 0, не задано.
`immediate-leave`	(Опционально) Удаление IGMP-записи с интерфейса при получении сообщения LEAVE без отправки GROUP SPECIFIC QUERY.
`last-member-query-interval SEC`	(Опционально) Установка таймера времени ожидания на GROUP SPECIFIC QUERY, по истечению которого будет удалена IGMP-запись.
`query-interval SEC`	(Опционально) Установка значения таймера после отправки сообщения GENERAL QUERY. По умолчанию: 125 секунд.
`query-response-interval SEC`	(Опционально) Установка значения таймера отправляемого в сообщениях GENERAL QUERY. Влияет на время, случайным образом, но в пределах которого подписчики должны отправить REPORT. И влияет на максимальный таймаут неответа на сообщения GENERAL QUERY, после которого IGMP-запись будет удалена. По умолчанию: 10 секунд.
`robustness NUM`	(Опционально) Установка значения множителя отправок сообщений GENERAL QUERY и GROUP SPECIFIC QUERY. Влияет на максимальный таймаут неответа на сообщения GENERAL QUERY, после которого IGMP-запись будет удалена. По умолчанию: 2.
`promiscuous disable`	(Опционально) Отключение обработки сообщений REPORT от подписчиков с адресов, не принадлежащих сети Querier.
`static-group GROUPADDR`	(Опционально) Создание статической IGMP-записи с указанием адреса группы и переход в режим её настройки.
`static-source SRCADDR`	(Опционально) Указание адреса источника для статической IGMP-записи.
`exit`	Возврат в режим конфигурации `router igmp interface`.
`exit`	Возврат в режим конфигурации `router igmp`.
`commit`	Применение произведенных настроек.

Пример настройки IGMP

```
router igmp
```

```
  interface tengigabitethernet 0/0/7.10
    immediate-leave
    robustness 3
    version 2
  exit
  interface tengigabitethernet 0/0/7.400
    filter groups s101
    static-group 225.54.205.140
    exit
    static-group 232.1.1.1
      static-source 77.77.77.77
    exit
    version 2
  exit
  ssm addresses ssm-addresses
  ssm mapping source 46.61.194.55
    address-list k1
  exit
exit
```

Проверка работоспособности протокола IGMP

show igmp groups

Вывод текущих групп, обработанных Querier или заданных статически. Пример:

```
0/ME5100:Router# show igmp groups
  IGMP Connected Group Membership

  Group Address            Interface               Uptime     Expires    Last
Reporter
  ------------------------ ----------------------- ---------- ----------
--------------
  225.54.205.135           te 0/0/7                00h00m42s  00h04m19s
192.168.10.100
  225.54.205.140           te 0/0/7                02h38m01s  never      0.0.0.0
  225.54.205.140           te 0/0/7.400            02h38m01s  never      0.0.0.0
  232.1.1.1                te 0/0/7.400            02h38m01s  never      0.0.0.0
```

show igmp interfaces

Вывод использующихся настроек версии, таймеров Querier и статистика принятых сообщений. Пример:

```
0/ME5100:Router# show igmp interfaces
  Tengigabitethernet 0/0/7.10 IGMP status is up
    IGMP is enabled on interface
    Drop policy: None
```

```
    Filtering multicast group-list: None
    Promiscuous mode is enabled
    Current IGMP version is 3
    Robustness is 2
    Query interval is 125 seconds
    Query timeout is 0 seconds
    Query response interval is 10 seconds
    Last member query interval is 1 seconds
    Querying router is 192.168.123.100 (this system)
    Groups/sources limit: not set/not set
```

show igmp sources

Вывод текущих групп с запрошенным источником, обработанных Querier или заданных статически. Пример:

```
0/ME5100:Router# show igmp sources

  Group Address            Source Address           Interface                Origin
codes
  ------------------------ ------------------------ ------------------------
-------------
  232.1.1.1                77.77.77.77              te 0/0/7.400             static
```

show igmp ssm map

Вывод таблицы соответствия адресов SSM-диапазона и применяемого к нему адреса источника. Пример:

```
0/ME5100:Router# show igmp ssm map

  Source Address      Address list
  ------------------- -------------
  46.61.193.101       cde
```

show igmp summary

Вывод обобщенной информации о группах на каждом включенном IGMP-интерфейсе. Пример:

```
0/ME5100:Router# show igmp summary
  IGMP summary

  Total groups on each interface: 5
  Total unique groups: 2
  Enabled Interfaces: 3
  Disabled Interfaces: 1
```

```
  Interface                Grp No  Max Grp No
  ------------------------ ------- -----------
  te0/0/7.11               1       0
  te 0/0/7                 2       1000
  te 0/0/7.10              0       0
  te 0/0/7.400             2       0
```

show igmp traffic

Вывод статистики по IGMP-сообщениям. Пример:

```
0/ME5100:Router# show igmp traffic
  IGMP Traffic Counter
    Processed messages:
      Queries:                          0
      Reports:                          239
      Leaves:                           0
     Total processed:                   239
    Filtered messages:
      Report version mismatch:          0
      Query version mismatch:           0
      Entries with limits excess:       0
      Entries with not allowed sources: 0
      Link local messages:              10
      Other reasons:                    0
     Total filtered:                    10
    Incorrect messages:
      Wrong checksum:                   0
      No router alert option:           0
      SSM messages with EXCLUDE:        0
      Other reasons:                    0
     Total incorrect:                   0

    Queries sent:                       238
```

Протокол PIM

Протокол служит для маршрутизации multicast, использует таблицу маршрутизации unicast на устройстве. Протокол предполагает установку соседств через выбранные интерфейсы и формирование топологии через проверку RPF, построение деревьев и формирование (*,G) и (S,G) записей. Реализация протоколов выполнена в соответствии с RFC 4601, RFC 3973 и RFC 3956.

Существует ряд функциональных особенностей:

- Устройство поддерживает только Sparse mode (SM) и может работать в режиме ASM и SSM;

- В текущей версии на устройстве поддержана настройка протокола BSR;
- Поддерживается Anycast-RP для повышения отказоустойчивости.

Порядок настройки PIM

1. Выполнить предварительную настройку;
2. Указать диапазоны обрабатываемых групп и режим их работы;
3. При наличии интерфейсов для построения соседств применить их в конфигурацию PIM;
4. При наличии IGMP-интерфейсов применить их в конфигурацию PIM в режиме passive;
5. При наличии интерфейса с мультикаст-потоками применить их в конфигурацию PIM в режиме passive;
6. При необходимости изменить протокольные настройки на интерфейсах, выставленные по умолчанию;
7. При необходимости изменить прочие протокольные настройки, выставленные по умолчанию.

Предварительная настройка PIM

Работа PIM основывается на таблице маршрутизации unicast и используется для RPF и построения деревьев. Таким образом, должны быть созданы ip-интерфейсы, на которых будут впоследствии включены PIM-соседства, и те, на которые придёт поток multicast. В последнем случае для создания (S,G) записей в топологии, подсеть интерфейса должна охватывать адреса источников multicast.

Пример настройки интерфейсов для организации соседств и определения потока multicast

```
interface tengigabitethernet 0/0/9
  description "Neighborhood with me5100_17_134 te 0/0/9"
  ipv4 address 100.26.134.134/24
exit
interface tengigabitethernet 0/0/1.30
  description "Obtain multicast with address 46.61.193.86"
  ipv4 address 46.61.193.134/24
  encapsulation outer-vid 30
exit
```

Настройка протокола PIM

Таблица 83. Порядок настройки PIM

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`router pim`	Создание PIM-процесса и переход в режим его настройки.

`vrf WORD`	(Опционально) Запуск PIM-процесса в указанном VRF и переход в режим настройки этого процесса. Нижеследующие команды применимы для процесса внутри global table и внутри специфичного vrf.
`address-family ipv4`	Переход в режим настройки адресного семейства IPv4.
`interface TYPE NUM`	Добавление интерфейса для обработки протоколом на устройстве и переход в режим его настройки.
`assert-override-interval SEC`	(Опционально) Задание интервала до следующей попытки отправки сообщения Assert, от последнего принятого сообщения Assert, если процесс на интерфейсе проиграл данные выборы.
`bsr-border`	(Опционально) Задание границы работы BSR. При наличии опции интерфейс перестанет отправлять и обрабатывать сообщения Bootstrap. По умолчанию интерфейс принимает и обрабатывает BSR-сообщения.
`dr-priority NUM`	(Опционально) Задание приоритета для выбора Designated router. При равных DR в домене выбирается хост со старшим адресом. По умолчанию: 1.
`hello-interval SEC`	(Опционально) Задание интервала между отправками сообщений PIM Hello с выбранного интерфейса. По умолчанию: 30 секунд.
`join-prune-interval SEC`	(Опционально) Задание интервала между отправками сообщений PIM Join/Prune с выбранного интерфейса согласно своей топологии. По умолчанию: 60 секунд.
`join-prune-holdtime SEC`	(Опционально) Задание времени удержания записей PIM Join/Prune в своей топологии. Обнуляется при получении Join/Prune на соответствующую запись. По умолчанию: 210 секунд.
`sg-state-limit NUM`	(Опционально) Задание максимального количества записей (S,G) обрабатываемых на указанном интерфейсе. По умолчанию: 0, лимита нет.
`star-g-state-limit NUM`	(Опционально) Задание максимального количества групп, для которых создаются записи (*,G, I) на указанном интерфейсе. По умолчанию: 5 секунд.
`triggered-hello-interval SEC`	(Опционально) Задание максимального значения интервала от старта процесса на интерфейсе до первой отправки PIM Hello, выбирается случайным образом от 0 до указанного значения. По умолчанию: 30 секунд.
`passive-interface`	(Опционально) Отключение создания соседства на данном интерфейсе.
`exit`	Возврат в режим конфигурации `router pim address-family ipv4`.

`keep-alive SEC`	(Опционально) Задание времени удержания записей (S,G) при отсутствии сообщений (S,G)Join. По умолчанию: 210 секунд.
`multipath group-nexthop hash|modulo`	(Опционально) Задание способа балансировки отправки PIM-сообщений между ECMP-линками.
`register probe-time SEC`	(Опционально) Задание времени ожидания сообщения Register-Stop после отправки Null-Register. По истечению стартует инкапсуляция multicast-трафика в сторону RP. По умолчанию: 5 секунд.
`register suppression-time SEC`	(Опционально) Задание максимального интервала от получения сообщения Register-Stop до прекращения инкапсуляции multicast-трафика в сторону RP. Выбирается случайным образом от 0 до указанного значения. По умолчанию: 60 секунд.
`trap interface state change`	(Опционально) Включение отправки SNMP-трапов при изменении статуса PIM-интерфейса.
`address-family ipv4`	Переход в режим настройки адресного семейства IPv4.
`static-rp PREFIX/MASK`	(Опционально) Создание диапазона групп для обработки протоколом на устройстве и переход в режим её настройки.
`pim-mode asm|ssm`	Выбор режима работы PIM для настраиваемого диапазона групп. По умолчанию: ASM.
`rp-address ADDR`	Задание адреса Rendezvous Point для настраиваемого диапазона групп, если выбран режим ASM.
`exit`	Возврат в режим конфигурации `router pim address-family ipv4`.
`bsr candidate-bsr IP-ADDR`	(Опционально) Создание экземпляра обработчика PIM bootstrap-сообщений и переход в режим его настройки.
`candidate-period NUM`	(Опционально) Задание периода отправки advertise-сообщений. По умолчанию: 60 секунд.
`hash-mask-len NUM`	(Опционально) Задание длины маски для hash-функции, используемой для выбора RP. По умолчанию: 30.
`priority NUM`	(Опционально) Указание приоритета в advertise-сообщениях. candidate-bsr выбирается по большему значению. По умолчанию: 0.
`exit`	Возврат в режим конфигурации `router pim address-family ipv4`.
`bsr candidate-rp IP-ADDR`	(Опционально) Создание экземпляра обработчика PIM CRP-сообщений и переход в режим его настройки.
`address-list WORD`	(Опционально) Задание списка адресов для анонса в CRP-сообщениях.

`hold-time NUM`	(Опционально) Задание времени сохранения RP в BSR-анонсах. По умолчанию: 150 секунд.
`interval NUM`	(Опционально) Задание интервала отправки сообщений RP Advertisement. По умолчанию: 60 секунд.
`priority NUM`	(Опционально) Указание приоритета в advertise-сообщениях. candidate-rp выбирается по меньшему значению. По умолчанию: 0.
`exit`	Возврат в режим конфигурации `router pim address-family ipv4`.
`anycast-rp ANYCAST-ADDR RP-ADDR`	(Опционально) Задание соответствия адреса RP и общего ip-адреса.
`exit`	Возврат в режим конфигурации `router pim`.
`commit`	Применение произведенных настроек.

Пример настройки PIM

```
router pim
  address-family ipv4
    static-rp 225.54.0.0/16
      rp-address 10.0.0.134
    exit
    interface tengigabitethernet 0/0/9
    exit
    interface tengigabitethernet 0/0/1.30
      passive-interface
    exit
  exit
exit
```

Проверка работоспособности протокола PIM

show pim bsr candidate-bsr

Вывод информации о победителе BSR-выборов:

```
0/ME5100:Router# show pim bsr candidate-bsr
  Address family: IPv4
    Address: 10.0.0.33
      Hash-mask: 30
      Priority: 0
      Candidate period: 60
        Elected BSR: true
        Bootstrap timer: 43 sec
```

show pim bsr candidate-rp

Вывод списка анонсируемых candidate-rp и соответствующих им address-list:

```
0/ME5100:Router# show pim bsr candidate-rp
  Address family: IPv4
  Cand-RP                 Prio  Bid  Inte  Hold-ti  Adv      Address-list
                          rity  ir   rval  me       (sec)
  ----------------------- ----- ---- ----- -------- -------- -------------
  10.0.0.26               0     no   60    150      0        test
```

show pim bsr election

Вывод информации о выборах BSR-router:

```
0/ME5100:Router# show pim bsr candidate-rp
  Address                 Prio  Hash-ma  Expiry-ti  Uptime
                          rity  sk       me
  ----------------------- ----- -------- ---------- ----------
  10.0.0.26               0     30       00h00m03s  00h06m06s
```

show pim bsr rp-cache

Вывод информации о передаваемых в BSR-сообщениях парах "RP-префикс":

```
0/ME5100:Router# show pim bsr rp-cache
  RP-Address              Prio  Holdtim  Expiry-ti  Group-prefix
                          rity  e        me
  ----------------------- ----- -------- ---------- -------------
  10.0.0.26               0     150      00h02m21s  232.0.0.0/8
  10.0.0.26               0     150      00h02m21s  239.0.0.0/8
```

show pim neighbors

Вывод текущих PIM-соседств:

```
0/ME5100:Router# show pim neighbors
  Neighbor         Interface               Uptime     Expires    BFD          DR pri
  ---------------- ----------------------- ---------- ---------- -------------
----------------
  100.99.11.111    bu1.4010                00h17m08s  00h01m36s  active       1 (DR)
  101.26.134.134   bu1.4033                00h17m15s  00h01m31s  active       1 (DR)
```

Детальный вывод о PIM-соседствах на интерфейсе:

```
0/ME5100:Router# show pim bundle-ether 1.4010
```

```
  IPv4 neighbor 100.99.11.111 at Bundle-ether1.4010
    Uptime: 00h18m19s, Expires: 00h01m25s
    BFD state is active
    DR priority is 1
    LAN prune delay options:
      Suppression is disabled
      Propagation delay is 500 msec
      Override interval is 2500 msec
```

Вывод статистики о PIM-соседстве на интерфейсе:

```
0/ME5100:Router# show pim bundle-ether 1.4010
  Bundle-ether1.4010

  Message type       Errors      Received
  -------------      ----------- -----------
  Assert             0           0
  Bootstrap          0           0
  DF election        0           0
  Graft              0           0
  Graft Ack          0           0
  Join/Prune         0           3
  State Refresh      0           0
  Hello              N/A         40
  Joined sources     N/A         0
  Pruned sources     N/A         3
```

show pim topology

Вывод текущих PIM-записей с их типами, состояниями, nexthop, rpf и списком исходящих интерфейсов. Например, вывод топологии для локального получателя с построенным SPT-деревом:

```
0/ME5100:Router# show pim topology
  IP PIM Multicast Topology Table
  Entry state: (*/S,G)[RPT/SPT] Mode, Protocol, Uptime, Info
  Interface state: Name, Uptime, Fwd, Info

    (46.61.193.86, 225.54.205.135) SPT, asm, Up: 00h00m29s
    JP: joined (00h00m30s), RPF: Tengigabitethernet 0/0/12.10, nexthop:
110.26.134.134, protocol: isis, prefix: 46.61.193.0/24
      No interfaces in immediate olist

    (46.61.193.86, 225.54.205.135) RPT not-prune, Up: 00h00m00s
      No interfaces in immediate olist

    (*, 225.54.205.135) asm, Up: 00h00m29s, RP: 10.0.0.134 is not local (config)
    JP: joined (00h00m30s), RPF: Tengigabitethernet 0/0/12.10, nexthop:
```

```
110.26.134.134, protocol: isis, prefix: 10.0.0.134/32
      te0/0/7 asm, Up: 00h00m29s is local
```

Пример вывода топологии для устройства, принимающего 2 multicast-группы:

```
0/ME5100:Router# show pim topology
  IP PIM Multicast Topology Table
  Entry state: (*/S,G)[RPT/SPT] Mode, Protocol, Uptime, Info
  Interface state: Name, Uptime, Fwd, Info

    (46.61.193.86, 225.54.205.135) SPT, asm, Up: 04h20m23s
    JP: joined (never), RPF: Tengigabitethernet 0/0/1.30, nexthop: 46.61.193.86,
protocol: local, prefix: 46.61.193.0/24
      No interfaces in immediate olist

    (46.61.193.86, 225.54.205.136) SPT, asm, Up: 04h20m23s
    JP: joined (never), RPF: Tengigabitethernet 0/0/1.30, nexthop: 46.61.193.86,
protocol: local, prefix: 46.61.193.0/24
      te0/0/9.10 asm, Up: 00h00m47s is not local
```

show pim interfaces

Вывод сконфигурированных pim-интерфейсов: их состояний, количества соседств и выбранный DR в домене.

```
0/ME5100:Router# show pim interfaces
  Address family: IPv4

  Address           Interface          Status    Nbr     (*,G)   (S,G)   DR
Designated
                                               Count   Count   Count   priority
Router
  ----------------- ------------------ --------- ------- ------- ------- -----------
---------------
  100.99.11.1       bu1.4010           up        1       0       0       1
100.99.11.111
  101.26.134.26     bu1.4033           up        1       0       0       1
101.26.134.134
  192.168.10.1      te0/0/7            up        -       0       0       1
local
```

show pim summary

Вывод обобщенной информации о записях различного типа.

```
0/ME5100:Router# show pim summary
  PIM IPv4 State Counters
```

```
    Keepalive period is 210 sec
    Register suppression time is 3 sec, probe time is 1 sec
    PIM multipath mode is highest-neighbor (disabled)
    Interface state change traps are enabled
    PIM graceful restart status is timed-out
      Backstop timer:     300 sec (0 remaining)
      Join startup timer: 60 sec (0 remaining)
    Different sources/RPs: 1/3
    Groups now/max: (*,G): 1/not set   (S,G): 1/not set
                    (*,G,I): 1/not set (S,G,I): 0/not set
```

show pim group-map

Вывод таблицы соответствия диапазонов multicast-групп, назначенной RP и способа задания соответствия.

```
0/ME5100:Router# show pim group-map
  IP PIM Group Mapping Table
  (* indicates group mappings being used)
  Group Range                Proto  Client  RP address
  -------------------------- ------ ------- ----------------
  239.0.0.0/8*               asm    config  10.0.0.26
  239.1.128.0/24*            asm    config  10.0.0.26
  225.54.205.0/24*           asm    config  10.0.0.134
  232.1.1.1/32               ssm    config  0.0.0.0
  225.0.0.0/8*               asm    bsr     10.0.0.3
  232.0.0.0/8*               ssm    config  0.0.0.0
  239.1.200.0/21*            asm    config  10.0.0.111
  ff3e::/32*                 ssm    config  ::
```

show pim summary statistics

Вывод статистики по сообщениям PIM Register различного вида.

```
0/ME5100:Router# show pim summary statistics
  PIM IPv4 statistics
    Message type        Errors      Sent        Received
    Assert              0           0           0
    Bootstrap           0           0           0
    C-RP-Advertisement  0           0           0
    DF election         0           0           0
    Graft               0           0           0
    Graft Ack           0           0           0
    Hello               0           391         97
    Join/Prune          0           91          13
    Joined sources      N/A         72          0
    Pruned sources      N/A         48          15
    S,G-updates w/MSDP  N/A         0           80
```

```
    State Refresh       0           0           0
    Register            0           0           0
    Register Stop       0           0           0
    Null Register       N/A         N/A         0
    C-RP-Adv filtered   0           N/A         N/A
    Incorrect checksum  0           N/A         N/A
    Short header        0           N/A         N/A
    Unsupported type    0           N/A         N/A
    Unknown type        0           N/A         N/A
    Unknown version     0           N/A         N/A
```

Протокол MSDP

Протокол служит для обмена информацией об имеющихся записях (S,G,RP) между соседями, находящимися в разных PIM-доменах. Устройство создаёт TCP-сессии с настроенными и доступными пирами, импортирует локальные (S,G)-записи из топологии PIM, производит рассылку согласно правилам фильтрации и MESH-модели, импортирует записи из чужих Source-Active-сообщений и инсталлирует их в локальную PIM-топологию. Реализация протоколов выполнена в соответствии с RFC 3618.

Порядок настройки MSDP

1. Обеспечить доступность адресов пиров согласно в таблице маршрутизации unicast;
2. Указать connect-source, сконфигурировать соседей и распределить их согласно MESH-модели сети;
3. При необходимости изменить прочие протокольные настройки, выставленные по умолчанию.

Предварительная настройка MSDP

Работа MSDP основывается на таблице маршрутизации unicast, используется для RPF и построения деревьев. В случае, если устройство выступает в роли получателя multicast, протокол используется для импорта записей (S,G) из топологи PIM.

Пример настройки интерфейсов для организации соседств и определения потока multicast

```
router pim
  address-family ipv4 static-rp 225.54.0.0/16
    rp-address 10.0.0.134
  exit
  address-family ipv4 interface tengigabitethernet 0/0/1.30
    passive-interface
  exit
```

Пример вывода о доступности маршрута соседа и локальных (S,G) записей.

```
0/ME5100:Router# show route 10.0.0.26
```

```
  Routing entry for 10.0.0.26/32
    Last update: N/A
    Routing Descriptor Blocks
      100.26.134.26, via te 0/0/9
      Known via isis, distance 116, metric 20
        type isis-level2-internal, protection N/A, route-type remote
0/ME5100:Router# show pim topology
  IP PIM Multicast Topology Table
  Entry state: (*/S,G)[RPT/SPT] Mode, Protocol, Uptime, Info
  Interface state: Name, Uptime, Fwd, Info

    (46.61.193.86, 225.54.205.135) SPT, asm, Up: 06h15m17s
    JP: joined (never), RPF: Tengigabitethernet 0/0/1.30, nexthop: 46.61.193.86,
protocol: local, prefix: 46.61.193.0/24
      No interfaces in immediate olist

    (46.61.193.86, 225.54.205.136) SPT, asm, Up: 06h15m17s
    JP: joined (never), RPF: Tengigabitethernet 0/0/1.30, nexthop: 46.61.193.86,
protocol: local, prefix: 46.61.193.0/24
      No interfaces in immediate olist
```

Настройка протокола MSDP

Таблица 84. Порядок настройки MSDP

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`router msdp`	Создание MSDP процесса и переход в режим его настройки.
`vrf WORD`	(Опционально) Запуск IGMP-процесса в указанном VRF и переход в режим настройки этого процесса. Нижеследующие команды применимы для процесса внутри global table и внутри специфичного vrf.
`connect-source ADDR`	Указать адрес, с которого будет строиться сессия (в сторону старшего адреса) или который будет ожидать сообщений (от младшего адреса).
`originator-id ADDR`	(Опционально) Указать адрес, который будет указываться в качестве RP в сообщениях Source-Active. По умолчанию равняется connect-source.
`keepalive SEC`	(Опционально) Интервал отправки сообщений TCP Keepalive. По умолчанию: 60 секунд.
`holdtime SEC`	(Опционально) Время жизни сессий с поднятыми пирами. По умолчанию: 75 секунд.
`cache-sa-holdtime SEC`	(Опционально) Время жизни записи в кэше Source-Active. По умолчанию: 150 секунд.
`peer ADDR`	Создание пира и вход в режим его конфигурации.

`connect-source ADDR`	(Опционально) Указать адрес, с которого будет строиться сессия (в сторону старшего адреса) или который будет ожидать сообщений (от младшего адреса) для конкретного пира.
`mesh-group NUM`	(Опционально) Указать индекс MESH-группы, в рамках которой не будут рассылаться сообщения SA.
`description STRING`	(Опционально) Задать описание пира.
`shutdown`	(Опционально) Отключить создание сессии с указанным пиром.
`exit`	Возврат в режим конфигурации `router msdp`.
`commit`	Применение произведенных настроек.

Таблица 85. Порядок настройки листов фильтрации MSDP

Команда	**Назначение**
`configure`	Переход в режим глобальной конфигурации.
`router msdp`	Переход в режим настройки MSDP.
`peer ADDR`	Переход в режим конфигурации пира.
`sa-filter in NUM`	Создание фильтра на записи из входящих SA-сообщений.
`group-address IPv4(A.B.C.D)/WCARD(A.B.C.D) | any`	Задание wildcard-записи для матчинга адреса группы.
`source-address IPv4(A.B.C.D)/WCARD(A.B.C.D) | any`	Задание wildcard-записи для матчинга адреса источника.
`rp-address IPv4(A.B.C.D)/WCARD(A.B.C.D) | any`	Задание wildcard-записи для матчинга адреса RP.
`action permit|deny`	Действие для созданного фильтра: permit — разрешить, deny — отклонить. По умолчанию: разрешить.
`exit`	Возврат в режим конфигурации `router msdp peer`.
`sa-filter out NUM`	Создание фильтра для (S,G,RP) записей при формировании исходящего SA-сообщения. Правила создания фильтра аналогичны вышеописанным.
`commit`	Применение произведенных настроек.

Пример настройки MSDP

```
router msdp
  connect-source 10.0.0.134
  keepalive 60
  originator-id 10.0.0.144
  peer 10.0.0.111
```

```
    sa-filter out 1
      source-address any
      group-address any
      rp-address 10.0.0.134/0.0.0.0
    exit
    mesh-group 1000
  exit
  peer 10.0.0.26
    mesh-group 1000
  exit
```

Проверка работоспособности протокола MSDP

show msdp source-active

Выводит таблицу соответствия (S,G,RP) и место происхождения. Пример локальных source-active:

```
0/ME5100:Router# show msdp source-active
  Group Address    Source address   Peer address     Originator       Uptime
  ---------------- ---------------- ---------------- ---------------- --------------
  225.54.205.135   46.61.193.86     local            10.0.0.144       07h38m04s
  225.54.205.136   46.61.193.86     local            10.0.0.144       07h38m04s
```

Пример source-active принятых от соседа:

```
0/ME5100:Router# show msdp source-active
  Group Address    Source address   Peer address     Originator       Uptime
  ---------------- ---------------- ---------------- ---------------- --------------
  225.54.205.135   46.61.193.86     10.0.0.134       10.0.0.144       00h13m12s
  225.54.205.136   46.61.193.86     10.0.0.134       10.0.0.144       00h13m12s
```

Пример PIM-топологии, содержащей импортированные SA:

```
0/ME5100:Router# show pim topology
  IP PIM Multicast Topology Table
  Entry state: (*/S,G)[RPT/SPT] Mode, Protocol, Uptime, Info
  Interface state: Name, Uptime, Fwd, Info

    (46.61.193.86, 225.54.205.135) asm, Up: 00h11m23s
    JP: not-joined (never), RPF: Tengigabitethernet 0/0/12, nexthop: 100.26.134.134,
protocol: isis, prefix: 46.61.193.0/24
      No interfaces in immediate olist

    (46.61.193.86, 225.54.205.136) asm, Up: 00h11m23s
    JP: not-joined (never), RPF: Tengigabitethernet 0/0/12, nexthop: 100.26.134.134,
protocol: isis, prefix: 46.61.193.0/24
```

```
      No interfaces in immediate olist
```

show msdp peers

Выводит таблицу настроенных пиров, адресов, состояния и статистики. Пример:

```
0/ME5100:Router# show msdp peers
  Peer Address     Local address    State        Uptime/Downtime  Active SA Count  TLV
sent/recv  Mesh-Group
  ---------------- ---------------- ------------ ---------------- ----------------
-------------- -----------
  10.0.0.26        10.0.0.134       ESTABLISHED  01h03m34s        0
128/64         1000
```

Сервисы MVPN

Это набор способов передачи multicast-трафика с использованием IP-VPN. В устройствах ME используется NG-MVPN с анонсированием маршрутов в BGP SAFI5 и построением LDP-P2MP туннелей.

Предварительная настройка MVPN

Работа MVPN основывается на анонсирование VPNv4-префиксов для последующего использования в качестве source-адресов в подписках.

Пример настройки интерфейса и инстанса BGP для анонсирования L3VPN-маршрутов

```
interface loopback 2
  ! loopback-интерфейс в VRF для поднятия в нём S-PMSI-маршрута
  ipv4 address 10.0.0.134/32
  vrf mvpn
exit
interface tengigabitethernet 0/0/1.4030
  encapsulation outer-vid 4030
  ipv4 address 46.61.193.134/24
  vrf mvpn
exit
router bgp 65534
  neighbor 10.0.0.26
    address-family ipv4 mvpn
    exit
    address-family vpnv4 unicast
      next-hop-self
    exit
    remote-as 65534
    send-community
    send-community-ext
    update-source 10.0.0.134
```

```
  exit
exit
```

Настройка MVPN

Таблица 86. Порядок настройки MVPN

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`vrf WORD`	(Опционально) Переход в указанный VRF, в котором будет выполняться работа с multicast-маршрутами.
`mvpn`	Создание обработчика MVPN и переход в режим его настройки.
`customer-site-type receiver-only|sender-only|sender-receiver`	(Опционально) Указание способа приём/анонсирования маршрутов
`provider-tunnel-type ldp-p2mp|rsvp-p2mp`	(Опционально) Указание типа туннелей для построения и привязки к MVPN-маршрутам
`originator-ip ADDR`	(Опционально) Адрес originating-router/root-node в анонсах S-PMSI-маршрутов. По умолчанию является router-id в данном vrf.
`spmsi-tunnel GROUP SOURCE`	(Опционально) Создание статического S-PMSI туннеля.
`spt-only`	(Опционально) Включение режима, когда пропускается этап создания Shared-дерева
`exit`	Возврат в режим конфигурации `vrf`.
`commit`	Применение произведенных настроек.

Настройка протоколов для передачи MVPN-маршрутов

Пример настройки PIM

```
router pim
  vrf test1
    address-family ipv4
      ! интерфейс источника multicast
      interface tengigabitethernet 0/0/1.4030
        passive-interface
      exit
      ! обрабатываемые группы
      static-rp 225.54.0.0/16
        rp-address 10.0.0.134
      exit
    exit
  exit
exit
```

Пример настройки BGP

```
router bgp 65534
  neighbor 10.0.0.26
    ! добавляем SAFI mvpn на всех необходимых устройствах в сети
    address-family ipv4 mvpn
    exit
    address-family vpnv4 unicast
      next-hop-self
    exit
    remote-as 65534
    send-community
    send-community-ext
    update-source 10.0.0.134
  exit
exit
```

Пример настройки LDP

```
mpls
  forwarding
    interface loopback 1
    interface tengigabitethernet 0/0/1.4033
  exit
  ldp
    discovery interface tengigabitethernet 0/0/1.4033
    exit
  exit
exit
```

Пример настройки VRF

```
vrf test1
  export route-target 5:5
  import route-target 5:5
  mvpn
    customer-site-type receiver-only
  exit
  rd 5:5
exit
```

Проверка работоспособности MVPN

show multicast counters vrf mvpn

Выводит таблицу зарегистрированных multicast-потоков. Пример:

```
0/ME5100:Router# show multicast counters vrf mvpn
```

```
  Source Address                          Group Address
Packets Recv           Bytes Recv             Status codes  Interface
  ------------------------------------ ------------------------------------
--------------------- --------------------- ------------ ----------
  46.61.193.86                            225.54.205.135
303880                 414492320                         te0/0/1.4030
  46.61.193.86                            225.54.205.136
303808                 414394112                         te0/0/1.4030
```

show bgp ipv4 mvpn

Выводит таблицу анонсируемых и принимаемых MVPN-маршрутов. Пример:

```
0/ME5100:Router# show bgp ipv4 mvpn

  Network                  Next hop         Metric  LocPrf  Weight  Path
  ------------------------ ---------------- ------- ------- ------- -----
   >i  5:5 [1][10.0.0.26]
                           10.0.0.26        0       100     0       i
   >   5:5 [1][10.0.0.134]
                           10.0.0.134       0       100     0       i
   >   5:5 [3][46.61.193.86][225.54.205.135][10.0.0.134]
                           10.0.0.134       0       100     0       i
   >   5:5 [5][46.61.193.86][225.54.205.135]
                           10.0.0.134       0       100     0       i
   >i  5:5 [7][65534][46.61.193.86][225.54.205.135]
                           10.0.0.26        0       100     0       i
```

show bgp ipv4 mvpn route-type

Выводит подробную информацию о MVPN-маршрутах определённого типа. Пример:

```
0/ME5100:Router# show bgp ipv4 mvpn route-type source-active-ad

    Route Distinguisher: 5:5
    Multicast Source: 46.61.193.86
    Multicast Group: 225.54.205.135
    AS path:
    10.0.0.134 from afm (0.0.0.0)
      Origin igp, metric 0, local-pref 100, weight 0, inactive, best
      Address family: ipv4/mvpn
      NLRI pathID: 0
      Aggregator AS: 0, Address: 0.0.0.0, Atomic aggregate: absent
      Extended Community: RT 5:5 (0.0.0.5)
      Is not stale, is not history
      Route flap penalty: 0, flap count 0, is not suppressed
      Route flap time left: 00:00:00, time start: never
```

```
      Route is not ECMP
```

show pim vrf mvpn topology

Выводит таблицу зарегистрированных multicast-потоков. Пример:

```
0/ME5100:Router# show pim vrf mvpn topology

  IP PIM Multicast Topology Table
  Entry state: (*/S,G)[RPT/SPT] Mode, Protocol, Uptime, Info
  Interface state: Name, Uptime, Fwd, Info

    (46.61.193.86, 225.54.205.135) SPT, asm, Up: 01h53m08s
    JP: joined (never), RPF: Tengigabitethernet0/0/1.4030, (46.61.193.86)
      pmsi/5:5/10.0.0.134/3 asm, Up: 00h00m26s is local

    (46.61.193.86, 225.54.205.136) SPT, asm, Up: 01h53m08s
    JP: joined (never), RPF: Tengigabitethernet0/0/1.4030, (46.61.193.86)
```

show mpls ldp bindings mldp

Выводит таблицу меток для P2MP-туннелей. Пример:

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

  LSR                 Label    Type    Root node             Opaque value
  ------------------- -------- ------- --------------------- -------------
  10.0.0.26:0         101      P2MP    10.0.0.134            1
  10.0.0.26:0         106      P2MP    10.0.0.134            2
```

show mpls rsvp lsps p2mp

Выводит таблицу меток для P2MP-туннелей. Пример:

```
0/ME5100:Router# show mpls rsvp lsps p2mp

  Role: I - Ingress, T - Transit, E - Egress, * - Detour, # - Facility backup
  Flags: E - Entropy Label Capability

  Name                                      Id     Source            P2MP-ID
S2L Sub LSP Destination   In/Out Label      Role  Flags  State
  ----------------------------------------- ------ ----------------- -----------------
------------------------ ----------------- ----- ------ ------
  10.0.0.134:65535:mvpn:test2              65535  10.0.0.134        167772294
10.0.0.26                 26/-              E            up
```

Сервис IGMP-snooping

В главе описан способ настройки механизма контроля многоадресной рассылки в бридж-домене и способ его интеграции с мультикастом на устройстве.

Предварительная настройка IGMP-snooping

Работа функционала предполагает его включение в bridge-domain. При этом на устройстве не должно быть портов на том же устройстве (линейной карты или pizzabox), которые бы использовались в EVPN-bridge-domain.

Пример настройки бридж-домена, в котором te0/0/7.500 — это AC для подписчиков, а te0/8/4.300 — порт для приёма мультикаст-трафика.

```
interface tengigabitethernet 0/0/7.500
  encapsulation outer-vid 500
  rewrite egress tag push outer-vid 500
  rewrite ingress tag pop one
exit

interface tengigabitethernet 0/8/4.300
  encapsulation outer-vid 300
  rewrite egress tag push outer-vid 300
  rewrite ingress tag pop one
exit

l2vpn
  bridge-group all
    bridge-domain for_igmp_snooping
      interface tengigabitethernet 0/0/7.500
      exit
      interface tengigabitethernet 0/8/4.300
      exit
    exit
  exit
exit
```

Настройка IGMP-snooping

Таблица 87. Порядок настройки профиля igmp-snooping

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`igmp-snooping`	Переход в режим настройки igmp-snooping.
`profile PROFILE`	Создание профиля настроек igmp-snooping.
`querier-addr ADDR`	(Опционально) Включение IGMP Querier и задание ipv4-адреса исходящих сообщений.

Команда	Назначение
exit	Возврат в режим конфигурации igmp-snooping.
commit	Применение произведенных настроек.

Пример настройки профиля igmp-snooping

```
igmp-snooping
  profile test_profile
    querier-addr 10.0.0.26
    robustness 3
  exit
exit
```

Таблица 88. Порядок настройки igmp-snooping в бридж-домене

Команда	Назначение
configure	Переход в режим глобальной конфигурации.
l2vpn	Переход в режим настройки l2vpn.
bridge-group GROUP	Переход в режим настройки бридж-группы.
bridge-domain BRIDGE	Переход в режим настройки бридж-домена.
igmp-snooping	Включение igmp-snooping в бридж-домене.
profile PROFILE_NAME	Задание профиля настроек igmp-snooping.
exit	Возврат в режим конфигурации igmp-snooping.
interface IF	Переход в режим настройки интерфейса бридж-домена.
igmp-snooping	Переход в настройки свойств igmp-snooping порта
mrouter	(Опционально) Установка режима работы порта multicast router.
exit	Возврат в режим конфигурации интерфейса бридж-домена.
exit	Возврат в режим конфигурации бридж-домена.
commit	Применение произведенных настроек.

Пример настройки PIM

```
l2vpn
  bridge-group all
    bridge-domain for_igmp_snooping
      interface tengigabitethernet 0/0/7.500
      exit
      interface tengigabitethernet 0/8/4.300
        igmp-snooping
          mrouter
        exit
      exit
```

```
      flooding multicast disable
      igmp-snooping
        profile test_profile
      exit
    exit
  exit
exit
```

Интеграция с мультикастом на устройстве

Подразумевается, что мультикаст и IGMP-запросы будут обрабатываться в PIM. Это потребует использования BVI — L3-интерфейса, который будет представлен в бридж-домене и `router pim`.

Использование routed-интерфейса в бридж-домене потребует выравнивания количества меток между AC (описание `rewrite ingress/egress tag` приводится в главе `interfaces`).

Пример настройки PIM

```
router pim
  address-family ipv4
    interface bundle-ether 1.4033
    exit
    static-rp 225.54.205.0/24
      rp-address 10.0.0.30
    exit
  exit
exit
```

Таблица 89. Добавление BVI-интерфейса в глобальную конфигурацию, `bridge-domain` и `router igmp`

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`interface bvi 100`	Добавление BVI-интерфейса
`ipv4 address 200.0.20.1/24`	Создание IPv4-адреса на интерфейсе
`exit`	Возврат в глобальный режим конфигурации.
`l2vpn bridge-group all bridge-domain for_igmp_snooping`	Переход в ранее созданный бридж-домен.
`routed interface bvi 100`	Добавление маршрутизируемого интерфейса в бридж-домен.
`root`	Возврат в глобальный режим конфигурации.
`router igmp`	Создание экземпляра и переход в режим настройки протокола IGMP.
`interface bvi 100`	Создание IGMP-интерфейса `bvi 100`.
`root`	Возврат в глобальный режим конфигурации.

Команда	Назначение
`router igmp`	Создание экземпляра и переход в режим настройки протокола IGMP.
`commit`	Применение произведенных настроек.

Пример настройки PIM

```
interface bvi 100
  ipv4 address 200.0.20.1/24
exit
router igmp
  interface bvi 100
  exit
exit
l2vpn
  bridge-group all
    bridge-domain for_igmp_snooping
      interface tengigabitethernet 0/0/7.500
      exit
      interface tengigabitethernet 0/8/4.300
        igmp-snooping
          mrouter
        exit
      exit
      flooding multicast disable
      igmp-snooping
        profile test_profile
      exit
      routed interface bvi 100
    exit
  exit
exit
```

Проверка работоспособности IGMP-snooping

show igmp-snooping members

Выводит участников таблицы igmp-snooping. Пример:

```
0/ME5100:Router# show igmp-snooping members
  Memberships in Multicast Groups with running IGMP-snooping

  Bridge domain    Group Address    Interface        HW status  Expires
  ---------------- ---------------- ---------------- ---------- ----------
  for_igmp_snoopi  225.54.205.135   te0/0/7.500      enable     00h01m59s
  ng
```

```
  Total entries: 1
```

show igmp groups

Выводит список активных групп, обрабатываемых router igmp в результате получения IGMP Report. Пример:

```
0/ME5100:Router# show igmp groups
  IGMP Connected Group Membership

  Group Address            Interface               Uptime      Expires     Last
Reporter
  ----------------------- ----------------------- ----------- -----------
--------------
  225.54.205.135           bvi100                  00h00m04s   00h04m15s   50.0.0.1

  Total entries: 1
```

show pim topology

Выводит список PIM-записей. Пример:

```
0/ME5100:Router# show pim topology
  IP PIM Multicast Topology Table
  Entry state: (*/S,G)[RPT/SPT] Mode, Protocol, Uptime, Info
  Interface state: Name, Uptime, Fwd, Info

    (46.61.193.86, 225.54.205.135) SPT, asm, Up: 00h00m08s
    JP: joined (00h00m51s), RPF: Bundle-ether1.4033, (101.26.134.134)
      No interfaces in immediate olist

    (46.61.193.86, 225.54.205.135) RPT not-prune, Up: 00h00m00s
      No interfaces in immediate olist


    (*, 225.54.205.135) asm, Up: 00h00m09s, RP: 10.0.0.30 is not local (config)
    JP: joined (00h00m50s), RPF: Bundle-ether1.4033, (101.26.134.134)
      bvi100 asm, Up: 00h00m09s is local
```

ЗЕРКАЛИРОВАНИЕ ТРАФИКА

Зеркалирование трафика — технология дублирования пакетов одного или нескольких портов (и/или VLAN) на другом. Предназначена для контроля сетевого трафика, для анализа и отладки данных или диагностики ошибок в сетях путем пересылки копий входящих и/или исходящих пакетов с одного или нескольких контролируемых портов на один контролирующий порт.

На маршрутизаторах серии ME возможно создание до 15 сессий мониторинга.

Локальное зеркалирование SPAN (The Switched Port Analyzer) является наиболее простой формой зеркалирования. Все контролируемые (source) порты расположены на том же сетевом устройстве, что контролирующий (destination) порт.

SPAN

Таблица 90. Настройка сессии мониторинга SPAN

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`monitor-session` *session_name*	Переход в режим конфигурации сессии мониторинга.
`description` *descr*	(Опционально) Добавить описание назначения сессии
`destination interface` *type num*	Задать контролирующий порт — интерфейс, на который будут отправляться копии перехваченных пакетов.
`source interface` *type num*	Переход в режим конфигурации контролируемого порта — интерфейса, с которого будут перехватываться пакеты.
`direction { both | rx-only | tx-only }`	Выбрать тип зеркалируемого трафика: входящий (rx-only), исходящий (tx-only), весь трафик. По умолчанию зеркалируется весь трафик (both).
`vlan` *vlan_tag*	Указать контролируемую VLAN и перейти в режим задания типа трафика.
`direction { both | rx-only | tx-only }`	(опционально) Выбрать тип зеркалируемого трафика для трафика с указанным VLAN ID: входящий (rx-only), исходящий (tx-only), весь трафик. По умолчанию зеркалируется весь трафик (both). **IMPORTANT** **Архитектура устройства позволяет зеркалировать полностью (both) в определенной VLAN только транзитный трафик. Исходящий трафик в VLAN с интерфейса не зеркалируется.**

Команда	Назначение
`exit`	Возврат в режим конфигурации контролируемых портов. Можно добавить дополнительные VLAN ID для перехвата трафика.
`exit`	Возврат в режим конфигурации сессии мониторинга.
`shutdown`	(Опционально) Отключение сессии мониторинга.
`exit`	(Опционально) Возврат в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

Remote SPAN (RSPAN)

Зеркалированный трафик также можно передавать на устройства мониторинга, не подключенные непосредственно к маршрутизатору. Зеркалированный трафик инкапсулируется в пакеты с внешним тегом RSPAN VLAN и передается по сети коммутаторов к удаленному устройству мониторинга.

Таблица 91. Настройка сессии мониторинга RSPAN

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`monitor-session` *session_name*	Переход в режим конфигурации сессии мониторинга.
`description` *descr*	(Опционально) Добавить описание назначения сессии.
`source interface` *type num*	Переход в режим конфигурации контролируемого порта.
`direction { both | rx-only | tx-only }`	Выбрать, какой трафик будет зеркалироваться. По умолчанию зеркалируется весь трафик (both).
`vlan` *vlan_tag*	Указать контролируемую VLAN.
`direction { both | rx-only | tx-only }`	Выбрать тип зеркалируемого трафика: входящий (rx-only), исходящий (tx-only), весь трафик. По умолчанию зеркалируется весь трафик (both).
`exit`	Возврат в режим конфигурации контролируемых портов. Можно добавить дополнительные VLAN ID для перехвата трафика.
`exit`	Возврат в режим конфигурации сессии мониторинга.
`destination remote`	Переход в режим настройки RSPAN VLAN.
`interface` *type num*	Указать интерфейс, через который копии пакетов будут отправляться к удаленному устройству мониторинга.
`vlan` *vlan_id*	Задать RSPAN VLAN — тег, который будет добавляться на копии перехваченных пакетов при их отправке к удаленному устройству мониторинга.

Команда	Назначение
`vlan-pcp` *value*	(Опционально) Изменить приоритет трафика, передаваемого в RSPAN VLAN (по умолчанию, значение приоритета равно 0).
`commit`	Применение произведенных настроек.

Пример настройки локальной сессии мониторинга (SPAN)

```
monitor-session test
  destination interface tengigabitethernet 0/0/16
  source interface tengigabitethernet 0/0/1
    direction rx-only
    vlan 55
    exit
    vlan 103
    exit
    vlan 500
    exit
  exit
exit
```

Пример настройки сессии удаленного мониторинга (RSPAN)

```
monitor-session test2
  destination remote
    interface tengigabitethernet 0/0/9
    vlan 1000
  exit
  source interface tengigabitethernet 0/0/3
    vlan 4094
    exit
  exit
exit
```

Информация о сессиях мониторинга содержится в выводе команды `show monitor-session`, также можно вывести информацию об определенной сессии, указав её имя в show-команде:

```
0/ME5100:Router# show monitor-session
Mon Dec 14 15:11:55 2020

  Session:     test
  Type:        local
  State:       up

    Source:
      Interface: te0/0/1
      Direction: rx-only
        VLAN:      55
        Direction: both
```

```
        VLAN:      103
        Direction: both
        VLAN:      500
        Direction: both

    Destination:
      Interface: te0/0/16

Session:     test2
Type:        remote
State:       up

    Source:
      Interface: te0/0/3
      Direction: both
        VLAN:      4094
        Direction: both

    Destination:
      Interface: te0/0/9
      VLAN:      1000
```

НАСТРОЙКА КАЧЕСТВА ОБСЛУЖИВАНИЯ QoS

В данной главе рассматриваются принципы настройки системы обеспечения качества обслуживания сети. Параметры качества обслуживания (Quality of Service) позволяют приоритизировать прохождение определенных типов трафика, производить перемаркировку (изменение приоритета) транзитному трафику, а также задавать полосу пропускания для разных типов трафика на различных интерфейсах. На маршрутизаторах серии ME можно гибко регулировать политики прохождения трафика.

Перемаркировка L3 трафика

В приведенном примере требуется ограничить клиентский трафик до 20Mbit/s в обоих направлениях, и, в то же время, не давать возможности приоритизированному трафику от клиента использовать ресурсы классов cs6 и cs7 (например, в дизайне под данные типы классов заложены каналы мониторинга и управления сети).

Таблица 92. Создание и настройка QoS-профайлов.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`qos`	Переход в режим конфигурирования и создания QoS параметров.
`shape profile` *PROFILE_NAME*	Создание ограничительного профиля для исходящего трафика. В данной версии ПО шейпинг применим только для исходящего трафика.
`rate` *KBPS*	Задание ограничительной скорости, при достижении которой превышающий трафик будет отброшен. Данный параметр является обязательным.
`exit`	Возврат в режим конфигурирования и создания QoS параметров.
`rate-limit profile` *PROFILE_NAME*	Создание ограничительного профиля для входящего трафика. В данной версии ПО входящий трафик возможно ограничить только посредством применения rate-limit.
`rate` *KBPS*	Задание максимальной скорости передачи трафика. Трафик со скоростью передачи, превышающей заданное значение, будет отброшен. Данный параметр является обязательным.
`exit`	Возврат в режим конфигурирования и создания QoS параметров.

Теперь для того, чтобы как-то помечать приходящий клиентский трафик, необходимо создать *tc-map* (карта классов трафика). На основе данной карты пакеты будут помечаться внутренними для устройства маркерами - *tc*, и уже на их основе проводиться выбранное пользователем действие - классификация в необходимый класс с помощью *class-map* или перемаркировка.

Таблица 93. Создание и настройка tc-map.

Команда	**Назначение**
`tc-map` *MAP_NUMBER*	Создание карты классов трафика.
`ipv4-dscp` *DSCP_VALUE*	Определяем какое значение DSCP в IPv4 пакете будет помечаться маркерами tc.
`tc` *INTERNAL_TC_VALUE*	Назначаем номер внутреннего для устройства tc-маркера. Данный параметр является обязательным.
`set ipv4-dscp` *DSCP_VALUE*	Применяем перемаркировку DSCP на необходимое значение по дизайну.
`exit`	Возврат в режим конфигурирования и создания QoS параметров.
`exit`	Возврат в режим глобальной конфигурации.

Остаётся последний шаг - применение на клиентский интерфейс *shape profile* для ограничения исходящей скорости, *rate-limit profile* для ограничения входящей скорости и *tc-map* для перемаркировки входящего от клиента маркированного трафика в нужный класс.

Таблица 94. Применение qos-настроек на интерфейс.

Команда	**Назначение**
`interface { tengigabitethernet | bundle-ether }` *num* | *num.subif_id*	Переход в режим конфигурирования интерфейса либо сабинтерфейса.
`shape output profile` *PROFILE_NAME*	Применение профиля ограничения скорости на исходящий трафик.
`rate-limit input` *PROFILE_NAME*	Применение профиля ограничения скорости на входящий трафик.
`tc-map input` *MAP_NUMBER*	Применение правила матчинга и перемаркировки входящего трафика.
`exit`	Возврат в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

Пример. Создание интерфейса с перемаркировкой клиентского трафика из cs6 и cs7 в cs5

```
qos
  tc-map 101
    ipv4-dscp 48-63
```

```
      set ipv4-dscp 40
      tc 5
    exit
  exit
  shape profile 20Mbits
    rate 20480
  exit
  rate-limit profile 20Mbits
    rate 20480
  exit
exit

interface tengigabitethernet 0/0/2.300
  tc-map input 101
  shape output profile 20Mbits
  rate-limit input profile 20Mbits
exit
```

Аналогичным образом можно отстроить и сервисы, предоставляемые клиентам посредством L2-VPN технологий, обеспечив требуемый уровень качества обслуживания сети. Отличие будет лишь в том, что теперь нас интересуют L2-заголовки клиентских фреймов и их значения PCP-поля (priority code point).

IMPORTANT

MPLS-заголовок, также имеющий в себе 3 бита для приоритизации, наследует значения приоритетов в зависимости от инкапсулируемой нагрузки. Т.е. для L3-VPN сервисов значение поля DSCP будет транслировано в MPLS-TC и передано в сеть, для L2-VPN за основу будет взято поле PCP. Необходимо учитывать данный момент в целевом дизайне предоставления услуг.

Перемаркировка MPLS-трафика

Если дизайн сети требует полную независимость MPLS-сегмента от приоритетов входящего в сегмент трафика, тогда на PE-маршрутизаторах требуется применять rewrite-правила.

Таблица 95. Создание и настройка rewrite-map для MPLS-интерфейсов.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`qos`	Переход в режим конфигурирования и создания QoS параметров.
`rewrite-map` *MAP_NUMBER*	Создание карты перемаркировки трафика.
`ipv4-dscp` *DSCP_VALUE*	Определяем на основе какого значения DSCP в IPv4 заголовке будет установлен приоритет в MPLS-пакете.
`set mpls-tc` *TC_VALUE*	Назначаем приоритет для исходящего MPLS-пакета.
`exit`	Возврат в режим конфигурирования rewrite-map.

Команда	Назначение
`exit`	Возврат в режим конфигурирования и создания QoS параметров.
`exit`	Возврат в режим глобальной конфигурации.

Последний шаг - применить *rewrite-map* на все MPLS-интерфейсы данного маршрутизатора.

NOTE	В случае появления новых MPLS-линков, требуется назначать и на них правила перемаркировки, так как *rewrite-map* является per-interface объектом.

Таблица 96. Применение QoS-правил на MPLS-интерфейсы.

Команда	Назначение
`interface { tengigabitethernet | bundle-ether }` *num* | *num.subif_id*	Переход в режим конфигурирования интерфейса либо сабинтерфейса.
`qos rewrite output` *MAP_NUMBER*	Применение карты перемаркировки на исходящий трафик.
`exit`	Возврат в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

Пример. Перемаркировка трафика, исходящего из PE-маршрутизатора в MPLS-сегмент.

```
qos
  rewrite-map 404
    ipv4-dscp 0-63
      set mpls-tc 1
    exit
  exit
exit

interface tengigabitethernet 0/0/1.400
  qos rewrite output 404
exit
```

Таким образом, весь исходящий L3-VPN трафик будет сохранять IPv4 DSCP приоритет, но mpls-tc будет равен 1.

Ограничение полосы по приоритетам трафика

Немного усложним задачу. Представим, что необходимо L3-трафику выделять определенную пропускную полосу, согласно приоритетам, например, cs1 ограничивать 20Mbit/s, cs5 ограничивать 10Mbit/s, cs7 ограничивать 5Mbit/s, а весь оставшийся трафик ограничивать 60Mbit/s. Таким образом, тот трафик, приоритет которого мы будем учитывать, необходимо задетектировать с помощью *tc-map*, затем произвести классификацию принятого трафика с помощью *class-map*, а уже после ограничивать

требуемой полосой с помощью *policy-map*.

Таблица 97. Создание и настройка policy-map.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`qos`	Переход в режим конфигурирования и создания QoS параметров.
`tc-map` *MAP_NUMBER*	Создание карты классов трафика.
`ipv4-dscp` *DSCP_VALUE*	Определяем какое значение DSCP в IPv4 пакете будет помечаться маркерами tc.
`tc` *TC_VALUE*	Назначаем номер внутреннего для устройства tc-маркера. Данный параметр является обязательным.
`exit`	Возврат в режим конфигурирования и создания QoS параметров.
`class-map` *CLASS_MAP_NAME*	Создание карты классификации трафика.
`match tc` *INTERNAL_TC_VALUE*	Назначение внутреннего для устройства tc-маркера.
`match-mode` { all | any }	(опционально) Режим работы классификации - либо должны быть соблюдены все условия, либо хотя бы одно из условий (режим по умолчанию).
`exit`	Возврат в режим конфигурирования и создания QoS параметров.
`policy-map` *POLICY_MAP_NAME*	Создание политики для ограничения исходящего трафика.
`class` *CLASS_MAP_NAME*	Настройка использования классов трафика в политике.
`shape rate` *KBPS*	Задание ограничительной скорости для класса, при достижении которой превышающий трафик будет отброшен.
`exit`	Возврат в режим конфигурирования *policy-map*.
`exit`	Возврат в режим конфигурирования и создания QoS параметров.
`exit`	Возврат в режим глобальной конфигурации.

Последний шаг - применить *policy-map* на интерфейсы маршрутизатора.

Таблица 98. Применение policy-map на интерфейсы.

Команда	Назначение
`interface { tengigabitethernet | bundle-ether } num | num.subif_id`	Переход в режим конфигурирования интерфейса либо сабинтерфейса.

Команда	Назначение
`tc-map input MAP_NUMBER`	Применение правила матчинга входящего трафика.
`service-policy output POLICY_MAP_NAME`	Применение сервисной политики на исходящий трафик.
`exit`	Возврат в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

Пример. Ограничение исходящего трафика согласно приоритетам.

```
qos
  tc-map 202
    ipv4-dscp 8
      tc 1
    exit
    ipv4-dscp 40
      tc 5
    exit
    ipv4-dscp 56
      tc 7
    exit
  exit
  class-map cs1
    match tc 1
  exit
  class-map cs5
    match tc 5
  exit
  class-map cs7
    match tc 7
  exit
  policy-map shape_cs_output
    class class-default
      shape rate 61440
    exit
    class cs1
      shape rate 20480
    exit
    class cs5
      shape rate 10240
    exit
    class cs7
      shape rate 5120
    exit
  exit
exit

interface tengigabitethernet 0/0/2.300
  tc-map input 202
exit
```

```
interface tengigabitethernet 0/0/1.400
  service-policy output shape_cs_output
exit
```

NOTE Т.к. в данном примере *tc-map* настроена на конкретные значения DSCP, то af11, af31, ef и все остальные классы трафика будут попадать под правило class-default и делить полосу в 60Mbit/s. По умолчанию class-default имеет внутренний маркер tc = 0.

NOTE Трафик, принятый на интерфейс с ненастроенной (не применённой) *tc-map*, будет классифицироваться как class-default.

НАСТРОЙКА ПРОТОКОЛОВ RIP И RIPng

В данной главе описаны принципы настройки протокола динамической маршрутизации RIP (Routing Information Protocol).

Протокол принадлежит к семейству протоколов состояния соединения и относится к группе IGP (Interior Gateway Protocol). Основан на алгоритме Беллхэма-Форда (вектор расстояния). Применяемая в протоколе RIP метрика представляет собой количество транзитных переходов до адреса назначения. Максимально допустимое количество транзитных переходов для RIP равно 15. Метрика 16 считается бесконечно большой, адрес недостижимым.

По умолчанию маршрутизатор отправляет обновления информации о маршрутах каждые 30 секунд. В обновлениях содержатся не только маршруты, которые подключены к нему напрямую, но и маршруты, полученные от других маршрутизаторов посредством протокола RIP. Если в течение 180 секунд роутер не получает обновлений, то маршруты, полученные при помощи предыдущих обновлений, помечаются как "необновленные". По истечении 120 секунд "необновленные" маршруты удаляются.

Версии протокола RIP

- RIP version 1 - может работать только с классовой адресацией. Широковещательная рассылка обновлений.
- RIP version 2 - протокол обновлен, добавлена поддержка бесклассовой адресации (поддержка VLSM, Variable Length Subnet Masks). Обновления передаются с помощью многоадресатной, а не широковещательной рассылки (адрес 224.0.0.9)
- RIPng (RIP next generation) - добавлена поддержка IPv6.

В маршрутизаторах серии ME поддержаны RIP version 2 и RIPng.

Принципы конфигурирования протокола RIP

Настройка процесса динамической маршрутизации RIP производится в разделе конфигурации `router rip`.
На устройстве возможно создать только один процесс маршрутизации RIP.
Внутри данного конфигурационного блока настраивается RIP как для глобальной таблицы, так и для имеющихся на маршрутизаторе экземпляров VRF.

Дальнейшая конфигурация также производится иерархически.

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

Таким образом, последовательность конфигурирования протокола RIP выглядит следующим образом:

1. Создание процесса маршрутизации.
2. Общая настройка протокола RIP на устройстве.
3. Добавление интерфейсов.

NOTE	Последовательность конфигурирования протокола RIPng на маршрутизаторах серии ME аналогична.

Базовая настройка протокола RIP

Настройка протокола производится согласно описанной выше иерархии.

Таблица 99. Базовая настройка протокола RIP

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`router rip` (`router ripng`)	Создание процесса маршрутизации RIP (либо RIPng) и переход в режим его настройки.
`interface { loopback | tengigabitethernet | bundle-ether | fortygigabitethernet | hundredgigabitethernet | tunnel-ip | twentyfivegigabitethernet}` *num*	Добавление соответствующего интерфейса (либо сабинтерфейса) переход в режим его настройки.
`receive disable`	(Опционально) Запретить прием обновлений на интерфейсе.
`send disable`	(Опционально) Запретить отправку обновлений с интерфейса.
`dscp` *value*	(Опционально) Задание значения поля DSCP, с которым будут генерироваться IP-пакеты.
`exit`	Возврат в режим настройки процесса маршрутизации.
`timers { update-interval | holddown-interval | flush-interval}` *SECONDS*	(Опционально) Задание таймеров протокола RIP: `update-interval` — интервал отправки обновлений. Принимает значения 1…50000 секунд. Дефолтное значение — 30 секунд; `holddown-interval` — интервал времени с момента получения последнего обновления, по истечении которого маршрут будет помечен как "возможно недоступный". Дефолтное значение — 180 секунд; `flush-interval` — интервал времени, после которого помеченный маршрут будет удален. Дефолтное значение — 120 секунд.
`exit`	Возврат в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

Пример. Базовая настройка протокола RIP

```
router rip
  interface loopback 1
  exit
  interface tengigabitethernet 0/0/5
  exit
exit
```

Настройка RIP для экземпляра VRF

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

NOTE	Процессы маршрутизации для разных VRF работают независимо друг от друга.

Таблица 100. Настройка протокола RIP для экземпляра VRF

Команда	**Назначение**
`configure`	Переход в режим глобальной конфигурации.
`router rip`	Создание процесса маршрутизации RIP и переход в режим его настройки.
`vrf` *VRF_NAME*	Включение RIP в соответствующем экземпляре VRF и переход в режим его настройки.
`interface { loopback | tengigabitethernet | bundle-ether | fortygigabitethernet | hundredgigabitethernet | tunnel-ip | twentyfivegigabitethernet}` *num*	Добавление соответствующего интерфейса (либо сабинтерфейса) переход в режим его настройки.
`receive disable`	(Опционально) Запретить прием обновлений на интерфейсе.
`send disable`	(Опционально) Запретить отправку обновлений с интерфейса.
`dscp` *value*	(Опционально) Задание значения поля DSCP, с которым будут генерироваться IP-пакеты.
`exit`	Возврат в режим настройки процесса маршрутизации.

Команда	Назначение
`timers { update-interval | holddown-interval | flush-interval}` *SECONDS*	(Опционально) Задание таймеров протокола RIP: `update-interval` — интервал отправки обновлений. Принимает значения 1…50000 секунд. Дефолтное значение — 30 секунд; `holddown-interval` — интервал времени с момента получения последнего обновления, по истечении которого маршрут будет помечен как "возможно недоступный". Дефолтное значение — 180 секунд; `flush-interval` — интервал времени, после которого помеченный маршрут будет удален. Дефолтное значение — 120 секунд.
`exit`	Возврат в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

Пример. Настройка RIP для экземпляра VRF.

```
router rip
 vrf example
  interface loopback 1
  exit
  interface tengigabitethernet 0/0/5
  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 RIP. При этом маршрутизатор будет пытаться установить BFD-сессии с IP-адресами всех соседей, которых протокол RIP обнаружит на интерфейсе. В случае успешного установления таких соседств статус RIP-сессии свяжется со статусом соответствующей BFD-сессии.

NOTE	Только для протокола RIP. Поддержка BFD для RIPng отсутствует.

Пример. Настройка протокола BFD для RIP-интерфейса.

```
router rip
    interface tengigabitethernet 0/0/5
      bfd fast-detect
    exit
exit
```

Редистрибуция маршрутной информации

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

В текущей версии программного обеспечения фильтрации маршрутов, подлежащих редистрибуции не поддержана, передаются все маршруты указанного протокола.

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 OSPFv2;
4. **isis** — маршрутная таблица протокола IS-IS;
5. **local** — маршруты, являющиеся спецификами /32 для адресов, назначенных на IP-интерфейсы маршрутизатора.
6. **static** — статические маршруты.

Таблица 101. Настройка редистрибуции в RIP маршрутной информации из других протоколов.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`router rip`	Создание процесса маршрутизации RIP и переход в режим его настройки.
`redistribution { bgp | connected | isis | local | ospf | static }` *RULE_NAME*	Создание правила редистрибуции с именем *RULE_NAME* из указанного источника (bgp/connected/isis/local/ospf/static) и переход в режим настройки этого правила.
`match { prefix` IPv4PREFIX/MASK `| nexthop` IPv4PREFIX/MASK `| prefix-list` NAME_prefix-list`}`	Указание фильтра, используемого для данного правила.
`metric-value` *METRIC*	Установить значение RIP-метрики для маршрутов, прошедших через данное правило.

Команда	Назначение
`priority` *RULE_PRIORITY*	Установить приоритет данного правила редистрибуции. Правила редистрибуции выполняются по очереди от низкого значения приоритета к высокому и срабатывают по первому вхождению.
`route-map` *ROUTEMAP_NAME*	Установка "карты маршрутов" для фильтрации анонсов. Карта маршрутов с именем, соответствующим *ROUTEMAP_NAME*, должна быть создана в конфигурации маршрутизатора.
`redistribute disable`	Запретить редистрибуцию маршрутов, попавших в текущее правило. При выполнении данной команды текущее правило становится запрещающим.
`exit`	Выход из режима настройки правила редистрибуции. Далее можно настроить следующие правила — для того же самого источника, либо для других источников редистрибуции.
`root`	Выход в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

Пример. Настройка процесса RIP с правилом редистрибуции connected-маршрутов.

```
router rip
    interface loopback 1
    exit
    interface tengigabitethernet 0/0/5
      bfd fast-detect
    exit
  redistribution connected CONNECT-OSPF
    match prefix 100.65.0.0/24
    priority 10
    redistribute disable
  exit
exit
```

Проверка работы RIP и диагностические команды

show route rip

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

Пример. show route rip

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

```
  Codes: R - RIP


  R      5.5.0.148/32    via 100.101.31.3 [120/3], 01h46m30s, te0/0/5
  R      5.5.0.200/32    via 100.101.31.3 [120/4], 01h46m30s, te0/0/5
  R      16.1.1.7/32    via 100.101.31.3 [120/2], 01h46m30s, te0/0/5
  R      17.0.1.0/24    via 100.101.31.3 [120/2], 01h46m30s, te0/0/5

  Total route count: 4
```

show rip

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

Пример. show rip

```
0/ME5100:Router# show rip
Thu Oct  6 16:37:16 2022
  Routing Information Protocol:

    Timers:
      Update interval: 30 sec
      Holddown interval: 180 sec
      Flush interval: 120 sec

    Interface(s):
      Interface        Send             Receive          Sent      Recv      Recv bad
Recv bad
                                                         updates   updates   packets
routes
      ---------------- ---------------- ---------------- --------- --------- ---------
---------
      te0/1/2.3        enabled          enabled          2         18        0
0


    Neighbor(s):
      IP address                   Interface        Last update      Version
BFD status       Recv bad  Recv bad

packets   routes
      ---------------------------- ---------------- ---------------- ----------------
---------------- --------- ---------
      100.101.31.3                 te0/1/2.3        00h00m02s        2
not-required     0         0
```

НАСТРОЙКА АГЕНТА DHCP RELAY

DHCP (Dynamic Host Configuration Protocol — протокол динамической настройки узла, RFC 2131) — сетевой протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Протокол DHCP работает по принципу клиент-сервер, обмен данными между клиентом и сервером осуществляется через порты 67 и 68. Для передачи информации от клиента к серверу DHCP использует порт 67, в обратном направлении — 68.

По умолчанию, запросы протокола DHCP передаются в пределах одной подсети. При расположении в разных широковещательных доменах клиентов и серверов обмен пакетами производится через специальный ретранслятор — DHCP Relay Agent.

Для передачи дополнительной информации о DHCP-клиенте на DHCP-сервер, а также для защиты от атак с использованием протокола DHCP используется опция 82.

Поле Option 82 в DHCP пакете имеет две стандартные области:

- Agent Circuit ID — содержит информацию о том, с какого порта пришел запрос на DHCP-ретранслятор.
- Agent Remote ID — идентификатор самого DHCP-ретранслятора (который задается при настройке, например, MAC-адрес устройства, имя или любое удобное значение).

Настройка L2 DHCP Relay агента

Таблица 102. Последовательность настройки L2 DHCP Relay агента

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`relay-agent` *name*	Переход в режим конфигурирования DHCP Relay Agent.
`interface` *type num*	Указать интерфейс и перейти в режим его настройки.
`trusted ipv4`	Добавляет интерфейс в список «доверенных». DHCP-пакеты (DHCPOFFER, DHCPACK, DHCPNAK или DHCPLEASEQUERY), отправляемые DHCP-сервером, полученные с этих интерфейсов не отбрасываются.
`exit`	Возврат в режим конфигурации DHCP Relay Agent.
`mode { append | discard | forward | replace }`	Изменить способ обработки DHCP-пакетов с опцией 82, полученных с клиентских (untrusted) интерфейсов • **append** — добавить в DHCP-пакет опцию 82; • **discard** — отбросить DHCP-пакет; • **forward** — передать без изменений (по умолчанию); • **replace** — заменить опцию 82.
`exit`	Возврат в режим глобальной конфигурации.

Команда	Назначение
`commit`	Применение произведенных настроек.

Пример: конфигурация L2 DHCP Relay агента. Интерфейсы объединены в бридж-домен.

```
interface tengigabitethernet 0/0/1.88
  description "to DHCP-server"
  encapsulation outer-vid 88
  rewrite egress tag push outer-vid 88
  rewrite ingress tag pop one
exit

interface tengigabitethernet 0/0/1.92
  description client1
  encapsulation outer-vid 92
  rewrite egress tag push outer-vid 92
  rewrite ingress tag pop one
exit

interface tengigabitethernet 0/0/1.93
  description client2
  encapsulation outer-vid 93
  rewrite egress tag push outer-vid 93
  rewrite ingress tag pop one
exit

l2vpn bridge-group default bridge-domain DHCP
  interface tengigabitethernet 0/0/1.88
  exit
  interface tengigabitethernet 0/0/1.92
  exit
  interface tengigabitethernet 0/0/1.93
  exit
exit

relay-agent test
  interface tengigabitethernet 0/0/1.88
    trusted ipv4
  exit
  interface tengigabitethernet 0/0/1.92
  exit
  interface tengigabitethernet 0/0/1.93
  exit
exit
```

Настройка L3 DHCP Relay агента.

Таблица 103. Последовательность настройки L3 DHCP Relay агента

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`relay-agent` *name*	Переход в режим конфигурирования DHCP Relay Agent.
`address-family ipv4`	Переход в режим настройки IP-адреса DHCP-сервера.
`helper-address` *ipv4address*	Указать IP-адрес DHCP-сервера.
`vrf` *vrf_name*	Указать экземпляр VRF, в котором доступен IP-адрес DHCP-сервера.
`exit`	Возврат в режим конфигурации DHCP Relay Agent.
`interface` *type num*	Указать интерфейс DHCP-клиента.
`mode { append | discard | forward | replace }`	Изменить способ обработки DHCP-пакетов с опцией 82, полученных с клиентских (untrusted) интерфейсов • **append** — добавить в DHCP-пакет опцию 82; • **discard** — отбросить DHCP-пакет; • **forward** — передать без изменений; • **replace** — заменить опцию 82.
`relay-source` *ipv4address*	(Опционально) Задать IP-адрес в качестве IP-адреса отправителя (src в IP заголовке) и IP-адреса клиентского интерфейса (relay agent IP address) при отправке пакетов на DHCP-сервер (DHCP discover). **IMPORTANT** Для обеспечения корректной работы необходимо воспользоваться командой "**keep-relay-address**" режима конфигурирования Relay агента.
`keep-relay-address`	(Опционально) Сохранить в DHCP-пакете (DHCP discover) в качестве relay agent IP address адрес интерфейса, с которого пришел DHCP-запрос от клиента.
`exit`	Возврат в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

Пример: конфигурация L3 DHCP Relay агента. Интерфейсы объединены в бридж-домен. В бридж-домен добавлен также маршрутизирующий виртуальный интерфейс (BVI)

```
relay-agent test
  address-family ipv4 helper-address 88.1.1.119
    vrf test
  exit
  interface bvi 23
  exit
exit
```

```
l2vpn bridge-group default bridge-domain DHCP
  interface tengigabitethernet 0/0/1.88
  exit
  interface tengigabitethernet 0/0/1.92
  exit
  interface tengigabitethernet 0/0/1.93
  exit
  routed interface bvi 23
  exit
exit

interface bvi 23
  ipv4 address 92.168.15.1/24
  vrf test
exit
```

Команды диагностики

Ниже перечислены show-команды, посредством которых можно получить различную диагностическую информацию о DHCP Relay агенте.

show relay-agent counters

Команда выводит статистику по всем Relay агентам системы.

Пример: show relay-agent counters

```
0/ME5100:Router#show relay-agent counters

  Relay agent name:         test
    IPv4 helper-address:    88.1.1.119
      VRF name:             test
    Interface:              bvi23
      Interface oper state: up
    IPv4 Counters
      DHCP Packets:
        Discover:         22
        Offer:            9
        Request:          45
        Decline:          0
        ACK:              45
        NAK:              0
        Release:          12
        Inform:           0
        Lease query:      0
        Lease unassigned: 0
        Lease unknown:    0
        Lease active:     0
      Failed packets
```

```
      Bad length:                  0
      To interface w/o IPv4:       0
      TTL expired:                 0
      Unexpected type:             0
      Bad Header length:           0
      Add options fail:            0
      Receive packet fail:         0
      Send packet fail:            0
      Deleted pending packet:      0
      To deleted interface:        0
      Strip options fail:          0
  IPv6 Counters
    DHCP Packets:
      Solicit:              0
      Advertise:            0
      Request:              0
      Confirm:              0
      Renew:                0
      Rebind:               0
      Release:              0
      Reply:                0
      Decline:              0
      Reconfigure:          0
      Information request:  0
      Relay forward:        0
      Relay reply:          0
      Lease query:          0
      Lease query reply:    0
      Lease query done:     0
      Lease query data:     0
      Lease query request:  0
      Reconfigure reply:    0
      Query:                0
      Response:             0
    Failed packets
      Unknown type:           0
      To interface w/o IPv6:  0
      TTL expired:            0
      Unexpected type:        0
      Receive packet fail:    0
      Send packet fail:       0
      Bad length:             0
      Msg w/o relay options:  0
      Unknown interface:      0
```

show relay-agent state

Команда выводит информацию о конфигурации Relay агентов системы.

Пример: show relay-agent state

```
0/ME5100:Router#show relay-agent state

 Relay agent name:         test
    IPv4 helper-address:    88.1.1.119
      VRF name:             default
    IPv6 helper-address:    88:1:1::119
      VRF name:             default
    Interface:              te0/0/1.55
      Interface oper state: up
      Interface is active
      L3 IPv4 enabled
         IPv6 disabled
    Interface:              te0/0/1.92
      Interface oper state: up
      Interface is active
      L3 IPv4 enabled
         IPv6 enabled
    Interface:              te0/0/1.95
      Interface oper state: down
      Interface is disabled

  Relay agent name:         new
    Interface:              te0/0/1.3001
      Interface oper state: up
      Interface is active
      L2 IPv4 trusted
    Interface:              te0/0/3.3335
      Interface oper state: up
      Interface is active
      L2 IPv4 untrusted
```

НАСТРОЙКА DHCP-СЕРВЕРА

Глава посвящена настройке DHCP-сервера.

Настройка экземпляра сервера

Экземпляр DHCP-сервера в VRF представляет собой процесс, который обрабатывает входящие и формирует DHCP-запросы на определённых интерфейсах.

Маршрутизаторы ME позволяют настроить один экземпляр DHCP-сервера в глобальной таблице маршрутизации и по одному экземпляру на каждый из VRF.

Конфигурация сервера

Таблица 104. Порядок конфигурации dhcp-server

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`interface IF`	Создание L3-интерфейса
`ipv4 address ADDR`	Задание адреса интерфейса.
`root`	Переход в режим глобальной конфигурации.
`dhcp-server`	Переход в режим настройки DHCP-сервера.
`interface IF`	Добавление прослушивания на интерфейсе.
`default-lease-time value`	Время аренды адреса в секундах, если клиент не запрашивает конкретное время аренды.
`maximum-lease-time value`	Максимальное аренды адреса в секундах, которое может быть предоставлено клиенту в ответ на его запрос.
`address-family ipv4|ipv6|both`	Задание AFI, в рамках которого будет работать сервер.
`address-range RANGE`	Задание диапазона адресов, из которых будет происходить выдача. Диапазон должен являться подмножеством сети интерфейса. Обязательный параметр.
`excluded-range RANGE`	Задание диапазона адресов из диапазона **address-range**, которые не могут быть выданы клиентам.

`options`	Вход в режим задания преднастроенных опций. • **default-router** - DHCP option 3 (Default router list) • **dns-server** - DHCP option 6 (DNS servers list) • **domain-name** - DHCP option 15 (Domain name) • **filename** - name of the initial boot file • **netbios-name-server** - DHCP option 44 (NetBIOS servers list) • **next-server** - next-server address • **ntp-server** - DHCP option 42 (NTP servers list) • **tftp-server-address** - tftp option 150 (TFTP server address) • **tftp-server-name** - tftp option 66 (TFTP server name) • **v6-info-refresh-time** - DHCPv6 option 32 (Info refresh time) • **v6-nis-domain-name** - DHCPv6 option 29 (NIS domain name) • **v6-nis-servers** - DHCPv6 option 27 (NIS servers addresses) • **v6-nisp-domain-name** - DHCPv6 option 30 (NIS+ domain name) • **v6-nisp-servers** - DHCPv6 option 28 (NIS+ servers addresses) • **v6-sip-servers-addresses** - DHCPv6 option 22 (SIP servers addresses) • **v6-sip-servers-names** - DHCPv6 option 21 (SIP servers names) • **v6-sntp-servers** - DHCPv6 option 31 (SNTP servers).
`exit`	Возврат в режим конфигурации `interface`.
`exit`	Возврат в режим конфигурации `dhcp-server`.
`static-bindings IP MAC`	Создание статической записи соответствия IP-MAC.
`commit`	Применение произведенных настроек.

Пример настройки dhcp-server для глобальной таблицы маршрутизации

```
dhcp-server vrf default
  interface tengigabitethernet 0/0/4.2000300
    address-family ipv4
    address-range 200.0.20.2-200.0.20.100
    address-range 200.0.40.2-200.0.40.100
  exit
exit
```

Проверка применённых списков адресов:

show dhcp-server interfaces

Вывод интерфейсов, на которых происходит обработка DHCP-сообщений. Пример:

```
0/ME5100:Router# show dhcp-server interfaces
  address-list cde
    1 permit 232.0.0.0/8
    2 permit 239.0.0.0/8

  address-list test
    1 permit 232.1.1.1/32
```

show dhcp-server bindings

Вывод активных аренд. Пример:

```
0/ME5100:Router# show dhcp-server bindings

  DHCP-server process is enabled in vrf default

  IP address        Hardware address   Type     Expires
  ----------------- ------------------ -------- -----------
  200.0.20.2        00:e0:6f:7d:01:2c  dynamic  16:21:43
  200.0.20.15       9c:ef:5e:6f:ec:fc  dynamic  16:25:55
  200.0.20.16       00:f1:38:28:84:d4  dynamic  16:26:07
  200.0.20.17       00:e7:64:31:3a:af  dynamic  16:26:10
```

СПИСКИ КОНТРОЛЯ ДОСТУПА (ACL)

Глава посвящена настройке списков доступа.

Создание списка доступа

Список доступа (далее — "Список") — это способ регулировать прохождение пакетов через интерфейс на основании значений заголовков, политик и действий. Он применяется на интерфейсе и обрабатывает входящий трафик. Список состоит из правил ("seq-num", далее — "Правило"). Правило обладает следующими атрибутами:

- Имеет порядковый номер для указания места в общей очереди сопоставления для её перебора;
- Содержит критерии для сопоставления. Как только будет найдено Правило, критерии которого удовлетворены, перебор прекратится;
- Содержит список действий, который будет применён к пакету.

Порядок создания Списка

Таблица 105. Порядок конфигурации access-list

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`access-list NAME`	Переход в режим настройки Списка.
`seq-num NUM`	Переход в режим настройки Правила.
`source NUM`	Переход в режим указания атрибутов "источник" различных заголовков для сопоставления.
`ipv4 A.B.C.D`	Задание ipv4-адреса для сопоставления с заголовком ipv4 полем "источник"
`exit`	Возврат в режим настройки Правила.
`destination NUM`	Переход в режим указания атрибутов "получатель" различных заголовков для сопоставления.
`port eq 179`	Задание атрибута "порта получателя" для сопоставления с соответствующим полем заголовка транспортного уровня.
`exit`	Возврат в режим настройки Правила.
`action deny`	Установка запрета на прохождение пакета.
`exit`	Возврат в режим настройки Списка.
`exit`	Возврат в режим глобальной конфигурации.
`interface te 0/8/4.3000`	Вход в режим настройки интерфейса.
`access-group ingress 1`	Задание Списка доступа на указанном интерфейсе.
`commit`	Применение произведенных настроек.

Пример настройки access-list

```
access-list 1
  seq-num 10
    action deny
    destination
      port eq 179
    exit
    log-enable
    source
      ipv4 10.0.0.26
    exit
  exit
  seq-num 20
  exit
exit
```

Для работы ACL на устройстве необходимо выставить соответствующие аппаратные настройки. Их включение и задание лимитов задействует ресурс TCAM чипа коммутации.

Таблица 106. Порядок конфигурации аппаратных настроек для ACL

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`hw-module enable acl-counters`	Включение поддержки счётчиков срабатывания ACL. Требует наличия установленного модуля статистики
`hw-module enable acl-default`	Включение поддержки сопоставления с таблицей маршрутизации, с попаданием трафика под действие маршрута по умолчанию.
`hw-module enable acl-qos`	Включение поддержки QoS для возможности задания TC, DSCP.
`hw-module maximum acl-entries 10`	Задание максимального количества правил в расчёте на один интерфейс.
`commit`	Применение произведенных настроек.

Пример настройки аппаратных настроек для ACL

```
hw-module enable acl-counters
hw-module enable acl-default
hw-module enable acl-qos
hw-module maximum acl-entries 10
```

Проверка применённых списков адресов:

show access-lists

Вывод сокращённой информации о списке доступа. Пример:

```
0/FMC0:example_router01# show access-lists 1
  access-list 1
    10, deny, any, src[10.0.0.26], dst[port eq 179] L2: 0, IPv4: 0, IPv6: 0 hits
    20, permit, any, src[any], dst[any] L2: 0, IPv4: 0, IPv6: 0 hits
```

show access-lists detailed 1

Вывод расширенной информации о списке доступа. Пример:

```
0/FMC0:example_router01# show access-lists detailed 1
Tue Mar 21 16:32:13 2023
  HW resources: 0/10 acl entries at LC0/0
                4/10 acl entries at LC0/8
                0/10 acl entries at LC0/11

  Access-list: 1
  Configured on interfaces:
    te0/8/4.3000, L2: 0, IPv4: 0, IPv6: 0 hits
  seq-num 10
    action:  deny
    match:   proto any, tos any, no fragments, flow-label any, vid any, pcp any, dei
any, ethertype any
             source: ipv4 10.0.0.26, ipv6 any, port any, mac any
             destination: ipv4 any, ipv6 any, port eq 179, mac any
    set:     none
    total:   L2: 0, IPv4: 0, IPv6: 0 hits
  seq-num 20
    action:  permit
    match:   proto any, tos any, no fragments, flow-label any, vid any, pcp any, dei
any, ethertype any
             source: ipv4 any, ipv6 any, port any, mac any
             destination: ipv4 any, ipv6 any, port any, mac any
    set:     none
    total:   L2: 0, IPv4: 0, IPv6: 0 hits
```

Создание группы объектов

Группа объектов — это список элементов одного уровня, которые могут применяться в качестве ссылки в правилах списка доступа.

Порядок создания группы объектов

Таблица 107. Порядок конфигурации object-group

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`object-group ipv4-group NAME`	Переход в режим настройки Группы.
`address A.B.C.D/N`	Задание ipv4-подсети.
`exit`	Возврат в режим глобальной конфигурации.
`commit`	Применение произведенных настроек.

Пример настройки object-group

```
object-group network ipv4-group OUTER_NETWORKS
  address 212.20.0.0/16
  description "OG to match enemy's networks"
exit
access-list 1
  seq-num 10
    action deny
    source
      ipv4 OUTER_NETWORKS
    exit
  exit
exit
```

ТЕСТЫ ELTEX IP SLA

IP SLA является функцией программного обеспечения, которая предоставляет пользователям возможность анализировать уровень обслуживания IP для приложений и сервисов. IP SLA использует метод активного тестирования за счет непрерывной генерации трафика надежным и предсказуемым методом. Активное тестирование дает возможность оценивать важные характеристики качества передачи данных в сетях, работающих на базе протокола IP.

На маршрутизаторах серии ME поддерживаются следующие типы тестов:

- icmp-echo;
- icmp-jitter;
- udp-echo;
- udp-jitter.

Маршрутизатор поддерживает возможность конфигурации до 128 тестов.

Один из самых простых примеров теста - проверка доступности ресурса с помощью простого “ping” (отправки ICMP-запроса и ожидания ICMP-ответа).

Более сложный - проверка качества канала по таким характеристикам как jitter и delay. Маршрутизатор отправляет сгенерированный пакет встречному устройству. После того как тестируемый маршрутизатор получает пакет, в зависимости от типа IP SLA измерения, он отправляет тестовый пакет обратно источнику с временной меткой для калькуляции сетевых показателей. IP SLA выполняет измерение параметров линка, используя протокол UDP.

Для работы UDP-тестов на оконечном устройстве должен быть включен респондер, позволяющий системе отвечать на тестовые запросы IP SLA, которые посылает sender. IP SLA респондер доступен на устройствах ELTEX серии ME и ESR. Генератор IP SLA может отправлять тестовые пакеты только с устройств ELTEX серии ME и ESR.

Респондер IP SLA ожидает на определенном порту (control-phase-dest-port) так называемое контрольное сообщение по протоколу управления от генератора IP SLA тестов сендера. После получения контрольного сообщения, IP SLA включает согласованный UDP или TCP порт. Респондер принимает запросы и отвечает на них. В целях дополнительной защиты для контрольного сообщения доступно шифрование. Для запуска IP SLA-теста необходимо указать:

- destination-address;
- source-address.

Для остальных параметров используются значения по умолчанию. Это минимальная конфигурация теста icmp-echo, который запустится после применения настроек и будет длиться бесконечно.

IP SLA sender

Ниже описывается конфигурация устройства-инициатора тестов IP SLA (сендер, *sender*).

Таблица 108. Настройка IP SLA sender

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`ip-sla sender`	Переход в режим конфигурации IP SLA sender.
`test` *num*	Задание номера теста и переход в режим его настройки.
`vrf` *vrf_name*	[Опционально] Указать VRF, в которой будет запущен тест.
`destination-address` *ipv4address*	Задание IP-адреса опрашиваемого хоста.
`destination-port` *value*	[Опционально] Задание порта, на который будут отправляться SLA-пакеты.
`source-address` *ipv4address*	Задать IP-адрес интерфейса, с которого будут отправляться SLA-пакеты.
`source-port` *value*	[Опционально] Задать порт, с которого будут отправляться SLA-пакеты.
`type { icmp-echo | icmp-jitter | udp-echo | udp-jitter }`	Выбрать тип теста.
`control-phase-dest-port` *value*	[Опционально] Указать порт, который прослушивает респондер. Через этот порт происходит согласование параметров теста между сендером и респондером, в частности, пароля и способа шифрования. Дефолтный порт - 1800. Настраивается на сендере и респондере. Используется только для тестов UDP.
`ip-sla-logging-traps`	Активировать функцию отправки SNMP-трапов при изменении состояния теста.
`dscp` *value*	[Опционально] Задать значение DSCP пакетов IP SLA.
`disable`	Отключить тест IP SLA.

Таблица 109. Настройка временных и количественных параметров. Производится в режиме настройки теста.

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`ip-sla sender`	Переход в режим конфигурации IP SLA sender.
`test` *num*	Задание номера теста и переход в режим его настройки.
`start-time { HH:MM | HH:MM:SS | YYYY.MM.DD-HH:MM:SS }`	Задание времени начала теста. Если не указывать время начала, тест запустится после выполнения команды "commit".

Команда	Назначение
`lifetime` *value*	Задание длительности теста в секундах.
`recurring`	Запускать тест раз в сутки в заданное (start-time) время с заданной (lifetime) продолжительностью.
`number-of-packets` *value*	Задание количества пакетов в тесте.
`packet-interval` *value*	Задание временного интервала между отправкой отдельных пакетов.
`packet-size` *value*	Задание размера пакета.
`test-interval` *value*	Задание временного интервала между тестами.
`rep-hist-count` *value*	Задание количества тестов, результаты которых войдут в статистику.
`ttl` *value*	Задать значение TTL пакетов IP SLA.
`commit`	Применение произведенных настроек.

IP SLA responder

Ниже описывается конфигурация устройства-ответчика для тестов IP SLA (респондер, *responder*).

Таблица 110. Настройка IP SLA responder

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`ip-sla responder`	Переход в режим конфигурации IP SLA responder.
`vrf` _vrf_name	[Опционально] Указать VRF, в которой будет запущен тест.
`address` {*ipv4address* | all }	Задание IP-адреса интерфейса, который будет отвечать на тестовые запросы IP SLA сендера и переход в режим его настройки.
`control-phase-dest-port` *value*	[Опционально] Указать порт, который "слушает" респондер. Дефолтный порт - 1800.
`exit`	(Опционально) Возврат в режим конфигурации респондера.
`disable`	Отключить респондер.
`commit`	Применение произведенных настроек.

Настройка аутентификации

Аутентификация должна быть настроена на сендере и респондере. При настройке необходимо выбрать тип аутентификации и задать пароль. По умолчанию аутентификация отключена. На сендере аутентификация может быть настроена для каждого теста в отдельности, на респондере - для всех интерфейсов.

Таблица 111. Настройка аутентификации IP SLA sender

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`ip-sla sender`	Переход в режим конфигурации IP SLA sender.
`test` *num*	Задание номера теста и переход в режим его настройки.
`auth { hmac-sha256 | sha256 | none }`	Выбор типа аутентификации. Задание параметра `'none'` отключает аутентификацию, что соответствует поведению по умолчанию.
`password {` *KEY_STRING* `| encrypted` *KEY_ENCRYPT* `}`	Задание ключа для аутентификации в открытом (*KEY_STRING*) либо в зашифрованном (*KEY_ENCRYPT*) виде.
`commit`	Применение произведенных настроек.

Таблица 112. Настройка аутентификации IP SLA responder

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`ip-sla responder`	Переход в режим конфигурации IP SLA responder.
`auth { hmac-sha256 | sha256 | none }`	Выбор типа аутентификации. Задание параметра `'none'` отключает аутентификацию, что соответствует поведению по умолчанию.
`password {` *KEY_STRING* `| encrypted` *KEY_ENCRYPT* `}`	Задание ключа для аутентификации в открытом (*KEY_STRING*) либо в зашифрованном (*KEY_ENCRYPT*) виде.
`commit`	Применение произведенных настроек.

Пример настройки теста UDP IP SLA. Линия тестируется большими пакетами, включена отсылка трапов на устройство мониторинга, настроена аутентификация. Тест запускается ежедневно в 16:10 и длится 1200 секунд.

```
ip-sla sender
  test 3
    auth sha256
    control-phase-dest-port 1808
    destination-address 5.5.0.30
    ip-sla-logging-traps
    lifetime 1200
    packet-size 1514
    password encrypted CDE650
    recurring
    source-address 5.5.0.31
    start-time 16:10
    type udp-jitter
  exit
exit
```

На встречном устройстве должен быть включен респондер.

```
ip-sla responder
  address 5.5.0.30
    control-phase-port 1808
  exit
  auth sha256
  password encrypted CDE650
exit
```

Диагностические команды

show ip-sla results

Команда выводит информацию обо всех тестах, запущенных в данный момент.

Пример. show ip-sla results

```
0/ME5100:Router# sh ip-sla results
Mon Jun 26 16:31:07 2023

  Test ID:                                        2
    Status:                                       fail
    Error description:                            control phase failed: timeout
    Start time:                                   2023.06.26-16:31:00
    Finish time:                                  2023.06.26-16:31:02
    Number of successfull tests:                  0
    Number of failed tests:                       1
    Number of test packets:                       0
    Number of Sender->Responder samples:          0
    Number of Responder->Sender samples:          0
    Number of Sender->Responder packets sent:     0
    Number of Responder->Sender packets received:  0
    Jitter values:
      Sender->Responder minimum:            0.000000 sec
      Sender->Responder average:            0.000000 sec
      Sender->Responder maximum:            0.000000 sec
      Sender->Responder current:            0.000000 sec
      Responder->Sender minimum:            0.000000 sec
      Responder->Sender average:            0.000000 sec
      Responder->Sender maximum:            0.000000 sec
      Responder->Sender current:            0.000000 sec
    Loss values:
      Sender->Responder loss:               0
      Sender->Responder loss percent:       0.000000
      Responder->Sender loss:               0
      Responder->Sender loss percent:       0.000000
      Duplicate:                            0
      Late Arrival:                         0
      Skipped:                              0
```

```
    One way latency values:
      Sender->Responder minimum delay:      0.000000 sec
      Sender->Responder average delay:      0.000000 sec
      Sender->Responder maximum delay:      0.000000 sec
      Responder->Sender minimum delay:      0.000000 sec
      Responder->Sender average delay:      0.000000 sec
      Responder->Sender maximum delay:      0.000000 sec
    Out of sequence values:
      Sender->Responder:                    0
      Responder->Sender:                    0
    RTT values:
      Minimum delay:                        0.000000 sec
      Average delay:                        0.000000 sec
      Maximum delay:                        0.000000 sec

  Test ID:                                  3
    Status:                                 successful
    Error description:
    Start time:                             2023.06.26-16:30:02
    Finish time:                            2023.06.26-16:30:12
    Number of successfull tests:            19
    Number of failed tests:                 0
    Number of test packets:                 100
    Number of Sender->Responder samples:    100
    Number of Responder->Sender samples:    100
    Number of Sender->Responder packets sent:      100
    Number of Responder->Sender packets received:  100
    Jitter values:
      Sender->Responder minimum:            0.000028 sec
      Sender->Responder average:            0.000032 sec
      Sender->Responder maximum:            0.000039 sec
      Sender->Responder current:            0.000030 sec
      Responder->Sender minimum:            0.000028 sec
      Responder->Sender average:            0.000032 sec
      Responder->Sender maximum:            0.000039 sec
      Responder->Sender current:            0.000030 sec
    Loss values:
      Sender->Responder loss:               0
      Sender->Responder loss percent:       0.000000
      Responder->Sender loss:               0
      Responder->Sender loss percent:       0.000000
      Duplicate:                            0
      Late Arrival:                         0
      Skipped:                              0
    One way latency values:
      Sender->Responder minimum delay:      0.000197 sec
      Sender->Responder average delay:      0.000223 sec
      Sender->Responder maximum delay:      0.000272 sec
      Responder->Sender minimum delay:      0.000197 sec
      Responder->Sender average delay:      0.000223 sec
      Responder->Sender maximum delay:      0.000272 sec
```

```
    Out of sequence values:
      Sender->Responder:                    0
      Responder->Sender:                    0
    RTT values:
      Minimum delay:                        0.000394 sec
      Average delay:                        0.000446 sec
      Maximum delay:                        0.000543 sec

0/ME5100:AR31-17-151#
```

Также можно вывести информацию по определенному тесту

Пример. show ip-sla results test 3

```
0/ME5100:Router# sh ip-sla results test 3
Mon Jun 26 16:33:53 2023

  Test ID:                                      3
    Status:                                     successful
    Error description:
    Start time:                                 2023.06.26-16:30:02
    Finish time:                                2023.06.26-16:30:12
    Number of successfull tests:                19
    Number of failed tests:                     0
    Number of test packets:                     100
    Number of Sender->Responder samples:        100
    Number of Responder->Sender samples:        100
    Number of Sender->Responder packets sent:   100
    Number of Responder->Sender packets received:  100
    Jitter values:
      Sender->Responder minimum:            0.000028 sec
      Sender->Responder average:            0.000032 sec
      Sender->Responder maximum:            0.000039 sec
      Sender->Responder current:            0.000030 sec
      Responder->Sender minimum:            0.000028 sec
      Responder->Sender average:            0.000032 sec
      Responder->Sender maximum:            0.000039 sec
      Responder->Sender current:            0.000030 sec
    Loss values:
      Sender->Responder loss:               0
      Sender->Responder loss percent:       0.000000
      Responder->Sender loss:               0
      Responder->Sender loss percent:       0.000000
      Duplicate:                            0
      Late Arrival:                         0
      Skipped:                              0
    One way latency values:
      Sender->Responder minimum delay:      0.000197 sec
      Sender->Responder average delay:      0.000223 sec
      Sender->Responder maximum delay:      0.000272 sec
      Responder->Sender minimum delay:      0.000197 sec
```

```
    Responder->Sender average delay:      0.000223 sec
    Responder->Sender maximum delay:      0.000272 sec
  Out of sequence values:
    Sender->Responder:                    0
    Responder->Sender:                    0
  RTT values:
    Minimum delay:                        0.000394 sec
    Average delay:                        0.000446 sec
    Maximum delay:                        0.000543 sec
```

Настройка LLDP

LLDP (Link Layer Discovery Protocol, 802.1ab) — протокол канального уровня, позволяющий сетевому оборудованию оповещать локальную сеть о своем существовании и характеристиках, а также собирать такие же оповещения, поступающие от соседнего оборудования.

В сети с поддержкой LLDP устройство объявляет локальную информацию о себе в блоках данных LLDP (LLDPDU) непосредственно подключенным устройствам. Информация, распространяемая через LLDP, хранится ее получателями в стандартных MIB, что позволяет системе управления сетью (NMS) получать доступ к этой информации через SNMP.

В LLDPDU передается следующая информация об устройстве:

- Основные возможности системы;
- IP-адрес управления системой;
- Идентификатор устройства;
- Идентификатор порта.

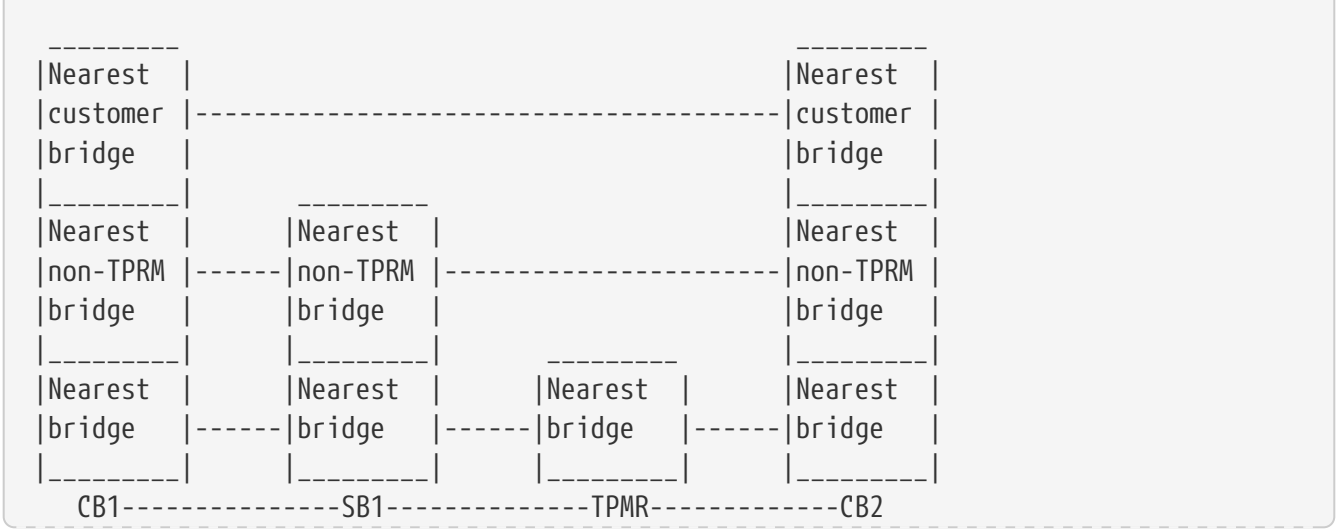
Агенты LLDP и режимы моста

Агент LLDP - это отображение объекта протокола, который реализует LLDP.
Несколько агентов LLDP могут работать на одном интерфейсе.

Агенты LLDP подразделяются на следующие типы:

- Ближайший агент моста (Nearest bridge)
- Ближайший агент моста клиента (Nearest customer bridge)
- Ближайший агент моста не-TPMR (Nearest non-TPRM bridge)

На схеме ниже приведен пример применения одновременного использования разных типов LLDP-мостов и прозрачного транзита LLDP-трафика для установления соседств между соответствующими устройствами.



```
Пример установления LLDP-соседства.
```

Оборудование передает кадры LLDP по сети Ethernet через определенные интервалы времени.

Кадры LLDP для режима моста "Nearest bridge" имеют Multicast MAC-адрес получателя 01:80:C2:00:00:0E.
Для режима моста "Nearest customer bridge" — 01:80:C2:00:00:00.
Для режима моста "Nearest non-TPRM bridge" — 01:80:C2:00:00:03.

Последовательность конфигурирования протокола LLDP выглядит следующим образом:

1. Общая настройка протокола LLDP на устройстве;
2. Добавление интерфейсов;
3. Выбор режима моста на интерфейсах.

Базовая настройка протокола LLDP

Настройка протокола производится согласно описанной выше иерархии.

Таблица 113. Базовая настройка протокола LLDP

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`lldp`	Включение LLDP и переход в режим его конфигурации.
`hold-multiplier` *value*	(Опционально) Задание множителя для расчета времени жизни (TTL) информации о соседе LLDP с момента последнего обновления. Дефолтное значение-4. (TTL=(hold-multiplier*interval)+1)
`interval` *value*	(Опционально) Задание интервала передачи LLDP-пакетов. Дефолтное значение-30 секунд.
`notification-interval` *value*	(Опционально) Задание времени отправки trap-сообщений после изменения LLDP таблицы. Дефолтное значение-30 секунд.
`optional-tlv { mgmt-addr | port-desc | system-cap | system-desc | system-name} disable`	(Опционально) Запрет передачи информации в TLV о выбранном параметре.
`optional-tlv mgmt-addr set {ipv4 address | ipv6 address}`	(Опционально) Задание IPv4 (IPv6)-адреса, который будет передаваться как адрес управления. По умолчанию в LLDPDU передается IPv4-адрес Loopback-интерфейса с наименьшим порядковым номером.

Команда	Назначение
`pps` *value*	(Опционально) Задание максимального количества последовательных LLDPDU в секунду, передаваемых при изменении локальной информации LLDP. Дефолтное значение-5.
`reinit` *value*	(Опционально) Задание минимального интервала времени в секундах перед повторной инициализацией LLDP. Дефолтное значение-2.
`disable`	(Опционально) Выключение LLDP на маршрутизаторе.
`lldp interface { tengigabitethernet | fortygigabitethernet | hundredgigabitethernet | twentyfivegigabitethernet }` *num_interface*	Включение LLDP на интерфейсе и переход в режим его конфигурации.
`agent { nearest-bridge | nearest-customer-bridge | nearest-non-tpmr-bridge }`	Задание режима моста, в котором будет работать интерфейс и переход в режим его конфигурации.
`neighbors-limit` *value*	(Опционально) Задание максимального количества соседей.
`optional-tlv { mgmt-addr | port-desc | system-cap | system-desc | system-name} disable`	(Опционально) Запрет передачи информации о выбранном параметре.
`optional-tlv mgmt-addr set {ipv4 address | ipv6 address}`	(Опционально) Задание IPv4 (IPv6)-адреса, который будет передаваться как адрес управления. По умолчанию в LLDPDU передается IPv4-адрес Loopback-интерфейса с наименьшим порядковым номером.
`port-id-type { interface-name | local | mac-address}`	(Опционально) Выбор параметра, который будет использоваться для идентификации интерфейса: · `interface-name`- имя интерфейса; · `local` - Interface index · `mac-address` - MAC-адрес интерфейса.
`notification device { enable | disable }`	Разрешить/запретить отправку SNMP-трапов при установлении нового LLDP-соседства.
`notification tables { enable | disable }`	Разрешить/запретить отправку SNMP-трапов при получении уведомления об изменении LLDP-информации от соседа.
`receive { disable | enable }`	Запретить /разрешить прием LLDP PDU на интерфейсе. По умолчанию прием разрешен.
`transmit { disable | enable }`	Запретить /разрешить передачу LLDP PDU на интерфейсе. По умолчанию передача разрешена.
`commit`	Применение произведенных настроек.

Пример конфигурации протокола LLDP

На порту маршрутизатора настроены два агента: agent nearest-bridge и agent nearest-customer-bridge. Для агента nearest-customer-bridge сконфигурирован свой mgmt-адрес. Также глобально задан mgmt-адрес, который будет передаваться со всех портов, на которых включен LLDP.

```
lldp
  interface tengigabitethernet 0/0/1
    agent nearest-bridge
    exit
    agent nearest-customer-bridge
      optional-tlv mgmt-addr set 5.5.0.31
    exit
  exit
  optional-tlv mgmt-addr set 192.168.17.151
exit
```

Диагностические команды

Ниже перечислены show-команды, посредством которых можно получить различную диагностическую информацию о работе LLDP на устройстве.

show lldp

Данная команда показывает глобальные настройки LLDP и в краткой табличной форме список LLDP-параметров всех интерфейсов, на которых включен протокол.

Пример: show lldp

```
0/ME5100:Router# show lldp
Fri Oct  3 15:12:38 2025
  System information:
        Chassis type        : MAC address
        Chassis ID          : a8:f9:4b:8b:bc:20
        System name         : AR31-17-151
        System description  : Eltex ME5100 carrier router

  Global LLDP information:
        LLDP tx interval            : 30 seconds
        LLDP hold multiplier        : 4
        LLDP TTL                    : 121 seconds
        LLDP reinitialization delay : 2 seconds
        LLDP notifications interval : 30 seconds
        LLDP pps                    : 5
        Management address          : 192.168.17.151

  LLDP agent codes:
        (N) Nearest Bridge, (NnT) Nearest non-TPMR Bridge
        (NC) Nearest Customer Bridge
```

```
  LLDP optional TLV codes:
        (MM) Enable management address TLV, (PD) Enable port description TLV
        (SC) Enable system capabilities TLV, (SD) Enable system description TLV
        (SM) Enable system name TLV

  Port            State TX  State RX  Optional TLVs     Notifications tables
Notifications device  Agent  Mgmt-addr
  --------------- --------- --------- ----------------- --------------------
-------------------- ------ -----------------
  te0/0/1         enabled   enabled   MM PD SC SD SM    enabled               enabled
N      192.168.17.151
  te0/0/1         enabled   enabled   MM PD SC SD SM    enabled               enabled
NC     5.5.0.31
```

show lldp interface

Данная команда показывает настройки LLDP на интерфейсах. Также можно показать конфигурацию определенного интерфейса, указав его в качестве ключа.

```
0/ME5100:Router# show lldp interface tengigabitethernet 0/0/1
show lldp interfaces tengigabitethernet 0/0/1
Tue Oct  7 16:50:47 2025
System information:
      Chassis type           : MAC address
      Chassis ID             : a8:f9:4b:8b:bc:20
      System name            : AR31-17-151
      System description     : Eltex ME5100 carrier router
      Management address     : 192.168.17.151
      Capabilities Available : Bridge, Router

Interface                    : Tengigabitethernet0/0/1
      Status                 : up
      Interface description  : -a MES3124F 17.31 te0/4
      Interface index        : 2
      MAC address            : a8:f9:4b:8b:bc:21

  Agent type                 : nearest-bridge
      Port-id type           : interface-name
      Neighbor limit         : 100
      Management address     : 192.168.17.151
      Tx                     : enabled
      Rx                     : enabled
      Notification tables    : enabled
      Notification device    : enabled

    Optional TLV
      Management address     : enabled
      Interface description  : enabled
      System capabilities    : enabled
```

```
      System description     : enabled
      System name            : enabled

  Agent type                 : nearest-customer-bridge
      Port-id type           : interface-name
      Neighbor limit         : 100
      Management address     : 5.5.0.31
      Tx                     : enabled
      Rx                     : enabled
      Notification tables    : enabled
      Notification device    : enabled

    Optional TLV
      Management address     : enabled
      Interface description  : enabled
      System capabilities    : enabled
      System description     : enabled
      System name            : enabled
```

show lldp local

Команда выводит информацию о конфигурации LLDP на интерфейсах в краткой табличной форме.

Пример: show lldp local

```
0/ME5100:Router# show lldp local
Fri Oct  3 15:17:03 2025
  Port        Agent  Mgmt-addr          Chassis ID         Capabilities     Port ID
Status      Port description
  ----------- ------ ------------------ ------------------ ---------------
------------------ ----------- -----------------
  te0/0/1     N      192.168.17.151     a8:f9:4b:8b:bc:20  Bridge, Router   te0/0/1
up          -a MES3124F 17.31 te0/4
  te0/0/1     NC     5.5.0.31           a8:f9:4b:8b:bc:20  Bridge, Router   te0/0/1
up          -a MES3124F 17.31 te0/4
```

show lldp neighbors

Данная команда показывает информацию об LLDP-нейборах в табличном виде. Использование ключа "detail" без параметров позволяет просмотреть полную информацию об LLDP-нейборах для всех интерфейсов.

Пример: show lldp neighbors

```
0/ME5100:Router# show lldp neighbors
Tue Oct  7 16:44:55 2025
  Capability codes:
        (R) Router, (B) Bridge, (T) Telephone, (D) DOCSIS Cable Device
```

```
        (W) WLAN Access Point, (r) Repeater, (H) Host, (s) Station only
        (TP) - Two Ports MAC Relay, (S) - S-VLAN, (C) - C-VLAN, (O) Other
  LLDP agent codes:
        (N) Nearest Bridge, (NnT) Nearest non-TPMR Bridge
        (NC) Nearest Customer Bridge
  Local port      Chassis id         Port id            Capabilities          Agent
System name
  --------------- ------------------ ------------------ -------------------- ------
------------
  te0/0/1         a8:f9:4b:8b:95:00  te0/1/2            B R                  NC
DR30-17-150
  te0/0/1         e8:28:c1:48:06:40  te0/0/1            B R                  NC
R17-200
  te0/0/1         a8:f9:4b:a6:4e:40  te1/0/4            B R                  N
```

show lldp statistics

Команда выводит LLDP-статистику по всем интерфейсам маршрутизатора. Также можно вывести статистику по определенному интерфейсу, указав его в качестве ключа.

Пример: show lldp statistics

```
0/ME5100:Router# show lldp statistics
Tue Oct  7 16:54:32 2025
  LLDP traffic statistics:
  Last neighbor change: 05h58m26s ago

        Neighbor entries added: 3
        Neighbor entries deleted: 0
        Neighbor entries aged out: 0
        Neighbor advertisements dropped: 0

  LLDP agent codes:
        (N) Nearest Bridge, (NnT) Nearest non-TPMR Bridge
        (NC) Nearest Customer Bridge)

  Port            TX frames total  TX frames errors  RX frames total  RX frames
discarded  Frames errors  RX TLVs discarded  RX TLVs unrecognized  RX ageouts total
Agent
  --------------- ---------------- ----------------- ----------------
------------------- -------------- ------------------ --------------------
----------------- ------
  te0/0/1         731              0                 2164             0
0              0                  0                    0                 N
  te0/0/1         726              0                 1450             0
0              0                  0                    0
```

ВСТРОЕННЫЙ МЕНЕДЖЕР СОБЫТИЙ EEM

Принцип работы

На маршрутизаторах серии ME реализован функционал встроенного менеджера событий (EEM, Embedded Event Manager), позволяющий создавать сценарии для автоматизации работы оборудования. Основной задачей данного функционала является отслеживание появления определенных пользователем событий (например, аварий) на устройстве и выполнение действий в случае активации или нормализации данных событий.

Сценарий EEM можно представить так:

```
Если "событие":
  то "выполнить действие (действия)"
```

В библиотеке EEM присутствуют две таблицы:

- **Tracks** - содержит все сконфигурированные треки.
- **Conditions** - содержит отслеживаемые Alarm сообщения.

Tracks содержит:

- Ключ, который представляет собой id трека.
- Сам класс track, который содержит все ключи отслеживаемых condition и все actions.

Conditions содержит:

- Ключ содержащий: alarm_code, ParamN.
- Condition, в котором собственно и хранится состояние отслеживаемого события.

Чтобы сконфигурировать трек (track), необходимо указать хотя бы одно событие (condition), которое может произойти на устройстве и хотя бы одно действие как реакцию на событие.
`action-on-event` - что нужно сделать, когда событие началось,
`action-on-dismiss` - что сделать, когда закончилось.
При задании action alias необходимо, чтобы данный alias был сконфигурирован на устройстве, иначе конфигурация применена не будет.

В настоящий момент на маршрутизаторах ME поддержан только один вид действий (`action`) - это `alias`. То есть выполняются стандартные команды CLI, перечень которых определен соответствующим алиасом (alias).

Track работает в одном из двух режимов — `and` или `or`:

- В случае and: реакция `action-on-event` запускается тогда, когда произошел хотя бы один отслеживаемый alarm, реакция `action-on-dismiss` запускается тогда, когда все отслеживаемые alarm'ы очистились.
- В случае or: реакция типа `action-on-event` запускается тогда, когда возникли все

отслеживаемые alarm'ы, реакция `action-on-dismiss` запускается тогда, когда произошел хотя бы один отслеживаемый alarm.

По умолчанию задан режим `and`.

Алиас (alias) - псевдоним, который позволяет пользователю запускать любую команду или группу команд вводом всего одного слова или даже символа.

Настройка алиаса

Таблица 114. Настройка алиаса

Команда	Назначение
`configure`	Переход в режим глобальной конфигурации.
`alias` *name*	Переход в режим конфигурации алиаса.
`description` *string*	(Опционально) Назначение имени-описания для алиаса. Описание следует заключать в кавычки в случае, если строка содержит символы пробела.
`seq` *num*	Создание элемента списка команд и переход в режим его настройки.
`command` *string*	Задание команды
`commit`	Применение произведенных настроек.

Пример. Конфигурация алиаса, который снимает логи и копирует их в папку на TFTP-сервере.

```
alias logs
  description tech-support
  seq 10
    command "show tech-support"
  exit
  seq 20
    command "copy fs://logs tftp://192.168.16.119/logs/ vrf mgmt-intf"
  exit
exit
```

Этот же алиас можно сконфигурировать в режиме командной строки.

```
0/ME5100:EOS# configure
0/ME5100:EOS(config)# alias logs
0/ME5100:EOS(config-alias)# description tech-support
0/ME5100:EOS(config-alias)# set
Insert commands as lines, insert ^C to close edit mode
> show tech
> copy fs://logs tftp://192.168.16.119/logs/ vrf mgmt-intf
>
0/ME5100:EOS(config-alias)# commit
```

Настройка трека

Для настройки трека EEM необходимо указать:

1. condition - условие-событие
2. Тип реакции на событие (`action-on-event` или `action-on-dismiss`)
3. alias - действие, которое должно выполниться при наступлении (`action-on-event`) или прекращении условия-события (`action-on-dismiss`)
4. (опционально) track-mode (`or` или `and`)

В качестве примера разберем следующий сценарий.

Допустим, нам необходимо отследить на маршрутизаторе состояние интерфейса te0/0/3.

В случае если интерфейс te0/0/3 находится в состоянии UP, то интерфейс te0/0/13 должен быть отключен. Если интерфейс te0/0/3 упадет, то активируется интерфейс te0/0/13.

Пример конфигурации.
.Создаем алиасы.

```
alias down_3
  seq 10
    command config
  exit
  seq 20
    command "interface te 0/0/13"
  exit
  seq 30
    command "shutdown"
  exit
  seq 40
    command commit
  exit
exit

alias up_3
  seq 10
   command config
  exit
  seq 20
    command "interface te0/0/13"
  exit
  seq 30
    command "no shutdown"
  exit
  seq 40
   command commit
  exit
```

```
exit
```

Далее отслеживаем состояние интерфейса te0/0/3:

```
event-tracking
  track 1
    action-on-dismiss 1
      alias down_3
    exit
    action-on-event 1
      alias up_3
    exit
    condition 1
      link-changed-oper-state-down   <==== Указываем параметры интерфейса. Где:
        param1 0   <================ Номер платы. В нашем случае это 0. (для
фиксированных устройств, дефолтное значение)
        param2 3   <================ Номер порта.
        param3 2   <================ Скорость порта. 1Gbit - 1; 10Gbit - 2; 25Gbit -
3; 40Gbit - 4; 100Gbit – 5. В нашем случае 2.
      exit
    exit
  exit
exit
```