



Спутниковые маршрутизаторы серии EVT, EVS
EVT-101, EVS-101
Руководство по эксплуатации
Версия ПО VSAT 1.1

Содержание

1	Введение	6
1.1	Аннотация.....	6
1.2	Целевая аудитория.....	6
1.3	Условные обозначения	7
1.4	Используемые термины и сокращения	7
1.5	Примечания и предупреждения.....	10
2	Описание устройства	11
2.1	Назначение	11
2.2	Конструктивное исполнение.....	11
2.2.1	Передняя панель устройства EVT-101/EVS-101	12
2.2.2	Задняя панель устройства EVT-101/EVS-101	14
2.2.3	Боковые панели устройства EVT-101/EVS-101	15
2.3	Световая индикация EVT-101/EVS-101	15
2.4	Основные технические характеристики	19
2.4.1	Характеристики помехоустойчивости.....	22
2.5	Функции устройств	22
2.5.1	Стандарты, протоколы и сервисы	22
2.5.2	Функции интерфейсов.....	23
2.5.3	Функции при работе с MAC-адресами	24
2.5.4	Функции второго уровня сетевой модели OSI.....	24
2.5.5	Функции третьего уровня сетевой модели OSI	24
2.5.6	Функции туннелирования трафика.....	26
2.5.7	Функции управления и конфигурирования	26
2.5.8	Функции сетевой защиты.....	27
2.6	Комплект поставки	27
3	Интерфейсы управления	28
3.1	Интерфейс командной строки (CLI)	28
3.2	Типы и порядок именования интерфейсов маршрутизатора	28
3.3	Типы и порядок именования туннелей маршрутизатора	30
4	Начальная настройка устройств	31
4.1	Подключение и конфигурирование маршрутизаторов	32
4.2	Подключение к маршрутизатору	32
4.2.1	Подключение по локальной сети Ethernet	32
4.2.2	Подключение через консольный порт RS-232	32
4.2.3	Применение изменения конфигурации	33

4.3	Установка лицензии.....	33
4.3.1	Установка корректной даты на устройство.....	33
4.3.2	Установка лицензий через USB-накопитель.....	34
4.3.3	Установка лицензии через TFTP.....	34
4.4	Смена режима работы спутникового модема.....	35
4.5	Настройка системы логирования событий.....	36
4.5.1	Пример настройки.....	36
4.6	Настройка политики использования паролей.....	37
4.6.1	Пример настройки.....	37
4.7	Настройка политики AAA.....	38
4.7.1	Пример настройки.....	38
4.8	Базовая настройка маршрутизатора.....	39
4.8.1	Изменение пароля пользователя «admin».....	40
4.8.2	Создание новых пользователей.....	40
4.8.3	Назначение имени устройства.....	41
4.8.4	Настройка параметров публичной сети.....	41
4.9	Настройка удаленного доступа к маршрутизатору.....	42
4.9.1	Настройка удалённого управления.....	43
4.9.2	Пример настройки.....	44
4.10	Рекомендации по безопасной настройке.....	45
4.11	Заводская конфигурация EVT-101/EVS-101.....	46
5	Рекомендации по безопасной настройке.....	47
5.1	Общие рекомендации.....	47
5.2	Настройка системы логирования событий.....	48
5.2.1	Рекомендации.....	48
5.2.2	Предупреждения.....	48
5.2.3	Пример настройки.....	48
5.3	Настройка политики использования паролей.....	49
5.3.1	Рекомендации.....	49
5.3.2	Пример настройки.....	49
5.4	Настройка политики AAA.....	50
5.4.1	Рекомендации.....	50
5.4.2	Предупреждения.....	50
5.4.3	Пример настройки.....	51
5.5	Настройка удалённого управления.....	52
5.5.1	Рекомендации.....	52
5.5.2	Пример настройки.....	53

6	Управление	54
6.1	Управление спутниковым интерфейсом	54
6.1.1	Настройка устройства для организации спутникового канала в режиме SCPC..	54
6.1.2	Настройка устройства для организации спутникового канала в режиме MCPC	62
6.1.3	Подключение BUC и LNB	78
6.1.4	Управление тестовыми режимами	79
6.2	Управление сетевыми интерфейсами	80
6.2.1	Настройка физического интерфейса	80
6.2.2	Настройка терминации на саб-интерфейсе	83
6.2.3	Настройка терминации на Q-in-Q интерфейсе	86
6.2.4	Управление QoS	90
6.2.5	Управление безопасностью	114
6.2.6	Управление маршрутизацией	142
6.2.7	Управление резервированием	252
6.2.8	Управление сервисами	280
6.2.9	Управление туннелированием	307
6.2.10	Управление функциями второго уровня (L2)	358
7	Мониторинг	383
7.1	Настройка Netflow	383
7.1.1	Алгоритм настройки	383
7.1.2	Пример настройки	385
7.2	Настройка SNMP	385
7.2.1	Алгоритм настройки	386
7.2.2	Пример настройки	391
7.3	Настройка Syslog	392
7.3.1	Алгоритм настройки	393
7.3.2	Пример настройки	397
7.4	Проверка целостности	398
7.4.1	Процесс настройки	398
7.4.2	Пример конфигурации	399
7.5	Настройка архивации конфигурации маршрутизатора	399
7.5.1	Процесс настройки	399
7.5.2	Пример конфигурации	400
7.6	Настройка SLA	401
7.6.1	Алгоритм настройки SLA-теста	401
7.6.2	Настройка SLA-responder	410
7.6.3	Пример настройки ICMP-режима тестирования	411

7.6.4	Пример настройки UDP-режима тестирования.....	412
7.6.5	Алгоритм настройки параметров аутентификации	414
7.6.6	Пример конфигурации UDP-теста с аутентификацией по ключ-строке.....	420
7.6.7	Пример конфигурации UDP-теста с аутентификацией по связке ключей.....	422
7.6.8	Настройка пороговых значений.....	424
7.6.9	Измерение характеристик канала связи	425
8	Часто задаваемые вопросы	427
9	Приложение А. Packet Flow	429
9.1	Порядок обработки входящего/исходящего трафика сетевыми службами маршрутизаторов EVT/EVS.....	429
9.2	Порядок обработки транзитного трафика сетевыми службами маршрутизаторов EVT/EVS	430
10	Управление лицензированием	432
10.1	Общие сведения Типы лицензий и поддерживаемые устройства Влияние лицензий на конфигурацию Базовые лицензии (SCPC, MCPC-TERMINAL, MCPC-HUB) Дополнительные лицензии (OQPSK) Смена режима работы спутникового модема Установка лицензий Установка корректной даты Установка лицензий через USB-накопитель Установка лицензии через TFTP.....	432
10.2	Общие сведения	432
10.3	Типы лицензий и поддерживаемые устройства.....	432
10.4	Влияние лицензий на конфигурацию	433
10.4.1	Базовые лицензии (SCPC, MCPC-TERMINAL, MCPC-HUB).....	433
10.4.2	Дополнительные лицензии (OQPSK).....	433
10.5	Смена режима работы спутникового модема	433
10.6	Установка лицензий.....	434
10.6.1	Установка корректной даты.....	434
10.6.2	Установка лицензий через USB-накопитель.....	434
10.6.3	Установка лицензии через TFTP.....	435

1 Введение

- [Аннотация](#)
- [Целевая аудитория](#)
- [Условные обозначения](#)
- [Используемые термины и сокращения](#)
- [Примечания и предупреждения](#)

1.1 Аннотация

В настоящее время осуществляются масштабные проекты по построению сетей связи. Одной из основных задач при реализации крупных мультисервисных сетей является создание надежных и высокопроизводительных транспортных сетей, которые являются опорными в многослойной архитектуре сетей следующего поколения.

Маршрутизаторы спутниковые EVT-101 и EVS-101 могут использоваться в телекоммуникационных сетях коммерческих и государственных ведомств, операторов спутниковой связи. Применяются в составе земных станций спутниковой связи и обеспечивают передачу данных по радиоканалу с использованием ИСЗ в соответствии со стандартом DVB-S2x.

В данном руководстве по эксплуатации изложены назначение, технические характеристики, конструктивное исполнение, порядок установки спутниковых маршрутизаторов EVT-101 и EVS-101. Рекомендации по обновлению программного обеспечения спутниковых маршрутизаторов EVT-101 и EVS-101 описано отдельно в документе «Руководство по обновлению ПО».

1.2 Целевая аудитория

Данное руководство пользователя предназначено для технического персонала, выполняющего установку, настройку и мониторинг устройства посредством интерфейса командной строки (CLI). Квалификация технического персонала предполагает знание базовых навыков в области спутниковой связи и основ работы стеков протоколов TCP/IP, принципов построения Ethernet-сетей.

1.3 Условные обозначения

Обозначение	Описание
[]	В квадратных скобках в командной строке указываются необязательные параметры, но их ввод предоставляет определенные дополнительные опции.
{ }	В фигурных скобках в командной строке указываются возможные обязательные параметры. Необходимо выбрать один из параметров.
«,» «-»	Данные знаки в описании команды используются для указания диапазонов.
« »	Данный знак в описании команды обозначает «или».
<Полужирный курсив>	Полужирным курсивом в угловых скобках указываются названия клавиш на клавиатуре.
Текст в рамке	В рамках с текстом указаны примеры и результаты выполнения команд.

1.4 Используемые термины и сокращения

Российская аббревиатура	Расшифровка
АЧХ	Амплитудно-частотная характеристика
ГОСТ	Государственный стандарт
ЗИП	Комплект запасных частей и принадлежностей
ИСЗ	Искусственный спутник Земли
ИРП	Индустриальные радиопомехи
КСН	Компенсация совмещенной несущей
МШУ	Малошумящий усилитель
ОТК	Отдел технического контроля
ПМ	Программа и методики испытаний
ПО	Программное обеспечение
ПС	Паспорт

Российская аббревиатура		Расшифровка
ПСИ		Приемо-сдаточные испытания
РФ		Российская Федерация
РЭ		Руководство по эксплуатации
СВЧ		Сверхвысокие частоты
ССБТ		Система стандартов безопасности труда
СРПП		Система разработки и постановки продукции на производство
ТУ		Технические условия
ФЗ		Федеральный закон
ЭПСС		Эквивалент полного сопротивления сети
Английская аббревиатура	Расшифровка	Перевод
APSK	Amplitude and Phase-Shift Keying	Амплитудная и фазовая манипуляция
ARP	Address Resolution Protocol	Протокол разрешения адресов
BGP	Border Gateway Protocol	Протокол пограничного шлюза
BUC	Block Upconverter	Блок-преобразователь частоты «вверх» и усилитель мощности
CLI	Command Line Interface	Интерфейс командной строки
DHCP	Dynamic Host Configuration Protocol	Протокол динамической настройки хоста
ETSI	European Telecommunications Standards Institute	Европейский институт телекоммуникационных стандартов
ICMP	Internet Control Message Protocol	Протокол межсетевых управляющих сообщений
IEC	International Electrotechnical Commission	Международная электротехническая комиссия
IP	Internet Protocol	Интернет протокол
ISO	International Organization for Standardization	Международной организации по стандартизации

Английская аббревиатура	Расшифровка	Перевод
LNB	Low-Noise Block	Маломощный усилитель принимаемого со спутника сигнала и понижающей преобразователь частоты
MMF	Multi Mode Fiber	Многомодовое оптическое волокно
NAT	Network Address Translation	Преобразование сетевых адресов
OQPSK	Offset Quadrature Phase-Shift Keying	Квадратурно-фазовая манипуляция со сдвигом (частоты)
OSPF	Open Shortest Path First	Протокол внутренней маршрутизации для IP-сетей
PSK	Phase-Shift Keying	Фазовая манипуляция
QPSK	Quadrature Phase-Shift Keying	Квадратурная фазовая манипуляция
RFC	Request for Comments	Рабочее предложение
RIP	Routing Information Protocol	Протокол маршрутизации информации
RJ	Registered Jack	Стандартизированный физический сетевой интерфейс
RX	Data Reception	Передача данных
SCPC	Single Channel per Carrier	Один канал на несущую (технология организации выделенного канала связи между двумя спутниковыми станциями)
SD	Secure Digital	Формат флеш-карты
SFP	Small Form-factor Pluggable	Стандарт модульных компактных приёмопередатчиков (трансиверов)
SMF	Single Mode Fiber	Одномодовое оптическое волокно
SSH	Secure Shell	Протокол для безопасного удаленного подключения
TCP	Transmission Control Protocol	Протокол управления передачей
Telnet	Teletype Network	Сетевой протокол удаленного подключения
TX	Data Transmission	Передача данных
USB	Universal Serial Bus	Последовательный интерфейс для подключения периферийных устройств

1.5 Примечания и предупреждения

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

 Предупреждения информируют пользователя о ситуациях, которые могут нанести вред устройству или человеку, привести к некорректной работе устройства или потере данных.

 Информация содержит справочные данные об использовании устройства.

2 Описание устройства

- Назначение
- Конструктивное исполнение
 - Передняя панель устройства EVT-101/EVS-101
 - Задняя панель устройства EVT-101/EVS-101
 - Боковые панели устройства EVT-101/EVS-101
- Световая индикация EVT-101/EVS-101
- Основные технические характеристики
 - Характеристики помехоустойчивости
- Функции устройств
 - Стандарты, протоколы и сервисы
 - Функции интерфейсов
 - Функции при работе с MAC-адресами
 - Функции второго уровня сетевой модели OSI
 - Функции третьего уровня сетевой модели OSI
 - Функции туннелирования трафика
 - Функции управления и конфигурирования
 - Функции сетевой защиты
- Комплект поставки

2.1 Назначение

Спутниковые маршрутизаторы серии EVT/EVS предназначены для построения географически распределённых сетей спутниковой связи класса VSAT в составе земных станций спутниковой связи в сетях по топологии «точка-точка» (SCPC), «точка-многоточка» (MCPC) в качестве каналообразующего оборудования, обеспечивающего модуляцию и демодуляцию сигналов стандарта DVB-S2X с IP-маршрутизацией.

Спутниковый маршрутизатор EVT-101	Спутниковый маршрутизатор EVS-101
Спутниковый маршрутизатор. Предназначен для работы в составе абонентской станции спутниковой связи, работающей в сетях по топологии «точка-точка» (SCPC) и «точка-многоточка» (MCPC). Включает в себя один модулятор, один демодулятор и производительный IP-маршрутизатор.	Многоканальный спутниковый маршрутизатор. Предназначен для работы в составе центральной (узловой) станции спутниковой связи, работающей в сетях по топологии «точка-многоточка» (MCPC). Включает в себя один модулятор, программный многоканальный демодулятор и производительный IP-маршрутизатор.

Устройство поддерживает функции межсетевого экрана для защиты сети организации и своей сетевой инфраструктуры, а также сочетает в себе средства обеспечения безопасности данных, шифрования и аутентификации.

2.2 Конструктивное исполнение

В данном разделе описано конструктивное исполнение устройства. Представлены изображения передней, задней и боковых панелей устройства. Описаны разъемы, светодиодные индикаторы и органы управления.

Устройство выполнено в металлическом корпусе с возможностью установки в 19" конструктив, высота корпуса 1U.

⚠ Спутниковые маршрутизаторы EVT-101 и EVS-101 не отличаются конструктивом.

2.2.1 Передняя панель устройства EVT-101/EVS-101

Внешний вид передней панели EVT-101/EVS-101 показан на рисунке 1.

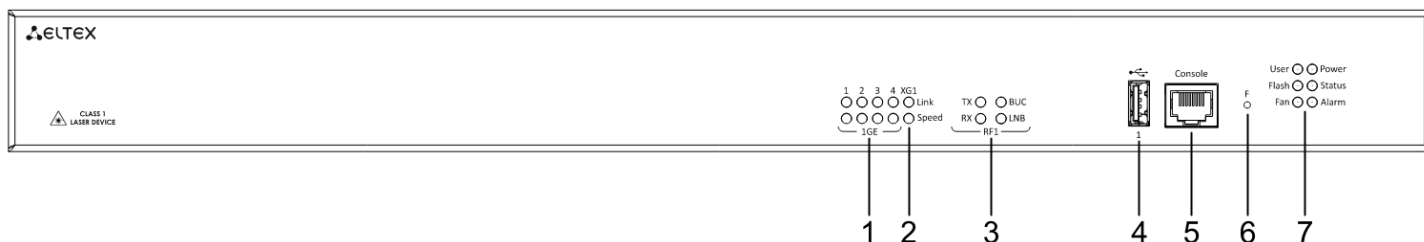


Рисунок 1 – Передняя панель EVT-101/EVS-101

В таблице 1 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели EVT-101/EVS-101.

Таблица 1 – Описание разъемов, индикаторов и органов управления передней панели EVT-101/EVS-101

№	Элемент передней панели	Описание
1	[1 .. 4] Link	4 светодиода Ethernet 10/100/1000BASE-T (RJ-45).
	[1 .. 4] Speed	4 светодиода Ethernet 10/100/1000BASE-T (RJ-45).
2	1 Link	1 светодиод 10GBASE-R (SPF+)/1000BASE-X (SFP).
	1 Speed	1 светодиод 10GBASE-R (SPF+)/1000BASE-X (SFP).
3	TX	Индикатор работы передатчика Tx (N-type).
	RX	Индикатор работы приёмника Rx (N-type).
	BUC	Индикатор работы BUC передней панели.
	LNB	Индикатор работы LNB передней панели.
4	USB1	Разъем USB 2.0 для подключения внешних USB-устройств.
5	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
6	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: - при удержании кнопки менее 10 секунд происходит перезагрузка устройства; - при удержании кнопки более 10 секунд происходит перезагрузка устройства и сброс к заводским настройкам.

№	Элемент передней панели	Описание
7	User	Индикатор, использующийся для пользовательских сценариев, которые можно назначить в режиме конфигурирования устройства.
	Flash	Индикатор карты.
	Fan	Индикатор вентиляторов.
	Power	Индикатор питания устройства.
	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.

2.2.2 Задняя панель устройства EVT-101/EVS-101

Внешний вид задней панели EVT-101/EVS-101 показан на рисунке 2.

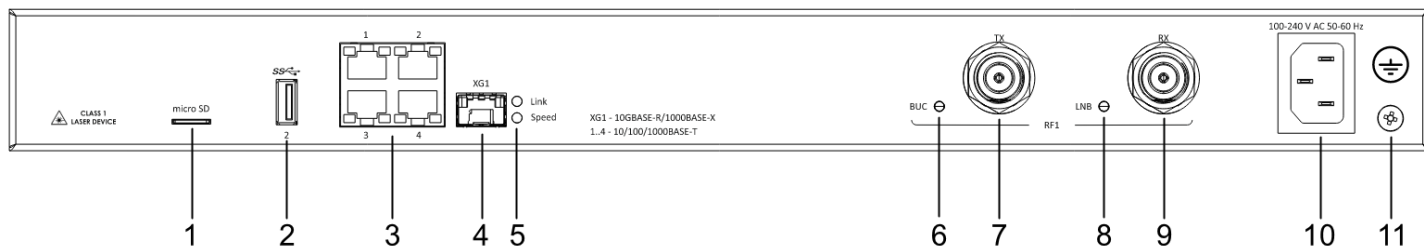


Рисунок 2 – Задняя панель EVT-101/EVS-101

В таблице 2 приведен перечень разъемов, расположенных на задней панели EVT-101/EVS-101.

Таблица 2 – Описание разъемов, индикаторов и органов управления задней панели EVT-101/EVS-101

№	Элемент задней панели	Описание
1	micro SD	Разъем для установки microSD-карт памяти.
2	USB2	Разъем USB 3.0 для подключения внешних USB-устройств.
3	[1 .. 4]	4 порта Ethernet 10/100/1000BASE-T (RJ-45).
4	XG1	1 порт 10GBASE-R (SFP+)/1000BASE-X (SFP).
5	1 Link 1 Speed	1 светодиод 10GBASE-R (SFP+)/1000BASE-X (SFP). 1 светодиод 10GBASE-R (SFP+)/1000BASE-X (SFP).
6	BUC	Индикатор работы BUC задней панели.
7	TX	Радиочастотный разъём для подключения BUC (Tx, N-type).
8	LNB	Индикатор работы LNB задней панели.
9	RX	Радиочастотный разъём для подключения LNB (Rx, N-type).
10	100-240 V AC 50-60 Hz	Источник питания.
11	Клемма	Клемма для заземления устройства.

2.2.3 Боковые панели устройства EVT-101/EVS-101

Внешний вид боковых панелей EVT-101/EVS-101 приведен на рисунках 3 и 4.

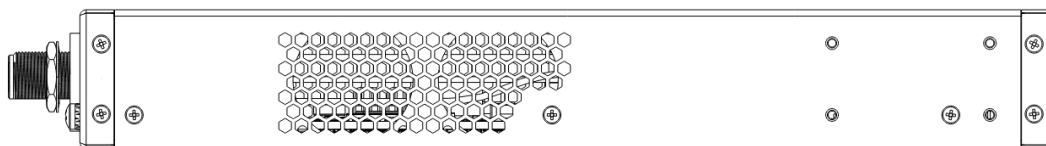


Рисунок 3 – Левая боковая панель EVT-101/EVS-101

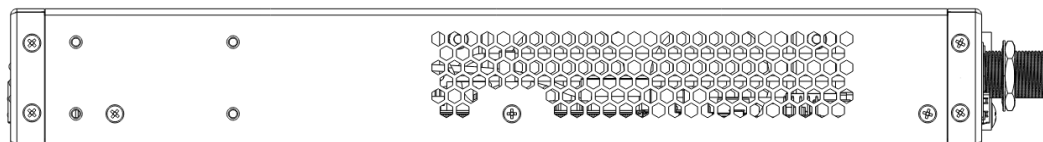


Рисунок 4 – Правая боковая панель EVT-101/EVS-101

На боковых панелях устройства расположены вентиляционные решетки, которые служат для отвода тепла. Не закрывайте вентиляционные отверстия посторонними предметами. Это может привести к перегреву компонентов устройства и вызвать нарушения в его работе.

- ✓ Рекомендации по установке устройства расположены в [Руководстве по установке и монтажу устройства](#).

2.3 Световая индикация EVT-101/EVS-101

Состояние интерфейсов Ethernet отображается двумя светодиодными индикаторами – *LINK/ACT* зеленого цвета и *SPEED* янтарного цвета.

Таблица 3 – Световая индикация состояния интерфейсов Ethernet

Свечение индикатора <i>SPEED</i>	Свечение индикатора <i>LINK/ACT</i>	Состояние интерфейса Ethernet
Выключен	Выключен	Порт выключен или соединение не установлено.
Выключен	Горит постоянно зелёным	Установлено соединение на скорости 10 или 100 Мбит/с.
Горит постоянно янтарным	Горит постоянно зелёным	Установлено соединение на скорости 1000 Мбит/с.
X	Мигает	Идет передача данных.

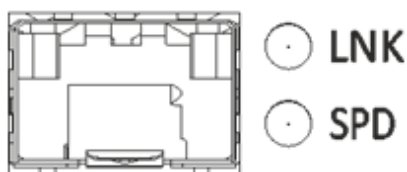


Рисунок 5 – Расположение индикаторов состояния SFP/SFP+-интерфейсов

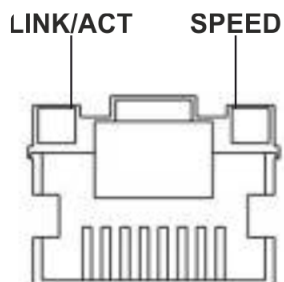


Рисунок 6 – Расположение индикаторов разъема RJ-45

В таблице 4 приведено описание состояний системных индикаторов устройства и их значений.

Таблица 4 – Состояния системных индикаторов

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Power	Индикатор питания устройства.	Зеленый	Питание устройства в норме. Источник питания работает нормально, основное ПО прогружено.
		Красный	Не прогружено основное ПО.
		Выключен	Отказ внутренних источников питания устройства.
Status	Индикатор текущего состояния устройства.	Зеленый	Устройство работает нормально.
		Мигает зеленым	Устройство находится в состоянии загрузки ПО.
Alarm	Индикатор наличия и уровня аварии устройства.	-	-
User	Индикатор, использующийся для пользовательских сценариев, которые можно назначить в режиме конфигурирования устройства.	-	-
Flash	Индикатор активности обмена с накопителем данных: SD-картой или USB Flash.	Зеленый	Выполнение операций чтения/записи по команде «сору».

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Fan	Состояние вентилятора охлаждения	Выключен	Все вентиляторы исправны.
		Красный	Отказ одного или более вентиляторов. Причиной возникновения аварии может быть неработоспособность хотя бы одного из вентиляторов – остановка или пониженная частота оборотов.
TX	Индикатор работы модулятора	Зеленый	Интерфейс satellite-modulator в активном состоянии, включена передача на модуляторе, либо любой тестовый режим.
		Моргает зелёным	Идет передача трафика на модуляторе.
		Выключен	Интерфейс satellite-modulator отключен, передача на модуляторе выключена.
RX	Индикатор работы демодулятора	Зеленый	Интерфейс satellite-demodulator в активном состоянии, есть захват сигнала по приёму на демодуляторе/на всех демодуляторах (EVT-101/EVS-101).
		Моргает зелёным	Идет передача трафика на демодуляторе/демодуляторах (EVT-101/EVS-101).

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
		Выключен	Интерфейс/интерфейсы (EVT-101/EVS-101) satellite-demodulator отключен/отключены.
		Красный	Интерфейс satellite-demodulator/один из интерфейсов satellite-demodulator (EVT-101/EVS-101) в активном состоянии, но нет захвата сигнала по приёму.
BUC	Индикатор работы BUC передней панели	Зеленый	Напряжение питания включено, BUC работает штатно.
		Выключен	Напряжение питания выключено.
		Красный	Напряжение питания отключено, сработала аварийная защита по питанию BUC.
LNB	Индикатор работы LNB передней панели	Зеленый	Напряжение питания включено, LNB работает штатно.
		Выключен	Напряжение питания выключено.
		Красный	Напряжение питания отключено, сработала аварийная защита по питанию LNB.
BUC	Индикатор работы BUC задней панели	Выключен	Напряжение питания выключено.
		Красный	Напряжение питания включено, подаётся на центральную жилу радиочастотного разъёма TX.
LNB	Индикатор работы LNB задней панели	Выключен	Напряжение питания выключено.

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
		Красный	Напряжение питания включено, подаётся на центральную жилу радиочастотного разъёма RX.

2.4 Основные технические характеристики

Основные технические параметры маршрутизаторов EVT-101 и EVS-101 приведены в таблице 5.

Таблица 5 – Основные технические характеристики EVT-101 и EVS-101

Наименование параметра	Значение		
	EVT-101		EVS-101
Параметры приёмо-передающего тракта			
Поддерживаемые режимы работы	SCPC	MCPC-TERMINAL	MCPC-HUB
Диапазон рабочих частот	от 950 до 2150 МГц с шагом 100 Гц		
Диапазон символьных скоростей	от 0,512 до 72 Мсим/с с шагом 1 сим/с	- по передаче: от 0,512 до 4,75 Мсим/с с шагом 1 сим/с - по приёму: от 0,512 до 72 Мсим/с с шагом 1 сим/с	- прямой канал: от 0,512 до 72 Мсим/с с шагом 1 сим/с - обратный канал: от 0,512 до 4,75 Мсим/с с шагом 1 сим/с
Количество каналов	1 прямой канал 1 обратный канал		1 прямой канал 4 обратных канала
Виды модуляции	QPSK, OQPSK, 8PSK, 16APSK, 32APSK, 64APSK	- по передаче: QPSK, 8PSK, 16APSK, 32APSK - по приёму: QPSK, 8PSK, 16APSK, 32APSK, 64APSK	- прямой канал: QPSK, 8PSK, 16APSK, 32APSK, 64APSK - обратный канал: QPSK, 8PSK, 16APSK; 32APSK
Уровень выходного сигнала	от -41,95 дБм до 0 дБм с шагом 0,05 дБм		
Динамический диапазон входного сигнала	от -75 до -5 дБм		

Максимально допустимая частотная расстройка входного сигнала, % от символьной скорости	от минус 20 до плюс 20 (более 5 Мсим/с) от минус 10 до плюс 10 (менее 5 Мсим/с)		
Максимальная скорость доплеровского изменения частоты на входе	не более 7 кГц/с		
Размер кадра, бит	64800, 16200	• по передаче: 16200 • по приёму: 16200, 64800	• прямой канал: 16200; 64800 • обратный канал: 16200
Коэффициент спада фильтра приподнятого косинуса, %	5, 10, 15, 20, 25, 35		
Поддержка инверсии спектра	Есть (автоматически доступна на демодуляторе, на модуляторе необходимо сконфигурировать)		
Электропитание BUC	24 В, до 4 А		
Электропитание LNB	13, 18, 24 В, до 0,5 А		
Синхронизация BUC, LNB	10 МГц, 0 дБм		
Параметры интерфейсов			
Интерфейсы	4 × Ethernet 10/100/1000BASE-T (RJ-45) 1 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) 1 × USB 3.0 1 × USB 2.0 1 × Слот для microSD-карты 1 × IF Tx (N-type) 1 × IF Rx (N-type)		
Типы оптических трансиверов	1000BASE-X SFP 10GBASE-R SFP+		
Дуплексный и полудуплексный режимы интерфейсов	• дуплексный и полудуплексный режимы для электрических портов • дуплексный режим для оптических портов		
Скорость передачи данных	• электрические интерфейсы 10/100/1000 Мбит/с • оптические интерфейсы 1/10 Гбит/с		
Количество VPN-туннелей	250		
Количество статических маршрутов	11k		

Максимальное количество конкурентных сессий	3,26М
Таблица VLAN	4094
Количество маршрутов BGPv4/BGPv6	2,5М
Количество маршрутов OSPFv2/OSPFv3/IS-IS	300k
Количество маршрутов RIP/RIPng	10k
Размер базы FIB	1,4М
VRF	32
Количество L3-интерфейсов	4000
Соответствие стандартам	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-T Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z Fiber Gigabit Ethernet IEEE 802.3cc 25GBASE-LR Ethernet IEEE 802.3by 25GBASE-SR Ethernet IEEE 802.3ba 40GBASE-SR4, 40GBASE-LR4 ANSI/IEEE 802.3 автоопределение скорости IEEE 802.3x контроль потоков данных IEEE 802.3ad объединение каналов LACP IEEE 802.1Q виртуальные локальные сети VLAN IEEE 802.1v, IEEE 802.3ac, IEEE 802.3ae, IEEE 802.1D, IEEE 802.1w, IEEE 802.1s
Управление	
Локальное управление	CLI
Удаленное управление	Telnet, SSH, SNMP
Физические характеристики и условия окружающей среды	
Источники питания	Сеть переменного тока: 230 В, 50 Гц
Максимальная потребляемая мощность	100 Вт (без BUC, LNB)
Масса	4,5 кг

Габаритные размеры (Ш × В × Г)	440 × 44 × 330 мм
Интервал рабочих температур	от 0 до +40 °C
Интервал температуры хранения	от -40 до +70 °C
Относительная влажность при эксплуатации (без образования конденсата)	не более 80 %
Относительная влажность при хранении (без образования конденсата)	от 10 до 95 %
Срок службы	не менее 10 лет

2.4.1 Характеристики помехоустойчивости

Таблица 6 – Характеристики помехоустойчивости EVT-101 и EVS-101

Es/N0, дБ при BER≤10 ⁻⁸ (normal frame/short frame)							
	1/2	2/3	3/4	4/5	5/6	8/9	9/10
QPSK/OQPSK	2,4/2,8	3,5/3,9	4,4/4,4	4,9/5,3	5,4/5,8	6,4/6,8	6,5
8PSK	-	6,9/7,3	8,0/8,4	-	9,5/9,9	10,7/11,1	11,0
16APSK	-	9,7/10,1	10,4/10,8	11,1/11,5	11,6/12,0	12,9/13,2	13,1
32APSK	-	-	13,2/13,6	13,9/14,3	14,5/14,9	15,9/16,3	16,1
64APSK	-	-	-	16,5	17,1	-	-

2.5 Функции устройств

- Передача и прием данных по радиоканалу с использованием ИСЗ в соответствии со стандартом DVB-S2х.
- Коммутация пакетов информации на основе пакетов информации типа кадр.
- Маршрутизация пакетов информации, обеспечивающие формирование и обновление таблиц маршрутизации в ручном или автоматическом режиме. Формирование и обновление таблиц маршрутизации в автоматическом режиме осуществляется посредством протоколов маршрутизации.

2.5.1 Стандарты, протоколы и сервисы

В оборудовании реализованы следующие стандарты, протоколы и сервисы:

Таблица 7 – Стандарты, протоколы, сервисы EVT-101 и EVS-101

Стандарт/протокол/сервис	Спецификации
Стандарт DVB-S2, DVB-S2x	ETSI EN 302 307-1, ETSI EN 302 307-2, ETSI TR 102 376-1, ETSI TR 102 376-2
Стандарт GSE	ETSI TS 102 606-1
IP-протоколы передачи пакетов	RFC 791 Internet Protocol (IPv4)
Протокол ICMP	RFC 792 Internet Control Message Protocol
Протокол разрешения адресов ARP в соответствии с пп.3 пункта 5 Правил	RFC 826 An Ethernet Address Resolution Protocol
Протокол OSPF (Open Shortest Path First)	RFC 2328. OSPF Version 2 RFC 6549. OSPFv2 Multi-Instance Extensions ISO/IEC 10589:2002. Intermediate System to Intermediate System intra-domain routing information exchange protocol
Протокол RIP (Routing Information Protocol)	RFC 2453. RIP Version 2
Протокол BGP (Border Gateway Protocol)	RFC 4271. A Border Gateway Protocol 4 (BGP-4) RFC 3260. New Terminology and Clarifications for Diffserv
DHCP сервер и клиент	RFC 2130 Dynamic Host Configuration Protocol
NAT (Network Address Translation)	RFC 3022 Traditional IP Network Address Translator (Traditional NAT)
TCP/IP	RFC 1122 и RFC 1123

2.5.2 Функции интерфейсов

В таблице 8 приведен список функций интерфейсов устройств.

Таблица 8 – Функции интерфейсов EVT-101 и EVS-101

Определение полярности подключения кабеля (Auto MDI/MDIX)	Автоматическое определение типа кабеля – перекрестный кабель или кабель прямого подключения. - MDI (Medium Dependent Interface – прямой) – стандарт кабелей для подключения оконечных устройств; - MDIX (Medium Dependent Interface with Crossover – перекрестный) – стандарт кабелей для подключения концентраторов и коммутаторов.
Поддержка обратного давления (Back pressure)	Метод обратного давления используется на полудуплексных соединениях для регулирования потока данных от встречного устройства путем создания коллизий. Метод позволяет избежать переполнения буферной памяти устройства и потери данных.

Агрегирование каналов (LAG, Link aggregation)	Агрегирование (объединение) каналов позволяет увеличить пропускную способность канала связи и повысить его надежность. Маршрутизаторы поддерживают статическое и динамическое агрегирование каналов. При динамическом агрегировании используется протокол LACP для управления группой каналов.

2.5.3 Функции при работе с MAC-адресами

Таблица 9 – Функции работы с MAC-адресами

Таблица MAC-адресов	Таблица MAC-адресов устанавливает соответствие между MAC-адресами и интерфейсами устройства и используется для маршрутизации пакетов данных. Маршрутизаторы имеют таблицу емкостью до 128k MAC-адресов и резервируют определенные MAC-адреса для использования системой.
Режим обучения	MAC-таблица может содержать либо статические адреса, либо адреса, изученные при прохождении пакетов данных через устройство. Изучение происходит за счет регистрации MAC-адресов отправителей пакетов с привязкой их к портам и VLAN. Впоследствии эти данные используются для маршрутизации встречных пакетов. Время хранения зарегистрированных MAC-адресов ограничено, его продолжительность может настраиваться администратором. Если MAC-адрес получателя, указанный в принятом устройством пакете, отсутствует в таблице, то такой пакет отправляется далее как широковещательный в пределах L2-сегмента сети.

2.5.4 Функции второго уровня сетевой модели OSI

Таблица 10 – Описание функций второго уровня (Layer 2 OSI)

Поддержка VLAN	VLAN (Virtual Local Area Network) – это средство разделения сети на изолированные сегменты на уровне L2. Использование VLAN позволяет повысить устойчивость работы крупных сетей за счет деления их на более мелкие сети, изолировать разнородный трафик данных между собой и решить многие другие задачи. Маршрутизаторы поддерживают различные способы организации VLAN: • VLAN на базе меток пакетов данных, в соответствии с IEEE 802.1Q; • VLAN на базе портов устройства (port-based); • VLAN на базе использования правил классификации данных (policy-based).

2.5.5 Функции третьего уровня сетевой модели OSI

Таблица 11 – Описание функций третьего уровня (Layer 3 OSI)

Статические IP-маршруты	Администратор маршрутизатора имеет возможность добавлять и удалять статические записи в таблицу маршрутизации.
Динамическая маршрутизация	Протоколы динамической маршрутизации позволяют устройству обмениваться маршрутной информацией с соседними маршрутизаторами и автоматически составлять таблицу маршрутов. Маршрутизатор поддерживает следующие протоколы: RIPv2, RIPv6, OSPFv2, OSPFv3, IS-IS, BGP.

Таблица ARP	ARP (Address Resolution Protocol) – протокол для выяснения соответствия адресов сетевого и канального уровней. Таблица ARP содержит информацию об изученном соответствии. Соответствие устанавливается на основе анализа ответов от сетевых устройств, адреса устройств запрашиваются с помощью широковещательных пакетов.
Клиент DHCP	Протокол DHCP (Dynamic Host Configuration Protocol) даёт возможность автоматизировать управление сетевыми устройствами. Клиент DHCP позволяет маршрутизатору получать сетевой адрес и дополнительные параметры от внешнего DHCP-сервера. Этот способ используется для получения сетевых настроек оператора публичной сети (WAN).
Сервер DHCP	Сервер DHCP предназначен для автоматизации и централизации конфигурирования сетевых устройств. Размещение DHCP-сервера на маршрутизаторе позволяет получить законченное решение для поддержки локальной сети. DHCP-сервер, входящий в состав маршрутизатора, позволяет назначать IP-адреса сетевым устройствам и передавать дополнительные сетевые параметры – адреса серверов, адреса шлюзов сети и другие необходимые параметры.
DHCP Relay	Функция DHCP Relay предназначена для перенаправления широковещательных DHCP Discover-пакетов из одного широковещательного домена в одноадресные (unicast) DHCP Discover-пакеты в другом широковещательном домене.
Трансляция сетевых адресов (NAT, Network Address Translation)	Трансляция сетевых адресов – это механизм, который позволяет преобразовывать IP-адреса и номера портов транзитных пакетов. Функция NAT позволяет использовать меньшее количество IP-адресов, транслируя несколько IP-адресов внутренней сети в один внешний публичный IP-адрес. Использование NAT позволяет увеличить защищённость локальной сети за счёт скрытия её внутренней структуры. Маршрутизаторы поддерживают следующие варианты NAT: • Source NAT (SNAT) – выполняется замена адреса, а также номера порта источника при прохождении пакета в одну сторону и обратной замене адреса назначения в ответном пакете; • Destination NAT (DNAT) – когда обращения извне транслируются маршрутизатором на компьютер пользователя в локальной сети, имеющий внутренний адрес и потому недоступный извне сети непосредственно (без NAT).

2.5.6 Функции туннелирования трафика

Таблица 12 – Функции туннелирования трафика

Протоколы туннелирования	Туннелирование – это способ преобразования пакетов данных при передаче их по сети, при котором происходит замена, модификация или добавление нового сетевого заголовка пакета. Такой способ может быть использован для согласования транспортных протоколов при прохождении данных через транзитную сеть, для создания защищенных соединений, при которых туннелированные данные подвергаются шифрованию. Маршрутизаторы поддерживают следующие виды туннелей: • GRE – инкапсуляция IP-пакета/Ethernet-кадра в другой IP-пакет с добавлением GRE (General Routing Encapsulation)-заголовка; • IPsec – туннель с шифрованием передаваемых данных;

2.5.7 Функции управления и конфигурирования

Таблица 13 – Основные функции управления и конфигурирования

Загрузка и выгрузка файла настройки	Параметры устройства сохраняются в файле настройки, который содержит данные конфигурации как всей системы в целом, так и определенного порта устройства. Для передачи файлов могут использоваться протоколы TFTP, FTP, SCP.
Интерфейс командной строки (CLI)	Управление посредством CLI осуществляется локально через последовательный порт RS-232 либо удаленно через Telnet, SSH. Интерфейс командной строки консоли (CLI) является промышленным стандартом. Интерпретатор CLI предоставляет список команд и ключевых слов для помощи пользователю и сокращению объема вводимых данных.
Syslog	Протокол Syslog обеспечивает передачу информационных сообщений о происходящих в системе событиях и ведение журнала событий.
Сетевые утилиты ping, traceroute	Утилиты ping и traceroute – предназначены для проверки доступности сетевых устройств и для определения маршрутов передачи данных в IP-сетях.
Управление контролируемым доступом – уровни привилегий	Маршрутизаторы поддерживают управление уровнем доступа пользователей к системе. Уровни доступа позволяют управлять зонами ответственности администраторов устройств. Уровни доступа нумеруются от 1 до 15, уровень 15 соответствует полному доступу к управлению устройством.
Аутентификация	Аутентификация – это процедура проверки подлинности пользователя. Маршрутизаторы поддерживают следующие методы аутентификации: • локальная – для аутентификации используется локальная база данных пользователей, хранящаяся на самом устройстве; • групповая – база данных пользователей хранится на сервере аутентификации. Для взаимодействия с сервером используются протоколы RADIUS и TACACS.
Сервер SSH/сервер Telnet	Функции сервера SSH и Telnet позволяют установить соединение с устройством для управления им.

Автоматическое восстановление конфигурации	Устройство поддерживает автоматическую систему восстановления конфигурации, которая предотвращает ситуации потери удаленного доступа к устройству после смены конфигурации. Если в течение заданного времени после изменения конфигурации не было введено подтверждение – произойдет автоматический откат конфигурации до предыдущего использовавшегося состояния.

2.5.8 Функции сетевой защиты

Таблица 14 – Функции сетевой защиты

Зоны безопасности	Все интерфейсы маршрутизатора распределяются по зонам безопасности. Для каждой пары зон настраиваются правила, определяющие возможность или невозможность прохождения данных между зонами, правила фильтрации трафика данных.
Фильтрация данных	Для каждой пары зон безопасности составляется набор правил, которые позволяют управлять фильтрацией данных, проходящих через маршрутизатор. Командный интерфейс устройства предоставляет средства для детальной настройки правил классификации трафика и для назначения результирующего решения о пропуске трафика.

2.6 Комплект поставки

В комплект поставки EVT-101 входят:

- маршрутизатор спутниковый EVT-101;
- комплект крепежа в стойку;
- шнур питания евровилка-С13-F-1.8м;
- консольный кабель;
- руководство по эксплуатации на CD-диске (опционально);
- памятка о документации;
- паспорт.

В комплект поставки EVS-101 входят:

- маршрутизатор спутниковый EVS-101;
- комплект крепежа в стойку;
- шнур питания евровилка-С13-F-1.8м;
- консольный кабель;
- руководство по эксплуатации на CD-диске (опционально);
- памятка о документации;
- паспорт.

3 Интерфейсы управления

- Интерфейс командной строки (CLI)
- Типы и порядок именования интерфейсов маршрутизатора
- Типы и порядок именования туннелей маршрутизатора

Для управления устройствами через интерфейс командной строки CLI используется сетевое подключение по протоколам Telnet и SSH или прямое подключение через консольный порт, соответствующий спецификации RS-232.

Мониторинг также может осуществляться через SNMP: взаимодействие через этот интерфейс описано в отдельном руководстве «EVT-101, EVS-101. Мониторинг и управление маршрутизаторами по SNMP».

3.1 Интерфейс командной строки (CLI)

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 протоколам Telnet, SSH или прямое подключение через консольный порт (например, HyperTerminal).

Интерфейс командной строки обеспечивает авторизацию пользователей и ограничивает их доступ к командам на основании уровня доступа, заданного администратором.

В системе может быть создано необходимое количество пользователей, права доступа задаются индивидуально для каждого из них.

Для обеспечения безопасности командного интерфейса все команды разделены на две категории – привилегированные и непривилегированные. К привилегированным в основном относятся команды конфигурирования. К непривилегированным – команды мониторинга.

Система позволяет нескольким пользователям одновременно подключаться к устройству.

При использовании интерфейса командной строки должна соблюдаться определенная, описанная здесь, последовательность изменения и применения конфигурации, позволяющая защитить устройство от некорректного конфигурирования.

3.2 Типы и порядок именования интерфейсов маршрутизатора

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 14 – Типы и порядок именования интерфейсов маршрутизатора

Тип интерфейса	Обозначение
Физические интерфейсы	Обозначение физического интерфейса включает в себя его тип и идентификатор. Идентификатор физических интерфейсов имеет вид <UNIT>/<SLOT>/<PORT>, где: • <UNIT> – номер устройства в группе устройств, • <SLOT> – номер модуля в составе устройства или 0 при отсутствии деления устройства на модули, • <PORT> – порядковый номер порта.

Тип интерфейса	Обозначение
Порты 1 Гбит/с	gigabitethernet <UNIT>/<SLOT>/<PORT> Пример обозначения: gigabitethernet 1/0/3  Допускается использовать сокращенное наименование, например gi1/0/3.
Порты 10 Гбит/с	tengigabitethernet <UNIT>/<SLOT>/<PORT> Пример обозначения: tengigabitethernet 1/0/1  Допускается использовать сокращенное наименование, например te1/0/1.
Группы агрегации каналов	Обозначение группы агрегации каналов включает в себя его тип и порядковый номер интерфейса: port-channel <CHANNEL_ID> Пример обозначения: port-channel 6  Допускается использовать сокращенное наименование, например po1.
Саб-интерфейсы	Обозначение саб-интерфейса образуется из обозначения базового интерфейса и идентификатора (VLAN) саб-интерфейса, разделенных точкой. Примеры обозначений: • gigabitethernet 1/0/3.100 • tengigabitethernet 1/0/1.123 • port-channel 1.6  Идентификатор саб-интерфейса может принимать значения [2..4094].
Q-in-Q интерфейсы	Обозначение Q-in-Q интерфейса образуется из обозначения базового интерфейса, идентификатора сервисного VLAN и идентификатора пользовательского VLAN, разделенных точкой. Примеры обозначений: • gigabitethernet 1/0/3.100.10 • tengigabitethernet 1/0/1.45.12 • port-channel 1.6.34  Идентификатор сервисного и пользовательского VLAN может принимать значения [1..4094].

Тип интерфейса	Обозначение
Логические интерфейсы	Обозначение логического интерфейса является порядковым номером интерфейса: Примеры обозначений: • loopback 4 • bridge 60
Интерфейсы satellite	Обозначение satellite интерфейса включает в себя его тип и идентификатор. Идентификатор satellite интерфейсов имеет вид <UNIT>/<RADIOFREQ>/<MOD> <DEMOD> <CHAN>}, где: • <UNIT> – номер устройства в группе устройств, • <RADIOFREQ> – номер радиочастотного канала, • <MOD> <DEMOD> <CHAN> – порядковый номер модулятора демодулятора канала.

-  1. Количество интерфейсов каждого типа зависит от модели маршрутизатора.
2. Некоторые команды поддерживают одновременную работу с группой интерфейсов. Для указания группы интерфейсов может быть использовано перечисление через запятую или указание диапазона идентификаторов через дефис «-».
- Примеры указания групп интерфейсов:

```
interface gigabitethernet 1/0/1, gigabitethernet 1/0/3
interface gigabitethernet 1/0/1-2
interface gil/0/1-3, gil/0/4, tel/0/1, fo1/0/1
```

3.3 Типы и порядок именования туннелей маршрутизатора

При работе маршрутизаторов используются сетевые туннели различного типа и назначения. Система именования позволяет однозначно адресовать туннели по их функциональному назначению. Далее в таблице приведен перечень типов туннелей.

В данной модели используется сетевой туннель GRE.

Таблица 15 – Типы и порядок именования туннелей маршрутизатора

Тип туннеля	Обозначение
GRE-туннель	Обозначение GRE-туннеля состоит из обозначения типа и порядкового номера туннеля: gre <GRE_ID> Пример обозначения: gre 1

-  Количество туннелей каждого типа зависит от модели и ПО маршрутизатора.

4 Начальная настройка устройств

- Подключение и конфигурирование маршрутизаторов
- Подключение к маршрутизатору
 - Подключение по локальной сети Ethernet
 - Подключение через консольный порт RS-232
 - Применение изменения конфигурации
- Установка лицензии
 - Установка корректной даты на устройство
 - Установка лицензий через USB-накопитель
 - Установка лицензии через TFTP
- Смена режима работы спутникового модема
- Настройка системы логирования событий
 - Пример настройки
- Настройка политики использования паролей
 - Пример настройки
- Настройка политики AAA
 - Пример настройки
- Базовая настройка маршрутизатора
 - Изменение пароля пользователя «admin»
 - Создание новых пользователей
 - Назначение имени устройства
 - Настройка параметров публичной сети
- Настройка удаленного доступа к маршрутизатору
 - Настройка удалённого управления
 - Пример настройки
- Рекомендации по безопасной настройке
- Заводская конфигурация EVT-101/EVS-101

4.1 Подключение и конфигурирование маршрутизаторов

Маршрутизаторы серии EVT и EVS предназначены для построения географически распределённых сетей спутниковой связи класса VSAT.

Базовая настройка маршрутизатора обеспечивает сетевой доступ к устройству по протоколу SSH.

Расширенные настройки зависят от требований конкретной схемы применения устройства и легко могут быть добавлены или изменены с помощью имеющихся интерфейсов управления.

4.2 Подключение к маршрутизатору

Предусмотрены следующие способы подключения к устройству:

4.2.1 Подключение по локальной сети Ethernet

 При первоначальном старте маршрутизатор загружается с заводской конфигурацией. Описание заводской конфигурации приведено в разделе [Заводская конфигурация EVT-101/EVS-101](#) данного руководства.

Подключите сетевой кабель передачи данных (патч-корд) к любому порту.

В заводской конфигурации маршрутизатора активирован DHCP-сервер с пулом IP-адресов в подсети **192.168.1.0/24**.

При подключении сетевого интерфейса управляющего компьютера он должен получить сетевой адрес от сервера.

Если IP-адрес не получен по какой-либо причине, то следует назначить адрес интерфейса вручную, используя любой адрес, кроме 192.168.1.1, в подсети 192.168.1.0/24.

4.2.2 Подключение через консольный порт RS-232

При помощи кабеля RJ-45/DBF9, который входит в комплект поставки устройства, соедините порт «**Console**» маршрутизатора с портом RS-232 компьютера.

Запустите терминальную программу (например, HyperTerminal или Minicom) и создайте новое подключение. Должен быть использован режим эмуляции терминала VT100.

Выполните следующие настройки интерфейса RS-232:

Скорость: 115200 бит/с
Биты данных: 8 бит
Четность: нет
Стоповые биты: 1
Управление потоком: нет

4.2.3 Применение изменения конфигурации

Любые изменения, внесенные в конфигурацию, вступят в действие только после применения команды:

```
evt# commit
Configuration has been successfully committed
```

После применения данной команды запускается таймер «отката» конфигурации. Для остановки таймера и механизма «отката» используется команда:

```
evt# confirm
Configuration has been successfully confirmed
```

Значение таймера «отката» по умолчанию – 600 секунд. Для изменения данного таймера используется команда:

```
evt(config)# system config-confirm timeout <TIME>
```

- <TIME> – интервал времени ожидания подтверждения конфигурации, принимает значение в секундах [120..86400].

Перед началом расширенного конфигурированию рекомендуется очистить базовую конфигурацию командой.

```
evt# copy system:default-config system:candidate-config
```

4.3 Установка лицензии

4.3.1 Установка корректной даты на устройство

Перед загрузкой лицензии необходимо убедиться, что на устройстве установлена корректная дата и время.

1. Установка корректной даты и время:

```
evt-101# set date YYYY-MM-DD HH:MM:SS
```

2. Проверить текущую дату и время командой:

```
evt-101# show date
"2028-01-27 21:05:49"
```

4.3.2 Установка лицензий через USB-накопитель

1. Определить метку тома подключенного USB-накопителя:

```
evt-101# show storage-devices usb
```

Name	Filesystem	Total, MB	Used, MB	Free, MB
<USB_DISK>	vfat	29544.55	383.50	29161.05

⚠ При выполнении команд копирования с USB-носителей необходимо вместо полей <USB_DISK> использовать настоящие метки тома, определенные выше.

2. Скопировать файл на используемый USB-накопитель:

```
evt-101# copy usb://<USB_DISK>:<MCPC-HUB.lic> system:licence
|*****| 100% (1993B) Licence loaded successfully.
```

3. Проверка установки лицензии:

```
evt-101# show licence
```

Feature	Valid from	Expiries	Source	State	Value
MCPC-TERMINAL	--	--	File (v2)	Active	true

4.3.3 Установка лицензии через TFTP

1. Необходимо настроить сетевой интерфейс для доступа к TFTP-серверу:

```
interface gigabitethernet 1/0/4
ip firewall disable
ip address 192.168.32.21/24
exit
```

Убедитесь, что устройство имеет IP-соединение с TFTP-сервером (например, ping 192.168.32.85).

2. Используйте команду copy для загрузки файла лицензии с TFTP-сервера:

```
evs-101# copy tftp://192.168.32.85:/MCPC-HUB.lic system:licence
|*****| 100% (1998B) Licence loaded successfully.
```

3. Проверка установки лицензии:

```

evs-101# sh licence
Feature                               Source      State      Value
Valid from                           Expiries    -----
-----
MCPC-HUB                             File (v2)   Active     true
--

```

4.4 Смена режима работы спутникового модема

Перед установкой режима необходимо установить лицензию соответствующего режима работы спутникового модема.

 Доступно только для устройств EVT.

 Если на устройстве уже активированы несколько лицензий, например, SCPC и MCPC-TERMINAL, необходимо вручную выбрать соответствующий режим работы спутникового модема.

Для этого используется команда:

```

evt-101# set satellite-modem mode
Select satellite-modem mode:
mcpc-terminal
scpc

```

Система предложит выбрать один из доступных режимов:

- mcpc-terminal — режим терминала MCPC;
- scpc — режим SCPC.

Пример выбора режима **MCPC-Terminal**:

```

evt-101# set satellite-modem mode mcpc-terminal

```

Система выведет предупреждение:

```

Warning: factory configuration will be applied after system reboot
Do you still want to change satellite-modem mode? (y/N): y

```

Подтвердите действие, введя «у», если уверены в необходимости смены режима. После подтверждения устройство необходимо перезагрузить для применения изменений.

 Переключение режима модема приводит к сбросу текущей конфигурации до заводских настроек после перезагрузки.

4.5 Настройка системы логирования событий

Рекомендации:

- Настроить хранение сообщений о событиях в файл syslog на устройстве и передачу этих событий на внешний syslog-сервер;
- Ограничить размер syslog-файла на устройстве;
- Настроить ротацию syslog-файлов на устройстве;
- Включить нумерацию сообщений syslog.



Данные, хранящиеся в файловой системе tmpsys:syslog, не сохраняются при перезагрузке устройства. Этот тип файловой системы рекомендуется использовать для хранения оперативных логов.

Не рекомендуется использовать файловую систему flash:syslog для хранения логов, так как это может привести к преждевременному выходу из строя устройств.

4.5.1 Пример настройки

Задача:

Настроить хранение сообщений о событиях уровня info и выше в файл syslog на устройстве и настроить передачу этих событий на внешний syslog-сервер. Ограничить файл размером 512 Кбайт. Включить ротацию 3 файлов. Включить нумерацию сообщений syslog.

Решение:

1. Настройте хранение syslog-сообщений в файле:

```
evt(config)# syslog file tmpsys:syslog/default
evt(config-syslog-file)# severity info
evt(config-syslog-file)# exit
```

2. Настройте ограничение размера и ротацию файлов:

```
evt(config)# syslog max-files 3
evt(config)# syslog file-size 512
```

3. Настройте передачу сообщений на внешний сервер:

```
evt(config)# syslog host mylog
evt(config-syslog-host)# remote-address 92.168.1.2
evt(config-syslog-host)# transport udp
evt(config-syslog-host)# port 514
evt(config-syslog-host)# severity info
evt(config-syslog-host)# exit
```

4. Включите нумерацию сообщений syslog:

```
evt(config)# syslog sequence-numbers
```

4.6 Настройка политики использования паролей

Рекомендации:

- Всегда включать требования на смену пароля по умолчанию пользователя admin;
- Ограничивать время жизни паролей и запрещать повторно использовать, как минимум, предыдущий пароль;
- Выставлять требования минимальной длины пароля больше 8 символов;
- Выставлять требования на использование строчных и прописных букв, цифр и спецсимволов.

4.6.1 Пример настройки

Задача:

Настроить парольную политику с обязательным требованием смены пароля по умолчанию, временем действия пароля 1 месяц и запретом на использование 12 последних паролей.

Задать минимальную длину пароля 16 символов, максимальную — 64 символа.

Пароль должен содержать не менее 3 прописных букв, не менее 5 строчных букв, не менее 4 цифр и не менее 2 спецсимволов. Пароль в обязательном порядке должен содержать все 4 типа символов.

Решение:

1. Включите запрос на смену пароля по умолчанию для пользователя admin:

```
evs(config)# security passwords default-expired
```

2. Установите время жизни пароля 30 дней и запрет на использование предыдущих 12 паролей:

```
evs(config)# security passwords lifetime 30
evs(config)# security passwords history 12
```

3. Установите ограничения на длину пароля:

```
evs(config)# security passwords min-length 16
evs(config)# security passwords max-length 64
```

4. Установите ограничения по минимальному количеству символов соответствующих типов:

```
evs(config)# security passwords upper-case 3
evs(config)# security passwords lower-case 5
evs(config)# security passwords special-case 2
evs(config)# security passwords numeric-count 4
evs(config)# security passwords symbol-types 4
```

4.7 Настройка политики AAA

Рекомендации:

- Использовать ролевую модель доступа на устройство;
- Использовать персональные учетные записи для аутентификации на устройстве;
- Включать логирование вводимых пользователем команд;
- Использовать несколько методов аутентификации для входа на устройства через консоль, удалённого входа на устройства и повышения привилегий. Оптимальной считается комбинация из аутентификации по одному из протоколов RADIUS/TACACS/LDAP и локальной аутентификации;
- Понизить уровень привилегий встроенной учётной записи admin до 1;
- Настроить логирование изменений локальных учётных записей;
- Настроить логирование изменений политики AAA.



Встроенную учётную запись admin удалить нельзя.

Команда по username admin не удаляет пользователя admin, сбрасывает его конфигурацию в значения по умолчанию. После применения этой команды пользователь admin не будет отображаться в конфигурации.

Команда по password для пользователя admin также не удаляет пароль пользователя admin, сбрасывает его в значение по умолчанию. После применения этой команды пароль пользователя admin перестает отображаться в конфигурации и становится 'password'.

Перед установкой пользователю admin пониженных привилегий у вас должен быть настроен пользователь с уровнем привилегий 15 или задан ENABLE-пароль.

4.7.1 Пример настройки

Задача:

Настроить политику AAA:

Для удалённого входа по протоколу SSH использовать аутентификации через RADIUS.

Для входа через локальную консоль использовать аутентификации через RADIUS, в случае отсутствия связи с RADIUS-серверами использовать локальную аутентификацию.

Использовать ENABLE-пароль, заданный через RADIUS, в случае отсутствия связи с RADIUS-серверами использовать локальный ENABLE-пароль.

Установить пользователю admin пониженный уровень привилегий.

Настроить логирование изменений локальных учётных записей.

Настроить логирование изменений политик AAA.

Настроить логирование вводимых команд.

Решение:

1. Создайте локального пользователя local-operator с уровнем привилегий 8:

```
evt(config)# username local-operator
evt(config-user)# password Pa$$w0rd1
evt(config-user)# privilege 8
evt(config-user)# exit
```

2. Задайте локальный ENABLE-пароль:

```
evt(config)# enable password $6e5c4r3e2t!
```

3. Далее необходимо понизить привилегии пользователя admin:

```
evt(config)# username admin
evt(config-user)# privilege 1
evt(config-user)# exit
```

4. Настройте связь с двумя RADIUS-серверами, основным 192.168.1.11 и резервным 192.168.2.12:

```
evt(config)# radius-server host 192.168.1.11
evt(config-radius-server)# key ascii-text encrypted 8CB5107EA7005AFF
evt(config-radius-server)# priority 100
evt(config-radius-server)# exit
evt(config)# radius-server host 192.168.2.12
evt(config-radius-server)# key ascii-text encrypted 8CB5107EA7005AFF
evt(config-radius-server)# priority 150
evt(config-radius-server)# exit
```

5. Настройте политику AAA:

```
evt(config)# aaa authentication login CONSOLE radius local
evt(config)# aaa authentication login SSH radius
evt(config)# aaa authentication enable default radius enable
evt(config)# aaa authentication mode break
evt(config)# line console
evt(config-line-console)# login authentication CONSOLE
evt(config-line-console)# exit
evt(config)# line ssh
evt(config-line-ssh)# login authentication SSH
evt(config-line-ssh)# exit
```

6. Настройте логирование:

```
evt(config)# logging userinfo
evt(config)# logging aaa
evt(config)# syslog cli-commands
```

4.8 Базовая настройка маршрутизатора

Процедура настройки маршрутизатора при первом включении состоит из следующих этапов:

1. Изменение пароля пользователя «admin»;
2. Создание новых пользователей;
3. Назначение имени устройства (Hostname);
4. Установка параметров подключения к публичной сети в соответствии с требованиями провайдера;
5. Настройка удаленного доступа к маршрутизатору;
6. Применение базовых настроек.

4.8.1 Изменение пароля пользователя «admin»

Для защищенного входа в систему необходимо сменить пароль привилегированного пользователя «admin».

 Учетная запись techsupport необходима для удаленного обслуживания сервисным центром; Учетная запись remote – аутентификация RADIUS, TACACS+, LDAP; Удалить пользователей admin, techsupport, remote нельзя. Можно только сменить пароль и уровень привилегий.

 Если информация о пользователе «admin» не отображается в конфигурации, значит параметры данного пользователя настроены по умолчанию (пароль «password», уровень привилегий 15).

Имя пользователя и пароль вводится при входе в систему во время сеансов администрирования устройства.

Для изменения пароля пользователя «admin» используются следующие команды:

```
evs# configure
evs(config)# username admin
evs(config-user)# password <new-password>
evs(config-user)# exit
```

4.8.2 Создание новых пользователей

Для создания нового пользователя системы или настройки любого из параметров: имени пользователя, пароля, уровня привилегий, – используются команды:

```
evs(config)# username <name>
evs(config-user)# password <password>
evs(config-user)# privilege <privilege>
evs(config-user)# exit
```

 Уровни привилегий 1–9 разрешают доступ к устройству и просмотр его оперативного состояния, но запрещают настройку. Уровни привилегий 10–14 разрешают как доступ, так и настройку большей части функций устройства. Уровень привилегий 15 разрешает как доступ, так и настройку всех функций устройства.

Пример команд для создания пользователя «**fedor**» с паролем «**12345678**» и уровнем привилегий **15** и создания пользователя «**ivan**» с паролем «**password**» и уровнем привилегий **1**:

```
evs# configure
evs(config)# username fedor
evs(config-user)# password 12345678
evs(config-user)# privilege 15
evs(config-user)# exit
evs(config)# username ivan
evs(config-user)# password password
evs(config-user)# privilege 1
evs(config-user)# exit
```


4.8.3 Назначение имени устройства

Для назначения имени устройства используются следующие команды:

```
evs# configure
evs(config)# hostname <new-name>
```

После применения конфигурации приглашение командной строки изменится на значение, заданное параметром **<new-name>**.

4.8.4 Настройка параметров публичной сети

Для настройки сетевого интерфейса маршрутизатора в публичной сети необходимо назначить устройству параметры, определённые провайдером сети – IP-адрес, маска подсети и адрес шлюза по умолчанию.

Пример команд настройки статического IP-адреса для суб-интерфейса **Gigabit Ethernet 1/0/2.150** для доступа к маршрутизатору через **VLAN 150**.

Параметры интерфейса:

- IP-адрес – 192.168.16.144;
- Маска подсети – 255.255.255.0;
- IP-адрес шлюза по умолчанию – 192.168.16.1.

```
evt# configure
evt(config)# interface gigabitethernet 1/0/2.150
evt(config-if-sub)# ip address 192.168.16.144/24
evt(config-if-sub)# exit
evt(config)# ip route 0.0.0.0/0 192.168.16.1
```

Чтобы убедиться, что адрес был назначен интерфейсу, после применения конфигурации введите следующую команду:

```
evt# show ip interfaces
```

IP address	Interface	Admin	Link
Type Precedence			
-----	-----	-----	-----
192.168.16.144/24	gi1/0/2.150	Up	Up
static primary			

Провайдер может использовать динамически назначаемые адреса в своей сети. Для получения IP-адреса может использоваться протокол DHCP, если в сети присутствует сервер DHCP.

Пример настройки, предназначенной для получения динамического IP-адреса от DHCP-сервера на интерфейсе **Gigabit Ethernet 1/0/10**:

```
evt# configure
evt(config)# interface gigabitethernet 1/0/10
evt(config-if)# ip address dhcp
evt(config-if)# exit
```

Чтобы убедиться, что адрес был назначен интерфейсу, введите следующую команду после применения конфигурации:

```

evt# show ip interfaces
IP address      Interface      Admin  Link
Type           Precedence
-----
-----
192.168.11.5/25  gi1/0/10      Up     Up
DHCP            --

```

4.9 Настройка удаленного доступа к маршрутизатору

В заводской конфигурации разрешен удаленный доступ к маршрутизатору по протоколам Telnet или SSH из зоны **«trusted»**. Для того чтобы разрешить удаленный доступ к маршрутизатору из других зон, например, из публичной сети, необходимо создать соответствующие правила в firewall.

При конфигурировании доступа к маршрутизатору правила создаются для пары зон:

- **source-zone** — зона, из которой будет осуществляться удаленный доступ;
- **self** — зона, в которой находится интерфейс управления маршрутизатором.

Для создания разрешающего правила используются следующие команды:

```

evt# configure
evt(config)# security zone-pair <source-zone> self
evt(config-zone-pair)# rule <number>
evt(config-zone-rule)# action permit
evt(config-zone-rule)# match protocol tcp
evt(config-zone-rule)# match source-address <network object-group>
evt(config-zone-rule)# match destination-address <network object-group>
evt(config-zone-rule)# match destination-port object-group <service object-group>
evt(config-zone-rule)# enable
evt(config-zone-rule)# exit
evt(config-zone-pair)# exit

```

Пример команд для разрешения пользователям из зоны «**untrusted**» с IP-адресами **132.16.0.5-132.16.0.10** подключаться к маршрутизатору с IP-адресом **40.13.1.22** по протоколу SSH:

```

evt# configure
evt(config)# object-group network clients
evt(config-addr-set)# ip address-range 132.16.0.5-132.16.0.10
evt(config-addr-set)# exit
evt(config)# object-group network gateway
evt(config-addr-set)# ip address-range 40.13.1.22
evt(config-addr-set)# exit
evt(config)# object-group service ssh
evt(config-port-set)# port-range 22
evt(config-port-set)# exit
evt(config)# security zone-pair untrusted self
evt(config-zone-pair)# rule 10
evt(config-zone-rule)# action permit
evt(config-zone-rule)# match protocol tcp
evt(config-zone-rule)# match source-address clients
evt(config-zone-rule)# match destination-address gateway
evt(config-zone-rule)# match destination-port object-group ssh
evt(config-zone-rule)# enable
evt(config-zone-rule)# exit
evt(config-zone-pair)# exit

```

4.9.1 Настройка удалённого управления

Рекомендации:

- Не рекомендуется включать удалённое управление по протоколу Telnet;
- Рекомендуется использовать криптостойкие алгоритмы аутентификации sha2-512 и отключить все остальные;
- Рекомендуется использовать криптостойкие алгоритмы шифрования aes256ctr и отключить все остальные;
- Рекомендуется использовать криптостойкий алгоритм обмена ключами шифрования dh-group-exchange-sha256 и отключить все остальные;
- Рекомендуется использовать криптостойкий алгоритм верификации Host-Key для SSH rsa и отключить все остальные;
- Рекомендуется разрешить доступ к удалённому управлению устройством только с определённых IP-адресов;
- Перед началом эксплуатации рекомендуется регенерировать ключи шифрования.

4.9.2 Пример настройки

Задача:

Сгенерировать новые ключи шифрования. Использовать криптостойкие алгоритмы.

Решение:

1. Отключите устаревшие и не криптостойкие алгоритмы:

```
evt(config)# ip ssh server
evt(config)# ip ssh authentication algorithm md5 disable
evt(config)# ip ssh authentication algorithm md5-96 disable
evt(config)# ip ssh authentication algorithm ripemd160 disable
evt(config)# ip ssh authentication algorithm sha1 disable
evt(config)# ip ssh authentication algorithm sha1-96 disable
evt(config)# ip ssh authentication algorithm sha2-256 disable
evt(config)# ip ssh encryption algorithm 3des disable
evt(config)# ip ssh encryption algorithm aes128 disable
evt(config)# ip ssh encryption algorithm aes128ctr disable
evt(config)# ip ssh encryption algorithm aes192 disable
evt(config)# ip ssh encryption algorithm aes192ctr disable
evt(config)# ip ssh encryption algorithm aes256 disable
evt(config)# ip ssh encryption algorithm arcfour disable
evt(config)# ip ssh encryption algorithm arcfour128 disable
evt(config)# ip ssh encryption algorithm arcfour256 disable
evt(config)# ip ssh encryption algorithm blowfish disable
evt(config)# ip ssh encryption algorithm cast128 disable
evt(config)# ip ssh key-exchange algorithm dh-group-exchange-sha1 disable
evt(config)# ip ssh key-exchange algorithm dh-group1-sha1 disable
evt(config)# ip ssh key-exchange algorithm dh-group14-sha1 disable
evt(config)# ip ssh key-exchange algorithm ecdh-sha2-nistp256 disable
evt(config)# ip ssh key-exchange algorithm ecdh-sha2-nistp384 disable
evt(config)# ip ssh key-exchange algorithm ecdh-sha2-nistp521 disable
evt(config)# ip ssh host-key algorithm dsa disable
evt(config)# ip ssh host-key algorithm ecdsa256 disable
evt(config)# ip ssh host-key algorithm ecdsa384 disable
evt(config)# ip ssh host-key algorithm ecdsa521 disable
evt(config)# ip ssh host-key algorithm ed25519 disable
```

2. Сгенерируйте новые ключи шифрования:

```
evt# update ssh-host-key rsa 2048
```

4.10 Рекомендации по безопасной настройке

Рекомендации по безопасной настройке носят общий характер и подходят для большинства инсталляций. Настоящие рекомендации в значительной степени повышают безопасность эксплуатации устройства, но не являются исчерпывающими. В зависимости от схемы применения устройства необходимо настраивать и другие параметры безопасности. В некоторых специфических случаях выполнение данных рекомендаций может привести к неработоспособности сети. При настройке устройства стоит в первую очередь следовать техническим требованиям и регламентам сетей, в которых будет эксплуатироваться данное устройство.

Общие рекомендации:

- Рекомендуется всегда отключать неиспользуемые физические интерфейсы с помощью команды shutdown;
- Рекомендуется всегда настраивать синхронизацию системных часов с доверенными источниками сетевого времени (NTP);
- Рекомендуется отключать NTP broadcast client, включённый по умолчанию в заводской конфигурации;
- Не рекомендуется использовать команду ip firewall disable, отключающую межсетевое экранирование. Следует всегда назначать интерфейсам соответствующие зоны безопасности и настраивать корректные правила межсетевого экрана.

4.11 Заводская конфигурация EVT-101/EVS-101

При отгрузке устройства потребителю на маршрутизатор загружена заводская конфигурация, которая включает минимально необходимые настройки, позволяющие получить сетевой доступ к устройству для выполнения расширенного конфигурирования с любого из следующих портов gigabitethernet 1/0/1-1/0/4, tengigabitethernet 1/0/1. Порты переведены в режим коммутации и находятся в одном домене с интерфейсом Bridge 1, на котором сконфигурирован статический IP-адрес 192.168.1.1/24. Созданный IP-интерфейс выступает в качестве IP-адреса для подключения к роутеру по протоколу SSH.

```

syslog max-files 3
syslog file-size 1024
syslog file tmpsys:syslog/default
  severity info
exit

bridge 1
  vlan 1
  ip address 192.168.1.1/24
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
exit
interface gigabitethernet 1/0/2
  mode switchport
exit
interface gigabitethernet 1/0/3
  mode switchport
exit
interface gigabitethernet 1/0/4
  mode switchport
exit
interface tengigabitethernet 1/0/1
  mode switchport
exit

security passwords default-expired

ip firewall disable

ip dhcp-server
ip dhcp-server pool lan-pool
  network 192.168.1.0/24
  address-range 192.168.1.2-192.168.1.254
  default-router 192.168.1.1
  dns-server 192.168.1.1
exit

ip ssh server

```

5 Рекомендации по безопасной настройке

- Общие рекомендации
- Настройка системы логирования событий
 - Рекомендации
 - Предупреждения
 - Пример настройки
- Настройка политики использования паролей
 - Рекомендации
 - Пример настройки
- Настройка политики AAA
 - Рекомендации
 - Предупреждения
 - Пример настройки
- Настройка удалённого управления
 - Рекомендации
 - Пример настройки

Рекомендации по безопасной настройке носят общий характер и подходят для большинства инсталляций. Настоящие рекомендации в значительной степени повышают безопасность эксплуатации устройства, но не являются исчерпывающими. В зависимости от схемы применения устройства необходимо настраивать и другие параметры безопасности. В некоторых специфических случаях выполнение данных рекомендаций может привести к неработоспособности сети. При настройке устройства стоит в первую очередь следовать техническим требованиям и регламентам сетей, в которых будет эксплуатироваться данное устройство.

5.1 Общие рекомендации

- Рекомендуется всегда отключать неиспользуемые физические интерфейсы с помощью команды; **shutdown**. Команда подробно описана в разделе [Конфигурирование и мониторинг интерфейсов](#) справочника команд CLI;
- Рекомендуется всегда настраивать синхронизацию системных часов с доверенными источниками сетевого времени (NTP). Алгоритм настройки NTP приведён в разделе [Настройка NTP](#) настоящего руководства. Подробная информация о командах для настройки NTP приведена в разделе [Управление системными часами](#) справочника команд CLI;
- Рекомендуется отключать NTP broadcast client, включённый по умолчанию в заводской конфигурации;
- Не рекомендуется использовать команду **ip firewall disable**, отключающую межсетевое экранирование. Следует всегда назначать интерфейсам соответствующие зоны безопасности и настраивать корректные правила межсетевого экрана. Алгоритм настройки межсетевого экрана приведён в разделе [Конфигурирование Firewall](#) настоящего руководства. Подробная информация о командах для настройки межсетевого экрана приведена в разделе [Управление Firewall](#) справочника команд CLI.

5.2 Настройка системы логирования событий

Алгоритмы настройки системы логирования событий приведены в подразделе «Настройка Syslog» раздела [Мониторинг](#) настоящего руководства.

Подробная информация о командах для настройки системы логирования событий приведена в разделе [Управление SYSLOG](#) справочника команд CLI.

5.2.1 Рекомендации

- Рекомендуется настроить хранение сообщений о событиях в файл syslog на устройстве и передачу этих событий на внешний syslog-сервер;
- Рекомендуется ограничивать размер syslog-файла на устройстве;
- Рекомендуется настраивать ротацию syslog-файлов на устройстве;
- Рекомендуется включать нумерацию сообщений syslog.

5.2.2 Предупреждения

- Данные, хранящиеся в файловой системе **tmpsys:syslog**, не сохраняются при перезагрузке устройства. Этот тип файловой системы рекомендуется использовать для хранения оперативных логов.
- Не рекомендуется использовать файловую систему **flash:syslog** для хранения логов, так как это может привести к преждевременному выходу из строя устройств.

5.2.3 Пример настройки

Задача:

Настроить хранение сообщений о событиях уровня info и выше в файл syslog на устройстве и настроить передачу этих событий на внешний syslog-сервер. Ограничить файл размером 512 Кбайт. Включить ротацию 3 файлов. Включить нумерацию сообщений syslog.

Решение:

Настраиваем хранение syslog-сообщений в файле:

```
evt(config)# syslog file tmpsys:syslog/default
evt(config-syslog-file)# severity info
evt(config-syslog-file)# exit
```

Настраиваем ограничение размера и ротацию файлов:

```
evt(config)# syslog max-files 3
evt(config)# syslog file-size 512
```


Настраиваем передачу сообщений на внешний сервер:

```
evt(config)# syslog host mylog
evt(config-syslog-host)# remote-address 92.168.1.2
evt(config-syslog-host)# transport udp
evt(config-syslog-host)# port 514
evt(config-syslog-host)# severity info
evt(config-syslog-host)# exit
```

Включаем нумерацию сообщений syslog:

```
evt(config)# syslog sequence-numbers
```

5.3 Настройка политики использования паролей

Алгоритмы настройки политики использования паролей приведены в разделе [Настройка AAA](#) настоящего руководства.

Подробная информация о командах для настройки политики использования паролей приведена в разделе [Настройка AAA](#) справочника команд CLI.

5.3.1 Рекомендации

- Рекомендуется всегда включать требования на смену пароля по умолчанию пользователя admin.
- Рекомендуется ограничивать время жизни паролей и запрещать повторно использовать, как минимум, предыдущий пароль.
- Рекомендуется выставлять требования минимальной длины пароля больше 8 символов.
- Рекомендуется выставлять требования на использование строчных и прописных букв, цифр и спецсимволов.

5.3.2 Пример настройки

Задача:

- Настроить парольную политику с обязательным требованием смены пароля по умолчанию, временем действия пароля 1 месяц и запретом на использование 12 последних паролей.
- Задать минимальную длину пароля 16 символов, максимальную — 64 символа.
- Пароль должен содержать не менее 3 прописных букв, не менее 5 строчных букв, не менее 4 цифр и не менее 2 спецсимволов. Пароль в обязательном порядке должен содержать все 4 типа символов.

Решение:

Включаем запрос на смену пароля по умолчанию для пользователя admin:

```
evs(config)# security passwords default-expired
```

Устанавливаем время жизни пароля 30 дней и запрет на использование предыдущих 12 паролей:

```
evs(config)# security passwords lifetime 30
evs(config)# security passwords history 12
```

Устанавливаем ограничения на длину пароля:

```
evs(config)# security passwords min-length 16
evs(config)# security passwords max-length 24
```

Устанавливаем ограничения по минимальному количеству символов соответствующих типов:

```
evs(config)# security passwords upper-case 3
evs(config)# security passwords lower-case 5
evs(config)# security passwords special-case 2
evs(config)# security passwords numeric-count 4
evs(config)# security passwords symbol-types 4
```

5.4 Настройка политики AAA

Алгоритмы настройки политики AAA приведены в разделе [Настройка AAA](#) настоящего руководства.

Подробная информация о командах для настройки политики AAA приведена в разделе [Настройка AAA](#) справочника команд CLI.

5.4.1 Рекомендации

- Рекомендуется использовать ролевую модель доступа на устройство.
- Рекомендуется использовать персональные учетные записи для аутентификации на устройстве.
- Рекомендуется включать логирование вводимых пользователем команд.
- Рекомендуется использовать несколько методов аутентификации для входа на устройства через консоль, удалённого входа на устройства и повышения привилегий. Оптимальной считается комбинация из аутентификации по одному из протоколов RADIUS/TACACS/LDAP и локальной аутентификации.
- Рекомендуется понизить уровень привилегий встроенной учётной записи **admin** до 1.
- Рекомендуется настроить логирование изменений локальных учётных записей.
- Рекомендуется настроить логирование изменений политики AAA.

5.4.2 Предупреждения

- Встроенную учётную запись **admin** удалить нельзя.
- Команда **no username admin** не удаляет пользователя **admin**, сбрасывает его конфигурацию в значения по умолчанию. После применения этой команды пользователь **admin** не будет отображаться в конфигурации.
- Команда **no password** для пользователя **admin** также не удаляет пароль пользователя **admin**, а сбрасывает его в значение по умолчанию. После применения этой команды пароль пользователя **admin** перестает отображаться в конфигурации и становится 'password'.
- Перед установкой пользователю **admin** пониженных привилегий у вас должен быть настроен пользователь с уровнем привилегий 15 или задан ENABLE-пароль.

5.4.3 Пример настройки

Задача:

Настроить политику AAA:

- Для удалённого входа по протоколу SSH использовать аутентификации через RADIUS.
- Для входа через локальную консоль использовать аутентификации через RADIUS, в случае отсутствия связи с RADIUS-серверами использовать локальную аутентификацию.
- Использовать ENABLE-пароль, заданный через RADIUS, в случае отсутствия связи с RADIUS-серверами использовать локальный ENABLE-пароль.
- Установить пользователю `admin` пониженный уровень привилегий.
- Настроить логирование изменений локальных учётных записей.
- Настроить логирование изменений политик AAA.
- Настроить логирование вводимых команд.

Решение:

Создаём локального пользователя **local-operator** с уровнем привилегий 8:

```
evt(config)# username local-operator
evt(config-user)# password Pa$$w0rd1
evt(config-user)# privilege 8
evt(config-user)# exit
```

Задаём локальный ENABLE-пароль:

```
evt(config)# enable password $6e5c4r3e2t!
```

Понижаем привилегии пользователя `admin`:

```
evt(config)# username admin
evt(config-user)# privilege 1
evt(config-user)# exit
```

Настраиваем связь с двумя RADIUS-серверами, основным 192.168.1.11 и резервным 192.168.2.12:

```
evt(config)# radius-server host 192.168.1.11
evt(config-radius-server)# key ascii-text encrypted 8CB5107EA7005AFF
evt(config-radius-server)# priority 100
evt(config-radius-server)# exit
evt(config)# radius-server host 192.168.2.12
evt(config-radius-server)# key ascii-text encrypted 8CB5107EA7005AFF
evt(config-radius-server)# priority 150
evt(config-radius-server)# exit
```

Настраиваем политику AAA:

```

evt(config)# aaa authentication login CONSOLE radius local
evt(config)# aaa authentication login SSH radius
evt(config)# aaa authentication enable default radius enable
evt(config)# aaa authentication mode break
evt(config)# line console
evt(config-line-console)# login authentication CONSOLE
evt(config-line-console)# exit
evt(config)# line ssh
evt(config-line-ssh)# login authentication SSH
evt(config-line-ssh)# exit

```

Настраиваем логирование:

```

evt(config)# logging userinfo
evt(config)# logging aaa
evt(config)# syslog cli-commands

```

5.5 Настройка удалённого управления

Подробная информация о командах настройки удалённого доступа приведена в разделе [Настройка доступа SSH, Telnet](#) справочника команд CLI.

5.5.1 Рекомендации

- Не рекомендуется включать удалённое управление по протоколу Telnet.
- Рекомендуется использовать криптостойкие алгоритмы аутентификации sha2-512 и отключить все остальные.
- Рекомендуется использовать криптостойкие алгоритмы шифрования aes256ctr и отключить все остальные.
- Рекомендуется использовать криптостойкий алгоритм обмена ключами шифрования dh-group-exchange-sha256 и отключить все остальные.
- Рекомендуется использовать криптостойкий алгоритм верификации Host-Key для SSH rsa и отключить все остальные.
- Рекомендуется разрешить доступ к удалённому управлению устройством только с определённых IP-адресов.
- Перед началом эксплуатации рекомендуется регенерировать ключи шифрования.

5.5.2 Пример настройки

Задача:

Сгенерировать новые ключи шифрования. Использовать криптостойкие алгоритмы.

Решение:

Отключаем устаревшие и не криптостойкие алгоритмы:

```
evs(config)# ip ssh server
evs(config)# ip ssh authentication algorithm md5 disable
evs(config)# ip ssh authentication algorithm md5-96 disable
evs(config)# ip ssh authentication algorithm ripemd160 disable
evs(config)# ip ssh authentication algorithm sha1 disable
evs(config)# ip ssh authentication algorithm sha1-96 disable
evs(config)# ip ssh authentication algorithm sha2-256 disable
evs(config)# ip ssh encryption algorithm 3des disable
evs(config)# ip ssh encryption algorithm aes128 disable
evs(config)# ip ssh encryption algorithm aes128ctr disable
evs(config)# ip ssh encryption algorithm aes192 disable
evs(config)# ip ssh encryption algorithm aes192ctr disable
evs(config)# ip ssh encryption algorithm aes256 disable
evs(config)# ip ssh encryption algorithm arcfour disable
evs(config)# ip ssh encryption algorithm arcfour128 disable
evs(config)# ip ssh encryption algorithm arcfour256 disable
evs(config)# ip ssh encryption algorithm blowfish disable
evs(config)# ip ssh encryption algorithm cast128 disable
evs(config)# ip ssh key-exchange algorithm dh-group-exchange-sha1 disable
evs(config)# ip ssh key-exchange algorithm dh-group1-sha1 disable
evs(config)# ip ssh key-exchange algorithm dh-group14-sha1 disable
evs(config)# ip ssh key-exchange algorithm ecdh-sha2-nistp256 disable
evs(config)# ip ssh key-exchange algorithm ecdh-sha2-nistp384 disable
evs(config)# ip ssh key-exchange algorithm ecdh-sha2-nistp521 disable
evs(config)# ip ssh host-key algorithm dsa disable
evs(config)# ip ssh host-key algorithm ecdsa256 disable
evs(config)# ip ssh host-key algorithm ecdsa384 disable
evs(config)# ip ssh host-key algorithm ecdsa521 disable
evs(config)# ip ssh host-key algorithm ed25519 disable
```

Генерируем новые ключи шифрования:

```
evs# update ssh-host-key rsa 2048
```

6 Управление

6.1 Управление спутниковым интерфейсом

- Настройка устройства для организации спутникового канала в режиме SCPC
 - Настройка передающего тракта
 - Настройка приёмного тракта
 - Настройка сигнализации
 - Передача данных через спутниковый сегмент
 - Транзитная передача данных в режиме маршрутизации (L3)
 - Транзитная передача данных в режиме моста (L2)
- Настройка устройства для организации спутникового канала в режиме MCPC
 - Настройка передающего тракта центральной (узловой) станции в режиме MCPC
 - Настройка приёмного тракта центральной (узловой) станции в режиме MCPC
 - Настройка абонентских станций в режиме MCPC
 - Передача данных через спутниковый сегмент
 - Транзитная передача данных в режиме моста (L3)
 - Транзитная передача данных в режиме моста (L2)
- Подключение BUC и LNB
- Управление тестовыми режимами
 - Включение немодулированной несущей CW
 - Включение режима Баланс (две немодулированные несущие)

6.1.1 Настройка устройства для организации спутникового канала в режиме SCPC

⚠ Конфигурация на маршрутизаторах EVT и EVS производится с помощью одинаковых команд. Ниже приведены примеры настройки EVT.

SCPC (Single Channel Per Carrier, «точка-точка») — выделенный канал связи между двумя ЗССС. В таком канале каждая станция передает закрепленную несущую, которая принимается другой АС. Такой канал может быть любой асимметричности и даже организован через различные транспондеры или спутники.

Для подготовки устройства к работе в сети спутниковой связи должны быть изменены параметры модулятора и демодулятора, установленные по умолчанию. Настройка параметров устройства осуществляется с использованием интерфейс командной строки.

Ниже приводится пример настройки для параметров канала связи, указанных в таблице 1.

Таблица 1. Параметры спутникового канала связи Ku-диапазона

Земная станция	Модуляция	FE C	Roll off, TX	Roll off, RX	Символьная скорость TX, ксим/с	Символьная скорость RX, ксим/с	Частота на TX, МГц	Частота на RX, МГц
ЗССС 1	QPSK	4/5	0,25	0,2	512	4000	14490,3890	11193,2500
ЗССС 2	8PSK	5/6	0,2	0,25	4000	512	14493,2500	11190,3890

В таблице 1 указаны параметры асимметричного канала связи и назначенные для организации канала частоты. Владелец спутникового ресурса указывает в спецификации спутниковой линии частоты на линии «Земля-космос» и на линии «космос-Земля», которые также могут называться линия «вверх» и линия «вниз», соответственно.

⚠ Внимание! Для расчёта частот передачи и приёма, которые должны быть установлены при настройке устройства, необходимо знать частоты гетеродинов трактов приёма и передачи. Обратитесь к технической документации на BUC и LNB, применённые в составе земной станции. Значение частоты гетеродина также может быть указано на корпусе BUC и LNB.

Для LNB Ku-диапазона частота гетеродина имеет значение 10 000 МГц или 9 750 МГц, для BUC Ku-диапазона – 13 050 МГц или 12 800 МГц. В данном примере будут использованы частота гетеродина LNB МГц и частота BUC МГц. Для расчёта частоты передачи F_{tx} и частоты приёма F_{rx} модемов использованы следующие соотношения (формулы справедливы для устройств с нижним гетеродином):

$$F_{tx} = F_{up} - F_{BUC}$$

и

$$F_{rx} = F_{down} - F_{LNB},$$

где:

F_{up} – частота сигнала на линии «вверх»;

F_{down} – частота сигнала на линии «вниз».

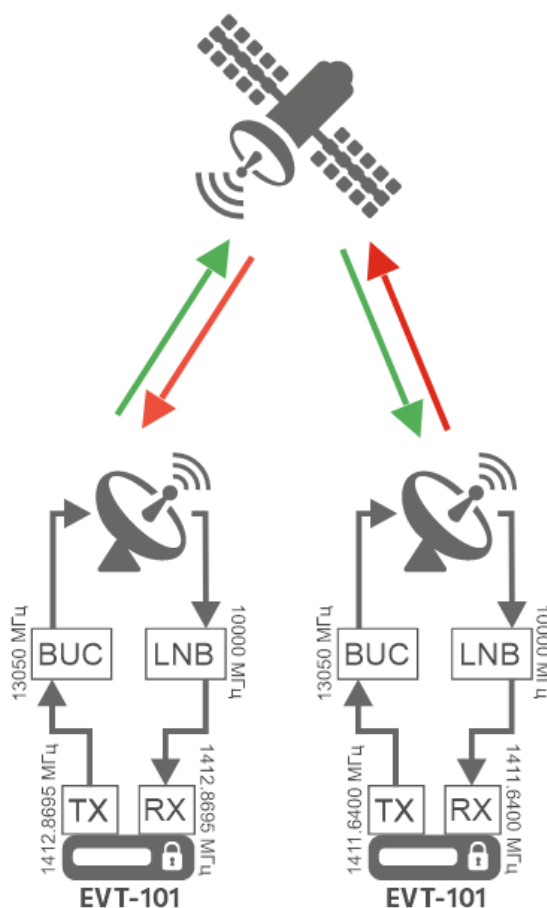


Рисунок 1. Частоты сигналов в спутниковой линии

На рисунке 1 зелёным цветом обозначен тракт прохождения сигнала от земной станции ЗС1 до земной станции ЗССС2, красным – от земной станции ЗССС2 до земной станции ЗССС1. В данном примере ретранслятор искусственного спутника Земли (ИСЗ) обеспечивает сдвиг принятого сигнала на 3300 МГц вниз. То есть любой сигнал, принятый ИСЗ на линии «вверх», будет передан на линии «вниз» на частоте меньшей, чем частота на линии «вверх», на 3300 МГц.

⚠ Важно! За информацией о конкретных значениях частотного сдвига сигналов в конкретных транспондерах ИСЗ следует обращаться к владельцам спутникового ресурса.

Значения параметров модуляторов и демодуляторов, которые необходимо установить на устройстве, входящих в состав ЗССС1 и ЗССС2 приведены в следующих конфигурациях.

Настройка передающего тракта

Конфигурация модулятора ЗССС 1:

```
interface satellite-modulator 1/1/1
 frame-length normal
 frequency 1440389.0
 rolloff 0.25
 symrate 512000
 tx-mode normal
 exit
```

Конфигурация модулятора ЗССС 2:

```
interface satellite-modulator 1/1/1
 frame-length normal
 frequency 1443250.0
 rolloff 0.2
 symrate 4000000
 tx-mode normal
 exit
```

По умолчанию пока параметры **frequency**, **symrate**, **rolloff** и **frame-length** не установлены, передатчик выключен. Контроль установленных параметров на модулятор осуществляется командой **show interfaces satellite-modulator**.

```
EVT-101# show interfaces satellite-modulator
Frequency, kHz:      1443250.0
Symrate, Symbols/s: 4000000
Output level, dBm:   -00.00
Frame length:       normal
Rolloff:             0.2
TX mode:             normal
Phase mode:          normal
Spectrum inversion: Disabled
Pilots:              Disabled
```

Регулировка уровня выходного сигнала модулятора производится командой **interface satellite-modulator output-level**. Значение ослабления выходного аттенюатора по умолчанию 0 дБ. Уменьшая ослабление следует установить допустимое значение ЭИИМ земной станции.

Настройка приёмного тракта

Конфигурация демодулятора ЗССС 1:

```
interface satellite-demodulator 1/1/1
 frame-length normal
 frequency 1193250.0
 rolloff 0.2
 symrate 4000000
 exit
```

Конфигурация демодулятора ЗССС 2:

```
interface satellite-demodulator 1/1/1
 frame-length normal
 frequency 1190389.0
 rolloff 0.25
 symrate 512000
 exit
```

Контроль установленных параметров, а также мониторинг параметров приёма на демодуляторе осуществляется командой **show interfaces satellite-demodulator**.

```
EVT-101# show interfaces satellite-demodulator 1/1/1
Frequency, kHz:      1193250.0
Symrate, Symbols/s:  4000000
Frame length:       normal
Rolloff:            0.2
Phase mode:         normal
Es/No local:        30.5
Frequency offset, kHz: 274.6
PL MODCOD:          8PSK 5/6
PL Frame length:    normal
Pilots:             Disabled
Es/No remote:       30.2
Last signaling, sec: --
MAC remote:         --
MAC remote last:    --
```

Настройка сигнализации

Устройства могут видеть друг друга при включённой сигнализации каждую секунду.

```
satellite-modem
 signaling enable
 exit
```

Контроль установленных параметров, а также мониторинг параметров приёма на демодуляторе осуществляется командой **show interfaces satellite-demodulator**.

```
EVT-101# show interfaces satellite-demodulator 1/1/1
Frequency, kHz:      1193250.0
Symrate, Symbols/s:  4000000
```

```

Frame length:      normal
Rolloff:           0.2
Phase mode:        normal
Es/No local:       30.5
Frequency offset, kHz: 274.6
PL MODCOD:         8PSK 5/6
PL Frame length:   normal
Pilots:            Disabled
Es/No remote:      30.2
Last signaling, sec: 1
MAC remote:        e4:5a:d4:df:5f:50
MAC remote last:   e4:5a:d4:df:5f:50

```

Передача данных через спутниковый сегмент

После установки указанных выше параметров между ЗССС1 и ЗССС2 должен установиться спутниковый радиоканал.

Конфигурация ЗССС 1:

```

system jumbo-frames
interface satellite-channel 1/1/1
  tx isi 10
  tx label gse 00:00:10
  tx modcod QPSK 4/5
  rx isi 20
  rx label gse 00:00:20
exit

```

Конфигурация ЗССС 2:

```

system jumbo-frames
interface satellite-channel 1/1/1
  tx isi 20
  tx label gse 00:00:20
  tx modcod 8PSK 5/6
  rx isi 10
  rx label gse 00:00:10
exit

```

Транзитная передача данных в режиме маршрутизации (L3)

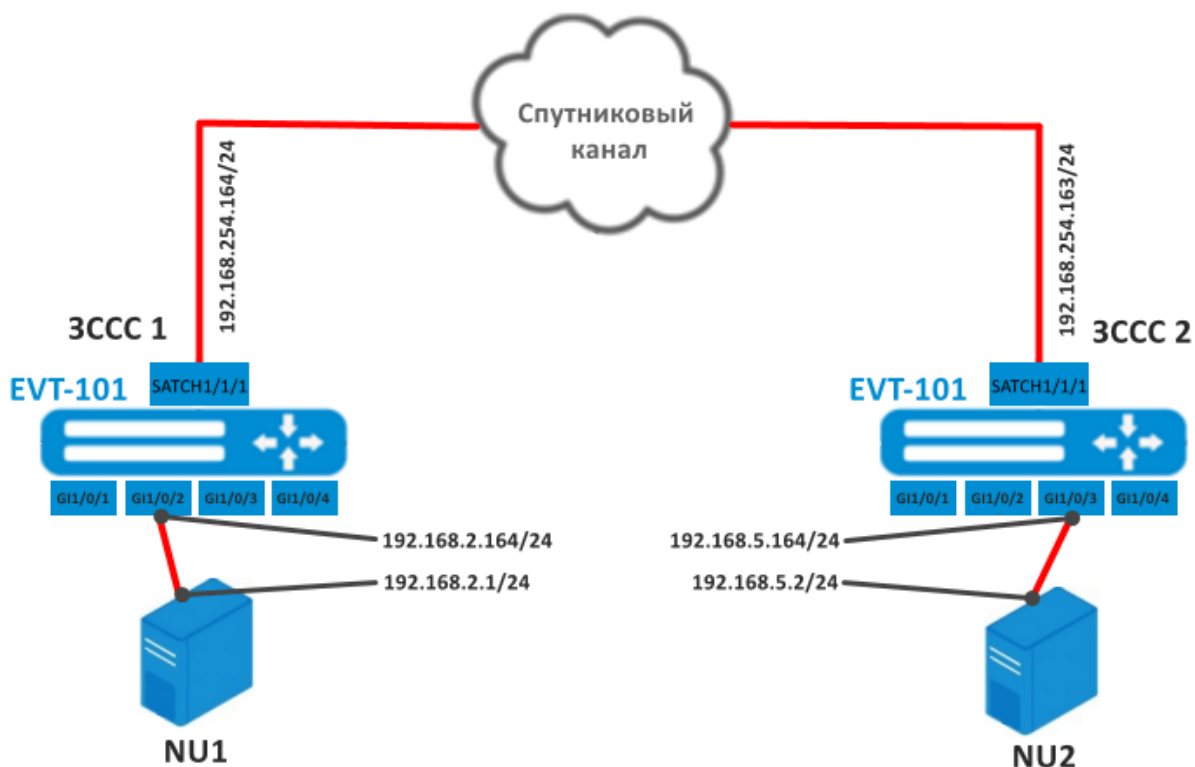


Рисунок 2. Пример применения устройства в режиме маршрутизатора

В заводской конфигурации все сетевые интерфейсы устройства подключены к маршрутизатору. Назначенные по умолчанию адреса указаны на рисунке 2. Четыре интерфейса GI1/0/1...GI1/0/4 обеспечивают подключение сетевых устройств с интерфейсами Ethernet. Интерфейс SATCH1/1/1 предназначен для сопряжения маршрутизатора со спутниковым каналом связи.

Далее рассматривается пример настройки устройства для соединения двух сетевых устройств NU1 и NU2, подключенных к земным станциям ЗССС1 и ЗССС2, соответственно. На ЗССС1 NU1 подключен к интерфейсу GI1/0/2, на ЗССС2 NU2 подключен к интерфейсу GI1/0/3.

Конфигурация ЗССС 1:

```
system jumbo-frames
interface gigabitethernet 1/0/2
 ip firewall disable
 ip address 192.168.2.164/24
exit
interface satellite-modulator 1/1/1
 frame-length normal
 frequency 1440389.0
 rolloff 0.25
 output-level -20.00
 symrate 512000
 tx-mode normal
exit
interface satellite-demodulator 1/1/1
 frame-length normal
 frequency 1193250.0
 rolloff 0.2
 symrate 4000000
exit
```

```

interface satellite-channel 1/1/1
  ip address 192.168.254.164/24
  tx isi 10
  tx label gse 00:00:10
  tx modcod QPSK 4/5
  rx isi 20
  rx label gse 00:00:20
exit
satellite-modem
  signaling enable
exit
ip route 192.168.5.0/24 192.168.254.163

```

Конфигурация ЗССС 2:

```

system jumbo-frames
interface gigabitethernet 1/0/3
  ip firewall disable
  ip address 192.168.5.164/24
exit
interface satellite-modulator 1/1/1
  frame-length normal
  frequency 1443250.0
  rolloff 0.2
  output-level -20.00
  symrate 4000000
  tx-mode normal
exit
interface satellite-demodulator 1/1/1
  frame-length normal
  frequency 1190389.0
  rolloff 0.25
  symrate 512000
exit
interface satellite-channel 1/1/1
  ip address 192.168.254.163/24
  tx isi 20
  tx label gse 00:00:20
  tx modcod 8PSK 5/6
  rx isi 10
  rx label gse 00:00:10
exit
satellite-modem
  signaling enable
exit
ip route 192.168.2.0/24 192.168.254.164

```

Транзитная передача данных в режиме моста (L2)

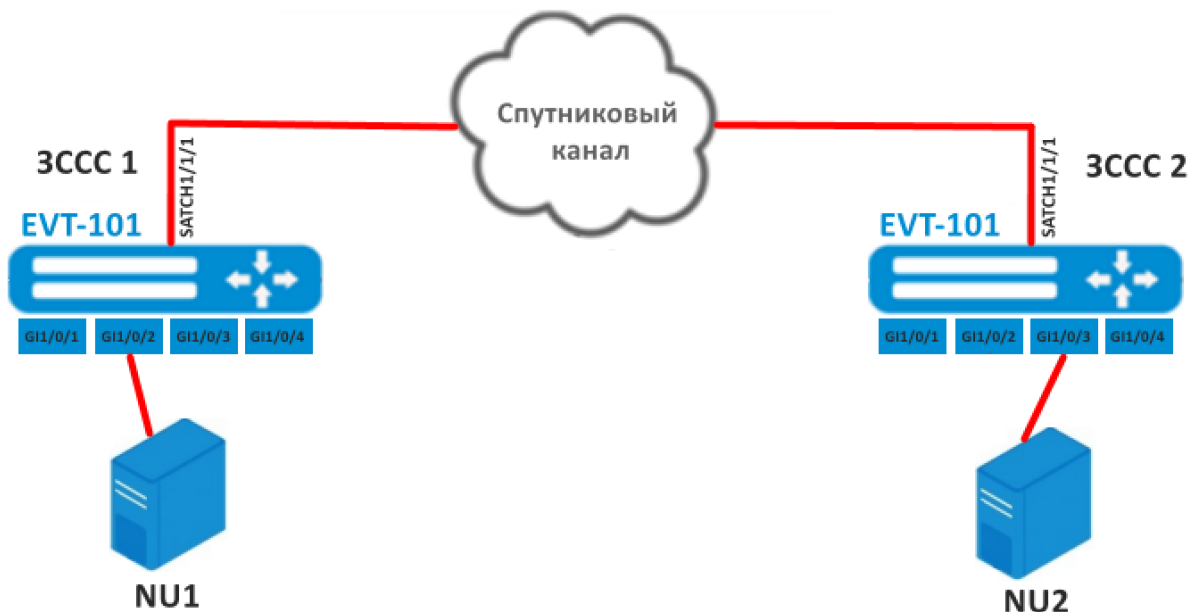


Рисунок 3. Пример применения устройства в режиме моста

В спутниковом маршрутизаторе настроен виртуальный коммутатор, к которому может быть подключен любой из интерфейсов устройства. Для организации моста уровня L2 достаточно соединить интерфейс SATCH1/1/1 через один из коммутаторов с любым из интерфейсов GI1/0/1...GI1/0/4 (см. рисунок 3).

Настройку режима можно выполнить из командного интерпретатора.

Конфигурация ZCCC 1:

```
system jumbo-frames
bridge 1
  ip firewall disable
  enable
exit
interface gigabitethernet 1/0/2
  mode switchport
  bridge-group 1
exit
interface satellite-modulator 1/1/1
  frame-length normal
  frequency 1440389.0
  rolloff 0.25
  output-level -20.00
  symrate 512000
  tx-mode normal
exit
interface satellite-demodulator 1/1/1
  frame-length normal
  frequency 1193250.0
  rolloff 0.2
  symrate 4000000
exit
interface satellite-channel 1/1/1
  mode switchport
  bridge-group 1
  tx isi 10
```

```

tx label gse 00:00:10
tx modcod QPSK 4/5
rx isi 20
rx label gse 00:00:20
exit
satellite-modem
    signaling enable
exit

```

Конфигурация ЗССС 2:

```

system jumbo-frames
bridge 1
    ip firewall disable
    enable
exit
interface gigabitethernet 1/0/3
    mode switchport
    bridge-group 1
exit
interface satellite-modulator 1/1/1
    frame-length normal
    frequency 1443250.0
    rolloff 0.2
    output-level -20.00
    symrate 4000000
    tx-mode normal
exit
interface satellite-demodulator 1/1/1
    frame-length normal
    frequency 1190389.0
    rolloff 0.25
    symrate 512000
exit
interface satellite-channel 1/1/1
    tx isi 20
    tx label gse 00:00:20
    tx modcod 8PSK 5/6
    rx isi 10
    rx label gse 00:00:10
exit
satellite-modem
    signaling enable
exit

```

6.1.2 Настройка устройства для организации спутникового канала в режиме МСРС

МСРС (Multiple Channels per Carrier, «точка-многоточка») — несколько каналов на одну несущую. В такой сети центральная (узловая) станция использует для передачи всем абонентским станциям сети единственную несущую — «прямой канал» (Forward Link). Разделение данных в «прямом канале», предназначенных разным абонентским станциям, осуществляется по логическим каналам: по одному на каждую абонентскую станцию с помощью идентификаторов потоков — ISI (Input Stream Identifier). Каждая абонентская станция принимает «прямой канал» и выбирает «свои данные» не на физическом уровне, а на уровне данных, по служебным заголовкам.

От каждой абонентской станции организуется обратные каналы (Return Link), каждый на своей частоте, которые принимаются многоканальным демодулятором (4 канала) центральной узловой станции.

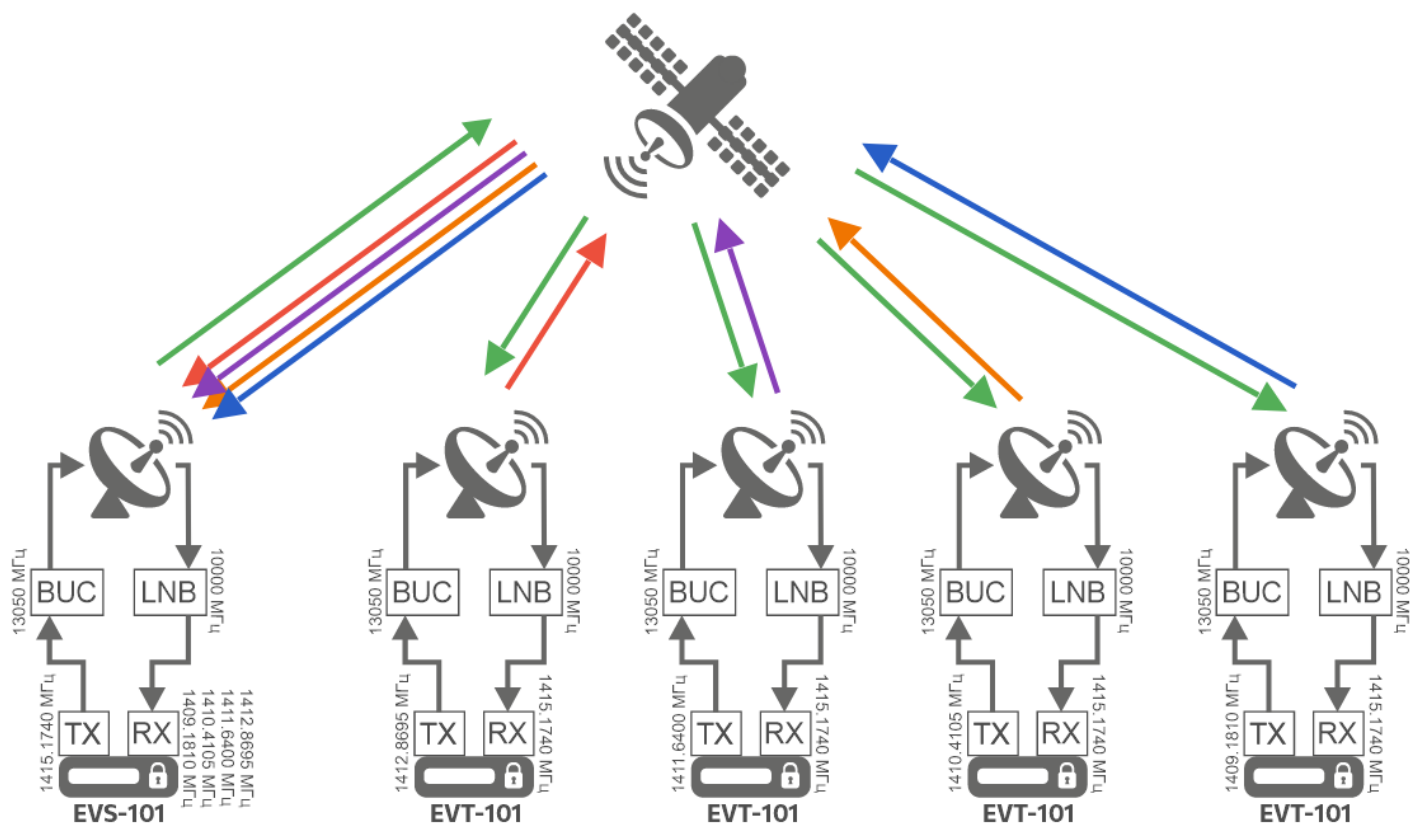


Рисунок 4. Частоты сигналов в спутниковой линии

Таблица 2. Параметры спутникового канала связи Ки-диапазона

Земная станция	Модуляция	FE C	Roll off, TX	Roll off, RX	Символьная скорость TX, ксим/с	Символьная скорость RX, ксим/с	Частота на TX, МГц	Частота на RX, МГц
ЦЗС*	QPSK	4/5	0.05	0.1	3072	1024	1415.1740	1412.8695 1411.6400 1410.4105 1409.1810
АЗС* 1	8PSK	5/6	0.1	0.05	1024	3072	1412.8695	1415.1740
АЗС 2	8PSK	5/6	0.1	0.05	1024	3072	1411.6400	1415.1740
АЗС 3	8PSK	5/6	0.1	0.05	1024	3072	1410.4105	1415.1740
АЗС 4	8PSK	5/6	0.1	0.05	1024	3072	1409.1810	1415.1740

*ЦЗС – Центральная Земная Станция;

*АЗС – Абонентская Земная Станция.

В таблице 2 указаны параметры асимметричного канала связи и назначенные для организации канала частоты. Владелец спутникового ресурса указывает в спецификации спутниковой линии частоты на линии «Земля-космос» и на линии «космос-Земля», которые также могут называться линия «вверх» и линия «вниз», соответственно.

⚠ Внимание! Для расчёта частот передачи и приёма, которые должны быть установлены при настройке устройства, необходимо знать частоты гетеродинов трактов приёма и передачи. Обратитесь к технической документации на BUC и LNB, применённые в составе земной станции. Значение частоты гетеродина также может быть указано на корпусе BUC и LNB.

Для LNB Ku-диапазона частота гетеродина имеет значение 10 000 МГц или 9 750 МГц, для BUC Ku-диапазона — 13 050 МГц или 12 800 МГц. В данном примере будут использованы частота гетеродина LNB МГц и частота BUC МГц. Для расчёта частоты передачи F_{tx} и частоты приёма F_{rx} модемов использованы следующие соотношения (формулы справедливы для устройств с нижним гетеродином):

$$F_{tx} = F_{up} - F_{BUC}$$

и

$$F_{rx} = F_{down} - F_{LNB},$$

где:

F_{up} – частота сигнала на линии «вверх»;

F_{down} – частота сигнала на линии «вниз».

Таблица 3. Параметры спутникового канала связи L-диапазона

Земная станция	Модуляция	FE C	Roll off, TX	Roll off, RX	Символьная скорость TX, ксим/с	Символьная скорость RX, ксим/с	Частота на TX, МГц	Частота на RX, МГц
ЦЗС	QPSK	4/5	0.05	0.1	3072	1024	1665.1740	1662.8695 1661.6400 1660.4105 1659.1810
A3C 1	8PSK	5/6	0.1	0.05	1024	3072	1662.8695	1665.1740
A3C 2	8PSK	5/6	0.1	0.05	1024	3072	1661.6400	1665.1740
A3C 3	8PSK	5/6	0.1	0.05	1024	3072	1660.4105	1665.1740
A3C 4	8PSK	5/6	0.1	0.05	1024	3072	1659.1810	1665.1740

Настройка передающего тракта центральной (узловой) станции в режиме MCPC

Конфигурация модулятора центральной (узловой) станции в режиме MCPC:

```
interface satellite-modulator 1/1/1
  frame-length normal
  frequency 1415174.0
  output-level 0.00
  rolloff 0.05
  symrate 3072000
exit
```

По умолчанию, пока параметры **frequency**, **symrate**, **rolloff** и **frame-length** не установлены, передатчик выключен. Контроль установленных параметров на модулятор осуществляется командой **show interfaces satellite-modulator**.


```

EVS-101# show interfaces satellite-modulator
Frequency, kHz:      1415174.0
Symrate, Symbols/s: 3072000
Output level, dBm:   -00.00
Frame length:        normal
Rolloff:              0.05
TX mode:              normal
Phase mode:           normal
Spectrum inversion: Disabled
Pilots:               Disabled

```

Регулировка уровня выходного сигнала модулятора производится командой **interface satellite-modulator output-level**. Значение ослабления выходного аттенюатора по умолчанию 0 дБ. Уменьшая ослабление следует установить допустимое значение ЭИИМ земной станции.

Настройка приёмного тракта центральной (узловой) станции в режиме MCPC

Конфигурация демодулятора центральной (узловой) станции в режиме MCPC:

```

interface satellite-demodulator 1/1/1
  frame-length short
  frequency 1412869.5
  rolloff 0.1
  symrate 1024000
exit
interface satellite-demodulator 1/1/2
  frame-length short
  frequency 1411640.0
  rolloff 0.1
  symrate 1024000
exit
interface satellite-demodulator 1/1/3
  frame-length short
  frequency 1410410.5
  rolloff 0.1
  symrate 1024000
exit
interface satellite-demodulator 1/1/4
  frame-length short
  frequency 1409181.0
  rolloff 0.1
  symrate 1024000
exit

```

Контроль установленных параметров, а также мониторинг параметров приёма на демодуляторе осуществляется командой **show interfaces satellite-demodulator**.

```

EVS-101# show interfaces satellite-demodulator

Frequency range, kHz: 1000000.0-1070000.0
Demodulator  Frequency,   Symrate,   Frame    Rolloff
                kHz         Symbols/s  length
-----
1             1412869.5    1024000   short    0.1
2             1411640.0    1024000   short    0.1
3             1410410.5    1024000   short    0.1

```

4	1409181.0	1024000	short	0.1	
Demodulator	Es/No local	Frequency offset, kHz	PL MODCOD	PL Frame length	Pilots
-----	-----	-----	-----	-----	-----
1	9.9	0.0	Dummy Frame	short	Disabled
2	25.2	-6.8	Dummy Frame	short	Disabled
3	-0.8	399.3	Dummy Frame	short	Enabled
4	-90.0	0.0	--	--	Disabled
Demodulator	Es/No remote	Last signaling, sec	MAC remote	MAC remote last	
-----	-----	-----	-----	-----	
1	-90.0	--	--	--	
2	31.6	1	e4:5a:d4:df:5f:58	e4:5a:d4:df:5f:58	
3	-90.0	--	--	--	
4	-90.0	--	--	--	

Настройка абонентских станций в режиме MCPC

Настройка производится аналогично режиму SCPC.

Конфигурация АЗС 1:

```
interface satellite-modulator 1/1/1
  frame-length short
  frequency 1412869.5
  output-level 0.00
  rolloff 0.1
  symrate 1024000
exit
interface satellite-demodulator 1/1/1
  frame-length normal
  frequency 1415174.0
  rolloff 0.05
  symrate 3072000
exit
```

Конфигурация АЗС 2:

```
interface satellite-modulator 1/1/1
  frame-length short
  frequency 1411640.0
  output-level 0.00
  rolloff 0.1
  symrate 1024000
exit
interface satellite-demodulator 1/1/1
  frame-length normal
  frequency 1415174.0
  rolloff 0.05
  symrate 3072000
exit
```

Конфигурация АЗС 3:

```

interface satellite-modulator 1/1/1
  frame-length short
  frequency 1410410.5
  output-level 0.00
  rolloff 0.1
  symrate 1024000
exit
interface satellite-demodulator 1/1/1
  frame-length normal
  frequency 1415174.0
  rolloff 0.05
  symrate 3072000
exit

```

Конфигурация АЗС 4:

```

interface satellite-modulator 1/1/1
  frame-length short
  frequency 1409181.0
  output-level 0.00
  rolloff 0.1
  symrate 1024000
exit
interface satellite-demodulator 1/1/1
  frame-length normal
  frequency 1415174.0
  rolloff 0.05
  symrate 3072000
exit

```

После установки указанных выше параметров между ЦЗС и АЗС 1–4 установится спутниковый радиоканал.

Передача данных через спутниковый сегмент

 **Важно!** Для одного ISI допустимо использовать только один MODCOD

Для передачи трафика между ЦЗС и АЗС 1–4 необходимо установить следующие параметры:

Конфигурация ЦЗС:

```

system jumbo-frames
interface satellite-channel 1/1/1
  tx gse label 00:01:01
  tx isi 1
  tx modcod QPSK 4/5
  rx gse label 00:01:02
  rx isi 2
  satellite-demodulator-group 1
exit
interface satellite-channel 1/1/2
  tx gse label 00:02:01
  tx isi 2
  tx modcod QPSK 4/5

```

```

rx gse label 00:02:02
rx isi 1
satellite-demodulator-group 2
exit
interface satellite-channel 1/1/3
tx gse label 00:03:01
tx isi 3
tx modcod QPSK 4/5
rx gse label 00:03:02
rx isi 1
satellite-demodulator-group 3
exit
interface satellite-channel 1/1/4
tx gse label 00:04:01
tx isi 4
tx modcod QPSK 4/5
rx gse label 00:04:02
rx isi 1
satellite-demodulator-group 4
exit

```

Конфигурация АЗС 1:

```

system jumbo-frames
interface satellite-channel 1/1/1
tx gse label 00:01:02
tx isi 2
tx modcod 8PSK 5/6
rx gse label 00:01:01
rx isi 1
exit

```

Конфигурация АЗС 2:

```

system jumbo-frames
interface satellite-channel 1/1/2
tx gse label 00:02:02
tx isi 1
tx modcod 8PSK 5/6
rx gse label 00:02:01
rx isi 2
exit

```

Конфигурация АЗС 3:

```

system jumbo-frames
interface satellite-channel 1/1/3
tx gse label 00:03:02
tx isi 3
tx modcod 8PSK 5/6
rx gse label 00:03:01
rx isi 1
exit

```

Конфигурация АЗС 4:

```

system jumbo-frames
interface satellite-channel 1/1/4
  tx gse label 00:04:02
  tx isi 4
  tx modcod 8PSK 5/6
  rx gse label 00:04:01
  rx isi 1
exit

```

Транзитная передача данных в режиме моста (L3)

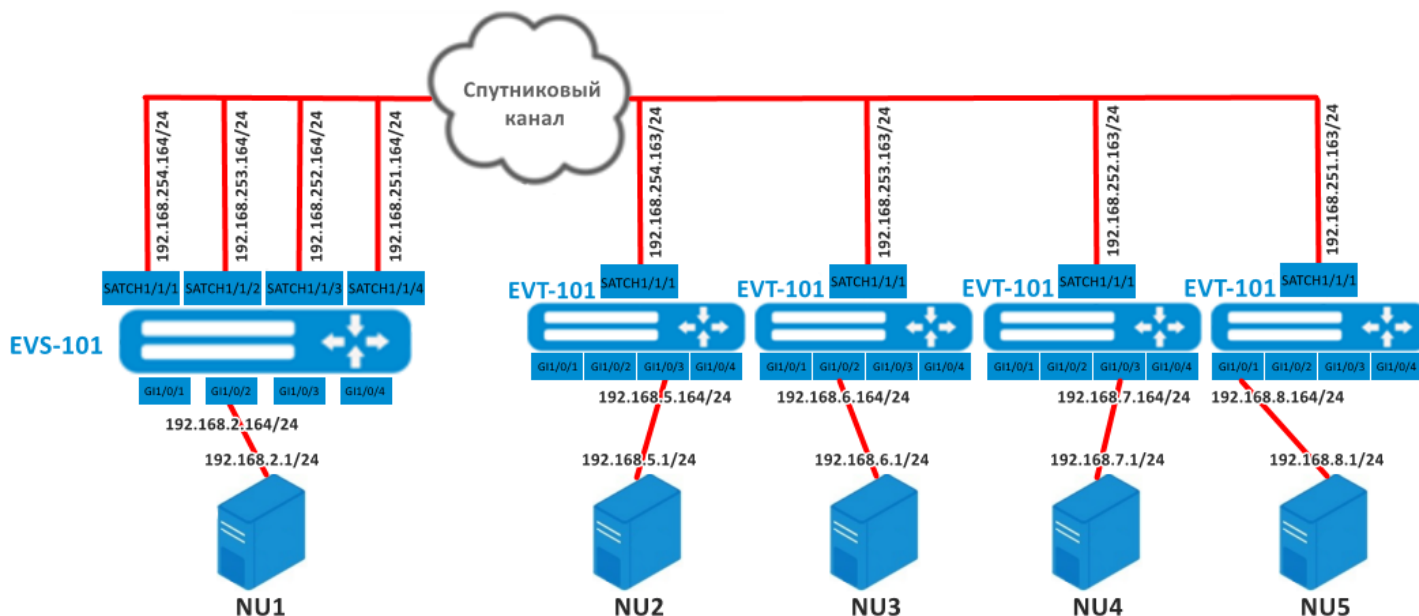


Рисунок 5. Пример применения устройства в режиме маршрутизатора

В заводской конфигурации все сетевые интерфейсы устройства подключены к маршрутизатору. Назначенные по умолчанию адреса указаны на рисунке 5. Четыре интерфейса GI1/0–GI1/0/4 обеспечивают подключение сетевых устройств с интерфейсами Ethernet. Интерфейсы SATCH1/1/1–4 предназначены для сопряжения маршрутизатора со спутниковым каналом связи.

Далее рассматривается пример настройки устройства для соединения пяти сетевых устройств NU1–5, подключенных к ЦЗС и АЗС 1–4, соответственно. На ЦЗС NU1 подключен к интерфейсу GI1/0/2, на АЗС 1 NU2 подключен к интерфейсу GI1/0/3, на АЗС 2 NU3 подключен к интерфейсу GI1/0/2, на АЗС 3 NU4 подключен к интерфейсу GI1/0/3, на АЗС 4 NU5 подключен к интерфейсу GI1/0/1.

Конфигурация ЦЗС:

```

system jumbo-frames
interface gigabitethernet 1/0/2
  ip firewall disable
  ip address 192.168.2.164/24
exit
interface satellite-modulator 1/1/1
  frame-length normal
  frequency 1440389.0
  rolloff 0.25
  output-level -20.00
  symrate 512000
  tx-mode normal
exit

```

```

interface satellite-demodulator 1/1/1
    frame-length short
    frequency 1412869.5
    rolloff 0.1
    symrate 1024000
exit
interface satellite-demodulator 1/1/2
    frame-length short
    frequency 1411640.0
    rolloff 0.1
    symrate 1024000
exit
interface satellite-demodulator 1/1/3
    frame-length short
    frequency 1410410.5
    rolloff 0.1
    symrate 1024000
exit
interface satellite-demodulator 1/1/4
    frame-length short
    frequency 1409181.0
    rolloff 0.1
    symrate 1024000
exit
interface satellite-channel 1/1/1
    ip address 192.168.254.164/24
    tx gse label 00:01:01
    tx isi 1
    tx modcod QPSK 4/5
    rx gse label 00:01:02
    rx isi 2
    satellite-demodulator-group 1
exit
interface satellite-channel 1/1/2
    ip address 192.168.253.164/24
    tx gse label 00:02:01
    tx isi 2
    tx modcod QPSK 4/5
    rx gse label 00:02:02
    rx isi 1
    satellite-demodulator-group 2
exit
interface satellite-channel 1/1/3
    ip address 192.168.252.164/24
    tx gse label 00:03:01
    tx isi 3
    tx modcod QPSK 4/5
    rx gse label 00:03:02
    rx isi 1
    satellite-demodulator-group 3
exit
interface satellite-channel 1/1/4
    ip address 192.168.251.164/24
    tx gse label 00:04:01
    tx isi 4
    tx modcod QPSK 4/5
    rx gse label 00:04:02
    rx isi 1
    satellite-demodulator-group 4
exit

```

```

satellite-modem
  demodulators frequency-range 1000000-1700000
  signaling enable
exit
ip route 192.168.5.0/24 192.168.254.163
ip route 192.168.6.0/24 192.168.253.163
ip route 192.168.7.0/24 192.168.252.163
ip route 192.168.8.0/24 192.168.251.163

```

Конфигурация АЗС 1:

```

system jumbo-frames
interface gigabitethernet 1/0/3
  ip firewall disable
  ip address 192.168.5.164/24
exit
interface satellite-modulator 1/1/1
  frame-length short
  frequency 1412869.5
  output-level 0.00
  rolloff 0.1
  symrate 1024000
exit
interface satellite-demodulator 1/1/1
  frame-length normal
  frequency 1415174.0
  rolloff 0.05
  symrate 3072000
exit
interface satellite-channel 1/1/1
  ip address 192.168.254.163/24
  tx gse label 00:01:02
  tx isi 2
  tx modcod 8PSK 5/6
  rx gse label 00:01:01
  rx isi 1
exit
satellite-modem
  signaling enable
exit
ip route 192.168.2.0/24 192.168.254.164

```

Конфигурация АЗС 2:

```

system jumbo-frames
interface gigabitethernet 1/0/2
  ip firewall disable
  ip address 192.168.6.164/24
exit
interface satellite-modulator 1/1/1
  frame-length short
  frequency 1412869.5
  output-level 0.00
  rolloff 0.1
  symrate 1024000
exit
interface satellite-demodulator 1/1/1
  frame-length normal

```

```

frequency 1415174.0
rolloff 0.05
symrate 3072000
exit
interface satellite-channel 1/1/1
ip address 192.168.253.163/24
tx gse label 00:01:02
tx isi 2
tx modcod 8PSK 5/6
rx gse label 00:01:01
rx isi 1
exit
satellite-modem
    signaling enable
exit
ip route 192.168.2.0/24 192.168.253.164

```

Конфигурация АЗС 3:

```

system jumbo-frames
interface gigabitethernet 1/0/3
ip firewall disable
ip address 192.168.7.164/24
exit
interface satellite-modulator 1/1/1
frame-length short
frequency 1410410.5
output-level 0.00
rolloff 0.1
symrate 1024000
exit
interface satellite-demodulator 1/1/1
frame-length normal
frequency 1415174.0
rolloff 0.05
symrate 3072000
exit
interface satellite-channel 1/1/1
ip address 192.168.252.163/24
tx gse label 00:03:02
tx isi 3
tx modcod 8PSK 5/6
rx gse label 00:03:01
rx isi 1
exit
satellite-modem
    signaling enable
exit
ip route 192.168.2.0/24 192.168.252.164

```

Конфигурация АЗС 4:

```

system jumbo-frames
interface gigabitethernet 1/0/1
ip firewall disable
ip address 192.168.8.164/24
exit
interface satellite-modulator 1/1/1

```



```

frame-length short
frequency 1409181.0
output-level 0.00
rolloff 0.1
symrate 1024000
exit
interface satellite-demodulator 1/1/1
frame-length normal
frequency 1415174.0
rolloff 0.05
symrate 3072000
exit
interface satellite-channel 1/1/1
ip address 192.168.251.163/24
tx gse label 00:04:02
tx isi 4
tx modcod 8PSK 5/6
rx gse label 00:04:01
rx isi 1
exit
satellite-modem
signaling enable
exit
ip route 192.168.2.0/24 192.168.251.164

```

Пример передачи трафика:

```

evs-101# ping 192.168.254.163
PING 192.168.254.163 (192.168.254.163) 56 bytes of data.
!!!!
--- 192.168.254.163 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 294.974/297.682/300.118/1.879 ms

```

Транзитная передача данных в режиме моста (L2)

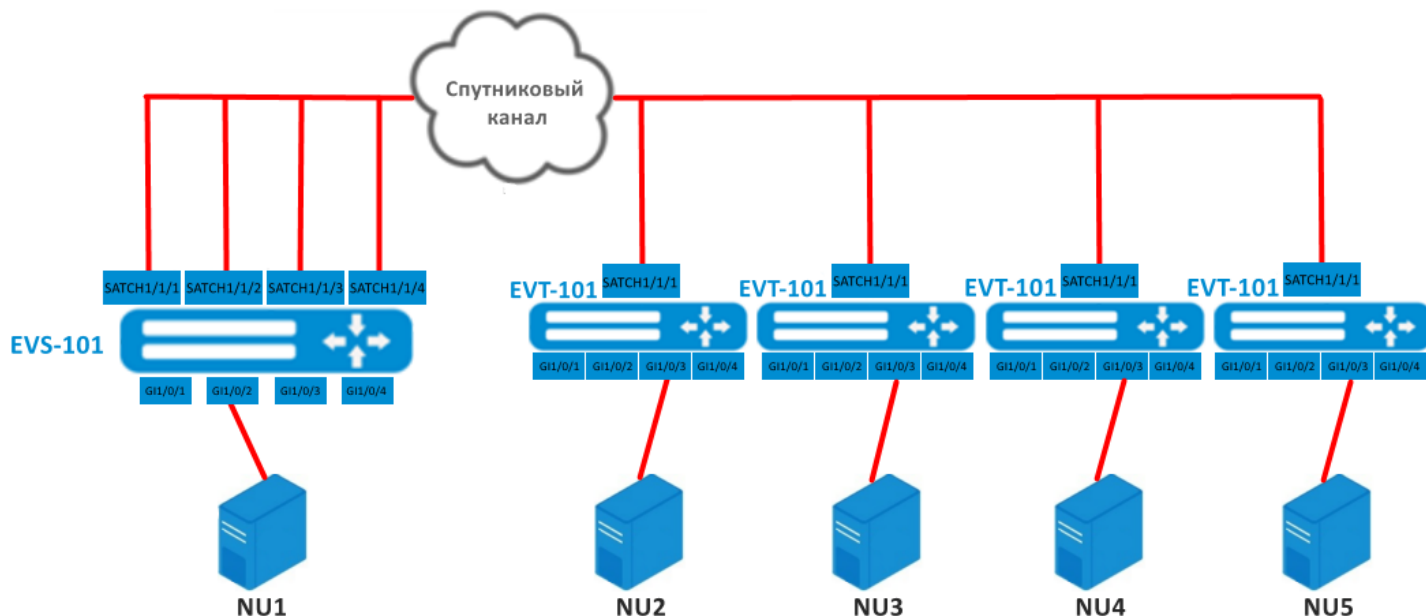


Рисунок 6. Пример применения устройства в режиме моста

В спутниковом маршрутизаторе настроен виртуальный коммутатор, к которому может быть подключен любой из интерфейсов устройства. Для организации моста уровня L2 достаточно соединить интерфейс SATCH1/1/1 через один из коммутаторов с любым из интерфейсов GI1/0/1...GI1/0/4 (см. рисунок 6).

Настройку режима можно выполнить из командного интерпретатора.

Конфигурация ЦЗС:

```
system jumbo-frames
bridge 1
    ip firewall disable
    enable
exit
interface gigabitethernet 1/0/2
    mode switchport
    bridge-group 1
exit
interface satellite-modulator 1/1/1
    frame-length normal
    frequency 1440389.0
    rolloff 0.25
    output-level -20.00
    symrate 512000
    tx-mode normal
exit
interface satellite-demodulator 1/1/1
    frame-length short
    frequency 1412869.5
    rolloff 0.1
    symrate 1024000
exit
interface satellite-demodulator 1/1/2
    frame-length short
    frequency 1411640.0
    rolloff 0.1
    symrate 1024000
exit
interface satellite-demodulator 1/1/3
    frame-length short
    frequency 1410410.5
    rolloff 0.1
    symrate 1024000
exit
interface satellite-demodulator 1/1/4
    frame-length short
    frequency 1409181.0
    rolloff 0.1
    symrate 1024000
exit
interface satellite-channel 1/1/1
    tx gse label 00:01:01
    tx isi 1
    tx modcod QPSK 4/5
    rx gse label 00:01:02
    rx isi 2
    satellite-demodulator-group 1
exit
interface satellite-channel 1/1/2
    tx gse label 00:02:01
    tx isi 2
```

```

tx modcod QPSK 4/5
rx gse label 00:02:02
rx isi 1
satellite-demodulator-group 2
exit
interface satellite-channel 1/1/3
tx gse label 00:03:01
tx isi 3
tx modcod QPSK 4/5
rx gse label 00:03:02
rx isi 1
satellite-demodulator-group 3
exit
interface satellite-channel 1/1/4
tx gse label 00:04:01
tx isi 4
tx modcod QPSK 4/5
rx gse label 00:04:02
rx isi 1
satellite-demodulator-group 4
exit
satellite-modem
demodulators frequency-range 1000000-1700000
signaling enable
exit

```

Конфигурация АЗС 1:

```

system jumbo-frames
bridge 1
ip firewall disable
enable
exit
interface gigabitethernet 1/0/3
mode switchport
bridge-group 1
exit
interface satellite-modulator 1/1/1
frame-length short
frequency 1412869.5
output-level 0.00
rolloff 0.1
symrate 1024000
exit
interface satellite-demodulator 1/1/1
frame-length normal
frequency 1415174.0
rolloff 0.05
symrate 3072000
exit
interface satellite-channel 1/1/1
tx gse label 00:01:02
tx isi 2
tx modcod 8PSK 5/6
rx gse label 00:01:01
rx isi 1
exit
satellite-modem
signaling enable

```

```
exit
```

Конфигурация АЗС 2:

```
system jumbo-frames
bridge 1
    ip firewall disable
    enable
exit
interface gigabitethernet 1/0/3
    mode switchport
    bridge-group 1
exit
interface satellite-modulator 1/1/1
    frame-length short
    frequency 1411640.0
    output-level 0.00
    rolloff 0.1
    symrate 1024000
exit
interface satellite-demodulator 1/1/1
    frame-length normal
    frequency 1415174.0
    rolloff 0.05
    symrate 3072000
exit
interface satellite-channel 1/1/1
    tx gse label 00:02:02
    tx isi 1
    tx modcod 8PSK 5/6
    rx gse label 00:02:01
    rx isi 2
exit
satellite-modem
    signaling enable
exit
```

Конфигурация АЗС 3:

```
system jumbo-frames
bridge 1
    ip firewall disable
    enable
exit
interface gigabitethernet 1/0/3
    mode switchport
    bridge-group 1
exit
interface satellite-modulator 1/1/1
    frame-length short
    frequency 1410410.5
    output-level 0.00
    rolloff 0.1
    symrate 1024000
exit
interface satellite-demodulator 1/1/1
    frame-length normal
    frequency 1415174.0
```

```

    rolloff 0.05
    symrate 3072000
exit
interface satellite-channel 1/1/1
    tx gse label 00:03:02
    tx isi 3
    tx modcod 8PSK 5/6
    rx gse label 00:03:01
    rx isi 1
exit
satellite-modem
    signaling enable
exit

```

Конфигурация АЗС 4:

```

system jumbo-frames
bridge 1
    ip firewall disable
    enable
exit
interface gigabitethernet 1/0/3
    mode switchport
    bridge-group 1
exit
interface satellite-modulator 1/1/1
    frame-length short
    frequency 1409181.0
    output-level 0.00
    rolloff 0.1
    symrate 1024000
exit
interface satellite-demodulator 1/1/1
    frame-length normal
    frequency 1415174.0
    rolloff 0.05
    symrate 3072000
exit
interface satellite-channel 1/1/1
    tx gse label 00:04:02
    tx isi 4
    tx modcod 8PSK 5/6
    rx gse label 00:04:01
    rx isi 1
exit
satellite-modem
    signaling enable
exit

```

6.1.3 Подключение BUC и LNB

Если BUC не имеет собственного опорного генератора, имеется возможность подать опорный сигнал 10 МГц с уровнем 0 дБм на центральный проводник разъема «Tx». Команда **satellite-modem buc reference-frequency** включает или отключает подачу опорного сигнала. По умолчанию опорная частота BUC отключена.

Для включения электропитания BUC по центральному проводнику кабеля ПЧ следует пользоваться командой **satellite-modem buc voltage**. В случае выбора напряжения питания BUC 24 В потребляемый ток BUC по цепи электропитания 24 В не должен быть более 3,5 А. При наличии питания BUC горит красный светодиод «BUC» на задней панели и зелёный светодиод на передней панели. Контроль установленных параметров BUC осуществляется командой **show satellite-modem configuration buc**. Мониторинг текущих параметров BUC – **show satellite-modem status buc**.

```
satellite-modem
  buc power enable
  buc reference-frequency enable
exit
```

```
evt-101# sh satellite-modem status buc
Current, A:  0.00
Voltage, V:  24.00
Overcurrent: No
evt-101# sh satellite-modem configuration buc
Reference frequency: Enable
Power: Enable
```

Если LNB не имеет собственного опорного генератора, имеется возможность подать опорный сигнал 10 МГц с уровнем 0 дБм на центральный проводник разъема «Rx». Команда **satellite-modem lnb reference-frequency** включает или отключает подачу опорного сигнала. По умолчанию опорная частота LNB отключена.

Включить электропитание LNB позволяет команда **satellite-modem lnb voltage**. По умолчанию электропитание LNB отключено. Изделие обеспечивает подачу на центральный проводник разъема «Rx» напряжений из ряда 13 В, 18 В или 24 В на выбор пользователя. Потребляемый ток LNB по цепи электропитания не должен превышать 0,5 А. При наличии питания LNB горит красный светодиод «LNB» на задней панели и зелёный светодиод на передней панели. Контроль установленных параметров LNB осуществляется командой **show satellite-modem configuration lnb**. Мониторинг текущих параметров LNB – **show satellite-modem status lnb**.

```
satellite-modem
  lnb voltage 24
  lnb reference-frequency enable
exit
```

```
evt-101# sh satellite-modem status lnb
Current, mA:  3.63
Voltage, V:   18.08
Overcurrent: No
evt-101# sh satellite-modem configuration lnb
Reference frequency: Enable
Voltage, V:      24
```

6.1.4 Управление тестовыми режимами

Включение немодулированной несущей CW

Немодулированная несущая (CW) на спутниковом модеме — это радиочастотный сигнал с постоянной амплитудой и частотой, который не содержит передаваемых данных («чистый синус»).

Используется для точного наведения антенной системы на спутник, проведения технических измерений в спутниковом тракте.

Пример включения CW:

```
interface satellite-modulator 1/1/1
frame-length normal
frequency 1550000.0
output-level 0.00
rolloff 0.05
symrate 1000000
tx-mode cw
exit
```

Включение режима Баланс (две немодулированные несущие)

В режиме Баланс (Balance) включаются две немодулированные несущие, при этом одна и вторая несущие смещены от выбранной частоты передачи на половину настроенной символьной скорости.

Используется для измерения параметров передающего тракта спутниковой станции.

Пример включения Balance:

```
interface satellite-modulator 1/1/1
frame-length normal
frequency 1550000.0
output-level 0.00
rolloff 0.05
symrate 1000000
tx-mode balance
exit
```

6.2 Управление сетевыми интерфейсами

- [Настройка физического интерфейса](#)
 - [Алгоритм настройки](#)
 - [Алгоритм настройки режима L3](#)
 - [Пример настройки в режиме L3](#)
- [Настройка терминции на саб-интерфейсе](#)
 - [Алгоритм настройки](#)
 - [Пример настройки саб-интерфейса](#)
- [Настройка терминции на Q-in-Q интерфейсе](#)
 - [Алгоритм настройки](#)
 - [Пример настройки Q-in-Q интерфейса](#)

 **Конфигурация на маршрутизаторах EVT и EVS производится с помощью одинаковых команд. Ниже приведены примеры настройки EVT.**

6.2.1 Настройка физического интерфейса

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Переход в режим конфигурирования функционала.	evt(config)# interface gigabitethernet evt(config)# interface tengigabitethernet evt(config)# interface port-channel <ID>	<ID> – порядковый номер группы агрегации каналов, принимает значения [1..12].
2	Включить/отключить интерфейс.	evt(config-if-gi)# shutdown/ no shutdown	
3	Задать описание (необязательно).	evt(config-if-gi)# description <text>	<text> – до 255 символов.
4	Задать MTU (необязательно).	evt(config-if-gi)# mtu <count>	<count> – 552–10000. Значение по умолчанию: 1500.
5	Задать скорость (необязательно).	evt(config-if-gi)# speed 1000M/100M/10M/10G/auto	Значение по умолчанию: auto.
6	Задать MAC-адрес (необязательно).	evt(config-if-gi)# mac-address <ADDR>	<ADDR> – MAC-адрес сетевого моста, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF].

Алгоритм настройки режима L3

Шаг	Описание	Команда	Ключи
1.1	Задать IP-адрес.	evt(config-if-gi)# ip address <ADDR/LEN> или evt(config-if-gi)# ip address <ADDR/LEN> secondary	<ADDR/LEN> – IP-адрес и длина маски подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. Ключ secondary указывает, что настроенный адрес является дополнительным IP-адресом. Если это ключевое слово отсутствует, настроенный адрес является основным IP-адресом. Возможно указать до 7 дополнительных IP-адресов.
1.2	Получить IP-адрес от DHCP-сервера.	evt(config-if-gi)# ip address dhcp	
2.1	Задать IPv6-адрес.	evt(config-if-gi)# ipv6 address <ADDR/P>	<ADDR/P> – IP-адрес и длина маски подсети, задаётся в виде <X:X:X:X::X/N> – где каждая буква X – это шестнадцатеричные значения шести 16-битных элементов адреса и N – длина префикса, принимает значения [1..128].
2.2	Получить IPv6-адрес от DHCP-сервера.	evt(config-if-gi)# ipv6 address dhcp	

Также для физического интерфейса в режиме L3 возможно настроить:

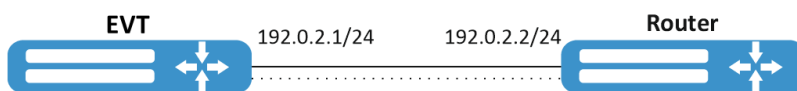
- QoS в базовом или расширенном режимах (см. раздел [Управление QoS](#));
- мониторинг трафика (см. разделы [Настройка Netflow](#));
- функционал протоколов маршрутизации (см. раздел [Управление маршрутизацией](#));
- протокол VRRF (см. раздел [Управление резервированием](#)).

 Для использования firewall необходимо произвести его настройку (см. в разделе [Конфигурирование Firewall](#)).

Пример настройки в режиме L3

Задача:

Настроить интерфейс для прохождения трафика.



Решение:

Перейдите в режим конфигурирования, включите интерфейс, отключите firewall и задайте IPv4-адрес из диапазона 192.0.2.0/24:

```
evt# configure
evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# no shutdown
evt(config-if-gi)# ip firewall disable
evt(config-if-gi)# ip address 192.0.2.1/24
```

Сохраните изменения:

```
evt(config)# commit
evt(config)# confirm
```

На противоположной стороне выдается адрес из той же подсети.

6.2.2 Настройка терминации на саб-интерфейсе

Для терминирования Ethernet-фреймов конкретного VLAN на определенном физическом интерфейсе необходимо создать саб-интерфейс с указанием номера VLAN, фреймы которого будут терминироваться. При создании двух саб-интерфейсов с одинаковыми VLAN, но на разных физических/агрегированных интерфейсах, коммутация Ethernet-фреймов между данными саб-интерфейсами будет невозможна, т. к. сегменты за пределами саб-интерфейсов будут являться отдельными широковещательными доменами. Для обмена данными между абонентами разных саб-интерфейсов (даже с одинаковым VLAN-ID) будет использоваться маршрутизация, т. е. обмен данными будет происходить на третьем уровне модели OSI.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать саб-интерфейс физического интерфейса (возможно только если физический интерфейс в режиме routepoint или hybrid).	evt(config)# interface gigabitethernet <PORT>.<S-VLAN> или interface tengigabitethernet <PORT>.<S-VLAN> или interface port-channel <CH>.<S-VLAN>	<PORT> – номер физического интерфейса. <CH> – номер агрегированного интерфейса. <S-VLAN> – идентификатор создаваемого S-VLAN. Если физический интерфейс включен в bridge-group, создать саб-интерфейс будет невозможно.
2	Задать описание саб-интерфейса (необязательно).	evt(config-if-sub)# description <DESCRIPTION>	<DESCRIPTION> – описание интерфейса, задаётся строкой до 255 символов.
3	Указать экземпляр VRF, в котором будет работать данный саб-интерфейс (необязательно).	evt(config-if-sub)# ip vrf forwarding <VRF>	<VRF> – имя VRF, задается строкой до 31 символа.

Шаг	Описание	Команда	Ключи
4	Указать IPv4/IPv6-адрес и маску подсети для конфигурируемого интерфейса или включить получение IP-адреса динамически.	evt(config-if-sub)# ip address <ADDR/LEN> или evt(config-if-sub)# ip address <ADDR/LEN> secondary	<ADDR/LEN> – IP-адрес и длина маски подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. Ключ secondary указывает, что настроенный адрес является дополнительным IP-адресом. Если это ключевое слово отсутствует, настроенный адрес является основным IP-адресом. Возможно указать до 7 дополнительных IP-адресов. Дополнительные функции IPv4-адресации см. в разделе Настройка IP-адресации .
		evt(config-if-sub)# ipv6 address <IPV6-ADDR/LEN>	<IPV6-ADDR/LEN> – IP-адрес и префикс подсети, задаётся в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128]. Дополнительные функции IPv6-адресации см. в разделе Настройка IPv6-адресации . Можно указать несколько IPv4/IPv6-адресов перечислением через запятую. Может быть назначено до 8 IPv4/IPv6-адресов на интерфейс.
		evt(config-if-sub)# ip address dhcp	Дополнительные функции при работе DHCP-клиента см. в разделе Управление DHCP-клиентом .
5	Отключить на интерфейсе функции Firewall или включить интерфейс в зону безопасности (см. раздел Конфигурирование Firewall).	evt(config-if-sub)# ip firewall disable	
		evt(config-if-sub)# security-zone <NAME>	<NAME> – имя зоны безопасности, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
6	Установить интервал времени, в течение которого собирается статистика о нагрузке на саб-интерфейс (необязательно).	evt(config-if-sub)# load-average <TIME>	<TIME> – интервал в секундах, принимает значения [5..150].
7	Установить время жизни IPv4/IPv6 записей в ARP-таблице, изученных на данном интерфейсе (необязательно).	evt(config-if-sub)# ip arp reachable-time <TIME> или evt(config-if-sub)# ipv6 nd reachable-time <TIME>	<TIME> – время жизни динамических MAC-адресов, в миллисекундах. Допустимые значения от 5000 до 100000000 миллисекунд. Реальное время обновления записи варьируется от [0,5;1,5]*<TIME>.
8	Изменить размер MTU (MaximumTransmissionUnit). MTU более 1500 будет активно только если применена команда "system jumbo-frames" (необязательно).	evt(config-if-sub)# mtu <MTU>	<MTU> – значение MTU в байтах. Значение по умолчанию: 1500.
9	Включить запись статистики использования текущего интерфейса (необязательно).	evt(config-if-sub)# history statistics	
10	Переопределить значение поля MSS (Maximum segment size) во входящих TCP-пакетах (необязательно).	evt(config-if-sub)# ip tcp adjust-mss <MSS> evt(config-if-sub)# ipv6 tcp adjust-mss <MSS>	<MSS> – значение MSS, принимает значения в диапазоне [500..1460]. Значение по умолчанию: 1460.

Также для саб-интерфейса возможно настроить:

- QoS в базовом или расширенном режимах (см. раздел [Управление QoS](#));
- мониторинг трафика (см. разделы [Настройка Netflow](#));
- функционал протоколов маршрутизации (см. раздел [Управление маршрутизацией](#));
- протокол VRRF (см. раздел [Управление резервированием](#)).

Пример настройки саб-интерфейса

Задача:

Настроить терминацию подсети 192.0.2.1/24 в VLAN: 828 на физическом интерфейсе gigabitethernet 1/0/1.

Решение:

Создадим саб-интерфейс для VLAN: 828:

```
evt(config)# interface gigabitethernet 1/0/1.828
```

Настроим IP-адрес из необходимой подсети:

```
evt(config)# interface gigabitethernet 1/0/1.828
evt(config-if-sub)# ip address 192.0.2.1/24
evt(config-if-sub)# exit
```

 Помимо назначения IP-адреса, на саб-интерфейсе необходимо либо отключить firewall, либо настроить соответствующую зону безопасности.

6.2.3 Настройка терминации на Q-in-Q интерфейсе

Q-in-Q — технология передачи пакетов с двумя 802.1q-тегами. Данная технология используется для расширения количества используемых VLAN в сети передачи данных. Внутренним тегом (InnerTag) называется 802.1q-заголовок ближе к payload. Также внутренний тег называют C-VLAN (Customer VLAN). Внешний тег (OuterTag) — это 802.1q-заголовок, добавленный к изначальному 802.1q-пакетом, также называется S-VLAN (Service VLAN). Использование двойных меток в Ethernet-фреймах описывается протоколом 802.1ad.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать саб-интерфейс физического интерфейса (возможно только если физический интерфейс в режиме routepoint или hybrid).	evt(config)# interface gigabitethernet <PORT>.<S-VLAN> или interface tengigabitethernet <PORT>.<S-VLAN> или interface port-channel <CH>.<S-VLAN>	<PORT> – номер физического интерфейса. <CH> – номер агрегированного интерфейса. <S-VLAN> – идентификатор создаваемого S-VLAN. Если физический интерфейс включен в bridge-group, создать саб-интерфейс будет невозможно.

Шаг	Описание	Команда	Ключи
2	Создать Q-in-Q интерфейс.	evt(config)# interface gigabitethernet <PORT>.<S- VLAN>.<C-VLAN> или evt(config)# interface tengigabitethernet <PORT>.<S- VLAN>.<C-VLAN> или evt(config)# interface port-channel <CH>.<S-VLAN>.<C-VLAN>	<PORT> – номер физического интерфейса. <CH> – номер агрегированного интерфейса. <S-VLAN> – идентификатор создаваемого S-VLAN. <C-VLAN> – идентификатор создаваемого C-VLAN. Если физический или саб-интерфейс включен в bridge-group, создать саб-интерфейс будет невозможно.
3	Задать описание Q-in-Q интерфейс (необязательно).	evt(config-if-qinq)# description <DESCRIPTION>	<DESCRIPTION> – описание интерфейса, задаётся строкой до 255 символов.
4	Указать экземпляр VRF, в котором будет работать данный Q-in-Q интерфейс (необязательно).	evt(config-if-qinq) # ip vrf forwarding <VRF>	<VRF> – имя VRF, задается строкой до 31 символа.
5	Указать IPv4/IPv6-адрес и маску подсети для конфигурируемого интерфейса или включить получение IP-адреса динамически.	evt(config-if-qinq)# ip address <ADDR/LEN> или evt(config-if-qinq)# ip address <ADDR/LEN> secondary	<ADDR/LEN> – IP-адрес и длина маски подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. Ключ secondary указывает, что настроенный адрес является дополнительным IP-адресом. Если это ключевое слово отсутствует, настроенный адрес является основным IP-адресом. Возможно указать до 7 дополнительных IP-адресов. Дополнительные функции IPv4-адресации см. в разделе Настройка IP-адресации .

Шаг	Описание	Команда	Ключи
		evt(config-if-qinq)# ipv6 address <IPv6-ADDR/LEN>	<IPv6-ADDR/LEN> – IP-адрес и префикс подсети, задаётся в виде X:X:X:X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128]. Дополнительные функции IPv6-адресации см. в разделе Настройка IPv6-адресации. Можно указать несколько UIIPv4/IPv6-адресов перечислением через запятую. Может быть назначено до 8 IPv4/IPv6-адресов на интерфейс.
		evt(config-if-qinq)# ip address dhcp	Дополнительные функции при работе DHCP-клиента см. в разделе Управление DHCP-клиентом .
6	Отключить на интерфейсе функции Firewall или включить интерфейс в зону безопасности (см. раздел Конфигурирование Firewall).	evt(config-if-qinq)# ip firewall disable	
		evt(config-if-qinq)# security-zone <NAME>	<NAME> – имя зоны безопасности, задаётся строкой до 31 символа.
7	Установить интервал времени, в течение которого собирается статистика о нагрузке на саб-интерфейс (необязательно).	evt(config-if-sub)# load-average <TIME>	<TIME> – интервал в секундах, принимает значения [5..150].
8	Установить время жизни IPv4/IPv6 записей в ARP-таблице, изученных на данном интерфейсе (необязательно).	evt(config-if-sub)# ip arp reachable-time <TIME> или evt(config-if-sub)# ipv6 nd reachable-time <TIME>	<TIME> – время жизни динамических MAC-адресов, в миллисекундах. Допустимые значения от 5000 до 100000000 миллисекунд. Реальное время обновления записи варьируется от [0,5;1,5]*<TIME>.
9	Изменить размер MTU (MaximumTransmissionUnit). MTU более 1500 будет активно только если применена команда "system jumbo-frames" (необязательно).	evt(config-if-sub)# mtu <MTU>	<MTU> – значение MTU в байтах. Значение по умолчанию: 1500.

Шаг	Описание	Команда	Ключи
10	Включить запись статистики использования текущего интерфейса (необязательно).	evt(config-if-sub)# history statistics	
11	Переопределить значение поля MSS (Maximum segment size) во входящих TCP-пакетах (необязательно).	evt(config-if-sub)# ip tcp adjust-mss <MSS> evt(config-if-sub)# ipv6 tcp adjust-mss <MSS>	<MSS> – значение MSS, принимает значения в диапазоне [500..1460]. Значение по умолчанию: 1460.

Также для Q-in-Q интерфейса возможно настроить:

- QoS в базовом или расширенном режимах (см. раздел [Управление QoS](#));
- мониторинг трафика (см. разделы [Настройка Netflow](#));
- функционал протоколов маршрутизации (см. раздел [Управление маршрутизацией](#));
- протокол VRRF (см. раздел [Управление резервированием](#)).

Пример настройки Q-in-Q интерфейса

Задача:

Настроить терминацию подсети 192.0.2.1/24 комбинации C-VLAN: 741, S-VLAN: 828 на физическом интерфейсе gigabitethernet 1/0/1.

Решение:

Создадим саб-интерфейс для S-VLAN: 828:

```
evt(config)# interface gigabitethernet 1/0/1.828
evt(config-if-sub)# exit
```

Создадим Q-in-Q-интерфейс для S-VLAN: 741 и настроим IP-адрес из необходимой подсети:

```
evt(config)# interface gigabitethernet 1/0/1.828.741
evt(config-if-qinq)# ip address 192.0.2.1/24
evt(config-if-qinq)# exit
```

 Помимо назначения IP-адреса, на Q-in-Q саб-интерфейсе необходимо либо отключить firewall, либо настроить соответствующую зону безопасности.

6.2.4 Управление QoS

- [Базовый QoS](#)
 - [Алгоритм настройки](#)
 - [Пример настройки](#)
 - [Пример расчета пропускной способности для взвешенных очередей](#)
- [Расширенный QoS](#)
 - [Алгоритм настройки](#)
 - [Пример настройки](#)
 - [Механизм работы полисера](#)

QoS (Quality of Service) – технология предоставления различным классам трафика различных приоритетов в обслуживании. Использование службы QoS позволяет сетевым приложениям сосуществовать в одной сети, не уменьшая при этом пропускную способность других приложений.

 **Конфигурация на маршрутизаторах EVT и EVS производится с помощью одинаковых команд. Ниже приведены примеры настройки EVT.**

Базовый QoS

В базовом режиме на маршрутизаторах EVT-101 и EVS-101 классификация (направление трафика в очередь) и перемаркировка работают только на входе (на интерфейсе, через который поступает трафик, должен быть включен QoS).

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Включить сервис QoS на интерфейсе /туннеле/сетевом мосту. Если на интерфейсе не назначена политика QoS, то интерфейс работает в режиме BasicQoS.	evt(config-if-gi)# qos enable	

Шаг	Описание	Команда	Ключи
2	Установить режим доверия к значениям кодов 802.1p и DSCP во входящих пакетах (не обязательно).	evt(config)# qos trust <MODE>	<MODE> – режим доверия к значениям кодов 802.1p и DSCP, принимает одно из следующих значений: • dscp – режим доверия значениям кодов DSCP в IP-заголовке. Не IP-пакеты будут направлены в очередь по умолчанию. • cos – режим доверия значениям кодов 802.1p в теге 802.1q. Нетегированные пакеты будут направлены в очередь по умолчанию. • cos - dscp – режим доверия значениям кодов DSCP для IP-пакетов и значениям кодов 802.1p для остальных пакетов.
3	Установить соответствие между значениями кодов DSCP входящих пакетов и исходящими очередями. Данное соответствие работает на входящие пакеты интерфейса/ туннеля/моста, на котором включен QoS (не обязательно).	evt(config)# qos map dscp-queue <DSCP> to <QUEUE>	<DSCP> – классификатор обслуживания в IP-заголовке пакета, принимает значения [0..63]; <QUEUE> – идентификатор очереди, принимает значения [1..8]. Значения по умолчанию: • DSCP: (0-7), очередь 1 • DSCP: (8-15), очередь 2 • DSCP: (16-23), очередь 3 • DSCP: (24-31), очередь 4 • DSCP: (32-39), очередь 5 • DSCP: (40-47), очередь 6 • DSCP: (48-55), очередь 7 • DSCP: (56-63), очередь 8

Шаг	Описание	Команда	Ключи
4	Установить соответствие между значениями кодов 802.1p входящих пакетов и исходящими очередями. Данное соответствие работает на входящие пакеты интерфейса/ туннеля/моста, на котором включен QoS (не обязательно).	evt(config)# qos map cos-queue <COS> to <QUEUE>	<COS> – классификатор обслуживания в теге 802.1p пакета, принимает значения [0..7]; <QUEUE> – идентификатор очереди, принимает значения [1..8]. Значения по умолчанию: • CoS: (0), очередь 1 • CoS: (1), очередь 2 • CoS: (2), очередь 3 • CoS: (3), очередь 4 • CoS: (4), очередь 5 • CoS: (5), очередь 6 • CoS: (6), очередь 7 • CoS: (7), очередь 8
5	Установить соответствие между значениями кодов DSCP входящих пакетов и кодов DSCP на выходе из устройства (в случае необходимости перемаркировки). Данное соответствие работает на входящие пакеты интерфейса/ туннеля/моста, на котором включен QoS.	evt(config)# qos map dscp-queue <DSCP> to <DSCP>	<DSCP> – классификатор обслуживания в IP-заголовке пакета, принимает значения [0..63].
6	Включить изменения кодов DSCP в соответствии с таблицей DSCP-Mutation (в случае необходимости перемаркировки).	evt(config)# qos dscp mutation	
7	Установить номер очереди по умолчанию, в которую попадает весь трафик, кроме IP, в режиме доверия DSCP-приоритетам.	evt(config)# qos queue default <QUEUE>	<QUEUE> – идентификатор очереди, принимает значения [1..8].

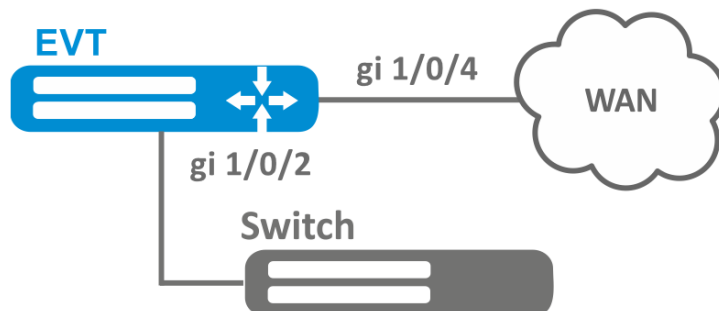
Шаг	Описание	Команда	Ключи
8	Задать количество приоритетных очередей. Оставшиеся очереди являются взвешенными (не обязательно).	evt(config)# priority-queue out num-of-queues <VALUE>	<VALUE> – количество очередей, принимает значение [0..8], где: • 0 – все очереди участвуют в WRR (WRR – механизм обработки очередей на основе веса); • 8 – все очереди обслуживаются как «strictpriority» (strictpriority – приоритетная очередь обслуживается сразу, как только появляются пакеты). Приоритетные очереди выделяются, начиная с 8, в сторону уменьшения номера очереди. Значение по умолчанию: 8.
9	Определить вес для соответствующих взвешенных очередей.	evt(config)# qos wrr-queue <QUEUE> bandwidth <WEIGHT>	<QUEUE> – идентификатор очереди, принимает значение [1..8]; <WEIGHT> – значение веса, принимает значение [1..255]. Значение по умолчанию: вес 1 для всех очередей.
10	Установить ограничение скорости исходящего трафика для определенной очереди или интерфейса в целом. Команда актуальна только для BasicQoS-режима интерфейса. Если трафик на входе был классифицирован при помощи расширенного QoS, ограничение не сработает (в случае необходимости ограничения скорости входящего потока).	evt(config-if-gi)# traffic-shape { <BANDWIDTH> [BURST] queue <QUEUE><BANDWIDTH> [BURST] }	<QUEUE> – идентификатор очереди, принимает значение [1..8]; <BANDWIDTH> – средняя скорость трафика в Кбит/с, принимает значение [3000..10000000] для TengegabitEthernet-интерфейсов и [64..1000000] для прочих интерфейсов и туннелей; <BURST> – размер сдерживающего порога в Кбайт, принимает значение [4..16000]. По умолчанию 128 Кбайт. Значение по умолчанию: отключено.

Шаг	Описание	Команда	Ключи
11	Установить ограничение скорости входящего трафика (в случае необходимости ограничения скорости исходящего потока).	evt(config-if-gi)# rate-limit <BANDWIDTH> [BURST]	<BANDWIDTH> – средняя скорость трафика в Кбит/с, принимает значение [3000..10000000] для TenggigabitEthernet-интерфейсов и [64..1000000] для прочих интерфейсов и туннелей; <BURST> – размер сдерживающего порога в Кбайт, принимает значение [4..16000]. По умолчанию 128 Кбайт. Значение по умолчанию: отключено.

Пример настройки

Задача:

Настроить следующие ограничения на интерфейсе gigabitethernet 1/0/2: передавать трафик с DSCP 22 в восьмую приоритетную очередь, трафик с DSCP 14 в седьмую взвешенную очередь, установить ограничение по скорости в 60 Мбит/с для седьмой очереди.



Решение:

Для того чтобы восьмая очередь осталась приоритетной, а очереди с первой по седьмую стали взвешенными, ограничим количество приоритетных очередей до 1:

```
evt(config)# priority-queue out num-of-queues 1
```

Перенаправим трафик с DSCP 22 в первую приоритетную очередь:

```
evt(config)# qos map dscp-queue 22 to 8
```

Перенаправим трафик с DSCP 14 в седьмую взвешенную очередь:

```
evt(config)# qos map dscp-queue 14 to 7
```

Включим QoS на входящем интерфейсе для корректной классификации трафика и направления в соответствующую очередь со стороны LAN:

```
evt(config)# interface gigabitethernet 1/0/4
evt(config-if-gi)# qos enable
evt(config-if-gi)# exit
```

Включим QoS на интерфейсе со стороны WAN для правильной обработки очередей и ограничения полосы пропускания:

```
evt(config)# interface gigabitethernet 1/0/2
evt(config-if-gi)# qos enable
```

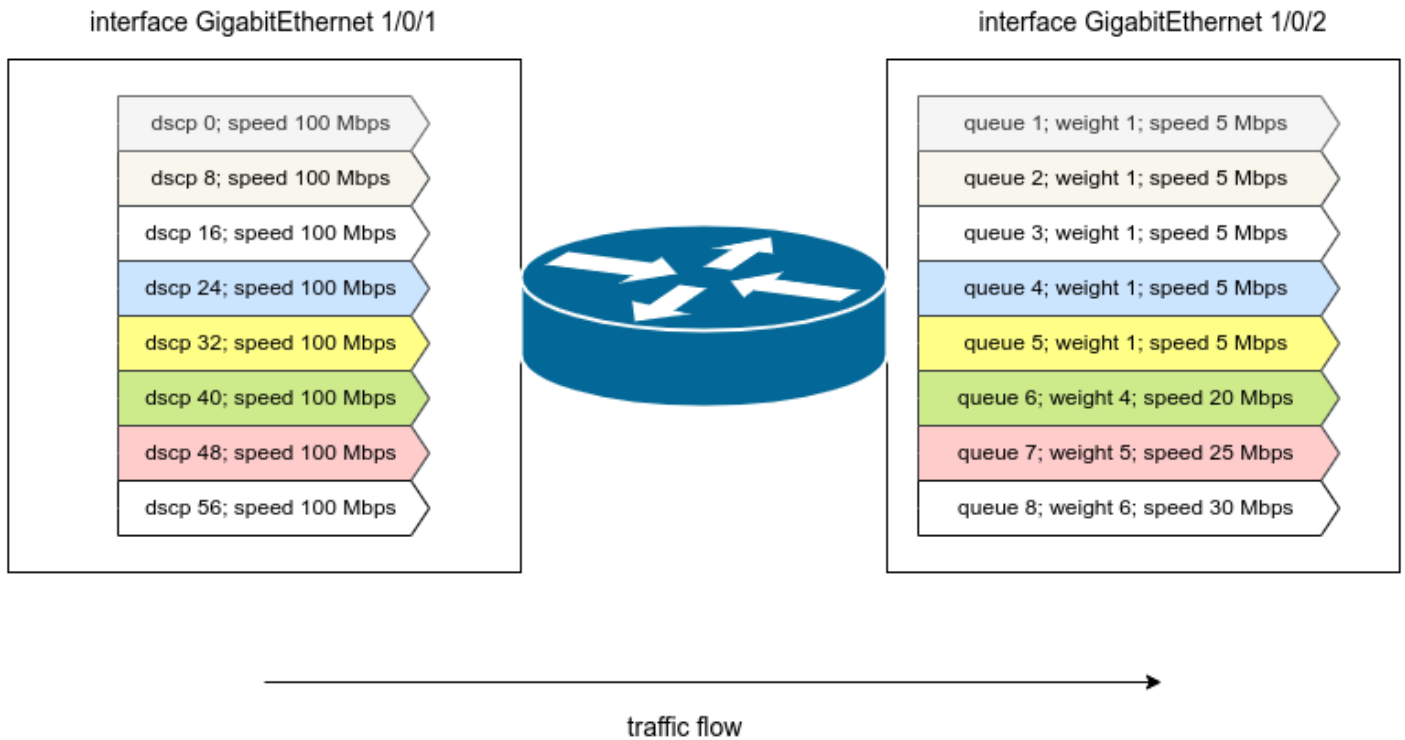
Установим ограничение по скорости в 60 Мбит/с для седьмой очереди:

```
evt(config-if)# traffic-shape queue 7 60000
evt(config-if)# exit
```

Просмотреть статистику по QoS можно командой:

```
evt# show qos statistics gigabitethernet 1/0/2
```

Пример расчета пропускной способности для взвешенных очередей



В рамках данного примера произведем расчет пропускной способности взвешенных очередей. Результаты являются примерными и могут отличаться от практических значений, т. к. не учитывают влияние всплесков.

Пример конфигурации:

Конфигурация EVT

```
hostname evt

qos wrr-queue 1 bandwidth 1
qos wrr-queue 2 bandwidth 1
qos wrr-queue 3 bandwidth 1
qos wrr-queue 4 bandwidth 1
qos wrr-queue 5 bandwidth 1
qos wrr-queue 6 bandwidth 4
qos wrr-queue 7 bandwidth 5
qos wrr-queue 8 bandwidth 6

interface gigabitethernet 1/0/1
 ip firewall disable
 ip address 10.100.0.1/30
 qos enable
exit

interface gigabitethernet 1/0/2
 ip firewall disable
 ip address 10.101.0.1/30
 traffic-shape 100000 512
 qos enable
exit
```

В приведенном примере настроены взвешенные очереди с соответствующими весами.

В команде `qos wrr-queue 7 bandwidth 5`:

- **7** – значение очереди,
- **5** – значение веса очереди.

На входящий интерфейс GigabitEthernet 1/0/1 поступают 8 потоков трафика с различными значениями DSCP со скоростью 100 Мбит/с каждый. По умолчанию маршрутизатор доверяет кодам DSCP, и распределение по очередям происходит в соответствии со следующей картой:

Map DSCP to queue

```
evt# show qos map dscp-queue
d1 : d2   0  1  2  3  4  5  6  7  8  9
-----
0         01 01 01 01 01 01 01 01 02 02
1         02 02 02 02 02 02 03 03 03 03
2         03 03 03 03 04 04 04 04 04 04
3         04 04 05 05 05 05 05 05 05 05
4         06 06 06 06 06 06 06 06 07 07
5         07 07 07 07 07 07 08 08 08 08
6         08 08 08 08
```

В соответствии с этими значениями распределение будет следующим: трафик с значением DSCP 0 попадет в очередь 1, DSCP 8 → очередь 2, DSCP 16 → очередь 3, DSCP 24 → очередь 4, DSCP 32 → очередь 5, DSCP 40 → очередь 6, DSCP 48 → очередь 7 и DSCP 56 → очередь 8 соответственно. На выходном интерфейсе (GigabitEthernet 1/0/2) настроен шейпер с полосой пропускания 100 Мбит/с.

Для расчета полосы пропускания каждой очереди на выходном интерфейсе необходимо выполнить следующие вычисления:

1. Найти суммарный вес всех очередей: $1+1+1+1+1+4+5+6 = 20$ (сложить все значения bandwidth из конфигурации);
2. С учетом значения шейпера (100 Мбит/с) найти пропускную способность очереди на единицу веса: $100/20 = 5$ Мбит/с;
3. Вычислить пропускную способность каждой очереди с учетом их весов:

```
Очередь 1: 1 * 5 = 5 Mbps;
Очередь 2: 1 * 5 = 5 Mbps;
Очередь 3: 1 * 5 = 5 Mbps;
Очередь 4: 1 * 5 = 5 Mbps;
Очередь 5: 1 * 5 = 5 Mbps;
Очередь 6: 4 * 5 = 20 Mbps;
Очередь 7: 5 * 5 = 25 Mbps;
Очередь 8: 6 * 5 = 30 Mbps;
```

Расширенный QoS

Алгоритм настройки

В расширенном режиме на маршрутизаторах evt классификация поступающего трафика возможна как на входящем, так и на исходящем интерфейсах.

Шаг	Описание	Команда	Ключи
1	Создать списки доступа для определения трафика, к которому должен быть применен расширенный QoS.		См. раздел Настройка списков доступа (ACL) .
2	Создать класс QoS и перейти в режим настройки параметров класса.	evt(config)# class-map <NAME>	<NAME> – имя создаваемого класса, задается строкой до 31 символа.
3	Задать описание класса QoS (не обязательно).	evt(config-class-map)# description <description>	<description> – до 255 символов.
4	Определить трафик, относящийся к конфигулируемому классу по списку контроля доступа (ACL).	evt(config-class-map)# match access-group <NAME>	<NAME> – имя списка контроля доступа, задается строкой до 31 символа.
5	Задать значение для классификации по полю DSCP в заголовке IP-пакета для конфигулируемого класса.	evt(config-class-map)# match dscp <DSCP>	<DSCP> – значение кода DSCP, принимает значения [0..63].
6	Задать значение для классификации по полю EXP в MPLS заголовке для конфигулируемого класса.	evt(config-class-map)# match mpls experimental topmost <EXP>	<EXP> – значение поля EXP, принимает значения [0..7].

Шаг	Описание	Команда	Ключи
7	Задать значение кода IP Precedence, которое будет установлено в IP-пакетах, соответствующих конфигулируемому классу (невозможно назначать одновременно с полями DSCP и CoS) (при необходимости перемаркировки).	evt(config-class-map)# set ip-precedence <IPP>	<IPP> – значение кода IP Precedence, принимает значения [0..7].
8	Задать значение 802.1p приоритета, которое будет установлено в пакетах, соответствующих конфигулируемому классу (невозможно назначать одновременно с полями DSCP и IP Precedence) (при необходимости перемаркировки).	evt(config-class-map)# set cos <COS>	<COS> – значение 802.1p приоритета, принимает значения [0..7].
9	Задать значение кода DSCP, которое будет установлено в IP-пакетах, соответствующих конфигулируемому классу (невозможно назначать одновременно с полями IP Precedence и CoS) (при необходимости перемаркировки).	evt(config-class-map)# set cos <DSCP>	<DSCP> – значение кода DSCP, принимает значения [0..63].
10	Создать политику QoS и осуществить переход в режим настройки параметров политики.	evt(config)# policy-map <NAME> evt(config-policy-map)#	<NAME> – имя создаваемой политики, задается строкой до 31 символа.
11	Задать описание политики QoS (не обязательно).	evt(config-policy-map)# description <description>	<description> – до 255 символов.

Шаг	Описание	Команда	Ключи
12	Установить гарантированную полосу пропускания исходящего трафика для политики в целом.	evt(config-policy-map)# shape average { <BANDWIDTH> percent <BANDWIDTH_PERCENT> } [BURST]	<BANDWIDTH> – гарантированная полоса трафика в Кбит/с, принимает значение [64..10000000]; <BANDWIDTH_PERCENT> – гарантированная полоса трафика в %, рассчитывается от (в порядке от более приоритетного к менее приоритетному значению): - значения shape average корневой политики; - значения traffic-shape на сетевом интерфейсе, bridge, туннеле; - значения speed сетевого интерфейса. Принимает значение [1..100]. <BURST> – размер сдерживающего порога в Кбайт, принимает значение [128..16000]. По умолчанию 128 Кбайт.

Шаг	Описание	Команда	Ключи
13	Включить работу полисера (при необходимости).	evt(config-policy-map)# police <RATE> [burst-conforming <BURST-CONFORM>] [conform- action <CONFORM-ACTION>] [exceed-action <EXCEED- ACTION>] [burst-excess <BURST- EXCEED> [violate-action <VIOLATE-ACTION>]]	<RATE> – скорость пополнения токенами conform-корзины в Кбит/с; <BURST-CONFORM> – размер conform-корзины в байтах; <BURST-EXCEED> – размер excess-корзины в байтах; <VIOLATE-ACTION> – действие, которое необходимо выполнить с пакетом, для которого имеются токены conform-корзины, принимает значения { permit deny set-cos <COS> set-dscp <DSCP> }; <CONFORM-ACTION> – действие, которое необходимо выполнить с пакетом, если исчерпаны токены conform-корзины, но имеются токены excess-корзины, принимает значения { permit deny set-cos <COS> set-dscp <DSCP> }; <EXCEED-ACTION> – действие, которое необходимо выполнить с пакетом, для которого исчерпаны токены excess-корзины, принимает значения { permit deny set-cos <COS> set-dscp <DSCP> }; <COS> – классификатор обслуживания в теге 802.1q пакета, принимает значения [0..7]; <DSCP> – значение кода DSCP, принимает значения [0..63].
14	Включить автоматическое распределение полосы пропускания между классами, в которых нет настройки полосы пропускания, включая класс по умолчанию (в случае необходимости).	evt(config-policy-map)# shape auto-distribution	

Шаг	Описание	Команда	Ключи
15	Включить указанный QoS-класс в политику и осуществить переход в режим настройки параметров класса в рамках политики.	evt(config-policy-map)# class <NAME> evt(config-class-policy-map)#	<NAME> – имя привязываемого класса, задается строкой до 31 символа. При указании значения «class-default» в данный класс попадает трафик, не классифицированный на входе.
16	Включить политику QoS в класс QoS для создания иерархического QoS.	evt(config-class-policy-map)# service-policy <NAME>	<NAME> – имя политики, задается строкой до 31 символа. Вкладываемая политика должна быть уже создана.
17	Установить гарантированную полосу пропускания исходящего трафика для класса в рамках политики (при необходимости).	evt(config-class-policy-map)# shape average { <BANDWIDTH> percent <BANDWIDTH_PERCENT> } [BURST]	<BANDWIDTH> – гарантированная полоса трафика в Кбит/с, принимает значение [64..10000000]; <BANDWIDTH_PERCENT> – гарантированная полоса трафика в %, рассчитывается от (в порядке от более приоритетного к менее приоритетному значению): - значения shape average корневой политики; - значения traffic-shape на сетевом интерфейсе, bridge, туннеле; - значения speed сетевого интерфейса. Принимает значение [1..100]. <BURST> – размер сдерживающего порога в Кбайт, принимает значение [4..16000]. По умолчанию 128 Кбайт.

Шаг	Описание	Команда	Ключи
18	Установить разделяемую полосу пропускания исходящего трафика для определенного класса. Данную полосу класс может занять, если менее приоритетный класс не занял свою гарантированную полосу (при необходимости).	evt(config-class-policy-map)# shape peak { <BANDWIDTH> percent <BANDWIDTH_PERCENT> } [BURST]	<BANDWIDTH> – общая для priority class полоса трафика в Кбит/с, конкуренция происходит на основании приоритета класса, принимает значение [64..10000000]; <BANDWIDTH_PERCENT> – общая для priority class полоса трафика в %, конкуренция происходит на основании приоритета класса, рассчитывается от (в порядке от более приоритетного к менее приоритетному значению): • значения shape average корневой политики; • значения traffic-shape на сетевом интерфейсе, bridge, туннеле; • значения speed сетевого интерфейса. Принимает значение [1..100]. <BURST> – размер сдерживающего порога в Кбайт, принимает значение [4..16000]. По умолчанию 128 Кбайт.

Шаг	Описание	Команда	Ключи
19	Включить работу полисера для определенного класса (при необходимости).	evt(config-class-policy-map)# police <RATE> [burst-conforming <BURST-CONFORM>] [conform-action <CONFORM-ACTION>] [exceed-action <EXCEED-ACTION>] [burst-excess <BURST-EXCEED> [violate-action <VIOLATE-ACTION>]]	<RATE> – скорость пополнения токенами conform-корзины Кбит/с; <BURST-CONFORM> – размер conform-корзины в байтах; <BURST-EXCEED> – размер excess-корзины в байтах; <VIOLATE-ACTION> – действие, которое необходимо выполнить с пакетом, для которого имеются токены conform-корзины, принимает значения { permit deny set-cos <COS> set-dscp <DSCP> }; <CONFORM-ACTION> – действие, которое необходимо выполнить с пакетом, если исчерпаны токены conform-корзины, но имеются токены excess-корзины, принимает значения { permit deny set-cos <COS> set-dscp <DSCP> }; <EXCEED-ACTION> – действие, которое необходимо выполнить с пакетом, для которого исчерпаны токены excess-корзины, принимает значения { permit deny set-cos <COS> set-dscp <DSCP> }; <COS> – классификатор обслуживания в теге 802.1q пакета, принимает значения [0..7]; <DSCP> – значение кода DSCP, принимает значения [0..63].

Шаг	Описание	Команда	Ключи
20	Определить режим работы класса (не обязательно).	evt(config-class-policy-map)# mode <MODE>	<MODE> – режим класса: • fifo – режим FIFO (First In, First Out); • gred – режим GRED (Generalized RED); • red – режим RED (Random Early Detection); • sfq – режим SFQ (очередь SFQ распределяет передачу пакетов на базе потоков). Значение по умолчанию: FIFO.
21	Задать приоритет класса в WRR-процессе (при необходимости).	evt(config-class-policy-map)# priority class <PRIORITY>	<PRIORITY> – приоритет класса в WRR-процессе, принимает значения [1..8]. Классы с наибольшим приоритетом обрабатываются в первую очередь.
22	Перевести класс в режим StrictPriority и задать приоритет класса (при необходимости).	evt(config-class-policy-map)# priority level <PRIORITY>	<PRIORITY> – уровень приоритета в StrictPriority-процессе, принимает значения [1..8]. Классы с наибольшим приоритетом обрабатываются в первую очередь. Значение по умолчанию: класс работает в режиме WRR, приоритет не задан.
23	Задать значение кода DSCP, которое будет установлено в IP-пакетах, соответствующих конфигурируемому классу (невозможно назначать одновременно с полями IP Precedence и CoS) (при необходимости перемаркировки параметрами класса в рамках политики).	evt(config-class-map)# match dscp <DSCP>	<DSCP> – значение кода DSCP, принимает значения [0..63].
24	Задать значение кода IP Precedence, которое будет установлено в IP-пакетах, соответствующих конфигурируемому классу (невозможно назначать одновременно с полями DSCP и CoS) (при необходимости перемаркировки параметрами класса в рамках политики).	evt(config-class-map)# set ip-precedence <IPP>	<IPP> – значение кода IP Precedence, принимает значения [0..7].

Шаг	Описание	Команда	Ключи
25	Задать значение 802.1p приоритета, которое будет установлено в пакетах, соответствующих конфигурируемому классу (невозможно назначать одновременно с полями DSCP и IP Precedence) (при необходимости перемаркировки параметрами класса в рамках политики).	evt(config-class-map)# set cos <COS>	<COS> – значение 802.1p приоритета, принимает значения [0..7].
26	Определить предельное количество виртуальных очередей (не обязательно).	evt(config-class-policy-map)# fair-queue <QUEUE-LIMIT>	<QUEUE-LIMIT> – предельное количество виртуальных очередей, принимает значения в диапазоне [16..4096]. Значение по умолчанию: 16.
27	Определить предельное количество пакетов для виртуальной очереди (не обязательно).	evt(config-class-policy-map)# queue-limit <QUEUE-LIMIT>	<QUEUE-LIMIT> – предельное количество пакетов в виртуальной очереди, принимает значения в диапазоне [2..4096]. Значение по умолчанию: 127.

Шаг	Описание	Команда	Ключи
28	Определить параметры RED (Random Early Detection) (при необходимости).	evt(config-class-policy-map)# random-detect <LIMIT> <MIN> <MAX> <APS> <APS-NUM> <PROBABILITY>	<LIMIT> – предельный размер очереди в байтах, принимает значения в диапазоне [1..1000000]; <MIN> – минимальный размер очереди в байтах, принимает значения в диапазоне [1..1000000]; <MAX> – максимальный размер очереди в байтах, принимает значения в диапазоне [1..1000000]; <APS> – средний размер пакета в байтах, принимает значение в диапазоне [1..10000000]; <APS-NUM> – количество пакетов среднего размера разрешенных для кратковременного пропускания, принимает значение в диапазоне [0..10000000]; <PROBABILITY> – вероятность отбрасывания пакетов, принимает значения [0..100]. При указании значений должны выполняться следующие правила: <MAX>> 2 * <MIN> <LIMIT>> 3 * <MAX>

Шаг	Описание	Команда	Ключи
29	Определить параметры GRED (Generalized Random Early Detection) (при необходимости).	evt(config-class-policy-map)# random-detect queue <QUEUE-NUM> [dscp <DSCP> precedence <IPP>] <LIMIT> <MIN> <MAX> <APS> <APS-NUM> <PROBABILITY>	<QUEUE-NUM> – номер очереди [1..16]; <DSCP> – классификатор обслуживания в IP-заголовке пакета, принимает значения [0..63]; <IPP> – значение кода IP Precedence, принимает значения [0..7]; <PRECEDENCE> – значение IP Precedence [0..7]; <LIMIT> – предельный размер очереди в байтах, принимает значения в диапазоне [1..1000000]; <MIN> – минимальный размер очереди в байтах, принимает значения в диапазоне [1..1000000]; <MAX> – максимальный размер очереди в байтах, принимает значения в диапазоне [1..1000000]; <APS> – средний размер пакета в байтах, принимает значение в диапазоне [1..10000000]; <APS-NUM> – количество пакетов среднего размера разрешенных для кратковременного пропуска, принимает значение в диапазоне [0..10000000]; <PROBABILITY> – вероятность отбрасывания пакетов, принимает значения [0..100] При указании значений должны выполняться следующие правила: <MAX>> 2 * <MIN> <LIMIT>> 3 * <MAX>

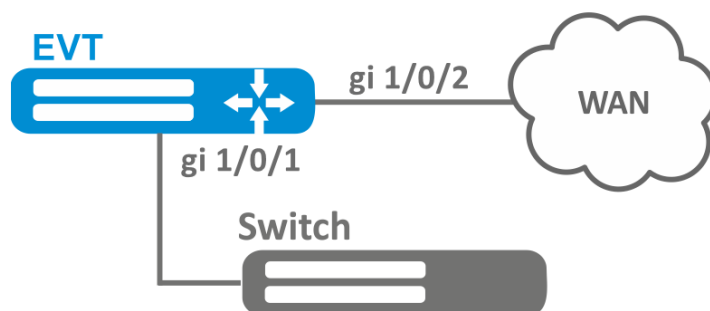
Шаг	Описание	Команда	Ключи
30	Определить очередь по умолчанию для механизма GRED.	evt(config-class-policy-map)# random-detect queue default <QUEUE-NUM>	Данной командой определяется очередь по умолчанию для механизма GRED. Для применения данной команды предварительно необходимо настроить команду random-detect queue <QUEUE-NUM> dscp <DSCP>/precedence <0-7> <LIMIT> <MIN> <MAX> <APS> <APS-NUM> <PROBABILITY>. После применения команд random-detect queue <QUEUE-NUM> dscp <DSCP>/precedence <0-7> <LIMIT> <MIN> <MAX> <APS> <APS-NUM> <PROBABILITY> и random-detect queue default <QUEUE-NUM> поля dscp/precedence в заголовке IP-пакетов данной очереди будут игнорироваться. <QUEUE-NUM> – номер очереди [1..16]; <DSCP> – классификатор обслуживания в IP-заголовке пакета, принимает значения [0..63]; <IPP> – значение кода IP Precedence, принимает значения [0..7]; <PRECEDENCE> – значение IP Precedence [0..7]; <LIMIT> – предельный размер очереди в байтах, принимает значения в диапазоне [1..1000000]; <MIN> – минимальный размер очереди в байтах, принимает значения в диапазоне [1..1000000]; <MAX> – максимальный размер очереди в байтах, принимает значения в диапазоне [1..1000000];

Шаг	Описание	Команда	Ключи
			<APS> – средний размер пакета в байтах, принимает значение в диапазоне [1..10000000]; <APS-NUM> – количество пакетов среднего размера, разрешенных для кратковременного пропускания, принимает значение в диапазоне [0..10000000]; <PROBABILITY> – вероятность отбрасывания пакетов, принимает значения [0..100].
31	Включить протокол компрессии tcp-заголовков для трафика отдельного класса (при необходимости).	evt(config-class-policy-map)# compression header ip tcp	
32	Включить сервис QoS на интерфейсе/туннеле/сетевом мосту.	evt(config-if-gi)# qos enable	
33	Назначить политику QoS на сконфигурируемом интерфейсе/туннеле/сетевом мосту для классификации входящего (input) или приоритизации исходящего (output) трафика.	evt(config-if-gi)# service-policy { input output } <NAME>	<NAME> – имя QoS-политики, задаётся строкой до 31 символа.

Пример настройки

Задача:

Классифицировать входящий трафик по подсетям (10.0.11.0/24, 10.0.12.0/24), произвести маркировку по DSCP (38 и 42) и разграничение по подсетям (40 Мбит/с и 60 Мбит/с), ограничить общую полосу до 250 Мбит/с, остальной трафик обрабатывать через механизм SFQ.



Решение:

Настроим списки доступа для фильтрации по подсетям, выходим в глобальный режим конфигурации:

```

evt(config)# ip access-list extended fl1
evt(config-acl)# rule 1
evt(config-acl-rule)# action permit
evt(config-acl-rule)# match protocol any
evt(config-acl-rule)# match source-address 10.0.11.0 255.255.255.0
evt(config-acl-rule)# match destination-address any
evt(config-acl-rule)# enable
evt(config-acl-rule)# exit
evt(config-acl)# exit
evt(config)# ip access-list extended fl2
evt(config-acl)# rule 1
evt(config-acl-rule)# action permit
evt(config-acl-rule)# match protocol any
evt(config-acl-rule)# match source-address 10.0.12.0 255.255.255.0
evt(config-acl-rule)# match destination-address any
evt(config-acl-rule)# enable
evt(config-acl-rule)# exit
evt(config-acl)# exit

```

Создаем классы fl1 и fl2, указываем соответствующие списки доступа, настраиваем маркировку:

```

evt(config)# class-map fl1
evt(config-class-map)# set dscp 38
evt(config-class-map)# match access-group fl1
evt(config-class-map)# exit
evt(config)# class-map fl2
evt(config-class-map)# set dscp 42
evt(config-class-map)# match access-group fl2
evt(config-class-map)# exit

```

Создаём политику и определяем ограничение общей полосы пропускания:

```

evt(config)# policy-map fl
evt(config-policy-map)# shape average 250000

```

Осуществляем привязку класса к политике, настраиваем ограничение полосы пропускания и выходим:

```

evt(config-policy-map)# class fl1
evt(config-class-policy-map)# shape average 40000
evt(config-class-policy-map)# exit
evt(config-policy-map)# class fl2
evt(config-class-policy-map)# shape average 60000
evt(config-class-policy-map)# exit

```

Для настройки ограничения полосы пропускания в процентах необходимо использовать команду **shape average percent**.

Для другого трафика настраиваем класс с режимом SFQ:

```
evt(config-policy-map)# class class-default
evt(config-class-policy-map)# mode sfq
evt(config-class-policy-map)# fair-queue 800
evt(config-class-policy-map)# exit
evt(config-policy-map)# exit
```

Включаем QoS на интерфейсах, политику на входе интерфейса gi 1/0/1 для классификации и на выходе gi1/0/2 для применения ограничений и режима SFQ для класса по умолчанию:

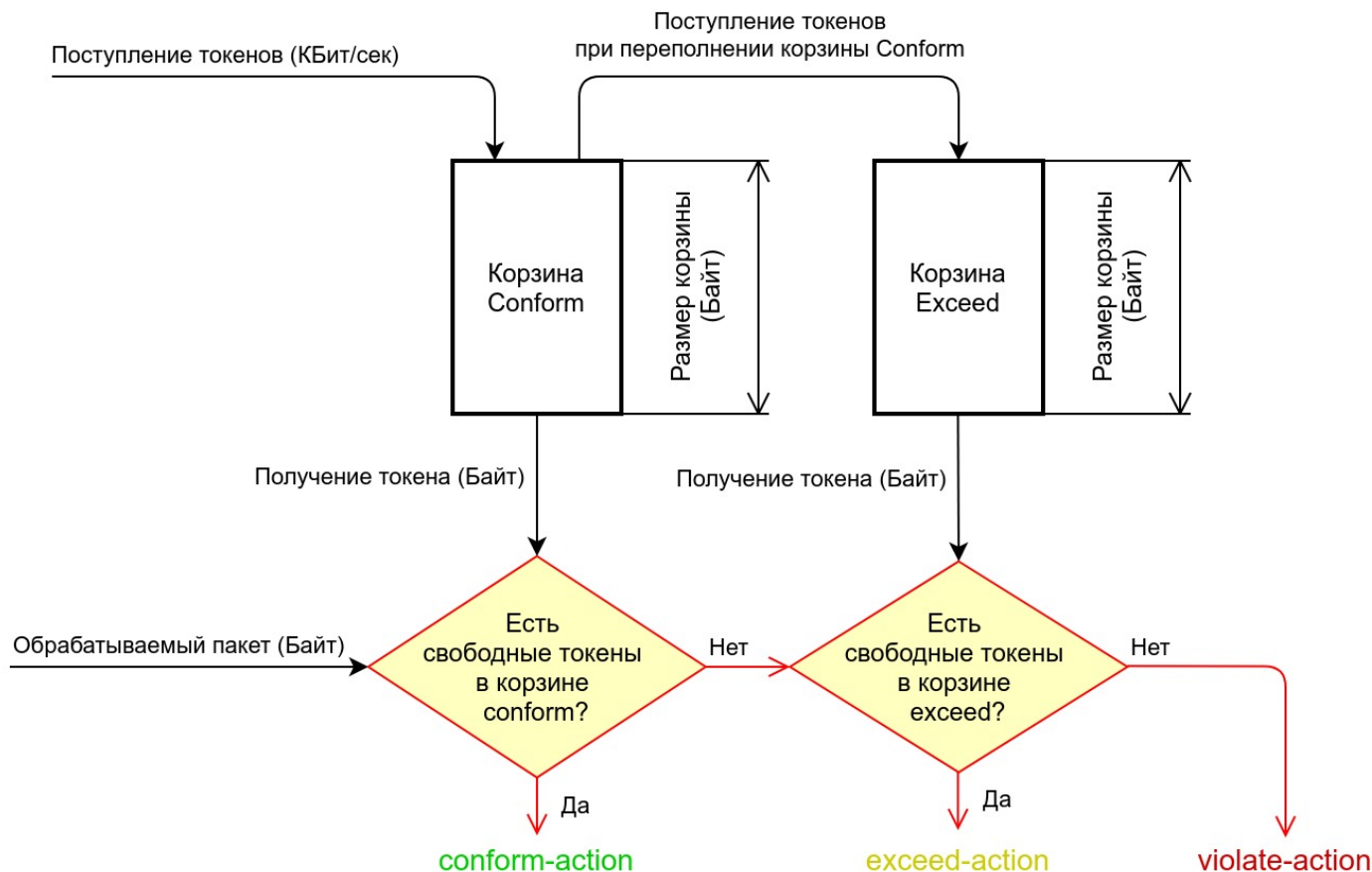
```
evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# qos enable
evt(config-if-gi)# service-policy input fl
evt(config-if-gi)# exit
evt(config)# interface gigabitethernet 1/0/2
evt(config-if-gi)# qos enable
evt(config-if-gi)# service-policy output fl
evt(config-if-gi)# exit
```

Для просмотра статистики используется команда:

```
evt# show qos policy statistics gigabitethernet 1/0/2
```


Механизм работы полисера

Механизм полисера реализован по алгоритму однокоростного трехцветного полисера (Single Rate Three Color Marker/Policers).



У такого механизма есть две корзины токенов (conform и exceed), каждая из которых имеет свой размер. Conform-корзина наполняется токенами до определенного размера с течением времени. Корзина exceed наполняется излишками токенов корзины conform.

Обрабатываемый evt трафик забирает из корзин токены размером, соответствующим размеру пакета. Если размер пришедшего пакета покрывает токены корзины conform, то пакет окрасится в «зелёный», и для него применится действие, соответствующее настройке conform-action. Если токенов в conform-корзине не хватило, но есть достаточно токенов в корзине exceed, то пакет окрасится в «жёлтый», и применится действие exceed-action. Если токенов недостаточно в обеих корзинах, то пакет будет окрашен в «красный», и применится действие violate-action.

Действия conform-action, exceed-action, violate-action определяются одним из следующих вариантов:

- пропустить (permit);
- отбросить (deny);
- пропустить и изменить cos/dscp (set cos, set dscp).

6.2.5 Управление безопасностью

- [Настройка AAA](#)
 - [Алгоритм настройки локальной аутентификации](#)
 - [Алгоритм настройки AAA по протоколу RADIUS](#)
 - [Алгоритм настройки AAA по протоколу TACACS](#)
 - [Алгоритм настройки AAA по протоколу LDAP](#)
 - [Пример настройки аутентификации по Telnet через RADIUS-сервер](#)
- [Настройка привилегий команд](#)
 - [Алгоритм настройки](#)
 - [Пример настройки привилегий команд](#)
- [Конфигурирование Firewall](#)
 - [Алгоритм настройки](#)
 - [Пример настройки Firewall](#)
 - [Пример настройки фильтрации приложений \(DPI\)](#)
- [Настройка списков доступа \(ACL\)](#)
 - [Алгоритм настройки](#)
 - [Пример настройки списка доступа](#)

Настройка AAA

AAA (Authentication, Authorization, Accounting) – используется для описания процесса предоставления доступа и контроля над ним.

- Authentication (аутентификация) – сопоставление персоны (запроса) существующей учётной записи в системе безопасности. Осуществляется по логину, паролю.
- Authorization (авторизация, проверка полномочий, проверка уровня доступа) – сопоставление учётной записи в системе и определённых полномочий.
- Accounting (учёт) – слежение за подключением пользователя или внесенным им изменениям.

 **Конфигурация на маршрутизаторах EVT и EVS производится с помощью одинаковых команд. Ниже приведены примеры настройки EVT.**

Алгоритм настройки локальной аутентификации

Шаг	Описание	Команда	Ключи
1	Указать local в качестве метода аутентификации.	evt(config)# aaa authentication login { default <NAME> } <METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]	<NAME> – имя списка, задаётся строкой до 31 символа. Способы аутентификации: • local – аутентификация с помощью локальной базы пользователей; • tacacs – аутентификация по списку TACACS-серверов; • radius – аутентификация по списку RADIUS-серверов; • ldap – аутентификация по списку LDAP-серверов.
2	Указать enable в качестве способа аутентификации повышения привилегий пользователей.	evt(config)# aaa authentication enable <NAME><METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]	<NAME> – имя списка, задаётся строкой до 31 символа. Способы аутентификации: • local – аутентификация с помощью локальной базы пользователей; • tacacs – аутентификация по списку TACACS-серверов; • radius – аутентификация по списку RADIUS-серверов; • ldap – аутентификация по списку LDAP-серверов.

Шаг	Описание	Команда	Ключи
3	Указать способ перебора методов аутентификации в случае отказа (не обязательно).	evt(config)# aaa authentication mode <MODE>	<MODE> – способы перебора методов: • chain – если сервер вернул FAIL, перейти к следующему в цепочке методу аутентификации; • break – если сервер вернул FAIL, прекратить попытки аутентификации. Если сервер недоступен, продолжить попытки аутентификации следующими в цепочке методами. Значение по умолчанию: chain.
4	Указать количество неудачных попыток аутентификации для блокировки логина пользователя и время блокировки (не обязательно).	evt(config)# aaa authentication attempts max-fail <COUNT> <TIME>	<COUNT> – количество неудачных попыток аутентификации, после которых произойдет блокировка пользователя, принимает значения [1..65535]; <TIME> – интервал времени в минутах, на который будет заблокирован пользователь, принимает значения [1..65535]. Значение по умолчанию: <COUNT> – 5; <TIME> – 300.
5	Включить запрос на смену пароля по умолчанию для пользователя admin (не обязательно).	evt(config)# security passwords default-expired	
6	Включить режим запрета на использование ранее установленных паролей локальных пользователей (не обязательно).	evt(config)# security passwords history <COUNT>	<COUNT> – количество паролей, сохраняемых в памяти маршрутизатора. Принимает значение в диапазоне [1..15]. Значение по умолчанию: 0.

Шаг	Описание	Команда	Ключи
7	Установить время действия пароля локального пользователя (не обязательно).	evt(config)# security passwords lifetime <TIME>	<TIME> – интервал времени действия пароля в днях. Принимает значение в диапазоне [1..365]. По умолчанию: время действия пароля локального пользователя не ограничено.
8	Установить ограничение на минимальную длину пароля локального пользователя и ENABLE-пароля (не обязательно).	evt(config)# security passwords min-length <NUM>	<NUM> – минимальное количество символов в пароле. Принимает значение в диапазоне [8..128]. Значение по умолчанию: 0.
9	Установить ограничение на максимальную длину пароля локального пользователя и ENABLE-пароля (не обязательно).	evt(config)# security passwords max-length <NUM>	<NUM> – максимальное количество символов в пароле. Принимает значение в диапазоне [8..128]. Значение по умолчанию: не ограничено.
10	Установить минимальное количество типов символов, которые должны присутствовать в пароле локального пользователя и ENABLE-пароле (не обязательно).	evt(config)# security passwords symbol-types <COUNT>	<COUNT> – минимальное количество типов символов в пароле. Принимает значение в диапазоне [1..4]. Значение по умолчанию: 1.
11	Установить минимальное количество строчных букв в пароле локального пользователя и ENABLE-пароле (не обязательно).	evt(config)# security passwords lower-case <COUNT>	<COUNT> – минимальное количество строчных букв в пароле локального пользователя и ENABLE-пароле. Принимает значение в диапазоне [0..128]. Значение по умолчанию: 0.
12	Установить минимальное количество прописных (заглавных) букв в пароле локального пользователя и ENABLE-пароле (не обязательно).	evt(config)# security passwords upper-case <COUNT>	<COUNT> – минимальное количество прописных (заглавных) букв в пароле. Принимает значение в диапазоне [0..128]. Значение по умолчанию: 0.
13	Установить минимальное количество цифр в пароле локального пользователя и ENABLE-пароле (не обязательно).	evt(config)# security passwords numeric-count <COUNT>	<COUNT> – минимальное количество цифр в пароле. Принимает значение в диапазоне [0..128]. Значение по умолчанию: 0.

Шаг	Описание	Команда	Ключи
14	Установить минимальное количество специальных символов в пароле локального пользователя и ENABLE-пароле (не обязательно).	evt(config)# security passwords special-case <COUNT>	<COUNT> – минимальное количество специальных символов в пароле. Принимает значение в диапазоне [0..128]. Значение по умолчанию: 0.
15	Добавить пользователя в локальную базу и перейти в режим настройки параметров пользователя.	evt(config)# username <NAME>	<NAME> – имя пользователя, задаётся строкой до 31 символа.
16	Установить пароль пользователя.	evt(config-user)# password { <CLEAR-TEXT> encrypted <HASH_SHA512> }	<CLEAR-TEXT> – пароль, задаётся строкой [8 .. 32] символов, принимает значения [0-9a-fA-F]; <HASH_SHA512> – хеш пароля по алгоритму sha512, задаётся строкой из 110 символов.
17	Установить уровень привилегий пользователя.	evt(config-user)# privilege <PRIV>	<PRIV> – необходимый уровень привилегий. Принимает значение [1..15].
18	Указать метод аутентификации SSH-сессий для пользователя (не обязательно).	evt(config-user)# ssh authentication method <METHOD>	<METHOD> – метод аутентификации SSH-сессий. Может принимать значения: • password – аутентификация пользователя при открытии SSH-сессий может быть произведена только по паролю; • pubkey – аутентификация пользователя при открытии SSH-сессий может быть произведена только по публичному ключу; • both – аутентификация пользователя при открытии SSH-сессий может быть произведена как по паролю, так и по публичному ключу.

Шаг	Описание	Команда	Ключи
19	Указать имя файла публичного ключа, который будет использован при аутентификации SSH-сессии пользователя (не обязательно).	evt(config-user)# ssh pubkey <NAME>	<NAME> – имя файла публичного ключа, расположенного в разделе crypto:public-key, задаётся строкой до 31 символа.
20	Перейти в режим конфигурирования соответствующего терминала.	evt(config)# line console или evt(config)# line telnet или evt(config)# line ssh	
21	Активировать список аутентификации входа пользователей в систему.	evt(config-line-ssh)# login authentication <NAME>	<NAME> – имя списка, задаётся строкой до 31 символа.
22	Активировать список аутентификации повышения привилегий пользователей.	evt(config-line-ssh)# enable authentication <NAME>	<NAME> – имя списка, задаётся строкой до 31 символа.
23	Задать интервал, по истечении которого будет разрываться бездействующая сессия.	evt(config-line-ssh)# exec-timeout <SEC>	<SEC> – период времени в минутах, принимает значения [1..65535].

Алгоритм настройки AAA по протоколу RADIUS

Шаг	Описание	Команда	Ключи
1	Задать глобальное значение кода DSCP для использования в IP-заголовках исходящих пакетов RADIUS-сервера (не обязательно).	evt(config)# radius-server dscp <DSCP>	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 63.
2	Задать глобальное значение количества перезапросов к последнему активному RADIUS-серверу (не обязательно).	evt(config)# radius-server retransmit <COUNT>	<COUNT> – количество перезапросов к RADIUS-серверу, принимает значения [1..10]. Значение по умолчанию: 1.
3	Задать глобальное значение интервала, по истечении которого маршрутизатор считает, что RADIUS-сервер недоступен (не обязательно).	evt(config)# radius-server timeout <SEC>	<SEC> – период времени в секундах, принимает значения [1..30]. Значение по умолчанию: 3 секунды.

Шаг	Описание	Команда	Ключи
4	Добавить RADIUS-сервер в список используемых серверов и перейти в режим его конфигурирования.	evt(config)# radius-server host { <IP-ADDR> <IPv6-ADDR> } [vrf <VRF>]	<IP-ADDR> – IP-адрес RADIUS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPv6-ADDR> – IPv6-адрес RADIUS-сервера, задаётся в виде X:X:X:X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF] <VRF> – имя экземпляра VRF, задаётся строкой до 31 символа.
5	Задать описание конфигурируемого RADIUS-сервера (не обязательно).	evt(config-radius-server)# description <description>	<description> – описание RADIUS-сервера, задаётся строкой до 255 символов.
6	Указать количество неудачных попыток аутентификации для блокировки логина пользователя и времени блокировки (не обязательно).	evt(config-radius-server)# aaa authentication attempts max-fail <COUNT> <TIME>	<COUNT> – количество неудачных попыток аутентификации, после которых произойдет блокировка пользователя, принимает значения [1..65535]; <TIME> – интервал времени в секундах, на который будет заблокирован пользователь, принимает значения [1..65535]. Значение по умолчанию: <COUNT> – 5; <TIME> – 300.
7	Задать пароль для аутентификации на удаленном RADIUS-сервере.	evt(config-radius-server)# key ascii-text { <TEXT> encrypted <ENCRYPTED-TEXT> }	<TEXT> – строка [8..16] ASCII-символов; <ENCRYPTED-TEXT> – зашифрованный пароль, размером [8..16] байт, задаётся строкой [16..32] символов.

Шаг	Описание	Команда	Ключи
8	Задать приоритет использования удаленного RADIUS-сервера (не обязательно).	evt(config-radius-server)# priority <PRIORITY>	<PRIORITY> – приоритет использования удаленного сервера, принимает значения [1..65535]. Чем ниже значение, тем приоритетнее сервер. Значение по умолчанию: 1.
9	Задать интервал, по истечении которого маршрутизатор считает, что данный RADIUS-сервер недоступен (не обязательно).	evt(config-radius-server)# timeout <SEC>	<SEC> – период времени в секундах, принимает значения [1..30]. Значение по умолчанию: используется значение глобального таймера.
10	Задать IPv4/IPv6-адрес, который будет использоваться в качестве IPv4/IPv6-адреса источника в отправляемых RADIUS-пакетах.	evt(config-radius-server)# source-address { <ADDR> object-group <NETWORK_OBJ_GROUP_NAME> }	<ADDR> – IP-адрес источника, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве source address.
11	Задать интерфейс или туннель маршрутизатора, IPv4/IPv6-адрес которого будет использоваться в качестве IPv4/IPv6-адреса источника в отправляемых RADIUS-пакетах.	evt(config-radius-server)# source-interface { <IF> <TUN> }	<IF> – имя интерфейса устройства, задается в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора; <TUN> – имя туннеля устройства, задается в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора.

Шаг	Описание	Команда	Ключи
12	Указать radius в качестве метода аутентификации.	evt(config)# aaa authentication login { default <NAME> } <METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]	<NAME> – имя списка, задаётся строкой до 31 символа. Способы аутентификации: • local – аутентификация с помощью локальной базы пользователей; • tacacs – аутентификация по списку TACACS-серверов; • radius – аутентификация по списку RADIUS-серверов; • ldap – аутентификация по списку LDAP-серверов.
13	Указать radius в качестве способа аутентификации повышения привилегий пользователей.	evt(config)# aaa authentication enable <NAME><METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]	<NAME> – имя списка строка до 31 символа; • default – имя списка по умолчанию. <METHOD> – способы аутентификации: • enable – аутентификация с помощью enable-паролей; • tacacs – аутентификация по протоколу TACACS; • radius – аутентификация по протоколу RADIUS; • ldap – аутентификация по протоколу LDAP.
14	Указать способ перебора методов аутентификации в случае отказа (не обязательно).	evt(config)# aaa authentication mode <MODE>	<MODE> – способы перебора методов: • chain – если сервер вернул FAIL, переход к следующему в цепочке методу аутентификации; • break – если сервер вернул FAIL, прекратить попытки аутентификации. Если сервер недоступен, продолжить попытки аутентификации следующими в цепочке методами. Значение по умолчанию: chain.

Шаг	Описание	Команда	Ключи
15	Сконфигурировать radius в списке способов учета сессий пользователей (не обязательно).	evt(config)# aaa accounting login start-stop <METHOD 1> [<METHOD 2>]	<METHOD> – способы учета: • tacacs – учет сессий по протоколу TACACS; • radius – учет сессий по протоколу RADIUS.
16	Перейти в режим конфигурирования соответствующего терминала.	evt(config)# line <TYPE>	<TYPE> – тип консоли: • console – локальная консоль; • ssh – защищенная удаленная консоль.
17	Активировать список аутентификации входа пользователей в систему.	evt(config-line-console)# login authentication <NAME>	<NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 8.
18	Активировать список аутентификации повышения привилегий пользователей.	evt(config-line-console)# enable authentication <NAME>	<NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 9.

Алгоритм настройки AAA по протоколу TACACS

Шаг	Описание	Команда	Ключи
1	Задать глобальное значение кода DSCP для использования в IP-заголовках исходящих пакетов TACACS-сервера (не обязательно).	evt(config)# tacacs-server dscp <DSCP>	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 63.
2	Задать глобальное значение интервала, по истечении которого маршрутизатор считает, что TACACS-сервер недоступен (не обязательно).	evt(config)# tacacs-server timeout <SEC>	<SEC> – период времени в секундах, принимает значения [1..30]. Значение по умолчанию: 3 секунды.

Шаг	Описание	Команда	Ключи
3	Добавить TACACS-сервер в список используемых серверов и перейти в режим его конфигурирования.	evt(config)# tacacs -server host { <IP-ADDR> <IPv6-ADDR> } [vrf <VRF>]	<IP-ADDR> – IP-адрес TACACS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255] <IPv6-ADDR> – IPv6-адрес TACACS -сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF] <VRF> – имя экземпляра VRF, задаётся строкой до 31 символа.
4	Задать описание конфигурируемого TACACS-сервера (не обязательно).	evt(config-tacacs-server)# description <description>	<description> – описание TACACS-сервера, задаётся строкой до 255 символов.
5	Указать количество неудачных попыток аутентификации для блокировки логина пользователя и время блокировки (не обязательно)	evt(config-tacacs-server)# aaa authentication attempts max-fail <COUNT> <TIME>	<COUNT> – количество неудачных попыток аутентификации, после которых произойдет блокировка пользователя, принимает значения [1..65535]; <TIME> – интервал времени в минутах, на который будет заблокирован пользователь, принимает значения [1..65535]. Значение по умолчанию: <COUNT> – 5; <TIME> – 300.
6	Задать пароль для аутентификации на удаленном TACACS-сервере	evt(config-tacacs-server)# key ascii-text { <TEXT> encrypted <ENCRYPTED-TEXT> }	<TEXT> – строка [8..16] ASCII-символов; <ENCRYPTED-TEXT> – зашифрованный пароль, размером [8..16] байт, задаётся строкой [16..32] символов.

Шаг	Описание	Команда	Ключи
7	Задать номер порта для обмена данными с удаленным TACACS-сервером (не обязательно).	evt(config-tacacs-server)# port <PORT>	<PORT> – номер TCP-порта для обмена данными с удаленным сервером, принимает значения [1..65535]. Значение по умолчанию: 49 для TACACS-сервера.
8	Задать приоритет использования удаленного TACACS сервера (не обязательно).	evt(config-tacacs-server)# priority <PRIORITY>	<PRIORITY> – приоритет использования удаленного сервера, принимает значения [1..65535]. Чем ниже значение, тем приоритетнее сервер. Значение по умолчанию: 1.
9	Задать IPv4/IPv6-адрес, который будет использоваться в качестве IP/IPv6-адреса источника в отправляемых TACACS-пакетах.	evt(config-tacacs-server)# source-address { <ADDR> object-group <NETWORK_OBJ_GROUP_NAME> }	<ADDR> – IP-адрес источника, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве source address.
10	Задать интерфейс или туннель маршрутизатора, IPv4/IPv6-адрес которого будет использоваться в качестве IPv4/IPv6-адреса источника в отправляемых TACACS-пакетах.	evt(config-tacacs-server)# source-interface { <IF> <TUN> }	<IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора; <TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора.

Шаг	Описание	Команда	Ключи
11	Указать TACACS в качестве способа аутентификации повышения привилегий пользователей.	evt(config)# aaa authentication enable <NAME><METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]	<NAME> – имя списка строка до 31 символа; • default – имя списка по умолчанию. <METHOD> – способы аутентификации: • enable – аутентификация с помощью enable-паролей; • tacacs – аутентификация по протоколу TACACS; • radius – аутентификация по протоколу RADIUS; • ldap – аутентификация по протоколу LDAP.
12	Указать способ перебора методов аутентификации в случае отказа (не обязательно).	evt(config)# aaa authentication mode <MODE>	<MODE> – способы перебора методов: • chain – если сервер вернул FAIL, переход к следующему в цепочке методу аутентификации; • break – если сервер вернул FAIL, прекратить попытки аутентификации. Если сервер недоступен, продолжить попытки аутентификации следующими в цепочке методами. Значение по умолчанию: chain.
13	Сконфигурировать список способов учета команд, введенных в CLI (не обязательно).	evt(config)# aaa accounting commands stop-only tacacs	
14	Сконфигурировать tacacs в списке способов учета сессий пользователей (не обязательно).	evt(config)# aaa accounting login start-stop <METHOD 1> [<METHOD 2>]	<METHOD> – способы учета: • tacacs – учет сессий по протоколу TACACS; • radius – учет сессий по протоколу RADIUS.
15	Перейти в режим конфигурирования соответствующего терминала.	evt(config)# line <TYPE>	<TYPE> – тип консоли: • console – локальная консоль; • ssh – защищенная удаленная консоль.

Шаг	Описание	Команда	Ключи
16	Активировать список аутентификации входа пользователей в систему.	evt(config-line-console)# login authentication <NAME>	<NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 7.
17	Активировать список аутентификации повышения привилегий пользователей.	evt(config-line-console)# enable authentication <NAME>	<NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 8.

Алгоритм настройки AAA по протоколу LDAP

Шаг	Описание	Команда	Ключи
1	Задать базовый DN (Distinguished name), который будет использоваться при поиске пользователей.	evt(config)# ldap-server base-dn <NAME>	<NAME> – базовый DN, задается строкой до 255 символов.
2	Задать интервал, по истечении которого устройство считает, что LDAP-сервер недоступен (не обязательно).	evt(config)# ldap-server bind timeout <SEC>	<SEC> – период времени в секундах, принимает значения [1..30]. Значение по умолчанию: 3 секунды.
3	Задать DN (Distinguished name) пользователя с правами администратора, под которым будет происходить авторизация на LDAP-сервере при поиске пользователей.	evt(config)# ldap-server bind authenticate root-dn <NAME>	<NAME> – DN пользователя с правами администратора, задается строкой до 255 символов.
4	Задать пароль пользователя с правами администратора, под которым будет происходить авторизация на LDAP-сервере при поиске пользователей.	evt(config)# ldap-server bind authenticate root-password ascii-text { <TEXT> encrypted <ENCRYPTED-TEXT> }	<TEXT> – строка [8..16] ASCII-символов; <ENCRYPTED-TEXT> – зашифрованный пароль, размером [8..16] байт, задаётся строкой [16..32] символов.
5	Задать имя класса объектов, среди которых необходимо выполнять поиск пользователей на LDAP-сервере (не обязательно).	evt(config)# ldap-server search filter user-object-class <NAME>	<NAME> – имя класса объектов, задаётся строкой до 127 символов. Значение по умолчанию: posixAccount.

Шаг	Описание	Команда	Ключи
6	Задать область поиска пользователей в дереве LDAP-сервера (не обязательно).	evt(config)# ldap-server search scope <SCOPE>	<SCOPE> – область поиска пользователей на LDAP-сервере, принимает следующие значения: • onelevel – выполнять поиск в объектах на следующем уровне после базового DN в дереве LDAP-сервера; • subtree – выполнять поиск во всех объектах поддерева базового DN в дереве LDAP-сервера. Значение по умолчанию: subtree.
7	Задать интервал, по истечении которого устройство считает, что LDAP-сервер не нашел записей пользователей, подходящих под условие поиска (не обязательно).	evt(config)# ldap-server search timeout <SEC>	<SEC> – период времени в секундах, принимает значения [0..30] Значение по умолчанию: 0 – устройство ожидает завершения поиска и получения ответа от LDAP-сервера.
8	Задать имя атрибута объекта, со значением которого идет сравнение имени искомого пользователя на LDAP-сервере (не обязательно).	evt(config)# ldap-server naming-attribute <NAME>	<NAME> – имя атрибута объекта, задаётся строкой до 127 символов. Значение по умолчанию: uid.
9	Задать имя атрибута объекта, значение которого будет определять начальные привилегии пользователя на устройстве (не обязательно).	evt(config)# ldap-server privilege-level-attribute <NAME>	<NAME> – имя атрибута объекта, задаётся строкой до 127 символов. Значение по умолчанию: priv-lvl.
10	Задать глобальное значение кода DSCP для использования в IP-заголовках исходящих пакетов LDAP-сервера (не обязательно).	evt(config)# ldap-server dscp <DSCP>	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 63.

Шаг	Описание	Команда	Ключи
11	Добавить LDAP-сервер в список используемых серверов и перейти в режим его конфигурирования.	evt(config)# ldap-server host { <IP-ADDR> <IPv6-ADDR> } [vrf <VRF>]	<IP-ADDR> – IP-адрес LDAP-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255] <IPv6-ADDR> – IPv6-адрес LDAP-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF] <VRF> – имя экземпляра VRF, задается строкой до 31 символа.
12	Задать описание конфигурируемого LDAP-сервера (не обязательно).	evt(config-ldap-server)# description <description>	<description> – описание LDAP-сервера, задается строкой до 255 символов.
12	Указать количество неудачных попыток аутентификации для блокировки логина пользователя и время блокировки (не обязательно).	evt(config-ldap-server)# aaa authentication attempts max-fail <COUNT> <TIME>	<COUNT> – количество неудачных попыток аутентификации, после которых произойдет блокировка пользователя, принимает значения [1..65535]; <TIME> – интервал времени в минутах, на который будет заблокирован пользователь, принимает значения [1..65535]. Значение по умолчанию: <COUNT> – 5; <TIME> – 300.
13	Задать номер порта для обмена данными с удаленным LDAP-сервером (не обязательно).	evt(config-ldap-server)# port <PORT>	<PORT> – номер TCP-порта для обмена данными с удаленным сервером, принимает значения [1..65535]. Значение по умолчанию: 389 для LDAP-сервера.

Шаг	Описание	Команда	Ключи
14	Задать приоритет использования удаленного LDAP-сервера (не обязательно).	evt(config-ldap-server)# priority <PRIORITY>	<PRIORITY> – приоритет использования удаленного сервера, принимает значения [1..65535]. Чем ниже значение, тем приоритетнее сервер. Значение по умолчанию: 1.
15	Задать IPv4/IPv6-адрес, который будет использоваться в качестве IP/IPv6-адреса источника в отправляемых LDAP-пакетах.	evt(config-ldap-server)# source-address { <ADDR> object-group <NETWORK_OBJ_GROUP_NAME> }	<ADDR> – IP-адрес источника, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве source address.
16	Задать интерфейс или туннель маршрутизатора, IPv4/IPv6-адрес которого будет использоваться в качестве IPv4/IPv6-адреса источника в отправляемых LDAP-пакетах.	evt(config-ldap-server)# source-interface { <IF> <TUN> }	<IF> – имя интерфейса устройства, задается в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора; <TUN> – имя туннеля устройства, задается в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора.
17	Указать LDAP в качестве метода аутентификации.	evt(config)# aaa authentication login { default <NAME> } <METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]	<NAME> – имя списка, задается строкой до 31 символа. Способы аутентификации: • local – аутентификация с помощью локальной базы пользователей; • tacacs – аутентификация по списку TACACS-серверов; • radius – аутентификация по списку RADIUS-серверов; • ldap – аутентификация по списку LDAP-серверов.

Шаг	Описание	Команда	Ключи
18	Указать LDAP в качестве способа аутентификации повышения привилегий пользователей.	evt(config)# aaa authentication enable <NAME> <METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]	<NAME> – имя списка строка до 31 символа; • default – имя списка по умолчанию. <METHOD> – способы аутентификации: • enable – аутентификация с помощью enable-паролей; • tacacs – аутентификация по протоколу TACACS; • radius – аутентификация по протоколу RADIUS; • ldap – аутентификация по протоколу LDAP.
19	Указать способ перебора методов аутентификации в случае отказа.	evt(config)# aaa authentication mode <MODE>	<MODE> – способы перебора методов: • chain – если сервер вернул FAIL, переход к следующему в цепочке методу аутентификации; • break – если сервер вернул FAIL, прекратить попытки аутентификации. Если сервер недоступен, продолжить попытки аутентификации следующими в цепочке методами. Значение по умолчанию: chain.
20	Перейти в режим конфигурирования соответствующего терминала.	evt(config)# line <TYPE>	<TYPE> – тип консоли: • console – локальная консоль; • ssh – защищенная удаленная консоль.
21	Активировать список аутентификации входа пользователей в систему.	evt(config-line-console)# login authentication <NAME>	<NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 14.
22	Активировать список аутентификации повышения привилегий пользователей.	evt(config-line-console)# enable authentication <NAME>	<NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 15.

Пример настройки аутентификации по Telnet через RADIUS-сервер

Задача:

Настроить аутентификацию пользователей, подключающихся по Telnet, через RADIUS (192.168.16.1/24).

Решение:

Настроим подключение к RADIUS-серверу и укажем ключ (password):

```
evt# configure
evt(config)# radius-server host 192.168.16.1
evt(config-radius-server)# key ascii-text encrypted 8CB5107EA7005AFF
evt(config-radius-server)# exit
```

Создадим профиль аутентификации:

```
evt(config)# aaa authentication login log radius
```

Укажем режим аутентификации, используемый при подключении по Telnet-протоколу:

```
evt(config)# line telnet
evt(config-line-telnet)# login authentication log
evt(config-line-telnet)# exit
evt(config)# exit
```

Просмотреть информацию по настройкам подключения к RADIUS-серверу можно командой:

```
evt# show aaa radius-servers
```

Посмотреть профили аутентификации можно командой:

```
evt# show aaa authentication
```

Настройка привилегий команд

Настройка привилегий команд является гибким инструментом, который позволяет назначить набору команд минимально необходимый уровень пользовательских привилегий (1-15). В дальнейшем при создании пользователя можно задать уровень привилегий, определяя ему доступный набор команд.

- 1-9 уровни – позволяют использовать все команды мониторинга (show ...);
- 10-14 уровни – позволяют использовать все команды кроме команд перезагрузки устройства, управления пользователями и ряда других;
- 15 уровень – позволяет использовать все команды.

Алгоритм настройки

Для изменения минимального уровня привилегий необходимого для выполнения команды CLI используется команда:

```
evt(config)# privilege <COMMAND-MODE> level <PRIV><COMMAND>
```

<COMMAND-MODE> – командный режим;

<PRIV> – необходимый уровень привилегий поддерева команд, принимает значение [1..15];

<COMMAND> – поддерево команд, задается строкой до 255 символов.

Пример настройки привилегий команд

Задача:

Перевести все команды просмотра информации об интерфейсах на уровень привилегий 10, кроме команды «show interfaces bridges». Команду «show interfaces bridges» перевести на уровень привилегий 3.

Решение:

В режиме конфигурирования определим команды, разрешенные на использование с уровнем привилегий 10 и уровнем привилегий 3:

```
evt(config)# privilege root level 3 "show interfaces bridge"
evt(config)# privilege root level 10 "show interfaces"
```

Конфигурирование Firewall

Firewall – комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Алгоритм настройки

Порядок обработки транзитного трафика правилами firewall

1. Трафик проверяется правилами zone-pair user-zone any.
Если трафик не попал ни под одно из правил текущей zone-pair, переходим к следующему шагу.
2. Если трафик передаётся с одного интерфейса на другой в пределах одной зоны (user-zone), то он проверяется правилами zone-pair user-zone user-zone.
Если трафик не попал ни под одно из правил текущей zone-pair, переходим к следующему шагу.
3. Если трафик передаётся с одного интерфейса на другой в разных зонах, то он проверяется правилами zone-pair user-zone1 user-zone2.
Если трафик не попал ни под одно из правил текущей zone-pair, переходим к следующему шагу.
4. Трафик проверяется правилами zone-pair any any.
Если трафик не попал ни под одно из правил текущей zone-pair, он отбрасывается.

Порядок обработки трафика, терминируемого на маршрутизаторе

1. Трафик проверяется правилами zone-pair any self.
Если трафик не попал ни под одно из правил текущей zone-pair, переходим к следующему шагу.
2. Трафик проверяется правилами zone-pair user-zone self.
Если трафик не попал ни под одно из правил текущей zone-pair, он отбрасывается.

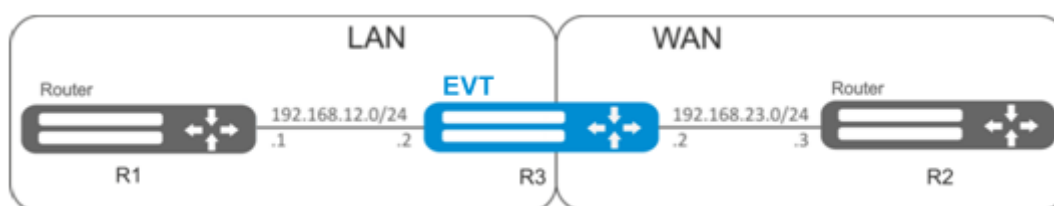
Каждая команда «match» может содержать ключ «not». При использовании данного ключа под правило будут подпадать пакеты, не удовлетворяющие заданному критерию.

Более подробная информация о командах для настройки межсетевого экрана содержится в справочнике команд CLI.

Пример настройки Firewall

Задача:

Разрешить обмен сообщениями по протоколу ICMP между устройствами R1, R2 и маршрутизатором EVT.



Решение:

Для каждой сети evt создадим свою зону безопасности:

```
evt# configure
evt(config)# security zone LAN
evt(config-security-zone)# exit
evt(config)# security zone WAN
evt(config-security-zone)# exit
```

Настроим сетевые интерфейсы и определим их принадлежность к зонам безопасности:

```
evt(config)# interface gi1/0/2
evt(config-if-gi)# ip address 192.168.12.2/24
evt(config-if-gi)# security-zone LAN
evt(config-if-gi)# exit
evt(config)# interface gi1/0/3
evt(config-if-gi)# ip address 192.168.23.2/24
evt(config-if-gi)# security-zone WAN
evt(config-if-gi)# exit
```

Для настройки правил зон безопасности потребуется создать профиль адресов сети «LAN», включающий адреса, которым разрешен выход в сеть «WAN», и профиль адресов сети «WAN».

```

evt(config)# object-group network WAN
evt(config-object-group-network)# ip address-range 192.168.23.2
evt(config-object-group-network)# exit
evt(config)# object-group network LAN
evt(config-object-group-network)# ip address-range 192.168.12.2
evt(config-object-group-network)# exit
evt(config)# object-group network LAN_GATEWAY
evt(config-object-group-network)# ip address-range 192.168.12.1
evt(config-object-group-network)# exit
evt(config)# object-group network WAN_GATEWAY
evt(config-object-group-network)# ip address-range 192.168.23.3
evt(config-object-group-network)# exit

```

Для пропуска трафика из зоны «LAN» в зону «WAN» создадим пару зон и добавим правило, разрешающее проходить ICMP-трафику от R1 к R2. Действие правил разрешается командой *enable*:

```

evt(config)# security zone-pair LAN WAN
evt(config-security-zone-pair)# rule 1
evt(config-security-zone-pair-rule)# action permit
evt(config-security-zone-pair-rule)# match protocol icmp
evt(config-security-zone-pair-rule)# match destination-address object-group WAN_GATEWAY
evt(config-security-zone-pair-rule)# match source-address object-group LAN_GATEWAY
evt(config-security-zone-pair-rule)# enable
evt(config-security-zone-pair-rule)# exit
evt(config-security-zone-pair)# exit

```

Для пропуска трафика из зоны «WAN» в зону «LAN» создадим пару зон и добавим правило, разрешающее проходить ICMP-трафику от R2 к R1. Действие правил разрешается командой *enable*:

```

evt(config)# security zone-pair WAN LAN
evt(config-security-zone-pair)# rule 1
evt(config-security-zone-pair-rule)# action permit
evt(config-security-zone-pair-rule)# match protocol icmp
evt(config-security-zone-pair-rule)# match destination-address object-group LAN_GATEWAY
evt(config-security-zone-pair-rule)# match source-address object-group WAN_GATEWAY
evt(config-security-zone-pair-rule)# enable
evt(config-security-zone-pair-rule)# exit
evt(config-security-zone-pair)# exit

```

На маршрутизаторе всегда существует зона безопасности с именем «self». Если в качестве получателя трафика выступает сам маршрутизатор, то есть трафик не является транзитным, то в качестве параметра указывается зона «self». Создадим пару зон для трафика, идущего из зоны «WAN» в зону «self». Добавим правило, разрешающее проходить ICMP-трафику между R2 и маршрутизатором evt, для того чтобы маршрутизатор начал отвечать на ICMP-запросы из зоны «WAN»:

```

evt(config)# security zone-pair WAN self
evt(config-security-zone-pair)# rule 1
evt(config-security-zone-pair-rule)# action permit
evt(config-security-zone-pair-rule)# match protocol icmp
evt(config-security-zone-pair-rule)# match destination-address object-group WAN
evt(config-security-zone-pair-rule)# match source-address object-group WAN_GATEWAY
evt(config-security-zone-pair-rule)# enable

```

```

evt(config-security-zone-pair-rule)# exit
evt(config-security-zone-pair)# exit

```

Создадим пару зон для трафика, идущего из зоны «LAN» в зону «self». Добавим правило, разрешающее проходить ICMP-трафику между R1 и evt, для того чтобы маршрутизатор начал отвечать на ICMP-запросы из зоны «LAN»:

```

evt(config)# security zone-pair LAN self
evt(config-security-zone-pair)# rule 1
evt(config-security-zone-pair-rule)# action permit
evt(config-security-zone-pair-rule)# match protocol icmp
evt(config-security-zone-pair-rule)# match destination-address object-group LAN
evt(config-security-zone-pair-rule)# match source-address object-group LAN_GATEWAY
evt(config-security-zone-pair-rule)# enable
evt(config-security-zone-pair-rule)# exit
evt(config-security-zone-pair)# exit
evt(config)# exit

```

Посмотреть членство портов в зонах можно с помощью команды:

```

evt# show security zone

```

Посмотреть пары зон и их конфигурацию можно с помощью команд:

```

evt# show security zone-pair
evt# show security zone-pair configuration

```

Посмотреть активные сессии можно с помощью команд:

```

evt# show ip firewall sessions

```

Пример настройки фильтрации приложений (DPI)

⚠ Использование механизма фильтрации приложений многократно снижает производительность маршрутизатора из-за необходимости проверки определенного объема пакетов в каждой сессии. Производительность снижается с ростом количества выбранных приложений для фильтрации. Механизм фильтрации приложений работает только для транзитных пакетов и только в режиме черного списка (запрет прохождения трафика для указанных приложений).

Задача:

Блокировать доступ пользователей в локальной сети к Telegram, Facebook Messenger (запрещенная на территории Российской Федерации организация) и Skype.



Решение:

Для каждой сети evt создадим свою зону безопасности:

```
evt# configure
evt(config)# security zone LAN
evt(config-security-zone)# exit
evt(config)# security zone WAN
evt(config-security-zone)# exit
```

Настроим сетевые интерфейсы и определим их принадлежность к зонам безопасности:

```
evt(config)# interface gi1/0/1
evt(config-if-gi)# ip address 10.0.0.1/24
evt(config-if-gi)# security-zone WAN
evt(config-if-gi)# exit
evt(config)# interface gi1/0/2
evt(config-if-te)# ip address 192.168.0.1/24
evt(config-if-te)# security-zone LAN
evt(config-if-te)# exit
```

Для настройки правил зон безопасности потребуется создать профиль приложений, которые необходимо будет блокировать.

```
evt(config)# object-group application BLACKLIST
evt(config-object-group-application)# application telegram
evt(config-object-group-application)# application facebook-messenger
evt(config-object-group-application)# application skype-teams
evt(config-object-group-application)# exit
```

Для установки правил прохождения трафика из зоны «WAN» в зону «LAN» создадим пару зон и добавим правило, запрещающее проходить трафику приложений, и правило, разрешающее проходить остальному трафику. Действие правил разрешается командой *enable*:

```
evt(config)# security zone-pair WAN LAN
evt(config-security-zone-pair)# rule 1
evt(config-security-zone-pair-rule)# action deny
evt(config-security-zone-pair-rule)# match application BLACKLIST
evt(config-security-zone-pair-rule)# enable
evt(config-security-zone-pair-rule)# exit
evt(config-security-zone-pair)# rule 2
evt(config-security-zone-pair-rule)# action permit
evt(config-security-zone-pair-rule)# enable
evt(config-security-zone-pair-rule)# exit
evt(config-security-zone-pair)# exit
```

Для установки правил прохождения трафика из зоны «LAN» в зону «WAN» создадим пару зон и добавим правило, запрещающее прохождение трафика приложений, и правило, разрешающее прохождение всего остального трафика. Действие правил разрешается командой **enable**:

```

evt(config)# security zone-pair LAN WAN
evt(config-security-zone-pair)# rule 1
evt(config-security-zone-pair-rule)# action deny
evt(config-security-zone-pair-rule)# match application BLACKLIST
evt(config-security-zone-pair-rule)# enable
evt(config-security-zone-pair-rule)# exit
evt(config-security-zone-pair)# rule 2
evt(config-security-zone-pair-rule)# action permit
evt(config-security-zone-pair-rule)# enable
evt(config-security-zone-pair-rule)# exit
evt(config-security-zone-pair)# exit

```

Посмотреть членство портов в зонах можно с помощью команды:

```

evt# show security zone

```

Посмотреть пары зон и их конфигурацию можно с помощью команд:

```

evt# show security zone-pair
evt# show security zone-pair configuration

```

Посмотреть активные сессии можно с помощью команд:

```

evt# show ip firewall sessions

```

Настройка списков доступа (ACL)

Access Control List или ACL — список контроля доступа, содержит правила, определяющие прохождение трафика через интерфейс.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать список контроля доступа и перейти в режим его конфигурирования.	evt(config)# ip access-list extended <NAME>	<NAME> – имя создаваемого списка контроля доступа, задаётся строкой до 31 символа.
2	Указать описание конфигурируемого списка контроля доступа (не обязательно).	evt(config-acl)# description <DESCRIPTION>	<DESCRIPTION> – описание списка контроля доступа, задаётся строкой до 255 символов.

Шаг	Описание	Команда	Ключи
3	Создать правило и перейти в режим его конфигурирования. Правила обрабатываются маршрутизатором в порядке возрастания их номеров.	evt(config-acl)# rule <ORDER>	<ORDER> – номер правила, принимает значения [1...4094].
4	Указать действие, которое должно быть применено для трафика, удовлетворяющего заданным критериям.	evt(config-acl-rule)# action <ACT>	<ACT> – назначаемое действие: • permit – прохождение трафика разрешается; • deny – прохождение трафика запрещается.
5	Установить имя/номер протокола, для которого должно срабатывать правило (не обязательно).	evt(config-acl-rule)# match protocol <TYPE>	<TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre. При указании значения «any» правило будет срабатывать для любых протоколов.
		evt(config-acl-rule)# match protocol-id <ID>	<ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF].
6	Установить IP-адреса отправителя, для которых должно срабатывать правило (не обязательно).	evt(config-acl-rule)# match source-address { <ADDR> <MASK> any }	<ADDR> – IP-адрес отправителя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];
7	Установить IP-адреса получателя, для которых должно срабатывать правило (не обязательно).	evt(config-acl-rule)# match destination-address { <ADDR> <MASK> any }	<MASK> – маска IP-адреса, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Биты маски, установленные в 0, задают биты IP-адреса, исключаемые из сравнения при поиске. При указании значения «any» правило будет срабатывать для любого IP-адреса отправителя/получателя.

Шаг	Описание	Команда	Ключи
8	Установить MAC-адреса отправителя, для которых должно срабатывать правило (не обязательно).	evt(config-acl-rule)# match source-mac <ADDR><WILDCARD>	<ADDR> – MAC-адрес отправителя, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF];
9	Установить MAC-адреса получателя, для которых должно срабатывать правило (не обязательно).	evt(config-acl-rule)# match destination-mac <ADDR><WILDCARD>	<WILDCARD> – маска MAC-адреса, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]. Биты маски, установленные в 0, задают биты MAC-адреса, исключаемые из сравнения при поиске.
10	Установить номер TCP/UDP-порта отправителя, для которого должно срабатывать правило (если указан протокол).	evt(config-acl-rule)# match source-port <TYPE> {<FROM-PORT> - <TO-PORT> <PORT>}	<TYPE> – тип аргумента, устанавливаемый в качестве порта:
11	Установить номер TCP/UDP-порта получателя, для которого должно срабатывать правило (если указан протокол).	evt(config-acl-rule)# match destination-port <TYPE> {<FROM-PORT> - <TO-PORT> <PORT>}	• port-range – указать диапазон портов; • any – установить в качестве порта любой порт. <FROM-PORT> – начальный порт диапазона; <TO-PORT> – конечный порт диапазона; <PORT> - Указание единичного порта
12	Установить значение 802.1p приоритета, для которого должно срабатывать правило (не обязательно).	evt(config-acl-rule)# match cos <COS>	<COS> – значение 802.1p приоритета, принимает значения [0..7].
13	Установить значение кода DSCP, для которого должно срабатывать правило (не обязательно). Невозможно использовать совместно с IP Precedence.	evt(config-acl-rule)# match dscp <DSCP>	<DSCP> – значение кода DSCP, принимает значения [0..63].
14	Установить значение кода IP Precedence, для которого должно срабатывать правило (не обязательно). Невозможно использовать совместно с DSCP.	evt(config-acl-rule)# match ip-precedence <IPP>	<IPP> – значение кода IP Precedence, принимает значения [0..7].

Шаг	Описание	Команда	Ключи
15	Установить значение идентификационного номера VLAN, для которого должно срабатывать правило (не обязательно).	evt(config-acl-rule)# match vlan <VID>	<VID> – идентификационный номер VLAN, принимает значения [1..4094].
16	Активировать правило.	evt(config-acl-rule)# enable	
17	Указать список контроля доступа к конфигурируемому интерфейсу для фильтрации входящего трафика.	evt(config-if-gi)# service-acl input <NAME>	<NAME> – имя списка контроля доступа, задаётся строкой до 31 символа.
18	Указать список контроля доступа к конфигурируемому интерфейсу для фильтрации исходящего трафика.	evt(config-if-gi)# service-acl output <NAME>	<NAME> – имя списка контроля доступа, задаётся строкой до 31 символа.

Также списки доступа могут использоваться для организации политик QoS.

Пример настройки списка доступа

Задача:

Разрешить прохождения трафика только из подсети 192.168.20.0/24.

Решение:

Настроим список доступа для фильтрации по подсетям:

```

evt# configure
evt(config)# ip access-list extended white
evt(config-acl)# rule 1
evt(config-acl-rule)# action permit
evt(config-acl-rule)# match source-address 192.168.20.0 255.255.255.0
evt(config-acl-rule)# enable
evt(config-acl-rule)# exit
evt(config-acl)# exit

```

Применим список доступа на интерфейс Gi1/0/1 для входящего трафика:

```

evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# service-acl input white

```

Просмотреть детальную информацию о списке доступа возможно через команду:

```

evt# show ip access-list white

```

6.2.6 Управление маршрутизацией

- Политика фильтрации маршрутной информации
 - Протокол RIP
 - Протокол OSPF
 - Протокол iBGP
 - Протокол eBGP
- Конфигурирование статических маршрутов
 - Алгоритм настройки
 - Пример настройки
- Конфигурирование статических multipath-маршрутов
 - Алгоритм настройки
 - Пример настройки
- Настройка RIP
 - Алгоритм настройки
 - Пример настройки
- Настройка RIPv2
 - Алгоритм настройки
 - Пример настройки
- Настройка OSPF
 - Алгоритм настройки
 - Пример настройки
 - Пример настройки OSPF stub area
 - Пример настройки Virtual link
- Настройка BGP
 - Алгоритм настройки
 - Пример настройки
 - Политика выбора лучшего маршрута в протоколе BGP
 - Условное анонсирование маршрутной информации (Conditional Advertisement)
 - Алгоритм настройки
 - Пример настройки
 - Быстрая деактивация пиринговых сессий
 - Метод на основе протокола BFD
 - Алгоритм настройки
 - Пример настройки
 - Метод на основе Fast Peer Deactivation (Fall-over)
 - Алгоритм настройки
 - Пример настройки
- Настройка BFD
 - Настройка таймеров
 - Алгоритм настройки
 - Пример настройки
- Настройка политики маршрутизации PBR
 - Алгоритм настройки Route-map для BGP
 - Пример настройки 1. Route-map для BGP
 - Пример настройки 2. Route-map для BGP
 - Пример настройки 3. Использование регулярных выражений в Route-map для BGP
 - Алгоритм настройки Route-map на основе списков доступа (Policy-based routing)
 - Пример настройки Route-map на основе списков доступа (Policy-based routing)
- Настройка VRF
 - Алгоритм настройки
 - Пример настройки
- Настройка MultiWAN
 - Алгоритм настройки

- [Пример настройки](#)

Политика фильтрации маршрутной информации

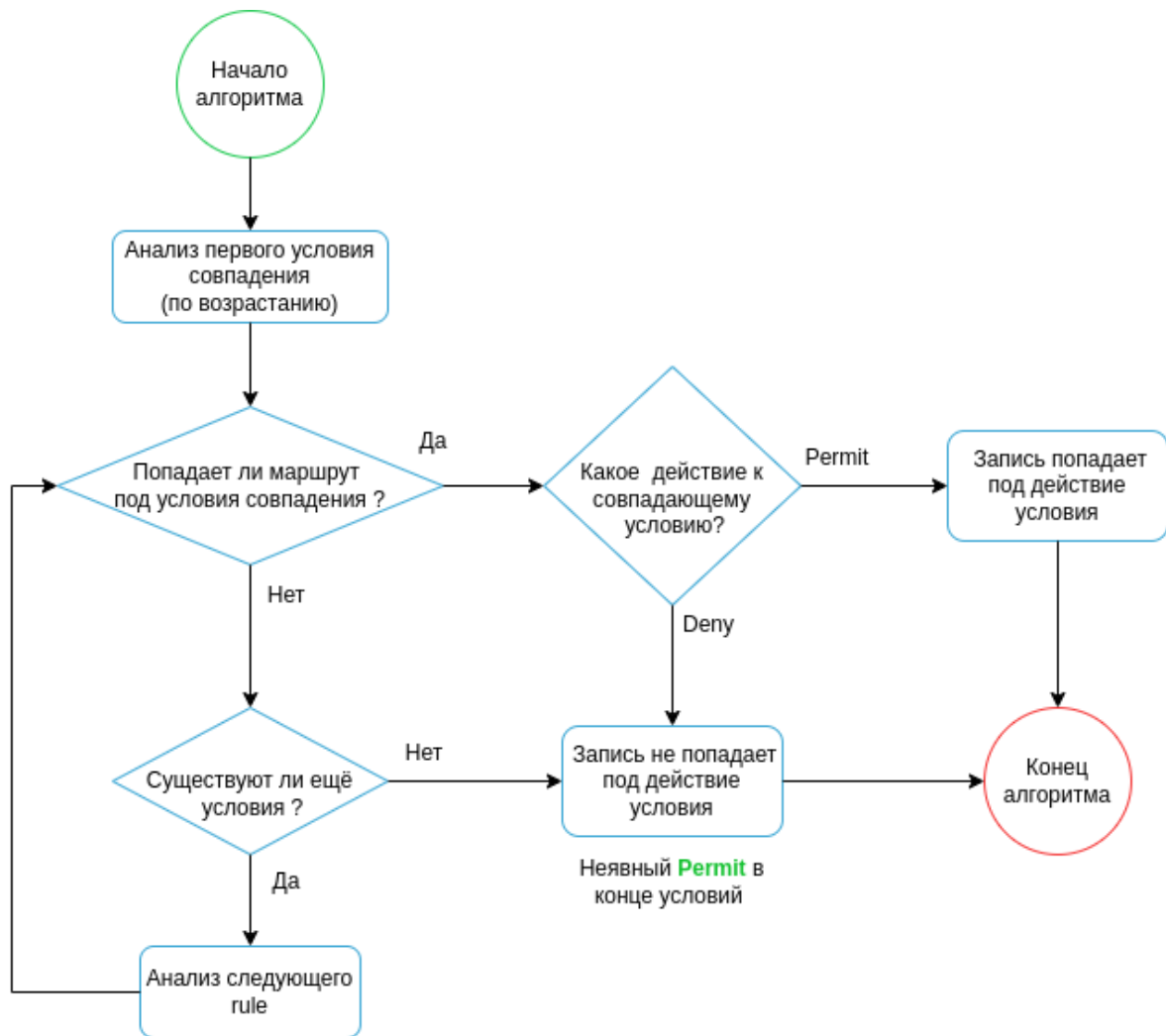
Фильтрация маршрутной информации в динамических протоколах маршрутизации осуществляется с помощью prefix-list и route-map. Структурно они состоят из последовательных условий, совпадений (match) и действий, применяемых для заданных условий – permit/deny. В зависимости от политики обработки маршрутов (импорт или экспорт) конечное неявное условие (правило) может быть разным для некоторых протоколов маршрутизации.

Правила фильтрации маршрутов в prefix-list и route-map выглядят следующим образом:

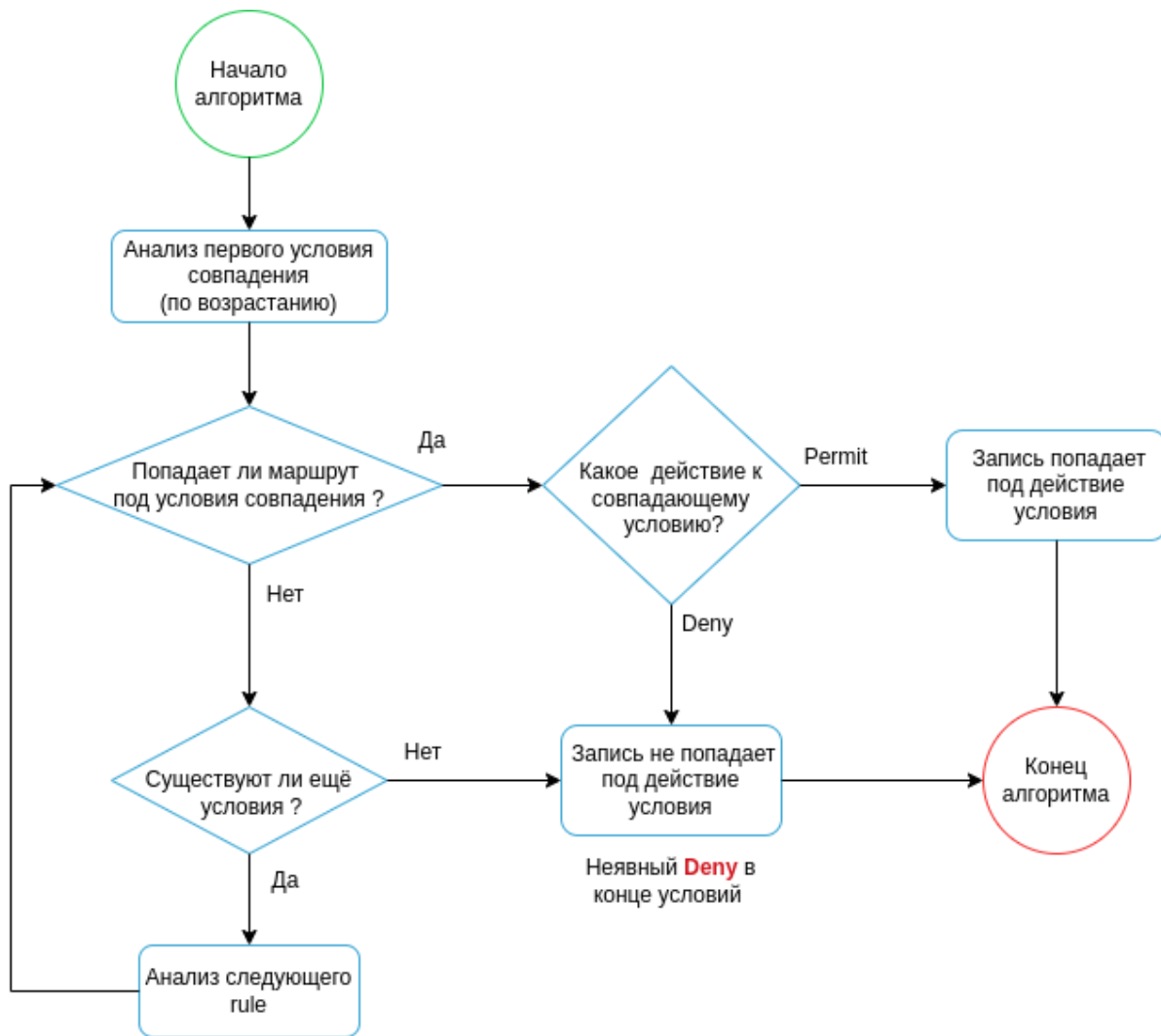
- В route-map: маршруты сопоставляются с IP-префиксами по очереди в списке правил в соответствии с их нумерацией – от самого младшего до самого старшего.
- В prefix-list: маршруты сопоставляются с IP-префиксами по очереди в списке IP-префиксов, указанных в prefix-list в том порядке, котором они были заданы при создании/редактировании этого prefix-list.
- Если маршрут соответствует префиксу, указанному в последовательности или правиле, к нему применяются описанные действия, и он перестает сопоставляться с другими префиксами в списке IP-префиксов.
- Если маршруты не соответствуют ни одному префиксу в списке IP-префиксов, к ним применяется неявное правило в конце prefix-list или route-map.

Ниже приведены блок-схемы с автоматом состояний обработки правил фильтрации маршрутной информации для политик import и export.

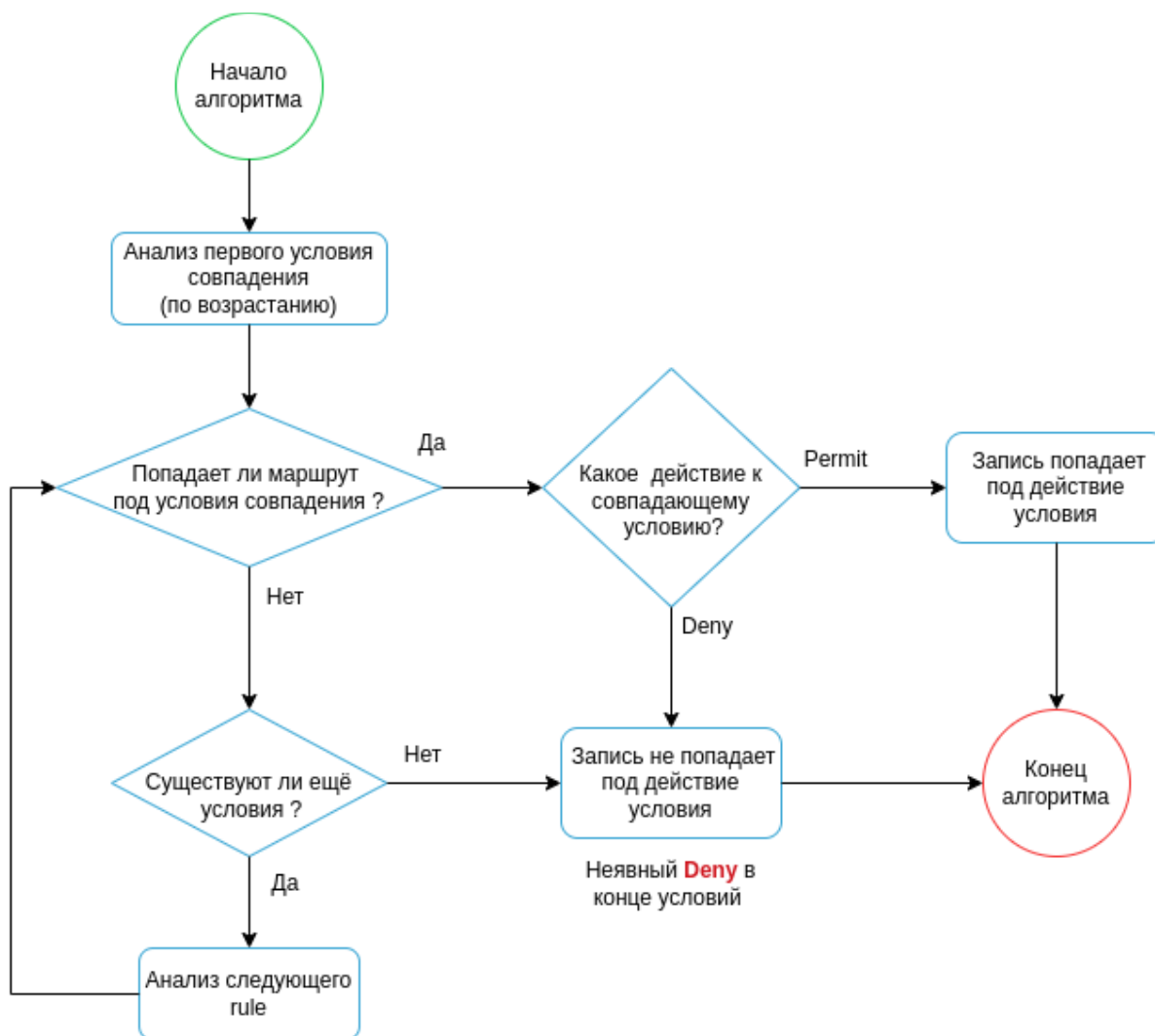
Обработка правил фильтрации маршрутной информации политики export для протоколов RIP, OSPF, iBGP:



Обработка правил фильтрации маршрутной информации политики import для протоколов RIP, OSPF, IS-IS, iBGP:



Обработка правил фильтрации маршрутной информации политик import/export для протокола eBGP:



Ниже приведены обобщенные таблицы по протоколам:

Протокол RIP

in/ out	Политика по умолчанию	Способы анонсирования	Способы фильтрации	Уровни применения политик фильтрации
Import	Получение маршрутной информации не ограничено.	Network, Redistribute	Route-map — последнее (неявное) правило <u>запрещает</u> все, что явно не разрешено предыдущими правилами. Prefix-list — последнее (неявное) правило <u>запрещает</u> все, что явно не разрешено предыдущими правилами.	Процесс RIP

in/ out	Политика по умолчанию	Способы анонсирования	Способы фильтрации	Уровни применения политик фильтрации
Export	Без отдельных команд анонсирования маршрутизатор не отправляет маршрутную информацию.		Prefix-list — последнее (неявное) правило <u>разрешает</u> все, что явно не запрещено предыдущими правилами. Prefix-list — последнее (неявное) правило <u>разрешает</u> все, что явно не запрещено предыдущими правилами.	

Протокол OSPF

in/ out	Политика по умолчанию	Способы анонсирования	Способы фильтрации	Уровни применения политик фильтрации
Import	Получение маршрутной информации не ограничено.	Redistribute	Route-map — последнее (неявное) правило <u>разрешает</u> все, что явно не разрешено предыдущими правилами.	Процесс OSPF
		Route-map, Prefix-list	Route-map — последнее (неявное) правило <u>запрещает</u> все, что явно не разрешено предыдущими правилами. Prefix-list — последнее (неявное) правило <u>запрещает</u> все, что явно не разрешено предыдущими правилами.	
Export	Анонсируется информация о интерфейсах, на которых включен протокол OSPF.	Route-map, Prefix-list	Route-map — последнее (неявное) правило <u>разрешает</u> все, что явно не запрещено предыдущими правилами. Prefix-list — последнее (неявное) правило <u>разрешает</u> все, что явно не запрещено предыдущими правилами. <i>Фильтрация анонсируемой маршрутной информации возможна для следующих типов OSPF-маршрутов: E2, E1.</i>	

Протокол iBGP

in/ out	Политика по умолчанию	Способы Анонсирования	Способы фильтрации	Уровни применения политик фильтрации
Import	Получение маршрутной информации не ограничено.	Network, Redistribute	Route-map — последнее (неявное) правило <u>запрещает</u> все, что явно не разрешено предыдущими правилами. Prefix-list — последнее (неявное) правило <u>запрещает</u> все, что явно не разрешено предыдущими правилами.	address-family, peer-group, neighbor
Export	Анонсируются все маршруты, попавшие в RIB по протоколу BGP.		Route-map — последнее (неявное) правило <u>разрешает</u> все, что явно не разрешено предыдущими правилами. Prefix-list — последнее (неявное) правило <u>разрешает</u> все, что явно не разрешено предыдущими правилами.	

Протокол eBGP

in/ out	Политика по умолчанию	Способы Анонсирования	Способы фильтрации	Уровни применения политик фильтрации
Import	Получение маршрутной информации не ограничено	Network, Redistribute	Route-map — последнее (неявное) правило <u>запрещает</u> все, что явно не разрешено предыдущими правилами. Prefix-list — последнее (неявное) правило <u>запрещает</u> все, что явно не разрешено предыдущими правилами.	address-family, peer-group, neighbor
Export	Анонсирование маршрутов <u>запрещено</u> до применения разрешающего route-map или prefix-list		Route-map — последнее (неявное) правило <u>запрещает</u> все, что явно не разрешено предыдущими правилами. Prefix-list — последнее (неявное) правило <u>запрещает</u> все, что явно не разрешено предыдущими правилами.	

Конфигурирование статических маршрутов

Статическая маршрутизация — вид маршрутизации, при котором маршруты указываются в явном виде при конфигурации маршрутизатора без использования протоколов динамической маршрутизации.

⚠ Конфигурация на маршрутизаторах EVT и EVS производится с помощью одинаковых команд. Ниже приведены примеры настройки EVT.

Алгоритм настройки

Добавить статический маршрут возможно командой в режиме глобальной конфигурации:

```
evt(config)# ip route [ vrf <VRF> ] <SUBNET> { { <NEXTHOP> [ resolve ] [ bfd ] [ unit <ID> ] |
interface <IF> | tunnel <TUN> | blackhole | unreachable | prohibit } [ track <TRACK-ID> ]
[ name <NAME> ] } | wan load-balance rule <RULE> } [ <METRIC> ]
no ip route [ vrf <VRF> ] <SUBNET> [ <METRIC> ] [ unit <ID> ]
```

- <VRF> – имя экземпляра VRF, задается строкой до 31 символа;
- <SUBNET> – адрес назначения, может быть задан в следующих видах:
 - AAA.BBB.CCC.DDD – IP-адрес хоста, где каждая часть принимает значения [0..255];
 - AAA.BBB.CCC.DDD/NN – IP-адрес подсети с маской в виде префикса, где AAA-DDD принимают значения [0..255] и NN принимает значения [1..32].
- <NEXTHOP> – IP-адрес шлюза, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];
- resolve – при указании данного параметра IP-адрес шлюза будет рекурсивно вычислен через таблицу маршрутизации. Если при рекурсивном вычислении не удастся найти шлюз из напрямую подключенной подсети, то данный маршрут не будет установлен в систему;
- <ID> – номер юнита, принимает значения [1..2];
- <IF> – имя IP-интерфейса, задается в виде, описанном в разделе [Типы и порядок именования интерфейсов маршрутизатора](#);
- <TUN> – имя туннеля, задается в виде, описанном в разделе [Типы и порядок именования туннелей маршрутизатора](#);
- <RULE> – номер правила wan, задается в диапазоне [1..50];
- blackhole – при указании команды пакеты до данной подсети будут удаляться устройством без отправки уведомлений отправителю;
- unreachable – при указании команды пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Host unreachable, code 1);
- prohibit – при указании команды пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Communication administratively prohibited, code 13);
- <METRIC> – метрика маршрута, принимает значения [0..255];
- <TRACK-ID> – идентификатор Tracking-объекта. Если маршрут привязан к Tracking-объекту, то он появится в системе только при выполнении всех условий, заданных в объекте;
- <NAME> – имя (описание) маршрута, текстовая переменная длиной до 31 символа;
- bfd – при указании данного ключа активируется удаление статического маршрута в случае недоступности next-hop. Для работы данного механизма должен быть запущен механизм BFD с IP-адресом next-hop (см. раздел [ip bfd neighbor](#)).
Проверка next-hop при помощи протокола BFD. В случае недоступности next-hop маршрут удаляется.

Для добавления статического IPv6-маршрута к указанной подсети используется команда:

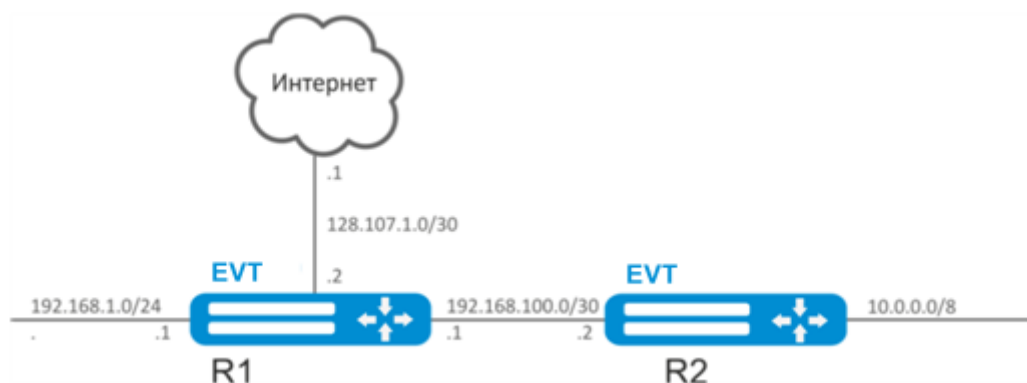
```
evt(config)# ipv6 route [ vrf <VRF> ] <SUBNET> { { <NEXTHOP> [ resolve ] [bfd] [ unit <ID> ] |
interface <IF> | blackhole | unreachable | prohibit [ <METRIC> ] [ name <NAME>] } | wan load-
balance rule <RULE> [ <METRIC> ] }
no ipv6 route [ vrf <VRF> ] <SUBNET> [ <METRIC> ] [ unit <ID> ]
```

- <VRF> – имя экземпляра VRF, задается строкой до 31 символа;
- <SUBNET> – адрес назначения, может быть задан в следующих видах:
 - X:X:X:X – IPv6-адрес хоста, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];
 - X:X:X:X::X/EE – IPv6-адрес подсети с маской в виде префикса, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128].
- <NEXTHOP> – IPv6-адрес шлюза, задается в виде X:X:X:X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];
- resolve – при указании данного параметра IPv6-адрес шлюза будет рекурсивно вычислен через таблицу маршрутизации. Если при рекурсивном вычислении не удастся найти шлюз из напрямую подключенной подсети, то данный маршрут не будет установлен в систему;
- <ID> – номер юнита, принимает значения [1..2];
- <IF> – имя IP-интерфейса, задается в виде, описанном в разделе [Типы и порядок именования интерфейсов маршрутизатора](#);
- blackhole – при указании команды пакеты до данной подсети будут удаляться устройством без отправки уведомлений отправителю;
- unreachable – при указании команды пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Host unreachable, code 1);
- prohibit – при указании команды пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Communication administratively prohibited, code 13);
- [METRIC] – метрика маршрута, принимает значения [0..255];
- <NAME> – имя (описание) маршрута, текстовая переменная длиной до 31 символа;
- bfd – при указании данного ключа активируется проверка next-hop при помощи протокола BFD. В случае недоступности next-hop маршрут удаляется.

Пример настройки

Задача:

Настроить доступ к сети Internet для пользователей локальных сетей 192.168.1.0/24 и 10.0.0.0/8, используя статическую маршрутизацию. На устройстве R1 создать шлюз для доступа к сети Internet. Трафик внутри локальной сети должен маршрутизироваться внутри зоны LAN, трафик из сети Internet должен относиться к зоне WAN.



Решение:

Зададим имя устройства для маршрутизатора R1:

```
evt# hostname R1
```

Для интерфейса gi1/0/1 укажем адрес 192.168.1.1/24 и зону «LAN». Через данный интерфейс R1 будет подключен к сети 192.168.1.0/24:

```
evt(config)# interface gi1/0/1
evt(config-if-gi)# security-zone LAN
evt(config-if-gi)# ip address 192.168.1.1/24
evt(config-if-gi)# exit
```

Для интерфейса gi1/0/2 укажем адрес 192.168.100.1/30 и зону «LAN». Через данный интерфейс R1 будет подключен к устройству R2 для последующей маршрутизации трафика:

```
evt(config)# interface gi1/0/2
evt(config-if-gi)# security-zone LAN
evt(config-if-gi)# ip address 192.168.100.1/30
evt(config-if-gi)# exit
```

Для интерфейса gi1/0/3 укажем адрес 128.107.1.2/30 и зону «WAN». Через данный интерфейс R1 будет подключен к сети Internet:

```
evt(config)# interface gi1/0/3
evt(config-if-gi)# security-zone WAN
evt(config-if-gi)# ip address 128.107.1.2/30
evt(config-if-gi)# exit
```

Создадим маршрут для взаимодействия с сетью 10.0.0.0/8, используя в качестве шлюза устройство R2 (192.168.100.2):

```
evt(config)# ip route 10.0.0.0/8 192.168.100.2
```

Создадим маршрут для взаимодействия с сетью Internet, используя в качестве nexthop шлюз провайдера (128.107.1.1):

```
evt(config)# ip route 0.0.0.0/0 128.107.1.1
```

Зададим имя устройства для маршрутизатора R2:

```
evt# hostname R2
```

Для интерфейса gi1/0/1 укажем адрес 10.0.0.1/8 и зону «LAN». Через данный интерфейс R2 будет подключен к сети 10.0.0.0/8:

```
evt(config)# interface gi1/0/1
evt(config-if-gi)# security-zone LAN
evt(config-if-gi)# ip address 10.0.0.1/8
evt(config-if-gi)# exit
```

Для интерфейса gi1/0/2 укажем адрес 192.168.100.2/30 и зону «LAN». Через данный интерфейс R2 будет подключен к устройству R1 для последующей маршрутизации трафика:

```
evt(config)# interface gi1/0/2
evt(config-if-gi)# security-zone LAN
evt(config-if-gi)# ip address 192.168.100.2/30
evt(config-if-gi)# exit
```

Создадим маршрут по умолчанию, указав в качестве nexthop IP-адрес интерфейса gi1/0/2 маршрутизатора R1 (192.168.100.1):

```
evt(config)# ip route 0.0.0.0/0 192.168.100.1
```

Проверить таблицу маршрутов можно командой:

```
evt# show ip route
```

Конфигурирование статических multipath-маршрутов

Статические multipath-маршруты позволяют использовать стратегию ECMP для эффективного распределения трафика между несколькими равнозначными маршрутами, без необходимости применения динамических протоколов маршрутизации.

Алгоритм настройки

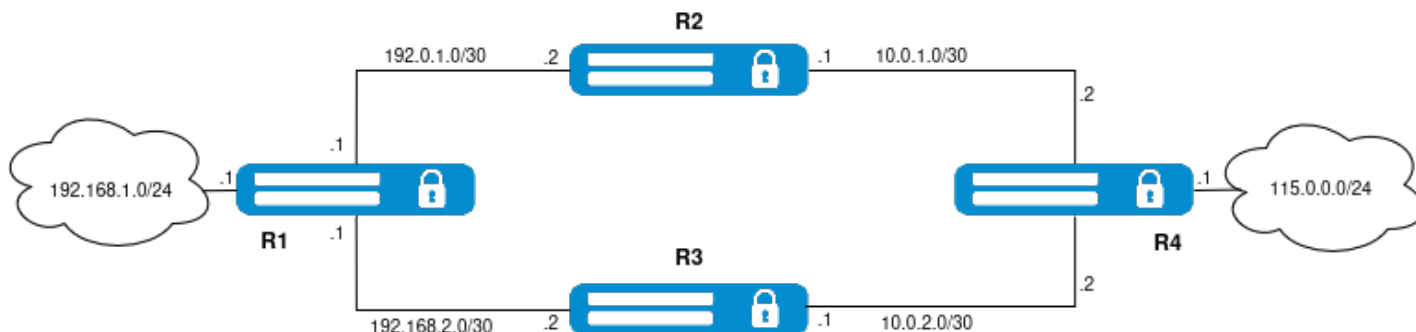
Шаг	Описание	Команда	Ключи
1	Создать статический multipath ipv4 маршрут.	evt(config)# ip route multipath [vrf <VRF>] <SUBNET> [track <TRACK-ID>] [name <NAME>] [<METRIC>]	<VRF> – имя экземпляра VRF, задается строкой до 31 символа; <SUBNET> – адрес назначения, может быть задан в следующих видах: • AAA.BBB.CCC.DDD – IP-адрес хоста, где каждая часть принимает значения [0..255]; • AAA.BBB.CCC.DDD/NN – IP-адрес подсети с маской в виде префикса, где AAA-DDD принимают значения [0..255] и NN принимает значения [1..32]. <TRACK-ID> – идентификатор Tracking-объекта. Если маршрут привязан к Tracking-объекту, то он появится в системе только при выполнении всех условий, заданных в объекте; <NAME> – имя (описание) маршрута, текстовая переменная длиной до 31 символа; <METRIC> – метрика маршрута, принимает значения [0..255].
2	Создать статический multipath ipv6 маршрут.	evt(config)# ipv6 route multipath [vrf <VRF>] <SUBNET> [name <NAME>] [<METRIC>]	<VRF> – имя экземпляра VRF, задается строкой до 31 символа; <SUBNET> – адрес назначения, может быть задан в следующих видах: • X:X:X:X::X – IPv6-адрес хоста, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; • X:X:X:X::X/EE – IPv6-адрес подсети с маской в виде префикса, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128]. <NAME> – имя (описание) маршрута, текстовая переменная длиной до 31 символа; <METRIC> – метрика маршрута, принимает значения [0..255].

Шаг	Описание	Команда	Ключи
3	Настроить шлюзы для маршрута.	evt(config)# gateway { <NEXTHOP> [<WEIGHT>] [bfd] [track <TRACK-ID>] [unit <ID>] <IF> [<WEIGHT>] [track <TRACK-ID>] <TUN> [<WEIGHT>] [track <TRACK-ID>] }	<NEXTHOP> – адрес шлюза, может быть задан в следующих видах: • AAA.BBB.CCC.DDD – IP-адрес шлюза, где каждая часть принимает значения [0..255]; • X:X:X:X::X – IPv6-адрес шлюза, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <WEIGHT> - метрика шлюза, принимает значения [0..255]. <ID> – номер юнита, принимает значения [1..2]; <IF> – имя IP-интерфейса, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора; <TUN> – имя туннеля, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора; <TRACK-ID> – идентификатор Tracking-объекта. Если маршрут привязан к Tracking-объекту, то он появится в системе только при выполнении всех условий, заданных в объекте. Доступно только для ipv4; bfd – при указании данного ключа активируется проверка доступности шлюза при помощи протокола BFD. В случае недоступности шлюз удаляется из таблицы маршрутизации.

Пример настройки

Задача:

Обеспечить связность сетей 192.168.1.0/24 и 115.0.0.0/24, распределяя трафик между R2 и R3 с помощью статического multipath-маршрута.



Решение:

Конфигурация R1:

R1

```

evt# hostname R1
evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# description "to LAN"
evt(config-if-gi)# ip firewall disable
evt(config-if-gi)# ip address 192.168.1.1/24
evt(config-if-gi)# exit
evt(config)# interface gigabitethernet 1/0/3
evt(config-if-gi)# description "to R2"
evt(config-if-gi)# ip firewall disable
evt(config-if-gi)# ip address 192.0.1.1/30
evt(config-if-gi)# exit
evt(config)# interface gigabitethernet 1/0/4
evt(config-if-gi)# description "to R3"
evt(config-if-gi)# ip address 192.0.2.1/30
evt(config-if-gi)# exit
evt(config)# ip route multipath 115.0.0.0/24
evt(config-multipath-route)# gateway 192.0.1.2
evt(config-multipath-route)# gateway 192.0.2.2
evt(config-multipath-route)# exit

```

Конфигурация R2:

R2

```
evt(config)# hostname R2
evt(config)# interface gigabitethernet 1/0/3
evt(config-if-gi)# description "to R1"
evt(config-if-gi)# ip firewall disable
evt(config-if-gi)# ip address 192.0.1.2/30
evt(config-if-gi)# exit
evt(config)# interface gigabitethernet 1/0/4
evt(config-if-gi)# description "to R4"
evt(config-if-gi)# ip firewall disable
evt(config-if-gi)# ip address 10.0.1.1/30
evt(config-if-gi)# exit
evt(config)#
evt(config)# ip route 115.0.0.0/24 10.0.1.2
evt(config)# ip route 192.168.0.0/24 192.0.1.1
```

Конфигурация R3:

R3

```
evt(config)# hostname R3
evt(config)# interface gigabitethernet 1/0/3
evt(config-if-gi)# description "to R1"
evt(config-if-gi)# ip firewall disable
evt(config-if-gi)# ip address 192.0.2.2/30
evt(config-if-gi)# exit
evt(config)# interface gigabitethernet 1/0/4
evt(config-if-gi)# description "to R4"
evt(config-if-gi)# ip firewall disable
evt(config-if-gi)# ip address 10.0.2.1/30
evt(config-if-gi)# exit
evt(config)# ip route 115.0.0.0/24 10.0.2.2
evt(config)# ip route 192.168.0.0/24 192.0.2.1
```

Конфигурация R4:

R4

```

evt(config)# hostname R4
evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# description "to LAN"
evt(config-if-gi)# ip firewall disable
evt(config-if-gi)# ip address 115.0.0.1/24
evt(config-if-gi)# exit
evt(config)# interface gigabitethernet 1/0/3
evt-30(config-if-gi)# description "to R2"
evt-30(config-if-gi)# ip firewall disable
evt-30(config-if-gi)# ip address 10.0.1.2/30
evt-30(config-if-gi)# exit
evt-30(config)# interface gigabitethernet 1/0/4
evt-30(config-if-gi)# description "to R3"
evt-30(config-if-gi)# ip firewall disable
evt-30(config-if-gi)# ip address 10.0.2.2/30
evt-30(config-if-gi)# exit
evt-30(config)# ip route multipath 192.168.0.0/24
evt-30(config-multipath-route)# gateway 10.0.1.1
evt-30(config-multipath-route)# gateway 10.0.2.1
evt-30(config-multipath-route)# exit

```

Проверить таблицу маршрутов можно командой:

```
evt# show ip route
```

Настройка RIP

RIP — дистанционно-векторный протокол динамической маршрутизации, который использует количество транзитных участков в качестве метрики маршрута. Максимальное количество транзитных участков (hop), разрешенное в RIP, равно 15. Каждый RIP-маршрутизатор по умолчанию вещает в сеть свою полную таблицу маршрутизации один раз в 30 секунд. RIP работает на 3 уровне стека TCP/IP, используя UDP-порт 520.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Настроить приоритетность протокола RIP-маршрутизации для основной таблицы маршрутизации (не обязательно).	evt(config)# ip protocols rip preference <VALUE>	<VALUE> – приоритетность протокола, принимает значения в диапазоне [1..255]. Значение по умолчанию: RIP (100).

Шаг	Описание	Команда	Ключи
2	Настроить емкость таблиц маршрутизации протокола RIP (не обязательно).	evt(config)# ip protocols rip max-routes <VALUE>	<VALUE> – количество маршрутов протокола RIP в маршрутной таблице, принимает значения в диапазоне [1..10000]; Значение по умолчанию: 10000.
3	Создать списки IP-подсетей, которые в дальнейшем будут использоваться для фильтрации анонсируемых и получаемых IP-маршрутов.	evt(config)# ip prefix-list <NAME>	<NAME> – имя конфигурируемого списка подсетей, задаётся строкой до 31 символа.
4	Разрешить (permit) или запретить (deny) списки префиксов.	evt(config-pl)# permit {object-group <OBJ-GROUP-NETWORK-NAME> <ADDR/LEN> <IPV6-ADDR/LEN> } [{ eq <LEN> le <LEN> ge <LEN> [le <LEN>] }] evt(config-pl)# deny {object-group <OBJ-GROUP-NETWORK-NAME> <ADDR/LEN> <IPV6-ADDR/LEN> } [{ eq <LEN> le <LEN> ge <LEN> [le <LEN>] }]	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа; <LEN> – длина префикса, принимает значения [1..32] в IP-списках префиксов; • eq – при указании команды длина префикса должна соответствовать указанной; • le – при указании команды длина префикса должна быть меньше либо соответствовать указанной; • ge – при указании команды длина префикса должна быть больше либо соответствовать указанной; • default - route – фильтрация маршрута по умолчанию.
5	Перейти в режим настройки параметров RIP-процесса.	evt(config)# router rip evt(config-rip)#	
6	Включить RIP-протокол.	evt(config-rip)# enable	
7	Определить алгоритм аутентификации протокола RIP (не обязательно).	evt(config-rip)# authentication algorithm { cleartext md5 }	• cleartext – пароль, передается открытым текстом; • md5 – пароль, хешируется по алгоритму md5.

Шаг	Описание	Команда	Ключи
8	Установить пароль для аутентификации с соседом (не обязательно).	evt(config-rip)# authentication key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> }	<CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).
9	Определить список паролей для аутентификации через алгоритм хеширования md5 (не обязательно).	evt(config-rip)# authentication key-chain <KEYCHAIN>	<KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов.
10	Выключить анонсирование маршрутов на интерфейсах/ туннелях/bridge, где это не нужно (не обязательно).	evt(config-rip)# passive-interface {<IF> <TUN> }	<IF> – интерфейс и идентификатор; <TUN> – имя и номер туннеля.
11	Установить временной интервал, по истечении которого производится анонсирование (не обязательно).	evt(config-rip)# timers update <TIME>	<TIME> – время в секундах, принимает значения [12..65535]. Значение по умолчанию: 180 секунд.
12	Установить временной интервал корректности маршрутной записи без обновления (не обязательно).	evt(config-rip)# timers invalid <TIME>	<TIME> – время в секундах, принимает значения [12..65535]. Значение по умолчанию: 180 секунд.
13	Установить временной интервал, по истечении которого производится удаление маршрута (не обязательно).	evt(config-rip)# timers flush <TIME>	<TIME> – время в секундах, принимает значения [12..65535]. При установке значения нужно учитывать следующее правило: «timersinvalid + 60» Значение по умолчанию: 240 секунд.

Шаг	Описание	Команда	Ключи
14	Включить анонсирование подсетей.	evt(config-rip)# network <ADDR/LEN>	<ADDR/LEN> – адрес подсети, указывается в следующем формате: AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32].
15	Добавить фильтрацию подсетей во входящих или исходящих обновлениях (не обязательно).	evt(config-rip)# prefix-list <PREFIX-LIST-NAME> { in out }	<PREFIX-LIST-NAME> – имя сконфигурированного списка подсетей, задаётся строкой до 31 символа. • in – фильтрация входящих маршрутов; • out – фильтрация анонсируемых маршрутов.
16	Включить анонсирование маршрутов, полученных альтернативным способом (не обязательно).	evt(config-rip)# redistribute static [route-map <NAME>]	<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых статических маршрутов, задаётся строкой до 31 символа.
		evt(config-rip)# redistribute connected [route-map <NAME>]	<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых напрямую подключенных подсетей, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
		<pre>evt(config-rip)# redistribute ospf <ID><ROUTE-TYPE> [route-map <NAME>]</pre>	<ID> – номер процесса, может принимать значение [1..65535]; <ROUTE-TYPE> – тип маршрута: • intra - area – анонсирование маршрутов OSPF-процесса в пределах зоны; • inter - area – анонсирование маршрутов OSPF-процесса между зонами; • external 1 – анонсирование внешних маршрутов OSPF-формата 1; • external 2 – анонсирование внешних маршрутов OSPF-формата 2; <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых OSPF-маршрутов, задаётся строкой до 31 символа.

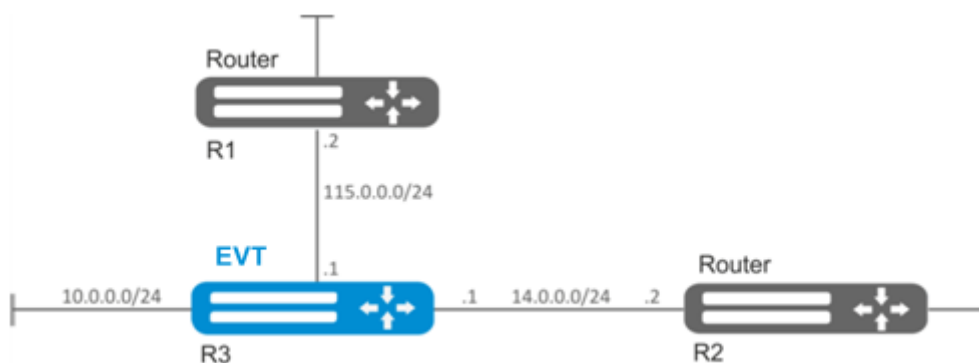
Шаг	Описание	Команда	Ключи
		evt(config-rip)# redistribute isis <ID><ROUTE-TYPE> [route-map <NAME>]	<ID> – номер процесса, может принимать значение [1..65535]; <ROUTE-TYPE> – тип маршрута: • level-1 – анонсирование маршрутов ISIS-процесса уровня 1; • level-2 – анонсирование маршрутов ISIS-процесса уровня 2; • inter-area – анонсирование межзоновых маршрутов ISIS-процесса. <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых ISIS-маршрутов, задаётся строкой до 31 символа.
		evt(config-rip)# redistribute bgp <AS> [route-map <NAME>]	<AS> – номер автономной системы, может принимать значения [1..4294967295]; <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых BGP-маршрутов, задаётся строкой до 31 символа.
17	Перейти в режим конфигурирования интерфейса/туннеля/сетевого моста.	evt(config)# interface <IF-TYPE><IF-NUM>	<IF-TYPE> – тип интерфейса; <IF-NUM> – F/S/P – F-фрейм (1), S – слот (0), P – порт.
		evt(config)# tunnel <TUN-TYPE><TUN-NUM>	<TUN-TYPE> – тип туннеля; <TUN-NUM> – номер туннеля.
		evt(config)# bridge <BR-NUM>	<BR-NUM> – номер bridge.
18	Установить величину метрики RIP-маршрутов на интерфейсе (не обязательно).	evt(config-if-gi)# ip rip metric <VALUE>	<VALUE> – величина метрики, задаётся в размере [0..32767]. Значение по умолчанию: 5.

Шаг	Описание	Команда	Ключи
19	Установить режим анонсирования маршрутов по протоколу RIP (не обязательно).	evt(config-if-gi)# ip rip mode <MODE>	<MODE> – режим анонсирования маршрутов: • multicast – маршруты анонсируются в многоадресном режиме; • broadcast – маршруты анонсируются в широковещательном режиме; • unicast – маршруты анонсируются в unicast-режиме соседям. Значение по умолчанию: multicast.
20	Задать IP-адрес соседа для установления отношения в unicast-режиме анонсирования маршрутов (не обязательно).	evt(config-if-gi)# ip rip neighbor <ADDR>	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
21	Включить суммаризацию подсетей (не обязательно).	evt(config-if-gi)# ip rip summary-address <ADDR/LEN>	<ADDR/LEN> – IP-адрес и маска подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].
22	Включить протокол BFD для протокола RIP (не обязательно).	evt(config-if-gi)# ip rip bfd-enable	

Пример настройки

Задача:

Настроить на маршрутизаторе протокол RIP для обмена маршрутной информацией с соседними маршрутизаторами. Маршрутизатор должен анонсировать статические маршруты и подсети 115.0.0.0/24, 14.0.0.0/24, 10.0.0.0/24. Анонсирование маршрутов должно происходить каждые 25 секунд.



Решение:

Предварительно нужно настроить IP-адреса на интерфейсах согласно схеме сети, приведенной на [рисунке](#).

Перейдём в режим конфигурирования протокола RIP:

```
evt(config)# router rip
```

Укажем подсети, которые будут анонсироваться протоколом: 115.0.0.0/24, 14.0.0.0/24 и 10.0.0.0/24:

```
evt(config-rip)# network 115.0.0.0/24  
evt(config-rip)# network 14.0.0.0/24  
evt(config-rip)# network 10.0.0.0/24
```

Для анонсирования протоколом статических маршрутов выполним команду:

```
evt(config-rip)# redistribute static
```

Настроим таймер, отвечающий за отправку маршрутной информации:

```
evt(config-rip)# timers update 25
```

После установки всех требуемых настроек включим протокол:

```
evt(config-rip)# enable
```

Для того чтобы просмотреть таблицу маршрутов RIP, воспользуемся командой:

```
evt# show ip rip
```

 Помимо настройки протокола RIP необходимо в firewall разрешить UDP-порт 520.

Настройка RIPng

RIPng – дистанционно-векторный протокол динамической маршрутизации, использующий алгоритм Беллмана-Форда для нахождения наилучшего маршрута. Данная версия протокола включает в себя поддержку работы с IPv6. RIPng работает на 3 уровне стека TCP/IP, используя UDP-порт 521.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Настроить приоритетность протокола RIPng для основной таблицы маршрутизации (не обязательно).	evt(config)# ipv6 protocols rip preference <VALUE>	<VALUE> – приоритетность протокола, принимает значения в диапазоне [1..255]. Значение по умолчанию: RIPng (100).
2	Настроить емкость таблиц маршрутизации протокола RIPng (не обязательно).	evt(config)# ipv6 protocols rip max-routes <VALUE>	<VALUE> – количество маршрутов протокола RIP в маршрутной таблице, принимает значения в диапазоне [1..10000]; Значение по умолчанию: 10000.
3	Создать списки IPv6-подсетей, которые в дальнейшем будут использоваться для фильтрации анонсируемых и получаемых IPv6-маршрутов.	evt(config)# ipv6 prefix-list <NAME>	<NAME> – имя конфигурируемого списка подсетей, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
4	Разрешить (permit) или запретить (deny) списки префиксов.	<pre> evt(config-pl)# permit {object-group <OBJ-GROUP-NETWORK-NAME> <IPV6-ADDR/LEN> } [{ eq <LEN> le <LEN> ge <LEN> [le <LEN>] }] evt(config-pl)# deny {object-group <OBJ-GROUP-NETWORK-NAME> <IPV6-ADDR/LEN> } [{ eq <LEN> le <LEN> ge <LEN> [le <LEN>] } </pre>	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа; <IPV6-ADDR/LEN> – IPv6-адрес и маска подсети, задаётся в виде X:X:X:X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128]; <LEN> – длина префикса, принимает значения [1..128] в IPv6-списках префиксов; • eq – при указании команды длина префикса должна соответствовать указанной; • le – при указании команды длина префикса должна быть меньше либо соответствовать указанной; • ge – при указании команды длина префикса должна быть больше либо соответствовать указанной.
5	Перейти в режим настройки параметров RIPng-процесса.	<pre> evt(config)# ipv6 router rip evt(config-ripng)# </pre>	
6	Включить протокол RIPng.	evt(config-ripng)# enable	
7	Отключить анонсирование маршрутов на интерфейсах/туннелях/bridge, где это не нужно (не обязательно).	evt(config-ripng)# passive-interface <IF> <TUN> <BR-NUM> }	<IF> – интерфейс и идентификатор; <BR-NUM> – номер bridge; <TUN> – имя и номер туннеля.
8	Установить временной интервал, по истечении которого производится анонсирование (не обязательно).	evt(config-ripng)# timers update <TIME>	<TIME> – время в секундах, принимает значения [12..65535]. Значение по умолчанию: 180 секунд.

Шаг	Описание	Команда	Ключи
9	Установить временной интервал корректности маршрутной записи без обновления (не обязательно).	evt(config-ripng)# timers invalid <TIME>	<TIME> – время в секундах, принимает значения [12..65535]. Значение по умолчанию: 180 секунд.
10	Установить временной интервал, по истечении которого производится удаление маршрута (не обязательно).	evt(config-ripng)# timers flush <TIME>	<TIME> – время в секундах, принимает значения [12..65535]. При установке значения нужно учитывать следующее правило: «timersinvalid + 60» Значение по умолчанию: 240 секунд.
11	Включить анонсирование подсетей.	evt(config-ripng)# network <IPv6-ADDR/LEN>	<IPv6-ADDR/LEN> – IPv6-адрес и маска подсети, задаётся в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128].
12	Добавить фильтрацию подсетей во входящих или исходящих обновлениях (не обязательно).	evt(config-ripng)# prefix-list <PREFIX-LIST-NAME> { in out }	<PREFIX-LIST-NAME> – имя сконфигурированного списка подсетей, задаётся строкой до 31 символа. • in – фильтрация входящих маршрутов; • out – фильтрация анонсируемых маршрутов.
13	Включить анонсирование маршрутов, полученных альтернативным способом (не обязательно).	evt(config-ripng)# redistribute static [route-map <NAME>]	<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых статических маршрутов, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
		evt(config-ripng)# redistribute connected [route-map <NAME>]	<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых напрямую подключенных подсетей, задаётся строкой до 31 символа.
		evt(config-ripng)# redistribute ospf <ID><ROUTE-TYPE> [route-map <NAME>]	<ID> – номер процесса, может принимать значение [1..65535]; <ROUTE-TYPE> – тип маршрута: • intra - area – анонсирование маршрутов OSPF-процесса в пределах зоны; • inter - area – анонсирование маршрутов OSPF-процесса между зонами; • external 1 – анонсирование внешних маршрутов OSPF-формата 1; • external 2 – анонсирование внешних маршрутов OSPF-формата 2. <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых OSPF-маршрутов, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
		evt(config-ripng)# redistribute isis <ID><ROUTE-TYPE> [route-map <NAME>]	<ID> – номер процесса, может принимать значение [1..65535]; <ROUTE-TYPE> – тип маршрута: • level-1 – анонсирование маршрутов ISIS-процесса уровня 1; • level-2 – анонсирование маршрутов ISIS-процесса уровня 2; • inter-area – анонсирование межзоновых маршрутов ISIS-процесса. <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых ISIS-маршрутов, задаётся строкой до 31 символа.
		evt(config-ripng)# redistribute bgp <AS> [route-map <NAME>]	<AS> – номер автономной системы, может принимать значения [1..4294967295]; <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых BGP-маршрутов, задаётся строкой до 31 символа.
14	Перейти в режим конфигурирования интерфейса/туннеля/сетевого моста.	evt(config)# interface <IF-TYPE><IF-NUM>	<IF-TYPE> – тип интерфейса; <IF-NUM> – F/S/P – F-фрейм (1), S – слот (0), P – порт.
		evt(config)# tunnel <TUN-TYPE><TUN-NUM>	<TUN-TYPE> – тип туннеля; <TUN-NUM> – номер туннеля.
		evt(config)# bridge <BR-NUM>	<BR-NUM> – номер bridge.
15	Установить величину метрики RIPng-маршрутов на интерфейсе (не обязательно).	evt(config-if-gi)# ipv6 rip metric <VALUE>	<VALUE> – величина метрики, задаётся в размере [0..32767]. Значение по умолчанию: 5.

Шаг	Описание	Команда	Ключи
16	Включить суммаризацию подсетей (не обязательно).	evt(config-if-gi)# ipv6 rip summary-address <IPv6-ADDR/LEN>	<IPv6-ADDR/LEN> – IPv6-адрес и маска подсети, задаётся в виде X:X:X:X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128].
17	Включить протокол BFD для протокола RIP (не обязательно).	evt(config-if-gi)# ipv6 rip bfd-enable	

Пример настройки

Задача:

Настроить на маршрутизаторах протокол RIPng для обмена маршрутной информацией. Маршрутизаторы должны анонсировать адреса, присвоенные Loopback-интерфейсам.



Решение:

Предварительно нужно настроить IPv6-адреса на интерфейсах согласно схеме сети, приведенной выше.

На первом маршрутизаторе перейдем в режим конфигурирования протокола RIPng и укажем сети, которые будут анонсироваться протоколом:

```
evt1(config)# ipv6 router rip
evt1(config-ripng)# network c00:0:1409:3900::1/128
```

На втором маршрутизаторе произведем аналогичные действия:

```
evt2(config)# ipv6 router rip
evt2(config-ripng)# network c00:0:1409:3900::2/128
```

Активируем протокол RIPng на обоих маршрутизаторах:

```
evt1(config-ripng)# enable
evt2(config-ripng)# enable
```

Проверяем распространение маршрутной информации:

```

evt1# sh ipv6 route rip
R      * fc00:0:1409:3900::2/128 [100/2]          via fe80::aaf9:4bff:fead:fed2 on gi1/0/1 [rip
06:01:33]

evt2# sh ipv6 route rip
R      * fc00:0:1409:3900::2/128 [100/2]          via fe80::aaf9:4bff:fead:fed1 on gi1/0/1 [rip
06:01:33]

```

На этом базовая настройка протокола RIPvng закончена.

Настройка OSPF

OSPF — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути алгоритм Дейкстры.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Настроить приоритетность протокола OSPF-маршрутизации для основной таблицы маршрутизации (не обязательно).	evt(config)# ip protocols ospf preference <VALUE>	<VALUE> – приоритетность протокола, принимает значения в диапазоне [1..255]. Значение по умолчанию: 150.
		evt(config-vrf)# ip protocols ospf preference <VALUE>	
2	Настроить емкость таблиц маршрутизации протокола OSPF (не обязательно).	evt(config)# ip protocols ospf max-routes <VALUE>	<VALUE> – количество маршрутов протокола OSPF в маршрутной таблице, принимает значения в диапазоне [1..300000] Значение по умолчанию для глобального режима (300000) Значение по умолчанию для VRF: 0.
		evt(config)# ipv6 protocols ospf max-routes <VALUE>	
3	Включить вывод информации о состоянии отношений с соседями для протокола маршрутизации OSPF (не обязательно).	evt(config)# router ospf log-adjacency-changes	
		evt(config)# ipv6 router ospf log-adjacency-changes	
4	Создать списки IP-подсетей, которые в дальнейшем будут использоваться для фильтрации анонсируемых и получаемых IP-маршрутов (не обязательно).	evt(config)# ip prefix-list <NAME>	<NAME> – имя конфигурируемого списка подсетей, задаётся строкой до 31 символа.
		evt(config)# ipv6 prefix-list <NAME>	

Шаг	Описание	Команда	Ключи
5	Разрешить (permit) или запретить (deny) списки префиксов (не обязательно).	evt(config-pl)# permit [{ object-group <OBJ-GROUP-NETWORK-NAME> <ADDR/LEN> <IPV6-ADDR/LEN> }] [{ eq <LEN> le <LEN> ge <LEN> [le <LEN>] }]	<OBJ-GROUP-NETWORK-NAME> – имя профиля IPv4/IPv6-адресов, задаётся строкой до 31 символа; <ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <LEN> – длина префикса, принимает значения [1..32] в IP-списках префиксов; • eq – при указании команды длина префикса должна соответствовать указанной; • le – при указании команды длина префикса должна быть меньше либо соответствовать указанной; • ge – при указании команды длина префикса должна быть больше либо соответствовать указанной.
		evt(config-pl)# deny [{ object-group <OBJ-GROUP-NETWORK-NAME> <ADDR/LEN> <IPV6-ADDR/LEN> }] [{ eq <LEN> le <LEN> ge <LEN> [le <LEN>] }]	
6	Добавить OSPF-процесс в систему и осуществить переход в режим настройки параметров OSPF-процесса.	evt(config)# router ospf <ID> [vrf <VRF>]	<ID> – номер автономной системы процесса, принимает значения [1..65535] <VRF> – имя экземпляра VRF, задаётся строкой до 31 символа, в рамках которого будет работать протокол маршрутизации.
		evt(config)# ipv6 router ospf <ID> [vrf <VRF>]	

Шаг	Описание	Команда	Ключи
7	Установить идентификатор маршрутизатора для данного OSPF-процесса.	evt(config-ospf)# router-id { <ID> <IF> <TUN> }	<ID> – идентификатор маршрутизатора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. <IF> – интерфейс, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора. <TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора.
		evt(config-ipv6-ospf)# router-id { <ID> <IF> <TUN> }	
8	Определить приоритетность маршрутов процесса OSPF (не обязательно).	evt(config-ospf)# preference <VALUE>	<VALUE> – приоритетность маршрутов процесса OSPF, принимает значения в диапазоне [1..255].
		evt(config-ipv6-ospf)# preference <VALUE>	
9	Определить референсное значение для автоматического расчёта стоимости (cost) интерфейсов (не обязательно).	evt(config-ospf)# auto-cost reference bandwidth <VALUE>	<VALUE> – референсное значение для расчета стоимости интерфейса в диапазоне [1..100000000K]. Значение по умолчанию: 100000K.
		evt(config-ipv6-ospf)# auto-cost reference bandwidth <VALUE>	
10	Определить максимальное количество равнозначных маршрутов до цели (не обязательно).	evt(config-ospf)# maximum-path <PATHS>	<PATHS> – количество равноценных маршрутов до цели, принимает значения в диапазоне [1..32]. Значение по умолчанию: 16.
		evt(config-ipv6-ospf)# maximum-path <PATHS>	
11	Включить совместимость с RFC 1583 (не обязательно).	evt(config-ospf)# compatible rfc1583	
		evt(config-ipv6-ospf)# compatible rfc1583	

Шаг	Описание	Команда	Ключи
12	Добавить фильтрацию подсетей во входящих или исходящих обновлениях (не обязательно).	evt(config-ospf)# prefix-list <PREFIX-LIST-NAME> { in out }	<PREFIX-LIST-NAME> – имя сконфигурированного списка подсетей, задаётся строкой до 31 символа. • in – фильтрация входящих маршрутов; • out – фильтрация анонсируемых маршрутов.
		evt(config-ipv6-ospf)# prefix-list <PREFIX-LIST-NAME> { in out }	
13	Включить анонсирование маршрутов, полученных альтернативным способом (не обязательно).	evt(config-ospf)# redistribute static [metric <TYPE> <METRIC>] [route-map <NAME>]	<TYPE> – тип атрибута OSPF Metric, принимает значение type-1 и type-2; <METRIC> – значение атрибута OSPF Metric, принимает значения [0..65535]. <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых статических маршрутов, задаётся строкой до 31 символа.
		evt(config-ipv6-ospf)# redistribute static [metric <TYPE> <METRIC>] [route-map <NAME>]	
		evt(config-ospf)# redistribute connected [metric <TYPE> <METRIC>] [route-map <NAME>]	<TYPE> – тип атрибута OSPF Metric, принимает значение type-1 и type-2; <METRIC> – значение атрибута OSPF Metric, принимает значения [0..65535]. <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых напрямую подключенных подсетей, задаётся строкой до 31 символа.
		evt(config-ipv6-ospf)# redistribute connected [metric <TYPE> <METRIC>] [route-map <NAME>]	

Шаг	Описание	Команда	Ключи
		evt(config-ospf)# redistribute rip [metric <TYPE> <METRIC>] [route-map <NAME>]	<TYPE> – тип атрибута OSPF Metric, принимает значение type-1 и type-2; <METRIC> – значение атрибута OSPF Metric, принимает значения [0..65535]. <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых RIP-маршрутов, задаётся строкой до 31 символа.
		evt(config-ospf)# redistribute isis <ID> <ROUTE-TYPE> [metric <TYPE> <METRIC>] [route-map <NAME>]	<TYPE> – тип атрибута OSPF Metric, принимает значение type-1 и type-2; <METRIC> – значение атрибута OSPF Metric, принимает значения [0..65535].
		evt(config-ipv6-ospf)# redistribute isis <ID> <ROUTE-TYPE> [route-map <NAME>]	<ID> – номер процесса, может принимать значение [1..65535]. <ROUTE-TYPE> – тип маршрута: • level-1 – анонсирование маршрутов ISIS-процесса уровня 1; • level-2 – анонсирование маршрутов ISIS-процесса уровня 2; • inter-area – анонсирование межзоновых маршрутов ISIS-процесса. <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых BGP-маршрутов, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
		evt(config-ospf)# redistribute bgp <AS> [metric <TYPE> <METRIC>] [route-map <NAME>]	<TYPE> – тип атрибута OSPF Metric, принимает значение type-1 и type-2;
14	Активировать OSPF-процесс.	evt(config-ipv6-ospf)# redistribute bgp <AS> [metric <TYPE> <METRIC>] [route-map <NAME>]	<METRIC> – значение атрибута OSPF Metric, принимает значения [0..65535]. <AS> – номер автономной системы, может принимать значения [1..4294967295]; <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых BGP-маршрутов, задаётся строкой до 31 символа.
		evt(config-ipv6-ospf)# enable	
15	Создать OSPF-область и перейти в режим конфигурирования области.	evt(config-ospf)# area <AREA_ID>	<AREA_ID> – идентификатор области, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
		evt(config-ipv6-ospf)# area <AREA_ID>	
16	Включить анонсирование подсетей (не обязательно).	evt(config-ospf-area)# network <ADDR/LEN>	<ADDR/LEN> – адрес подсети, указывается в следующем формате: AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32].
		evt(config-ipv6-ospf-area)# network <IPV6-ADDR/LEN>	<IPV6-ADDR/LEN> – IPv6-адрес и маска подсети, задаётся в виде X:X:X:X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128].

Шаг	Описание	Команда	Ключи
17	Определить тип области (не обязательно).	evt(config-ospf-area)# area-type <TYPE> [no-summary]	<TYPE> – тип области: • stub – устанавливает значение stub (тупиковая область); no-summary – команда в связке с параметром «stub» образует область «totallystubby» (для передачи информации за пределы области используется только маршрут по умолчанию). • nssa – устанавливает значение nssa (область NSSA); no-summary – в связке с параметром nssa образует область totallynssa (автоматически генерирует маршрут по умолчанию как межобластной).
		evt(config-ipv6-ospf-area)# area-type <TYPE> [no-summary]	
18	Включить генерацию маршрута по умолчанию для NSSA или stub-области и анонсирование его в качестве Type-7 или Type-3 LSA соответственно (не обязательно).	evt(config-ospf-area)# default-information-originate	
		evt(config-ipv6-ospf-area)# default-information-originate	
19	Определить тип метрики маршрута по умолчанию для NSSA-области (не обязательно).	evt(config-ospf-area)# default-metric-type <TYPE>	• type-1 – устанавливает тип метрики E1 для маршрута по умолчанию в NSSA-области; • type-2 – устанавливает тип метрики E2 для маршрута по умолчанию в NSSA-области.
		evt(config-ipv6-ospf-area)# default-metric-type <TYPE>	
20	Активировать OSPF-область.	evt(config-ospf-area)# enable	
		evt(config-ipv6-ospf-area)# enable	
21	Установить виртуальное соединение между основной и удаленными областями, имеющими между ними несколько областей (не обязательно).	evt(config-ospf-area)# virtual-link <ID>	<ID> – идентификатор маршрутизатора, с которым устанавливается виртуальное соединение, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
		evt(config-ipv6-ospf-area)# virtual-link <ID>	

Шаг	Описание	Команда	Ключи
22	Установить интервал времени в секундах, по истечении которого маршрутизатор повторно отправит пакет, который не получил подтверждения о получении (не обязательно).	evt(config-ospf- vlink)# retransmit-interval <TIME>	<TIME> – время в секундах, принимает значения [1..65535].
		evt(config-ipv6-ospf- vlink)# retransmit-interval <TIME>	Значение по умолчанию: 5 секунд.
23	Установить интервал времени в секундах, по истечении которого маршрутизатор отправляет следующий hello-пакет (не обязательно).	evt(config-ospf- vlink)# hello- interval <TIME>	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 10 секунд.
		evt(config-bgp-neighbor)# fall- over bfd	
24	Установить интервал времени в секундах, по истечении которого сосед будет считаться неактивным (не обязательно). Этот интервал должен быть кратным значению «hello-interval».	evt(config-ospf- vlink)# dead- interval <TIME>	<TIME> – время в секундах, принимает значения [1..65535]. Для (config-(ipv6)-ospf- vlink) - [2..65535] Значение по умолчанию: 40 секунд.
		evt(config-ipv6-ospf-vlink)# dead- interval <TIME>	
25	Определяется интервал времени в секундах, по истечении которого маршрутизатор выберет DR в сети (не обязательно).	evt(config-ospf- vlink)# wait- interval <TIME>	<TIME> – время в секундах, принимает значения [2..65535]. Значение по умолчанию: 40 секунд.
		evt(config-ipv6-ospf- vlink)# wait- interval <TIME>	
26	Определить алгоритм аутентификации (не обязательно).	evt(config-ospf- vlink)# authentication algorithm <ALGORITHM>	<ALGORITHM> – алгоритм аутентификации: • cleartext – пароль, передается открытым текстом (доступно только для RIP и OSPF-VLINK); • md 5 – пароль, хешируется по алгоритму md5.
27	Установить пароль для аутентификации с соседом (не обязательно).	evt(config-ospf- vlink)# authentication key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> }	<CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов. <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).

Шаг	Описание	Команда	Ключи
28	Определить список паролей для аутентификации через алгоритм хеширования md5 (не обязательно).	evt(config-ospf- vlink)# authentication key chain <KEYCHAIN>	<KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов.
29	Активировать виртуальное соединение (не обязательно).	evt(config-ospf- vlink)# enable	
30	Перейти в режим конфигурирования интерфейса/туннеля/сетевого моста.	evt(config)# interface <IF-TYPE><IF-NUM>	<IF-TYPE> – тип интерфейса; <IF-NUM> – F/S/P – F-фрейм (1), S – слот (0), P – порт.
		evt(config)# tunnel <TUN-TYPE><TUN-NUM>	<TUN-TYPE> – тип туннеля; <TUN-NUM> – номер туннеля.
		evt(config)# bridge <BR-NUM>	<BR-NUM> – номер bridge.
31	Определить принадлежность интерфейса/туннеля/сетевого моста к определенному OSPF-процессу.	evt(config-if-gi)# ip ospf instance <ID>	<ID> – номер процесса, принимает значения [1..65535].
		evt(config-if-gi)# ipv6 ospf instance <ID>	
32	Определить принадлежность интерфейса к определенной области OSPF-процесса.	evt(config-if-gi)# ip ospf area <AREA_ID>	<AREA_ID> – идентификатор области, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
		evt(config-if-gi)# ipv6 ospf area <AREA_ID>	
33	Включить маршрутизацию по протоколу OSPF на интерфейсе.	evt(config-if-gi)# ip ospf	
		evt(config-if-gi)# ipv6 ospf	
34	Включить режим, в котором OSPF-процесс будет игнорировать значение MTU интерфейса во входящих Database Description-пакетах (не обязательно).	evt(config-if-gi)# ip ospf mtu-ignore	
		evt(config-if-gi)# ipv6 ospf mtu-ignore	
35	Определить алгоритм аутентификации протокола OSPF (не обязательно).	evt(config-if-gi)# ip ospf authentication algorithm <ALGORITHM>	<ALGORITHM> – алгоритм аутентификации: • cleartext – пароль, передается открытым текстом; • md 5 – пароль, хешируется по алгоритму md5.

Шаг	Описание	Команда	Ключи
36	Установить пароль для аутентификации с OSPF-соседом при передаче пароля открытым текстом (не обязательно).	evt(config-if-gi)# ip ospf authentication key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> }	<CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).
37	Определить список паролей для аутентификации по алгоритму хеширования md5 с соседом (не обязательно).	evt(config-if-gi)# ip ospf authentication key-chain <KEYCHAIN>	<KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов.
38	Определить пропускную способность интерфейса для расчёта стоимости (cost) интерфейса (не обязательно).	evt(config-if-gi)# ip ospf bandwidth <VALUE> evt(config-if-gi)# ipv6 ospf bandwidth <VALUE>	<VALUE> – пропускная способность интерфейса, принимает значения [1..100000000K].
39	Определить интервал времени в секундах, по истечении которого маршрутизатор выберет DR в сети (не обязательно).	evt(config-if-gi)# ip ospf wait-interval <TIME> evt(config-if-gi)# ipv6 ospf wait-interval <TIME>	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 40 секунд.
40	Установить интервал времени в секундах, по истечении которого маршрутизатор повторно отправит пакет, на который не получил подтверждения о получении (не обязательно).	evt(config-if-gi)# ip ospf retransmit-interval <TIME> evt(config-if-gi)# ipv6 ospf retransmit-interval <TIME>	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 5 секунд.
41	Установить интервал времени в секундах, по истечении которого маршрутизатор отправляет следующий hello-пакет (не обязательно).	evt(config-if-gi)# ip ospf hello-interval <TIME> evt(config-if-gi)# ipv6 ospf hello-interval <TIME>	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 10 секунд.
42	Установить интервал времени в секундах, по истечении которого сосед будет считаться неактивным (не обязательно). Этот интервал должен быть кратным значению hello-interval.	evt(config-if-gi)# ip dead-interval <TIME> evt(config-if-gi)# ipv6 dead-interval <TIME>	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 40 секунд.

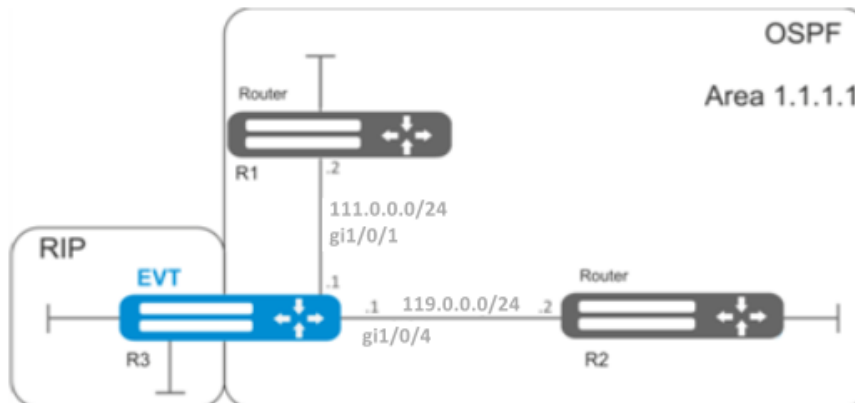
Шаг	Описание	Команда	Ключи
43	Установить интервал времени, в течение которого NBMA-интерфейс ждет, прежде чем отправить hello-пакет соседу, даже в случае, если сосед неактивен (не обязательно).	evt(config-if-gi)# ip poll-interval <TIME>	<TIME> – время в секундах, принимает значения [1 .. 65535].
		evt(config-if-gi)# ipv6 poll-interval <TIME>	Значение по умолчанию: 120 секунд.
44	Задать статический IP-адрес соседа для установления отношения в NMBA и P2MP (Point-to-MultiPoint) сетях (не обязательно).	evt(config-if-gi)# ip ospf neighbor <IP> [non-eligible]	<IP> – IP-адрес соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. non-eligible – опциональный параметр, запрещает устройству участвовать в процессе выбора DR в NBMA-сетях. По умолчанию при создании ipv6 ospf neighbor соединение устанавливается в режиме eligible.
		evt(config-if-gi)# ipv6 ospf neighbor <IPV6-ADDR> [non-eligible]	<IPV6-ADDR> – IPv6-адрес соседа, задаётся в виде X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; non-eligible – опциональный параметр, запрещает устройству участвовать в процессе выбора DR в NBMA-сетях. По умолчанию при создании ipv6 ospf neighbor соединение устанавливается в режиме eligible.

Шаг	Описание	Команда	Ключи
45	Определить тип сети для установления OSPF-соседства (не обязательно).	evt(config-if-gi)# ip ospf network <TYPE>	<TYPE> – тип сети: • broadcast – тип соединения широковещательный; • non - broadcast – тип соединения NBMA; • point - to - multipoint – тип соединения точка-многоточие; • point-to-multipoint non-broadcast – тип соединения NBMA точка-многоточие; • point - to - point – тип соединения точка-точка. Значение по умолчанию: broadcast.
		evt(config-if-gi)# ipv6 ospf network <TYPE>	
46	Перевести интерфейс в пассивный режим работы. В этом режиме не рассылаются hello-пакеты, не устанавливаются отношения соседства, но подключенная сеть анонсируется соседям (не обязательно).	evt(config-if-gi)# ip ospf passive-interface	
		evt(config-if-gi)# ipv6 ospf passive-interface	
47	Установить приоритет маршрутизатора, который используется для выбора DR и BDR (не обязательно).	evt(config-if-gi)# ip ospf priority <VALUE>	<VALUE> – приоритет интерфейса, принимает значения [1..65535]. Значение по умолчанию: 120.
		evt(config-if-gi)# ipv6 ospf priority <VALUE>	
48	Установить величину метрики на интерфейсе или туннеле (не обязательно).	evt(config-if-gi)# ip ospf cost <VALUE>	<VALUE> – величина метрики, задаётся в размере [0..32767]. Значение по умолчанию: 10.
		evt(config-if-gi)# ipv6 ospf cost <VALUE>	
49	Включить протокол BFD для протокола OSPF (не обязательно).	evt(config-if-gi)# ip ospf bfd-enable	
		evt(config-if-gi)# ipv6 ospf bfd-enable	
50	Включить механизм ttl-security hops (не обязательно).	evt(config-if-gi)# ip ospf ttl-security-hops <VALUE>	<VALUE> – значение ttl, задаётся в размере [1..255]. Значение по умолчанию: 0.
		evt(config-if-gi)# ipv6 ospf ttl-security-hops <VALUE>	

Пример настройки

Задача:

Настроить протокол OSPF на маршрутизаторе для обмена маршрутной информацией с соседними маршрутизаторами. Маршрутизатор должен находиться в области с идентификатором 1.1.1.1 и анонсировать маршруты, полученные по протоколу RIP.



Решение:

Предварительно нужно настроить IP-адреса на интерфейсах согласно схеме, приведенной на [рисунке](#).

Создадим OSPF-процесс с идентификатором 10 и перейдем в режим конфигурирования протокола OSPF:

```
evt(config)# router ospf 10
```

Создадим и включим требуемую область:

```
evt(config-ospf)# area 1.1.1.1
evt(config-ospf-area)# enable
evt(config-ospf-area)# exit
```

Включим анонсирование маршрутной информации из протокола RIP:

```
evt(config-ospf)# redistribute rip
```

Включим OSPF-процесс:

```
evt(config-ospf)# enable
evt(config-ospf)# exit
```

Соседние маршрутизаторы подключены к интерфейсам gi1/0/1 и gi1/0/4. Для установления соседства с другими маршрутизаторами привяжем их к OSPF-процессу и области. Далее включим на интерфейсе маршрутизацию по протоколу OSPF:

```

evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# ip ospf instance 10
evt(config-if-gi)# ip ospf area 1.1.1.1
evt(config-if-gi)# ip ospf
evt(config-if-gi)# exit

```

```

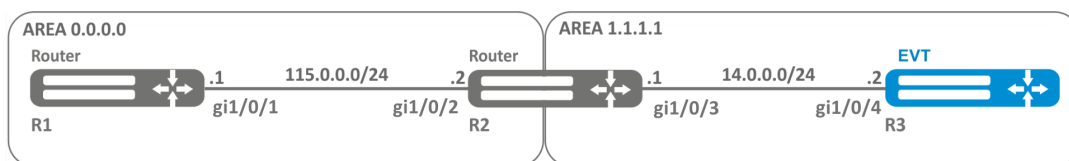
evt(config)# interface gigabitethernet 1/0/4
evt(config-if-gi)# ip ospf instance 10
evt(config-if-gi)# ip ospf area 1.1.1.1
evt(config-if-gi)# ip ospf
evt(config-if-gi)# exit
evt(config)# exit

```

Пример настройки OSPF stub area

Задача:

Изменить тип области 1.1.1.1, область должна быть тупиковой.



Решение:

Предварительно нужно настроить протокол OSPF и IP-адреса на интерфейсах согласно схеме, приведенной на [рисунке](#).

Изменим тип области на тупиковый. На каждом маршрутизаторе из области 1.1.1.1 в режиме конфигурирования области выполним команду:

```

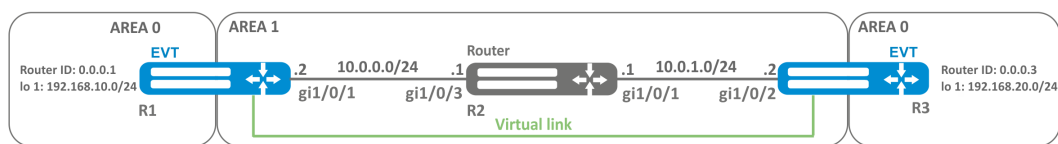
evt(config-ospf-area)# area-type stub

```


Пример настройки Virtual link

Задача:

Объединить две магистральные области в одну с помощью virtual link.



Решение:

⚠ В firewall необходимо разрешить протокол OSPF (89).

Virtual link — это специальное соединение, которое позволяет соединять разорванную на части зону или присоединить зону к магистральной через другую зону. Настраивается между двумя пограничными маршрутизаторами зоны (Area Border Router, ABR).

Предварительно нужно настроить протокол OSPF и IP-адреса на интерфейсах согласно схеме, приведенной на [рисунке](#).

На маршрутизаторе R1 перейдем в режим конфигурирования области 1.1.1.1:

```
evt(config-ospf)# area 1.1.1.1
```

Создадим virtual link с идентификатором 0.0.0.3 и включим его:

```
evt(config-ospf-area)# virtual-link 0.0.0.3
evt(config-ospf-vlink)# enable
```

На маршрутизаторе R3 перейдем в режим конфигурирования области 1.1.1.1:

```
evt(config-ospf)# area 1.1.1.1
```

Создадим virtual link с идентификатором 0.0.0.1 и включим его:

```
evt(config-ospf-area)# virtual-link 0.0.0.1
evt(config-ospf-vlink)# enable
```

Рассмотрим таблицу маршрутизации на маршрутизаторе R1:

```
evt# show ip route
C    * 10.0.0.0/24      [0/0]    dev gil/0/1,                [direct 00:49:34]
O    * 10.0.1.0/24      [150/20] via 10.0.0.1 on gil/0/1,    [ospf1 00:49:53] (0.0.0.3)
O    * 192.168.20.0/24  [150/30] via 10.0.0.1 on gil/0/1,    [ospf1 00:50:15] (0.0.0.3)
C    * 192.168.10.0/24  [0/0]    dev lo1,                  [direct 21:32:01]
```

Рассмотрим таблицу маршрутизации на маршрутизаторе R3:

```

evt# show ip route
O    * 10.0.0.0/24      [150/20] via 10.0.1.1 on gil/0/1,      [ospf1 14:38:35] (0.0.0.2)
C    * 10.0.1.0/24      [0/0]    dev gil/0/1,                  [direct 14:35:34]
C    * 192.168.20.0/24   [0/0]    dev lo1,                             [direct 14:32:58]
O    * 192.168.10.0/24   [150/30] via 10.0.1.1 on gil/0/1,      [ospf1 14:39:54] (0.0.0.1)

```

Так как OSPF считает виртуальный канал частью области, в таблице маршрутизации R1 маршруты, полученные от R3, отмечены как внутризоновые и наоборот.

Для просмотра соседей можно воспользоваться следующей командой:

```

evt# show ip ospf neighbors 10

```

Таблицу маршрутов протокола OSPF можно просмотреть командой:

```

evt# show ip ospf 10

```

Настройка BGP

Протокол BGP предназначен для обмена информацией о достижимости подсетей между автономными системами (далее AS), то есть группами маршрутизаторов под единым техническим управлением, использующими протокол внутридоменной маршрутизации для определения маршрутов внутри себя и протокол междоменной маршрутизации для определения маршрутов доставки пакетов в другие AS. Передаваемая информация включает в себя список AS, к которым имеется доступ через данную систему. Выбор наилучших маршрутов осуществляется исходя из правил, принятых в сети.

Алгоритм настройки

 Для установлении BGP-сессии необходимо в firewall разрешить TCP-порт 179.

Шаг	Описание	Команда	Ключи
1	Настроить приоритетность протокола BGP-маршрутизации для основной таблицы маршрутизации (не обязательно).	evt(config)# ip protocols bgp preference <VALUE>	<VALUE> – приоритетность протокола, принимает значения в диапазоне [1..255]. Значение по умолчанию: BGP (170).

Шаг	Описание	Команда	Ключи
2	Настроить емкость таблиц маршрутизации протокола BGP (не обязательно при использовании глобальной таблицы маршрутизации).	evt(config)# ip protocols bgp max-routes <VALUE>	<VALUE> – количество маршрутов протокола BGP в маршрутной таблице, принимает значения в диапазоне [1..5000000] Значение по умолчанию для глобальной таблицы маршрутизации [2500000] Значение по умолчанию для VRF: 0.
		evt(config)# ipv6 protocols bgp max-routes <VALUE>	
		evt(config-vrf)# ip protocols bgp max-routes <VALUE>	
		evt(config-vrf)# ipv6 protocols bgp max-routes <VALUE>	
3	Включить вывод информации о состоянии отношений с соседями для протокола маршрутизации BGP (не обязательно).	evt(config)# router bgp log-neighbor-changes	
		evt(config)# ipv6 router bgp log-neighbor-changes	
4	Включить ECMP и определяется максимальное количество равноценных маршрутов до цели.	evt(config)# router bgp maximum-paths <VALUE>	<VALUE> – количество допустимых равноценных маршрутов до цели, принимает значения [1..16].
5	Выбрать метод фильтрации для передаваемой информации между роутерами (обязательно при конфигурировании eBGP для анонсирования подсетей).		
5.1.1	При выборе метода фильтрации на основе route-map создать список правил, который в дальнейшем будет использоваться для фильтрации анонсируемых и получаемых IP-маршрутов.	evt(config)# route-map <NAME>	<NAME> – имя конфигурируемых правил маршрутизации, задаётся строкой до 31 символа.
5.1.2	Создать правило.	(config-route-map)# rule <ORDER>	<ORDER> – номер правила, принимает значения [1 .. 10000].

Шаг	Описание	Команда	Ключи
5.1.3	Определить список подсетей, которые затрагиваются правилом.	<pre> evt(config-route-map-rule)#match ip address { <ADDR/LEN> object- group <OBJ-GRP-NETNAME> } [{ eq <LEN> le <LEN> ge <LEN 1> [le <LEN 2>] }] </pre> <pre> evt(config-route-map-rule)#match ipv6 address { <IPV6-ADDR/LEN> object-group <OBJ-GRP- NETNAME> } [{ eq <LEN> le <LEN> ge <LEN 1> [le <LEN 2>] }] </pre>	<ADDR/LEN> – IP-адрес и маска подсети, задается в виде: • AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32]; <IPV6-ADDR/LEN> – IPv6-адрес и маска подсети, задается в виде: • X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128]; <OBJ-GRP-NETNAME> – имя профиля IP-адресов, задается строкой до 31 символа. При использовании фильтрации по object-group их необходимо создать заранее; <LEN>, <LEN 1>, <LEN 2> – длина префикса, принимает значения [1..32] в IP-списках префиксов для IPv4 и [1..128] для IPv6; eq – при указании команды длина префикса должна соответствовать указанной; le – при указании команды длина префикса должна быть меньше либо соответствовать указанной; ge – при указании команды длина префикса должна быть больше либо соответствовать указанной; ge <LEN 1> le <LEN 2> – при указании команды длина префикса должна быть больше либо соответствовать <LEN>, но меньше или равна <LEN1>.

Шаг	Описание	Команда	Ключи
5.1.4	Разрешить (permit) или запретить (deny) действие для указанных подсетей в правиле.	evt(config-route-map-rule)# action {deny permit}	
5.2.1	При выборе метода фильтрации на основе префикс-листов создать списки IP-подсетей, которые в дальнейшем будут использоваться для фильтрации анонсируемых и получаемых IP-маршрутов.	evt(config)# ip prefix-list <NAME> evt(config)# ipv6 prefix-list <NAME>	<NAME> – имя конфигурируемого списка подсетей, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
5.2.2	Разрешить (permit) или запретить (deny) списки префиксов.	<pre> evt(config-pl)# permit { <ADDR/LEN> object-group <OBJ-GRP-NETNAME> } [{ eq <LEN> le <LEN> ge <LEN 1> [le <LEN 2>] }] evt(config-pl)# deny { <ADDR/LEN> object-group <OBJ-GRP-NETNAME> } [{ eq <LEN> le <LEN> ge <LEN 1> [le <LEN 2>] }] evt(config-ipv6-pl)# permit { <IPV6-ADDR/LEN> object-group <OBJ-GRP-NETNAME> } [{ eq <LEN> le <LEN> ge <LEN 1> [le <LEN 2>] }] evt(config-ipv6-pl)# deny { <IPV6-ADDR/LEN> object-group <OBJ-GRP-NETNAME> } [{ eq <LEN> le <LEN> ge <LEN 1> [le <LEN 2>] }] </pre>	<ADDR/LEN> – IP-адрес и маска подсети, задается в виде: • AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32]; <IPV6-ADDR/LEN> – IPv6-адрес и маска подсети, задается в виде: • X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128]; <OBJ-GRP-NETNAME> – имя профиля IP-адресов, задается строкой до 31 символа. При использовании фильтрации по object-group их необходимо создать заранее; <LEN>, <LEN 1>, <LEN 2> – длина префикса, принимает значения [1..32] в IP-списках префиксов для IPv4 и [1..128] для IPv6; eq – при указании команды длина префикса должна соответствовать указанной; le – при указании команды длина префикса должна быть меньше либо соответствовать указанной; ge – при указании команды длина префикса должна быть больше либо соответствовать указанной; ge <LEN 1> le <LEN 2> – при указании команды длина префикса должна быть больше либо соответствовать <LEN> но меньше или равна <LEN1>.

Шаг	Описание	Команда	Ключи
6	Добавить BGP-процесс в систему и осуществить переход в режим настройки параметров BGP-процесса.	evt(config)# router bgp <AS>	<AS> – номер автономной системы процесса, принимает значения [1..4294967295].
7	Установить идентификатор маршрутизатора.	evt(config-bgp)# router-id { <ID> <IF> <TUN> }	<ID> – идентификатор маршрутизатора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. <IF> – интерфейс, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора. <TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора.
8	Установить идентификатор Route-Reflector кластера, которому принадлежит BGP-процесс маршрутизатора (при необходимости).	evt(config-bgp)# cluster-id <ID>	<ID> – идентификатор Route-Reflector кластера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
9	Включить генерацию и отправку маршрута по умолчанию, если маршрут по умолчанию есть в таблице маршрутизации FIB (не обязательно).	evt(config-bgp)# default-information-originate	
10	Установить временной интервал, по истечении которого идет проверка соединения со встречной стороной (не обязательно).	evt(config-bgp-af)# timers keepalive <TIME>	<TIME> – время в секундах, принимает значения [1..32767]. Значение по умолчанию: 60 секунд.
11	Установить временной интервал, по истечении которого встречная сторона считается недоступной (не обязательно).	evt(config-bgp-af)# timers holdtime <TIME>	<TIME> – время в секундах, принимает значения [2..65535]. Значение по умолчанию: 180 секунд.

Шаг	Описание	Команда	Ключи
12	Установить время минимальной и максимальной задержки, в течение которого запрещено устанавливать соединение, в целях защиты от частых разрывов соединения (не обязательно).	evt(config-bgp)# timers error-wait <TIME1> <TIME2>	<TIME1> – время минимальной задержки в секундах, принимает значения [1..65535]; <TIME2> – время максимальной задержки в секундах, принимает значения [1..65535].
13	Определить глобальный алгоритм аутентификации с соседями (при необходимости).	evt(config-bgp)# authentication algorithm <ALGORITHM>	<ALGORITHM> – алгоритм шифрования: • md5 – пароль шифруется по алгоритму md5. Значение по умолчанию: шифрование не используется.
14	Установить глобальный пароль для аутентификации с соседями (используется совместно с "authentication algorithm").	evt(config-bgp)# authentication key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> }	<CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).
15	Активировать BGP-процесс.	evt(config-bgp)# enable	
16	Определить тип конфигурируемой маршрутной информации и перейти в данный режим настройки.	evt(config-bgp)# address-family { ipv4 ipv6 } unicast	ipv 4 – семейство IPv4; ipv 6 – семейство IPv6.
17	Включить анонсирование маршрутов процессом BGP полученных альтернативным образом (при необходимости).	evt(config-bgp-af)# redistribute static [route-map <NAME>]	<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых статических маршрутов, задаётся строкой до 31 символа.
		evt(config-bgp-af)# redistribute connected [route-map <NAME>]	<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых напрямую подключенных подсетей, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
		evt(config-bgp-af)# redistribute rip [route-map <NAME>]	<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых RIP-маршрутов, задаётся строкой до 31 символа.
		evt(config-bgp-af)# redistribute ospf <ID> <ROUTE-TYPE 1> [<ROUTE-TYPE 2>] [<ROUTE-TYPE 3>] [<ROUTE-TYPE 4>] [route-map <NAME>]	<ID> – номер процесса, может принимать значение {1..65535}; <ROUTE-TYPE> – тип маршрута: • intra - area – анонсирование маршрутов OSPF-процесса в пределах зоны; • inter - area – анонсирование маршрутов OSPF-процесса между зонами; • external 1 – анонсирование внешних маршрутов OSPF-формата 1; • external 2 – анонсирование внешних маршрутов OSPF-формата 2; <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых OSPF-маршрутов, задаётся строкой до 31 символа.
		evt(config-bgp-af)# redistribute bgp <AS> [route-map <NAME>]	<AS> – номер автономной системы, может принимать значения [1..4294967295]; <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых BGP-маршрутов, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
18	Включить анонсирование подсетей.	evt(config-bgp-af)# network <ADDR/LEN> [route-map <NAME>]	<ADDR/LEN> – адрес подсети, указывается в одном из следующих формате: • AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32]; • X:X:X:X::X/EE – IPv6-адрес и маска подсети, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128]. <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых BGP-маршрутов, задаётся строкой до 31 символа.
19	Осуществить выход из режима глобального конфигурирования анонсов маршрутной информации процесса BGP	evt(config-bgp-af)# exit	
20	Добавить BGP-соседа и осуществить переход в режим настройки параметров BGP-соседа.	evt(config-bgp)# neighbor <ADDR> <IPv6-ADDR>	<ADDR> – IP-адрес соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPv6-ADDR> – IPv6-адрес клиента, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
21	Задать описание соседа (не обязательно).	evt(config-bgp-neighbor)# description <DESCRIPTION>	<DESCRIPTION> – описание соседа, задаётся строкой до 255 символов.

Шаг	Описание	Команда	Ключи
22	Установить временной интервал, по истечении которого идет проверка соединения со встречной стороной (не обязательно).	evt(config-bgp-neighbor)# timers keepalive <TIME>	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 60 секунд.
23	Установить временной интервал, по истечении которого встречная сторона считается недоступной (не обязательно).	evt(config-bgp- neighbor)# timers holdtime <TIME>	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 180 секунд.
24	Установить время минимальной и максимальной задержки, в течение которого запрещено устанавливать соединение, в целях защиты от частых разрывов соединения (не обязательно).	evt(config-bgp)# timers error-wait <TIME1> <TIME2>	<TIME1> – время минимальной задержки в секундах, принимает значения [1..65535]; <TIME2> – время максимальной задержки в секундах, принимает значения [1..65535]. Значение по умолчанию: 60 и 300 секунд.
25	Установить номер автономной системы BGP-соседа.	evt(config-bgp-neighbor)# remote-as <AS>	<AS> – номер автономной системы, принимает значения [1..4294967295].
26	Разрешить подключение к соседям, которые находятся не в напрямую подключенных подсетях (не обязательно).	evt(config-bgp-neighbor)# ebgp-multihop <NUM>	<NUM> – максимальное количество хопов при установке EBGП (используется для TTL).
27	Указать, что BGP-сосед является Route-Reflector клиентом (не обязательно).	evt(config-bgp-neighbor)# route-reflector-client	

Шаг	Описание	Команда	Ключи
28	Задать IP/IPv6-адрес маршрутизатора, который будет использоваться в качестве IP/IPv6-адреса источника в отправляемых обновлениях маршрутной информации BGP (не обязательно).	evt(config-bgp-neighbor)# update-source { <ADDR> <IPv6-ADDR> <IF> <TUN> }	<ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPv6-ADDR> – IPv6-адрес источника, задаётся в виде X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. <IF> – интерфейс, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора. <TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора.
29	Включить режим, в котором разрешен приём маршрутов в BGP-атрибуте, AS Path которых содержит номера автономной системы процесса (не обязательно).	evt(config-bgp-neighbor)# allow-local-as <NUMBER>	<NUMBER> – пороговое число вхождений номера автономной системы процесса в атрибуте AS Path, при которых маршрут будет принят, диапазон допустимых значений [1..10].
30	Включить BFD-протокол на конфигурируемом BGP-соседе (не обязательно, используется совместно с параметром update-source).	evt(config-bgp-neighbor)# fall-over bfd	
31	Включить режим, при котором соседство BGP разрывается, как только указанный маршрут к соседу удаляется из таблицы маршрутизации.	evt(config-bgp-neighbor)# fall-over route-map [route-map <NAME>]	<NAME> – имя маршрутной карты, которая будет использоваться для отслеживания наличия маршрута, задаётся строкой до 31 символа.
32	Определить алгоритм аутентификации с соседом (не обязательно).	evt(config-bgp-neighbor)# authentication algorithm <ALGORITHM>	<ALGORITHM> – алгоритм шифрования: md5 – пароль шифруется по алгоритму md5.

Шаг	Описание	Команда	Ключи
33	Установить пароль для аутентификации с соседом (не обязательно).	evt(config-bgp-neighbor)# authentication key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> }	<CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).
34	Сделать соседство активным.	evt(config-bgp-neighbor)# enable	
35	Определить тип конфигурируемой маршрутной информации соседа и перейти в данный режим настройки.	evt(config-bgp-neighbor)# address-family { ipv4 ipv6 vpnv4 } unicast	ipv 4 – семейство IPv4; ipv 6 – семейство IPv6; vpnv4 – семейство VPNv4.
36	При выборе режима фильтрации на основе префикс-листов добавить фильтрацию подсетей во входящих или исходящих обновлениях (обязательно при конфигурировании eBGP для анонсирования подсетей).	evt(config-bgp-neighbor-af)# prefix-list <PREFIX-LIST-NAME> { in out }	<PREFIX-LIST-NAME> – имя сконфигурированного списка подсетей, задаётся строкой до 31 символа. in – фильтрация входящих маршрутов; out – фильтрация анонсируемых маршрутов.
37	Задать режим, в котором BGP-соседу в обновлении на ряду с другими маршрутами всегда отправляется маршрут по умолчанию. (не обязательно, отсутствует для vpnv4).	evt(config-bgp-neighbor-af)# default-originate	
38	Задать режим, в котором все обновления отправляются BGP-соседу с указанием в качестве next-hop IP-адреса исходящего интерфейса локального маршрутизатора. По умолчанию изменяет next-hop только eBGP-маршрутов (не обязательно, отсутствует для vpnv4).	evt(config-bgp-neighbor-af)# next-hop-self [all]	all – заменить next-hop для eBGP-, iBGP-маршрутов.
39	Определить приоритетность маршрутов, получаемых от соседа (не обязательно).	evt(config-bgp-neighbor-af)# preference <VALUE>	<VALUE> – приоритетность маршрутов соседа, принимает значения в диапазоне [1..255]. Значение по умолчанию: 170.

Шаг	Описание	Команда	Ключи
40	Задать режим, в котором перед отправлением обновления из BGP-атрибута AS Path маршрутов удаляются приватные номера автономных систем (в соответствии с RFC 6996) (не обязательно, отсутствует для vprnv4).	evt(config-bgp-neighbor-af)# remove-private-as [{ all nearest replace }]	all – удалить все частные номера AS из AS-path; nearest – заменить ближайшие частные AS в AS-path на рядом стоящую публичную AS; replace – заменить все частные номера AS номером текущего процесса BGP. Значение по умолчанию: all.
41	Включить обмен маршрутной информацией.	evt(config-bgp-neighbor-af)# enable	
42	Задать режим, в котором маршрутизатор будет представляться указанным номером автономной системы вместо реального номера автономной системы (не обязательно).	evt(config-bgp-neighbor)# local-as <AS>	<AS> – номер автономной системы, принимает значения [1..4294967295].
43	Не добавлять указанный в local-as номер автономной системы в AS-Path при приёме маршрута (не обязательно).	evt(config-bgp-local-as)# no- prepend	
44	Добавлять в AS-Path только номер автономной системы, указанный в local-as (не обязательно).	evt(config-bgp-local-as)# replace- as	
45	Включить агрегирование маршрутной информации (не обязательно).	evt(config-bgp)# aggregate- address { <ADDR/LEN> <IPV6- ADDR/LEN }	<ADDR/LEN> – IP-адрес и маска подсети, задается в виде: • AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32]; <IPV6-ADDR/LEN> – IPv6-адрес и маска подсети, задается в виде: • X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128];

Шаг	Описание	Команда	Ключи
46	Задать route-map для установки дополнительных условий агрегирования маршрутов (не обязательно).	evt(config-bgp-aggregate)# advertise-map [route-map <NAME>]	<NAME> – имя маршрутной карты, которая будет использоваться для задания условий агрегирования BGP-маршрутов, задаётся строкой до 31 символа.
47	Добавлять в AS-Path агрегированного маршрута номера автономных систем из AS-Path его компонентов (не обязательно).	evt(config-bgp-aggregate)# as-set	
48	Задать route-map для установки дополнительных атрибутов агрегированного маршрута (не обязательно).	evt(config-bgp-aggregate)# attribute-map [route-map <NAME>]	<NAME> – имя маршрутной карты, которая будет использоваться для задания атрибутов агрегированного BGP-маршрута, задаётся строкой до 31 символа.
49	Подавлять все компоненты агрегированного маршрута (не обязательно).	evt(config-bgp-aggregate)# summary-only	
50	Задать route-map для подавления компонентов агрегированного маршрута (не обязательно).	evt(config-bgp-aggregate)# suppress-map [route-map <NAME>]	<NAME> – имя маршрутной карты, которая будет использоваться для задания подавляемых компонентов агрегированного BGP-маршрута, задаётся строкой до 31 символа.
51	Задать возможность динамически устанавливать BGP-сессию без указания конкретного адреса соседа. Соседство может быть установлено с любым адресом, попадающим в указанную подсеть (не обязательно).	evt(config-bgp-aggregate)# listen- range { <ADDR/LEN> <IPV6- ADDR/LEN }	<ADDR/LEN> – IP-адрес и маска подсети, задается в виде: • AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32]; <IPV6-ADDR/LEN> – IPv6-адрес и маска подсети, задается в виде: • X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128].

Шаг	Описание	Команда	Ключи
52	Разрешить возможность динамической установки BGP-сессии только с соседями, которые имеют определённые номера AS.	evt(config-bgp-listen)# as-range <AS-PATH>	<AS-PATH> – список номеров автономных систем, задается в виде AS-AS,AS,AS-AS, принимает значения [1..4294967295].
53	Установить пассивный режим установки соединения с BGP-пиром (не обязательно)	evt(config-bgp-neighbor)# connection-mode passive	

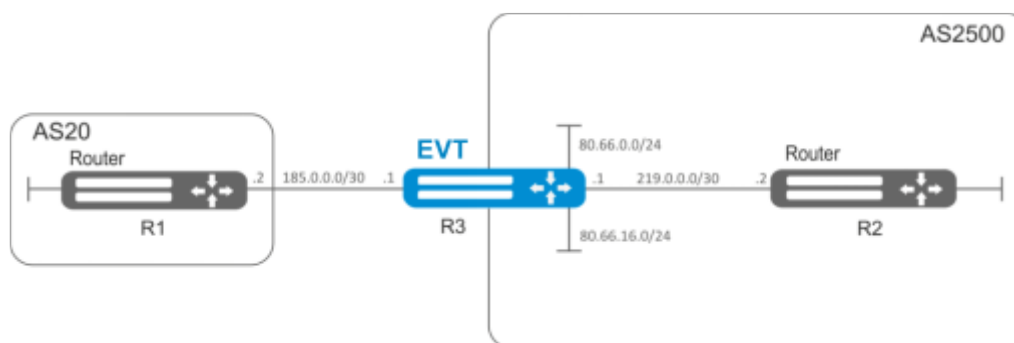
- ✓ Часто бывает, особенно при конфигурировании iBGP, что в одном bgp-процессе необходимо настроить несколько bgp neighbor с одинаковыми параметрами. Во избежание избыточности конфигурации рекомендуется использовать bgp peer-group, в которой возможно описать общие параметры, а в конфигурации bgp neighbor просто указать причастность к bgp peer-group.

Пример настройки

Задача:

Настроить BGP-протокол на маршрутизаторе R3 со следующими параметрами:

- собственные подсети: 80.66.0.0/24, 80.66.16.0/24;
- анонсирование подсетей, подключенных напрямую;
- собственная AS 2500;
- первое соседство – подсеть 219.0.0.0/30, собственный IP-адрес 219.0.0.1, IP-адрес соседа 219.0.0.2, AS2500;
- второе соседство – подсеть 185.0.0.0/30, собственный IP-адрес 185.0.0.1, IP-адрес соседа 185.0.0.2, AS20.



Решение:

Сконфигурируем необходимые сетевые интерфейсы:

```

evt-R3(config)# interface gigabitethernet 1/0/1
evt-R3(config-if-gi)# ip address 185.0.0.1/30
evt-R3(config-if-gi)# exit
evt-R3(config)# interface gigabitethernet 1/0/2
evt-R3(config-if-gi)# ip address 219.0.0.1/30
evt-R3(config-if-gi)# exit
evt-R3(config)# interface gigabitethernet 1/0/3
evt-R3(config-if-gi)# ip address 80.66.0.1/24
evt-R3(config-if-gi)# exit
evt-R3(config)# interface gigabitethernet 1/0/4
evt-R3(config-if-gi)# ip address 80.66.16.1/24
evt-R3(config-if-gi)# exit

```

Сконфигурируем firewall для приема маршрутизатором BGP-трафика из зоны безопасности WAN:

```

evt-R3(config)# object-group service og_bgp
evt-R3(config-object-group-service)# port-range 179
evt-R3(config-object-group-service)# exit
evt-R3(config)# security zone wan
evt-R3(config-zone)# exit
evt-R3(config)# security zone-pair wan self
evt-R3(config-zone-pair)# rule 100
evt-R3(config-zone-pair-rule)# match protocol tcp
evt-R3(config-zone-pair-rule)# match destination-port object-group og_bgp
evt-R3(config-zone-pair-rule)# action permit
evt-R3(config-zone-pair-rule)# enable
evt-R3(config-zone-pair-rule)# exit
evt-R3(config-zone-pair)# exit

```

И укажем принадлежность интерфейсов к зоне безопасности:

```

evt-R3(config)# interface gigabitethernet 1/0/1
evt-R3(config-if-gi)# security-zone wan
evt-R3(config-if-gi)# exit
evt-R3(config)# interface gigabitethernet 1/0/2
evt-R3(config-if-gi)# security-zone wan
evt-R3(config-if-gi)# exit

```

Создадим route-map, который будет использоваться в дальнейшем при настройке разрешающих анонсов роутерам из другой AS:

```

evt-R3(config)# route-map bgp-general
evt-R3(config-route-map)# rule 1
evt-R3(config-route-map-rule)# match ip address 80.66.0.0/24
evt-R3(config-route-map-rule)# action permit
evt-R3(config-route-map-rule)# exit
evt-R3(config-route-map)# rule 2
evt-R3(config-route-map-rule)# match ip address 80.66.16.0/24
evt-R3(config-route-map-rule)# action permit
evt-R3(config-route-map-rule)# exit
evt-R3(config-route-map)# exit

```

Создадим BGP процесс для AS 2500 и войдем в режим конфигурирования параметров процесса:

```

evt(config)# router bgp 2500

```

Сконфигурируем анонсирование подсетей, подключенных напрямую:

```

evt-R3(config-bgp)# address-family ipv4 unicast
evt-R3(config-bgp-af)# redistribute connected
evt-R3(config-bgp-af)# exit

```

Создадим соседство с роутером R2 по iBGP:

```

evt-R3(config-bgp)# neighbor 219.0.0.2
evt-R3(config-bgp-neighbor)# remote-as 2500
evt-R3(config-bgp-neighbor)# enable

```

И включим обмен IPv4-маршрутами:

```

evt-R3(config-bgp-neighbor)# address-family ipv4 unicast
evt-R3(config-bgp-neighbor-af)# enable
evt-R3(config-bgp-neighbor-af)# exit
evt-R3(config-bgp-neighbor)# exit

```

Создадим соседство с роутером R1 по eBGP:

```

evt-R3(config-bgp)# neighbor 185.0.0.2
evt-R3(config-bgp-neighbor)# remote-as 20
evt-R3(config-bgp-neighbor)# enable

```

И включим обмен IPv4-маршрутами, разрешив необходимые маршруты для анонса при помощи заранее подготовленного route-map:

```

evt-R3(config-bgp-neighbor)# address-family ipv4 unicast
evt-R3(config-bgp-neighbor-af)# route-map bgp-general out
evt-R3(config-bgp-neighbor-af)# enable
evt-R3(config-bgp-neighbor-af)# exit
evt-R3(config-bgp-neighbor)# exit

```

Включим работу протокола:

```
evt-R3(config-bgp)# enable  
evt-R3(config-bgp)# exit
```

Информацию о BGP-пирах можно посмотреть командой:

```
evt# show bgp neighbors
```

Таблицу маршрутов протокола BGP можно просмотреть с помощью команды:

```
evt# show bgp ipv4 unicast
```

Политика выбора лучшего маршрута в протоколе BGP

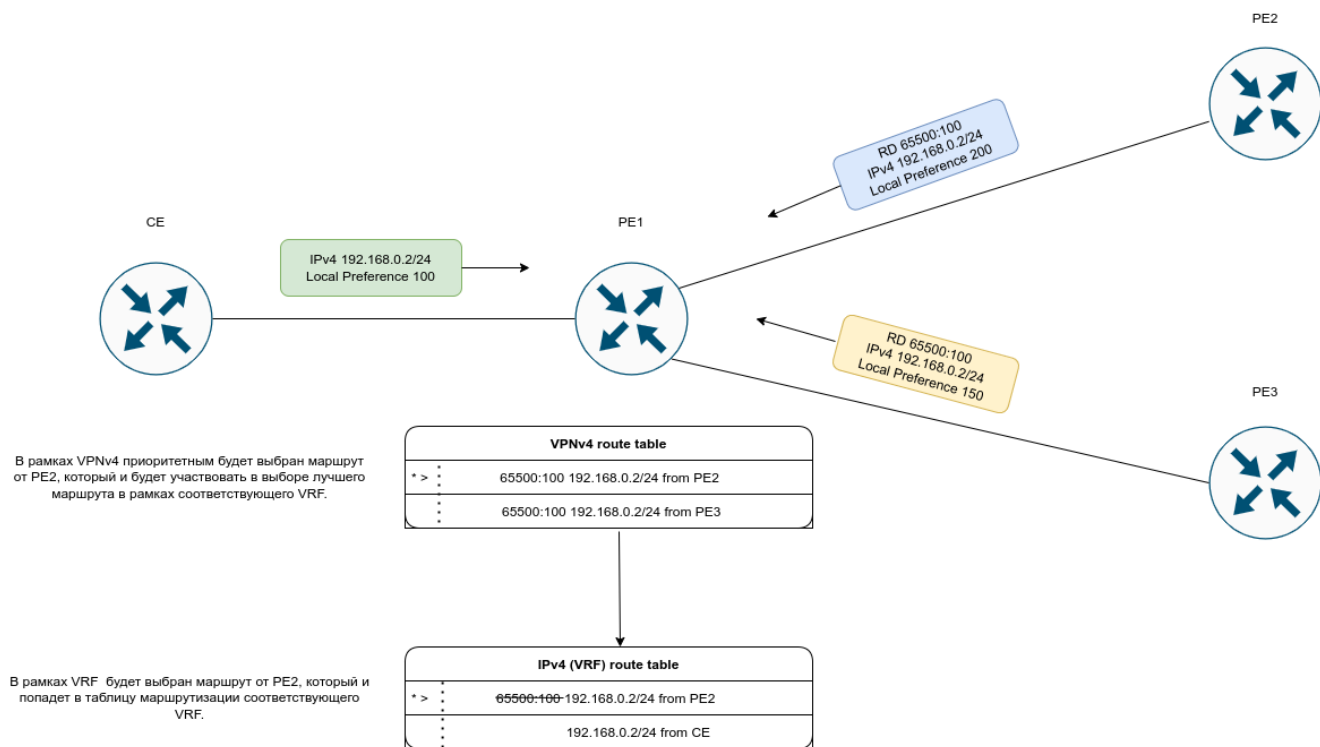
В процессе работы BGP обычно вычисляет один лучший маршрут до каждой полученной подсети. Если нет более приоритетного маршрута, полученного при помощи другого протокола маршрутизации до этой подсети, то маршрут устанавливается в таблицу маршрутизации.

 Если включен механизм ECMP (`router bgp maximum-paths ..`), то в таблицу маршрутизации могут попасть до 16 активных маршрутов до одной подсети.
При анонсировании BGP пирам будут использоваться атрибуты лучшего маршрута.

Ниже приведен алгоритм выбора лучшего маршрута в протоколе BGP:

 Алгоритм применяется для следующих address family: unicast IPv4, unicast IPv6, VPNv4 unicast, VPLS.

- i** Для VPNv4 маршрутов выбор лучшего маршрута происходит следующим образом: Сначала выбор лучшего маршрута происходит в рамках своего RD, затем в рамках VRF, куда он попадет в соответствии со своим RT.



Прежде всего проверяется доступность next-hop-а у маршрута. Next-hop считается доступным, если до него можно определить connected-маршрут.

1. Маршрут, помеченный как «stale», является менее приоритетным, чем маршрут без таковой метки. Маршрут помечается как «stale» в процессе работы технологии LLGR;
2. Сравнивается значение атрибута Weight – лучшим становится маршрут, имеющий большее значение;
3. Сравнивается значение атрибута Local preferences – лучшим становится маршрут, имеющий большее значение;
4. Сравнивается длина AS-path – маршрут с меньшим количеством hop-ов становится лучшим;
5. Сравнивается значение атрибута Origin – IGP является самым приоритетным. EGP приоритетнее, чем Incomplete;
6. Для маршрутов, принятых от одной и той же автономной системы, сравнивается значение атрибута multiple exit discriminator (MED) – наименьшее значение атрибута имеет больший приоритет;
7. Маршрут, полученный от EBGP-пира, имеет больший приоритет по сравнению с маршрутом, полученным от IBGP-пира;
8. Сравнивается IGP-метрика сети, через который доступен маршрут – наименьшее значение имеет больший приоритет;
- 8.1 Если включен ECMP, то дальнейших сравнений не производится и маршрут (multipath) попадет в таблицу маршрутизации;
9. Сравнивается параметр Router-Id – маршрут, полученный от BGP-соседа с наименьшим Router-Id, является приоритетным. При наличии атрибута Originator ID будет учитываться Router-id источника маршрута;
10. Сравнивается количество адресов в Cluster list – маршрут, имеющий наименьшее количество адресов становится лучшим;

11. Сравниваются адреса BGP-пиров – маршрут, полученный от BGP-пира с наименьшим из адресов, является приоритетным.

В выводе маршрутной информации для определенного префикса лучший маршрут будет отмечен как «Best»:

```

evt# show bgp ipv4 unicast 192.0.2.0/24
192.0.2.0/24 via 100.64.28.1 on gil/0/1.2800 [bgp65514 2022-05-22] (65041i)
  Administrative Distance: 170
  Type: unicast
  Origin: IGP
  AS PATH: 65054 65055 65056 65077 65098 65059
  Next Hop: 100.64.28.1
  Local Preference: 100
  Community: (3356:2) (3356:22) (3356:86) (3356:501) (3356:666) (3356:903) (335
6:2065)
              (12389:6) (65000:64990)
  Weight: 0
  Valid
192.0.2.0/24 via 101.7.0.1 on gil/0/1.2800 [bgp65514 2022-05-22] (65041i)
  Administrative Distance: 170
  Type: unicast
  Origin: IGP
  AS PATH: 65020 65030
  Next Hop: 101.7.0.1
  Local Preference: 200
  Community: (3356:2) (3356:22) (3356:86) (3356:501) (3356:666) (3356:903) (335
6:2065)
              (12389:6) (65000:64990)
  Weight: 0
  Valid,Best

```

Условное анонсирование маршрутной информации (Conditional Advertisement)

В обычных сценариях BGP анонсирует все лучшие маршруты из своей BGP RIB. Иногда необходимо более гибкое управление анонсируемой маршрутной информацией. В этом случае рекомендуется использование функции Conditional advertisement, которая позволяет описать условия, при совпадении которых будет анонсироваться (или наоборот отзываться) необходимая маршрутная информация.

- i** В текущей реализации функционал поддержан для IPv4 (AFI -1, SAFI -1), IPv6 (AFI -2, SAFI -1) маршрутов.
Реализована поддержка как для GRT, так и в VRF.

Для работы Conditional advertisement необходимо выполнить следующие шаги:

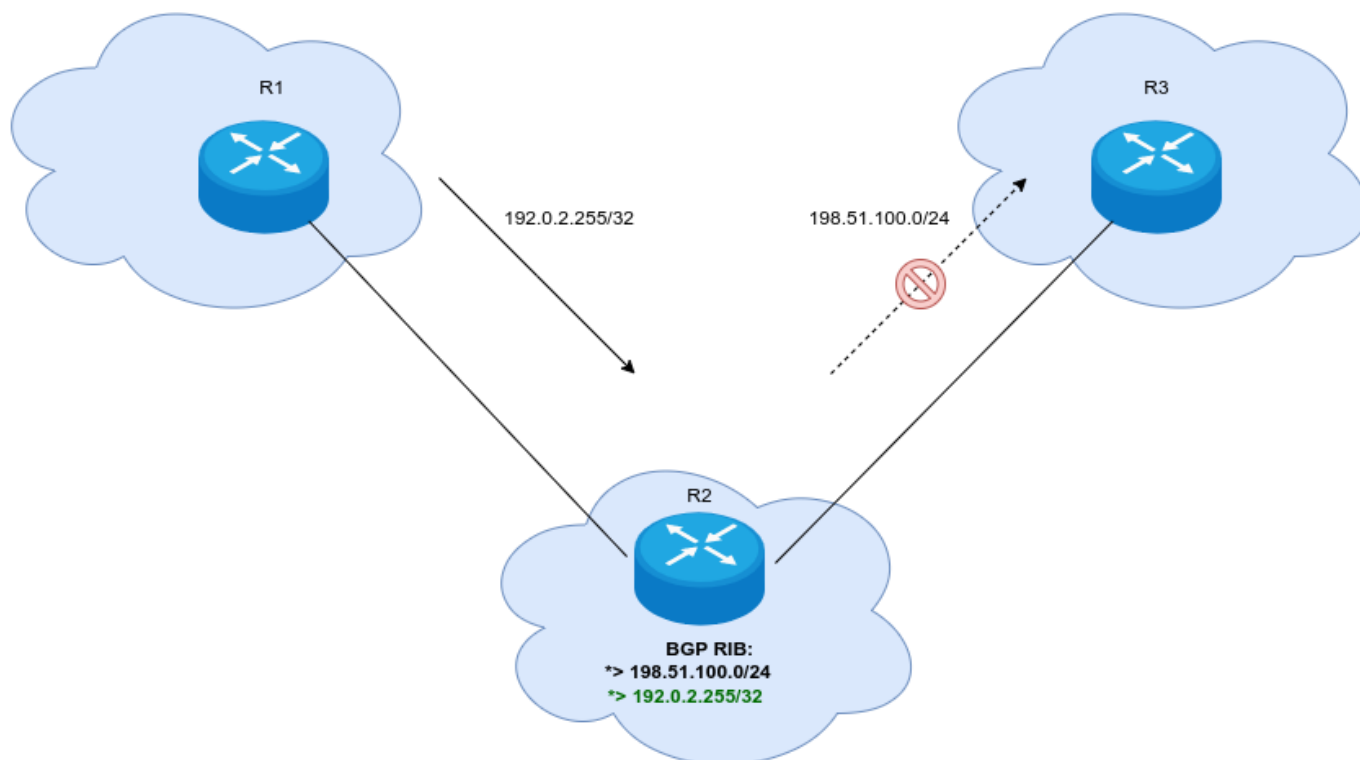
1. Описать маршрутные карты condition-map и advertise-map:

- Condition-map – это карта, в которой необходимо описать маршрутную информацию для проверки. Планировщик будет запускаться каждые 60 секунд для проверки наличия в BGP RIB маршрутной информации, описанной в этой карте;
- Advertise-map – это карта, в которой необходимо описать маршрутную информацию, которая будет анонсироваться при выполнении условий, описанных в condition-map.

2. В контексте настройки BGP-соседа необходимо задать условие, при котором будет анонсироваться маршрутная информация, описанная в advertise-map. Рассмотрим этот пункт на примере ниже:

Условие EXIST-MAP:

- Если R2 содержит в BGP RIB маршрут 192.0.2.255/32, то R2 анонсирует в сторону R3 маршрут 198.51.100.0/24 (пример на рисунке ниже);
- Если R2 не содержит в BGP RIB маршрут 192.0.2.255/32, то анонсирование маршрута 198.51.100.0/24 соседу R3 не происходит.



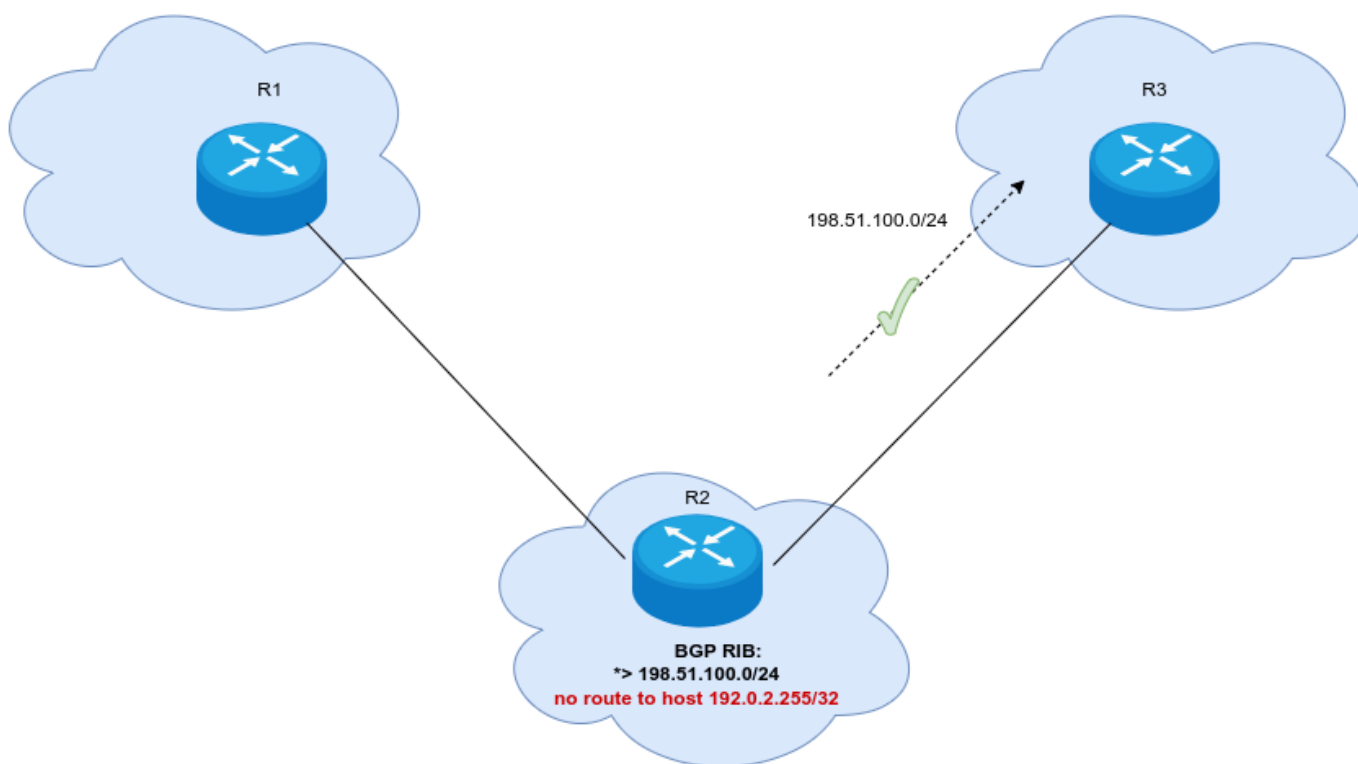
```

route-map CONDITION
  rule 1
    match ip address 192.0.2.255/32
  exit
exit
route-map ADVERTISE
  rule 1
    match ip address 198.51.100.0/24
  exit
exit
router bgp 65540
  neighbor R3
    description "To R3"
    address-family ipv4 unicast
      advertise-map ADVERTISE exist-map CONDITION
    enable
  exit

```

Условие not EXIST-MAP:

- Если R2 содержит в BGP RIB маршрут 192.0.2.255/32, то анонсирование маршрута 198.51.100.0/24 соседу R3 не происходит;
- Если R2 не содержит в BGP RIB маршрут 192.0.2.255/32, то R2 анонсирует в сторону R3 маршрут 198.51.100.0/24 (пример на рисунке ниже).

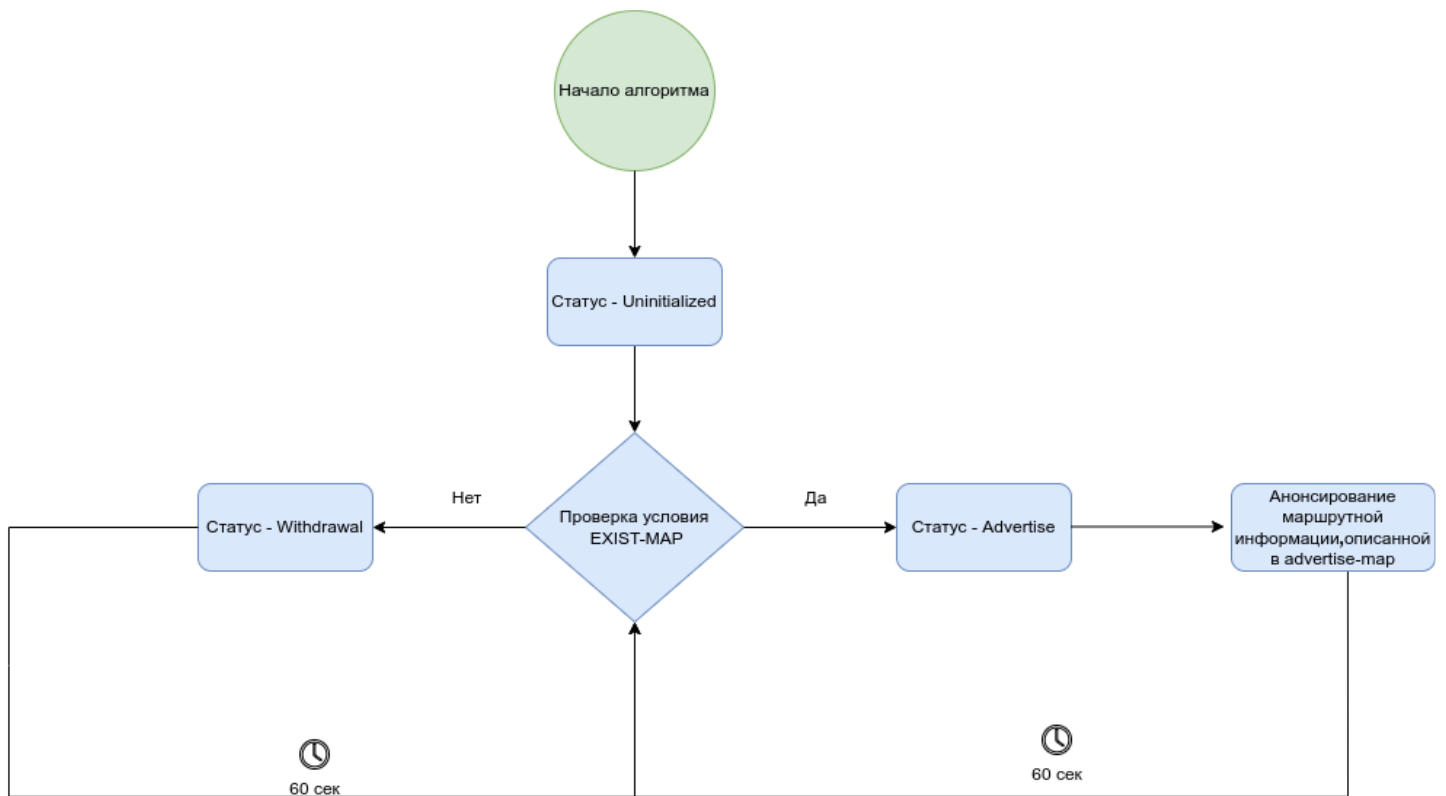


```

route-map CONDITION
  rule 1
    match ip address 192.0.2.255/32
  exit
exit
route-map ADVERTISE
  rule 1
    match ip address 198.51.100.0/24
  exit
exit
router bgp 65540
  neighbor R3
    description "To R3"
    address-family ipv4 unicast
      advertise-map ADVERTISE not exist-map CONDITION
    enable
  exit

```

Ниже приведена диаграмма состояний для условия EXIST-MAP:



После активации функции Conditional advertisement находится в состоянии «Uninitialized». На этом этапе анонсируется вся разрешенная маршрутная информация, происходит инициализация планировщика для дальнейшей работы. Время нахождения в этом состоянии – 60 секунд:

```
vevt# sh bgp neighbors
BGP neighbor is 192.0.2.2
  BGP state: Established
  Type: Static neighbor
  Neighbor address: 192.0.2.2
  Neighbor AS: 202766
  Neighbor ID: 192.0.2.2
  Neighbor caps: refresh enhanced-refresh restart-aware AS4
  Session: external AS4
  Source address: 192.0.2.1
  Weight: 0
  Hold timer: 136/180
  Keepalive timer: 35/60
  Address family ipv4 unicast:
    Send-label: No
    Default originate: No
    Default information originate: No
    Incoming route-map: IN
    Outgoing route-map: OUT
    Advertise-map: ADVERTISE
    Condition-map: CONDITION
    Conditional advertisement status: Uninitialized <-----
  Uptime: 12 s
```

Далее планировщик проверяет условие EXIST-MAP для соответствующей condition-map. Если условие истинно, происходит анонсирование (обновление) маршрутной информации в соответствии с правилами, заданными в advertise-map. Состояние статуса меняется на «Advertise». Время нахождения в этом состоянии – 60 секунд:

```
vevt# sh bgp neighbors
BGP neighbor is 192.0.2.2
  BGP state:                Established
  Type:                    Static neighbor
  Neighbor address:        192.0.2.2
  Neighbor AS:             202766
  Neighbor ID:             192.0.2.2
  Neighbor caps:           refresh enhanced-refresh restart-aware AS4
  Session:                 external AS4
  Source address:          192.0.2.1
  Weight:                  0
  Hold timer:              136/180
  Keepalive timer:         41/60
  Address family ipv4 unicast:
    Send-label:            No
    Default originate:     No
    Default information originate: No
    Incoming route-map:    IN
    Outgoing route-map:    OUT
    Advertise-map:         ADVERTISE
    Condition-map:         CONDITION
    Conditional advertisement status: Advertise    <----
  Uptime:                  1119 s
```

Если условие EXIST-MAP для соответствующей condition-map не выполняется, происходит отзыв маршрутной информации, описанной в соответствующей advertise-map. Состояние статуса меняется на «Withdrawal». Время нахождения в этой стадии – 60 секунд:

```
vevt# sh bgp neighbors
BGP neighbor is 192.0.2.2
  BGP state:                Established
  Type:                    Static neighbor
  Neighbor address:        192.0.2.2
  Neighbor AS:             202766
  Neighbor ID:             192.0.2.2
  Neighbor caps:           refresh enhanced-refresh restart-aware AS4
  Session:                 external AS4
  Source address:          192.0.2.1
  Weight:                  0
  Hold timer:              136/180
  Keepalive timer:         41/60
  Address family ipv4 unicast:
    Send-label:            No
    Default originate:     No
    Default information originate: No
    Incoming route-map:    IN
    Outgoing route-map:    OUT
    Advertise-map:         ADVERTISE
    Condition-map:         CONDITION
    Conditional advertisement status: Withdrawal    <----
  Uptime:                  1119 s
```

- ⚠** Порядок выполнения политик фильтрации маршрутной информации:
1. Выполняется политика, заданная при редистрибуции маршрутов (AF_POLICY_OUT);
 2. Применяется advertise-map, описанная в Conditional advertisement (advertise-map ADVERTISE ..);
 3. Обрабатывается политика фильтрации исходящей маршрутной информации (route-map OUT out).

```

route-map ADVERTISE
  rule 1
    match ip address 10.100.0.255/32
    action set local-preference 101
    action set metric bgp 78
  exit
exit
route-map OUT
  rule 1
    action set local-preference 200
  exit
exit
route-map CONDITION
  rule 1
    match ip address 10.100.0.255/32
  exit
exit
route-map AF_POLICY_OUT
  rule 1
    match ip address 10.100.0.255/32
    action set community 65:65
  exit
exit
router bgp 64512
  neighbor 192.0.2.2
    remote-as 64512
    address-family ipv4 unicast
      route-map OUT out <----- 3
      advertise-map ADVERTISE exist-map CONDITION <----- 2
    enable
  exit
  enable
exit
address-family ipv4 unicast
  redistribute static route-map AF_POLICY_OUT <----- 1
exit
enable
exit

```

Вывод атрибутов BGP маршрута после прохождения всех политик:

```

show bgp ipv4 unicast 10.100.0.255/32
Administrative Distance: 170
Type: unicast
Origin: Incomplete
AS path: --
Next Hop: 192.168.1.1

```

```

Output Label: --
Input Label: imp-null
Local Preference: 200
MED: 78
Cluster List: --
Community: 65:65
EXT Community: --
Weight: --

```

Алгоритм настройки

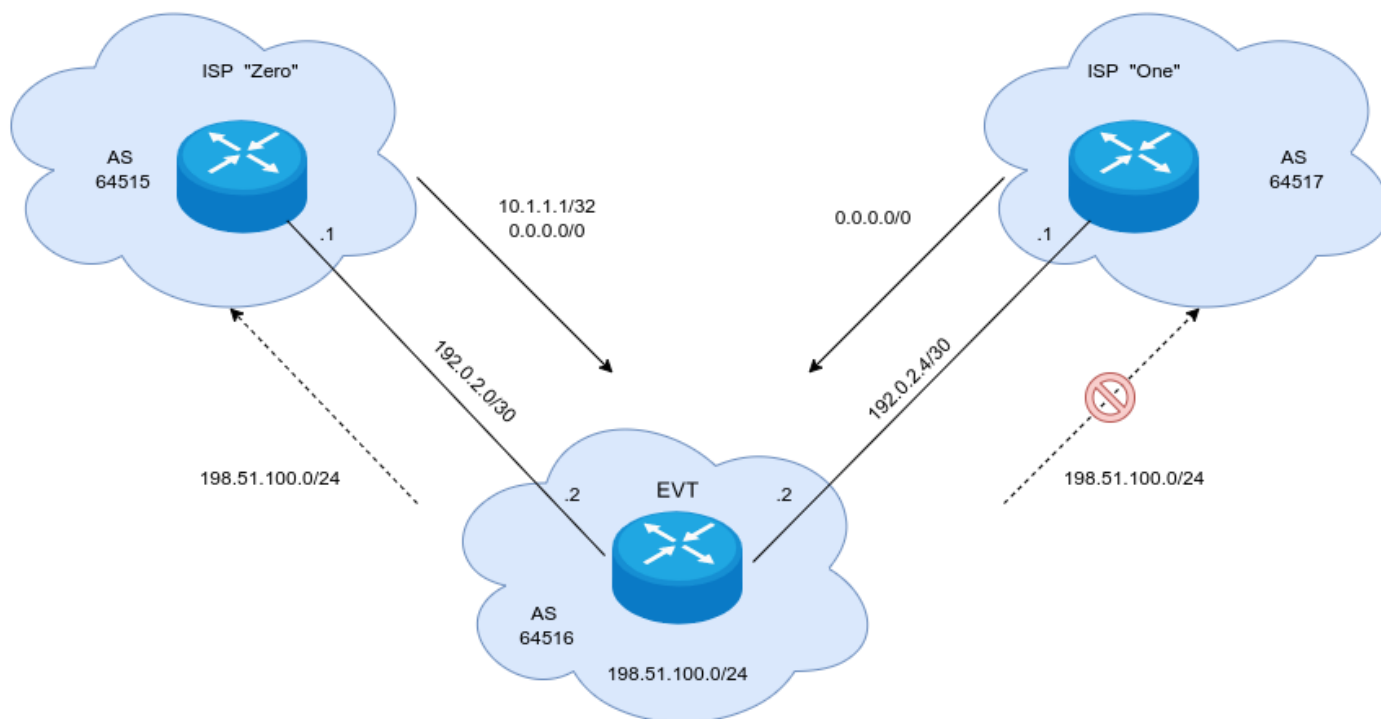
Шаг	Описание	Команда	Ключ
1	Настроить протокол BGP (см. раздел Настройка BGP).		
2	Создать advertise-map, описав в нем список подсетей для дальнейшего анонсирования.	evt(config)# route-map <ADVERTISE>	<ADVERTISE> – имя конфигурируемых правил маршрутизации, задаётся строкой до 31 символа.
3	Создать condition-map, описав в нем список подсетей по которым будет осуществляться проверка.	evt(config)# route-map <CONDITION>	<CONDITION> – имя конфигурируемых правил маршрутизации, задаётся строкой до 31 символа.
4	В контексте настройки address-family заданного BGP соседа указать условие и созданные ранее маршрутные карты.	evt(config-bgp-neighbor-af)# advertise-map <ADVERTISE> {EXIST-MAP NOT-EXIST-MAP} <CONDITION>	<ADVERTISE> – имя конфигурируемых правил маршрутизации, задаётся строкой до 31 символа. <CONDITION> – имя конфигурируемых правил маршрутизации, задаётся строкой до 31 символа. <EXIST-MAP> – условие проверки: если маршруты, описанные в condition-map, присутствуют в BGP RIB, то происходит анонсирование маршрутов, описанных в advertise-map. <NOT-EXIST-MAP> – условие проверки: если маршруты, описанные в condition-map, отсутствуют в BGP RIB, то происходит анонсирование маршрутов, описанных в advertise-map.

Пример настройки

Задача:

EVT/EVS получает маршрут по умолчанию от двух провайдеров – ISP «Zero» и «ISP One». Дополнительно ISP «Zero» анонсирует маршрут 10.1.1.1/32, наличие которого в BGP RIB в дальнейшем и будет отслеживаться.

Необходимо в случае присутствия маршрута 10.1.1.1/32 в BGP RIB анонсировать маршрут 198.51.100.0/24 провайдеру ISP «Zero», если маршрут 10.1.1.1/32 отсутствует в BGP RIB – анонсировать 198.51.100.0/24 провайдеру ISP «One».



Решение:

Сконфигурируем необходимые сетевые интерфейсы на каждом устройстве в сети:

```
ISP-ZERO(config)# interface gigabitethernet 1/0/1
ISP-ZERO(config-if-gi)# ip firewall disable
ISP-ZERO(config-if-gi)# ip address 192.0.2.1/30
ISP-ZERO(config-if-gi)# do commit
ISP-ZERO(config-if-gi)# do confirm
```

```
evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# ip firewall disable
evt(config-if-gi)# description "FROM ISP-ZERO"
evt(config-if-gi)# ip address 192.0.2.2/30
evt(config-if-gi)# exit
evt(config)# interface gigabitethernet 1/0/2
evt(config-if-gi)# ip firewall disable
evt(config-if-gi)# ip address 192.0.2.5/30
evt(config-if-gi)# description "TO ISP-ONE"
evt(config-if-gi)# exit
evt(config)# do commit
evt(config)# do confirm
```

```
ISP-ONE(config)# interface gigabitethernet 1/0/1
ISP-ONE(config-if-gi)# ip firewall disable
ISP-ONE(config-if-gi)# ip address 192.0.2.6/30
ISP-ONE(config-if-gi)# do commit
ISP-ONE(config-if-gi)# do confirm
```

Произведем настройку BGP:

```

ISP-ZERO(config)# ip route 10.1.1.1/32 blackhole
ISP-ZERO(config)# ip route 0.0.0.0/0 blackhole
ISP-ZERO(config)# route-map OUT
ISP-ZERO(config-route-map)# rule 1
ISP-ZERO(config-route-map-rule)# exit
ISP-ZERO(config-route-map)# exit
ISP-ZERO(config)# router bgp 64515
ISP-ZERO(config-bgp)# neighbor 192.0.2.2
ISP-ZERO(config-bgp-neighbor)# remote-as 64516
ISP-ZERO(config-bgp-neighbor)# enable
ISP-ZERO(config-bgp-neighbor)# address-family ipv4 unicast
ISP-ZERO(config-bgp-neighbor-af)# route-map OUT out
ISP-ZERO(config-bgp-neighbor-af)# enable
ISP-ZERO(config-bgp-neighbor-af)# exit
ISP-ZERO(config-bgp-neighbor)# exit
ISP-ZERO(config-bgp)# enable
ISP-ZERO(config-bgp)# address-family ipv4 unicast
ISP-ZERO(config-bgp-af)# redistribute static
ISP-ZERO(config-bgp-af)# do commit
ISP-ZERO(config-bgp-af)# do confirm

```

```

evt(config)# route-map OUT
evt(config-route-map)# rule 1
evt(config-route-map-rule)# match ip address 198.51.100.0/24
evt(config-route-map-rule)# exit
evt(config-route-map)# exit
evt(config)# router bgp 64516
evt(config-bgp)# neighbor 192.0.2.1
evt(config-bgp-neighbor)# remote-as 64515
evt(config-bgp-neighbor)# address-family ipv4 unicast
evt(config-bgp-neighbor-af)# route-map OUT out
evt(config-bgp-neighbor-af)# enable
evt(config-bgp-neighbor-af)# exit
evt(config-bgp-neighbor)# enable
evt(config-bgp-neighbor)# exit
evt(config-bgp)# neighbor 192.0.2.6
evt(config-bgp-neighbor)# remote-as 64517
evt(config-bgp-neighbor)# address-family ipv4 unicast
evt(config-bgp-neighbor-af)# enable
evt(config-bgp-neighbor-af)# route-map OUT out
evt(config-bgp-neighbor-af)# exit
evt(config-bgp-neighbor)# enable
evt(config-bgp-neighbor)# exit
evt(config-bgp)# enable
evt(config-bgp)# do commit
evt(config-bgp)# do confirm

```

```

ISP-ONE(config)# ip route 0.0.0.0/0 blackhole
ISP-ONE(config)# route-map OUT
ISP-ONE(config-route-map)# rule 1
ISP-ONE(config-route-map-rule)# exit
ISP-ONE(config-route-map)# exit
ISP-ONE(config)# router bgp 64517
ISP-ONE(config-bgp)# neighbor 192.0.2.5

```

```
ISP-ONE(config-bgp-neighbor)# address-family ipv4 unicast
ISP-ONE(config-bgp-neighbor-af)# route-map OUT out
ISP-ONE(config-bgp-neighbor-af)# enable
ISP-ONE(config-bgp-neighbor-af)# exit
ISP-ONE(config-bgp-neighbor)# remote-as 64516
ISP-ONE(config-bgp-neighbor)# enable
ISP-ONE(config-bgp-neighbor)# exit
ISP-ONE(config-bgp)# enable
ISP-ONE(config-bgp)# address-family ipv4 unicast
ISP-ONE(config-bgp-af)# redistribute static
ISP-ONE(config-bgp-af)# do commit
ISP-ONE(config-bgp-af)# do confirm
```

Опишем advertise и condition maps на evt:

```
evt(config)# ip route 198.51.100.0/24 blackhole
evt(config)# route-map CONDITION
evt(config-route-map)# rule 1
evt(config-route-map-rule)# match ip address 10.1.1.1/32
evt(config-route-map-rule)# exit
evt(config-route-map)# exit
evt(config)# route-map ADVERTISE
evt(config-route-map)# rule 1
evt(config-route-map-rule)# match ip address 198.51.100.0/24
evt(config-route-map-rule)# exit
evt(config-route-map)# exit
evt(config)# router bgp 64516
evt(config-bgp)# address-family ipv4 unicast
evt(config-bgp-af)# network 198.51.100.0/24
evt(config-bgp-af)# do commit
evt(config-bgp-af)# do confirm
```

Активируем функцию Conditional advertisement, применив ранее созданные маршрутные карты:

```
evt(config)# router bgp 64516
evt(config-bgp)# neighbor 192.0.2.6
evt(config-bgp-neighbor)# address-family ipv4 unicast
evt(config-bgp-neighbor-af)# advertise-map ADVERTISE not exist-map CONDITION
evt(config-bgp-neighbor-af)# do commit
evt(config-bgp-neighbor-af)# do confirm
```


Проверяем наличие маршрута 10.1.1.1/32 в BGP RIB:

```

evt# sh bgp ipv4 unicast 10.1.1.1/32
10.1.1.1/32 via 192.0.2.1 on gi1/0/1 [bgp64516 07:07:59] (64515?)
  Administrative Distance: 170
  Type: unicast
  Origin: Incomplete
  AS path: 64515
  Next Hop: 192.0.2.1
  Output Label: --
  Input Label: --
  Local Preference: 100
  MED: --
  Cluster List: --
  Community: --
  EXT Community: --
  Weight: 0
  Valid, Best

```

Проверяем статус conditional advertisement и отсутствие анонса 198.51.100.0/24 провайдеру ISP "One":

```

evt# sh bgp ipv4 unicast neighbor 192.0.2.6 advertise-routes

evt# sh bgp neighbors 192.0.2.6
BGP neighbor is 192.0.2.6
  BGP state: Established
  Type: Static neighbor
  Neighbor address: 192.0.2.6
  Neighbor AS: 64517
  Neighbor ID: 192.0.2.6
  Neighbor caps: refresh enhanced-refresh restart-aware AS4
  Session: external AS4
  Source address: 192.0.2.5
  Weight: 0
  Hold timer: 99/180
  Keepalive timer: 4/60
  RR client: No
  Address family ipv4 unicast:
    Send-label: No
    Default originate: No
    Default information originate: No
    Outgoing route-map: OUT
    Advertise-map: ADVERTISE
    Condition-map: CONDITION
    Conditional advertisement status: Withdrawal
    Preference: 170
    Remove private AS: No
    Next-hop self: No
    Next-hop unchanged: No
  Uptime: 1300 s

```

Настройка завершена.

Быстрая деактивация пиринговых сессий

В случае когда возникновения проблем между соседями BGP, по умолчанию BGP ожидает 180 секунд (3 таймера кеераливе) для того чтобы разорвать соседство и отозвать все маршруты полученные от неактивного соседа. Для обхода данной проблемы существуют методы, которые помогают быстрее обнаружить проблемы в работе сети и произвести отключение соседа, улучшая время реакции на изменения смежности с соседями BGP. Рассмотрим существующие реализации этих методов.

Метод на основе протокола BFD

BFD (Bidirectional Forwarding Detection) — протокол для быстрого обнаружения проблем на канальном уровне. В текущей реализации для его работы необходима настройка с обеих сторон (на каждом BGP-пире).

По умолчанию BFD-сессия устанавливается в следующем режиме:

Протокол	Режим
eBGP	single-hop
eBGP multi-hop	multi-hop
iBGP	multi-hop

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Настроить протокол BGP (см. раздел Настройка BGP).		
2	Включить поддержку протокола BFD в контексте настройки пира или пир-группы	evt(config-bgp-neighbor)# fall-over bfd	

Пример настройки

Задача:

Необходимо настроить eBGP между маршрутизаторами R1, R2 и включить протокол BFD.



Решение:

На R1 предварительно необходимо настроить интерфейс Gi1/0/1:

```
evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# ip firewall disable
evt(config-if-gi)# ip address 10.0.0.1/24
```

Следующим шагом на R1 настроим eBGP и включим BFD:

```
evt(config)# router bgp 100
evt(config-bgp)# neighbor 10.0.0.2
evt(config-bgp-neighbor)# remote-as 200
evt(config-bgp-neighbor)# update-source 10.0.0.1
evt(config-bgp-neighbor)# fall-over bfd
evt(config-bgp-neighbor)# enable
evt(config-bgp-neighbor)# exit
evt(config-bgp)# enable
evt(config-bgp)# exit
```

На R2 предварительно необходимо настроить интерфейс Gi1/0/1:

```
evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# ip firewall disable
evt(config-if-gi)# ip address 10.0.0.2/24
```

Далее на R2 настроим eBGP и включим BFD:

```
evt(config)# router bgp 200
evt(config-bgp)# neighbor 10.0.0.1
evt(config-bgp-neighbor)# remote-as 100
evt(config-bgp-neighbor)# update-source 10.0.0.2
evt(config-bgp-neighbor)# fall-over bfd
evt(config-bgp-neighbor)# enable
evt(config-bgp-neighbor)# exit
evt(config-bgp)# enable
evt(config-bgp)# exit
```

Настройка завершена. Для просмотра оперативной информации можно использовать следующие команды:

```

evt# sh bgp neighbors
BGP neighbor is 10.0.0.2
  BGP state:                Established      <---- BGP сессия установлена
  Type:                     Static neighbor
  Neighbor address:         10.0.0.2
  Neighbor AS:              200
  Neighbor ID:              10.0.0.2
  Neighbor caps:            refresh enhanced-refresh restart-aware AS4
  Session:                  external AS4
  Source address:           10.0.0.1
  Weight:                   0
  Hold timer:               144/180
  Keepalive timer:          29/60
  Uptime (d,h:m:s):         00,00:00:20
  BFD address:              10.0.0.2
  BFD state:                Up              <---- Статус протокола BFD
  BFD interval:             0.300 s
  BFD timeout:              1.500 s

evtv# sh bfd neighbors 10.0.0.2
Neighbor address:           10.0.0.2
Local address:              10.0.0.1
Interface:                  gil/0/1
Remote discriminator:       889907056
Local discriminator:        924658435
State:                      Up
Session type:               Control
Session mode:               Single-hop
Local diagnostic code:      No Diagnostic
Remote diagnostic code:     No Diagnostic
Minimal Tx Interval:        300 ms
Minimal Rx Interval:        300 ms
Multiplier:                 5
Actual Tx Interval:         300 ms
Actual Detection Interval:   1500 ms
Number of transmitted packets: 257
Number of received packets: 156
Uptime (d,h:m:s):           00,00:00:38
Client:                     BGP
Last received packet:
  Desired Min Tx Interval:   200 ms
  Required Min Rx Interval:  200 ms
  Multiplier:                5

```

Метод на основе Fast Peer Deactivation (Fall-over)

BGP Fast Peer Deactivation – это метод оптимизации конвергенции BGP, при котором соседство BGP разрывается, как только указанный маршрут (или более/менее специфичный) к соседу удаляется из таблицы маршрутизации. Механизм реализован с совместным использованием маршрутных карт (route-map).

- ❗ Если правило route-map будет пустым, то под правило будет попадать любой доступный маршрут до соседа в таблице маршрутизации.

- ❗ Функционал поддержан для IPv4 (AFI -1 , SAFI -1), IPv6 (AFI -2 , SAFI -1) маршрутов. В route-map поддерживаются все значения команды **match**. Команды **action set** игнорируются. Реализована поддержка как для GRT, так и в VRF.

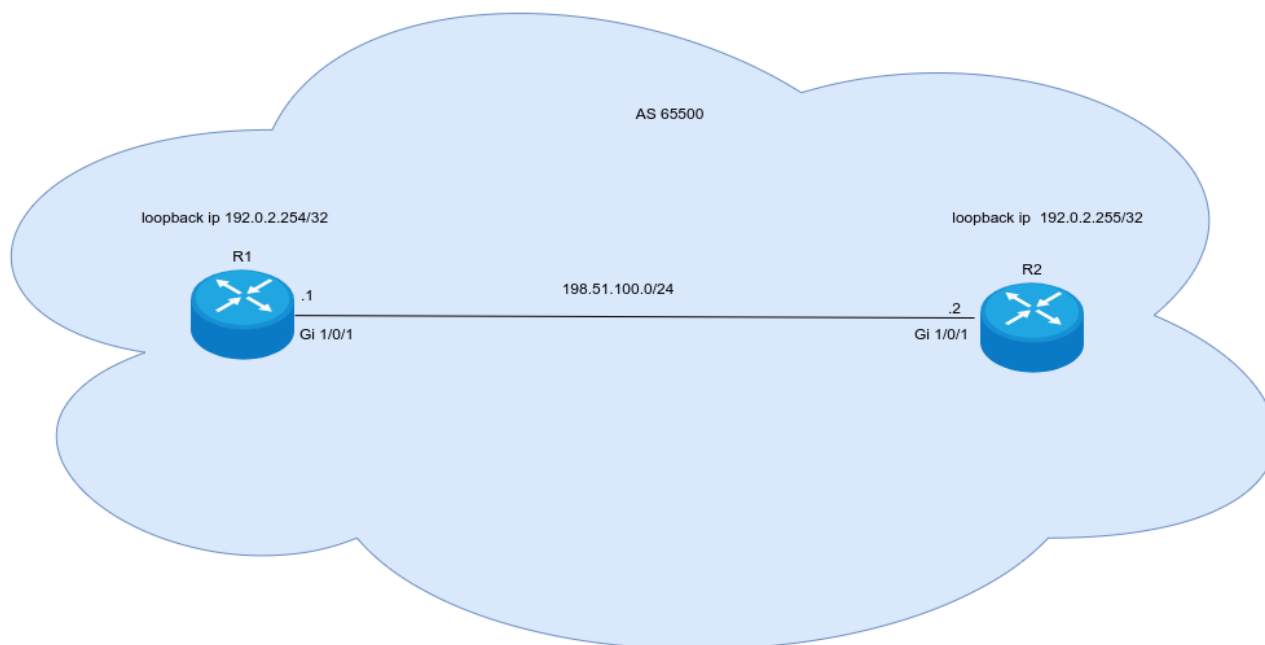
Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Настроить протокол BGP (см. раздел Настройка BGP).		
2	Описать в маршрутной карте подсеть, наличие которой будет отслеживаться в таблице маршрутизации (см. раздел Настройка Route-map).		
3	Активировать функционал, привязав маршрутную карту в соответствующему пиру или пир-группе.	evt(config-bgp-neighbor)# fall-over route-map <NAME>	<NAME> – имя маршрутной карты, задается строкой до 31 символа.

Пример настройки

Задача:

Настроить механизм Fast Peer Deactivation между iBGP пирами R1 и R2.



Решение:

Предварительно настроим связность между маршрутизаторами в схеме:

R1

```
R1(config)# interface gigabitethernet 1/0/1
R1(config-if-gi)# ip firewall disable
R1(config-if-gi)# ip address 198.51.100.1/24
```

R2

```
R2(config)# interface gigabitethernet 1/0/1
R2(config-if-gi)# ip firewall disable
R2(config-if-gi)# ip address 198.51.100.2/24
```

На каждом устройстве настроим протокол OSPF и анонсируем адреса loopback-интерфейсов:

R1

```
R1(config)# router ospf 1
R1(config-ospf)# area 0.0.0.0
R1(config-ospf-area)# enable
R1(config-ospf-area)# exit
R1(config-ospf)# enable
R1(config-ospf)# exit
R1(config)# interface loopback 1
R1(config-if-loopback)# ip ospf instance 1
R1(config-if-loopback)# ip ospf
R1(config-if-loopback)# exit
R1(config)# interface gigabitethernet 1/0/1
R1(config-if-gi)# ip ospf instance 1
R1(config-if-gi)# ip ospf
```

R2

```
R2(config)# router ospf 1
R2(config-ospf)# area 0.0.0.0
R2(config-ospf-area)# enable
R2(config-ospf-area)# exit
R2(config-ospf)# enable
R2(config-ospf)# exit
R2(config)# interface loopback 1
R2(config-if-loopback)# ip address 192.0.2.255/32
R2(config-if-loopback)# ip ospf instance 1
R2(config-if-loopback)# ip ospf
R2(config-if-loopback)# exit
R2(config)# interface gigabitethernet 1/0/1
R2(config-if-gi)# ip ospf instance 1
R2(config-if-gi)# ip ospf
```

Настроим протокол BGP на обоих маршрутизаторах:

R1

```
R1(config)# router bgp 65500
R1(config-bgp)# neighbor 192.0.2.255
R1(config-bgp-neighbor)# remote-as 65500
R1(config-bgp-neighbor)# update-source loopback 1
R1(config-bgp-neighbor)# enable
R1(config-bgp-neighbor)# exit
R1(config-bgp)# enable
```

```

R2(config)# router bgp 65500
R2(config-bgp)# neighbor 192.0.2.254
R2(config-bgp-neighbor)# remote-as 65500
R2(config-bgp-neighbor)# update-source loopback 1
R2(config-bgp-neighbor)# enable
R2(config-bgp-neighbor)# exit
R2(config-bgp)# enable

```

Создадим маршрутную карту, в которой опишем адрес BGP-пира для дальнейшего отслеживания с помощью функционала Fast Peer Deactivation:

R1

```

R1(config)# route-map Failover
R1(config-route-map)# rule 1
R1(config-route-map-rule)# match ip address 192.0.2.255/32
R1(config-route-map-rule)# exit
R1(config-route-map)# exit

```

R2

```

R2(config)# route-map Failover
R2(config-route-map)# rule 1
R2(config-route-map-rule)# match ip address 192.0.2.254/32

```

Привяжем созданные маршрутные карты в контексте настройки BGP-пира:

R1

```

R1(config)# router bgp 65500
R1(config-bgp)# neighbor 192.0.2.255
R1(config-bgp-neighbor)# fall-over route-map Failover

```

R2

```

R2(config)# router bgp 65500
R2(config-bgp)# neighbor 192.0.2.254
R2(config-bgp-neighbor)# fall-over route-map Failover

```


Для просмотра оперативного состояния можно воспользоваться следующей командой:

```
R2# sh bgp neighbors
BGP neighbor is 192.0.2.254
  BGP state:                Established
  Type:                     Static neighbor
  Neighbor address:         192.0.2.254
  Neighbor AS:              65500
  Neighbor ID:              192.0.2.254
  Neighbor caps:            refresh enhanced-refresh restart-aware AS4
  Session:                  internal multihop AS4
  Source address:           192.0.2.255
  Weight:                   0
  Hold timer:               164/180
  Keepalive timer:          23/60
  Uptime:                   437 s
  Fall-over route-map:      Failover          <---- Функционал активирован

R2# sh bgp neighbors 192.0.2.254
BGP neighbor is 192.0.2.254
  BGP state:                Down
  Type:                     Static neighbor
  Neighbor address:         192.0.2.254
  Neighbor AS:              65500
  Fall-over route-map:      Failover
  Last error:               Error: Fall over route-map  <---- Сессия BGP была
разорвана из-за отработавшего механизма Fast Peer Deactivation
```

Настройка завершена.

Настройка BFD

BFD (Bidirectional Forwarding Detection) — это протокол, работающий поверх других протоколов и позволяющий сократить время обнаружения проблемы до 50 мс. BFD является двусторонним протоколом, т. е. требует настройки обоих маршрутизаторов (оба маршрутизатора генерируют BFD-пакеты и отвечают друг другу).

По умолчанию сессия устанавливается в следующем режиме:

Протокол	Режим
iBGP	multi-hop
eBGP	single-hop
eBGP multi-hop	multi-hop
OSPF	single-hop
Static route	single-hop
RIP	single-hop

Для изменения поведения (режима) необходимо вручную переопределить параметры сессии, указав необходимый режим. Рассмотрим на примере.

Допустим, мы установили eBGP-соседство и включили для него BFD:

```

evt# show running-config routing bgp
router bgp 65516
  neighbor 10.100.0.2
    remote-as 65515
    update-source 10.100.0.1
    fall-over bfd
    enable
  exit
enable
exit

evt# show bfd neighbors 10.100.0.2
Neighbor address:      10.100.0.2
Local address:         10.100.0.1
Interface:             --
Remote discriminator:  3751534121
Local discriminator:   1670865501
State:                 Up
Session type:          Control
Session mode:          Single-hop
Local diagnostic code:  No Diagnostic
Remote diagnostic code: No Diagnostic
Minimal Tx Interval:   300 ms
Minimal Rx Interval:   300 ms
Multiplier:           5
Actual Tx Interval:    300 ms
Actual Detection Interval: 1500 ms
Number of transmitted packets: 1149
Number of received packets: 1153
Uptime:                2m
Client:                BGP
Last received packet:
  Desired Min Tx Interval: 300 ms
  Required Min Rx Interval: 300 ms
  Multiplier:             5

```

Как видно, по умолчанию BFD установился в режиме single-hop. Переключим режим в multi-hop:

```

evt(config)# ip bfd neighbor 10.100.0.2 local-address 10.100.0.1 multihop
evt(config)# do commit
evt(config)# do confirm

```

```

evt-200# sh bfd neighbors 10.100.0.2
Neighbor address:      10.100.0.2
Local address:         10.100.0.1
Interface:             --
Remote discriminator:   3751534121
Local discriminator:    1670865501
State:                 Up
Session type:           Control
Session mode:           Multi-hop
Local diagnostic code:   No Diagnostic
Remote diagnostic code:  No Diagnostic
Minimal Tx Interval:    300 ms
Minimal Rx Interval:    300 ms
Multiplier:            5
Actual Tx Interval:     300 ms
Actual Detection Interval: 1500 ms
Number of transmitted packets: 9
Number of received packets: 11
Uptime:                2m
Client:                 BGP
Last received packet:
  Desired Min Tx Interval: 300 ms
  Required Min Rx Interval: 300 ms
  Multiplier:             5

```

Настройка таймеров

- ✔ Значение таймеров индивидуально для каждой сети и во многом зависит от ее параметров. В случае частого флапинга BFD рекомендуется увеличить значение таймеров.

Таймеры, вне зависимости от режима работы протокола (single или multi-hop mode), могут быть настроены в контексте глобальной конфигурации или на определенных интерфейсах. Настройка на интерфейсах имеет наибольший приоритет.

```

evt(config)# ip bfd min-tx-interval 1000
evt(config)# ip bfd min-rx-interval 1000
evt(config)# do commit

evt# sh ip bfd
Minimum RX interval: 1000 ms
Minimum TX interval: 1000 ms
Idle TX interval:    1000 ms
Multiplier:         5 packets
Passive:             No

```

После того как BFD-сессия установлена, каждая сторона индивидуально вычисляет свои Tx Interval и Detection Interval. Tx Interval выбирается как наибольшее значение из локального Tx Interval и удаленного RX Interval. Detection Interval вычисляется по следующей формуле: $\text{Detection Interval} = \text{remoteMultiplier} * \text{MAX}(\text{RxLocal} || \text{TxRemote})$, где remoteMultiplier – значение Multiplier удаленной стороны, RxLocal – локальный Tx Interval, TxRemote – Tx Interval удаленной стороны.

Локально настроенные таймеры, таймеры удаленной стороны, а также вычисленные таймеры можно посмотреть следующим образом:

```

evt-200# sh bfd neighbors 10.100.0.2
Neighbor address:      10.100.0.2
Local address:         10.100.0.1
Interface:             --
Remote discriminator:  3751534121
Local discriminator:   1670865501
State:                 Up
Session type:          Control
Session mode:          Multi-hop
Local diagnostic code:  No Diagnostic
Remote diagnostic code: No Diagnostic
Minimal Tx Interval:   300 ms      <----- Локальный Tx Interval
Minimal Rx Interval:   300 ms      <----- Локальный Rx Interval
Multiplier:           5           <----- Локальный Multiplier
Actual Tx Interval:    300 ms      <----- Вычисленный Tx Interval
Actual Detection Interval: 1500 ms  <----- Вычисленный Detection Interval
Number of transmitted packets: 21781
Number of received packets: 21804
Uptime:               1d21h54m
Client:               BGP
Last received packet:
  Desired Min Tx Interval: 300 ms      <-----
  Required Min Rx Interval: 300 ms      <----- Таймеры удаленной стороны
  Multiplier:             5           <-----

```

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Активировать BFD для протокола OSPF на интерфейсе.	evt(config-if-gi)# ip ospf bfd-enable	
2	Активировать BFD для neighbor протокола BGP.	evt(config-bgp-neighbor)# fall-over bfd	
3	Активировать BFD для протокола RIP на интерфейсе.	evt(config-if-gi)# ip rip bfd-enable	
4	Задать интервал, по истечении которого происходит отправка BFD-сообщения соседу. Глобально (не обязательно).	evt(config)# ip bfd idle-tx-interval <TIMEOUT>	<TIMEOUT> – интервал, по истечении которого происходит отправка BFD-пакета, принимает значение в миллисекундах в диапазоне [300..65535]. По умолчанию: 1 секунда.
5	Включить логирование изменений состояния BFD-протокола (не обязательно).	evt(config)# ip bfd log-adjacency-changes	

Шаг	Описание	Команда	Ключи
6	Задать минимальный интервал, по истечении которого сосед должен сгенерировать BFD-сообщение. Глобально (не обязательно).	evt(config)# ip bfd min-rx-interval <TIMEOUT>	<TIMEOUT> – интервал, по истечении которого должна происходить отправка BFD-сообщения соседом, принимает значение в миллисекундах в диапазоне [300..65535]. По умолчанию 300 миллисекунд.
7	Задать минимальный интервал, по истечении которого происходит отправка BFD-сообщения соседу. Глобально (не обязательно).	evt(config)# ip bfd min-tx-interval <TIMEOUT>	<TIMEOUT> – интервал, по истечении которого должна происходить отправка BFD-сообщения соседом, принимает значение в миллисекундах в диапазоне [300..65535]. По умолчанию 300 миллисекунд.
8	Задать число пропущенных пакетов, после достижения которого BFD-сосед считается недоступным. Глобально.	evt(config)# ip bfd multiplier <COUNT>	<COUNT> – число пропущенных пакетов, после достижения которого сосед считается недоступным, принимает значение в диапазоне [1..100]. По умолчанию: 5.
9	Запустить работу механизма BFD с определенным IP-адресом.	evt(config)# ip bfd neighbor <ADDR> [{ interface <IF> tunnel <TUN> }] [local-address <ADDR> [multihop]] [vrf <VRF>]	<ADDR> – IP-адрес шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IF> – интерфейс или группы интерфейсов; <TUN> – тип и номер туннеля; <VRF> – имя экземпляра VRF, задается строкой до 31 символа; multihop – ключ для установки TTL=255, для работы механизма BFD через маршрутизируемую сеть.

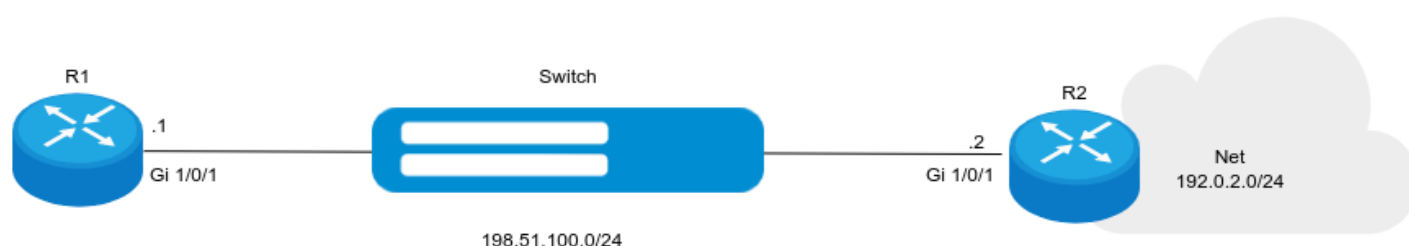
Шаг	Описание	Команда	Ключи
10	Перевести BFD-сессию в пассивный режим, то есть BFD-сообщения не будут отправляться до тех пор, пока не будут получены сообщения от BFD-соседа. Глобально (не обязательно).	evt(config)# ip bfd passive	
11	Задать интервал, по истечении которого происходит отправка BFD-сообщения соседу. На интерфейсе (не обязательно).	evt(config-if-gi)# ip bfd idle-tx-interval <TIMEOUT>	<TIMEOUT> – интервал, по истечении которого происходит отправка BFD-пакета, принимает значение в миллисекундах в диапазоне [300..65535]. По умолчанию: 1 секунда.
12	Задать минимальный интервал, по истечении которого сосед должен сгенерировать BFD-сообщение. На интерфейсе (не обязательно).	evt(config-if-gi)# ip bfd min-rx-interval <TIMEOUT>	<TIMEOUT> – интервал, по истечении которого должна происходить отправка BFD-сообщения соседом, принимает значение в миллисекундах в диапазоне [300..65535]. По умолчанию 300 миллисекунд.
13	Задать минимальный интервал, по истечении которого происходит отправка BFD-сообщения соседу. На интерфейсе (не обязательно).	evt(config-if-gi)# ip bfd min-tx-interval <TIMEOUT>	<TIMEOUT> – интервал, по истечении которого должна происходить отправка BFD-сообщения соседом, принимает значение в миллисекундах в диапазоне [300..65535]. По умолчанию 300 миллисекунд.
14	Задать число пропущенных пакетов, после достижения которого BFD-сосед считается недоступным. На интерфейсе (не обязательно).	evt(config-if-gi)# ip bfd multiplier <COUNT>	<COUNT> – число пропущенных пакетов, после достижения которого сосед считается недоступным, принимает значение в диапазоне [1..100]. По умолчанию: 5.
15	Перевести BFD-сессию в пассивный режим, то есть BFD-сообщения не будут отправляться до тех пор, пока не будут получены сообщения от BFD-соседа. На интерфейсе (не обязательно).	evt(config-if-gi)# ip bfd passive	

Шаг	Описание	Команда	Ключи
16	При активизации работы протока BFD на интерфейсе с включенным firewall, необходимо разрешить работу протокола UDP порт назначения – 3784 из зоны сконфигурированной на интерфейсе в зону self. Как создать необходимое правило описано в разделе Конфигурирование Firewall .		

Пример настройки

Задача:

Необходимо настроить протокол BFD для статического маршрута на маршрутизаторе R1.



Решение:

Предварительно необходимо настроить интерфейс Gi1/0/1 на R1 и R2:

R1

```
R1(config)# interface gigabitethernet 1/0/1
R1(config-if-gi)# ip firewall disable
R1(config-if-gi)# ip address 198.51.100.1/24
```

R2

```
R2(config)# interface gigabitethernet 1/0/1
R2(config-if-gi)# ip firewall disable
R2(config-if-gi)# ip address 198.51.100.2/24
```

На R1 настроим статический маршрут и привяжем к нему функционал BFD:

R1

```
R1(config)# ip route 192.0.2.0/24 198.51.100.2 bfd
```

Для установки BFD-сессии на R2 также необходимо настроить соседа:

R2

```
R2(config)# ip bfd neighbor 198.51.100.1
```

Для вывода оперативной информации возможно использование следующих команд:

```
R1# sh bfd neighbors
Neighbor                               Discriminator State      Interface
-----
198.51.100.2                          2907010617    Up        gi1/0/1
R1# sh bfd neighbors 198.51.100.2
Neighbor address: 198.51.100.2
Local address:    198.51.100.1
Interface:        gi1/0/1
Remote discriminator: 2907010617
Local discriminator: 2856477782
State:            Up                <--- состояние протокола
Session type:     Control
Session mode:     Single-hop
Local diagnostic code: No Diagnostic
Remote diagnostic code: No Diagnostic
Minimal Tx Interval: 300 ms
Minimal Rx Interval: 300 ms
Multiplier:       5
Actual Tx Interval: 300 ms
Actual Detection Interval: 1500 ms
Number of transmitted packets: 1444
Number of received packets: 1402
Uptime (d,h:m:s): 00,00:03:39
Client:           STATIC            <---- сервис, который подписан на
отслеживание изменения состояния

R1# sh ip route 192.0.2.0/24
Codes: C - connected, S - static, R - RIP derived,
       O - OSPF derived, IA - OSPF inter area route,
       E1 - OSPF external type 1 route, E2 - OSPF external type 2 route
       B - BGP derived, D - DHCP derived, K - kernel route, V - VRRP route
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       H - NHRP, * - FIB route

S      * 192.0.2.0/24      [1/0]                via 198.51.100.2 on gi1/0/1      [static 16:22:27]

R1# sh bfd neighbors
Neighbor                               Discriminator State      Interface
-----
198.51.100.2                          2907010617    Up        gi1/0/1
R1# sh ip route 192.0.2.0/24
Codes: C - connected, S - static, R - RIP derived,
       O - OSPF derived, IA - OSPF inter area route,
       E1 - OSPF external type 1 route, E2 - OSPF external type 2 route
       B - BGP derived, D - DHCP derived, K - kernel route, V - VRRP route
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       H - NHRP, * - FIB route

S      * 192.0.2.0/24      [1/0]                via 198.51.100.2 on gi1/0/1      [static 16:22:27]
<---- маршрут присутствует в FIB
```

После того как BFD-сессия разрушилась, отслеживаемый маршрут удален из FIB:

```
R1# sh bfd neighbors
Neighbor                               Discriminator State      Interface
-----
```



```
198.51.100.2          2907010617      Down      gi1/0/1
```

```
R1# sh ip route 192.0.2.0/24
```

```
Codes: C - connected, S - static, R - RIP derived,
       O - OSPF derived, IA - OSPF inter area route,
       E1 - OSPF external type 1 route, E2 - OSPF external type 2 route
       B - BGP derived, D - DHCP derived, K - kernel route, V - VRRP route
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       H - NHRP, * - FIB route
```

```
R1#
```

Настройка завершена.

Конфигурацию необходимо производить на обоих устройствах. После переустановки сессии ее режим сменится на multi-hop:

Настройка политики маршрутизации PBR

Алгоритм настройки Route-map для BGP

Route-map могут служить фильтрами, позволяющими обрабатывать маршрутную информацию при приеме этой информации от соседа либо при ее передаче соседу. Обработка может включать в себя фильтрацию на основании различных признаков маршрута, а также установку атрибутов (MED, AS-PATH, community, LocalPreference и другое) на соответствующие маршруты.

Шаг	Описание	Команда	Ключи
1	Создать маршрутную карту для фильтрации и модификации IP-маршрутов.	evt(config)# route-map <NAME>	<NAME> – имя маршрутной карты, задается строкой до 31 символа.
2	Создать правило маршрутной карты.	evt(config-route-map)# rule <ORDER>	<ORDER> – номер правила, принимает значения [1 .. 10000].
3	Указать действие, которое должно быть применено для маршрутной информации.	evt(config-route-map-rule)# action <ACT>	<ACT> – назначаемое действие: • permit – прием или анонсирование маршрутной информации разрешено; • deny – запрещено.

Шаг	Описание	Команда	Ключи
4	Задать значение атрибута BGP AS-Path в маршруте, для которого должно срабатывать правило (не обязательно).	evt(config-route-map-rule)# match as-path { [begin contain end] <AS-PATH> empty regex <REGEX> }	<AS-PATH> – список номеров автономных систем, задается в виде AS,AS,AS, принимает значения [1..4294967295]. Опциональные параметры: <REGEX> – регулярное выражение, задаётся по стандарту POSIX-Extended Regular Expressions. • begin – значение атрибута начинается с указанных номеров AS; • contain – значение атрибута содержит указанные номера AS; • empty – значение атрибута пусто; • end – значение атрибута заканчивается указанными номерами AS; • regex – значение атрибута соответствует регулярному выражению.
5	Задать значение атрибута BGP Community, для которого должно срабатывать правило (не обязательно).	evt(config-route-map-rule)# match community { <COMMUNITY-LIST> regex <REGEX> }	<COMMUNITY-LIST> – список community, задается в виде AS:N,AS:N, принимает значения [1..4294967295]. Можно указать до 64 community. • regex – значение атрибута соответствует регулярному выражению. <REGEX> – регулярное выражение, задаётся по стандарту POSIX-Extended Regular Expressions.
6	Задать значение атрибута BGP Extended Community, для которого должно срабатывать правило (не обязательно).	evt(config-route-map-rule)# match extcommunity { <EXTCOMMUNITY-LIST> regex <REGEX> }	<EXTCOMMUNITY-LIST> – список extcommunity, задается в виде KIND:AS:N, KIND:AS:N, где KIND – тип extcommunity: • rt (Route Target); • ro (Route Origin). N – номер extcommunity, принимает значения [1..65535]. • regex – значение атрибута соответствует регулярному выражению. <REGEX> – регулярное выражение, задаётся по стандарту POSIX-Extended Regular Expressions.

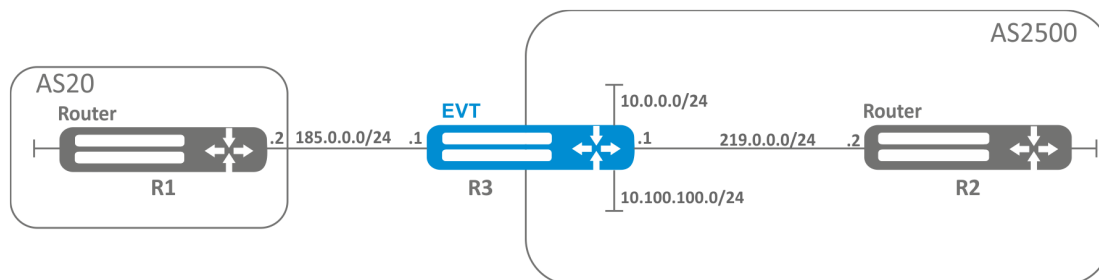
Шаг	Описание	Команда	Ключи
7	Задать профиль IP-адресов, содержащий значения подсетей назначения в маршруте (не обязательно).	evt(config-route-map-rule)# match ip address object-group <OBJ-GROUP-NETWORK-NAME>	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, содержащего префиксы подсетей назначения, задаётся строкой до 31 символа.
		evt(config-route-map-rule)# match ipv6 address object-group <OBJ-GROUP-NETWORK-NAME>	
8	Задать профиль IP-адресов, содержащий значения атрибута BGP Next-Хоп в маршруте для которого должно срабатывать правило (не обязательно).	evt(config-route-map-rule)# match ip bgp next-hop object-group <OBJ-GROUP-NETWORK-NAME>	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, содержащего префиксы подсетей назначения, задается строкой до 31 символа.
		evt(config-route-map-rule)# match ipv6 bgp next-hop object-group <OBJ-GROUP-NETWORK-NAME>	
9	Задать профиль, содержащий IP-адреса маршрутизатора, анонсировавшего маршрут, для которого должно срабатывать правило (не обязательно).	evt(config-route-map-rule)# match ip route-source object-group <OBJ-GROUP-NETWORK-NAME>	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, содержащего префиксы подсетей назначения, задается строкой до 31 символа.
		evt(config-route-map-rule)# match ipv6 route-source object-group <OBJ-GROUP-NETWORK-NAME>	
10	Задать ACL-группу, для которой должно срабатывать правило (не обязательно).	evt(config-route-map-rule)# match access-group <NAME>	<NAME> – имя списка контроля доступа, задается строкой до 31 символа.
11	Задать значение атрибута BGP MED в маршруте для которого должно срабатывать правило (не обязательно).	evt(config-route-map-rule)# match metric bgp <METRIC>	<METRIC> – значение атрибута BGPMED, принимает значения [0..4294967295].
12	Задать значение атрибута OSPF Metric в маршруте, для которого должно срабатывать правило.	evt(config-route-map-rule)# match metric ospf <TYPE> <METRIC>	<TYPE> – тип атрибута OSPF Metric, принимает значение type-1 и type-2; <METRIC> – значение атрибута OSPF Metric, принимает значения [0..65535].
13	Задать значение атрибута RIP Metric в маршруте, для которого должно срабатывать правило.	evt(config-route-map-rule)# match metric rip <METRIC>	<METRIC> – значение атрибута RIP Metric, принимает значения [0..16].

Шаг	Описание	Команда	Ключи
14	Задать значение атрибута OSPF Tag в маршруте, для которого должно срабатывать правило.	evt(config-route-map-rule)# match tag ospf <TAG>	<TAG> – значение атрибута OSPF Tag, принимает значения [0..4294967295].
15	Задать значение атрибута RIP Tag в маршруте, для которого должно срабатывать правило.	evt(config-route-map-rule)# match tag rip <TAG>	<RIP> – значение атрибута RIP Tag, принимает значения [0..65535].
16	Задать значение атрибута BGP AS-Path, которое будет добавляться в начало списка AS-Path (не обязательно).	evt(config-route-map-rule)# action set as-path prepend <AS-PATH> {track <TRACK-ID>}	<AS-PATH> – список номеров автономных систем, который будет добавлен к текущему значению в маршруте. Задаётся в виде AS,AS,AS, принимает значения [1..4294967295]. <TRACK-ID> – идентификатор vrrp-tracking, при котором будет исполняться указанное действие. Изменяется в диапазоне [1..60].
16.1	Заменять номер или последовательность номеров AS в атрибуте BGP AS-Path на номер локальной AS (не обязательно).	evt(config-route-map-rule)# action set as-path replace { any <AS-PATH> }	<AS-PATH> – список номеров автономных систем, который будет заменён на локальный номер AS. Задаётся в виде AS,AS,AS, принимает значения [1..4294967295]. • any – заменять любой номер AS.
17	Задать значение атрибута BGP Community, которое будет установлено в маршруте (не обязательно).	evt(config-route-map-rule)# action set community {COMMUNITY-LIST} no- advertise no-export }	<COMMUNITY-LIST> – список community, задается в виде AS:N,AS:N, где каждая часть принимает значения [1..65535]; • no - advertise – маршруты, передаваемые с данным community, не должны анонсироваться другим BGP-соседям; • no - export – маршруты, передаваемые с таким community, не должны анонсироваться eBGP-соседям, но анонсируются внешним соседям в конфедерации.
18	Задать значение атрибута BGP ExtCommunity, которое будет установлено в маршруте (не обязательно).	evt(config-route-map-rule)# action set extcommunity <EXTCOMMUNITY-LIST>	<EXTCOMMUNITY-LIST> – список extcommunity, задается в виде KIND:AS:N, KIND:AS:N, где KIND – тип extcommunity: • rt (Route Target); • ro (Route Origin). N – номер extcommunity, принимает значения [1..65535].

Шаг	Описание	Команда	Ключи
19	Задать атрибут BGP Next-Hop, который будет установлен в маршруте при анонсировании (не обязательно).	evt(config-route-map-rule)# action set ip bgp-next-hop <ADDR>	<ADDR> – IP-адрес шлюза, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
		evt(config-route-map-rule)# action set ipv6 bgp-next-hop <IPV6-ADDR>	<IPV6-ADDR> – IPv6-адрес шлюза, задается в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
20	Задать значение Next-Hop, которое будет установлено в маршруте, полученном по BGP (не обязательно).	evt(config-route-map-rule)# action set ip next-hop {NEXTHOP} blackhole unreachable prohibit}	<NEXTHOP> – IP-адрес шлюза, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; • blackhole – пакеты до данной подсети будут удаляться без отправки уведомлений отправителю; • unreachable – пакеты до данной подсети будут удаляться, отправитель получит в ответ ICMP Destination unreachable (Host unreachable, code 1); • prohibit – пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Communication administratively prohibited code 13).
		evt(config-route-map-rule)# action set ipv6 next-hop <IPV6- NEXTHOP>	<IPV6-NEXTHOP> – IPv6-адрес шлюза, задается в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
21	Задать значение атрибута BGP Local Preference, который будет установлен в маршруте (не обязательно).	evt(config-route-map-rule)# action set local-preference <PREFERENCE>	<PREFERENCE> – значение атрибута BGP Local Preference, принимает значения [0..255].
22	Задать значение атрибута BGP Origin, которое будет установлено в маршруте (не обязательно).	evt(config-route-map-rule)# action set origin <ORIGIN>	<ORIGIN> – значение атрибута BGP Origin: • egp – маршрут выучен по протоколу EGP; • igp – маршрут получен внутри исходной AS; • incomplete – маршрут выучен другим образом.
23	Задать значение BGP MED, которое будет установлено в маршруте (не обязательно).	evt(config-route-map-rule)# action set metric bgp <METRIC>	<METRIC> – значение атрибута BGP MED, принимает значения [0..4294967295].

Шаг	Описание	Команда	Ключи
24	Добавить фильтрацию и модификацию маршрутов во входящих или исходящих направлениях.	evt(config-bgp-neighbor)# route-map <NAME><DIRECTION> evt(config-ipv6-bgp-neighbor)# route-map <NAME><DIRECTION>	<NAME> – имя сконфигурированной маршрутной карты; <DIRECTION> – направление: • in – фильтрация и модификация получаемых маршрутов; • out – фильтрация и модификация анонсируемых маршрутов.

Пример настройки 1. Route-map для BGP



Задача:

Назначить community для маршрутной информации, приходящей из AS20:

Предварительно нужно выполнить следующие действия:

- Настроить BGP с AS2500 на маршрутизаторе evt;
- Установить соседство с AS20.

Решение:

Создаем политику:

```
evt# configure
evt(config)# route-map from-as20
```

Создаем правило 1:

```
evt(config-route-map)# rule 1
```

Если AS PATH содержит AS20, то назначаем ему community 20:2020 и выходим:

```
evt(config-route-map-rule)# match as-path contain 20
evt(config-route-map-rule)# action set community 20:2020
evt(config-route-map-rule)# exit
evt(config-route-map)# exit
```

В BGP процессе AS2500 заходим в настройки параметров соседа:

```
evt(config)# router bgp 2500
evt(config-bgp)# neighbor 185.0.0.2
evt(config-bgp-neighbor)# address-family ipv4 unicast
```

Привязываем политику к принимаемой маршрутной информации:

```
evt(config-bgp-neighbor-af)# route-map from-as20 in
```

Пример настройки 2. Route-map для BGP

Задача:

Для всей передаваемой маршрутной информации (с community 2500:25) назначить MED, равный 240, и указать источник маршрутной информации EGP:

Предварительно:

Настроить BGP с AS2500 на EVT/EVS.

Решение:

Создаем политику:

```
evt(config)# route-map to-as20
```

Создаем правило:

```
evt(config-route-map)# rule 1
```

Если community содержит 2500:25, то назначаем ему MED 240 и Origin EGP:

```
evt(config-route-map-rule)# match community 2500:25
evt(config-route-map-rule)# action set metric bgp 240
evt(config-route-map-rule)# action set origin egp
evt(config-route-map-rule)# exit
evt(config-route-map)# exit
```

В BGP процессе AS2500 заходим в настройки параметров соседа:

```
evt(config)# router bgp 2500
evt(config-bgp)# neighbor 185.0.0.2
evt(config-bgp-neighbor-af)# address-family ipv4 unicast
```

Привязываем политику к анонсируемой маршрутной информации:

```
evt(config-bgp-neighbor-af)# route-map to-as20 out
evt(config-bgp-neighbor-af)# exit
evt(config-bgp-neighbor)# exit
evt(config-bgp)# exit
```

Пример настройки 3. Использование регулярных выражений в Route-map для BGP

Начиная с версии 1.23 доступно использование регулярных выражений в Route-map для контроля распространения маршрутной информации по протоколу BGP. Контроль можно производить по трём атрибутам BGP: AS-path, community, extcommunity. Синтаксис регулярных выражений соответствует стандарту POSIX ERE. В таблице ниже представлены некоторые примеры регулярных выражений.

Условие совпадения	Регулярное выражение
Маршруты с любым содержимым AS-path	.*
Маршруты с пустым AS-path	^\$
Маршруты с одной любой AS в AS-path	^[0-9]+\$
Маршруты с двумя любыми AS в AS-path	^[0-9]+ [0-9]+\$
Маршруты, зарожждённые в AS 15	(^ .*)15\$
Маршруты, полученные из AS 20	^20(.* \$)
Маршруты, проходящие через AS 22	.* 22 .*
Маршруты, проходящие через AS 30, а затем через AS 22	.* 22 30 .*
Маршруты, проходящие через AS 30 или AS 43	.* (30 43) .*
Маршруты, зарождённые в AS 66 и проходящие через AS 60	.* 60 (.*)*66\$
Маршруты, зарождённые в AS 70 или проходящие через неё	.* 70(.* \$)
Маршруты, содержащие приватные AS в AS-path	(^ .*)((6451[2-9]) (645[2-9][0-9]) (64[6-9][0-9]{2}) (65[0-4][0-9]{2}) (655[0-2][0-9]) (6553[0-4]))(.* \$)
Номер AS 100, номер community 200	^100:200\$

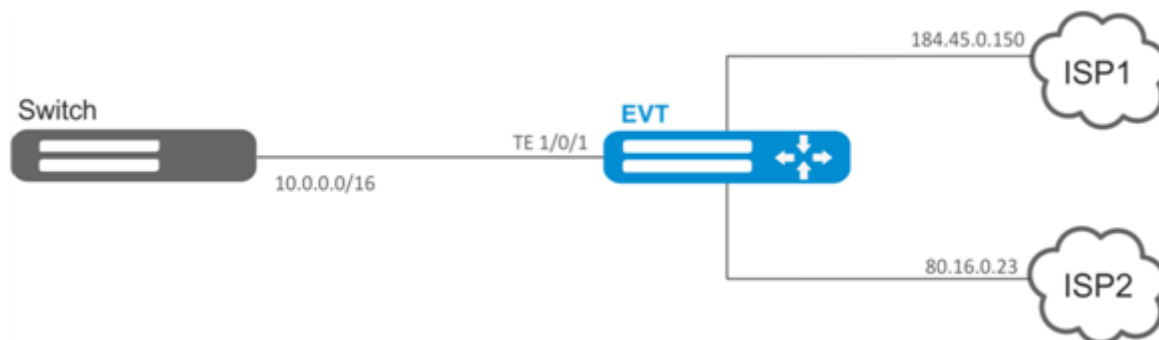
Условие совпадения	Регулярное выражение
Номера AS 112 или 232, любой номер community	^(112 232):[0-9]*\$
Номер AS 277, номер community начинается с 3	^277:3[0-9]*\$
Любой номер AS, номер community в диапазоне 150-1230	^([0-9]*):((1[5-9][0-9]) ([2-9][0-9]{2}) (1[0-2][0-2][0-9]) (1230))\$
Тип route target, IP-адрес 10.10.10.1, номер extcommunity 653 и 654	^rt:10\10\10\1:65[34]\$

Алгоритм настройки Route-map на основе списков доступа (Policy-based routing)

Шаг	Описание	Команда	Ключи
1	Создать маршрутную карту для фильтрации и модификации IP-маршрутов.	evt(config)# route-map <NAME>	<NAME> – имя маршрутной карты, задаётся строкой до 31 символа.
2	Создать правило маршрутной карты.	evt(config-route-map)# rule <ORDER>	<ORDER> – номер правила, принимает значения [1..10000].
3	Указать действие, которое должно быть применено для маршрутной информации.	evt(config-route-map-rule)# action <ACT>	<ACT> – назначаемое действие: • permit – прием или анонсирование маршрутной информации разрешено; • deny – запрещено.
4	Задать ACL, для которого должно срабатывать правило (не обязательно).	evt(config-route-map-rule)# match ip access-group <NAME>	<NAME> – имя списка контроля доступа, задаётся строкой до 31 символа.
5	Задать Next-Hop для пакетов, которые попадают под критерии в указанном списке доступа (ACL) (не обязательно).	evt(config-route-map-rule)# action set ip next-hop verify-availability <NEXTHOP><METRIC>	<NEXTHOP> – IP-адрес шлюза задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <METRIC> – метрика маршрута, принимает значения [0..255].
6	Назначить политику маршрутизации на основе списков доступа (ACL).	evt(config-if-gi)# ip policy route-map <NAME>	<NAME> – имя сконфигурированной политики маршрутизации, строка до 31 символа.

Шаг	Описание	Команда	Ключи
7	Разрешить фильтрацию и модификацию локального трафика на основе политики маршрутизации.	evt(config)# ip local policy [vrf <VRF>] route-map <NAME>	<NAME> – имя сконфигурированной политики маршрутизации, строка до 31 символа.

Пример настройки Route-map на основе списков доступа (Policy-based routing)



Задача:

Распределить трафик между Интернет-провайдерами на основе подсетей пользователей.

Предварительно нужно назначить IP-адреса на интерфейсы.

Требуется направлять трафик с адресов 10.0.20.0/24 через ISP1 (184.45.0.150), а трафик с адресов 10.0.30.0/24 – через ISP2 (80.16.0.23). Требуется контролировать доступность адресов провайдеров (работоспособность подключений к ISP), и при неработоспособности одного из подключений переводить с него на рабочее подключение весь трафик.

Решение:

Создаем ACL:

```

evt# configure
evt(config)# ip access-list extended sub20
evt(config-acl)# rule 1
evt(config-acl-rule)# match source-address 10.0.20.0 255.255.255.0
evt(config-acl-rule)# match destination-address any
evt(config-acl-rule)# match protocol any
evt(config-acl-rule)# action permit
evt(config-acl-rule)# enable
evt(config-acl-rule)# exit
evt(config-acl)# exit
evt(config)# ip access-list extended sub30
evt(config-acl)# rule 1
evt(config-acl-rule)# match source-address 10.0.30.0 255.255.255.0
evt(config-acl-rule)# match destination-address any
evt(config-acl-rule)# match protocol any
evt(config-acl-rule)# action permit
evt(config-acl-rule)# enable
evt(config-acl-rule)# exit
evt(config-acl)# exit

```

Создаем политику:

```
evt(config)# route-map PBR
```

Создаем правило 1:

```
evt(config-route-map)# rule 1
```

Указываем список доступа (ACL) в качестве фильтра:

```
evt(config-route-map-rule)# match ip access-group sub20
```

Указываем next-hop для sub20:

```
evt(config-route-map-rule)# action set ip next-hop verify-availability 184.45.0.150 10
evt(config-route-map-rule)# action set ip next-hop verify-availability 80.16.0.23 30
evt(config-route-map-rule)# exit
evt(config-route-map)# exit
```

Правилом 1 будет обеспечена маршрутизация трафика из сети 10.0.20.0/24 на адрес 184.45.0.150, а при его недоступности – на адрес 80.16.0.23. Приоритетность шлюзов задается значениями метрик – 10 и 30.

Создаем правило 2:

```
evt(config-route-map)# rule 2
```

Указываем список доступа (ACL) в качестве фильтра:

```
evt(config-route-map-rule)# match ip access-group sub30
```

Указываем nexthop для sub30 и выходим:

```
evt(config-route-map-rule)# action set ip next-hop verify-availability 80.16.0.23 10
evt(config-route-map-rule)# action set ip next-hop verify-availability 184.45.0.150 30
evt(config-route-map-rule)# exit
evt(config-route-map)# exit
```

Правилом 2 будет обеспечена маршрутизация трафика из сети 10.0.30.0/24 на адрес 80.16.0.23, а при его недоступности – на адрес 184.45.0.150. Приоритетность задается значениями метрик.

Заходим на интерфейс TE 1/0/1:

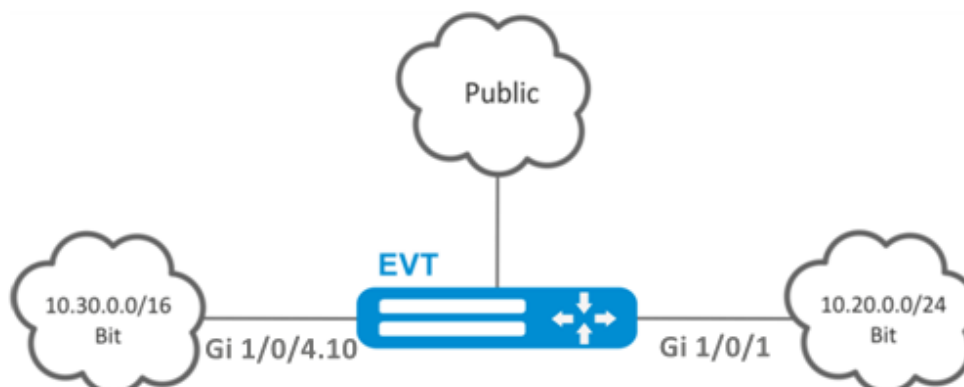
```
evt(config)# interface tengigabitethernet 1/0/1
```

Привязываем политику на соответствующий интерфейс:

```
evt(config-if-te)# ip policy route-map PBR
```

Настройка VRF

VRF (Virtual Routing and Forwarding) – технология, которая позволяет изолировать маршрутную информацию, принадлежащую различным классам (например, маршруты одного клиента).



Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать экземпляр VRF и перейти в режим настройки параметров экземпляра VRF.	evt(config)# ip vrf <VRF>	<VRF> – имя экземпляра VRF, задается строкой до 31 символа.
2	Назначить описание конфигурируемого экземпляра VRF.	evt(config-vrf)# description <DESCRIPTION>	<DESCRIPTION> – описание экземпляра VRF, задается строкой до 255 символов.
3	Настроить емкость таблиц маршрутизации в конфигурируемом VRF для IPv4/IPv6 протоколов маршрутизации (не обязательно).	evt(config-vrf)# ip protocols <PROTOCOL> max-routes <VALUE> evt(config-vrf)#ipv6 protocols <PROTOCOL> max-routes <VALUE>	<PROTOCOL> – вид протокола, принимает значения: ospf, bgp; <VALUE> – количество маршрутов в маршрутной таблице, принимает значения в диапазоне: • OSPF - [1..300000] • BGP - [1..2500000] Значение по умолчанию: 0.
4	Включить и настроить протоколы динамической маршрутизации трафика (Static/OSPF/BGP/IS-IS) в экземпляре VRF (не обязательно). См. соответствующий раздел Конфигурирование статических маршрутов , Настройка OSPF и Настройка BGP .		

Шаг	Описание	Команда	Ключи
5	В режиме конфигурирования физического/логического интерфейса, туннеля, правила DNAT/ SNAT, DAS-сервера или SNMPv3 пользователя указать имя экземпляра VRF для которого будет использоваться (при необходимости).	evt(config-snat-ruleset)# ip vrf forwarding <VRF>	<VRF> – имя экземпляра VRF, задается строкой до 31 символа.
6	Настроить LT-туннель для передачи трафика в глобальный режим или другие VRF (при необходимости).		См. раздел Настройка LT-туннелей .

Пример настройки

Задача:

К маршрутизатору evt подключены 2 сети, которые необходимо изолировать от остальных сетей.

Решение:

Создадим VRF:

```
evt(config)# ip vrf bit
evt(config-vrf)# exit
```

Создадим зону безопасности:

```
evt(config)# security zone vrf-sec
evt(config-zone)# ip vrf forwarding bit
evt(config-zone)# exit
```

Создадим правило для пары зон и разрешим любой TCP/UDP-трафик:

```
evt(config)# security zone-pair vrf-sec vrf-sec
evt(config-zone-pair)# rule 1
evt(config-zone-rule)# match protocol udp
evt(config-zone-rule)# action permit
evt(config-zone-rule)# enable
evt(config-zone-rule)# exit
evt(config-zone-pair)# rule 2
evt(config-zone-rule)# match protocol tcp
evt(config-zone-rule)# action permit
evt(config-zone-rule)# enable
evt(config-zone-rule)# exit
```

Создадим привязку интерфейсов, назначим IP-адреса, укажем принадлежность к зоне:

```

evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# ip vrf forwarding bit
evt(config-if-gi)# ip address 10.20.0.1/24
evt(config-if-gi)# security-zone vrf-sec
evt(config-if-gi)# exit
evt(config)# interface gigabitethernet 1/0/4.10
evt(config-if-sub)# ip vrf forwarding bit
evt(config-if-sub)# ip address 10.30.0.1/16
evt(config-if-sub)# security-zone vrf-sec
evt(config-if-sub)# exit
evt(config)# exit

```

Информацию об интерфейсах, привязанных к VRF, можно посмотреть командой:

```

evt# show ip vrf

```

Таблицу маршрутов VRF можно просмотреть с помощью команды:

```

evt# show ip route vrf bit

```

Настройка MultiWAN

Технология MultiWAN позволяет организовать отказоустойчивое соединение с резервированием линков от нескольких провайдеров, а также решает проблему балансировки трафика между резервными линками.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Сконфигурировать интерфейсы, по которым будет работать MultiWAN: установить IP-адреса и указать security-zone.		
2	Прописать статические маршруты через WAN (если необходимо).	evt(config)# ip route <SUBNET> wan load-balance rule <ID> [<METRIC>]	<ID> – идентификатор создаваемого правила из п.2. [METRIC] – метрика маршрута, принимает значения [0..255].
3	Создать правило WAN и перейти в режим настройки параметров правила.	evt(config)# wan load-balance rule <ID>	<ID> – идентификатор создаваемого правила, принимает значения [1..50].

Шаг	Описание	Команда	Ключи
4	Задать интерфейсы или туннели, которые являются шлюзами в маршруте, создаваемом службой MultiWAN.	evt(config-wan-rule)# outbound { interface <IF> tunnel <TUN> } [WEIGHT]	<IF> – имя интерфейса; <TUN> – имя туннеля; [WEIGHT] – вес туннеля или интерфейса, определяется в диапазоне [1..255]. Если установить значение 2, то по данному интерфейсу будет передаваться в 2 раза больше трафика, чем по интерфейсу со значением по умолчанию. В режиме резервирования активным будет маршрут с наибольшим весом. Значение по умолчанию 1.
5	Описать правила (не обязательно).	evt(config-wan-rule)# description <DESCRIPTION>	<DESCRIPTION> – описание правила wan, задаётся строкой до 255 символов.
6	Данной командой осуществляется переключение из режима балансировки в режим резервирования (если необходимо).	evt(config-wan-rule)# failover	
7	Данной командой включается отправка ответных пакетов сессии через тот же интерфейс, через который получены входящие пакеты сессии (если необходимо).	evt(config-wan-rule)# stickiness	
8	Включить wan-правило.	evt(config-wan-rule)# enable	
9	Создать список IP-адресов для проверки целостности соединения и осуществить переход в режим настройки параметров списка.	evt(config)# wan load-balance target-list <NAME>	<NAME> – название списка, задаётся строкой до 31 символа.
10	Задать цель проверки и перейти в режим настройки параметров цели.	evt(config-target-list)# target <ID>	<ID> – идентификатор цели, задаётся в пределах [1..50]. Если при удалении используется значение параметра «all», то будут удалены все цели для конфигурируемого списка целей.
11	Описать target (не обязательно).	evt(config-wan-target)# description <DESCRIPTION>	<DESCRIPTION> – описание target, задаётся строкой до 255 символов.

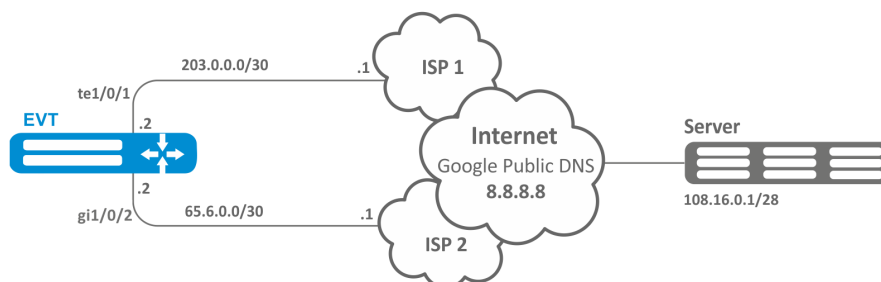
Шаг	Описание	Команда	Ключи
12	Указать время ожидания ответа на запрос по протоколу ICMP (не обязательно).	evt(config-wan-target)# resp-time <TIME>	<TIME> – время ожидания, определяется в секундах [1..30].
13	Указать IP-адрес проверки.	evt(config-wan-target)# ip address <ADDR>	<ADDR> – IP-адрес назначения, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
		evt(config-wan-target)# ipv6 address <IPV6-ADDR>	<IPV6-ADDR> – IPv6-адрес назначения, задаётся в виде X:X:X:X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
14	Включить проверку цели.	evt(config-wan-target)# enable	
Команды для пунктов 14–17 необходимо применить на интерфейсах/туннелях в MultiWAN.			
15	Включить WAN-режим на интерфейсе для IPv4/IPv6-стека.	evt(config-if-gi)# wan load-balance enable	
		evt(config-if-gi)# ipv6 wan load-balance enable	
16	Задать количество неудачных попыток проверки соединения, после которых, при отсутствии ответа от встречной стороны, соединение будет считаться неактивным (не обязательно).	evt(config-if-gi)# wan load-balance failure-count <VALUE>	<VALUE> – количество попыток, определяется в диапазоне [1..10]. Значение по умолчанию: 1.
		evt(config-if-gi)# ipv6 wan load-balance failure-count <VALUE>	
17	Задать количество успешных попыток проверки соединения, после которых, в случае успеха, соединение считается вновь активным (не обязательно).	evt(config-if-gi)# wan load-balance success-count <VALUE>	<VALUE> – количество попыток, определяется в диапазоне [1..10]. Значение по умолчанию: 1.
		evt(config-if-gi)# ipv6 wan load-balance success-count <VALUE>	

Шаг	Описание	Команда	Ключи
18	Задать IP-адрес соседа, который будет указан в качестве одного из шлюзов в статическом маршруте, создаваемом службой MultiWAN.	evt(config-if-gi)# wan load-balance nexthop { <IP> dhcp enable tunnel enable }	<IP> – IP-адрес назначения (шлюз), задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. dhcp enable – если на интерфейсе IP-адрес получен через DHCP-клиента, используется шлюз с DHCP-сервера. tunnel enable – использовать в качестве nexthop – p-t-p адрес назначения. Применимо для подключаемых интерфейсов, работающих через ppp.
		evt(config-if-gi)# ipv6 wan load-balance nexthop { <IPV6> }	<IPV6> – IPv6-адрес назначения (шлюз), задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
19	Данной командой будут проверяться IP-адреса из списка проверки целостности. В случае недоступности всех (по умолчанию)/хотя бы одной (с использованием ключа check-all) из проверяемых узлов, шлюз будет считаться недоступным.	evt(config-if-gi)# wan load-balance target-list { check-all <NAME> }	<NAME> – проверку производить на основании конкретного target листа (заданного в п.7).
		evt(config-if-gi)# ipv6 wan load-balance target-list { check-all <NAME> }	check-all – проверку производить на основании всех target листа.
20	Прописать статические маршруты через WAN.	evt(config)# ip route <SUBNET> wan load-balance rule <ID> [METRIC]	<ID> – идентификатор создаваемого правила из п.2. [METRIC] – метрика маршрута, принимает значения [0..255].
		evt(config)# ipv6 route <SUBNET> wan load-balance rule <ID> [METRIC]	

Пример настройки

Задача:

Настроить маршрут к серверу (108.16.0.1/28) с возможностью балансировки нагрузки.



Решение:

Предварительно нужно выполнить следующие действия:

- настроить зоны для интерфейсов te1/0/1 и gi1/0/2;
- указать IP-адреса для интерфейсов te1/0/1 и gi1/0/2.

Основной этап конфигурирования:

Настроим маршрутизацию:

```
evt(config)# ip route 108.16.0.0/28 wan load-balance rule 1
```

Создадим правило WAN:

```
evt(config)# wan load-balance rule 1
```

Укажем участвующие интерфейсы:

```
evt(config-wan-rule)# outbound interface gigabitethernet 1/0/2
evt(config-wan-rule)# outbound interface tengigabitethernet 1/0/1
```

Включим созданное правило балансировки и выйдем из режима конфигурирования правила:

```
evt(config-wan-rule)# enable
evt(config-wan-rule)# exit
```

Создадим список для проверки целостности соединения:

```
evt(config)# wan load-balance target-list google
```

Создадим цель проверки целостности:

```
evt(config-target-list)# target 1
```

Зададим адрес для проверки, включим проверку указанного адреса и выйдем:

```
evt(config-wan-target)# ip address 8.8.8.8
evt(config-wan-target)# enable
evt(config-wan-target)# exit
```

Настроим интерфейсы. В режиме конфигурирования интерфейса te1/0/1 указываем nexthop:

```
evt(config)# interface tengigabitethernet 1/0/1
evt(config-if)# wan load-balance nexthop 203.0.0.1
```

В режиме конфигурирования интерфейса te1/0/1 указываем список целей для проверки соединения:

```
evt(config-if)# wan load-balance target-list google
```

В режиме конфигурирования интерфейса te1/0/1 включаем WAN-режим и выходим:

```
evt(config-if)# wan load-balance enable
evt(config-if)# exit
```

В режиме конфигурирования интерфейса gi1/0/2 указываем nexthop:

```
evt(config)# interface gigabitethernet 1/0/2
evt(config-if)# wan load-balance nexthop 65.6.0.1
```

В режиме конфигурирования интерфейса gi1/0/2 указываем список целей для проверки соединения:

```
evt(config-if)# wan load-balance target-list google
```

В режиме конфигурирования интерфейса gi1/0/2 включаем WAN-режим и выходим:

```
evt(config-if)# wan load-balance enable
evt(config-if)# exit
```

Для переключения в режим резервирования настроим следующее:

Заходим в режим настройки правила WAN:

```
evt(config)# wan load-balance rule 1
```

Функция MultiWAN также может работать в режиме резервирования, в котором трафик будет направляться в активный интерфейс с наибольшим весом. Включить данный режим можно следующей командой:

```
evt(config-wan-rule)# failover
```

6.2.7 Управление резервированием

- [Настройка VRRP](#)
 - [Алгоритм настройки](#)
 - [Пример настройки 1](#)
 - [Пример настройки 2](#)
- [Настройка tracking](#)
 - [Алгоритм настройки](#)
 - [Пример настройки](#)
- [Настройка Firewall/NAT failover](#)
 - [Алгоритм настройки](#)
 - [Пример настройки](#)
- [Настройка DHCP failover](#)
 - [Алгоритм настройки](#)
 - [Пример настройки](#)

 **Конфигурация на маршрутизаторах EVT и EVS производится с помощью одинаковых команд. Ниже приведены примеры настройки EVT.**

Настройка VRRP

VRRP (англ. *Virtual Router Redundancy Protocol*) – сетевой протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию. Это достигается путём объединения группы маршрутизаторов в один виртуальный маршрутизатор и назначения им общего IP-адреса, который и будет использоваться как шлюз по умолчанию для компьютеров в сети.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим конфигурирования интерфейса/сетевого моста, для которого необходимо настроить протокол VRRP.	evt(config)# interface <IF-TYPE><IF-NUM>	<IF-TYPE> – тип интерфейса; <IF-NUM> – F/S/P – F-фрейм (1), S – слот (0), P – порт.
		evt(config)# tunnel <TUN-TYPE><TUN-NUM>	<TUN-TYPE> – тип туннеля; <TUN-NUM> – номер туннеля.
		evt(config)# bridge <BR-NUM>	<BR-NUM> – номер сетевого моста.
2	Настроить необходимые параметры на интерфейсе/сетевом мосту, включая IP-адрес.		
3	Включить VRRP-процесс на IP-интерфейсе.	evt(config-if-gi)# vrrp	
		evt(config-if-gi)# ipv6 vrrp	

Шаг	Описание	Команда	Ключи
4	Установить виртуальный IP-адрес VRRP-маршрутизатора.	evt(config-if-gi)# vrrp ip <ADDR/LEN> [secondary]	<ADDR/LEN> – виртуальный IP-адрес и длина маски, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. Можно указать несколько IP-адресов перечислением через запятую. Может быть назначено до 8 IP-адресов на интерфейс. secondary – ключ для установки дополнительного IP-адреса.
		evt(config-if-gi)# ipv6 vrrp ip <IPV6-ADDR>	<IPV6-ADDR> – виртуальный IPv6-адрес, задаётся в виде X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. Можно указать до 8 IPv6-адресов перечислением через запятую.
5	Установить идентификатор VRRP-маршрутизатора.	evt(config-if-gi)# vrrp id <VRID>	<VRID> – идентификатора VRRP-маршрутизатора, принимает значения [1..255].
		evt(config-if-gi)# ipv6 vrrp id <VRID>	
6	Установить приоритет VRRP-маршрутизатора (не обязательно).	evt(config-if-gi)# vrrp priority <PR>	<PR> – приоритет VRRP-маршрутизатора, принимает значения [1..254]. Значение по умолчанию: 100.
		evt(config-if-gi)# ipv6 vrrp priority <PR>	
7	Установить принадлежность VRRP-маршрутизатора к группе. Группа предоставляет возможность синхронизировать несколько VRRP-процессов, так если в одном из процессов произойдет смена мастера, то в другом процессе также произойдёт смена ролей (не обязательно).	evt(config-if-gi)# vrrp group <GRID>	<GRID> – идентификатор группы VRRP-маршрутизатора, принимает значения [1..32].
		evt(config-if-gi)# ipv6 vrrp group <GRID>	

Шаг	Описание	Команда	Ключи
8	Установить наследование состояний VRRP. Статус интерфейса наследника будет следовать состояниям VRRP родителя, идентификатор которого был задан (не обязательно).	evt(config-if-gi)# vrrp inherit-vrrp-id <VRID>	<VRID> – идентификатора VRRP-маршрутизатора, принимает значения [1..255].
		evt(config-if-gi)# ipv6 vrrp inherit-vrrp-id <VRID>	
9	Установить IP-адрес, который будет использоваться в качестве IP-адреса отправителя для VRRP-сообщений (не обязательно).	evt(config-if-gi)# vrrp source-ip <IP>	<IP> – IP-адрес отправителя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
		evt(config-if-gi)# ipv6 vrrp source-ip <IPV6>	<IPV6> – IPv6-адрес отправителя, задаётся в виде X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
10	Установить интервал между отправкой VRRP-сообщений (не обязательно).	evt(config-if-gi)# vrrp timers advertise <TIME>	<TIME> – время в секундах, принимает значения [1..40].
		evt(config-if-gi)# ipv6 vrrp timers advertise <TIME>	Значение по умолчанию: 1 секунда.
11	Установить интервал, по истечении которого происходит отправка GratuitousARP-сообщения(ий) при переходе маршрутизатора в состояние Master (не обязательно).	evt(config-if-gi)# vrrp timers garp delay <TIME>	<TIME> – время в секундах, принимает значения [1..60]. Значение по умолчанию: 5 секунд.
12	Установить количество GratuitousARP-сообщений, которые будут отправлены при переходе маршрутизатора в состояние Master (не обязательно).	evt(config-if-gi)# vrrp timers garp repeat <COUNT>	<COUNT> – количество сообщений, принимает значения [1..60]. Значение по умолчанию: 5.
13	Установить интервал, по истечении которого будет происходить периодическая отправка GratuitousARP-сообщения(ий), пока маршрутизатор находится в состоянии Master (не обязательно).	evt(config-if-gi)# vrrp timers garp refresh <TIME>	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: периодическая отправка отключена.

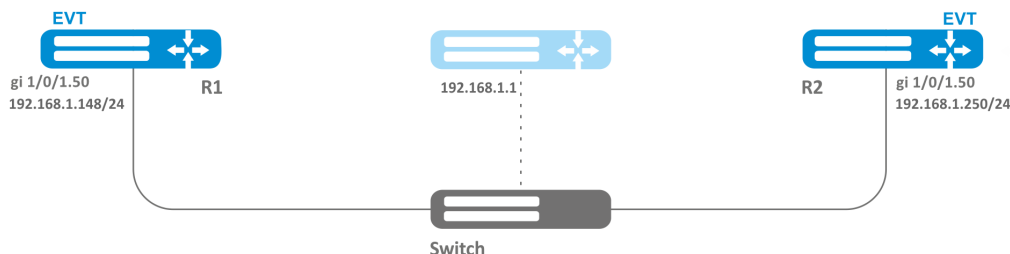
Шаг	Описание	Команда	Ключи
14	Установить количество GratuitousARP-сообщений, которые будут отправляться с периодом garpprefresh, пока маршрутизатор находится в состоянии Master (не обязательно).	evt(config-if-gi)# vrrp timers garp refresh-repeat <COUNT>	<COUNT> – количество сообщений, принимает значения [1..60]. Значение по умолчанию: 1.
15	Определить, будет ли Backup-маршрутизатор с более высоким приоритетом пытаться перехватить на себя роль Master у текущего Master-маршрутизатора с более низким приоритетом (не обязательно).	evt(config-if-gi)# vrrp preempt disable evt(config-if-gi)# ipv6 vrrp preempt disable	
16	Установить временной интервал, по истечении которого Backup-маршрутизатор с более высоким приоритетом будет пытаться перехватить на себя роль Master у текущего Master-маршрутизатора с более низким приоритетом (не обязательно).	evt(config-if-gi)# vrrp preempt delay <TIME> evt(config-if-gi)# ipv6 vrrp preempt delay <TIME>	<TIME> – время ожидания, определяется в секундах [1..1000]. Значение по умолчанию: 0.
17	Установить пароль для аутентификации с соседом (не обязательно).	evt(config-if-gi)# vrrp authentication key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> }	<CLEAR-TEXT> – ключ, задаётся строкой от 1 до 8 символов; <ENCRYPTED-TEXT> – зашифрованный ключ размером от 1 до 8 байт (от 2 до 16 символов). Задаётся в шестнадцатеричном формате (0xYYYY...) или (YYYY...).
18	Определить алгоритм аутентификации (не обязательно).	evt(config-if-gi)# vrrp authentication algorithm <ALGORITHM>	<ALGORITHM> – алгоритм аутентификации: • cleartext – пароль, передается открытым текстом; • md 5 – пароль хешируется по алгоритму md5.
19	Задать версию VRRP-протокола (не обязательно).	evt(config-if-gi)# vrrp version <VERSION>	<VERSION> – версия VRRP-протокола: 2, 3.
20	Установить режим, когда vrrp IP-адрес остается в состоянии UP вне зависимости от состояния самого интерфейса (не обязательно).	evt(config-if-gi)# vrrp force-up	

Шаг	Описание	Команда	Ключи
21	Определить задержку между установлением ipv6 vrrp состояния MASTER и началом рассылки ND-сообщений (не обязательно).	evt(config-if-gi)# ipv6 vrrp timers nd delay <TIME>	<TIME> – время в секундах, принимает значения [1..60]. Значение по умолчанию: 5.
22	Определить период обновления информации протокола ND для ipv6 vrrp в состоянии MASTER (не обязательно).	evt(config-if-gi)# ipv6 vrrp timers nd refresh <TIME>	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 5.
23	Определить количество ND сообщений отправляемых за период обновления для ipv6 vrrp в состоянии MASTER (не обязательно).	evt(config-if-gi)# ipv6 vrrp timers nd refresh-repeat <NUM>	<NUM> – количество, принимает значения [1..60]. Значение по умолчанию: 0.
24	Определить количество отправок ND-пакетов после установки ipv6 vrrp в состоянии MASTER (не обязательно).	evt(config-if-gi)# ipv6 vrrp timers nd repeat <NUM>	<NUM> – количество, принимает значения [1..60]. Значение по умолчанию: 1.

Пример настройки 1

Задача:

Организовать виртуальный шлюз для локальной сети в VLAN 50, используя протокол VRRP. В качестве локального виртуального шлюза используется IP-адрес 192.168.1.1.



Решение:

Предварительно нужно выполнить следующие действия:

- создать соответствующий саб-интерфейс;
- настроить зону для саб-интерфейса;
- указать IP-адрес для саб-интерфейса.

Основной этап конфигурирования:

Настроим маршрутизатор R1.

В созданном саб-интерфейсе настроим VRRP. Укажем уникальный идентификатор VRRP:

```
R1(config)#interface gi 1/0/1.50
R1(config-if-sub)# vrrp id 10
```


Укажем IP-адрес виртуального шлюза 192.168.1.1/24:

```
R1(config-if-sub)# vrrp ip 192.168.1.1
```

Включим VRRP:

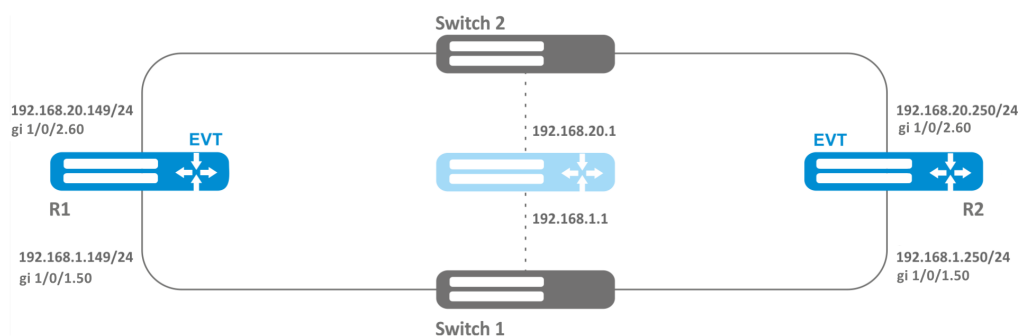
```
R1(config-if-sub)# vrrp
R1(config-if-sub)# exit
```

После чего необходимо произвести аналогичные настройки на R2.

Пример настройки 2

Задача:

Организовать виртуальные шлюзы для подсети 192.168.1.0/24 в VLAN 50 и подсети 192.168.20.0/24 в VLAN 60, используя протокол VRRP с функцией синхронизации мастера. Для этого используем объединение VRRP-процессов в группу. В качестве виртуальных шлюзов используются IP-адреса 192.168.1.1 и 192.168.20.1.



Решение:

Предварительно нужно выполнить следующие действия:

- создать соответствующие саб-интерфейсы;
- настроить зону для саб-интерфейсов;
- указать IP-адреса для саб-интерфейсов.

Основной этап конфигурирования:

Настроим маршрутизатор R1.

Настроим VRRP для подсети 192.168.1.0/24 в созданном саб-интерфейсе.

Укажем уникальный идентификатор VRRP:

```
R1(config-sub)#interface gi 1/0/1.50
R1(config-if-sub)# vrrp id 10
```

Укажем IP-адрес виртуального шлюза 192.168.1.1:

```
R1(config-if-sub)# vrrp ip 192.168.1.1
```

Укажем идентификатор VRRP-группы:

```
R1(config-if-sub)# vrrp group 5
```

Включим VRRP:

```
R1(config-if-sub)# vrrp
R1(config-if-sub)# exit
```

Настроим VRRP для подсети 192.168.20.0/24 в созданном суб-интерфейсе.

Укажем уникальный идентификатор VRRP:

```
R1(config-sub)#interface gi 1/0/2.60
R1(config-if-sub)# vrrp id 20
```

Укажем IP-адрес виртуального шлюза 192.168.20.1:

```
R1(config-if-sub)# vrrp ip 192.168.20.1
```

Укажем идентификатор VRRP-группы:

```
R1(config-if-sub)# vrrp group 5
```

Включим VRRP:

```
R1(config-if-sub)# vrrp
R1(config-if-sub)# exit
```

Произвести аналогичные настройки на R2.

 Помимо создания туннеля необходимо в firewall разрешить протокол VRRP (112).

 При использовании IPsec с VRRP рекомендуется настраивать DPD для ускорения перестроения IPsec-туннеля.

Настройка tracking

Tracking — механизм, позволяющий активировать сущности в зависимости от состояния VRRP/IP-SLA/туннеля/интерфейса.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Настроить VRRP согласно разделу Алгоритм настройки VRRP , настроить SLA по инструкции Настройка SLA , или сконфигурировать туннель/интерфейс.		
2	Добавить в систему Tracking-объект и перейти в режим настройки параметров Tracking-объекта.	evt(config)# track <ID>	<ID> – номер Tracking-объекта, принимает значения [1..100].
3	Задать правило слежения, на основании которых Tracking-объект будет переходить в активное состояние.	evt(config-track)# track vrrp id <VRID> state [not] { master backup fault } [vrf <VRF>]	<VRID> – идентификатор отслеживаемого VRRP-маршрутизатора, принимает значения [1..255]; <VRF> – имя экземпляра VRF, задается строкой до 31 символа.
		evt(config-track)# track sla test <NUM> [mode <MODE>]	<NUM> – номер SLA-теста, задается в диапазоне [1..10000]; <MODE> – режим слежения за sla-тестом, может принимать значения: • state success – отслеживается успешное состояние sla-теста; • state fail – отслеживается провальное состояние sla-теста; • reachability – отслеживаются состояние канала связи, по которому осуществляется sla-тест.

Шаг	Описание	Команда	Ключи
		evt(config-track)# track { interface <IF> tunnel <TUN> } [state <STATE>]	<IF> – имя IP-интерфейса, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора; <TUN> – имя туннеля, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора; <STATE> – режим слежения за sla-тестом, может принимать значения: • up – административное состояние "Up" ; • down – административное состояние "Down".
4	Включить Tracking-объект.	evt(config-track)# enable	
5	Установить задержку смены состояния отслеживаемого объекта (не обязательно).	evt(config-track)# delay { down up } <TIME>	<TIME> – время задержки в секундах, задается в диапазоне [1..300].
6	Задать режим работы track (не обязательно).	evt(config-track)# mode <MODE>	<MODE> – условие нахождения объекта отслеживания в активном состоянии, принимает значения: • and – объект будет находиться в активном состоянии, если выполняются все отслеживаемые условия; • or – объект будет находиться в активном состоянии, если выполняется хотя бы одно из отслеживаемых условий.
7	Создать сущность на evt, которая будет меняться в зависимости от состояния Tracking-объекта.		

Шаг	Описание	Команда	Ключи
7.1	Добавить возможность управления статическим IP-маршрутом к указанной подсети (не обязательно).	<pre> evt(config)# ip route [vrf <VRF>] <SUBNET> { <NEXTHOP> [resolve] interface <IF> tunnel <TUN> wan load-balance rule <RULE> blackhole unreachable prohibit } [<METRIC>] [track <TRACK-ID>] </pre>	<VRF> – имя экземпляра VRF, задается строкой до 31 символа; <SUBNET> – адрес назначения, может быть задан в следующих видах: AAA.BBB.CCC.DDD – IP-адрес хоста, где каждая часть принимает значения [0..255]; AAA.BBB.CCC.DDD/NN – IP-адрес подсети с маской в виде префикса, где AAA-DDD принимают значения [0..255] и NN принимает значения [1..32]. <NEXTHOP> – IP-адрес шлюза задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; • resolve – при указании данного параметра IP-адрес шлюза будет рекурсивно вычислен через таблицу маршрутизации. Если при рекурсивном вычислении не удастся найти шлюз из напрямую подключенной подсети, то данный маршрут не будет установлен в систему; <IF> – имя IP-интерфейса, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора; <TUN> – имя туннеля, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора; <RULE> – номер правила wan, задаётся в диапазоне [1..50]; • blackhole – при указании команды пакеты до данной подсети будут удаляться устройством без отправки уведомлений отправителю;

Шаг	Описание	Команда	Ключи
			• unreachable – при указании команды пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Host unreachable, code 1); • prohibit – при указании команды, пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Communication administratively prohibited, code 13); [METRIC] – метрика маршрута, принимает значения [0..255]; <TRACK-ID> – идентификатор Tracking-объекта. Если маршрут привязан к Tracking-объекту, то он появится в системе только при выполнении всех условий, заданных в объекте.
7.2	Добавить возможность управления логическим состоянием интерфейса (не обязательно).	evt(config-if-gi)# shutdown track <ID>	<ID> – номер Tracking-объекта, принимает значения [1..100].
7.3	Добавить возможность управления приоритетом VRRP-процесса (не обязательно).	evt(config-if-gi)# vrrp priority track <ID> { <PRIO> increment <INC> decrement <DEC> }	<ID> – номер Tracking-объекта, принимает значения в диапазоне [1..100]; <PRIO> – приоритет VRRP-процесса, который выставится, если Tracking-объект будет в активном состоянии, принимает значения в диапазоне [1..254]; <INC> – значение на которое увеличится приоритет VRRP-процесса, если Tracking-объект будет в активном состоянии, принимает значения в диапазоне [1..254]; <DEC> – значение на которое уменьшится приоритет VRRP-процесса, если Tracking-объект будет в активном состоянии, принимает значения в диапазоне [1..254].

Шаг	Описание	Команда	Ключи
7.4	Добавить возможность управления Next-Хоп для пакетов, которые попадают под критерии в указанном списке доступа (ACL) (не обязательно).	evt(config-route-map-rule)# action set ip next-hop verify-availability <NEXTHOP> <METRIC> track <ID>	<NEXTHOP> – IP-адрес шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <METRIC> – метрика маршрута, принимает значения [0..255]; <ID> – номер Tracking-объекта, принимает значения [1..100].
7.5	Добавить возможность управления атрибутом BGP AS-Path, которое будет добавляться в начало списка AS-Path в маршруте (не обязательно).	evt(config-route-map-rule)# action set as-path prepend <AS-PATH> track <ID> [default <AS-PATH>]	<AS-PATH> – список номеров автономных систем, который будет добавлен к текущему значению в маршруте. Задаётся в виде AS,AS,AS, принимает значения [1..4294967295]; <ID> – номер Tracking-объекта, принимает значения [1..100].
7.6	Добавить возможность управления атрибутом BGP MED в маршруте, для которого должно срабатывать правило (не обязательно).	evt(config-route-map-rule)# action set metric bgp { <METRIC> increment <INC> decrement <DEC> } track <ID> [default { <METRIC> increment <INC> decrement <DEC> }]	<ID> – номер Tracking-объекта, принимает значения [1..100]; <METRIC> – значение атрибута BGP MED, принимает значения [0..4294967295]; <INC> – значение, на которое увеличится атрибут BGP MED, если Tracking-объект будет в активном состоянии. Принимает значения [0..4294967295]; <DEC> – значение, на которое уменьшится атрибут BGP MED, если Tracking-объект будет в активном состоянии. Принимает значения [0..4294967295];

Шаг	Описание	Команда	Ключи
7.7	Добавить возможность управления атрибутом BGP Community в маршруте, для которого должно срабатывать правило (не обязательно).	evt(config-route-map-rule)# action { set add remove } community { no-advertise no-export <COMMUNITY-LIST> } track <TRACK-ID> [default <COMMUNITY-LIST>]	<COMMUNITY-LIST> – список community, задаётся в виде AS:N,AS:N,AS:N, где AS-часть принимает значения [0..65535], N-часть принимает значения [0..65535]. Можно указать до 64 community; <TRACK-ID> – идентификатор объекта отслеживания, при выполнении всех условий которого будет исполняться указанное действие. Изменяется в диапазоне [1..100]; no-advertise – при указании команды маршруты, которые передаются с данным значением атрибута community, не должны анонсироваться другим BGP-соседям; no-export – при указании команды маршруты, которые передаются с таким значением атрибута community, не должны анонсироваться за пределы конфедерации (автономная система, которая не является частью конфедерации, считается конфедерацией). То есть, маршруты не анонсируются eBGP-соседям, но анонсируются внешним соседям в конфедерации.

Шаг	Описание	Команда	Ключи
7.8	Добавить возможность управления атрибутом BGP ExtCommunity в маршруте, для которого должно срабатывать правило (не обязательно).	evt(config-route-map-rule)# action { set add remove } extcommunity <EXTCOMMUNITY-LIST> track <TRACK-ID> [default <EXTCOMMUNITY-LIST>]	<TRACK-ID> – идентификатор объекта отслеживания, при выполнении всех условий которого будет исполняться указанное действие. Изменяется в диапазоне [1..100]; <EXTCOMMUNITY-LIST> – список community, задаётся в виде KIND:AS:N,KIND:AS:N,KIND:AS:N, где: • KIND – тип extcommunity, принимает значения rt (Route Target) и ro (Route Origin); • AS – номер автономной системы, принимает значения [1..4294967295]; • N – номер extcommunity, определяющий политику маршрутизации трафика, принимает значения [1..65535].
7.9	Добавить возможность управления атрибутом BGP Local Preference в маршруте, для которого должно срабатывать правило (не обязательно).	evt(config-route-map-rule)# action set local-preference {<PREFERENCE> increment < VALUE > decrement < VALUE >} track <TRACK-ID> [default <PREFERENCE>] }	<VALUE> – значение дельты изменения атрибута BGP Local Preference относительно исходного значения. Принимает значение [1..2147483647]. Если в результате применения операции increment/decrement значение метрики выйдет за допустимый диапазон, значение Local Preference принимается равным максимально или минимально допустимому значению соответственно; <PREFERENCE> – значение атрибута BGP Local Preference, принимает значения [1..2147483647]; <TRACK-ID> – идентификатор tracking-объекта, при выполнении всех условий которого будет исполняться указанное действие. Изменяется в диапазоне [1..100].

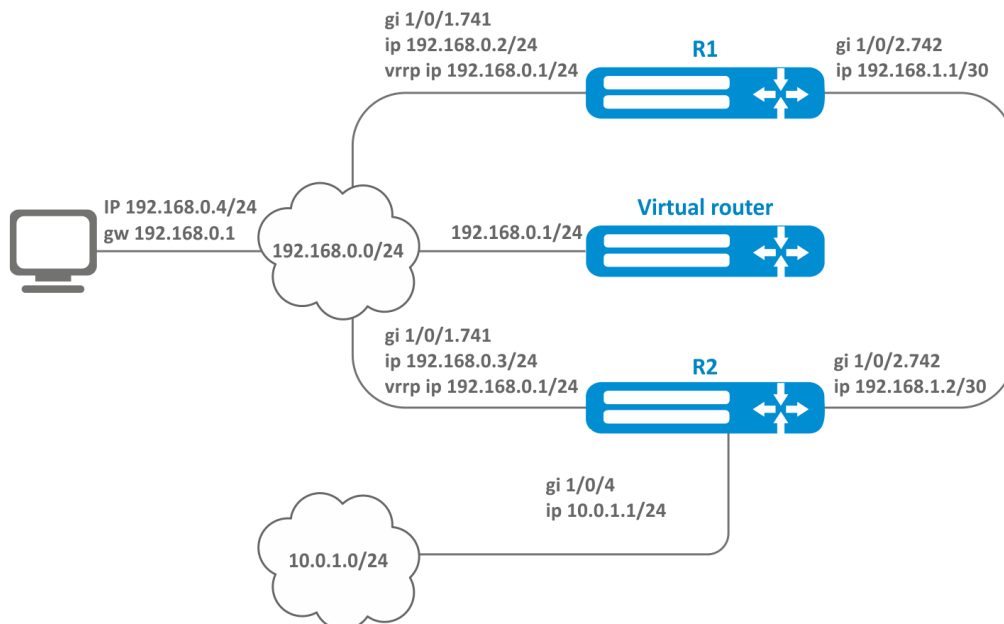
Шаг	Описание	Команда	Ключи
7.10	Добавить возможность управления атрибутом BGP Origin в маршруте, для которого должно срабатывать правило (не обязательно).	evt(config-route-map-rule)# action set origin <ORIGIN> track <TRACK-ID> [default <ORIGIN>]	<TRACK-ID> – идентификатор объекта отслеживания, при выполнении всех условий которого будет исполняться указанное действие. Изменяется в диапазоне [1..100]; <ORIGIN> – значение атрибута BGP Origin, принимает следующие значения: • egr – маршрут выучен по протоколу Exterior Gateway Protocol (EGP); • igp – маршрут получен внутри исходной автономной системы; • incomplete – маршрут выучен другим образом.
7.11	Добавить возможность управления атрибутом BGP Weight в маршруте, для которого должно срабатывать правило (не обязательно).	evt(config-route-map-rule)# action set weight bgp {< WEIGHT > increment < VALUE > decrement < VALUE >} track <TRACK-ID> [default <WEIGHT>]	<WEIGHT> – значение атрибута BGP weight, принимает значения [0..65535]; <TRACK-ID> – идентификатор объекта отслеживания, при выполнении всех условий которого будет исполняться указанное действие. Изменяется в диапазоне [1..100].
7.7	Добавить возможность управления активацией IPsec-туннеля.	evt(config-ipsec-vpn)# enable track <ID>	<ID> – номер tracking-объекта, принимает значения [1..100];

Пример настройки

Задача:

Для подсети 192.168.0.0/24 организован виртуальный шлюз 192.168.0.1/24 с использованием протокола VRRP на основе аппаратных маршрутизаторов R1 и R2. Также между маршрутизаторами R1 и R2 есть линк с вырожденной подсетью 192.168.1.0/30. Подсеть 10.0.1.0/24 терминируется только на маршрутизаторе R2. ПК имеет IP-адрес 192.168.0.4/24 и шлюз по умолчанию 192.168.0.1.

Когда маршрутизатор R1 находится в состоянии vrrp backup, трафик от ПК в подсеть 10.0.1.0/24 пойдет без дополнительных настроек. Когда маршрутизатор R1 находится в состоянии vrrp master, необходим дополнительный маршрут для подсети 10.0.1.0/24 через интерфейс 192.168.1.2.



Исходные конфигурации маршрутизаторов:

Маршрутизатор R1

```
hostname R1
interface gigabitethernet 1/0/1
    switchport forbidden default-vlan
exit
interface gigabitethernet 1/0/1.741
    ip firewall disable
    ip address 192.168.0.2/24
    vrrp id 10
    vrrp ip 192.168.0.1/24
    vrrp
exit
interface gigabitethernet 1/0/2
    switchport forbidden default-vlan
exit
interface gigabitethernet 1/0/2.742
    ip firewall disable
    ip address 192.168.1.1/30
exit
```

Маршрутизатор R2

```
hostname R2
interface gigabitethernet 1/0/1
    switchport forbidden default-vlan
exit
interface gigabitethernet 1/0/1.741
    ip firewall disable
    ip address 192.168.0.3/24
    vrrp id 10
    vrrp ip 192.168.0.1/24
```

```

vrrp
exit
interface gigabitethernet 1/0/2
  switchport forbidden default-vlan
exit
interface gigabitethernet 1/0/2.742
  ip firewall disable
  ip address 192.168.1.2/30
exit
interface gigabitethernet 1/0/4
  ip firewall disable
  ip address 10.0.1.1/24
exit

```

Решение:

На маршрутизаторе R2 никаких изменений не требуется, так как подсеть 10.0.1.0/24 terminates на нем, и в момент, когда R2 выступает в роли vrrp master, пакеты будут переданы в соответствующий интерфейс. На маршрутизаторе необходимо создать маршрут для пакетов с IP-адресом назначения из сети 10.0.1.0/24 в момент, когда R1 выступает в роли vrrp master.

Для этого создадим track-object с соответствующим условием:

```

R1(config)# track 1
R1(config-track)# track vrrp id 10 state master
R1(config-track)# enable
R1(config-track)# exit

```

Создадим статический маршрут в подсеть 10.0.1.0/24 через 192.168.1.2, который будет работать в случае удовлетворения условия из track 1:

```

R1(config)# ip route 10.0.1.0/24 192.168.1.2 track 1

```

Настройка Firewall/NAT failover

Firewall failover необходим для резервирования сессий firewall.

 При включенном на устройстве firewall failover увеличивается потребление оперативной памяти на хранение firewall сессий.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перед настройкой сервисов резервирования необходимо настроить общие параметры failover.		
2	Переход в конфигурационное меню общих настроек failover-сервисов.	evt(config)# ip failover [vrf <VRF>]	<VRF> – имя VRF, задается строкой до 31 символа.

Шаг	Описание	Команда	Ключи
3	Установка IP-адреса, на котором failover-сервисы принимают failover-сообщения при работе в режиме резервирования.	evt(config-failover)# local-address { <ADDR> object-group <NETWORK_OBJ_GROUP_NAME> }	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве local address.
4	Установка многоадресного IP-адреса, который будет использоваться для обмена информацией при работе резервирования failover-сервисов в multicast-режиме.	evt(config-failover)# multicast-address <ADDR>	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];
5	Установка идентификатора multicast-группы для обмена информацией при работе резервирования failover-сервисов в multicast-режиме.	evt(config-failover)# multicast-group <GROUP>	<GROUP> – multicast-группа, указывается в диапазоне [1000..9999].
6	Установка IP-адреса, на который failover-сервисы отправляют failover-сообщения при работе в режиме резервирования.	evt(config-failover)# remote-address { <ADDR> object-group <NETWORK_OBJ_GROUP_NAME> }	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве local address.
7	Выбор VRRP-группы, по состоянию которой будет определяться мастерство при работе failover-сервисов в режиме Active-Standby.	evt(config-failover)# vrrp-group <GRID>	<GRID> – идентификатор группы VRRP-маршрутизатора, принимает значения [1..32].
8	Переход в конфигурационное меню настроек Firewall failover.	evt(config)# ip firewall failover [vrf <VRF>]	<VRF> – имя VRF, задается строкой до 31 символа.
9	Выбор режима обмена информацией между маршрутизаторами.	evt(config-firewall-failover)# sync-type <MODE>	<MODE> – режим обмена информацией: • unicast – режим unicast; • multicast – режим multicast.
10	Настройка номера UDP-порта службы резервирования сессий Firewall, через который происходит обмен информацией при работе в unicast-режиме (не обязательно).	evt(config-firewall-failover)# port <PORT>	<PORT> – номер порта службы резервирования сессий Firewall, указывается в диапазоне [1..65535].

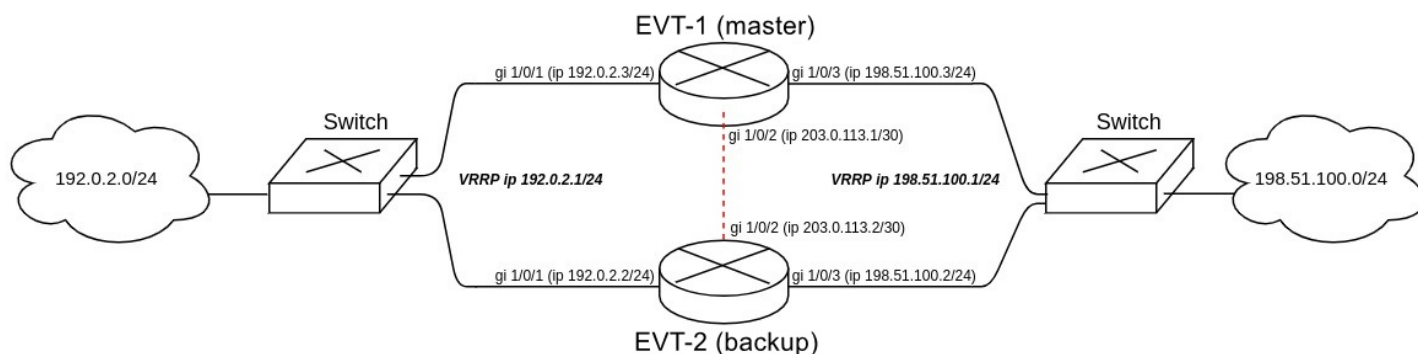
Шаг	Описание	Команда	Ключи
11	Включение резервирования сессий Firewall.	evt(config-firewall-failover)# enable	

⚠ При настройке firewall failover также будут синхронизироваться NAT-сессии между устройствами.

Пример настройки

Задача:

Настроить резервирование сессий firewall для VRRP-группы в unicast-режиме. Необходимо организовать резервирование для двух подсетей с помощью протокола VRRP, синхронизировать vrrp-процессы на маршрутизаторах.



Основные этапы решения задачи:

- 1) Необходимо настроить vrrp-процессы на маршрутизаторах. Для master будем использовать vrrp priority 20, для backup будем использовать vrrp priority 10.
- 2) Необходимо настроить firewall failover в режиме unicast с номером udp-порта 3333 для VRRP-группы.
- 3) Необходимо настроить зону безопасности для протокола vrrp и протокола udp.

Решение:

Настроим маршрутизатор EVT-1 (master).

Предварительно на интерфейсах настроим IP-адрес и определим принадлежность к зоне безопасности.

```

master(config)# interface gigabitethernet 1/0/1
master(config-if-gi)# security-zone trusted
master(config-if-gi)# ip address 192.0.2.3/24
master(config-if-gi)# exit
master(config)# interface gigabitethernet 1/0/2
master(config-if-gi)# security-zone trusted
master(config-if-gi)# ip address 203.0.113.1/30
master(config-if-gi)# exit
master(config)# interface gigabitethernet 1/0/3
master(config-if-gi)# security-zone trusted
master(config-if-gi)# ip address 198.51.100.3/24
master(config-if-gi)# exit

```

Настроим vrrp-процессы на интерфейсах. Необходимо настроить следующие параметры на интерфейсах маршрутизатора: идентификатор VRRP, IP-адрес VRRP, приоритет VRRP, принадлежность VRRP-маршрутизатора к группе.

Также дополнительно на master необходимо настроить vrrp preempt delay, в результате чего появится время на установление синхронизации firewall перед тем, как backup-маршрутизатор передаст мастерство.

После чего необходимо включить vrrp-процесс с помощью команды **vrrp**.

⚠ Вместо настройки vrrp preempt delay есть возможность выбора режима работы vrrp preempt disable, в результате которого маршрутизатор с более высоким vrrp-приоритетом не будет забирать мастерство у маршрутизатора с более низким vrrp-приоритетом после возвращения в работу.

⚠ На маршрутизаторе необходимо установить принадлежность vrrp-процессов к одной группе для синхронизации состояния vrrp-процессов (master, backup), а также для синхронизации сессий vrrp-процессов с помощью firewall failover.

```
master(config)# interface gigabitethernet 1/0/1
master(config-if-gi)# vrrp id 1
master(config-if-gi)# vrrp ip 192.0.2.1/24
master(config-if-gi)# vrrp priority 20
master(config-if-gi)# vrrp group 1
master(config-if-gi)# vrrp preempt delay 60
master(config-if-gi)# vrrp
master(config-if-gi)# exit
```

```
master(config)# interface gigabitethernet 1/0/3
master(config-if-gi)# vrrp id 3
master(config-if-gi)# vrrp ip 198.51.100.1/24
master(config-if-gi)# vrrp priority 20
master(config-if-gi)# vrrp group 1
master(config-if-gi)# vrrp preempt delay 60
master(config-if-gi)# vrrp
master(config-if-gi)# exit
```

Настроим общие параметры failover:

```
master(config)# ip failover
master(config-failover)# local-address 203.0.113.1
master(config-failover)# remote-address 203.0.113.2
master(config-failover)# vrrp-group 1
master(config-failover)# exit
```

Настроим firewall failover.

Выберем режим резервирование сессий unicast:

```
master(config)# ip firewall failover
master(config-firewall-failover)# sync-type unicast
```

Настроим номер UDP-порта службы резервирования сессий Firewall:

```
master(config-firewall-failover)# port 3333
```

Включим резервирования сессий Firewall:

```
master(config-firewall-failover)# enable
```

Для настройки правил зон безопасности потребуется создать профиль для порта firewall failover:

```
master(config)# object-group service failover
master(config-object-group-service)# port-range 3333
master(config-object-group-service)# exit
```

Дополнительно в security zone-pair trusted self необходимо разрешить следующие протоколы:

```
master(config)# security zone-pair trusted self
master(config-zone-pair)# rule 66
master(config-zone-pair-rule)# action permit
master(config-zone-pair-rule)# match protocol vrrp
master(config-zone-pair-rule)# enable
master(config-zone-pair-rule)# exit
master(config-zone-pair)# rule 67
master(config-zone-pair-rule)# action permit
master(config-zone-pair-rule)# match protocol udp
master(config-zone-pair-rule)# match destination-port failover
master(config-zone-pair-rule)# enable
master(config-zone-pair-rule)# exit
master(config-zone-pair)# exit
```

Посмотреть статус vrrp-процессов есть возможность с помощью следующей команды:

```
master# show vrrp
```

Virtual router	Virtual IP	Priority	Preemption	State	Inherit
Sync group ID					
-----	-----	-----	-----	-----	-----
1	192.0.2.1/24	20	Enabled	Master	--
1					
3	198.51.100.1/24	20	Enabled	Master	--
1					

Посмотреть состояние резервирования сессий Firewall есть возможность с помощью следующей команды:

```
master# show ip firewall failover
```

Communication	interface:	gigabitethernet 1/0/2
Status:		Running
Bytes sent:		2496
Bytes received:		640
Packets sent:		271
Packets received:		40
Send errors:		0
Receive errors:		0

Посмотреть состояние систем резервирования устройства есть возможность с помощью следующей команды:

```
master# show high-availability state
AP Tunnels:
  State:                Disabled
  Last state change:    --
DHCP server:
  State:                Disabled
  Last state change:    --
Firewall sessions:
  State:                successful synchronization
  Last synchronization: 09:38:00 05.08.2021
```

Настроим маршрутизатор EVT-2 (backup).

Настройка интерфейсов:

```
backup(config)# interface gigabitethernet 1/0/1
backup(config-if-gi)# security-zone trusted
backup(config-if-gi)# ip address 192.0.2.2/24
backup(config-if-gi)# vrrp id 1
backup(config-if-gi)# vrrp ip 192.0.2.1/24
backup(config-if-gi)# vrrp priority 10
backup(config-if-gi)# vrrp group 1
backup(config-if-gi)# vrrp
backup(config-if-gi)# exit
```

```
backup(config)# interface gigabitethernet 1/0/2
backup(config-if-gi)# security-zone trusted
backup(config-if-gi)# ip address 203.0.113.2/30
backup(config-if-gi)# exit
```

```
backup(config)# interface gigabitethernet 1/0/3
backup(config-if-gi)# security-zone trusted
backup(config-if-gi)# ip address 198.51.100.2/24
backup(config-if-gi)# vrrp id 3
backup(config-if-gi)# vrrp ip 198.51.100.1/24
backup(config-if-gi)# vrrp priority 10
backup(config-if-gi)# vrrp group 1
backup(config-if-gi)# vrrp
backup(config-if-gi)# exit
```

Настройка firewall failover:

```
backup(config)# ip failover
backup(config-failover)# local-address 203.0.113.2
backup(config-failover)# remote-address 203.0.113.1
backup(config-failover)# vrrp-group 1
backup(config-failover)# exit
backup(config)# ip firewall failover
backup(config-firewall-failover)# sync-type unicast
backup(config-firewall-failover)# port 3333
backup(config-firewall-failover)# enable
```

Настройка зоны безопасности аналогична настройке на маршрутизаторе EVT-1 (master).

Настройка DHCP failover

DHCP failover используется для резервирования базы IP-адресов, которые были динамически выданы в процессе работы DHCP-server.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перед настройкой сервисов резервирования необходимо настроить общие параметры failover.		
2	Переход в конфигурационное меню общих настроек failover-сервисов.	evt(config)# ip failover [vrf <VRF>]	<VRF> – имя VRF, задается строкой до 31 символа;
3	Установка IP-адреса, на котором failover-сервисы принимают failover-сообщения при работе в режиме резервирования.	evt(config-failover)# local-address { <ADDR> object-group <NETWORK_OBJ_GROUP_NAME> }	<ADDR> – IP-адрес, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве local address.
4	Установка IP-адреса, на который failover сервисы отправляют failover-сообщения при работе в режиме резервирования.	evt(config-failover)# remote-address { <ADDR> object-group <NETWORK_OBJ_GROUP_NAME> }	<ADDR> – IP-адрес, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве local address.
5	Выбор VRRP-группы, по состоянию которой будет определяться мастерство при работе failover сервисов в режиме Active-Standby.	evt(config-failover)# vrrp-group <GRID>	<GRID> – идентификатор группы VRRP-маршрутизатора, принимает значения [1..32].
6	Переход в конфигурационное меню DHCP failover для его настройки.	evt(config)# ip dhcp-server failover [vrf <VRF>]	<VRF> – имя VRF, задается строкой до 31 символа;
7	Выбор режима работы DHCP failover.	evt(config-dhcp-server-failover)# mode { active-active active-standby }	active-active – режим работы с двумя активными маршрутизаторами; active-standby – режим работы с одним активным маршрутизатором и одним резервным.

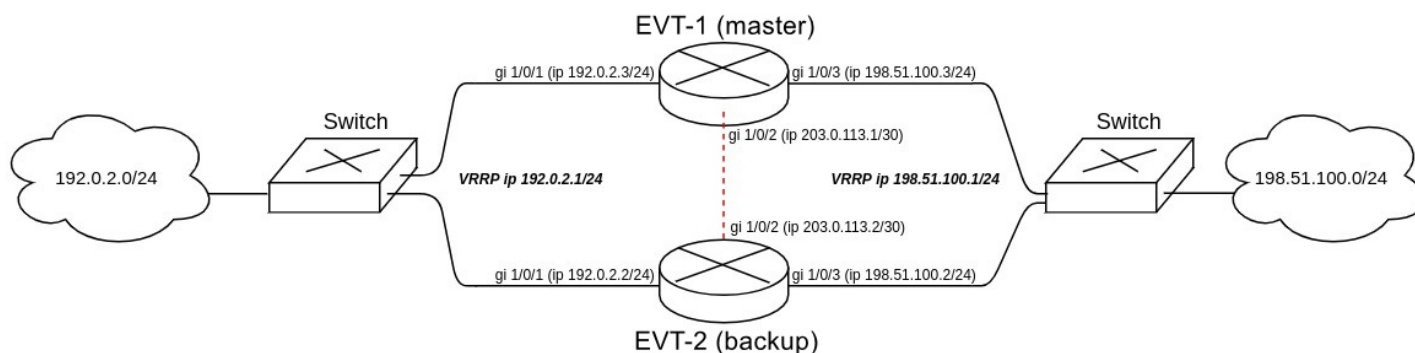
Шаг	Описание	Команда	Ключи
8	Настройка роли DHCP failover, при работе резервирования в режиме Active-Active.	evt(config-dhcp-server-failover)# role <ROLE>	<ROLE> – роль DHCP-сервера при работе в режиме резервирования: • primary – режим активного DHCP-сервера; • secondary – режим резервного DHCP-сервера.
9	Включение резервирования DHCP failover.	evt(config-dhcp-server-failover)# enable	

⚠ Режим active-standby не поддерживан в VRF.

Пример настройки

Задача:

Настроить резервирование DHCP-сервера в режиме Active-Standby. Необходимо организовать резервирование для двух подсетей с помощью протокола VRRP, синхронизировать vrrp-процессы на маршрутизаторах.



Основные этапы решения задачи:

- 1) Необходимо настроить vrrp-процессы на маршрутизаторах. Для master будем использовать vrrp priority 20, для backup будем использовать vrrp priority 10.
- 2) Необходимо настроить DHCP failover в режиме Active-Standby.
- 3) Необходимо настроить зону безопасности для протоколов vrrp, udp и tcp.

Решение:**1. Настройка маршрутизатора EVT-1 (master).**

Предварительно на интерфейсах настроим IP-адрес и определим принадлежность к зоне безопасности.

```

master(config)# interface gigabitethernet 1/0/1
master(config-if-gi)# security-zone trusted
master(config-if-gi)# ip address 192.0.2.3/24
master(config-if-gi)# exit
master(config)# interface gigabitethernet 1/0/2
master(config-if-gi)# security-zone trusted
master(config-if-gi)# ip address 203.0.113.1/30
master(config-if-gi)# exit
master(config)# interface gigabitethernet 1/0/3
master(config-if-gi)# security-zone trusted
master(config-if-gi)# ip address 198.51.100.3/24
master(config-if-gi)# exit

```

Настроим vrrp-процессы на интерфейсах. Необходимо настроить следующие параметры на интерфейсах маршрутизатора: идентификатор VRRP, IP-адрес VRRP, приоритет VRRP, принадлежность VRRP-маршрутизатора к группе.

После чего необходимо включить vrrp-процесс с помощью команды "vrrp".

⚠ Вместо настройки vrrp preempt delay есть возможность выбора режима работы vrrp preempt disable, в результате которого маршрутизатор с более высоким vrrp-приоритетом не будет забирать мастерство у маршрутизатора с более низким vrrp-приоритетом после возвращения в работу.

⚠ На маршрутизаторе необходимо установить принадлежность vrrp-процессов к одной группе для синхронизации состояния vrrp-процессов (master, backup).

```

master(config)# interface gigabitethernet 1/0/1
master(config-if-gi)# vrrp id 1
master(config-if-gi)# vrrp ip 192.0.2.1/24
master(config-if-gi)# vrrp priority 20
master(config-if-gi)# vrrp group 1
master(config-if-gi)# vrrp
master(config-if-gi)# exit
master(config)# interface gigabitethernet 1/0/3
master(config-if-gi)# vrrp id 3
master(config-if-gi)# vrrp ip 198.51.100.1/24
master(config-if-gi)# vrrp priority 20
master(config-if-gi)# vrrp group 1
master(config-if-gi)# vrrp
master(config-if-gi)# exit

```

Настроим DHCP failover. Для DHCP failover необходимо настроить следующие параметры: mode, local-address, remote-address, принадлежность VRRP-маршрутизатора к группе.

```
master(config)# ip dhcp-server pool LAN
master(config-dhcp-server)# network 192.0.2.0/24
master(config-dhcp-server)# address-range 192.0.2.10-192.0.2.20
master(config-dhcp-server)# exit
master(config)# ip dhcp-server
master(config)# ip failover
master(config-failover)# local-address 203.0.113.1
master(config-failover)# remote-address 203.0.113.2
master(config-failover)# vrrp-group 1
master(config-failover)# exit
master(config)# ip dhcp-server failover
master(config-dhcp-server-failover)# mode active-standby
master(config-dhcp-server-failover)# enable
master(config-dhcp-server-failover)# exit
```

⚠ Для запуска DHCP failover необходимо предварительно настроить и включить DHCP-server, который будет резервироваться.

Для настройки правил зон безопасности потребуется создать профиль для порта DHCP failover:

```
master(config)# object-group service dhcp_failover
master(config-object-group-service)# port-range 873
master(config-object-group-service)# exit
```

⚠ DHCP failover для синхронизации использует TCP-порт 873, его необходимо разрешить при настройке firewall.

Дополнительно в security zone-pair trusted self необходимо разрешить следующие протоколы:

```
master(config)# security zone-pair trusted self
master(config-zone-pair)# rule 66
master(config-zone-pair-rule)# action permit
master(config-zone-pair-rule)# match protocol vrrp
master(config-zone-pair-rule)# enable
master(config-zone-pair-rule)# exit
master(config-zone-pair)# rule 67
master(config-zone-pair-rule)# action permit
master(config-zone-pair-rule)# match protocol tcp
master(config-zone-pair-rule)# match destination-port dhcp_failover
master(config-zone-pair-rule)# enable
master(config-zone-pair-rule)# exit
master(config-zone-pair)# rule 68
master(config-zone-pair-rule)# action permit
master(config-zone-pair-rule)# match protocol udp
master(config-zone-pair-rule)# enable
master(config-zone-pair-rule)# exit
```

Посмотреть статус vrrp-процессов есть возможность с помощью следующей команды:

```
master# show vrrp
Virtual router    Virtual IP          Priority    Preemption    State    Inherit
Sync group ID
-----
1                192.0.2.1/24       20         Enabled      Master   --
1
3                198.51.100.1/24    20         Enabled      Master   --
1
```

Посмотреть состояние резервирования сессий Firewall есть возможность с помощью следующей команды:

```
master# show ip dhcp server failover
VRF:      --
State: Successful
```

Посмотреть состояние систем резервирования устройства есть возможность с помощью следующей команды:

```
master# show high-availability state
AP Tunnels:
  State:                Disabled
  Last state change:    --
DHCP option 82 table:
  State:                Disabled
  Last state change:    --
DHCP server:
VRF:      --
  State:                Successful synchronization
  State:                Disabled
  Last synchronization: --
```

 Для успешной синхронизации сервиса DHCP failover на устройствах должно быть выставлено идентичное время.

2. Настройка маршрутизатора EVT-2 (backup).

Настройка интерфейсов:

```
backup(config)# interface gigabitethernet 1/0/1
backup(config-if-gi)# security-zone trusted
backup(config-if-gi)# ip address 192.0.2.2/24
backup(config-if-gi)# vrrp id 1
backup(config-if-gi)# vrrp ip 192.0.2.1/24
backup(config-if-gi)# vrrp priority 20
backup(config-if-gi)# vrrp group 1
backup(config-if-gi)# vrrp
backup(config-if-gi)# exit
backup(config)# interface gigabitethernet 1/0/2
backup(config-if-gi)# security-zone trusted
backup(config-if-gi)# ip address 203.0.113.2/30
backup(config-if-gi)# exit
backup(config)# interface gigabitethernet 1/0/3
backup(config-if-gi)# security-zone trusted
backup(config-if-gi)# ip address 198.51.100.2/24
backup(config-if-gi)# vrrp id 3
backup(config-if-gi)# vrrp ip 198.51.100.1/24
backup(config-if-gi)# vrrp priority 10
backup(config-if-gi)# vrrp group 1
backup(config-if-gi)# vrrp
backup(config-if-gi)# exit
```

Настройка DHCP failover:

```
backup(config)# ip dhcp-server pool LAN
backup(config-dhcp-server)# network 192.0.2.0/24
backup(config-dhcp-server)# address-range 192.0.2.10-192.0.2.20
backup(config-dhcp-server)# exit
backup(config)# ip dhcp-server
backup(config)# ip failover
backup(config-failover)# local-address 203.0.113.2
backup(config-failover)# remote-address 203.0.113.1
backup(config-failover)# vrrp-group 1
backup(config-failover)# exit
backup(config)# ip dhcp-server failover
backup(config-dhcp-server-failover)# mode active-standby
backup(config-dhcp-server-failover)# enable
backup(config-dhcp-server-failover)# exit
```

Настройка зоны безопасности аналогична настройке на маршрутизаторе EVT-1 (master).

6.2.8 Управление сервисами

- [Настройка DHCP-сервера](#)
 - [Алгоритм настройки](#)
 - [Пример настройки](#)
- [Конфигурирование Destination NAT](#)
 - [Алгоритм настройки](#)
 - [Пример настройки Destination NAT](#)
- [Конфигурирование Source NAT](#)
 - [Алгоритм настройки](#)
 - [Пример настройки 1](#)
 - [Пример настройки 2](#)
- [Конфигурирование Static NAT](#)
 - [Алгоритм настройки](#)
 - [Пример настройки Static NAT](#)
- [Настройка NTP](#)
 - [Алгоритм настройки](#)
 - [Пример настройки](#)

Настройка DHCP-сервера

Встроенный DHCP-сервер маршрутизатора может быть использован для настройки сетевых параметров устройств в локальной сети. DHCP-сервер маршрутизаторов способен передавать дополнительные опции на сетевые устройства, например:

- default-router – IP-адрес маршрутизатора, используемого в качестве шлюза по умолчанию;
- domain-name – доменное имя, которое должен будет использовать клиент при разрешении имен хостов через Систему Доменных Имен (DNS);
- dns-server – список адресов серверов доменных имен в данной сети, о которых должен знать клиент. Адреса серверов в списке располагаются в порядке убывания предпочтения.

 **Конфигурация на маршрутизаторах EVT и EVS производится с помощью одинаковых команд. Ниже приведены примеры настройки EVT.**

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Включить IPv4/IPv6 DHCP-сервер.	evt(config)# ip dhcp-server [vrf <VRF>]	<VRF> – имя экземпляра VRF, в рамках которого будет работать DHCP-сервер. Задается строкой до 31 символа.
		evt(config)# ipv6 dhcp-server [vrf <VRF>]	
2	Задать значение кода DSCP для использования в IP-заголовке исходящих пакетов DHCP-сервера (не обязательно).	evt(config)# ip dhcp-server dscp <DSCP>	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 61.

Шаг	Описание	Команда	Ключи
3	Создать пул IPv4/IPv6-адресов DHCP-сервера и перейти в режим его конфигурирования.	evt(config)# ip dhcp-server pool <NAME> [vrf <VRF>]	<NAME> – имя пула IPv4/IPv6-адресов DHCP-сервера, задаётся строка до 31 символа. <VRF> – имя экземпляра VRF, в рамках которого будет работать данный пул IP-адресов DHCP-сервера. Задаётся строкой до 31 символа
		evt(config)# ipv6 dhcp-server pool <NAME> [vrf <VRF>]	
4	Задать IPv4/IPv6-адрес и маску для подсети, из которой будет выделен пул IPv4/IPv6-адресов.	evt(config-dhcp-server)# network <ADDR/LEN>	<ADDR/LEN> – IP-адрес и префикс подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].
		evt(config-ipv6-dhcp-server)# network <IPV6-ADDR/LEN>	
5	Добавить диапазон IPv4/IPv6-адресов к пулу адресов, конфигурируемого DHCP-сервера.	evt(config-dhcp-server)# address-range <FROM-ADDR>-<TO-ADDR>	<FROM-ADDR> – начальный IP-адрес диапазона; <TO-ADDR> – конечный IP-адрес диапазона, Адреса задаются в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Можно указать до 32 диапазонов IP-адресов, список задаётся через запятую.

Шаг	Описание	Команда	Ключи
		evt(config-ipv6-dhcp-server)# address-range <FROM-ADDR>-<TO-ADDR>	<FROM-ADDR> – начальный IPv6-адрес диапазона; <TO-ADDR> – конечный IP-адрес диапазона; Адреса задаются в виде X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
6	Добавить IPv4/IPv6-адрес для определенного физического адреса к пулу адресов конфигурируемого DHCP-сервера (не обязательно).	evt(config-dhcp-server)# address <ADDR> {mac-address <MAC> client-identifier <CI>}	<ADDR> – IP-адрес клиента, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <MAC> – MAC-адрес клиента, которому будет выдан IP-адрес, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]. <CI> – идентификатор клиента согласно DHCP Option 61. Может быть задан в одном из следующих видов: • HH:HH:HH:HH:HH:HH:HH:HH: – идентификатор клиента в шестнадцатеричной форме и MAC-адрес клиента; • STRING – текстовая строка длиной от 1 до 64 символов.
		evt(config-ipv6-dhcp-server)# address <ADDR> mac-address <MAC>	<IPv6-ADDR> – IPv6-адрес клиента, задаётся в виде X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <MAC> – MAC-адрес клиента, которому будет выдан IPv6-адрес, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF].

Шаг	Описание	Команда	Ключи
7	Задать список IPv4-адресов шлюзов по умолчанию, которые DHCP-сервер будет сообщать клиентам, используя DHCP-опцию 3.	evt(config-dhcp-server)# default-router <ADDR>	<ADDR> – IP-адрес шлюза по умолчанию, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Можно указать до 8 IP-адресов, список задаётся через запятую.
8	Задать DNS-имя сетевого домена. Имя домена передаётся клиентам в составе DHCP-опции 15 (не обязательно).	evt(config-dhcp-server)# domain-name <NAME> evt(config-ipv6-dhcp-server)# domain-name <NAME>	<NAME> – DNS-имя домена клиента, задаётся строкой до 255 символов.
9	Задать список IPv4/IPv6-адресов DNS-серверов. Список передаётся клиентам в составе DHCP-опции 6 (не обязательно).	evt(config-dhcp-server)# dns-server <ADDR> evt(config-ipv6-dhcp-server)# dns-server <IPv6-ADDR>	<ADDR> – IP-адрес DNS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Можно указать до 8 IP-адресов, список задаётся через запятую. <IPv6-ADDR> – IPv6-адрес DNS-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. Можно указать до 8 IPv6-адресов, список задаётся через запятую.
10	Задать максимальное время аренды IP-адресов (не обязательно). Если DHCP-клиент запрашивает время аренды, превосходящее максимальное значение, то будет установлено время, заданное этой командой.	evt(config-dhcp-server)# max-lease-time <TIME> evt(config-ipv6-dhcp-server)# max-lease-time <TIME>	<TIME> – максимальное время аренды IP-адреса, задаётся в формате DD:HH:MM, где: - DD – количество дней, принимает значения [0..364]; - HH – количество часов, принимает значения [0..23]; - MM – количество минут, принимает значения [0..59]. Значение по умолчанию: 1 день.

Шаг	Описание	Команда	Ключи
11	Задать время аренды, на которое клиенту будет выдан IP-адрес (не обязательно). Данное время будет использоваться если клиент не запрашивал определенное время аренды.	evt(config-dhcp-server)# default-lease-time <TIME>	<TIME> – максимальное время аренды IP-адреса, задаётся в формате DD:HH:MM, где: • DD – количество дней, принимает значения [0..364]; • HH – количество часов, принимает значения [0..23]; • MM – количество минут, принимает значения [0..59]. Значение по умолчанию: 12 часов.
		evt(config-ipv6-dhcp-server)# default-lease-time <TIME>	
12	Создать идентификатор класса поставщика (DHCP Опция 60) (не обязательно).	evt(config)# ip dhcp-server vendor-class-id <NAME>	<NAME> – идентификатор класса поставщика, задаётся строкой до 31 символа.
		evt(config)# ipv6 dhcp-server vendor-class-id <NAME>	
13	Задать специфическую информацию поставщика (DHCP Опция 43).	evt(config-dhcp-vendor-id)# vendor-specific-options <HEX>	<HEX> – специфическая информация поставщика, задаётся в шестнадцатеричном формате до 128 символов.
		evt(config-ipv6-dhcp-vendor-id)# vendor-specific-options <HEX>	
14	Задать IP-адрес NetBIOS-сервера (DHCP опция 44) (не обязательно).	evt(config-dhcp-server)# netbios-nameserver <ADDR>	<ADDR> – IP-адрес NetBIOS-сервера задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Можно задать до 4 IP-адресов.
15	Задать IP-адрес tftp-сервера (DHCP Option 150) (не обязательно).	evt(config-dhcp-server)# tftp-server <ADDR>	<ADDR> – IP-адрес DNS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

 Для продления ресурса внутреннего flash-накопителя информация о выданных сервером IP-адресах хранится в энергозависимой памяти. Поэтому стоит учитывать, что при перезагрузке маршрутизатора сервер начинает выдавать адреса заново. Занятость адресов будет проверяться с помощью ICMP-запросов.

Пример настройки

Задача:

Настроить работу DHCP-сервера в локальной сети, относящейся к зоне безопасности «trusted». Задать пул IP-адресов из подсети 192.168.1.0/24 для раздачи клиентам. Задать время аренды адресов 1 день. Настроить передачу клиентам маршрута по умолчанию, доменного имени и адресов DNS-серверов с помощью DHCP-опций.

Решение:

Создадим зону безопасности «trusted» и установим принадлежность используемых сетевых интерфейсов к зонам:

```
evt# configure
evt(config)# security zone trusted
evt(config-zone)# exit
```

Создадим пул адресов с именем «Simple» и добавим в данный пул адресов диапазон IP-адресов для выдачи в аренду клиентам сервера. Укажем параметры подсети, к которой принадлежит данный пул, и время аренды для выдаваемых адресов:

```
evt# configure
evt(config)# ip dhcp-server pool Simple
evt(config-dhcp-server)# network 192.168.1.0/24
evt(config-dhcp-server)# address-range 192.168.1.100-192.168.1.125
evt(config-dhcp-server)# default-lease-time 1:00:00
```

Сконфигурируем передачу клиентам дополнительных сетевых параметров:

- маршрут по умолчанию: 192.168.1.1;
- имя домена: eltex.loc;
- список DNS-серверов: DNS1: 172.16.0.1, DNS2: 8.8.8.8.

```
evt(config-dhcp-server)# domain-name "eltex.loc"
evt(config-dhcp-server)# default-router 192.168.1.1
evt(config-dhcp-server)# dns-server 172.16.0.1,8.8.8.8
evt(config-dhcp-server)# exit
```

Для того чтобы DHCP-сервер мог раздавать IP-адреса из конфигурируемого пула, на маршрутизаторе должен быть создан IP-интерфейс, принадлежащий к той же подсети, что и адреса пула.

```
evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# security-zone trusted
evt(config-if-gi)# ip address 192.168.1.1/24
evt(config-if-gi)# exit
```

Для разрешения прохождения сообщений протокола DHCP к серверу необходимо создать соответствующие профили портов, включающие порт источника 68 и порт назначения 67, используемые протоколом DHCP, и создать разрешающее правило в политике безопасности для прохождения пакетов протокола UDP:

```

evt(config)# object-group service dhcp_server
evt(config-object-group-service)# port-range 67
evt(config-object-group-service)# exit
evt(config)# object-group service dhcp_client
evt(config-object-group-service)# port-range 68
evt(config-object-group-service)# exit
evt(config)# security zone-pair trusted self
evt(config-zone-pair)# rule 30
evt(config-zone-rule)# match protocol udp
evt(config-zone-rule)# match source-port object-group dhcp_client
evt(config-zone-rule)# match destination-port object-group dhcp_server
evt(config-zone-rule)# action permit
evt(config-zone-rule)# enable
evt(config-zone-rule)# exit
evt(config-zone-pair)# exit

```

Разрешим работу сервера:

```

evt(config)# ip dhcp-server
evt(config)# exit

```

Просмотреть список арендованных адресов можно с помощью команды:

```

evt# show ip dhcp binding

```

Просмотреть сконфигурированные пулы адресов можно командами:

```

evt# show ip dhcp server pool
evt# show ip dhcp server pool Simple

```

 Конфигурирование настроек для IPv6 производится по аналогии с IPv4.

Конфигурирование Destination NAT

Функция Destination NAT (DNAT) состоит в преобразовании IP-адреса назначения у пакетов, проходящих через сетевой шлюз.

DNAT используется для перенаправления трафика, идущего на некоторый «виртуальный» адрес в публичной сети, на «реальный» сервер в локальной сети, находящийся за сетевым шлюзом. Эту функцию можно использовать для организации публичного доступа к серверам, находящимся в частной сети и не имеющим публичного сетевого адреса.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим настройки сервиса трансляции адресов получателя.	evt(config)# nat destination	
2	Создать пул IP-адресов и/или TCP/UDP-портов с определённым именем (не обязательно).	evt(config-dnat)# pool <NAME>	<NAME> – имя пула NAT-адресов, задаётся строкой до 31 символа.
3	Установить внутренний IP-адрес, на который будет заменяться IP-адрес получателя.	evt(config-dnat-pool)# ip address <ADDR>	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
4	Установить внутренний TCP/UDP-порт, на который будет заменяться TCP/UDP-порт получателя.	evt(config-dnat-pool)# ip port <PORT>	<PORT> – TCP/UDP-порт, принимает значения [1..65535].
5	Создать группу правил с определённым именем.	evt(config-dnat)# ruleset <NAME>	<NAME> – имя группы правил, задаётся строкой до 31 символа.
6	Указать экземпляр VRF, в котором будет работать данная группа правил (не обязательно).	evt(config-dnat-ruleset)# ip vrf forwarding <VRF>	<VRF> – имя VRF, задается строкой до 31 символа.
7	Задать область применения группы правил. Правила будут применяться только для трафика, идущего из определенной зоны или интерфейса.	evt(config-dnat-ruleset)# from { zone <NAME> interface <IF> tunnel <TUN> default }	<NAME> – имя зоны изоляции; <IF> – имя интерфейса устройства; <TUN> – имя туннеля устройства. default – обозначает группу правил для всего трафика, источник которого не попал под критерии других групп правил.
8	Задать правило с определённым номером. Правила обрабатываются в порядке возрастания.	evt(config-dnat-ruleset)# rule <ORDER>	<ORDER> – номер правила, принимает значения [1...10000].

9	Задать IP-адреса {отправителя получателя}, для которых должно срабатывать правило.	<pre> evt(config-dnat-rule)# match [not] {source destination}-address <TYPE> {<FROM-ADDR> - <TO- ADDR> <OBJ-GROUP-NAME> <ADDR/LEN>} </pre>	<TYPE> – тип аргумента, устанавливаемый в качестве адреса: • address-range – указать диапазон IPv4/IPv6 адресов; • object-group – указать имя профиля; • prefix – указать адрес подсети и префикс; • any – установить в качестве адреса любой адрес. <FROM-ADDR> – начальный IP-адрес диапазона; <TO-ADDR> – конечный IP-адрес диапазона; <OBJ-GROUP-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа; <ADDR/LEN> – IP-адрес и маска подсети сервера.
10	Задать сервисы (TCP/UDP-портов) {отправителя получателя}, для которых должно срабатывать правило (не обязательно).	<pre> evt(config-dnat-rule)# match [not] {source destination}-port <TYPE> {<PORT-SET-NAME> <FORM- PORT> - <TO-PORT>} </pre>	<TYPE> – тип аргумента, устанавливаемый в качестве адреса: • address-range – указать диапазон IPv4/IPv6 адресов; • object-group – указать имя профиля; • any – установить в качестве адреса любой адрес. <PORT-SET-NAME> – имя профиля порта, задаётся строкой до 31 символа; <FROM-PORT> – начальный порт диапазона; <TO-PORT> – конечный порт диапазона.

11	Установить имя или номер IP-протокола, для которого должно срабатывать правило (не обязательно).	evt(config-dnat-rule)# match [not] {protocol <TYPE> protocol-id <ID> }	<TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre. Значение «any» указывает на любой тип протокола. <ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF].
12	Задать тип и код сообщений протокола ICMP, для которых должно срабатывать правило (если в качестве протокола выбран ICMP) (не обязательно).	evt(config-dnat-rule)# match [not] icmp {<ICMP_TYPE><ICMP_CODE> <TYPE-NAME>}	<ICMP_TYPE> – тип сообщения протокола ICMP, принимает значения [0..255]. <ICMP_CODE> – код сообщения протокола ICMP, принимает значения [0..255]. Значение «any» указывает на любой код сообщения. <TYPE-NAME> – имя типа ICMP-сообщения.
13	Задать действие «трансляция адреса и порта получателя» для трафика, удовлетворяющего критериям, заданным командами «match».	evt(config-dnat-rule)# action destination-nat { off pool <NAME> netmap <ADDR/LEN> }	off – трансляция отключена; pool <NAME> – имя пула, содержащего набор IP-адресов и/или TCP/UDP-портов; netmap <ADDR/LEN> – IP-адрес и маска подсети, используемые при трансляции. Параметр задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].
14	Активировать конфигурируемое правило.	evt(config-dnat-rule)# enable	

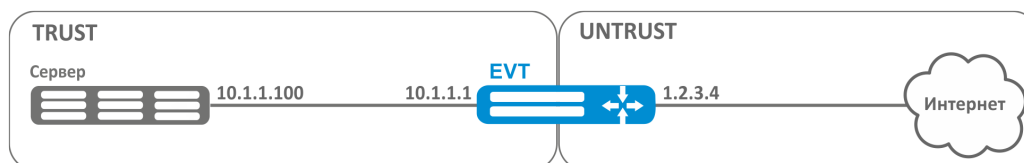
15	Включить функцию отслеживания сессий уровня приложений для протоколов FTP, SIP, H323, netbios-ns, PPTP (не обязательно).	evt(config)# ip firewall sessions tracking {<PROTOCOL> sip [port <OBJECT-GROUP-SERVICE>] all}	all – включает функцию отслеживания сессий уровня приложений для всех доступных протоколов; <PROTOCOL> – протокол уровня приложений, сессии которого должны отслеживаться, принимает значения [ftp, h323, pptp, netbios-ns]; <OBJECT-GROUP-SERVICE> – имя профиля TCP/UDP-портов sip-сессии, задаётся строкой до 31 символа. Если группа не указана, то отслеживание сессий sip будет осуществляться для порта 5060.
16	Включить функцию трансляции IP-адресов в заголовках уровня приложений (не обязательно).	evt(config)# nat alg {<PROTOCOL> all}	all – включает трансляцию IP-адресов в заголовках всех доступных протоколов. <PROTOCOL> – протокол уровня приложений, в заголовках которого должна работать трансляция адресов, принимает значения [ftp, h323, pptp, netbios-ns, gre, sip, tftp].

⚠ При использовании ключа *not* правило будет срабатывать для значений, которые не входят в указанный профиль.
Каждая команда «match» может содержать ключ «not». При использовании данного ключа под правило будут подпадать пакеты, не удовлетворяющие заданному критерию.
Более подробная информация о командах для настройки маршрутизатора содержится в справочнике команд CLI.

Пример настройки Destination NAT

Задача:

Организовать доступ из публичной сети, относящейся к зоне «UNTRUST», к серверу локальной сети в зоне «TRUST». Адрес сервера в локальной сети – 10.1.1.100. Сервер должен быть доступным извне по адресу 1.2.3.4, доступный порт 80.



Решение:

Создадим зоны безопасности «UNTRUST» и «TRUST». Установим принадлежность используемых сетевых интерфейсов к зонам. Одновременно назначим IP-адреса интерфейсам.

```

evt# configure
evt(config)# security zone UNTRUST
evt(config-zone)# exit
evt(config)# security zone TRUST
evt(config-zone)# exit
evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# security-zone TRUST
evt(config-if-gi)# ip address 10.1.1.1/25
evt(config-if-gi)# exit
evt(config)# interface tengigabitethernet 1/0/1
evt(config-if-te)# ip address 1.2.3.4/29
evt(config-if-te)# security-zone UNTRUST
evt(config-if-te)# exit

```

Создадим профили IP-адресов и портов, которые потребуются для настройки правил Firewall и правил DNAT.

- NET_UPLINK – профиль адресов публичной сети;
- SERVER_IP – профиль адресов локальной сети;
- SRV_HTTP – профиль портов.

```

evt(config)# object-group network NET_UPLINK
evt(config-object-group-network)# ip address 1.2.3.4
evt(config-object-group-network)# exit

```

```

evt(config)# object-group service SRV_HTTP
evt(config-object-group-service)# port 80
evt(config-object-group-service)# exit

```

```

evt(config)# object-group network SERVER_IP
evt(config-object-group-network)# ip address 10.1.1.100
evt(config-object-group-network)# exit

```

Войдем в режим конфигурирования функции DNAT и создадим пул адресов и портов назначения, в которые будут транслироваться адреса пакетов, поступающие на адрес 1.2.3.4 из внешней сети.

```

evt(config)# nat destination
evt(config-dnat)# pool SERVER_POOL
evt(config-dnat-pool)# ip address 10.1.1.100
evt(config-dnat-pool)# ip port 80
evt(config-dnat-pool)# exit

```

Создадим набор правил «DNAT», в соответствии с которыми будет производиться трансляция адресов. В атрибутах набора укажем, что правила применяются только для пакетов, пришедших из зоны «UNTRUST». Набор правил включает в себя требования соответствия данных по адресу и порту назначения (match destination-address, match destination-port) и по протоколу. Кроме этого в наборе

задано действие, применяемое к данным, удовлетворяющим всем правилам (action destination-nat). Набор правил вводится в действие командой **enable**.

```

evt(config-dnat)# ruleset DNAT
evt(config-dnat-ruleset)# from zone UNTRUST
evt(config-dnat-ruleset)# rule 1
evt(config-dnat-rule)# match destination-address object-group NET_UPLINK
evt(config-dnat-rule)# match protocol tcp
evt(config-dnat-rule)# match destination-port object-group SRV_HTTP
evt(config-dnat-rule)# action destination-nat pool SERVER_POOL
evt(config-dnat-rule)# enable
evt(config-dnat-rule)# exit
evt(config-dnat-ruleset)# exit
evt(config-dnat)# exit

```

Для пропуска трафика, идущего из зоны «UNTRUST» в «TRUST», создадим соответствующую пару зон. Пропускать следует только трафик с адресом назначения, соответствующим заданному в профиле «SERVER_IP» и прошедший преобразование DNAT.

```

evt(config)# security zone-pair UNTRUST TRUST
evt(config-zone-pair)# rule 1
evt(config-zone-pair-rule)# match destination-address object-group SERVER_IP
evt(config-zone-pair-rule)# match destination-nat
evt(config-zone-pair-rule)# action permit
evt(config-zone-pair-rule)# enable
evt(config-zone-pair-rule)# exit
evt(config-zone-pair)# exit
evt(config)# exit

```

Произведенные настройки можно посмотреть с помощью команд:

```

evt# show ip nat destination pools
evt# show ip nat destination rulesets
evt# show ip nat proxy-arp
evt# show ip nat translations

```

Конфигурирование Source NAT

Функция Source NAT (SNAT) используется для подмены адреса источника у пакетов, проходящих через сетевой шлюз. При прохождении пакетов из локальной сети в публичную сеть адрес источника заменяется на один из публичных адресов шлюза. Дополнительно к адресу источника может применяться замена порта источника. При прохождении пакетов из публичной сети в локальную происходит обратная подмена адреса и порта.

Функция SNAT может быть использована для предоставления доступа в Интернет компьютерам, находящимся в локальной сети. При этом не требуется назначения публичных IP-адресов этим компьютерам.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим настройки сервиса трансляции адресов отправителя.	evt(config)# nat source	

Шаг	Описание	Команда	Ключи
2	Создать пул IP-адресов и/или TCP/UDP-портов с определённым именем (не обязательно).	evt(config-snat)# pool <NAME>	<NAME> – имя пула NAT-адресов, задаётся строкой до 31 символа.
3	Установить диапазон IP-адресов, для которых будет заменяться IP-адрес отправителя.	evt(config-snat-pool)# ip address-range <IP>[-<ENDIP>]	<IP> – IP-адрес начала диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <ENDIP> – IP-адрес конца диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Если не указывать IP-адрес конца диапазона, то в качестве IP-адреса для трансляции используется только IP-адрес начала диапазона.
4	Задать диапазон внешних TCP/UDP-портов, на которые будет заменяться TCP/UDP-порт отправителя.	evt(config-snat-pool)# ip port-range <PORT>[-<ENDPORT>]	<PORT> – TCP/UDP-порт начала диапазона, принимает значения [1..65535]; <ENDPORT> – TCP/UDP-порт конца диапазона, принимает значения [1..65535]. Если не указывать TCP/UDP-порт конца диапазона, то в качестве TCP/UDP-порта для трансляции используется только TCP/UDP-порт начала диапазона.
5	Установить внешний TCP/UDP-порт, на который будет заменяться TCP/UDP-порт отправителя.	evt(config-snat-pool)# ip port <PORT>	<PORT> – TCP/UDP-порт, принимает значения [1..65535].
6	Включить функции NAT persistent.	evt(config-snat-pool)# persistent	
7	Создать группу правил с определённым именем.	evt(config-snat)# ruleset <NAME>	<NAME> – имя группы правил, задаётся строкой до 31 символа.
8	Указать экземпляр VRF, в котором будет работать данная группа правил (не обязательно).	evt(config-snat-ruleset)# ip vrf forwarding <VRF>	<VRF> – имя VRF, задается строкой до 31 символа.

Шаг	Описание	Команда	Ключи
9	Задать область применения группы правил. Правила будут применяться только для трафика, идущего в определенную зону или интерфейс.	evt(config-snat-ruleset)# to { zone <NAME> interface <IF> tunnel <TUN> default }	<NAME> – имя зоны изоляции; <IF> – имя интерфейса устройства; <TUN> – имя туннеля устройства default – обозначает группу правил для всего трафика, источник которого не попал под критерии других групп правил.
10	Задать правило с определённым номером. Правила обрабатываются в порядке возрастания.	evt(config-snat-ruleset)# rule <ORDER>	<ORDER> – номер правила, принимает значения [1..10000].
11	Задать профиль IP-адресов {отправителя получателя}, для которых должно срабатывать правило.	evt(config-snat-rule)# match [not] {source destination}-address <TYPE> {<FROM-ADDR> - <TO-ADDR> <OBJ-GROUP-NETWORK-NAME> <ADDR/LEN>}	<TYPE> – тип аргумента, устанавливаемый в качестве адреса: • address-range – указать диапазон IPv4/IPv6 адресов; • object-group – указать имя профиля; • prefix – указать адрес подсети и префикс; • any – установить в качестве адреса любой адрес. <FROM-ADDR> – начальный IP-адрес диапазона; <TO-ADDR> – конечный IP-адрес диапазона; <OBJ-GROUP-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа; <ADDR/LEN> – IP-адрес и маска подсети.

Шаг	Описание	Команда	Ключи
12	Задать профиль IP-адресов {отправителя получателя}, для которых должно срабатывать правило (не обязательно).	evt(config-snat-rule)# match [not] {source destination}-port <TYPE> {<PORT-SET-NAME> <FROM-PORT> - <TO-PORT>}	<TYPE> – тип аргумента, устанавливаемый в качестве адреса: • address-range – указать диапазон IPv4/IPv6 адресов; • object-group – указать имя профиля; • any – установить в качестве адреса любой адрес. <PORT-SET-NAME> – имя профиля порта, задаётся строкой до 31 символа; <FROM-PORT> – начальный порт диапазона; <TO-PORT> – конечный порт диапазона.
13	Установить имя или номер IP-протокола, для которого должно срабатывать правило (не обязательно).	evt(config-snat-rule)# match [not] {protocol protocol-id} <TYPE>	<TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre. Значение «any» указывает на любой тип протокола; <ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF].
14	Задать тип и код сообщений протокола ICMP, для которых должно срабатывать правило (не обязательно).	evt(config-snat-rule)# match [not] icmp {<ICMP_TYPE><ICMP_CODE> <TYPE-NAME>}	<ICMP_TYPE> – тип сообщения протокола ICMP, принимает значения [0..255]; <ICMP_CODE> – код сообщения протокола ICMP, принимает значения [0..255]. Значение «any» указывает на любой код сообщения; <TYPE-NAME> – имя типа ICMP сообщения

Шаг	Описание	Команда	Ключи
15	Задать действие «трансляция адреса и порта отправителя» для трафика, удовлетворяющего критериям, заданным командами «match».	evt(config-snat-rule)# action source-nat { off pool <NAME> netmap <ADDR/ LEN> [static] interface [FIRST_PORT – LAST_PORT] }	off – трансляция отключена; pool<NAME> – имя пула, содержащего набор IP-адресов и/или TCP/UDP-портов; netmap <ADDR/LEN> – IP-адрес и маска подсети, используемые при трансляции; static – опция для организации статического NAT. Параметр задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. interface [FIRST_PORT – LAST_PORT] – задаёт трансляцию в IP-адрес интерфейса. Если дополнительно задан диапазон TCP/UDP-портов, то трансляция будет происходить только для TCP/UDP-портов отправителя, входящих в указанный диапазон.
16	Активировать конфигурируемое правило.	evt(config-snat-rule)# enable	

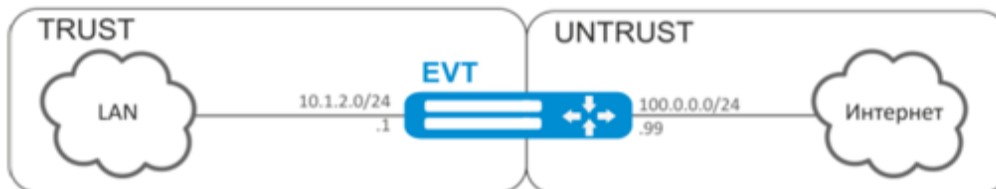
Шаг	Описание	Команда	Ключи
17	Включить функцию отслеживания сессий уровня приложений для протоколов FTP, SIP, H323, netbios-ns, PPTP (не обязательно).	evt(config)# ip firewall sessions tracking {<PROTOCOL> sip [port <OBJECT-GROUP-SERVICE>] all}	all – включает функцию отслеживания сессий уровня приложений для всех доступных протоколов <PROTOCOL> – протокол уровня приложений, сессии которого должны отслеживаться, принимает значения [ftp, h323, pptp, netbios-ns]. <OBJECT-GROUP-SERVICE> – имя профиля TCP/UDP-портов sip-сессии, задаётся строкой до 31 символа. Если группа не указана, то отслеживание сессий sip будет осуществляться для порта 5060.
18	Включить функцию трансляции IP-адресов в заголовках уровня приложений (не обязательно).	evt(config)# nat alg {<PROTOCOL> all}	all – включает трансляцию IP-адресов в заголовках всех доступных протоколов. <PROTOCOL> – протокол уровня приложений, в заголовках которого должна работать трансляция адресов, принимает значения [ftp, h323, pptp, netbios-ns, gre, sip, tftp].

 При использовании ключа not правило будет срабатывать для значений, которые не входят в указанный профиль.
Каждая команда «match» может содержать ключ «not». При использовании данного ключа под правило будут подпадать пакеты, не удовлетворяющие заданному критерию.
Более подробная информация о командах для настройки маршрутизатора содержится в справочнике команд CLI.

Пример настройки 1

Задача:

Настроить доступ пользователей локальной сети 10.1.2.0/24 к публичной сети с использованием функции Source NAT. Задать диапазон адресов публичной сети для использования SNAT 100.0.0.100-100.0.0.249.



Решение:

Конфигурирование начнем с создания зон безопасности, настройки сетевых интерфейсов и определения их принадлежности к зонам безопасности. Создадим доверенную зону «TRUST» для локальной сети и зону «UNTRUST» для публичной сети.

```

evt# configure
evt(config)# security zone UNTRUST
evt(config-zone)# exit
evt(config)# security zone TRUST
evt(config-zone)# exit
evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# ip address 10.1.2.1/24
evt(config-if-gi)# security-zone TRUST
evt(config-if-gi)# exit
evt(config)# interface tengigabitethernet 1/0/1
evt(config-if-te)# ip address 100.0.0.99/24
evt(config-if-te)# security-zone UNTRUST
evt(config-if-te)# exit

```

Для конфигурирования функции SNAT и настройки правил зон безопасности потребуется создать профиль адресов локальной сети «LOCAL_NET», включающий адреса, которым разрешен выход в публичную сеть, и профиль адресов публичной сети «PUBLIC_POOL».

```

evt(config)# object-group network LOCAL_NET
evt(config-object-group-network)# ip address-range 10.1.2.2-10.1.2.254
evt(config-object-group-network)# exit
evt(config)# object-group network PUBLIC_POOL
evt(config-object-group-network)# ip address-range 100.0.0.100-100.0.0.249
evt(config-object-group-network)# exit

```

Для пропуска трафика из зоны «TRUST» в зону «UNTRUST» создадим пару зон и добавим правила, разрешающие проходить трафику в этом направлении. Дополнительно включена проверка адреса источника данных на принадлежность к диапазону адресов «LOCAL_NET» для соблюдения ограничения на выход в публичную сеть. Действие правил разрешается командой **enable**.

```

evt(config)# security zone-pair TRUST UNTRUST
evt(config-zone-pair)# rule 1
evt(config-zone-pair-rule)# match source-address object-group LOCAL_NET
evt(config-zone-pair-rule)# action permit
evt(config-zone-pair-rule)# enable
evt(config-zone-pair-rule)# exit
evt(config-zone-pair)# exit

```

Конфигурируем сервис SNAT. Первым шагом создаётся пул адресов публичной сети, используемых для сервиса SNAT.

```

evt(config)# nat source
evt(config-snat)# pool TRANSLATE_ADDRESS
evt(config-snat-pool)# ip address-range 100.0.0.100-100.0.0.249
evt(config-snat-pool)# exit

```

Вторым шагом создаётся набор правил SNAT. В атрибутах набора укажем, что правила применяются только для пакетов, направляющихся в публичную сеть – в зону «UNTRUST». Правила включают проверку адреса источника данных на принадлежность к пулу «LOCAL_NET».

```

evt(config-snat)# ruleset SNAT
evt(config-snat-ruleset)# to zone UNTRUST
evt(config-snat-ruleset)# rule 1
evt(config-snat-rule)# match source-address object-group LOCAL_NET
evt(config-snat-rule)# action source-nat pool TRANSLATE_ADDRESS
evt(config-snat-rule)# enable
evt(config-snat-rule)# exit
evt(config-snat-ruleset)# exit

```

Для того чтобы маршрутизатор отвечал на запросы протокола ARP для адресов, входящих в публичный пул, необходимо запустить сервис ARP Proxy. Сервис ARP Proxy настраивается на интерфейсе, которому принадлежит IP-адрес из подсети профиля адресов публичной сети «PUBLIC_POOL».

```

evt(config)# interface tengigabitethernet 1/0/1
evt(config-if-te)# ip nat proxy-arp PUBLIC_POOL

```

Для того чтобы устройства локальной сети могли получить доступ к публичной сети, на них должна быть настроена маршрутизация – адрес 10.1.2.1 должен быть назначен адресом шлюза.

На самом маршрутизаторе также должен быть создан маршрут для направления на публичную сеть. Этот маршрут может быть назначен маршрутом по умолчанию с помощью следующей команды.

```

evt(config)# ip route 0.0.0.0/0 100.0.0.1
evt(config)# exit

```

Пример настройки 2

Задача:

Настроить доступ пользователей локальной сети 21.12.2.0/24 к публичной сети с использованием функции Source NAT без использования межсетевого экрана (firewall). Диапазон адресов публичной сети для использования SNAT 200.10.0.100-200.10.0.249.



Решение:

Конфигурирование начнем с настройки сетевых интерфейсов и отключения межсетевого:

```

evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# ip address 21.12.2.1/24
evt(config-if-gi)# ip firewall disable
evt(config-if-gi)# exit
  
```

```

evt(config)# interface tengigabitethernet 1/0/1
evt(config-if-te)# ip address 200.10.0.1/24
evt(config-if-te)# ip firewall disable
evt(config-if-te)# exit
  
```

Для конфигурирования функции SNAT потребуется создать профиль адресов локальной сети «LOCAL_NET», включающий адреса, которым разрешен выход в публичную сеть, и профиль адресов публичной сети «PUBLIC_POOL»:

```

evt(config)# object-group network LOCAL_NET
evt(config-object-group-network)# ip address-range 21.12.2.2-21.12.2.254
evt(config-object-group-network)# exit

evt(config)# object-group network PUBLIC_POOL
evt(config-object-group-network)# ip address-range 200.10.0.100-200.10.0.249
evt(config-object-group-network)# exit
  
```

Конфигурируем сервис SNAT.

Первым шагом создаётся пул адресов публичной сети, используемых для сервиса SNAT:

```

evt(config)# nat source
evt(config-snat)# pool TRANSLATE_ADDRESS
evt(config-snat-pool)# ip address-range 200.10.0.100-200.10.0.249
evt(config-snat-pool)# exit
  
```

Вторым шагом создаётся набор правил SNAT. В атрибутах набора укажем, что правила применяются только для пакетов, направляющихся в публичную сеть через порт te1/0/1. Правила включают проверку адреса источника данных на принадлежность к пулу «LOCAL_NET»:

```

evt(config-snat)# ruleset SNAT
evt(config-snat-ruleset)# to interface te1/0/1
evt(config-snat-ruleset)# rule 1
evt(config-snat-rule)# match source-address object-group LOCAL_NET
evt(config-snat-rule)# action source-nat pool TRANSLATE_ADDRESS
evt(config-snat-rule)# enable
evt(config-snat-rule)# exit
evt(config-snat-ruleset)# exit

```

Для того чтобы маршрутизатор отвечал на запросы протокола ARP для адресов, входящих в публичный пул, необходимо запустить сервис ARP Proxy. Сервис ARP Proxy настраивается на интерфейсе, которому принадлежит IP-адрес из подсети профиля адресов публичной сети «PUBLIC_POOL»:

```

evt(config)# interface tengigabitethernet 1/0/1
evt(config-if-te)# ip nat proxy-arp PUBLIC_POOL

```

Для того чтобы устройства локальной сети могли получить доступ к публичной сети, на них должна быть настроена маршрутизация – адрес 21.12.2.1 должен быть назначен адресом шлюза.

На самом маршрутизаторе также должен быть создан маршрут для направления на публичную сеть. Этот маршрут может быть назначен маршрутом по умолчанию с помощью следующей команды:

```

evt(config)# ip route 0.0.0.0/0 200.10.0.254
evt(config)# exit

```

Конфигурирование Static NAT

Static NAT – статический NAT задает однозначное соответствие одного адреса другому. Иными словами, при прохождении через маршрутизатор, адрес меняется на другой строго заданный адрес, один-к-одному. Запись о такой трансляции хранится неограниченно долго, пока не будет произведена перенастройка NAT на маршрутизаторе.

Алгоритм настройки

Настройка Static NAT осуществляется средствами Source NAT, алгоритм настройки которой описан в разделе [Конфигурирование Source NAT, алгоритм настройки](#) настоящего руководства.

Пример настройки Static NAT

Задача:

Настроить двухстороннюю и постоянную трансляцию из локальной сети для диапазона адресов 21.12.2.100-21.12.2.150 в публичную сеть 200.10.0.0/24. Диапазон адресов публичной сети для использования трансляции – 200.10.0.100-200.10.0.150.



Решение:

Начнем конфигурирование с настройки сетевых интерфейсов и отключения межсетевого экрана:

```

evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# ip address 21.12.2.1/24
evt(config-if-gi)# ip firewall disable
evt(config-if-gi)# exit
  
```

```

evt(config)# interface tengigabitethernet 1/0/1
evt(config-if-te)# ip address 200.10.0.1/24
evt(config-if-te)# ip firewall disable
evt(config-if-te)# exit
  
```

Для конфигурирования Static NAT потребуется создать профиль адресов локальной сети «LOCAL_NET», включающий локальную подсеть:

```

evt(config)# object-group network LOCAL_NET
evt(config-object-group-network)# ip prefix 21.12.2.0/24
evt(config-object-group-network)# exit
  
```

Диапазон адресов публичной сети для использования Static NAT задаем в профиле «PROXY»:

```

evt(config)# object-group network PROXY
evt(config-object-group-network)# ip address-range 200.10.0.100-200.10.0.150
evt(config-object-group-network)# exit
  
```

Конфигурируем сервис Static NAT в режиме конфигурирования SNAT. В атрибутах набора укажем, что правила применяются только для пакетов, направляющихся в публичную сеть через порт te1/0/1. Правила включают проверку адреса источника данных на принадлежность к пулу «LOCAL_NET».

```

evt(config)# nat source
evt(config-snat)# ruleset SNAT
evt(config-snat-ruleset)# to interface te1/0/1
evt(config-snat-ruleset)# rule 1
evt(config-snat-rule)# match source-address object-group LOCAL_NET
evt(config-snat-rule)# action source-nat netmap 200.10.0.0/24 static
evt(config-snat-rule)# enable
evt(config-snat-rule)# exit
evt(config-snat-ruleset)# exit
  
```

Для того чтобы маршрутизатор отвечал на запросы протокола ARP для адресов, входящих в пул трансляции «PROXY», необходимо запустить сервис ARP Proxy. Сервис ARP Proxy настраивается на интерфейсе, которому принадлежит IP-адрес из подсети профиля адресов «PROXY».

```

evt(config)# interface tengigabitethernet 1/0/1
evt(config-if-te)# ip nat proxy-arp PROXY

```

Для того чтобы устройства локальной сети могли получить доступ к сети 200.10.0.0/24, на них должна быть настроена маршрутизация – адрес 21.12.2.1 должен быть назначен адресом шлюза.

Изменения конфигурации вступают в действие по команде применения.

```

evt# commit
Configuration has been successfully committed
evt# confirm
Configuration has been successfully confirmed

```

Посмотреть активные трансляции можно с помощью команды:

```

evt# show ip nat translations

```

Настройка NTP

NTP (англ. *Network Time Protocol* – протокол сетевого времени) – сетевой протокол для синхронизации внутренних часов оборудования с использованием IP-сетей, использует для своей работы протокол UDP, учитывает время передачи и использует алгоритмы для достижения высокой точности синхронизации времени.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Включить NTP.	evt(config)# ntp enable	
2	Задать IP-адрес NTP-сервера, либо участника NTP-синхронизации.	evt(config)# ntp { pool server peer } { <IPv4> <NAME> IPv6}	<IPv4> – IP-адрес назначения (шлюз), задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. <NAME> – DNS-имя сервера, задаётся строкой до 31 символа. <IPv6> – IP-адрес назначения (шлюз), задаётся в виде X:X:X::X, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF].
3	Включить отправку нескольких пакетов вместо одного при установке соединения.	evt(config-ntp)# burst	
4	Включить отправку нескольких пакетов вместо одного в случае разрыва соединения.	evt(config-ntp)# iburst	

Шаг	Описание	Команда	Ключи
5	Задать ключ для аутентификации (не обязательно).	evt(config-ntp)# key <ID>	<ID> – идентификатор ключа, задается в диапазоне [1..255].
6	Установить максимальное значение интервала времени между отправкой сообщений NTP-серверу (не обязательно).	evt(config-ntp)# maxpoll <INTERVAL>	<INTERVAL> – максимальное значение интервала опроса. Параметр команды используется как показатель степени двойки при вычислении длительности интервала в секундах, вычисляется путем возведения двойки в степень, заданную параметром команды, принимает значение [10..17]. Значение по умолчанию: 10 (2^{10} = 1024 секунды или 17 минут 4 секунды).
7	Установить минимальное значение интервала времени между отправкой сообщений NTP-серверу (не обязательно).	evt(config-ntp)# minpoll <INTERVAL>	<INTERVAL> – минимальное значение интервала опроса в секундах вычисляется путем возведения двойки в степень, заданную параметром команды, принимает значение [4..6]. Значение по умолчанию: 6 (2^6 = 64 секунды или 1 минута 4 секунды).
8	Отметить данный NTP-сервер как предпочтительный (не обязательно).	evt(config-ntp)# prefer	
9	Определить список доверенных IP-адресов, с которыми может происходить обмен ntp-пакетами (не обязательно).	evt(config)# ntp access-addresses <NAME>	<NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.
10	Указать идентификатор ключа из профиля связки ключей (не обязательно).	evt(config)# ntp authentication trusted-key <ID>	<ID> – идентификатор ключа из профиля связки ключей.
11	Указать имя профиля связки ключей (не обязательно).	evt(config)# ntp authentication key-chain <WORD>	<WORD> – имя профиля связки ключей.
12	Активировать аутентификацию для NTP по ключу (не обязательно).	evt(config)# ntp authentication enable	

Шаг	Описание	Команда	Ключи
13	Включить режим приёма широковещательных сообщений NTP-серверов для глобальной конфигурации и всех существующих VRF (не обязательно).	evt(config)# ntp broadcast-client enable	
14	Задать значение кода DSCP для использования в IP-заголовке исходящих пакетов NTP-сервера (не обязательно).	evt(config)# ntp dscp <DSCP>	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 46.
15	Включить режим query-only, ограничивающий взаимодействие по NTP для определенного профиля IP-адресов (не обязательно).	evt(config)# ntp object-group query-only <NAME>	<NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.
16	Включить режим serve-only, ограничивающий взаимодействие по NTP для определенного профиля IP-адресов (не обязательно).	evt(config)# ntp object-group serve-only <NAME>	<NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.
17	Указать source-IP-адреса для NTP-пакетов для всех peer (не обязательно).	evt(config)# ntp source address <ADDR>	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
18	Задать текущее время и дату в ручном режиме (не обязательно).	evt# set date <TIME> [<DAY> <MONTH> [<YEAR>]]	<TIME> – устанавливаемое системное время, задаётся в виде HH:MM:SS, где: • HH – часы, принимает значение [0..23]; • MM – минуты, принимает значение [0 .. 59]; • SS – секунды, принимает значение [0 .. 59]. • <DAY> – день месяца, принимает значения [1..31]; <MONTH> – месяц, принимает значения [January/February/March/April/May/June/July/August/September/October/November/December]; <YEAR> – год, принимает значения [2001..2037].

Пример настройки

Задача:

Настроить синхронизацию времени от NTP-сервера.

IP-адрес маршрутизатора EVT – 192.168.52.8,

IP-адрес NTP-сервера – 192.168.52.41.

**Решение:**

- ⚠ Предварительно нужно выполнить следующие действия:
- указать зону безопасности для интерфейса gi1/0/1;
 - настроить IP-адрес для интерфейса gi1/0/1, чтобы обеспечить IP-связность с NTP-сервером.

Пример:

```

security zone untrust
exit
object-group service NTP
  port-range 123
exit
interface gigabitethernet 1/0/1
  security-zone untrust
  ip address 192.168.52.8/24
exit
security zone-pair untrust self
  rule 10
    action permit
    match protocol udp
    match destination-port object-group NTP
  enable
exit
exit

```

Основной этап конфигурирования:

Включение синхронизации системных часов с удаленными серверами:

```
evt(config)# ntp enable
```

Настройка NTP-сервера:

```
evt-(config)# ntp server 192.168.52.41
```

Указать предпочтительность данного NTP-сервера (необязательно):

```
evt-1000(config-ntp)# prefer
```

Указать интервал времени между отправкой сообщений NTP-серверу:

```
evt(config-ntp)# minpoll 4
evt(config-ntp)# end
evt# commit
evt# confirm
```

Команда для просмотра текущей конфигурации протокола NTP:

```
evt# show ntp configuration
```

Команда для просмотра текущего состояния NTP-серверов (пиров):

```
evt# show ntp peers
```

6.2.9 Управление туннелированием

- [Настройка GRE-туннелей](#)
 - [Алгоритм настройки](#)
 - [Пример настройки IP-GRE-туннеля](#)
- [Настройка IPsec VPN](#)
 - [Алгоритм настройки Route-based IPsec VPN](#)
 - [Пример настройки Route-based IPsec VPN](#)
 - [Алгоритм настройки Policy-based IPsec VPN](#)
 - [Пример настройки Policy-based IPsec VPN](#)
 - [Алгоритм настройки Remote Access IPsec VPN](#)
 - [Пример настройки Remote Access IPsec VPN](#)
 - [Пример настройки DPD \(Dead Peer Detection\)](#)
- [Настройка LT-туннелей](#)
 - [Алгоритм настройки](#)
 - [Пример настройки](#)

⚠ Конфигурация на маршрутизаторах EVT и EVS производится с помощью одинаковых команд. Ниже приведены примеры настройки EVT.

Настройка GRE-туннелей

GRE (англ. *Generic Routing Encapsulation* — общая инкапсуляция маршрутов) — протокол туннелирования сетевых пакетов. Его основное назначение — инкапсуляция пакетов сетевого уровня сетевой модели OSI в IP-пакеты. GRE может использоваться для организации VPN на 3 уровне модели OSI.

В маршрутизаторе EVT/EVS реализованы статические неуправляемые GRE-туннели, то есть туннели создаются вручную путем конфигурирования на локальном и удаленном узлах. Параметры туннеля для каждой из сторон должны быть взаимосогласованными или переносимые данные не будут декапсулироваться партнером.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Сконфигурировать L3-интерфейс, от которого будет строиться GRE-туннель.		
2	Создать GRE-туннель и перейти в режим его конфигурирования.	evt(config)# tunnel gre <INDEX>	<INDEX> – идентификатор туннеля в диапазоне – [1..250]
3	Указать экземпляр VRF, в котором будет работать данный GRE-туннель (необязательно).	evt(config-gre)# ip vrf forwarding <VRF>	<VRF> – имя VRF, задается строкой до 31 символа.
4	Указать имя VRF от IP-интерфейса которого будет строиться данный GRE-туннель (необязательно).	evt-(config-gre)# tunnel-source vrf <VRF>	<VRF> – имя экземпляра VRF, задается строкой до 31 символа. Без указания ключа "vrf" и имени экземпляра VRF будет использоваться IP-интерфейс глобальной конфигурации.
5	Указать описание конфигурируемого туннеля (необязательно).	evt(config-gre)# description <DESCRIPTION>	<DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов.
6	Установить локальный IP-адрес для установки туннеля.	evt(config-gre)# local address <ADDR>	<ADDR> – IP-адрес локального шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
		evt(config-gre)# local interface <IF>	<IF> – интерфейс, от IP-адреса которого устанавливается туннель.
7	Установить удаленный IP-адрес для установки туннеля.	evt(config-gre)# remote address <ADDR>	<ADDR> – IP-адрес локального шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Шаг	Описание	Команда	Ключи
8	Указать режим инкапсуляции для GRE-туннеля.	evt(config-gre)# mode <MODE>	<MODE> – режим инкапсуляции для GRE-туннеля: • ip – инкапсуляция IP-пакетов в GRE; • ethernet – инкапсуляция Ethernet-фреймов в GRE. Значение по умолчанию: ip
9	Установить IP-адрес локальной стороны туннеля (только в режиме ip).	evt(config-gre)# ip address <ADDR/LEN> [unit <ID>] или evt(config-gre)# ip address <ADDR/LEN> secondary [unit <ID>]	<ADDR/LEN> – IP-адрес и префикс подсети задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. <ID> – номер юнита, принимает значения [1..2]. Ключ secondary указывает, что настроенный адрес является дополнительным IP-адресом. Если это ключевое слово отсутствует, настроенный адрес является основным IP-адресом. Возможно указать до 7 дополнительных IP-адресов. Дополнительные функции IPv4-адресации см. в разделе Настройка IP-адресации.
10	Назначить широковещательный домен для инкапсуляции в GRE-пакеты данного туннеля (только в режиме ethernet).	evt(config-gre)# bridge-group <BRIDGE-ID>	<BRIDGE-ID> – идентификационный номер моста, принимает значения в диапазоне – [1..250];
11	Включить GRE-туннель в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall (см. раздел Конфигурирование Firewall).	evt(config-gre)# security-zone<NAME>	<NAME> – имя зоны безопасности, задаётся строкой до 12 символов.
		evt(config-gre)# ip firewall disable	

Шаг	Описание	Команда	Ключи
12	Указать размер MTU (Maximum Transmission Unit) для туннеля (необязательно). MTU более 1500 будет активно, только если применена команда "system jumbo-frames".	evt(config-gre)# mtu <MTU>	<MTU> – значение MTU, принимает значения в диапазоне – [1280..9500]; Значение по умолчанию: 1500.
13	Указать значение времени жизни TTL для туннельных пакетов (необязательно).	evt(config-gre)# ttl <TTL>	<TTL> – значение TTL, принимает значения в диапазоне [1..255]. Значение по умолчанию: наследуется от инкапсулируемого пакета.
14	Указать DSCP для использования в IP-заголовке инкапсулирующего пакета (необязательно).	evt(config-gre)# dscp <DSCP>	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: наследуется от инкапсулируемого пакета.
15	Разрешить передачу ключа (key) в туннельном заголовке GRE (в соответствии с RFC 2890) и установить значение ключа. Настраивается только с обеих сторон туннеля (необязательно).	evt(config-gre)# key <KEY>	<KEY> – значение KEY, принимает значения в диапазоне [1..2000000]. Значение по умолчанию: ключ не передаётся.
16	Включить вычисление контрольной суммы и занесение её в GRE-заголовок отправляемых пакетов. При этом на удаленной стороне необходимо включить проверку контрольной суммы (необязательно).	evt(config-gre)# local checksum	
17	Включить проверку наличия и соответствия значений контрольной суммы в заголовках принимаемых GRE-пакетов. При этом на удаленной стороне необходимо включить вычисление контрольной суммы (необязательно).	evt(config-gre)# remote checksum	
18	Включить проверку доступности удаленного шлюза туннеля (необязательно).	evt(config-gre)# keepalive enable	

Шаг	Описание	Команда	Ключи
19	Изменить время ожидания keepalive пакетов от встречной стороны (необязательно).	evt(config-gre)# keepalive timeout <TIME>	<TIME> – время в секундах, принимает значения в диапазоне [1..32767]. Значение по умолчанию: 10.
20	Изменить количество попыток проверки доступности удаленного шлюза туннеля (необязательно).	evt(config-gre)# keepalive retries <VALUE>	<VALUE> – количество попыток, принимает значения в диапазоне [1..255]. Значение по умолчанию: 5.
21	Указать IP-адрес для работы механизма keepalive (обязательно в режиме ethernet).	evt(config-gre)# keepalive dst-address <ADDR>	<ADDR> – IP-адрес для проверки работоспособности GRE-туннеля.
22	Изменить интервал времени, за который усредняется статистика о нагрузке на туннеле (необязательно).	evt(config-gre)# load-average <TIME>	<TIME> – интервал в секундах, принимает значения [5..150]. Значение по умолчанию: 5.
23	Включить отправку snmp-trap о включении/отключении туннеля.	evt(config-gre)# snmp init-trap	
24	Включить механизм перезапроса IP-адресов по протоколу DHCP на указанных интерфейсах при отключении GRE-туннеля по keepalive (необязательно).	evt(config-gre)# keepalive dhcp dependent-interface <IF>	<IF> – физический/логический интерфейс, на котором включено получение IP-адреса по DHCP.
25	Задать интервал времени между отключением GRE-туннеля и перезапросом IP-адреса на интерфейсе/интерфейсах, указанных командой keepalive dhcp dependent-interface (необязательно).	evt(config-gre)# keepalive dhcp link-timeout <SEC>	<SEC> – интервал между отключением GRE-туннеля и перезапросом IP-адреса по DHCP на интерфейсах.
26	Переопределить значение поля MSS (Maximum segment size) во входящих TCP-пакетах (необязательно).	evt(config-gre)# ip tcp adjust-mss <MSS>	<MSS> – значение MSS, принимает значения в диапазоне [500..1460]. Значение по умолчанию: 1460.
27	Включить запись статистики использования текущего туннеля (необязательно).	evt(config-gre)# history statistics	
28	Активировать туннель.	evt(config-gre)# enable	

Шаг	Описание	Команда	Ключи
	Также для GRE-туннеля возможно настроить: • QoS в базовом или расширенном режимах (см. раздел Управление QoS); • мониторинг трафика (см. разделы Настройка Netflow); • функционал протоколов маршрутизации (см. раздел Управление маршрутизацией).		

Пример настройки IP-GRE-туннеля

Задача:

Организовать L3-VPN между офисами компании через IP-сеть, используя для туннелирования трафика протокол GRE.

- в качестве локального шлюза для туннеля используется IP-адрес 115.0.0.1;
- в качестве удаленного шлюза для туннеля используется IP-адрес 114.0.0.10;
- IP-адрес туннеля на локальной стороне 25.0.0.1/24.



Решение:

Предварительно на маршрутизаторах должны быть настроены интерфейсы для связи с сетью WAN разрешено получение пакетов протокола GRE из зоны безопасности, в которой работают интерфейсы, подключенные к сети WAN.

Создадим туннель GRE 10:

```
evt(config)# tunnel gre 10
```

Укажем локальный и удаленный шлюз (IP-адреса интерфейсов, граничащих с WAN):

```
evt(config-gre)# local address 115.0.0.1
evt(config-gre)# remote address 114.0.0.10
```

Укажем IP-адрес туннеля 25.0.0.1/24:

```
evt(config-gre)# ip address 25.0.0.1/24
```

Также туннель должен принадлежать к зоне безопасности, для того чтобы можно было создать правила, разрешающие прохождение трафика в firewall. Принадлежность туннеля к зоне задается следующей командой:

```
evt(config-gre)# security-zone untrusted
```

Включим туннель:

```
evt(config-gre)# enable
evt(config-gre)# exit
```

На маршрутизаторе должен быть создан маршрут до локальной сети партнера. В качестве интерфейса назначения указываем ранее созданный туннель GRE:

```
evt(config)# ip route 172.16.0.0/16 tunnel gre 10
```

После применения настроек трафик будет инкапсулироваться в туннель и отправляться партнеру, независимо от наличия GRE-туннеля и правильности настроек с его стороны.

Опционально для GRE-туннеля можно указать следующие параметры:

- Включить вычисление и включение в пакет контрольной суммы заголовка GRE и инкапсулированного пакета для исходящего трафика:

```
evt(config-gre)# local checksum
```

- Включить проверку наличия и корректности контрольной суммы GRE для входящего трафика:

```
evt(config-gre)# remote checksum
```

- Указать уникальный идентификатор:

```
evt(config-gre)# key 15808
```

- Указать значение DSCP, MTU, TTL:

```
evt(config-gre)# dscp 44
evt(config-gre)# mtu 1426
evt(config-gre)# ttl 18
```

- Включить и настроить механизм keepalive:

```
evt(config-gre)# keepalive enable
evt(config-gre)# keepalive timeout <TIME>
evt(config-gre)# keepalive retries <VALUE>
```

Состояние туннеля можно посмотреть командой:

```
evt# show tunnels status gre 10
```

Счетчики входящих и отправленных пакетов можно посмотреть командой:

```
evt# show tunnels counters gre 10
```

Конфигурацию туннеля можно посмотреть командой:

```
evt# show tunnels configuration gre 10
```

Настройка туннеля IPv4-over-IPv4 производится аналогичным образом.

⚠ При создании туннеля необходимо в firewall разрешить протокол GRE (47).

Настройка IPsec VPN

IPsec — это набор протоколов, которые обеспечивают защиту передаваемых с помощью IP-протокола данных. Данный набор протоколов позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и шифрование IP-пакетов, а также включает в себя протоколы для защищённого обмена ключами в сети Интернет.

Алгоритм настройки Route-based IPsec VPN

Шаг	Описание	Команда	Ключи
1	Создать VTI-туннель и перейти в режим его конфигурирования.	evt(config)# tunnel vti <TUN>	<TUN> – имя туннеля устройства.
2	Указать локальный IP-адрес VTI-туннеля.	evt(config-vti)# local address <ADDR>	<ADDR> – IP-адрес локального шлюза.
3	Указать удаленный IP-адрес VTI-туннеля.	evt(config-vti)# remote address <ADDR>	<ADDR> – IP-адрес удаленного шлюза.
4	Установить IP-адрес локальной стороны VTI-туннеля.	evt(config-vti)# ip address <ADDR/LEN> [unit <ID>] или evt(config-vti)# ip address <ADDR/LEN> secondary [unit <ID>]	<ADDR/LEN> – IP-адрес и префикс подсети задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]; <ID> – номер юнита, принимает значения [1..2]. Ключ secondary указывает, что настроенный адрес является дополнительным IP-адресом. Если это ключевое слово отсутствует, настроенный адрес является основным IP-адресом. Возможно указать до 7 дополнительных IP-адресов.
5	Включить VTI-туннель в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall для VTI-туннеля.	evt(config-vti)# security-zone<NAME> evt(config-vti)# ip firewall disable	<NAME> – имя зоны безопасности, задаётся строкой до 12 символов.
6	Включить туннель.	evt(config-vti)#enable	
7	Создать IKE-профиль и перейти в режим его конфигурирования.	evt(config)# security ike proposal <NAME>	<NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
8	Указать описание конфигурируемого IKE-профиля (необязательно).	evt(config-ike-proposal)# description<DESCRIPTION>	<DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов.
9	Определить алгоритм аутентификации для IKE (необязательно).	evt(config-ike-proposal)# authentication algorithm <ALGORITHM>	<ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2-384, sha2-512. Значение по умолчанию: sha1.
10	Определить алгоритм шифрования для IKE (необязательно).	evt(config-ike-proposal)# encryption algorithm <ALGORITHM>	<ALGORITHM> – протокол шифрования, принимает значения: des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256. Значение по умолчанию: 3des.
11	Определить номер группы Диффи-Хэллмана (необязательно).	evt(config-ike-proposal)# dh-group <DH-GROUP>	<DH-GROUP> – номер группы Диффи-Хэллмана, принимает значения [1, 2, 5, 14, 15, 16, 17, 18]. Значение по умолчанию: 1.
12	Создать IKE-политику и перейти в режим её конфигурирования.	evt(config)# security ike policy <NAME>	<NAME> – имя политики IKE, задаётся строкой до 31 символа.
13	Определить режим аутентификации IKE (необязательно).	evt(config-ike-policy)# authentication method <METHOD>	<METHOD> – метод аутентификации ключа. Может принимать значения: • pre - shared - key – метод аутентификации, использующий предварительно полученные ключи шифрования; • public - key – метод аутентификации, использующий сертификат. Значение по умолчанию: pre-shared-key.

Шаг	Описание	Команда	Ключи
14	Задать время жизни соединения протокола IKE (необязательно).	evt(config-ike-policy)# lifetime seconds <SEC>	<SEC> – период времени, принимает значения [4 ..86400] секунд. Значение по умолчанию: 10800.
15	Привязать IKE-профиль к IKE-политике.	evt(config-ike-policy)# proposal <NAME>	<NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа.
16	Указать ключ аутентификации (обязательно, если в качестве режима аутентификации выбран pre-shared-key).	evt(config-ike-policy)# pre-shared-key ascii-text<TEXT>	<TEXT> – строка [1..64] ASCII-символов.
17	Создать IKE-шлюз и перейти в режим его конфигурирования.	evt(config)# security ike gateway <NAME>	<NAME> – имя шлюза протокола IKE, задаётся строкой до 31 символа.
18	Привязать IKE-политику к IKE-шлюзу.	evt(config-ike-gw)# ike-policy <NAME>	<NAME> – имя политики протокола IKE, задаётся строкой до 31 символа.
19	Указать версию IKE (необязательно).	evt(config-ike-gw)# version <VERSION>	<version> – версия IKE-протокола: v1-only или v2-only. Значение по умолчанию: v1-only.
20	Установить режим перенаправления трафика в туннель – route-based.	evt(config-ike-gw)# mode route-based	
21	Указать действие для DPD (необязательно).	evt(config-ike-gw)# dead-peer-detection action <MODE>	<MODE> – режим работы DPD: • restart – соединение переустанавливается; • clear – соединение останавливается; • hold – соединение поддерживается; • none – механизм выключен, никаких действий не предпринимается. Значение по умолчанию: none.

Шаг	Описание	Команда	Ключи
22	Указать интервал между отправкой сообщений механизмом DPD (необязательно).	evt(config-ike-gw)# dead-peer-detection interval <SEC>	<SEC> – интервал между отправкой сообщений механизмом DPD, принимает значения [1..180] секунд. Значение по умолчанию: 2.
23	Указать период времени ожидания ответа на сообщения механизма DPD при использовании протокола IKE версии 1 (необязательно).	evt(config-ike-gw)# dead-peer-detection timeout <SEC>	<SEC> – период времени ожидания ответа на сообщения механизма DPD при использовании протокола IKE версии 1, принимает значения [1..180] секунд. Значение по умолчанию: 30 секунд.
24	Указать базовый период времени ожидания ответа на сообщения механизма DPD при использовании протокола IKE версии 2 (необязательно).	evt(config-ike-gw)# dead-peer-detection retransmit timeout <SEC>	<SEC> – базовый период времени ожидания ответа на сообщения механизма DPD при использовании протокола IKE версии 2, принимает значения [1..30] секунд. Значение по умолчанию: 4 секунды.
25	Указать количество попыток повторной отправки сообщений механизма DPD после наступления таймаута ожидания ответа при использовании протокола IKE версии 2 (необязательно).	evt(config-ike-gw)# dead-peer-detection retransmit tries <TRIES>	<TRIES> – количество попыток повторной отправки сообщений механизма DPD в случае наступления таймаута ожидания ответа при использовании протокола IKE версии 2, принимает значения от 1 до 10. Для первого отправленного сообщения DPD период времени ожидания ответа будет равен базовому периоду, указанному в команде dead-peer-detection retransmit timeout , а для последующих попыток интервал ожидания будет рассчитан по формуле: "dead-peer-detection retransmit timeout" * 1.8 ^ (N-1), где N - номер попытки. Значение по умолчанию: 5 попыток.

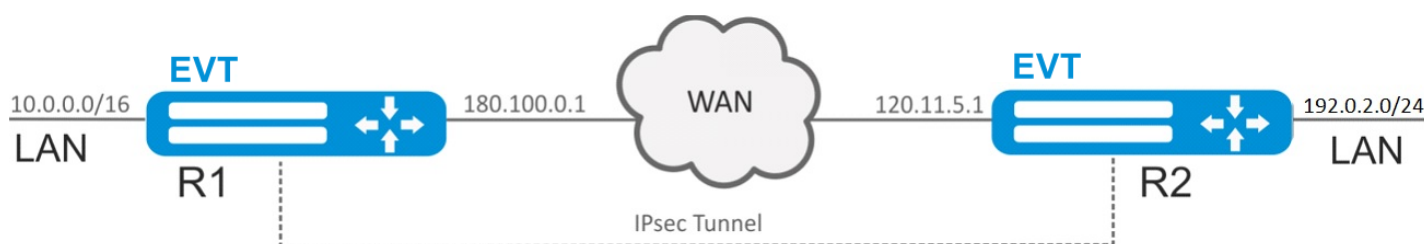
Шаг	Описание	Команда	Ключи
26	Указать уровень случайного разброса периода ожидания ответа на сообщения механизма DPD при использовании протокола IKE версии 2 (необязательно).	evt(config-ike-gw)# dead-peer-detection retransmit jitter <VALUE>	<VALUE> – максимальный процент разброса значений, принимает значения [0..100]. Значение по умолчанию: 0 %
27	Указать ограничение максимального периода времени ожидания ответа на сообщения механизма DPD при использовании протокола IKE версии 2 (необязательно).	evt(config-ike-gw)# dead-peer-detection retransmit limit <SEC>	<SEC> – максимальный период времени ожидания ответа на сообщения механизма DPD при использовании протокола IKE версии 2, принимает значения [15..300] секунд. Значение по умолчанию: 0 секунд, у периода нет верхнего предела.
28	Данная команда отключает расширение MOBIKE IKEv2, которое позволяет инициатору ike-сессии изменять local address в соответствии с RFC 4555.	evt(config-ike-gw)# mobike disable	
29	Привязать VTI-туннель к IKE-шлюзу.	evt(config-ike-gw)# bind-interface vti <VTI>	<VTI> – идентификационный номер интерфейса VTI.
30	Создать в IPsec-профиль.	evt(config)# security ipsec proposal <NAME>	<NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа.
31	Определить алгоритм аутентификации для IPsec (необязательно).	evt(config-ipsec-proposal)# authentication algorithm <ALGORITHM>	<ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2-384, sha2-512. Значение по умолчанию: sha1.
32	Определить алгоритм шифрования для IPsec (необязательно).	evt(config-ipsec-proposal)# encryption algorithm <ALGORITHM>	<ALGORITHM> – протокол шифрования, принимает значения: des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256. Значение по умолчанию: 3des.

Шаг	Описание	Команда	Ключи
33	Указать протокол инкапсуляции для IPsec (необязательно).	evt(config-ipsec-proposal)# protocol <PROTOCOL>	<PROTOCOL> – инкапсулирующий протокол, принимает значения: • ah – данный протокол осуществляет только аутентификацию трафика, шифрование данных не выполняется; • esp – данный протокол осуществляет аутентификацию и шифрование трафика. Значение по умолчанию: esp.
34	Создать IPsec-политику и перейти в режим её конфигурирования.	evt(config)# security ipsec policy <NAME>	<NAME> – имя политики IPsec, задаётся строкой до 31 символа.
35	Привязать IPsec-профиль к IPsec-политике.	evt(config-ipsec-policy)# proposal <NAME>	<NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа.
36	Задать время жизни IPsec-туннеля (необязательно).	evt(config-ipsec-policy)# lifetime { seconds <SEC> packets <PACKETS> kilobytes <KB> }	<SEC> – период времени жизни IPsec-туннеля, по истечении происходит пересогласование. Принимает значения [1140..86400] секунд. <PACKETS> – количество пакетов, после передачи которого происходит пересогласование IPsec-туннеля. Принимает значения [4..86400]. <KB> – объем трафика, после передачи которого происходит пересогласование IPsec-туннеля. Принимает значения [4..4608000] секунд. Значение по умолчанию: 28800 секунд.
37	Создать IPsec VPN и перейти в режим конфигурирования.	evt(config)# security ipsec vpn <NAME>	<NAME> – имя VPN, задаётся строкой до 31 символа.
38	Определить режим согласования данных, необходимых для активации VPN.	evt(config-ipsec-vpn)# mode <MODE>	<MODE> – режим работы VPN.

Шаг	Описание	Команда	Ключи
39	Привязать IPsec-политику к IPsec-VPN.	evt(config-ipsec-vpn)# ike ipsec-policy <NAME>	<NAME> – имя IPsec-политики, задаётся строка до 31 символа.
40	Задать значение DSCP для использования в IP-заголовке исходящих пакетов IKE-протокола (необязательно).	evt(config-ipsec-vpn)# ike dscp <DSCP>	DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 63.
41	Установить режим активации VPN.	evt(config-ipsec-vpn)# ike establish-tunnel <MODE>	<MODE> – режим активации VPN: • by - request – соединение активируется встречной стороной; • route – соединение активируется при появлении трафика, маршрутизируемого в туннель; • immediate – туннель активируется автоматически после применения конфигурации.
42	Осуществить привязку IKE-шлюза к IPsec-VPN.	evt(config-ipsec-vpn)# ike gateway <NAME>	<NAME> – имя IKE-шлюза, задаётся строкой до 31 символа.
43	Установить значение временного интервала в секундах, по истечению которого соединение закрывается, если не было принято или передано ни одного пакета через SA (необязательно).	evt(config-ipsec-vpn)# ike idle-time <TIME>	<TIME> – интервал в секундах, принимает значения [4..86400].
44	Отключить пересогласование ключей до разрыва IKE-соединения по истечению времени, количеству переданных пакетов или байт (необязательно).	evt(config-ipsec-vpn)# ike rekey disable	

Шаг	Описание	Команда	Ключи
45	Настроить начало пересогласования ключей IKE-соединения до истечения времени жизни (необязательно).	evt(config-ipsec-vpn)# ike rekey margin { seconds <SEC> packets <PACKETS> kilobytes <KB> }	<SEC> – интервал времени в секундах, оставшийся до закрытия соединения (задается командой <code>lifetimeseconds</code>, см. 22.2.13). Принимает значения [4..86400]. <PACKETS> – количество пакетов, оставшихся до закрытия соединения (задается командой <code>lifetimepackets</code>). Принимает значения [4..86400] <KB> – объем трафика в килобайтах, оставшийся до закрытия соединения (задается командой <code>lifetimekilobytes</code>). Принимает значения [4..86400] Значение по умолчанию: - Пересогласование ключей до истечения времени – за 540 секунд. - Пересогласование ключей до истечения объема трафика и количества пакетов – отключено.
46	Установить уровень случайного разброса значений параметров <code>margin seconds</code> , <code>margin packets</code> , <code>margin kilobytes</code> (необязательно).	evt(config-ipsec-vpn)# ike rekey randomization <VALUE>	<VALUE> – максимальный процент разброса значений, принимает значения [1..100]. Значение по умолчанию: 100%
47	Указать описание для IPsec-VPN (необязательно).	evt(config-ipsec-vpn)# description <DESCRIPTION>	<DESCRIPTION> – описание профиля, задаётся строкой до 255 символов.
48	Активировать IPsec VPN.	evt(config-ipsec-vpn)# enable	

Пример настройки Route-based IPsec VPN



Задача:

Настроить IPsec-туннель между R1 и R2.

- R1 IP-адрес – 120.11.5.1;
- R2 IP-адрес – 180.100.0.1.

IKE:

- группа Диффи-Хэллмана: 2;
- алгоритм шифрования: AES 128 bit;
- алгоритм аутентификации: MD5.

IP sec:

- алгоритм шифрования: AES 128 bit;
- алгоритм аутентификации: MD5.

Решение:

 Предварительно в firewall необходимо разрешить протокол ESP и ISAKMP (UDP-порт 500, 4500).

1. Конфигурирование R1

Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```

evt# configure
evt(config)# interface gi 1/0/1
evt(config-if-gi)# ip address 180.100.0.1/24
evt(config-if-gi)# security-zone untrusted
evt(config-if-gi)# exit

```

Создадим туннель VTI. Трафик будет перенаправляться через VTI в IPsec-туннель. В качестве локального и удаленного шлюза указываются IP-адреса интерфейсов, граничащих с WAN:

```

evt(config)# tunnel vti 1
evt(config-vti)# local address 180.100.0.1
evt(config-vti)# remote address 120.11.5.1
evt(config-vti)# ip address 10.10.10.1/30
evt(config-vti)# enable
evt(config-vti)# exit

```

Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```

evt(config)# object-group service ISAKMP
evt(config-object-group-service)# port-range 500,4500
evt(config-object-group-service)# exit

```

Создадим статический маршрут до удаленной LAN-сети. Для каждой подсети, которая находится за IPsec-туннелем, нужно указать маршрут через VTI-туннель:

```

evt(config)# ip route 192.0.2.0/24 tunnel vti 1

```

Создадим профиль протокола IKE. В профиле укажем группу Диффи-Хэллмана 2, алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IKE-соединения:

```

evt(config)# security ike proposal ike_prop1
evt(config-ike-proposal)# dh-group 2
evt(config-ike-proposal)# authentication algorithm md5
evt(config-ike-proposal)# encryption algorithm aes128
evt(config-ike-proposal)# exit

```

Создадим политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы и ключ аутентификации:

```

evt(config)# security ike policy ike_pol1
evt(config-ike-policy)# pre-shared-key hexadecimal 123FFF
evt(config-ike-policy)# proposal ike_prop1
evt(config-ike-policy)# exit

```

Создадим шлюз протокола IKE. В данном профиле указывается VTI-туннель, политика, версия протокола и режим перенаправления трафика в туннель. Поддержка MOBIKE отключается для route-based IPsec в обязательном порядке:

```

evt(config)# security ike gateway ike_gw1
evt(config-ike-gw)# ike-policy ike_pol1
evt(config-ike-gw)# mode route-based
evt(config-ike-gw)# mobike disable
evt(config-ike-gw)# bind-interface vti 1
evt(config-ike-gw)# version v2-only
evt(config-ike-gw)# exit

```

Создадим профиль параметров безопасности для IPsec-туннеля. В профиле укажем алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IPsec-туннеля:

```

evt(config)# security ipsec proposal ipsec_prop1
evt(config-ipsec-proposal)# authentication algorithm md5
evt(config-ipsec-proposal)# encryption algorithm aes128
evt(config-ipsec-proposal)# exit

```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы:

```

evt(config)# security ipsec policy ipsec_pol1
evt(config-ipsec-policy)# proposal ipsec_prop1
evt(config-ipsec-policy)# exit

```

Создадим IPsec VPN. В VPN указывается шлюз IKE-протокола, политика IP sec-туннеля, режим обмена ключами и способ установления соединения. После ввода всех параметров включим туннель командой **enable**:

```

evt(config)# security ipsec vpn ipsec1
evt(config-ipsec-vpn)# mode ike
evt(config-ipsec-vpn)# ike establish-tunnel route
evt(config-ipsec-vpn)# ike gateway ike_gw1
evt(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
evt(config-ipsec-vpn)# enable
evt(config-ipsec-vpn)# exit
evt(config)# exit

```

2. Конфигурирование R2

Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```

evt# configure
evt(config)# interface gi 1/0/1
evt(config-if)# ip address 120.11.5.1/24
evt(config-if)# security-zone untrusted
evt(config-if)# exit

```

Создадим туннель VTI. Трафик будет перенаправляться через VTI в IPsec-туннель. В качестве локального и удаленного шлюза указываются IP-адреса интерфейсов, граничащих с WAN:

```

evt(config)# tunnel vti 1
evt(config-vti)# remote address 180.100.0.1
evt(config-vti)# local address 120.11.5.1
evt(config-vti)# ip address 10.10.10.2/30
evt(config-vti)# enable
evt(config-vti)# exit

```

Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```

evt(config)# object-group service ISAKMP
evt(config-object-group-service)# port-range 500,4500
evt(config-object-group-service)# exit

```

Создадим статический маршрут до удаленной LAN-сети. Для каждой подсети, которая находится за IPsec-туннелем, нужно указать маршрут через VTI-туннель:

```

evt(config)# ip route 10.0.0.0/16 tunnel vti 1

```

Создадим профиль протокола IKE. В профиле укажем группу Диффи-Хэллмана 2, алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IKE-соединения:

```

evt(config)# security ike proposal ike_prop1
evt(config-ike-proposal)# dh-group 2
evt(config-ike-proposal)# authentication algorithm md5
evt(config-ike-proposal)# encryption algorithm aes128
evt(config-ike-proposal)# exit
evt(config)#

```

Создадим политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы и ключ аутентификации:

```

evt(config)# security ike policy ike_pol1
evt(config-ike-policy)# pre-shared-key hexadecimal 123FFF
evt(config-ike-policy)# proposal ike_prop1
evt(config-ike-policy)# exit

```

Создадим шлюз протокола IKE. В данном профиле указывается VTI-туннель, политика, версия протокола и режим перенаправления трафика в туннель:

```

evt(config)# security ike gateway ike_gw1
evt(config-ike-gw)# ike-policy ike_pol1
evt(config-ike-gw)# mode route-based
evt(config-ike-gw)# bind-interface vti 1
evt(config-ike-gw)# version v2-only
evt(config-ike-gw)# exit

```

Создадим профиль параметров безопасности для IPsec-туннеля. В профиле укажем алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IPsec-туннеля:

```

evt(config)# security ipsec proposal ipsec_prop1
evt(config-ipsec-proposal)# authentication algorithm md5
evt(config-ipsec-proposal)# encryption algorithm aes128
evt(config-ipsec-proposal)# exit

```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы.

```

evt(config)# security ipsec policy ipsec_pol1
evt(config-ipsec-policy)# proposal ipsec_prop1
evt(config-ipsec-policy)# exit

```

Создадим IPsec VPN. В VPN указывается шлюз IKE-протокола, политика IP sec-туннеля, режим обмена ключами и способ установления соединения. После ввода всех параметров включим туннель командой **enable**:

```

evt(config)# security ipsec vpn ipsec1
evt(config-ipsec-vpn)# mode ike
evt(config-ipsec-vpn)# ike establish-tunnel route
evt(config-ipsec-vpn)# ike gateway ike_gw1
evt(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
evt(config-ipsec-vpn)# enable
evt(config-ipsec-vpn)# exit
evt(config)# exit

```

Состояние туннеля можно посмотреть командой:

```

evt# show security ipsec vpn status ipsec1

```

Конфигурацию туннеля можно посмотреть командой:

```

evt# show security ipsec vpn configuration ipsec1

```

Алгоритм настройки Policy-based IPsec VPN

Шаг	Описание	Команда	Ключи
1	Создать IKE-экземпляр и перейти в режим его конфигурирования.	evt(config)# security ike proposal <NAME>	<NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа.
2	Указать описание конфигурируемого туннеля (необязательно).	evt(config-ike-proposal)# description<DESCRIPTION>	<DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов.
3	Определить алгоритм аутентификации для IKE.	evt(config-ike-proposal)# authentication algorithm <ALGORITHM>	<ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2-384, sha2-512.
4	Определить алгоритм шифрования для IKE.	evt(config-ike-proposal)# encryption algorithm <ALGORITHM>	<ALGORITHM> – протокол шифрования, принимает значения: des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256.

Шаг	Описание	Команда	Ключи
5	Определить номер группы Диффи-Хэллмана.	evt(config-ike-proposal)# dh-group <DH-GROUP>	<DH-GROUP> – номер группы Диффи-Хэллмана, принимает значения [1, 2, 5, 14, 15, 16, 17, 18].
6	Создать политику для профиля IKE и перейти в режим её конфигурирования.	evt(config)# security ike policy <NAME>	<NAME> – имя политики IKE, задаётся строкой до 31 символа.
7	Определить режим аутентификации.	evt(config-ike-policy)# authentication method <METHOD>	<METHOD> – метод аутентификации ключа. Может принимать значения: • pre - shared - key – метод аутентификации, использующий предварительно полученные ключи шифрования; • public - key – метод аутентификации, использующий сертификат.
8	Задать время жизни соединения протокола IKE (необязательно).	evt(config-ike-policy)# lifetime seconds <SEC>	<SEC> – период времени, принимает значения [4 ..86400] секунд. Значение по умолчанию: 10800.
9	Привязать политику к профилю.	evt(config-ike-policy)# proposal <NAME>	<NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа.
10	Указать ключ аутентификации.	evt(config-ike-policy)# pre-shared-key ascii-text<TEXT>	<TEXT> – строка [1..64] ASCII-символов.
11	Создать шлюз для IKE и перейти в режим его конфигурирования.	evt(config)# security ike gateway <NAME>	<NAME> – имя шлюза протокола IKE, задаётся строкой до 31 символа.
12	Привязать политику IKE.	evt(config-ike-gw)# ike-policy <NAME>	<NAME> – имя политики протокола IKE, задаётся строкой до 31 символа.
13	Указать версию IKE (необязательно).	evt(config-ike-gw)# version <VERSION>	<version> – версия IKE-протокола: v1-only или v2-only .

Шаг	Описание	Команда	Ключи
14	Установить режим перенаправления трафика в туннель.	evt(config-ike-gw)# mode<MODE>	<MODE> – режим перенаправления трафика в туннель, принимает значения: • policy - based – трафик перенаправляется на основе принадлежности к указанным в политиках подсетям; • route - based – трафик перенаправляется на основе маршрутов, шлюзом у которых является туннельный интерфейс.
15	Указать действие для DPD (необязательно).	evt(config-ike-gw)# dead-peer-detection action <MODE>	<MODE> – режим работы DPD: • restart – соединение переустанавливается; • clear – соединение останавливается; • hold – соединение поддерживается; • none – механизм выключен, никаких действий не предпринимается.
16	Указать интервал между отправкой сообщений механизмом DPD (необязательно).	evt(config-ike-gw)# dead-peer-detection interval <SEC>	<SEC> – интервал между отправкой сообщений механизмом DPD, принимает значения [1..180] секунд.
17	Указать период времени ожидания ответа на сообщения механизма DPD при использовании протокола IKE версии 1 (необязательно).	evt(config-ike-gw)# dead-peer-detection timeout <SEC>	<SEC> – период времени ожидания ответа на сообщения механизма DPD при использовании протокола IKE версии 1, принимает значения [1..180] секунд. Значение по умолчанию: 30 секунд.
18	Указать базовый период времени ожидания ответа на сообщения механизма DPD при использовании протокола IKE версии 2 (необязательно).	evt(config-ike-gw)# dead-peer-detection retransmit timeout <SEC>	<SEC> – базовый период времени ожидания ответа на сообщения механизма DPD при использовании протокола IKE версии 2, принимает значения [1..30] секунд. Значение по умолчанию: 4 секунды.

Шаг	Описание	Команда	Ключи
19	Указать количество попыток повторной отправки сообщений механизма DPD после наступления таймаута ожидания ответа при использовании протокола IKE версии 2 (необязательно).	evt(config-ike-gw)# dead-peer-detection retransmit tries <TRIES>	<TRIES> – количество попыток повторной отправки сообщений механизма DPD в случае наступления таймаута ожидания ответа при использовании протокола IKE версии 2, принимает значения от 1 до 10. Для первого отправленного сообщения DPD период времени ожидания ответа будет равен базовому периоду, указанному в команде dead-peer-detection retransmit timeout, а для последующих попыток интервал ожидания будет рассчитан по формуле: "dead-peer-detection retransmit timeout" * 1.8 ^ (N-1), где N - номер попытки. Значение по умолчанию: 5 попыток.
20	Указать уровень случайного разброса периода ожидания ответа на сообщения механизма DPD при использовании протокола IKE версии 2 (необязательно).	evt(config-ike-gw)# dead-peer-detection retransmit jitter <VALUE>	<VALUE> – максимальный процент разброса значений, принимает значения [0..100]. Значение по умолчанию: 0 %
21	Указать ограничение максимального периода времени ожидания ответа на сообщения механизма DPD при использовании протокола IKE версии 2 (необязательно).	evt(config-ike-gw)# dead-peer-detection retransmit limit <SEC>	<SEC> – максимальный период времени ожидания ответа на сообщения механизма DPD при использовании протокола IKE версии 2, принимает значения [15..300] секунд. Значение по умолчанию: 0 секунд, у периода нет верхнего предела.
22	Установить IP-адрес удаленного шлюза IPsec-туннеля.	evt(config-ike-gw)# remote address <ADDR>	<ADDR> – IP-адрес удаленного шлюза.

Шаг	Описание	Команда	Ключи
23	Установить IP-адрес подсети получателя, а также IP-протокол и порт.	evt(config-ike-gw)# remote network <ADDR/LEN> [protocol { <TYPE> <ID> } [port <PORT>]]	<ADDR/LEN> – IP-адрес и маска подсети отправителя. Параметр задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]; <TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre; <ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF]; <PORT> – TCP/UDP-порт, принимает значения [1..65535].
24	Создать в профиль IPsec.	evt(config)# security ipsec proposal <NAME>	<NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа.
25	Определить алгоритм аутентификации для IPsec.	evt(config-ipsec-proposal)# authentication algorithm <ALGORITHM>	<ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2-384, sha2-512.
26	Определить алгоритм шифрования для IPsec.	evt(config-ipsec-proposal)# encryption algorithm <ALGORITHM>	<ALGORITHM> – протокол шифрования, принимает значения: des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256.

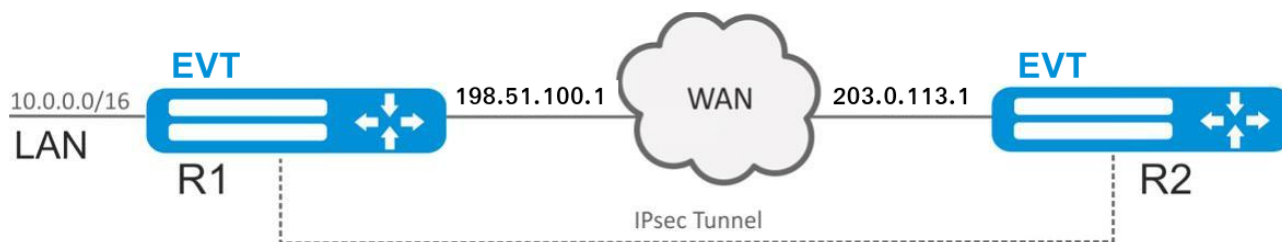
Шаг	Описание	Команда	Ключи
27	Указать протокол (необязательно).	evt(config-ipsec-proposal)# protocol <PROTOCOL>	<PROTOCOL> – инкапсулирующий протокол, принимает значения • ah – данный протокол осуществляет только аутентификацию трафика, шифрование данных не выполняется; • esp – данный протокол осуществляет аутентификацию и шифрование трафика. Значение по умолчанию: esp.
28	Создать политику для профиля IPsec и перейти в режим её конфигурирования.	evt(config)# security ipsec policy <NAME>	<NAME> – имя политики IPsec, задаётся строкой до 31 символа.
29	Привязать политику к профилю.	evt(config-ipsec-policy)# proposal <NAME>	<NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа.
30	Задать время жизни IPsec-туннеля (необязательно).	evt(config-ipsec-policy)# lifetime { seconds <SEC> packets <PACKETS> kilobytes <KB> }	<SEC> – период времени жизни IPsec-туннеля, по истечении которого происходит пересогласование. Принимает значения [1140..86400] секунд. <PACKETS> – количество пакетов, после передачи которых происходит пересогласование IPsec-туннеля. Принимает значения [4..86400]. <KB> – объем трафика, после передачи которого происходит пересогласование IPsec-туннеля. Принимает значения [4..4608000] секунд.
31	Создать IPsec VPN и перейти в режим конфигурирования.	evt(config)# security ipsecvpn <NAME>	<NAME> – имя VPN, задаётся строкой до 31 символа.
32	Определить режим согласования данных, необходимых для активации VPN.	evt(config-ipsec-vpn)# mode <MODE>	<MODE> – режим работы VPN.

Шаг	Описание	Команда	Ключи
33	Привязать IPsec политику к VPN.	evt(config-ipsec-vpn)# ike ipsec-policy <NAME>	<NAME> – имя IPsec-политики, задаётся строка до 31 символа.
34	Задать значение DSCP для использования в IP-заголовке исходящих пакетов IKE-протокола (необязательно).	evt(config-ipsec-vpn)# ike dscp <DSCP>	DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].
35	Установить режим активации VPN.	evt(config-ipsec-vpn)# ike establish-tunnel <MODE>	<MODE> – режим активации VPN: • by - request – соединение активируется встречной стороной; • route – соединение активируется при появлении трафика, маршрутизируемого в туннель; • immediate – туннель активируется автоматически после применения конфигурации.
36	Осуществить привязка IKE-шлюза к VPN.	evt(config-ipsec-vpn)# ike gateway <NAME>	<NAME> – имя IKE-шлюза, задаётся строкой до 31 символа.
37	Установить значение временного интервала в секундах, по истечению которого соединение закрывается, если не было принято или передано ни одного пакета через SA (необязательно).	evt(config-ipsec-vpn)# ike idle-time <TIME>	<TIME> – интервал в секундах, принимает значения [4..86400].
38	Отключить пересогласование ключей до разрыва IKE-соединения по истечению времени, количеству переданных пакетов или байт (необязательно).	evt(config-ipsec-vpn)# ike rekey disable	

Шаг	Описание	Команда	Ключи
39	Настроить начало пересогласования ключей IKE-соединения до истечения времени жизни (необязательно).	evt(config-ipsec-vpn)# ike rekey margin { seconds <SEC> packets <PACKETS> kilobytes <KB> }	<SEC> – интервал времени в секундах, оставшийся до закрытия соединения (задается командой <code>lifetimeseconds</code>). Принимает значения [4..86400]. <PACKETS> – количество пакетов, оставшихся до закрытия соединения (задается командой <code>lifetimepackets</code>). Принимает значения [4..86400]. <KB> – объем трафика в килобайтах, оставшийся до закрытия соединения (задается командой <code>lifetimekilobytes</code>). Принимает значения [4..86400].
40	Установить уровень случайного разброса значений параметров <code>marginseconds</code> , <code>marginpackets</code> , <code>marginkilobytes</code> (необязательно).	evt(config-ipsec-vpn)# ike rekey randomization <VALUE>	<VALUE> – максимальный процент разброса значений, принимает значения [1..100].
41	Описать VPN (необязательно).	evt(config-ipsec-vpn)# description <DESCRIPTION>	<DESCRIPTION> – описание профиля, задаётся строкой до 255 символов.
42	Активировать IPsec VPN.	evt(config-ipsec-vpn)# enable	

Пример настройки Policy-based IPsec VPN

Задача:



Настроить IPsec-туннель между R1 и R2.

R1 IP-адрес – 198.51.100.1;

R2 IP-адрес – 203.0.113.1.

IKE:

- группа Диффи-Хэллмана: 2;
- алгоритм шифрования: AES 128 bit;
- алгоритм аутентификации: MD5.

IPsec:

- алгоритм шифрования: AES 128 bit;
- алгоритм аутентификации: MD5.

Решение:

 Предварительно в firewall необходимо разрешить протокол ESP и ISAKMP (UDP-порт 500, 4500).

1. Конфигурирование R1

Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```
evt# configure
evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# ip address 198.51.100.1/24
evt(config-if-gi)# security-zone untrusted
evt(config-if-gi)# exit
```

Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```
evt(config)# object-group service ISAKMP
evt(config-object-group-service)# port-range 500,4500
evt(config-object-group-service)# exit
```

Создадим профиль протокола IKE. В профиле укажем группу Диффи-Хэллмана 2, алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IKE-соединения:

```
evt(config)# security ike proposal ike_prop1
evt(config-ike-proposal)# dh-group 2
evt(config-ike-proposal)# authentication algorithm md5
evt(config-ike-proposal)# encryption algorithm aes128
evt(config-ike-proposal)# exit
```

Создадим политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы и ключ аутентификации:

```
evt(config)# security ike policy ike_pol1
evt(config-ike-policy)# pre-shared-key hexadecimal 123FFF
evt(config-ike-policy)# proposal ike_prop1
evt(config-ike-policy)# exit
```

Создадим шлюз протокола IKE. В данном профиле указывается VTI-туннель, политика, версия протокола и режим перенаправления трафика в туннель:

```

evt(config)# security ike gateway ike_gw1
evt(config-ike-gw)# ike-policy ike_pol1
evt(config-ike-gw)# local address 198.51.100.1
evt(config-ike-gw)# local network 10.0.0.0/16
evt(config-ike-gw)# remote address 203.0.113.1
evt(config-ike-gw)# remote network 192.0.2.0/24
evt(config-ike-gw)# mode policy-based
evt(config-ike-gw)# exit

```

Создадим профиль параметров безопасности для IPsec-туннеля. В профиле укажем алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IPsec-туннеля:

```

evt(config)# security ipsec proposal ipsec_prop1
evt(config-ipsec-proposal)# authentication algorithm md5
evt(config-ipsec-proposal)# encryption algorithm aes128
evt(config-ipsec-proposal)# exit

```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы.

```

evt(config)# security ipsec policy ipsec_pol1
evt(config-ipsec-policy)# proposal ipsec_prop1
evt(config-ipsec-policy)# exit

```

Создадим IPsec VPN. В VPN указывается шлюз IKE-протокола, политика IP sec-туннеля, режим обмена ключами и способ установления соединения. После ввода всех параметров включим туннель командой **enable**:

```

evt(config)# security ipsec vpn ipsec1
evt(config-ipsec-vpn)# mode ike
evt(config-ipsec-vpn)# ike establish-tunnel route
evt(config-ipsec-vpn)# ike gateway ike_gw1
evt(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
evt(config-ipsec-vpn)# enable
evt(config-ipsec-vpn)# exit
evt(config)# exit

```

2. Конфигурирование R2

Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```

evt# configure
evt(config)# interface gi 1/0/1
evt(config-if)# ip address 203.0.113.1/24
evt(config-if)# security-zone untrusted
evt(config-if)# exit

```

Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```

evt(config)# object-group service ISAKMP
evt(config-addr-set)# port-range 500
evt(config-addr-set)# exit

```


Создадим профиль протокола IKE. В профиле укажем группу Диффи-Хэллмана 2, алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IKE-соединения:

```

evt(config)# security ike proposal ike_prop1
evt(config-ike-proposal)# dh-group 2
evt(config-ike-proposal)# authentication algorithm md5
evt(config-ike-proposal)# encryption algorithm aes128
evt(config-ike-proposal)# exit
evt(config)#

```

Создадим политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы и ключ аутентификации:

```

evt(config)# security ike policy ike_pol1
evt(config-ike-policy)# pre-shared-key hexadecimal 123FFF
evt(config-ike-policy)# proposal ike_prop1
evt(config-ike-policy)# exit

```

Создадим шлюз протокола IKE. В данном профиле указывается VTI-туннель, политика, версия протокола и режим перенаправления трафика в туннель:

```

evt(config)# security ike gateway ike_gw1
evt(config-ike-gw)# ike-policy ike_pol1
evt(config-ike-gw)# remote address 198.51.100.1
evt(config-ike-gw)# remote network 10.0.0.0/16
evt(config-ike-gw)# local address 203.0.113.1
evt(config-ike-gw)# local network 192.0.2.0/24
evt(config-ike-gw)# mode policy-based
evt(config-ike-gw)# exit

```

Создадим профиль параметров безопасности для IPsec-туннеля. В профиле укажем алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IPsec-туннеля:

```

evt(config)# security ipsec proposal ipsec_prop1
evt(config-ipsec-proposal)# authentication algorithm md5
evt(config-ipsec-proposal)# encryption algorithm aes128
evt(config-ipsec-proposal)# exit

```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы.

```

evt(config)# security ipsec policy ipsec_pol1
evt(config-ipsec-policy)# proposal ipsec_prop1
evt(config-ipsec-policy)# exit

```

Создадим IPsec VPN. В VPN указывается шлюз IKE-протокола, политика IPsec-туннеля, режим обмена ключами и способ установления соединения. После ввода всех параметров включим туннель командой **enable**:

```

evt(config)# security ipsec vpn ipsec1
evt(config-ipsec-vpn)# mode ike
evt(config-ipsec-vpn)# ike establish-tunnel route
evt(config-ipsec-vpn)# ike gateway ike_gw1
evt(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
evt(config-ipsec-vpn)# enable
evt(config-ipsec-vpn)# exit
evt(config)# exit

```

Состояние туннеля можно посмотреть командой:

```

evt# show security ipsec vpn status ipsec1

```

Конфигурацию туннеля можно посмотреть командой:

```

evt# show security ipsec vpn configuration ipsec1

```

Алгоритм настройки Remote Access IPsec VPN

Remote Access IPsec VPN – сценарий организации временных VPN-подключений, в котором сервер IPsec VPN находится в режиме ожидания входящих подключений, а клиенты осуществляют временные подключения к серверу для получения доступа к сетевым ресурсам.

Дополнительной особенностью RA IPsec VPN является возможность использования двухфакторной аутентификации IPsec, где первым фактором аутентификации является Extended Authentication (XAUTH) или Extensible Authentication Protocol (EAP), а вторым фактором аутентификации является пара логин-пароль для клиента IPsec VPN.

Шаг	Описание	Команда	Ключи
1	Создать IKE-экземпляр и перейти в режим его конфигурирования.	evt(config)# security ike proposal <NAME>	<NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа.
2	Указать описание конфигурируемого туннеля (необязательно).	evt(config-ike-proposal)# description <DESCRIPTION>	<DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов.
3	Определить алгоритм аутентификации для IKE (необязательно).	evt(config-ike-proposal)# authentication algorithm <ALGORITHM>	<ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2-384, sha2-512. Значение по умолчанию: sha1.

Шаг	Описание	Команда	Ключи
4	Установить IP-адрес локальной стороны VTI-туннеля (необязательно).	evt(config-vti)# ip address <ADDR/LEN> [unit <ID>] или evt(config-vti)# ip address <ADDR/LEN> secondary [unit <ID>]	<ADDR/LEN> – IP-адрес и префикс подсети задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..31]; <ID> – номер юнита, принимает значения [1..2]. Ключ secondary указывает, что настроенный адрес является дополнительным IP-адресом. Если это ключевое слово отсутствует, настроенный адрес является основным IP-адресом. Возможно указать до 7 дополнительных IP-адресов.
5	Определить номер группы Диффи-Хэллмана (необязательно).	evt(config-ike-proposal)# dh-group <DH-GROUP>	<DH-GROUP> – номер группы Диффи-Хэллмана, принимает значения [1, 2, 5, 14, 15, 16, 17, 18]. Значение по умолчанию: 1.
6	Создать политику для профиля IKE и перейти в режим её конфигурирования.	evt(config)# security ike policy <NAME>	<NAME> – имя политики IKE, задаётся строкой до 31 символа.
7	Определить режим аутентификации.	evt(config-ike-policy)# authentication method <METHOD>	<METHOD> – метод аутентификации ключа. Может принимать значения: • xauth - psk - key – метод двухфакторной аутентификации, использующий пару логин-пароль и предварительно полученные ключи шифрования; • eap - метод двухфакторной аутентификации, использующий пару логин-пароль и предварительно полученные сертификаты.
8	Задать режим клиента (только для клиента).	evt(config-ike-policy)# authentication mode client	

Шаг	Описание	Команда	Ключи
9	Задать время жизни соединения протокола IKE (необязательно).	evt(config-ike-policy)# lifetime seconds <SEC>	<SEC> – период времени, принимает значения [4 ..86400] секунд. Значение по умолчанию: 3600.
10	Привязать политику к профилю.	evt(config-ike-policy)# proposal <NAME>	<NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа.
11	Указать ключ аутентификации.	evt(config-ike-policy)# pre-shared-key ascii-text <TEXT>	<TEXT> – строка [1..64] ASCII символов.
12	Указать сертификаты и ключи (только для метода EAP)	evt-10(config-ike-policy)# crypto <CERTIFICATE-TYPE> <NAME>	<CERTIFICATE-TYPE> – тип сертификата или ключа, может принимать следующие значения: • ca – сертификат удостоверяющего сервера; • crl – список отозванных сертификатов; • local-crt – публичный сертификат сервера удалённого доступа; • local-crt-key – приватный ключ сервера удалённого доступа. <NAME> – имя сертификата или ключа, задаётся строкой до 31 символа. На стороне сервера необходимо добавить набор сертификатов (ca, local-crt, local-key). На стороне клиента необходимо указать только корневой сертификат (ca).
13	Создать профиль доступа.	evt(config)# access profile <NAME>	<NAME> – имя профиля доступа, задаётся строкой до 31 символа.
14	Создать имя пользователя.	evt(config-access-profile)# user <LOGIN>	<LOGIN> – логин клиента, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
15	Задать пароль пользователя.	evt(config-profile)# password ascii-text <TEXT>	<TEXT> – строка [8..32] ASCII символов.
16	Создать пул адресов назначения (только для сервера).	evt(config)# address-assignment pool <NAME>	<NAME> – имя пула адресов назначения, задаётся строкой до 31 символа.
17	Задать подсеть, из которой будут выдаваться IP клиентам (только для сервера).	evt(config-pool)# ip prefix <ADDR/ LEN>	<ADDR/LEN> – адрес подсети и префикс.
18	Создать шлюз для IKE и перейти в режим его конфигурирования.	evt(config)# security ike gateway <NAME>	<NAME> – имя шлюза протокола IKE, задаётся строкой до 31 символа.
19	Привязать политику IKE.	evt(config-ike-gw)# ike-policy <NAME>	<NAME> – имя политики протокола IKE, задаётся строкой до 31 символа.
20	Установить режим перенаправления трафика в туннель.	evt(config-ike-gw)# mode <MODE>	<MODE> – режим перенаправления трафика в туннель, принимает значения: • policy - based – трафик перенаправляется на основе принадлежности к указанным в политиках подсетям.
21	Указать действие для DPD (необязательно).	evt(config-ike-gw)# dead-peer- detection action <MODE>	<MODE> – режим работы DPD: • restart – соединение переустанавливается; • clear – соединение останавливается; • hold – соединение поддерживается; • none – механизм выключен, никаких действий не предпринимается. Значение по умолчанию: none.
22	Указать интервал между отправкой сообщений механизмом DPD (необязательно).	evt(config-ike-gw)# dead-peer- detection interval <SEC>	<SEC> – интервал между отправкой сообщений механизмом DPD, принимает значения [1..180] секунд. Значение по умолчанию: 2.

Шаг	Описание	Команда	Ключи
23	Указать период времени ожидания ответа на сообщения механизма DPD при использовании протокола IKE версии 1 (необязательно).	evt(config-ike-gw)# dead-peer-detection timeout <SEC>	<SEC> – период времени ожидания ответа на сообщения механизма DPD при использовании протокола IKE версии 1, принимает значения [1..180] секунд. Значение по умолчанию: 30 секунд.
24	Указать базовый период времени ожидания ответа на сообщения механизма DPD при использовании протокола IKE версии 2 (необязательно).	evt(config-ike-gw)# dead-peer-detection retransmit timeout <SEC>	<SEC> – базовый период времени ожидания ответа на сообщения механизма DPD при использовании протокола IKE версии 2, принимает значения [1..30] секунд. Значение по умолчанию: 4 секунды.
25	Указать количество попыток повторной отправки сообщений механизма DPD после наступления таймаута ожидания ответа при использовании протокола IKE версии 2 (необязательно).	evt(config-ike-gw)# dead-peer-detection retransmit tries <TRIES>	<TRIES> – количество попыток повторной отправки сообщений механизма DPD в случае наступления таймаута ожидания ответа при использовании протокола IKE версии 2, принимает значения от 1 до 10. Для первого отправленного сообщения DPD период времени ожидания ответа будет равен базовому периоду, указанному в команде dead-peer-detection retransmit timeout, а для последующих попыток интервал ожидания будет рассчитан по формуле: "dead-peer-detection retransmit timeout" * 1.8 ^ (N-1), где N - номер попытки. Значение по умолчанию: 5 попыток.
26	Указать уровень случайного разброса периода ожидания ответа на сообщения механизма DPD при использовании протокола IKE версии 2 (необязательно).	evt(config-ike-gw)# dead-peer-detection retransmit jitter <VALUE>	<VALUE> – максимальный процент разброса значений, принимает значения [0..100]. Значение по умолчанию: 0 %

Шаг	Описание	Команда	Ключи
27	Указать ограничение максимального периода времени ожидания ответа на сообщения механизма DPD при использовании протокола IKE версии 2 (необязательно).	evt(config-ike-gw)# dead-peer-detection retransmit limit <SEC>	<SEC> – максимальный период времени ожидания ответа на сообщения механизма DPD при использовании протокола IKE версии 2, принимает значения [15..300] секунд. Значение по умолчанию: 0 секунд, у периода нет верхнего предела.
28	Задать пул динамического выделения IP-адресов клиентам (только для сервера).	evt(config-ike-gw)# remote network dynamic pool <NAME>	<NAME> – имя пула адресов назначения, задаётся строкой до 31 символа.
29	Задать режим динамического установления удаленной подсети (только для клиента).	evt(config-ike-gw)# remote network dynamic client	
30	Задать профиль доступа (только для сервера).	evt(config-ike-gw)# access-profile <NAME>	<NAME> – имя профиля доступа, задаётся строкой до 31 символа.
31	Задать профиль доступа и логин (только для клиента).	evt(config-ike-gw)# access-profile <NAME> client <LOGIN>	<NAME> – имя профиля доступа, задаётся строкой до 31 символа; <LOGIN> – логин клиента, задаётся строкой до 31 символа.
32	Задать интерфейс терминции выделенного IP для построения IPsec VPN (только для клиента).	evt(config-ike-gw)# assign-interface loopback <INDEX>	<INDEX> – индекс интерфейса, принимает значения [1..65535].
33	Создать профиль IPsec.	evt(config)# security ipsec proposal <NAME>	<NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа.
34	Определить алгоритм аутентификации для IPsec (необязательно).	evt(config-ipsec-proposal)# authentication algorithm <ALGORITHM>	<ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2-384, sha2-512. Значение по умолчанию: sha1.

Шаг	Описание	Команда	Ключи
35	Определить алгоритм шифрования для IPsec (необязательно).	evt(config-ipsec-proposal)# encryption algorithm <ALGORITHM>	<ALGORITHM> – протокол шифрования, принимает значения: des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256. Значение по умолчанию: 3des.
36	Указать протокол (необязательно).	evt(config-ipsec-proposal)# protocol <PROTOCOL>	<PROTOCOL> – инкапсулирующий протокол, принимает значения: • ah – данный протокол осуществляет только аутентификацию трафика, шифрование данных не выполняется; • esp – данный протокол осуществляет аутентификацию и шифрование трафика. Значение по умолчанию: esp.
37	Задать config-ipsec-proposal конфигурирования.	evt(config)# security ipsec policy <NAME>	<NAME> – имя политики IPsec, задаётся строкой до 31 символа.
38	Привязать политику к профилю.	evt(config-ipsec-policy)# proposal <NAME>	<NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
39	Задать время жизни IPsec-туннеля (необязательно).	evt(config-ipsec-policy)# lifetime { seconds <SEC> packets <PACKETS> kilobytes <KB> }	<SEC> – период времени жизни IPsec-туннеля, по истечении которого происходит пересогласование. Принимает значения [1140..86400] секунд. Значение по умолчанию: 540. <PACKETS> – количество пакетов, после передачи которых происходит пересогласование IPsec-туннеля. Принимает значения [4..86400]. Значение по умолчанию: отключено. <KB> – объем трафика, после передачи которого происходит пересогласование IPsec-туннеля. Принимает значения [4..4608000] секунд. Значение по умолчанию: отключено.
40	Создать IPsec VPN и перейти в режим конфигурирования.	evt(config)# security ipsec vpn <NAME>	<NAME> – имя VPN, задаётся строкой до 31 символа.
41	Определить режим согласования данных, необходимых для активации VPN.	evt(config-ipsec-vpn)# mode <MODE>	<MODE> – режим работы VPN, принимает значения: ike, manual.
42	Привязать IPsec политику к VPN.	evt(config-ipsec-vpn)# ike ipsec-policy <NAME>	<NAME> – имя IPsec-политики, задаётся строка до 31 символа.
43	Задать значение DSCP для использования в IP-заголовке исходящих пакетов IKE-протокола (необязательно).	evt(config-ipsec-vpn)# ike dscp <DSCP>	DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 63.

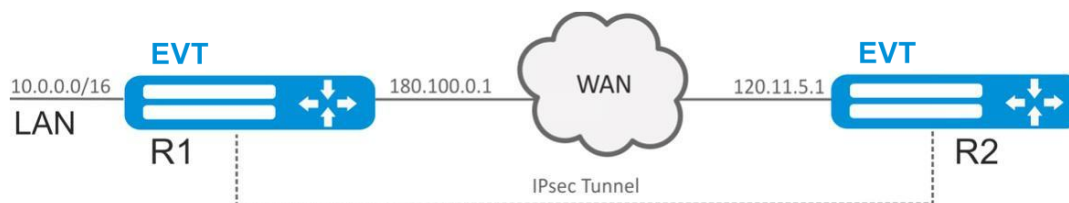
Шаг	Описание	Команда	Ключи
44	Устанавливается режим активации VPN.	evt(config-ipsec-vpn)# ike establish-tunnel <MODE>	<MODE> – режим активации VPN: • by - request – соединение активируется встречной стороной, доступно для сервера; • route – соединение активируется при появлении трафика, маршрутизируемого в туннель, доступно для сервера; • immediate – туннель активируется автоматически после применения конфигурации, доступно для клиента.
45	Осуществить привязку IKE-шлюза к VPN.	evt(config-ipsec-vpn)# ike gateway <NAME>	<NAME> – имя IKE-шлюза, задаётся строкой до 31 символа.
46	Установить значение временного интервала в секундах, по истечению которого соединение закрывается, если не было принято или передано ни одного пакета через SA (необязательно).	evt(config-ipsec-vpn)# ike idle-time <TIME>	<TIME> – интервал в секундах, принимает значения [4..86400]. Значение по умолчанию: 0.
47	Отключить пересогласование ключей до разрыва IKE-соединения по истечению времени, количеству переданных пакетов или байт (необязательно).	evt(config-ipsec-vpn)# ike rekey disable	Значение по умолчанию: включено.

Шаг	Описание	Команда	Ключи
48	Настроить начало пересогласования ключей IKE-соединения до истечения времени жизни (необязательно).	evt(config-ipsec-vpn)# ike rekey margin { seconds <SEC> packets <PACKETS> kilobytes <KB> }	<SEC> – интервал времени в секундах, оставшийся до закрытия соединения (задается командой <code>lifetimeseconds</code>). Принимает значения [4..86400]. Значение по умолчанию: 540 <PACKETS> – количество пакетов, оставшихся до закрытия соединения (задается командой <code>lifetimepackets</code>). Принимает значения [4..86400]. Значение по умолчанию: отключено. <KB> – объем трафика в килобайтах, оставшийся до закрытия соединения (задается командой <code>lifetimekilobytes</code>). Принимает значения [4..86400] Значение по умолчанию: отключено.
49	Установить уровень случайного разброса значений параметров <code>marginseconds</code> , <code>marginpackets</code> , <code>marginkilobytes</code> (необязательно).	evt(config-ipsec-vpn)# ike rekey randomization <VALUE>	<VALUE> – максимальный процент разброса значений, принимает значения [1..100]. Значение по умолчанию: 100.
50	Описать VPN (необязательно).	evt(config-ipsec-vpn)# description <DESCRIPTION>	<DESCRIPTION> – описание профиля, задаётся строкой до 255 символов.
51	Активировать IPsec VPN.	evt(config-ipsec-vpn)# enable	

Шаг	Описание	Команда	Ключи
52	Включить режим переподключения клиентов XAUTH с одним логином/паролем (только для сервера) (необязательно).	evt(config-ipsec-vpn)# security ike session uniqueids <MODE>	<MODE> – режим переподключения, принимает следующие значения: • no – установленное подключение XAUTH будет удалено, если для нового подключения XAUTH инициатором соединения будет отправлено уведомление "INITIAL_CONTACT", будет назначен ранее использованный IP-адрес. В противном случае, установленное соединение XAUTH будет удержано. Для нового подключения XAUTH будет назначен новый IP-адрес. • never – установленное подключение XAUTH будет удержано. Для нового подключения XAUTH будет назначен новый IP-адрес. Уведомление "INITIAL_CONTACT" будет в любом случае проигнорировано. • replace – установленное подключение XAUTH будет удалено. Для нового подключения XAUTH будет использован ранее использованный IP-адрес. • keep – установленное подключение XAUTH будет удержано. Новое подключение XAUTH будет отклонено.

Пример настройки Remote Access IPsec VPN

Задача:



Настроить Remote Access IPsec VPN между R1 и R2 с использованием второго фактора аутентификации IPsec - XAUTH. В качестве сервера IPsec VPN настроить маршрутизатор R1, а маршрутизатор R2 в качестве клиента IPsec VPN.

R2 IP-адрес – 120.11.5.1;

R1 IP-адрес – 180.100.0.1;

Клиентам IPsec VPN:

- выдавать адреса из пула подсети 192.0.2.0/24
- предоставлять доступ до LAN подсети 10.0.0.0/16

IKE:

- группа Диффи-Хэллмана: 2;
- алгоритм шифрования: 3DES;
- алгоритм аутентификации: SHA1.

IPsec:

- алгоритм шифрования: 3DES;
- алгоритм аутентификации: SHA1.

XAUTH:

- логин: client1;
- пароль: password123.

Решение:

 Предварительно в firewall необходимо разрешить протокол ESP и ISAKMP (UDP-порт 500, 4500).

1. Конфигурирование R1

Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```

evt# configure
evt(config)# security zone untrusted
evt(config-zone)# exit
evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# security-zone untrusted
evt(config-if-gi)# ip address 180.100.0.1/24
evt(config-if-gi)# exit

```

Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```

evt(config)# object-group service ISAKMP
evt(config-object-group-service)# port-range 500,4500
evt(config-object-group-service)# exit

```

Создадим профиль протокола IKE. В профиле укажем группу Диффи-Хэлла 2, алгоритм шифрования 3 DES, алгоритм аутентификации SHA1. Данные параметры безопасности используются для защиты IKE-соединения:

```

evt(config)# security ike proposal IKEPROP
evt(config-ike-proposal)# dh-group 2
evt(config-ike-proposal)# authentication algorithm sha1
evt(config-ike-proposal)# encryption algorithm 3des
evt(config-ike-proposal)# exit

```

Создадим политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы, ключ аутентификации и метод аутентификации XAUTH по ключу:

```

evt(config)# security ike policy IKEPOLICY
evt(config-ike-policy)# pre-shared-key hexadecimal 123FFF
evt(config-ike-policy)# authentication method xauth-psk-key
evt(config-ike-policy)# proposal IKEPROP
evt(config-ike-policy)# exit

```

Создадим профиль доступа и заведем в нем пару логин и пароль для клиента IPsec VPN:

```

evt(config)# access profile XAUTH
evt(config-access-profile)# user client1
evt(config-profile)# password ascii-text password123
evt(config-profile)# exit
evt(config-access-profile)# exit

```

Создадим пул адресов назначения, из которого будут выдаваться IP клиентам IPsec VPN:

```

evt-1000(config)# address-assignment pool CLIENT_POOL
evt-1000(config-pool)# ip prefix 192.0.2.0/24
evt-1000(config-pool)# exit

```

Создадим шлюз протокола IKE. В данном профиле необходимо указать политику протокола IKE, указать локальную подсеть, в качестве удаленной подсети указать пул адресов назначения, задать режим перенаправления трафика в туннель по политике и использование второго фактора аутентификации XAUTH:

```

evt(config)# security ike gateway IKEGW
evt(config-ike-gw)# ike-policy IKEPOLICY
evt(config-ike-gw)# local address 180.100.0.1
evt(config-ike-gw)# local network 10.0.0.0/16
evt(config-ike-gw)# remote address any
evt(config-ike-gw)# remote network dynamic pool CLIENT_POOL
evt(config-ike-gw)# dead-peer-detection action clear
evt(config-ike-gw)# mode policy-based
evt(config-ike-gw)# access-profile XAUTH

```

```
evt(config-ike-gw)# exit
```

Создадим профиль параметров безопасности для IPsec-туннеля. В профиле укажем алгоритм шифрования 3DES, алгоритм аутентификации SHA1. Данные параметры безопасности используются для защиты IPsec-туннеля:

```
evt(config)# security ipsec proposal IPSECPROP
evt(config-ipsec-proposal)# authentication algorithm sha1
evt(config-ipsec-proposal)# encryption algorithm 3des
evt(config-ipsec-proposal)# exit
```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы.

```
evt(config)# security ipsec policy IPSECPOLICY
evt(config-ipsec-policy)# proposal IPSECPROP
evt(config-ipsec-policy)# exit
```

Создадим IPsec VPN. В VPN указывается шлюз IKE-протокола, политика IPsec-туннеля, режим обмена ключами и режим ожидания входящего соединения IPsec – *by-request*. После ввода всех параметров включим туннель командой **enable**:

```
evt(config)# security ipsec IPSECVPN
evt(config-ipsec-vpn)# mode ike
evt(config-ipsec-vpn)# ike establish-tunnel by-request
evt(config-ipsec-vpn)# ike gateway IKEGW
evt(config-ipsec-vpn)# ike ipsec-policy IPSECPOLICY
evt(config-ipsec-vpn)# enable
evt(config-ipsec-vpn)# exit
```

Разрешим протокол esp и udp порты 500, 4500 в конфигурации firewall для установления IPsec VPN:

```
evt(config)# security zone-pair untrusted self
evt(config-zone-pair)# rule 1
evt(config-zone-pair-rule)# action permit
evt(config-zone-pair-rule)# match protocol udp
evt(config-zone-pair-rule)# match destination-port ISAKMP
evt(config-zone-pair-rule)# enable
evt(config-zone-pair-rule)# exit
evt(config-zone-pair)# rule 2
evt(config-zone-pair-rule)# action permit
evt(config-zone-pair-rule)# match protocol esp
evt(config-zone-pair-rule)# enable
evt(config-zone-pair-rule)# exit
evt(config-zone-pair)# end
```

2. Конфигурирование R2

Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```
evt# configure
evt(config)# interface gi 1/0/1
evt(config-if)# ip address 120.11.5.1/24
evt(config-if)# security-zone untrusted
evt(config-if)# exit
```

Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```

evt(config)# object-group service ISAKMP
evt(config-addr-set)# port-range 500,4500
evt(config-addr-set)# exit

```

Создадим профиль протокола IKE. В профиле укажем группу Диффи-Хэллмана 2, алгоритм шифрования 3 DES, алгоритм аутентификации SHA1. Данные параметры безопасности используются для защиты IKE-соединения:

```

evt(config)# security ike proposal IKEPROP
evt(config-ike-proposal)# dh-group 2
evt(config-ike-proposal)# authentication algorithm sha1
evt(config-ike-proposal)# encryption algorithm 3des
evt(config-ike-proposal)# exit

```

Создадим политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы, ключ аутентификации, метод аутентификации XAUTH по ключу и режим аутентификации – клиент:

```

evt(config)# security ike policy IKEPOLICY
evt(config-ike-policy)# pre-shared-key hexadecimal 123FFF
evt(config-ike-policy)# authentication method xauth-psk-key
evt(config-ike-policy)# authentication mode client
evt(config-ike-policy)# proposal IKEPROP
evt(config-ike-policy)# exit

```

Создадим профиль доступа и заведем в нем пару логин и пароль:

```

evt(config)# access profile XAUTH
evt(config-access-profile)# user client1
evt(config-profile)# password ascii-text password123
evt(config-profile)# exit
evt(config-access-profile)# exit

```

Создадим интерфейс loopback для терминции IP-адреса, полученного от IPsec VPN сервера:

```

evt(config)# interface loopback 8
evt(config-loopback)# exit

```

Создадим шлюз протокола IKE. В данном профиле указывается политика, интерфейс терминции, режим динамического установления удаленной подсети, выбор профиля доступа для XAUTH и режим перенаправления трафика в туннель по политике:

```

evt(config)# security ike gateway IKEGW
evt(config-ike-gw)# ike-policy IKEPOLICY
evt(config-ike-gw)# assign-interface loopback 8
evt(config-ike-gw)# local address 120.11.5.1
evt(config-ike-gw)# remote address 180.100.0.1
evt(config-ike-gw)# remote network dynamic client
evt(config-ike-gw)# mode policy-based
evt(config-ike-gw)# access-profile xauth client client1
evt(config-ike-gw)# exit

```


Создадим профиль параметров безопасности для IPsec-туннеля. В профиле укажем алгоритм шифрования 3DES, алгоритм аутентификации SHA1. Данные параметры безопасности используются для защиты IPsec-туннеля:

```

evt(config)# security ipsec proposal IPSECPROP
evt(config-ipsec-proposal)# authentication algorithm sha1
evt(config-ipsec-proposal)# encryption algorithm 3des
evt(config-ipsec-proposal)# exit

```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы:

```

evt(config)# security ipsec policy IPSECPOLICY
evt(config-ipsec-policy)# proposal IPSECPROP
evt(config-ipsec-policy)# exit

```

Создадим IPsec VPN. В VPN указывается шлюз IKE-протокола, политика IP sec-туннеля, режим обмена ключами и способ установления соединения. После ввода всех параметров включим туннель командой **enable**:

```

evt(config)# security ipsec vpn IPSECVPN
evt(config-ipsec-vpn)# mode ike
evt(config-ipsec-vpn)# ike establish-tunnel route
evt(config-ipsec-vpn)# ike gateway IKEGW
evt(config-ipsec-vpn)# ike ipsec-policy IPSECPOLICY
evt(config-ipsec-vpn)# enable
evt(config-ipsec-vpn)# exit

```

Разрешим протокол esp и udp порты 500,4500 в конфигурации firewall для установления IPsec VPN:

```

evt(config)# security zone-pair untrusted self
evt(config-zone-pair)# rule 1
evt(config-zone-pair-rule)# action permit
evt(config-zone-pair-rule)# match protocol udp
evt(config-zone-pair-rule)# match destination-port ISAKMP
evt(config-zone-pair-rule)# enable
evt(config-zone-pair-rule)# exit
evt(config-zone-pair)# rule 2
evt(config-zone-pair-rule)# action permit
evt(config-zone-pair-rule)# match protocol esp
evt(config-zone-pair-rule)# enable
evt(config-zone-pair-rule)# exit
evt(config-zone-pair)# end

```

Состояние туннеля можно посмотреть командой:

```

evt# show security ipsec vpn status IPSECVPN

```

Конфигурацию туннеля можно посмотреть командой:

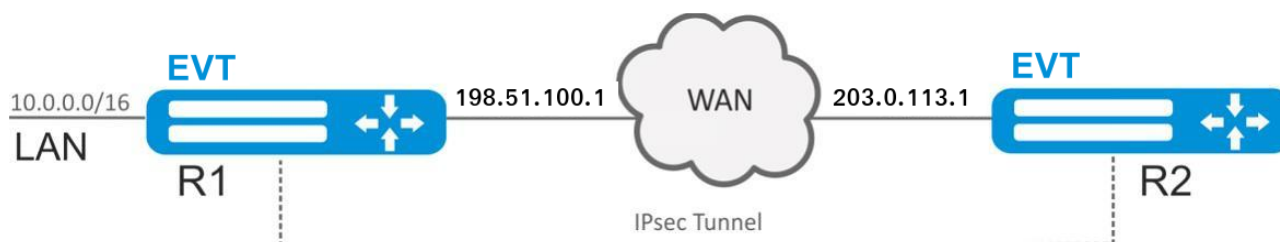
```

evt# show security ipsec vpn configuration IPSECVPN

```

Пример настройки DPD (Dead Peer Detection)

Задача:



Настроить Dead Peer Detection на R1 для Policy-based IPsec VPN между R1 и R2.

Исходную конфигурацию можно взять из [примера настройки Policy-based IPsec VPN](#).

Решение:

На R1 в шлюзе протокола IKE укажем: режим работы DPD – restart, интервал опроса – 1 секунду, таймаут – 4 секунды:

```

evt# configure
evt(config)# security ike gateway ike_gw1
evt(config-ike-gw)# dead-peer-detection action restart
evt(config-ike-gw)# dead-peer-detection interval 1
evt(config-ike-gw)# dead-peer-detection timeout 4
evt(config-ike-gw)# exit

```

Состояние туннеля можно посмотреть командой:

```

evt# show security ipsec vpn status ipsec1

```

Конфигурацию туннеля можно посмотреть командой:

```

evt# show security ipsec vpn configuration ipsec1

```

После разрыва соединения между R1 и R2 на R1 IPsec-туннель начнет перестраиваться спустя 4 секунды после разрыва.

```

evt# show security ipsec vpn status
Name                               Local host      Remote host      Initiator spi
Responder spi                      State
-----
ipsec1                             198.51.100.1    203.0.113.1     0x7a77a25a55853255
0xb62fd04f2db43d08               Established
2037-10-30T07:52:53+00:00 %CLI-I-CMD: user admin from console  input: show security ipsec vpn
status
evt# show security ipsec vpn status
Name                               Local host      Remote host      Initiator spi
Responder spi                      State
-----

```

```

ipsec1          198.51.100.1      203.0.113.1      0x77706e37b4e68cce
0x0000000000000000 Connecting
2037-10-30T07:52:57+00:00 %CLI-I-CMD: user admin from console input: show security ipsec vpn
status

```

Настройка LT-туннелей

LT (англ. Logical Tunnel – логический туннель) – тип туннелей, предназначенный для передачи маршрутной информации и трафика между различными виртуальными маршрутизаторами (VRF), сконфигурированными на одном аппаратном маршрутизаторе. LT-туннель может использоваться для организации взаимодействия между двумя или более VRF с применением ограничений firewall.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать LT-туннели для каждого из существующих VRF.	evt(config)# tunnel lt <ID>	<ID> – идентификатор туннеля в диапазоне [1..128].
2	Указать описание конфигулируемых туннелей (необязательно).	evt(config-lt)# description <DESCRIPTION>	<DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов.
3	Включить каждый LT-туннель в соответствующий VRF.	evt(config-lt)# ip vrf forwarding <VRF>	<VRF> – имя VRF, задается строкой до 31 символа.
4	Включить каждый LT-туннель в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall для LT-туннеля.	evt(config-lt)# security-zone<NAME>	<NAME> – имя зоны безопасности, задаётся строкой до 12 символов.
		evt(config-lt)# ip firewall disable	
5	Для каждого LT-туннеля задать номер противоположный LT туннель (в другом VRF).	evt(config-lt)# peer lt <ID>	<ID> – идентификатор туннеля в диапазоне [1..128].

Шаг	Описание	Команда	Ключи
6	Для каждого LT-туннеля указать IP-адрес для маршрутизации пакетов. Для взаимодействующих LT-туннелей, IP-адреса должны быть из одной IP-подсети.	evt(config-lt)# ip address <ADDR/LEN> [unit <ID>] или evt(config-lt)# ip address <ADDR/LEN> secondary [unit <ID>]	<ADDR/LEN> – IP-адрес и префикс подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]; <ID> – номер юнита, принимает значения [1..2]. Ключ secondary указывает, что настроенный адрес является дополнительным IP-адресом. Если это ключевое слово отсутствует, настроенный адрес является основным IP-адресом. Возможно указать до 7 дополнительных IP-адресов.
7	Включить туннели.	evt(config-lt)# enable	
8	Для каждого VRF настроить необходимые протоколы маршрутизации через LT-туннель.		
9	Задать интервал времени, за который усредняется статистика о нагрузке на туннеле (необязательно).	evt(config-lt)# load-average <TIME>	<TIME> – интервал в секундах, принимает значения [5..150]. Значение по умолчанию: 5.
10	Указать размер MTU (Maximum Transmission Unit) пакетов, которые может пропускать данный bridge (необязательно; возможно, если в bridge включен только VLAN). MTU более 1500 будет активно только в случае применения команды "system jumbo-frames".	evt(config-lt)# mtu <MTU>	<MTU> – значение MTU, принимает значения в диапазоне – [1280..9500]; Значение по умолчанию: 1500.

Пример настройки

Задача:

Организовать взаимодействие между хостами, терминированными в двух VRF vrf_1 и vrf_2.

Исходная конфигурация:

```
hostname evt
ip vrf vrf_1
exit
```

```

ip vrf vrf_2
exit
interface gigabitethernet 1/0/1
 ip vrf forwarding vrf_1
 ip firewall disable
 ip address 10.0.0.1/24
exit
interface gigabitethernet 1/0/2
 ip vrf forwarding vrf_2
 ip firewall disable
 ip address 10.0.1.1/24
exit

```

Решение:

Создадим LT-туннели для каждого VRF с указанием IP-адресов из одной подсети:

```

evt(config)# tunnel lt 1
evt(config-lt)# ip vrf forwarding vrf_1
evt(config-lt)# ip firewall disable
evt(config-lt)# ip address 192.168.0.1/30
evt(config-lt)# exit
evt(config)# tunnel lt 2
evt(config-lt)# ip vrf forwarding vrf_2
evt(config-lt)# ip firewall disable
evt(config-lt)# ip address 192.168.0.2/30
evt(config-lt)# exit

```

Укажем для каждого LT-туннеля LT-туннель из VRF, с которым необходимо установить связь, и активируем их:

```

evt(config)# tunnel lt 1
evt(config-lt)# peer lt 2
evt(config-lt)# enable
evt(config-lt)# exit
evt(config)# tunnel lt 2
evt(config-lt)# peer lt 1
evt(config-lt)# enable
evt(config-lt)# exit

```

⚠ Если в VRF не сконфигурирован ни один из протоколов динамической маршрутизации, то необходимо указать статические маршруты для каждого VRF:

```

evt(config)# ip route vrf vrf_1 0.0.0.0/0 192.168.0.2
evt(config)# ip route vrf vrf_2 0.0.0.0/0 192.168.0.1

```

6.2.10 Управление функциями второго уровня (L2)

- [Настройка физического интерфейса](#)
 - [Алгоритм настройки](#)
 - [Пример настройки режима L2](#)
- [Настройка VLAN](#)
 - [Алгоритм настройки](#)
 - [Манипуляции с VLAN на интерфейсе](#)
 - [Пример настройки 1](#)
 - [Разрешение обработки VLAN в тегированном и нетегированном режимах](#)
 - [Пример настройки 1](#)
 - [Пример настройки Private Vlan](#)
- [Настройка LLDP](#)
 - [Алгоритм настройки](#)
 - [Пример настройки](#)
- [Настройка Bridge](#)
 - [Алгоритм настройки](#)
 - [Пример настройки bridge для VLAN](#)
 - [Пример настройки добавления/удаления второго VLAN-тега](#)
- [Настройка зеркалирования \(SPAN/RSPAN\)](#)
 - [Алгоритм настройки](#)
 - [Пример настройки](#)
- [Настройка LACP](#)
 - [Алгоритм настройки](#)
 - [Пример настройки](#)

⚠ Конфигурация на маршрутизаторах EVT и EVS производится с помощью одинаковых команд. Ниже приведены примеры настройки EVT.

Настройка физического интерфейса

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Переход в режим конфигурирования функционала.	evt(config)# interface gigabitethernet evt(config)# interface tengigabitethernet evt(config)# interface port-channel <ID>	<ID> – порядковый номер группы агрегации каналов, принимает значения [1..12].
2	Выключить интерфейс.	evt(config-if-gi)# shutdown	
3	Задать описание (не обязательно).	evt(config-if-gi)# description <text>	<text> – до 255 символов.
4	Задать MTU (не обязательно).	evt(config-if-gi)# mtu <count>	<count> – 552–10000. Значение по умолчанию: 1500.

Шаг	Описание	Команда	Ключи
5	Задать скорость и режим работы приемопередатчика (не обязательно).	evt(config-if-gi)# speed <SPEED> <DUPLEX>	<SPEED> – значение скорости: • 10M – значение скорости 10 Мбит/с; • 100M – значение скорости 100 Мбит/с; • 1000M – значение скорости 1000 Мбит/с; • 10G – значение скорости 10 Гбит/с; • auto – автоматический выбор режима (недоступно для 10G-интерфейсов). Значение по умолчанию: auto. <DUPLEX> – режим работы приемопередатчика, принимает значения: • full-duplex – дуплекс; • half-duplex – полудуплекс.
6	Задать MAC-адрес (не обязательно).	evt(config-if-gi)# mac-address <ADDR>	<ADDR> – MAC-адрес сетевого моста, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF].

i На данном этапе настройки нет необходимости в задании настроек firewall.

Пример настройки режима L2

Задача:

Настроить интерфейс gigabitethernet 1/0/1 на прохождение трафика следующим образом:

- Задать MAC-address 68:13:e2:7e:e4:9a;
- Перевести интерфейс в режим Switchport;
- Установить значение MTU=1400;
- Перевести интерфейс в режим работы Full-duplex на скорости 10M.



Решение:

Перейдём в режим конфигурирования интерфейса gigabitethernet 1/0/1 и зададим на нём MAC-address 68:13:e2:7e:e4:9a:

```
evt# configure
evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# mac-address 68:13:e2:7e:e4:9a
```

Переведём интерфейс в режим switchport:

```
evt(config-if-gi)# mode switchport
```

Установим значение MTU на интерфейсе, равное 1400:

```
evt(config-if-gi)# mtu 1400
```

Установим на интерфейсе скорость 10М и согласуем режим работы приемопередатчика в полном дуплексе. Выйдем из режима конфигурирования, применим и сохраним настройки:

```
evt(config-if-gi)# speed 10m full-duplex
evt(config-if-gi)# end
evt# commit
evt# confirm
```

Проверим настроенные параметры на интерфейсе:

```
evt# show interfaces switch-port status gigabitethernet 1/0/1
Interface      gigabitethernet 1/0/1
Status:        Up
Media:         copper
Speed:         10M
Duplex:        full
Flow Control:  Disabled
MDI Mode:      MDI
```

Настройка VLAN

VLAN (англ. *Virtual Local Area Network*) — логическая («виртуальная») локальная сеть, представляет собой группу устройств, которые взаимодействуют между собой на канальном уровне независимо от их физического местонахождения. Работа VLAN основана на использовании дополнительных полей Ethernet-заголовка согласно стандарту 802.1q. По сути, VLAN изолирует широковещательный домен путем ограничения коммутации Ethernet-фреймов только с одинаковым VLAN-ID в Ethernet-заголовке.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать VLAN.	evt(config)# vlan <VID>	<VID> – идентификатор VLAN, задаётся в диапазоне [2..4094]. Также есть возможность создания нескольких vlan (через запятую), диапазона vlan (через дефис или комбинированную запись, содержащую запятые и дефисы).
2	Задать имя vlan (не обязательно).	evt(config-vlan)# name <vlan-name>	<vlan-name> – до 255 символов.
3	Отключить отслеживание состояния интерфейсов, на которых разрешена обработка Ethernet-фреймов данного VLAN (не обязательно).	evt(config-vlan)# force-up	
4	Установить режим работы физического интерфейса.	evt(config-if-gi)# mode switchport	
5	Отключить обработку входящих нетегированных Ethernet-фреймов на основе таблицы коммутации VLAN-а по умолчанию (VLAN-ID – 1) (не обязательно).	evt(config-if-gi)# switchport forbidden default-vlan	
6	Задать режим работы L2-интерфейса.	evt(config-if-gi)# switchport mode access	Данный режим является режимом по умолчанию и не отображается в конфигурации.
		evt(config-if-gi)# switchport mode trunk	
7	Настроить список VLAN на интерфейсе.	evt(config-if-gi)# switchport trunk allowed vlan <ACT> <VID>	<ACT> – назначаемое действие: add – включение интерфейса во VLAN; remove – исключение интерфейса из VLAN. <VID> – идентификационный номер VLAN, задаётся в диапазоне [2...4094]. Можно задать диапазоном через «-» или перечислением через «,».

Шаг	Описание	Команда	Ключи
8	Настроить VLAN в качестве Default VLAN на данном интерфейсе для нетегированного трафика, поступающего на данный порт.	evt(config-if-gi)# switchport trunk native-vlan <VID>	<VID> – идентификатор VLAN, задаётся в диапазоне [2..4094].
10	Разрешить на интерфейсе обработку Ethernet-фреймов всех созданных на маршрутизаторе VLAN (не обязательно).	evt(config-if-gi)# switchport trunk allowed vlan auto-all	
11	Перевести интерфейс в режим изоляции по группам (не обязательно).	evt(config-if-gi)# switchport protected-port	
12	Добавить интерфейс в группу изоляции (не обязательно). Данная команда актуальна, только если порт находится в режиме изоляции по группам.	evt(config-if-gi)# switchport community	<ID> – идентификатор группы, принимает значение в диапазоне [1...30].
13	Включить функцию Private VLAN на интерфейсе (не обязательно).	evt(config-if-gi)# switchport protected	<IF> – интерфейс, задается в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора .

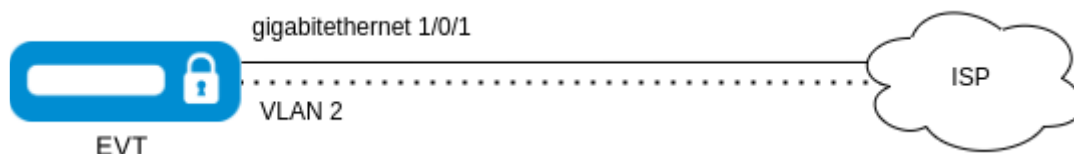
Манипуляции с VLAN на интерфейсе

Пример настройки 1

i Данный пример предназначен для использования при конфигурировании VLAN на всех EVT/EVS.

Задача:

На основе заводской конфигурации для EVT-101 удалить из VLAN 2 порт gigabitethernet 1/0/1 и назначить его на интерфейс gigabitethernet 1/0/2 в нетегированном режиме.



Решение:

Попадём на интерфейс gigabitethernet 1/0/1 и удалим его из VLAN 2:

```
evt# configure
evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# no switchport access vlan
evt(config-if-gi)# exit
```

Перейдём на интерфейс gigabitethernet 1/0/2 и назначим его в VLAN 2:

```
evt(config)# interface gigabitethernet 1/0/2
evt(config-if-gi)# switchport access vlan 2
```

Применим и сохраним изменения конфигурации:

```
evt(config-if-gi)# end
evt# commit
evt# confirm
```

Проверим, что внесенные изменения вступили в силу, и теперь интерфейс gigabitethernet 1/0/2 принадлежит к VLAN 2 в нетегированном режиме:

```
evt# show vlans 2
```

VID	Name	Tagged	Untagged
2	--		gi1/0/2, te1/0/1

Разрешение обработки VLAN в тегированном и нетегированном режимах

Пример настройки 1

i Данный пример предназначен для использования при конфигурировании VLAN на всех устройствах EVT/EVS.

Задача:

На EVT-101 настроить интерфейс gigabitethernet 1/0/1 на режим trunk для передачи и приема фреймов в VLAN 2, VLAN 64, VLAN 2000 в тегированном режиме в сторону устройства Switch. Интерфейс gigabitethernet 1/0/2 настроить на режим access для определения нетегированного трафика от PC в VLAN 2.



Решение:

Перейдём в глобальный режим конфигурирования устройства и создадим VLAN 2, VLAN 64, VLAN 2000:

```

evt(config)# vlan 2,64,2000
evt(config-vlan)# exit
  
```

Перейдём в режим настройки интерфейса gigabitethernet 1/0/1, запретим использование default-vlan (VLAN 1) и настроим его принадлежность к VLAN 2, VLAN 64, VLAN 2000 в тегированном режиме:

```

evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# mode switchport
evt(config-if-gi)# switchport forbidden default-vlan
evt(config-if-gi)# switchport mode trunk
evt(config-if-gi)# switchport trunk allowed vlan add 2,64,2000
evt(config-if-gi)# exit
  
```

Перейдём в режим настройки интерфейса gigabitethernet 1/0/2 и определим его к VLAN 2 в нетегированном режиме:

```

evt(config)# interface gigabitethernet 1/0/2
evt(config-if-gi)# mode switchport
evt(config-if-gi)# switchport access vlan 2
  
```

Применим и сохраним изменения конфигурации:

```

evt(config-if-gi)# end
evt# commit
evt# confirm
  
```

Проверим, что внесенные изменения вступили в силу, и теперь интерфейс gigabitethernet 1/0/1 принадлежит к VLAN 2, 64, 2000, настроенным в тегированном режиме, а интерфейс gigabitethernet 1/0/2 принадлежит к VLAN 2 в нетегированном режиме:

```

evt# show vlans
VID      Name      Tagged      Untagged
-----
2        --        gi1/0/1     gi1/0/2
64       --        gi1/0/1
2000    --        gi1/0/1

```

Пример настройки Private Vlan

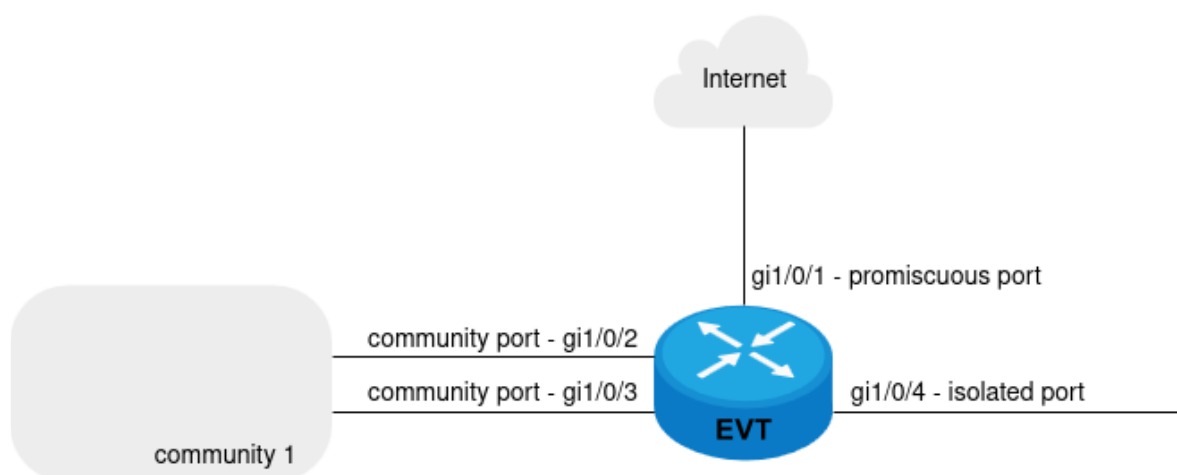
Технология Private VLAN (PVLAN) позволяет производить разграничение трафика на втором уровне модели OSI между портами маршрутизатора, которые находятся в одном широковещательном домене.

На маршрутизаторе может быть сконфигурировано три типа PVLAN-портов:

- promiscuous – это порт, который способен обмениваться данными между любыми интерфейсами, включая isolated- и community-порты PVLAN;
- isolated – это порт, который полностью изолирован от других портов внутри одного и того же PVLAN, но не от promiscuous-портов. PVLAN блокируют весь трафик, идущий в сторону isolated-портов, кроме трафика со стороны promiscuous-портов; пакеты со стороны isolated-портов могут передаваться только в сторону promiscuous-портов;
- community – это группа портов, которые могут обмениваться данными между собой и promiscuous-портами, эти интерфейсы отделены на втором уровне модели OSI от всех остальных community-интерфейсов, а также isolated-портов внутри PVLAN.

Задача:

Настроить изоляцию портов в одном широковещательном домене (PVLAN). Порты gi1/0/2 и gi1/0/3 должны относиться к community 1, порт gi1/0/4 должен быть изолирован в сторону promission port. В качестве promission port выступает gi1/0/1.



Решение:

Создайте VLAN 10:

```
evt(config)# vlan 10
evt(config-vlan)# exit
```

Настройте интерфейс gi1/0/1 в режиме «promiscuous port»:

```
evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# mode switchport
evt(config-if-gi)# switchport forbidden default-vlan
evt(config-if-gi)# switchport mode trunk
evt(config-if-gi)# switchport trunk allowed vlan add 10
evt(config-if-gi)# exit
```

Настройте интерфейсы gi1/0/2, gi1/0/3 в режиме «community port»:

```
evt(config)# interface gigabitethernet 1/0/2
evt(config-if-gi)# mode switchport
evt(config-if-gi)# switchport protected-port
evt(config-if-gi)# switchport community 1
evt(config-if-gi)# switchport forbidden default-vlan
evt(config-if-gi)# switchport mode trunk
evt(config-if-gi)# switchport trunk allowed vlan add 10
evt(config-if-gi)# exit
evt(config)# interface gigabitethernet 1/0/3
evt(config-if-gi)# mode switchport
evt(config-if-gi)# switchport protected-port
evt(config-if-gi)# switchport community 1
evt(config-if-gi)# switchport forbidden default-vlan
evt(config-if-gi)# switchport mode trunk
evt(config-if-gi)# switchport trunk allowed vlan add 10
evt(config-if-gi)# exit
```

Настройте интерфейс gi1/0/4 в режиме «isolated port»:

```
evt(config)# interface gigabitethernet 1/0/4
evt(config-if-gi)# mode switchport
evt(config-if-gi)# switchport protected gigabitethernet 1/0/1
evt(config-if-gi)# switchport forbidden default-vlan
evt(config-if-gi)# switchport mode trunk
evt(config-if-gi)# switchport trunk allowed vlan add 10
evt(config-if-gi)# exit
```

Информацию о состоянии физических интерфейсов в режиме изоляции по группам можно узнать с помощью команды:

```
evt# show interfaces protected-ports
```

Настройка LLDP

Link Layer Discovery Protocol (LLDP) — протокол канального уровня, позволяющий сетевому оборудованию оповещать оборудование, работающее в локальной сети, о своём существовании и передавать ему свои характеристики, а также получать от него аналогичные сведения.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Активировать LLDP на маршрутизаторе.	evt(config)# lldp enable	
2	Включить прием и обработку LLDPDU на физическом интерфейсе.	evt(config-if-gi)# lldp receive	
3	Включить отправку LLDPDU на физическом интерфейсе.	evt(config-if-gi)# lldp transmit	
4	Установить период отправки LLDPDU (не обязательно).	evt(config)# lldp timer <SEC>	<SEC> – период времени в секундах, принимает значение [1..32768]. Значение по умолчанию: 30.
5	Установить период, в течение которого маршрутизатор хранит информацию, полученную по LLDP (не обязательно).	evt(config)# lldp hold-multiplier <SEC>	<SEC> – период времени в секундах, принимает значение [1..10]. Значение по умолчанию: 4.
6	Установить IP-адрес, который будет передаваться в LLDP TLV в качестве management-address (не обязательно).	evt(config)# lldp management-address <ADDR>	<ADDR> – IP-адрес, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. По умолчанию задается один из существующих.
7	Установить поле system-description, которое будет передаваться в LLDP TLV в качестве system-description (не обязательно).	evt(config)# lldp system-description <DESCRIPTION>	<DESCRIPTION> – описание системы, задается строкой до 255 символов. По умолчанию содержит информацию о модели и версии ПО маршрутизатора.
8	Установить поле system-name, которое будет передаваться в LLDP TLV в качестве system-name (не обязательно).	evt(config)# lldp system-name <NAME>	<NAME> – имя системы, задается строкой до 255 символов. По умолчанию совпадает с заданным hostname.

Пример настройки

Задача:

Организовать обмен и обработку LLDPDU между маршрутизаторами EVT-1 и EVT-2.



Решение:

1. Конфигурирование R1

Включим LLDP глобально на маршрутизаторе:

```
evt(config)# lldp enable
```

Включим прием и отправку LLDPDU на интерфейсе gi 1/0/1:

```
evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# lldp receive
evt(config-if-gi)# lldp transmit
```

2. Конфигурирование R2

Включим LLDP глобально на маршрутизаторе:

```
evt(config)# lldp enable
```

Включим прием и отправку LLDPDU на интерфейсе gi 1/0/1:

```
evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# lldp receive
evt(config-if-gi)# lldp transmit
```

Общую информацию по LLDP соседям можно посмотреть командой:

```
evt# show lldp neighbors
```

Подробную информацию по соседу конкретного интерфейса можно посмотреть командой:

```
evt# show lldp neighbors gigabitethernet 1/0/1
```

Общую статистику по LLDP можно посмотреть командой:

```
evt# show lldp statistics
```


Настройка Bridge

Bridge (мост) — это способ соединения двух и более сегментов Ethernet на канальном уровне без использования протоколов более высокого уровня, таких как IP. Пакеты передаются на основе Ethernet-адресов, а не IP-адресов. Поскольку передача выполняется на канальном уровне (уровень 2 модели OSI), трафик протоколов более высокого уровня прозрачно проходит через мост.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Добавить сетевой мост (bridge) в систему и перейти в режим настройки его параметров.	evt(config)# bridge <BRIDGE-ID>	<BRIDGE-ID> – идентификационный номер моста, принимает значения в диапазоне – [1..250];
2	Активировать сетевой мост.	evt(config-bridge)# enable	
3	Указать экземпляр VRF, в котором будет работать данный интерфейс (не обязательно).	evt(config-bridge)# ip vrf forwarding <VRF>	<VRF> – имя VRF, задается строкой до 31 символа.
4	Назначить описание конфигурируемому сетевому мосту (не обязательно).	evt(config-bridge)# description <DESCRIPTION>	<DESCRIPTION> – описание сетевого моста, задаётся строкой до 255 символов.
5	Связать саб-интерфейс, qinq-интерфейс, L2GRE-туннель или L2TPv3-туннель с сетевым мостом. Связанные интерфейсы/туннели и сетевые мосты автоматически становятся участниками общего L2-домена (не обязательно).	evt(config-if-gi)# bridge-group <BRIDGE-ID> evt(config-if-l2tpv3)# bridge-group <BRIDGE-ID>	<BRIDGE-ID> – идентификационный номер моста, принимает значения в диапазоне – [1..250];
6	Связать текущий сетевой мост с VLAN. Все интерфейсы и L2-туннели, являющиеся членами назначаемого VLAN, автоматически включаются в сетевой мост и становятся участниками общего L2-домена (не обязательно).	evt(config-bridge)# vlan <VID>	<VID> – идентификатор VLAN, задаётся в диапазоне [1..4094].
7	Указать размер MTU (Maximum Transmission Unit) пакетов, которые может пропускать данный bridge (не обязательно; возможно, если в bridge включен только VLAN). MTU более 1500 будет активно только в случае применения команды "system jumbo-frames".	evt(config-bridge)# mtu <MTU>	<MTU> – значение MTU, принимает значения в диапазоне – [552..9500]; Значение по умолчанию: 1500.

Шаг	Описание	Команда	Ключи
8	Указать IPv4/IPv6-адрес и маску подсети для конфигурируемого интерфейса или включить получение IP-адреса динамически.	evt(config-bridge)# ip address <ADDR/LEN> [unit <ID>] или evt(config-bridge)# ip address <ADDR/LEN> secondary [unit <ID>]	<ADDR/LEN> – IP-адрес и длина маски подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. <ID> – номер юнита, принимает значения [1..2]. Ключ secondary указывает, что настроенный адрес является дополнительным IP-адресом. Если это ключевое слово отсутствует, настроенный адрес является основным IP-адресом. Возможно указать до 7 дополнительных IP-адресов. Дополнительные функции IPv4-адресации см. в разделе Настройка IP-адресации.
		evt(config-bridge)# ipv6 address <IPV6-ADDR/LEN> [unit <ID>]	<IPV6-ADDR/LEN> – IP-адрес и префикс подсети, задаётся в виде X:X:X:X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128]. <ID> – номер юнита, принимает значения [1..2]. Дополнительные функции IPv6-адресации см. в разделе Настройка IPv6-адресации. Можно указать несколько IPv4/IPv6-адресов перечислением через запятую. Может быть назначено до 8 IPv4/IPv6-адресов на интерфейс.
		evt(config-bridge)# ip address dhcp	Дополнительные функции при работе DHCP-клиента см. в разделе Управление DHCP-клиентом.

Шаг	Описание	Команда	Ключи
9	Отключить на интерфейсе функции Firewall или включить интерфейс в зону безопасности (см. раздел Конфигурирование Firewall).	evt(config-bridge)# ip firewall disable	
		evt(config-bridge)# security-zone <NAME>	<NAME> – имя зоны безопасности, задаётся строкой до 31 символа.
10	Включить запись статистики использования текущего интерфейса (не обязательно).	evt(config-bridge)# history statistics	
11	Задать интервал времени, за который усредняется статистика о нагрузке на bridge (не обязательно).	evt(config-bridge)# load-average <TIME>	<TIME> – интервал в секундах, принимает значения [5..150]. Значение по умолчанию: 5.
12	Задать MAC-адрес сетевого моста, отличный от системного (не обязательно).	evt(config-bridge)# mac-address <ADDR>	<ADDR> – MAC-адрес сетевого моста, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF].

Шаг	Описание	Команда	Ключи
13	Включить на bridge режим изоляции интерфейсов. В данном режиме обмен трафиком между членами сетевого моста запрещен (не обязательно). Командой protected-ports exclude {<IF> <TUN> <VLAN>} исключаются из списка изолируемых сущности, включенные в сетевой мост.	evt(config-bridge)# protected-ports <MODE>	• none – изоляция интерфейсов отключена. В данном режиме коммутация кадров между членами сетевого моста разрешена; • local – изоляция интерфейсов включена. В данном режиме коммутация кадров между членами сетевого моста запрещена; • radius – изоляция интерфейсов включена. Для использования данного режима требуется настройка Wi-Fi контроллера туннелей в режиме "radius". В данном режиме коммутация кадров между членами сетевого моста запрещена, за исключением SoftGRE DATA туннелей. Для SoftGRE DATA-туннелей параметры изоляции запрашиваются у RADIUS-сервера.
		evt(config-bridge)# protected-ports exclude {<IF> <TUN> <VLAN>}	<IF> – интерфейс, задается в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора. <TUN> – имя туннеля, задается в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора. <VLAN> – vlan, связанный с сетевым мостом.

Шаг	Описание	Команда	Ключи
14	Запретить коммутацию трафика unknown-unicast (когда MAC-адрес назначения не содержится в таблице коммутации) в данном bridge (не обязательно; применимо только на evt-1000/1200/1500/1511/1700/3100/3200/3200L/3300).	evt(config-bridge)# unknown-unicast-forwarding disable	
15	Установить время жизни IPv4/IPv6-записей в ARP-таблице, изученных на данном bridge (не обязательно).	evt(config-bridge)# ip arp reachable-time <TIME> или evt(config-bridge)# ipv6 nd reachable-time <TIME>	<TIME> – время жизни динамических MAC-адресов, в миллисекундах. Допустимые значения от 5000 до 100000000 миллисекунд. Реальное время обновления записи варьируется от [0,5;1,5]*<TIME>.

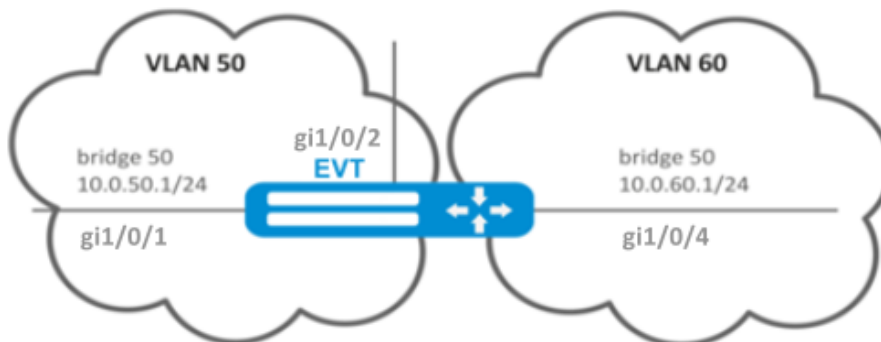
Также для bridge-интерфейса возможно настроить:

- QoS в базовом или расширенном режимах (см. раздел [Управление QoS](#));
- мониторинг трафика (см. разделы [Настройка Netflow](#));
- функции протоколов маршрутизации (см. раздел [Управление маршрутизацией](#));
- протокол VRRF (см. раздел [Управление резервированием](#));

Пример настройки bridge для VLAN

Задача:

Настроить маршрутизацию между VLAN 50 (10.0.50.0/24) и VLAN 60 (10.0.60.0/24). VLAN 50 должен относиться к зоне «LAN1», VLAN 60 – к зоне «LAN2». Необходимо разрешить свободную передачу трафика между зонами.



Решение:

Создадим VLAN 50, 60:

```
evt(config)# vlan 50,60
evt(config-vlan)# exit
```

Создадим зоны безопасности «LAN1» и «LAN2»:

```
evt(config)# security-zone LAN1
evt(config-zone)# exit
evt(config)# security-zone LAN2
evt(config-zone)# exit
```

Назначим интерфейсам gi1/0/1, gi1/0/2 VLAN 50:

```
evt(config)# interface gigabitethernet 1/0/1-2
evt(config-if-gi)# switchport general allowed vlan add 50 tagged
```

Назначим интерфейсу gi1/0/4 VLAN 60:

```
evt(config)# interface gigabitethernet 1/0/4
evt(config-if-gi)# switchport general allowed vlan add 60 tagged
```

Создадим bridge 50, привяжем VLAN 50, укажем IP-адрес 10.0.50.1/24 и членство в зоне «LAN1»:

```
evt(config)# bridge 50
evt(config-bridge)# vlan 50
evt(config-bridge)# ip address 10.0.50.1/24
evt(config-bridge)# security-zone LAN1
evt(config-bridge)# enable
```

Создадим bridge 60, привяжем VLAN 60, укажем IP-адрес 10.0.60.1/24 и членство в зоне «LAN2»:

```

evt(config)# bridge 60
evt(config-bridge)# vlan 60
evt(config-bridge)# ip address 10.0.60.1/24
evt(config-bridge)# security-zone LAN2
evt(config-bridge)# enable

```

Создадим правила в Firewall, разрешающие свободное прохождение трафика между зонами:

```

evt(config)# security zone-pair LAN1 LAN2
evt(config-zone-pair)# rule 1
evt(config-zone-pair-rule)# action permit
evt(config-zone-pair-rule)# enable
evt(config-zone-pair-rule)# exit
evt(config-zone-pair)# exit
evt(config)# security zone-pair LAN2 LAN1
evt(config-zone-pair)# rule 1
evt(config-zone-pair-rule)# action permit
evt(config-zone-pair-rule)# enable
evt(config-zone-pair-rule)# exit
evt(config-zone-pair)# exit
evt(config)# exit

```

Посмотреть членство интерфейсов в мосте можно командой:

```

evt# show interfaces bridge

```

Пример настройки добавления/удаления второго VLAN-тега

Задача:

На интерфейс gigabitethernet 1/0/1 поступают Ethernet-кадры с различными VLAN-тегами. Необходимо перенаправить их в интерфейс gigabitethernet 1/0/2, добавив второй VLAN-ID 828. При поступлении на интерфейс gigabitethernet 1/0/2 Ethernet-кадров с VLAN-ID 828 данный тег должен быть удален и отправлен в интерфейс gigabitethernet 1/0/1.

Решение:

Создадим на маршрутизаторе bridge без VLAN и без IP-адреса:

```

evt(config)# bridge 1
evt(config-bridge)# enable
evt(config-bridge)# exit

```

Включим интерфейс gigabitethernet 1/0/1 в bridge 1:

```

evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# bridge-group 1
evt(config-if-gi)# exit

```

Включим саб-интерфейс gigabitethernet 1/0/2.828 в bridge 1:

```
evt(config)# interface gigabitethernet 1/0/2.828
evt(config-if-sub)# bridge-group 1
evt(config-if-sub)# exit
```

⚠ При добавлении второго VLAN-тега в Ethernet-кадр его размер увеличивается на 4 байта. На интерфейсе маршрутизатора gigabitethernet 1/0/2 и на всем оборудовании, передающем Q-in-Q кадры, необходимо увеличить MTU на 4 байта или более.

Настройка зеркалирования (SPAN/RSPAN)

⚠ В текущей версии ПО функция удаленного зеркалирования (RSPAN) поддерживается на всех маршрутизаторах EVT/EVS.

Зеркалирование трафика – функция маршрутизатора, предназначенная для перенаправления трафика с одного порта маршрутизатора на другой порт этого же маршрутизатора (локальное зеркалирование) или на удаленное устройство (удаленное зеркалирование).

Алгоритм настройки

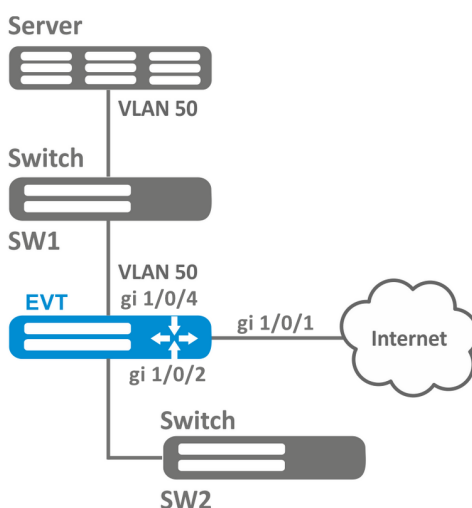
Шаг	Описание	Команда	Ключи
1	Определить VLAN, по которому будет передаваться отзеркалированный трафик (в случае использования удаленного зеркалирования).	evt(config)# port monitor remote vlan <VID> <DIRECTION>	<VID> – идентификационный номер VLAN, задаётся в диапазоне [2...4094]; <DIRECTION> – направление трафика: • tx – зеркалирование в указанный VLAN только исходящего трафика; • rx – зеркалирование в указанный VLAN только входящего трафика.
2	Включить режим удаленного зеркалирования (в случае использования удаленного зеркалирования).	evt(config)# port monitor remote	
3	Определить режим порта, передающего отзеркалированный трафик (не обязательно).	evt(config)# port monitor mode <MODE>	<MODE> – режим: • network – совмещенный режим передачи данных и зеркалирование (по умолчанию); • monitor-only – только зеркалирование.

Шаг	Описание	Команда	Ключи
4	В режиме конфигурации интерфейса включить зеркалирование.	evt(config-if-gi)# port monitor interface <IF> [<DIRECTION>]	<IF> – интерфейс, с которого будут зеркалироваться кадры; <DIRECTION> – направление трафика: • tx – зеркалирование только исходящего трафика; • rx – зеркалирование только входящего трафика.

Пример настройки

Задача:

Организовать удаленное зеркалирование трафика по VLAN 50 с интерфейса gi1/0/1 для передачи на сервер для обработки.



Решение:

Предварительно нужно выполнить следующие действия:

- Создать VLAN 50;
- На интерфейсе gi 1/0/4 добавить VLAN 50 в режиме general.

Основной этап конфигурирования:

Укажем VLAN, по которой будет передаваться зеркалированный трафик:

```
esr1000(config)# port monitor remote vlan 50
```

На интерфейсе gi 1/0/4 укажем порт для зеркалирования:

```
esr1000(config)# interface gigabitethernet 1/0/4
esr1000(config-if-gi)# port monitor interface gigabitethernet 1/0/1
```

Укажем на интерфейсе gi 1/0/4 режим удаленного зеркалирования:

```
esr1000(config-if-gi)# port monitor remote
```

Настройка LACP

LACP — протокол для агрегирования каналов, позволяет объединить несколько физических каналов в один логический. Такое объединение позволяет увеличивать пропускную способность и надежность канала.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Установить приоритет системы для протокола LACP.	evt(config)# lacp system-priority <PRIORITY>	<PRIORITY> – приоритет, указывается в диапазоне [1..65535]. Значение по умолчанию: 1.
2	Установить механизм балансировки нагрузки для групп агрегации каналов.	evt(config)# port-channel load-balance { src-dst-mac-ip src-dst-mac src-dst-ip src-dst-mac-ip-port }	• src - dst - mac - ip – механизм балансировки основывается на MAC-адресе и IP-адресе отправителя и получателя; • src - dst - mac – механизм балансировки основывается на MAC-адресе отправителя и получателя; • src - dst - ip – механизм балансировки основывается на IP-адресе отправителя и получателя; • src - dst - mac - ip - port – механизм балансировки основывается на MAC-адресе, IP-адресе и порте отправителя и получателя.
3	Установить административный таймаут протокола LACP.	evt(config)# lacp timeout {short long }	• long – длительное время таймаута; • short – короткое время таймаута. Значение по умолчанию: long.

Шаг	Описание	Команда	Ключи
4	Создать и перейти в режим конфигурирования агрегированного интерфейса.	evt(config)# interface port-channel <CH>	<CH> – порядковый номер группы агрегации каналов, принимает значения [1..12].
		evt(config)# interface port-channel <CH>.<S-VLAN>	<CH> – номер агрегированного интерфейса. <S-VLAN> – идентификатор создаваемого S-VLAN.
		evt(config)# interface port-channel <CH>.<S-VLAN>.<C-VLAN>	<C-VLAN> – идентификатор создаваемого C-VLAN.
5	Настроить необходимые параметры агрегированного канала.	evt(config-if-port-channel)# mode switchport	Установить интерфейс в режим L2
		evt(config-if-port-channel)# mode routerport	Установить интерфейс в режим L3
6	Задать скорость (не обязательно).	evt(config-if-port-channel)# speed <SPEED>	<SPEED> – значение скорости: • 10M – значение скорости 10 Мбит/с; • 100M – значение скорости 100 Мбит/с; • 1000M – значение скорости 1000 Мбит/с; • 10G – значение скорости 10 Гбит/с; • 25G – значение скорости 25 Гбит/с; • 40G – значение скорости 40 Гбит/с; • 100G – значение скорости 100 Гбит/с; Параметр наследуют все физические интерфейсы, принадлежащие данной группе агрегации каналов. Значение по умолчанию: 1000M

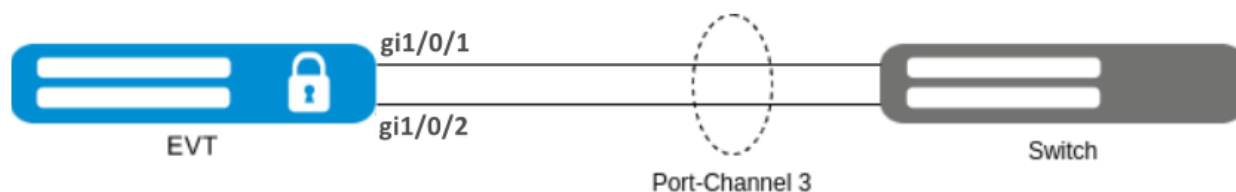
Шаг	Описание	Команда	Ключи
7	Изменить размер MTU (MaximumTransmissionUnit). MTU более 1500 будет активно, только если применена команда system jumbo-frames (не обязательно).	evt(config-if-port-channel)# mtu <MTU>	<MTU> – значение MTU в байтах. Параметр наследуют все физические интерфейсы, принадлежащие данной группе агрегации каналов. Значение по умолчанию: 1500.
8	Перейти в режим конфигурирования физического интерфейса.	evt(config)# interface <IF-TYPE><IF-NUM>	<IF-TYPE> – тип интерфейса (gigabitethernet или tengigabitethernet). <IF-NUM> – U/S/P – U-юнит (1), S – слот (0), P – порт.
9	Включить физический интерфейс в группу агрегации каналов с указанием режима формирования группы агрегации каналов.	evt(config-if-gi)# channel-group <ID> mode <MODE>	<ID> – порядковый номер группы агрегации каналов, принимает значения [1..12]. <MODE> – режим формирование группы агрегации каналов: • auto – добавить интерфейс в динамическую группу агрегации с поддержкой протокола LACP; • on – добавить интерфейс в статическую группу агрегации.
10	Установить LACP-приоритет интерфейса Ethernet.	evt(config-if-gi)# lacp port-priority <PRIORITY>	<PRIORITY> – приоритет, указывается в диапазоне [1..65535]. Значение по умолчанию: 1.
11	Установить интервал времени, в течение которого собирается статистика о нагрузке на интерфейс (не обязательно).	evt(config-if-gi)# load-average <TIME>	<TIME> – интервал в секундах, принимает значения [5..150].
12	Включить запись статистики использования текущего интерфейса (не обязательно).	evt(config-if-gi)# history statistics	

Шаг	Описание	Команда	Ключи
Также для агрегированного интерфейса возможно настроить: - IPv4/IPv6-адресацию (см. в разделах Настройка IP-адресации, Настройка IPv6-адресации и Управление DHCP-клиентом); - Firewall (см. раздел Конфигурирование Firewall); - QoS в базовом или расширенном режимах (см. раздел Управление QoS); - мониторинг трафика (см. разделы Настройка Netflow); - функции протоколов маршрутизации (см. раздел Управление маршрутизацией); - протокол VRRF (см. раздел Управление резервированием)			

Пример настройки

Задача:

Настроить агрегированный канал между маршрутизатором EVT и коммутатором с помощью gigabitethernet-интерфейсов со значением MTU 9000 в режиме Trunk для передачи всех VLAN, созданных на маршрутизаторе.



Решение:

Предварительная конфигурация:

Предварительно на устройствах необходимо включить поддержку Jumbo-фреймов:

```
evt (config)# system jumbo-frames
```

Также на устройствах должны быть созданы необходимые VLAN для передачи в режиме Trunk.

Основной этап конфигурирования:

Создадим интерфейс port-channel 3:

```
evt(config)# interface port-channel 3
```

Переведём интерфейс в режим switchport:

```
evt(config-if-port-channel)# mode switchport
```

Зададим размер MTU = 9000:

```
evt(config-if-port-channel)# mtu 9000
```

Установим значение скорости физических интерфейсов, на которых будет работать агрегированный интерфейс:

```
evt(config-if-port-channel)# speed 1G
```

Настроим работу интерфейса в режиме trunk с передачей всех VLAN, созданных на маршрутизаторе:

```
evt(config-if-port-channel)# switchport mode trunk  
evt(config-if-port-channel)# switchport trunk allowed vlan auto-all
```

Перейдём к настройке физических интерфейсов. Переведём интерфейсы gigabitethernet1/0/1 и gigabitethernet1/0/2 в режим работы switchport:

```
evt(config)# interface gigabitethernet 1/0/1-2  
evt(config-if-te)# mode switchport
```

Включим интерфейсы в созданную группу агрегации каналов с ID 3 в режиме auto с поддержкой протокола LACP:

```
evt(config-if-te)# channel-group 3 mode auto
```

Дальнейшая конфигурация port-channel проводится как на обычном физическом интерфейсе.

7 Мониторинг

- [Настройка Netflow](#)
 - [Алгоритм настройки](#)
 - [Пример настройки](#)
- [Настройка SNMP](#)
 - [Алгоритм настройки](#)
 - [Пример настройки](#)
- [Настройка Syslog](#)
 - [Алгоритм настройки](#)
 - [Пример настройки](#)
- [Проверка целостности](#)
 - [Процесс настройки](#)
 - [Пример конфигурации](#)
- [Настройка архивации конфигурации маршрутизатора](#)
 - [Процесс настройки](#)
 - [Пример конфигурации](#)
- [Настройка SLA](#)
 - [Алгоритм настройки SLA-теста](#)
 - [Настройка SLA-responder](#)
 - [Пример настройки ICMP-режима тестирования](#)
 - [Пример настройки UDP-режима тестирования](#)
 - [Алгоритм настройки параметров аутентификации](#)
 - [Пример конфигурации UDP-теста с аутентификацией по ключ-строке](#)
 - [Пример конфигурации UDP-теста с аутентификацией по связке ключей](#)
 - [Настройка пороговых значений](#)
 - [Измерение характеристик канала связи](#)

7.1 Настройка Netflow

Netflow — сетевой протокол, предназначенный для учета и анализа трафика. Netflow позволяет передавать данные о трафике (адрес отправителя и получателя, порт, количество информации и др.) с сетевого оборудования (сенсора) на коллектор. В качестве коллектора может использоваться обычный сервер.

i В текущей реализации трафик, отброшенный маршрутизатором по каким-либо причинам, не будет учитываться в статистике.

7.1.1 Алгоритм настройки

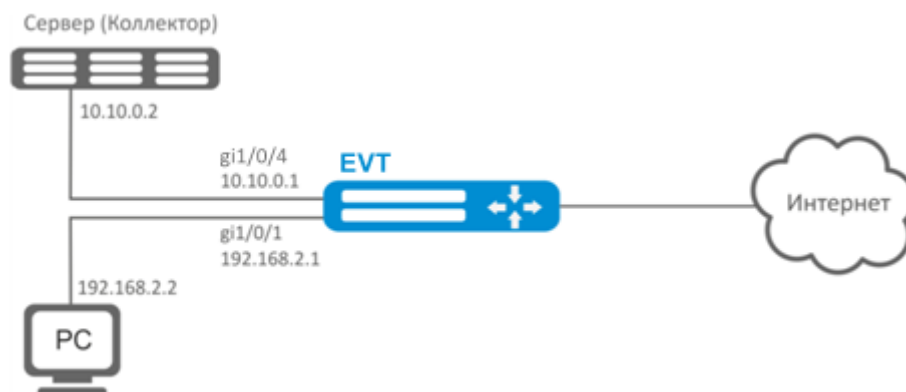
Шаг	Описание	Команда	Ключи
1	Задать версию Netflow-протокола.	evt(config)# netflow version <VERSION>	<VERSION> – версия Netflow-протокола: 5, 9 и 10.
2	Установить максимальное количество наблюдаемых сессий.	evt(config)# netflow max-flows <COUNT>	<COUNT> – количество наблюдаемых сессий, принимает значение [10000..2000000]. Значение по умолчанию: 512000.

Шаг	Описание	Команда	Ключи
3	Установить интервал, по истечении которого информация об активных сессиях экспортируются на коллектор.	evt(config)# netflow active-timeout <TIMEOUT>	<TIMEOUT> – интервал времени, по истечении которого информация об активных сессиях экспортируются на коллектор, задается в секундах, принимает значение [5..36000]. Значение по умолчанию: 1800 секунд.
4	Установить интервал, по истечении которого информация об устаревших сессиях экспортируются на коллектор.	evt(config)# netflow inactive-timeout <TIMEOUT>	<TIMEOUT> – задержка перед отправкой информации об устаревших сессиях, задается в секундах, принимает значение [0..240]. Значение по умолчанию: 15 секунд.
5	Установить частоту отправки статистики на Netflow-коллектор.	evt(config)# netflow refresh-rate <RATE>	<RATE> – частота отправки статистики, задается в пакетах на поток, принимает значение [1..10000]. Значение по умолчанию: 10.
6	Активировать Netflow на маршрутизаторе.	evt(config)# netflow enable	
7	Создать коллектор Netflow и перейти в режим его конфигурирования.	evt(config)# netflow collector <ADDR>	<ADDR> – IP-адрес коллектора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
8	Установить порт Netflow-сервиса на сервере сбора статистики.	evt(config-netflow-host)# port <PORT>	<PORT> – номер UDP-порта, указывается в диапазоне [1..65535]. Значение по умолчанию: 2055.
9	Включить отправку статистики на Netflow-сервер в режим конфигурирования интерфейса/ туннеля/сетевого моста.	evt(config-if-gi)# ip netflow export	

7.1.2 Пример настройки

Задача:

Организовать учет трафика с интерфейса gi1/0/1 для передачи на сервер через интерфейс gi1/0/4 для обработки.



Решение:

Предварительно необходимо настроить адресацию на интерфейсах.

Основной этап конфигурирования:

Укажем IP-адрес коллектора:

```
evt(config)# netflow collector 10.10.0.2
```

Включим сбор экспорта статистики Netflow на сетевом интерфейсе gi1/0/1:

```
evt(config)# interface gigabitethernet 1/0/1
evt(config-if-gi)# ip netflow export
```

Активируем Netflow на маршрутизаторе:

```
esr(config)# netflow enable
```

Для просмотра статистики Netflow используется команда:

```
evt# show netflow statistics
```

7.2 Настройка SNMP

SNMP (англ. *Simple Network Management Protocol* — простой протокол сетевого управления) — протокол, предназначенный для управления устройствами в IP-сетях на основе архитектур TCP/UDP. SNMP предоставляет данные для управления в виде переменных, описывающих конфигурацию управляемой системы.

7.2.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Включить SNMP-сервер.	evt(config)# snmp-server	
2	Определить community для доступа по протоколу SNMPv2c.	evt(config)# snmp-server community <COMMUNITY> [<TYPE>] [{ <IP-ADDR> <IPv6-ADDR> }] [client-list <OBJ-GROUP- NETWORK-NAME>] [<VERSION>] [view <VIEW- NAME>] [vrf <VRF>]	<COMMUNITY> – сообщество для доступа по протоколу SNMP; <TYPE> – уровень доступа: • ro – доступ только для чтения; • rw – доступ для чтения и записи. <IP-ADDR> – IP-адрес клиента, которому предоставлен доступ, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPv6-ADDR> – IPv6-адрес клиента, задаётся в виде X:X:X:X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, от которых обрабатываются snmp-запросы, задаётся строкой до 31 символа; <VERSION> – версия snmp, поддерживаемая данным community, принимает значения v1 или v2c; <VIEW-NAME> – имя профиля SNMP view, задаётся строкой до 31 символа; <VRF> – имя экземпляра VRF, из которого будет разрешен доступ, задается строкой до 31 символа.

Шаг	Описание	Команда	Ключи
3	Устанавливает значение переменной SNMP, содержащей контактную информацию.	evt(config)# snmp-server contact <CONTACT>	<CONTACT> – контактная информация, задается строкой до 255 символов.
4	Установить значение кода DSCP для использования в IP-заголовке исходящих пакетов SNMP-сервера (не обязательно).	evt(config)# snmp-server dscp <DSCP>	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 63.
5	Разрешить перезагрузку маршрутизатора при помощи snmp-сообщений (не обязательно).	evt(config)# snmp-server system-shutdown	
6	Создать SNMPv3-пользователь.	evt(config)# snmp-server user <NAME>	<NAME> – имя пользователя, задается строкой до 31 символа.
7	Устанавливает значение переменной SNMP, содержащей информацию о расположении оборудования.	evt(config)# snmp-server location <LOCATION>	<LOCATION> – информация о расположении оборудования, задается строкой до 255 символов.
8	Определить уровень доступа пользователя по протоколу SNMPv3.	evt(config-snmp-user)# access <TYPE>	<TYPE> – уровень доступа: • ro – доступ только для чтения; • rw – доступ для чтения и записи.
9	Определить режим безопасности пользователя по протоколу SNMPv3.	evt(config-snmp-user)# authentication access <TYPE>	<TYPE> – режим безопасности: • auth – используется только аутентификация; • priv – используется аутентификация и шифрование данных.

Шаг	Описание	Команда	Ключи
10	Определить алгоритм аутентификации SNMPv3-запросов.	evt(config-snmp-user)# authentication algorithm <ALGORITHM>	<ALGORITHM> – алгоритм шифрования: • md 5 – пароль шифруется по алгоритму md5; • sha 1 – пароль шифруется по алгоритму sha1.
11	Установить пароль для аутентификации SNMPv3-запросов.	evt(config-snmp-user)# authentication key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> }	<CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов; • encrypted – при указании команды задается зашифрованный пароль: <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).
12	Активировать фильтрацию и установить профиль IP-адресов, с которых могут приниматься SNMPv3-пакеты с данным именем SNMPv3-пользователя.	evt(config-snmp-user)# client-list <NAME>	<NAME> – имя ранее созданной object-group, задаётся строкой до 31 символа.
13	Указать vrf для SNMPv3-пользователя (не обязательно).	evt-21(config-snmp-user)# ip vrf forwarding <VRF>	<VRF> – имя экземпляра VRF, из которого будет разрешен доступ, задаётся строкой до 31 символа.
14	Активировать фильтрацию и установить IPv4/IPv6-адрес, которому предоставлен доступ к маршрутизатору под данным SNMPv3-пользователем.	evt(config-snmp-user)# ip address <ADDR>	<ADDR> – IP-адрес клиента, которому предоставлен доступ, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Шаг	Описание	Команда	Ключи
		evt(config-snmp-user)# ipv6 address <ADDR>	<IPv6-ADDR> – IPv6-адрес клиента, задаётся в виде X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
15	Активировать SNMPv3-пользователя.	evt(config-snmp-user)# enable	Значение по умолчанию: процесс выключен.
16	Определить алгоритм шифрования передаваемых данных.	evt(config-snmp-user)# privacy algorithm <ALGORITHM>	<ALGORITHM> – алгоритм шифрования: • aes 128 – использовать алгоритм шифрования AES-128; • des – использовать алгоритм шифрования DES.
17	Установить пароль для шифрования передаваемых данных.	evt(config-snmp-user)# privacy key ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> }	<CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).
18	Установить профиль snmp view, позволяющий разрешать или запрещать доступ к тем или иным OID для user.	evt(config-snmp-user)# view <VIEW-NAME>	<VIEW-NAME> – имя SNMP view профиля, на основании которого обеспечивается доступ к OID, задается строкой до 31 символа.

Шаг	Описание	Команда	Ключи
19	Включить передачу SNMP-уведомлений на указанный IP-адрес и перейти в режим настройки SNMP-уведомлений.	evt(config)# snmp-server host { <IP-ADDR> <IPv6-ADDR> } [vrf <VRF>]	<IP-ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. <IPv6-ADDR> – IPv6-адрес, задаётся в виде X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <VRF> – имя экземпляра VRF, в котором находится коллектор SNMP-уведомлений, задается строкой до 31 символа.
20	Определить порт коллектора SNMP-уведомлений на удаленном сервере (не обязательно).	evt(config-snmp-host)# port <PORT>	<PORT> – номер UDP-порта, указывается в диапазоне [1..65535]. Значение по умолчанию: 162.
21	Установить IP-адрес для отправки уведомлений на удаленный сервер.	evt(config-snmp-host)# source-address { <ADDR> <IPv6-ADDR> object-group <NETWORK_OBJ_GROUP_NAME> }	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPv6-ADDR> – IPv6-адрес, задаётся в виде X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве source address. Значение по умолчанию: IPv4/IPv6 – адрес интерфейса, ближайшего к удаленному SNMP-серверу.

Шаг	Описание	Команда	Ключи
22	Установить интерфейс или туннель маршрутизатора, IPv4/IPv6-адрес которого будет использоваться для отправки уведомлений на удаленный сервер.	evt(config-snmp-host)# source-interface { <IF> <TUN> }	<IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора; <TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора.
23	Разрешить отправку SNMP-уведомлений различных типов.	evt(config)# snmp-server enable traps <TYPE>	<TYPE> – тип фильтруемых сообщений. Может принимать значения: config, entry, entry-sensor, environment, envmon, files-operations, flash, flash-operations, interfaces, links, ports, screens, snmp, syslog. Дополнительные параметры зависят от типа фильтра. См. справочник команд CLI.
24	Создать профиль snmp view, позволяющий разрешать или запрещать доступ к тем или иным OID для community (SNMPv2) и user (SNMPv3).	evt(config)# snmp-server enable traps <TYPE>	<VIEW-NAME> – имя профиля SNMP view, задаётся строкой до 31 символа.

7.2.2 Пример настройки

Задача:

Настроить SNMPv3-сервер с аутентификацией и шифрованием данных для пользователя admin. IP-адрес маршрутизатора EVT – 192.168.52.8, IP-адрес сервера – 192.168.52.41.



Решение:

Предварительно нужно выполнить следующие действия:

- указать зону для интерфейса gi1/0/1;
- настроить IP-адрес для интерфейсов gi1/0/1.

Основной этап конфигурирования:

Включаем SNMP-сервер:

```
evt(config)# snmp-server
```

Создаем пользователя SNMPv3:

```
evt(config)# snmp-server user admin
```

Определим режим безопасности:

```
evt(snmp-user)# authentication access priv
```

Определим алгоритм аутентификации для SNMPv3-запросов:

```
evt(snmp-user)# authentication algorithm md5
```

Установим пароль для аутентификации SNMPv3-запросов:

```
evt(snmp-user)# authentication key ascii-text 123456789
```

Определим алгоритм шифрования передаваемых данных:

```
evt(snmp-user)# privacy algorithm aes128
```

Установим пароль для шифрования передаваемых данных:

```
evt(snmp-user)# privacy key ascii-text 123456789
```

Активируем SNMPv3-пользователя:

```
evt(snmp-user)# enable
```

Определяем сервер-приемник Trap-PDU-сообщений:

```
evt(config)# snmp-server host 192.168.52.41
```

7.3 Настройка Syslog

Syslog (англ. *System Log* — системный журнал) — стандарт отправки и регистрации сообщений о происходящих в системе событиях, используется в сетях, работающих по протоколу IP.

7.3.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Включить отправку syslog-сообщений на snmp-сервер в виде snmp-trap.	evt(config)# syslog snmp	
2	Активировать или деактивировать отправку на snmp-сервер событий работы отдельных процессов маршрутизатора (не обязательно).	evt(config-syslog-snmp)# match [not] process-name <PROCESS-NAME>	<PROCESS-NAME> – см. в справочнике команд CLI. Если описаны разрешающие критерии (match process-name) – логируются только сообщения указанных процессов. Если указаны запрещающие критерии (match not process-name) – логируются сообщения всех не запрещенных процессов. По умолчанию разрешено логирование сообщений всех процессов.
3	Указать уровень важности сообщений, которые будут отправляться на snmp-сервер.	evt(config-syslog-snmp)# severity <SEVERITY>	<SEVERITY> – уровень важности сообщения, принимает значения (в порядке убывания важности): • emerg – в системе произошла критическая ошибка, система неработоспособна; • alert – сигналы тревоги, необходимо немедленное вмешательство персонала; • crit – критическое состояние системы, сообщение о событии; • error – сообщения об ошибках; • warning – предупреждения, неаварийные сообщения; • notice – сообщения о важных системных событиях; • info – информационные сообщения системы; • debug – отладочные сообщения, предоставляют пользователю информацию для корректной настройки системы; • none – отключает вывод syslog-сообщений.

Шаг	Описание	Команда	Ключи
4	Включить отображение syslog-сообщений при удаленных подключениях (Telnet, SSH) (не обязательно).	evt(config)# syslog monitor	
5	Активировать или деактивировать отображение при удаленных подключениях событий работы отдельных процессов маршрутизатора (не обязательно).	evt(config-syslog-monitor)# match [not] process-name <PROCESS-NAME>	<PROCESS-NAME> – описано во 2 пункте.
6	Указать уровень важности сообщений, которые будут отображаться при удаленных подключениях.	evt(config-syslog-monitor)# severity <SEVERITY>	<SEVERITY> – описано в 3 пункте.
7	Включить отображение syslog-сообщений при консольном подключении (не обязательно).	evt(config)# syslog console	
8	Активировать или деактивировать отображение при консольном подключении событий работы отдельных процессов маршрутизатора (не обязательно).	evt(config-syslog-console)# match [not] process-name <PROCESS-NAME>	<PROCESS-NAME> – описано во 2 пункте.
9	Указать уровень важности сообщений, которые будут отображаться при консольном подключении.	evt(config-syslog-console)# severity <SEVERITY>	<SEVERITY> – описано в 3 пункте.
10	Указать категорию сообщений, которые будут сохраняться в локальный syslog-файл или отправляться на удаленный syslog-сервер.	evt(config)# syslog facility <FACILITY>	<FACILITY> – категория сообщений, принимает значения [local0..local7].
11	Включить сохранение сообщений syslog в указанный файл журнала (при необходимости ведения локального syslog-файла).	evt(config)# syslog file <NAME>	<NAME> – имя файла, в который будет производиться запись сообщений заданного уровня, задается строкой до 31 символа.
12	Активировать или деактивировать сохранение в локальный syslog-файл событий работы отдельных процессов маршрутизатора (не обязательно).	evt(config-syslog-file)# match [not] process-name <PROCESS-NAME>	<PROCESS-NAME> – описано во 2 пункте.

Шаг	Описание	Команда	Ключи
13	Указать уровень важности сообщений, которые будут сохраняться в локальный syslog-файл.	evt(config-syslog-file)# severity <SEVERITY>	<SEVERITY> – описано в 3 пункте.
14	Указать максимальный размер файла журнала (не обязательно).	evt(config)# syslog file-size <SIZE>	<SIZE> – размер файла, принимает значение [10..10000000] Кбайт.
15	Задать максимальное количество файлов, сохраняемых при ротации (не обязательно).	evt(config)# syslog max-files <NUM>	<NUM> – максимальное количество файлов, принимает значения [1.. 1000].
16	Включить передачу сообщений syslog на удаленный syslog-сервер (при необходимости отправки сообщений на удаленный syslog-сервер).	evt(config)#syslog host <HOSTNAME>	<HOSTNAME> – наименование syslog-сервера, задаётся строкой до 31 символа. Используется только для идентификации сервера при конфигурировании. Значение «all» используется в команде по syslog host для удаления всех syslog-серверов;
17	Указать IPv4/IPv6-адрес удаленного syslog-сервера.	evt(config-syslog-host)# remote-address { <ADDR> <IPV6-ADDR> }	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
18	Указать IPv4/IPv6-адрес маршрутизатора, от которого будут отправляться пакеты на удаленный syslog-сервер (не обязательно).	evt(config-syslog-host)# source-address { <ADDR> <IPV6-ADDR> object-group <NETWORK_OBJ_GROUP_NAME> }	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве source address; Значение по умолчанию: IPv4/IPv6-адрес интерфейса, с которого отправляются пакеты на удаленный syslog-сервер.

Шаг	Описание	Команда	Ключи
19	Указать транспортный протокол для передачи пакетов на удаленный syslog-сервер (не обязательно).	evt(config-syslog-host)# transport { tcp udp }	<VRF> – имя экземпляра VRF, в котором доступен удаленный syslog-сервер, задается строкой до 31 символа; Значение по умолчанию: отсутствует (глобальная таблица маршрутизации).
20	Указать имя экземпляра VRF, в рамках которого будут отправляться пакеты на удаленный syslog-сервер (не обязательно).	evt(config-syslog-host)# vrf <VRF>	
21	Указать номер TCP/UDP-порта, на который будут отправляться пакеты с syslog-сообщениями (не обязательно).	evt(config-syslog-host)# port <PORT>	<PORT> – номер TCP/UDP-порта, на который будут отправляться пакеты с syslog-сообщениями. Значение по умолчанию: 514.
22	Активировать или деактивировать отправку на удаленный syslog-сервер событий работы отдельных процессов маршрутизатора (не обязательно).	evt(config-syslog-host)# match [not] process-name <PROCESS-NAME>	<PROCESS-NAME> – описано во 2 пункте.
23	Указать уровень важности сообщений, которые будут сохраняться в локальный syslog-файл.	evt(config-syslog-host)# severity <SEVERITY>	<SEVERITY> – описано в 3 пункте.
24	Включить вывод отладочных сообщений во время загрузки устройства (не обязательно).	evt(config)#syslog reload debugging	
25	Включить процесс логирования введенных команд пользователя на локальный syslog-сервер (не обязательно).	evt(config)# syslog cli-commands	
26	Включить нумерацию сообщений (не обязательно).	evt(config)#syslog sequence-numbers	
27	Включить точность даты сообщений до миллисекунд (не обязательно).	evt(config)#syslog timestamp msec	
28	Включить отображение имени процесса, который сформировал сообщение (не обязательно).	evt(config)#syslog program-name	

Шаг	Описание	Команда	Ключи
29	Включить регистрацию неудачных аутентификаций (не обязательно).	evt(config)#logging login on-failure	
30	Включить регистрацию изменений настроек системы аудита (не обязательно).	evt(config)#logging syslog configuration	
31	Включить регистрацию изменений настроек пользователя (не обязательно).	evt(config)#logging userinfo	

7.3.2 Пример настройки

Задача:

Настроить отправку сообщений для следующих системных событий:

- неудачная аутентификация пользователя;
- внесены изменения в конфигурацию логирования системных событий;
- старт/остановка системного процесса;
- внесены изменения в профиль пользователей.

IP-адрес маршрутизатора EVT – 192.168.52.8, IP-адрес Syslog-сервера – 192.168.52.41. Использовать параметры по умолчанию для отправки сообщений – протокол UDP порт 514.



Решение:

Предварительно нужно выполнить следующие действия:

- указать зону для интерфейса gi1/0/1;
- настроить IP-адрес для интерфейсов gi1/0/1.

Основной этап конфигурирования:

Создаем файл на маршрутизаторе для системного журнала, уровень сообщений для журналирования – info:

```

evt(config)# syslog file tmpsys:syslog/evt
evt(config-syslog-file)# severity info
evt(config-syslog-file)# exit
  
```

Указываем IP-адрес и параметры удаленного syslog-сервера:

```
evt(config)# syslog host SERVER
evt(config-syslog-host)# remote-address 192.168.52.41
evt(config-syslog-host)# severity info
evt(config-syslog-host)# exit
```

Задаем логирование неудачных попыток аутентификации:

```
evt(config)# logging login on-failure
```

Задаем логирование изменений конфигурации syslog:

```
evt(config)# logging syslog configuration
```

Задаем логирование старта/остановки системных процессов:

```
evt(config)# logging service start-stop
```

Задаем логирование внесений изменений в профиль пользователей:

```
evt(config)# logging userinfo
```

Изменения конфигурации вступят в действие после применения:

```
evt# commit
Configuration has been successfully committed
evt# confirm
Configuration has been successfully confirmed
```

Посмотреть текущую конфигурацию системного журнала:

```
evt# show syslog configuration
```

Посмотреть записи системного журнала:

```
evt# show syslog evt
```

7.4 Проверка целостности

Проверка целостности подразумевает проверку целостности хранимых исполняемых файлов.

7.4.1 Процесс настройки

Шаг	Описание	Команда	Ключи
1	Запустить проверку целостности системы	evt# verify filesystem <detailed>	detailed – детальный вывод информации в консоль.

7.4.2 Пример конфигурации

Задача:

Проверить целостность файловой системы.

Решение:

Запускаем проверку целостности:

```
evt# verify filesystem
Filesystem Successfully Verified
```

7.5 Настройка архивации конфигурации маршрутизатора

На маршрутизаторах EVT/EVS предусмотрена функция локального и/или удаленного копирования конфигурации по таймеру или при применении конфигурации.

7.5.1 Процесс настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим настройки параметров резервирования конфигурации.	evt(config)# archive	
2	Установить тип сохранения резервных конфигураций маршрутизатора (не обязательно).	evt(config-ahchive)# type <TYPE>	<TYPE> – тип сохранения резервных конфигураций маршрутизатора. Принимает значения: • local; • remote; • both. Значение по умолчанию: remote.
3	Включить режим резервирования конфигурации по таймеру (не обязательно).	evt(config-ahchive)# auto	
4	Включить режим резервирования конфигурации после каждого успешного применения конфигурации (не обязательно).	evt(config-ahchive)# by-commit	

Шаг	Описание	Команда	Ключи
5	Указать путь для удаленного копирования конфигураций маршрутизатора (обязательно для типов remote и both).	evt(config-ahchive)# path <PATH>	<PATH> – определяет протокол, адрес сервера, расположение и префикс имени файла на сервере.
6	Задать период времени для автоматического резервирования конфигурации (не обязательно, актуально только для режима auto).	evt(config-ahchive)# time-period <TIME>	<TIME> – периодичность автоматического резервирования конфигурации, принимает значение в минутах [1..525600]. Значение по умолчанию: 720 минут.
7	Задать максимальное количество локально сохраняемых резервных копий конфигураций (не обязательно, актуально при типах local и both).	evt(config-ahchive)# count-backup <NUM>	<NUM> – максимальное количество локально сохраняемых резервных копий конфигураций. Принимает значения в диапазоне [1..100]. Значение по умолчанию: 1.

7.5.2 Пример конфигурации

Задача:

Настроить локальное и удаленное резервное копирование конфигурации маршрутизатора 1 раз в сутки и при успешном изменении конфигурации. Удаленные копии необходимо отправлять на tftp-сервер 172.16.252.77 в подпапку EVT-example. Максимальное количество локальных копий – 30.

Решение:

Для успешной работы удаленной архивации конфигураций, между маршрутизатором и сервером должна быть организована IP-связность, настроены разрешения на прохождение tftp-трафика по сети и сохранения файлов на сервере.

Основной этап конфигурирования:

Перейти в режим конфигурирования резервного копирования конфигураций:

```
evt# configure
evt(config)# archive
```

Задать режим локального и удаленного резервного копирования конфигурации:

```
evt(config-archive)# type both
```


Настроить путь для удаленного копирования конфигураций и максимальное количество локальных резервных копий:

```
evt(config-archive)# path tftp://172.16.252.77:/evt-example/evt-example.cfg
evt(config-archive)# count-backup 30
```

Задать интервал резервного копирования конфигурации в случае отсутствия изменений:

```
evt(config-archive)# time-period 1440
```

Включить режимы архивации конфигурации маршрутизатора по таймеру и при успешном изменении конфигурации:

```
evt(config-archive)# auto
evt(config-archive)# by-commit
```

После применения данной конфигурации 1 раз в сутки и при каждом успешном изменении конфигурации маршрутизатора на tftp-сервер будет отправляться конфигурационный файл с именем вида "evt-exampleYYYYMMDD_HHMMSS.cfg". Также на самом маршрутизаторе в разделе flash:backup/ будет создаваться файл с именем вида "config_YYYYMMDD_HHMMSS". Когда в разделе flash:backup/ накопится 30 таких файлов, при создании нового будет удаляться наиболее старый. Посмотреть можно командой:

```
evt(config)# show archive configuration
```

7.6 Настройка SLA

IP SLA (Internet Protocol Service Level Agreement) — технология измерения активных компьютерных сетей. На маршрутизаторах EVT/EVS, сервис IP SLA использует непрерывную генерацию трафика для тестирования качественных и количественных характеристик каналов связи в сети передачи данных на базе протокола IP. Два основных понятия при рассмотрении сервиса IP-SLA: SLA-agent (SLA-sender) – тестирующий маршрутизатор, отправляющий запросы; SLA-responder – удаленный/тестируемый маршрутизатор или произвольный хост, принимающий запросы от SLA-sender.

7.6.1 Алгоритм настройки SLA-теста

Шаг	Описание	Команда	Ключи
1	Создать в системе новый SLA-тест и перейти в режим его конфигурирования.	evt(config)# ip sla test <NUM>	<NUM> – номер SLA-теста, задается в диапазоне [1..10000].
2	Задать режим тестирования канала связи и параметры тестирования. Разные режимы подразумевают различный набор параметров, которые необходимо указать. Для одного SLA-теста возможно указать только один набор параметров тестирования.		

Шаг	Описание	Команда	Ключи
2.1	Конфигурирование ICMP-режима тестирования канала связи.	evt(config-sla-test)# icmp-echo { <DST-ADDRESS> <IPV6-DST-ADDRESS> } { source-ip { <SRC-ADDRESS> <IPV6-SRC-ADDRESS> object-group <NETWORK_OBJ_GROUP_NAME> } source-interface { <IF> <TUN> } } [interval <INTERVAL>] [num-packets <NUM-PACKETS>]	<DST-ADDRESS> – IPv4-адрес, на который будут направляться тестовые пакеты. Задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-DST-ADDRESS> – IPv6-адрес, на который будут направляться тестовые пакеты. Задаётся в виде X:X:X:X::X, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF]; <SRC-ADDRESS> – IPv4-адрес, с которого будут отправляться тестовые пакеты. Задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-SRC-ADDRESS> – IPv6-адрес, с которого будут отправляться тестовые пакеты. Задаётся в виде X:X:X:X::X, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF]; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве source address; <IF> – тип и идентификатор интерфейса, IP-адрес которого будет использоваться в качестве адреса источника пакетов. Задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора; <TUN> – тип и идентификатор туннеля, IP-адрес которого будет использоваться в качестве адреса источника пакетов. Задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора;

Шаг	Описание	Команда	Ключи
		evt(config-sla-test)# icmp-jitter <DST-ADDRESS> { source-ip { <SRC-ADDRESS> object-group <NETWORK_OBJ_GROUP_NAME> } source-interface { <IF> <TUN> } } [interval <INTERVAL>] [num-packets <NUM-PACKETS>]	<INTERVAL> – интервал между отправкой каждого последующего тестового пакета. Может принимать значение [1..255] миллисекунд; <NUM-PACKETS> – количество тестовых пакетов, отправляемых в рамках одной сессии тестирования. Может принимать значение [1..100000].

Шаг	Описание	Команда	Ключи
2.2	Конфигурирование UDP-режима тестирования канала связи. Для корректной работы UDP-режим предполагает сконфигурированный Eltex SLA-responder на удаленной стороне.	<pre> evt(config-sla-test)# udp-jitter { <DST-ADDRESS> <IPv6-DST-ADDRESS> } <DST-PORT> { source-ip { <SRC-ADDRESS> <IPv6-SRC-ADDRESS> object-group <NETWORK_OBJ_GROUP_NAME> } source-interface { <IF> <TUN> } } [source-port <SRC-PORT>] [interval <INTERVAL>] [num-packets <NUM-PACKETS>] </pre>	<DST-ADDRESS> – IPv4-адрес, на который будут направляться тестовые пакеты. Задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPv6-DST-ADDRESS> – IPv6-адрес, на который будут направляться тестовые пакеты. Задаётся в виде X:X:X:X::X, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF]; <DST-PORT> – номер UDP-порта назначения тестовых пакетов, принимает значения [1..65535]; <SRC-ADDRESS> – IPv4-адрес, с которого будут отправляться тестовые пакеты. Задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPv6-SRC-ADDRESS> – IPv6-адрес, с которого будут отправляться тестовые пакеты. Задаётся в виде X:X:X:X::X, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF]; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве source address; <IF> – тип и идентификатор интерфейса, с IP-адреса которого будут отправляться тестовые пакеты. Задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора; <TUN> – тип и идентификатор туннеля, с IP-адреса которого будут отправляться тестовые пакеты. Задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора;

Шаг	Описание	Команда	Ключи
			<SRC-PORT> – номер UDP-порта источника тестовых пакетов, принимает значения [1..65535]; <INTERVAL> – интервал между отправкой каждого последующего тестового пакета. Может принимать значение [1..255] миллисекунд; <NUM-PACKETS> – количество тестовых пакетов, отправляемых в рамках одной сессии тестирования. Может принимать значение [1..100000].

Шаг	Описание	Команда	Ключи
2.3	Конфигурирование TCP-режима тестирования канала связи.	evt(config-sla-test)# tcp-connect { <DST-ADDRESS> <IPV6-DST-ADDRESS> } { source-ip { <SRC-ADDRESS> <IPV6-SRC-ADDRESS> object-group <NETWORK_OBJ_GROUP_NAME> } source-interface { <IF> <TUN> } } [source-port <SRC-PORT>]	<DST-ADDRESS> – IPv4-адрес, на который будут направляться тестовые пакеты. Задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-DST-ADDRESS> – IPv6-адрес, на который будут направляться тестовые пакеты. Задаётся в виде X:X:X:X::X, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF]; <DST-PORT> – номер TCP-порта назначения тестовых пакетов, принимает значения [1..65535]; <SRC-ADDRESS> – IPv4-адрес, с которого будут отправляться тестовые пакеты. Задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-SRC-ADDRESS> – IPv6-адрес, с которого будут отправляться тестовые пакеты. Задаётся в виде X:X:X:X::X, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF]; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве source address; <IF> – тип и идентификатор интерфейса, с IP-адреса которого будут отправляться тестовые пакеты. Задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора; <TUN> – тип и идентификатор туннеля, с IP-адреса которого будут отправляться тестовые пакеты. Задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора;

Шаг	Описание	Команда	Ключи
			<SRC-PORT> – номер TCP-порта источника тестовых пакетов, принимает значения [1..65535].
3	Установить значение dscp, которым будут помечаться тестовые пакеты (необязательно).	evt(config-sla-test)# dscp <DSCP>	<DSCP> – значение кода DSCP, может принимать значение [0..63].
4	Установить частоту перезапуска SLA-теста (необязательно).	evt(config-sla-test)# frequency <TIME>	<TIME> – частота перезапуска SLA-теста, может принимать значение [1..604800] секунд.
5	Установить размер исходящего тестового пакета (необязательно).	evt(config-sla-test)# packet-size <SIZE>	<SIZE> – размер тестового пакета SLA-теста, может принимать значение [70..10000] байт.
6	Установить максимальное время ожидания ответа от удаленной стороны на тестовый пакет (необязательно).	evt(config-sla-test)# timeout <TIME>	<TIME> – время ожидания ответного пакета от удаленной стороны, может принимать значение [1..4294967295] миллисекунд.
7	Установить значение TTL для исходящих пакетов SLA-теста (необязательно).	evt(config-sla-test)# ttl <TTL>	<TTL> – значение TTL, может принимать значение [1..255].
8	Указать экземпляр VRF, в адресном пространстве которого должен работать SLA-тест (если подразумевается конфигурацией).	evt(config-sla-test)# vrf <VRF>	<VRF> – имя экземпляра VRF, задается строкой до 31 символа.

Шаг	Описание	Команда	Ключи
9	Установить пороговые значения характеристик канала (необязательно).	evt(config-sla-test)# thresholds <TYPE> { high <VALUE_H> low <VALUE_L> forward [{ high <VALUE_H> low <VALUE_L> }] reverse [{ high <VALUE_H> low <VALUE_L> }] } [from-last <NUM-CHECK> { all over <NUM-LIMIT> }]	<TYPE> – тип отслеживаемой величины, может принимать значения: • delay – допустимые значения задержек в канале; • jitter – допустимые значения джиттера в канале; • losses – допустимые значения потерь пакетов в канале. <VALUE_H> – верхнее пороговое значение, при пересечении которого сессия тестирования будет считаться проваленной; <VALUE_L> – нижнее пороговое значение, при пересечении которого сессия тестирования будет вновь считаться успешной; <NUM-CHECKS> – количество итераций теста, в течение которых проверяется соблюдение пороговых значений характеристик канала; <NUM-LIMIT> – количество итераций теста с превышением установленного порога, после превышения которого тест считается проваленным.
10	Запретить фрагментацию тестовых пакетов (необязательно).	evt(config-sla-test)# disallow-fragmentation	
11	Установить количество записей о результатах тестирования, отображающихся в истории измерений (необязательно).	evt(config-sla-test)# history <SIZE>	<SIZE> – число сохраняемых результатов, может принимать значение [1..1000].
12	Задать описание SLA-теста (необязательно).	evt(config-sla-test)# description <DESCRIPTION>	<DESCRIPTION> – описание SLA-теста, задается строкой до 255 символов.
13	Настроить параметры аутентификации, согласно алгоритму настройки параметров аутентификации (только для UDP-тестов, необязательно).		

Шаг	Описание	Команда	Ключи
14	Активировать SLA-тест.	evt(config-sla-test)# enable	
15	Выйти из параметров конфигурирования SLA-теста.	evt(config-sla-test)# exit	
16	Задать расписание запуска активированных SLA-тестов.	evt(config)# ip sla schedule { <TEST-NUMBER> all } [life { <LIFE-TIME> forever }] [start-time { <MONTH> <DAY> <TIME> now }]	<TEST-NUMBER> – номер SLA-теста, может принимать значение [1..10000]. При использовании ключа "all" вместо номера, устанавливается расписание работы для всех активированных SLA-тестов; <LIFE-TIME> – время жизни теста, может принимать значение [1..2147483647] секунд; forever – время жизни теста не ограничено; <TIME> – время начала теста, задаётся в виде HH:MM:SS, где: HH – часы, может принимать значение [0..23]; MM – минуты, может принимать значение [0..59]; SS – секунды, может принимать значение [0..59]; <MONTH> – месяц начала теста, принимает значения [January / February / March / April / May / June / July / August / September / October / November / December]; <DAY> – день месяца начала теста, может принимать значение [1..31]; now – начать тест немедленно.

Шаг	Описание	Команда	Ключи
17	Активировать вывод информационных сообщений групп событий (необязательно). Каждая из групп активируется отдельно.	evt(config)# ip sla logging <TYPE>	<TYPE> – название группы информационных сообщений, может принимать значения: • error – отображение сообщений об ошибках в работе SLA-тестов, причинах их провала, а также ошибок в работе SLA-responder (если таковой сконфигурирован в системе); • delay – отображение сообщений о превышении/нормализации значений, установленных в thresholds delay; • jitter – отображение сообщений о превышении/нормализации значений, установленных в thresholds jitter; • losses – отображение сообщений о превышении/нормализации значений, установленных в thresholds losses; • status – отображение сообщений о смене статуса SLA-теста.
18	Активировать сервис SLA-agent.	evt(config)# ip sla	

7.6.2 Настройка SLA-responder

Шаг	Описание	Команда	Ключи
1	В режиме конфигурирования интерфейса на маршрутизаторе, который является удаленной стороной SLA-теста, активировать SLA-responder.	evt(config-if-gi)# ip sla responder <TYPE> evt(config-if-gi)# ipv6 sla responder eltex	<TYPE> – название целевой платформы SLA-agent, может принимать значения: • eltex – функционал Eltex SLA-responder для Eltex SLA-agent; • cisco – функционал Cisco SLA-responder для Cisco SLA-agent.
2	Установить UDP-порт, на котором будет идти прослушивание запросов аутентификации от SLA-agent (если при конфигурировании SLA-теста был указан порт прохождения контрольной фазы, отличный от порта по умолчанию).		

Шаг	Описание	Команда	Ключи
2.1	Конфигурирование UDP-порта для прослушивания запросов аутентификации от Eltex SLA-agent (необязательно).	evt(config-if-gi)# ip sla responder eltex port <PORT>	<PORT> – номер UDP-порта, может принимать значение [1..65535].
		evt(config-if-gi)# ipv6 sla responder eltex port <PORT>	
2.2	Конфигурирование UDP-порта для прослушивания запросов аутентификации от Cisco SLA-agent (необязательно).	evt(config-if-gi)# ip sla responder cisco port <PORT>	<PORT> – номер UDP-порта, может принимать значение [1..65535].

7.6.3 Пример настройки ICMP-режима тестирования

Задача:

Настроить постоянную проверку доступности публичного DNS-сервера с IP-адресом 8.8.8.8. Интерфейс, имеющий доступ в сеть Интернет gi1/0/1, имеет адрес 192.168.44.15.

Решение:

Для выяснения сетевой доступности достаточной является проверка с помощью ICMP-запросов. Для этого настроим SLA-тест с типом icmp-echo и всеми параметрами по умолчанию:

```

evt# configure
evt(config)# ip sla test 1
evt(config-sla-test)# icmp-echo 8.8.8.8 source-ip 192.168.44.15
evt(config-sla-test)# enable
evt(config-sla-test)# exit
evt(config)# ip sla schedule 1 life forever start-time now

```

Также включим логирование событий смены статуса теста и сообщений о причинах неудачи (на случай, если адрес перестанет быть доступен).

```

evt(config)# ip sla logging status
evt(config)# ip sla logging error
evt(config)# ip sla
evt(config)# exit
evt# commit

```

После применения конфигурации тест стартует, и выводится сообщение о его текущем состоянии:

```

evt# 2023-12-13T14:01:55+00:00 %IP_SLA-I-STATUS: (test 1) State changed to success

```

Сводную информацию о результате и конфигурации теста можно вывести командой:

```

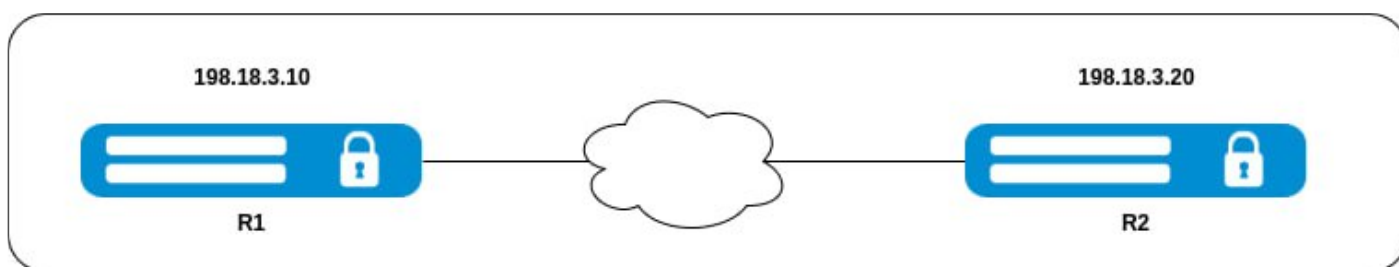
evt# show ip sla test status
Test      Type      Source      Destination      Status      Last Run
-----
1         icmp-echo  192.168.44.15  8.8.8.8          Successful  1 second(s) ago

```

7.6.4 Пример настройки UDP-режима тестирования

Задача:

Настроить тестирование качества канала связи между двумя устройствами. Устройства находятся в одной подсети 198.18.3.0/24.



Решение:

Измерение качества канала связи (задержки, потери, дубликаты при передаче трафика и др.) возможно с использованием UDP-тестирования. Сконфигурируем SLA-тест с типом `udp-jitter`, который будет измерять количественные характеристики канала связи, а также сигнализировать о превышении установленных порогов.

Сконфигурируем на R1 SLA-тест `udp-jitter` с адресом назначения R2 (198.18.3.20). Поскольку ограничений на выбор портов не обозначено, воспользуемся портами 20002 на отправку и на получение. Также укажем интервал между пакетами, равный 10 мс, чтобы ускорить общий поток тестового трафика.

```

R1# configure
R1(config)# ip sla test 2
R1(config-sla-test)# udp-jitter 198.18.3.20 20002 source-ip 198.18.3.10 source-port 20002
interval 10

```

Далее установим пороговые значения для информирования об ухудшении качества канала: максимальные значения двусторонней задержки – 15 мс, джиттера – 5мс и потерь – 5 пакетов (из 100 в настройках по умолчанию):

```

R1(config-sla-test)# thresholds delay high 15
R1(config-sla-test)# thresholds jitter forward high 5
R1(config-sla-test)# thresholds jitter reverse high 5
R1(config-sla-test)# thresholds losses high 5

```

Активируем тест и зададим расписание, согласно которому тест запустится немедленно и не будет иметь ограничений по следующим перезапускам:

```
R1(config-sla-test)# enable
R1(config)# ip sla schedule 2 start-time now life forever
```

Включим отображение всех групп сообщений, активируем сервис SLA-agent и применим конфигурацию:

```
R1(config)# ip sla logging status
R1(config)# ip sla logging error
R1(config)# ip sla logging delay
R1(config)# ip sla logging jitter
R1(config)# ip sla logging losses
R1(config)# ip sla
R1(config)# exit
R1# commit
```

Тест будет завершаться ошибкой до тех пор, пока не будет активирован Eltex SLA-responder на второй стороне – маршрутизаторе R2:

```
R1# 2023-12-13T14:01:55+00:00 %IP_SLA-I-STATUS: (test 2) State changed to fail
R1# 2023-12-13T14:01:55+00:00 %IP_SLA-E-ERROR: (test 2) Control phase failed: destination host
is not responding
```

Для этого перейдем в режим конфигурирования интерфейса, адрес которого ранее был указан как адрес назначения SLA-теста, и включим на нем Eltex SLA-responder:

```
R2(config)# interface gigabitethernet 1/0/1
R2(config-if-gi)# ip sla responder eltex
R2(config-if-gi)# exit
R2(config)# exit
R2# commit
```

- ✓ Порт назначения пакетов аутентификации по умолчанию – 1800 и должен быть открыт на R2. Если прохождение трафика по данному порту запрещено, необходимо изменить настройку портов, воспользовавшись [алгоритмом настройки параметров аутентификации](#), а также командами из раздела [Настройка SLA-Responder](#).

После активации SLA-responder тест перейдет в состояние 'Успешно'.

```
2023-12-13T15:35:32+00:00 %IP_SLA-I-STATUS: (test 2) State changed to success
```

При ухудшении характеристик канала и, вследствие, превышения обозначенных пороговых значений, на R1 будут выводиться сообщения вида:

```
2023-12-13T15:59:22+00:00 %IP_SLA-I-DELAY: (test 2) Two-way delay is high: 50.71ms > 15ms
2023-12-13T16:00:40+00:00 %IP_SLA-I-LOSSES: (test 2) Total losses are high: 43 > 5
2023-12-13T16:04:04+00:00 %IP_SLA-I-JITTER: (test 2) One-way jitter in forward direction is
high: 9.41ms > 5ms
2023-12-13T16:04:04+00:00 %IP_SLA-I-JITTER: (test 2) One-way jitter in reverse direction is
high: 9.41ms > 5ms
```

Сам SLA-тест при этом перейдет в состояние Fail и будет оставаться в нем до тех пор, пока характеристики канала не вернуться в допустимые пределы.

Просмотреть результаты измерений теста можно командой:

```
R1# show ip sla test statistics 2
Test number:                2
Test status:                Successful
Transmitted packets:        100
Lost packets:               39 (39.00%)
Lost packets in forward direction: 0 (0.00%)
Lost packets in reverse direction: 39 (39.00%)
One-way delay forward min/avg/max: 0.08/94.10/130.86 milliseconds
One-way delay reverse min/avg/max: 0.08/94.10/130.86 milliseconds
One-way jitter forward:     35.94 milliseconds
One-way jitter reverse:     35.94 milliseconds
Two-way delay min/avg/max:  0.15/188.19/261.73 milliseconds
Duplicate packets:          5
Out of sequence packets in forward direction: 0
Out of sequence packets in reverse direction: 40
```

7.6.5 Алгоритм настройки параметров аутентификации

Шаг	Описание	Команда	Ключи
1	В режиме конфигурирования SLA-теста, установить тип алгоритма, который будет использоваться при хешировании ключей аутентификации.	evt(config-sla-test)# control-phase authentication algorithm <ALGORITHM>	<ALGORITHM> – алгоритм хеширования, принимает значения [sha-256, hmac-sha-256].
2	Задать ключ, который будет использоваться в процессе прохождения контрольной фазы для аутентификации. Может быть использован один из двух видов ключей аутентификации: ключ-строка, указываемая непосредственно в режиме конфигурирования SLA-теста, и ключ, содержащийся в предварительно сконфигурированной связке ключей (key-chain).		
2.1	При использовании ключ-строки установить ее непосредственно в режиме конфигурирования SLA-теста.	evt(config-sla-test)# control-phase authentication key-string ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> }	<CLEAR-TEXT> – строка длиной от 8 до 16 символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).
2.2.1	При использовании ключа из связки ключей вернуться в общий режим конфигурирования, а затем создать новую связку ключей.	evt(config)# key-chain <KEYCHAIN>	<KEYCHAIN> – идентификатор связки ключей, задается строкой длиной до 16 символов.

Шаг	Описание	Команда	Ключи
2.2.2	В режиме конфигурирования связки ключей создать новый ключ.	evt(config-key-chain)# key <NUM>	<NUM> – номер-идентификатор ключа в связке ключей, может принимать значение [1..255].
2.2.3	Привязать к созданному ключу ключ-строку.	evt(config-key-chain-key)# key-string ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> }	<CLEAR-TEXT> – строка длиной от 8 до 16 символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).

Шаг	Описание	Команда	Ключи
2.2.4	Установить период времени, в течение которого данный ключ может использоваться для аутентификации исходящих пакетов (необязательно).	evt(config-keychain-key)# send-lifetime <TIME_B> <DAY_B> <MONTH_B> <YEAR_B> <TIME_E> <DAY_E> <MONTH_E> <YEAR_E>	<TIME_B> – устанавливаемое время начала действия ключа, задаётся в виде HH:MM:SS, где: HH – часы, принимает значение [0..23]; MM – минуты, принимает значение [0 .. 59]; SS – секунды, принимает значение [0 .. 59]. <DAY_B> – день месяца начала действия ключа, принимает значения [1..31]; <MONTH_B> – месяц начала использования ключа, принимает значения [January/February/March/April/May/June/July/August/September/October/November/December]; <YEAR_B> – год начала использования ключа, принимает значения [2001..2037]; <TIME_E> – устанавливаемое время окончания действия ключа, задаётся в виде HH:MM:SS, где: HH – часы, принимает значение [0..23]; MM – минуты, принимает значение [0 .. 59]; SS – секунды, принимает значение [0 .. 59]. <DAY_E> – день месяца окончания действия ключа, принимает значения [1..31]; <MONTH_E> – месяц окончания действия ключа, принимает значения [January/February/March/April/May/June/July/August/September/October/November/December]; <YEAR_E> – год окончания действия ключа, принимает значения [2001..2037].

Шаг	Описание	Команда	Ключи
2.2.5	Установить период времени, в течение которого данный ключ может использоваться для аутентификации входящих пакетов (необязательно).	evt(config-keychain-key)# accept-lifetime <TIME_B> <DAY_B> <MONTH_B> <YEAR_B> <TIME_E> <DAY_E> <MONTH_E> <YEAR_E>	<TIME_B> – устанавливаемое время начала действия ключа, задаётся в виде HH:MM:SS, где: HH – часы, принимает значение [0..23]; MM – минуты, принимает значение [0 .. 59]; SS – секунды, принимает значение [0 .. 59]. <DAY_B> – день месяца начала действия ключа, принимает значения [1..31]; <MONTH_B> – месяц начала использования ключа, принимает значения [January/February/March/April/May/June/July/August/September/October/November/December]; <YEAR_B> – год начала использования ключа, принимает значения [2001..2037]; <TIME_E> – устанавливаемое время окончания действия ключа, задаётся в виде HH:MM:SS, где: HH – часы, принимает значение [0..23]; MM – минуты, принимает значение [0 .. 59]; SS – секунды, принимает значение [0 .. 59]. <DAY_E> – день месяца окончания действия ключа, принимает значения [1..31]; <MONTH_E> – месяц окончания действия ключа, принимает значения [January/February/March/April/May/June/July/August/September/October/November/December]; <YEAR_E> – год окончания действия ключа, принимает значения [2001..2037].

Шаг	Описание	Команда	Ключи
2.2.6	Вернуться в общий режим конфигурирования и привязать ранее созданную связку ключей к сервису SLA.	evt(config)# ip sla key-chain <KEYCHAIN>	<KEYCHAIN> – идентификатор связки ключей, задается строкой длиной до 16 символов.
2.2.7	Перейти в режим конфигурирования ранее созданного SLA-теста и установить необходимый ключ из связки ключей, указав его номер.	evt(config-sla-test)# control-phase authentication key-id <NUM>	<NUM> – номер-идентификатор ключа в связке ключей, может принимать значение [1..255].
3	Указать порт, на который будут направляться пакеты для аутентификации в ходе контрольной фазы (необязательно).	evt(config-sla-test)# control-phase destination-port <PORT>	<PORT> – номер UDP-порта, может принимать значение [1..65535].
4	Указать порт, с которого будут отправляться пакеты для аутентификации в ходе контрольной фазы (необязательно).	evt(config-sla-test)# control-phase source-port <PORT>	<PORT> – номер UDP-порта, может принимать значение [1..65535].
5	Установить периодичность попыток повторного прохождения контрольной фазы в случае её неудачи.	evt(config-sla-test)# control-phase retry <TIME>	<TIME> – интервал между попытками, может принимать значение [1..86400] секунд.
6	Установить максимальное время ожидания ответного пакета аутентификации от удаленной стороны в ходе контрольной фазы.	evt(config-sla-test)# control-phase timeout <TIME>	<TIME> – время ожидания, может принимать значение [1..86400] секунд.
Далее необходимо симметрично настроить параметры аутентификации на удаленном маршрутизаторе (принимающая сторона).			
7	Перейти в режим конфигурирования сервиса SLA-responder.	evt(config)# ip sla responder [vrf <VRF>]	<VRF> – имя экземпляра VRF, задается строкой длиной до 31 символа. При указании данного параметра, SLA-responder включается в указанном VRF.
8	Установить максимальное время ожидания следующего тестового пакета (необязательно).	evt(config-sla-responder)# timeout <TIME>	<TIME> – время ожидания следующего пакета, может принимать значение [1..4294967295] миллисекунд.

Шаг	Описание	Команда	Ключи
9	Установить тип алгоритма, который будет использоваться при хешировании ключей аутентификации.	evt(config-sla-responder)# authentication algorithm <ALGORITHM>	<ALGORITHM> – алгоритм хеширования, принимает значения [sha-256, hmac-sha-256].
10	Задать ключ, который будет использоваться для аутентификации приходящих запросов от SLA-agent. Может быть использован один из двух видов ключей аутентификации: ключ-строка, указываемая непосредственно в режиме конфигурирования SLA-responder, и предварительно сконфигурированная связка ключей (key-chain).		
10.1	При использовании ключ-строки установить ее непосредственно в режиме конфигурирования SLA-responder.	evt(config-sla-responder)# authentication key-string ascii-text { <CLEAR-TEXT> encrypted <ENCRYPTED-TEXT> }	<CLEAR-TEXT> – строка длиной от 8 до 16 символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).
10.2.1	При использовании связки ключей необходимо вернуться в общий режим конфигурирования, а затем создать новую связку ключей. Процесс создания повторяет создание связки на тестирующем маршрутизаторе и описан в рамках шагов 2.2.1 - 2.2.5 данного алгоритма.		
10.2.2	Привязать ранее созданную связку ключей к SLA-responder.	evt(config-sla-responder)# authentication key-chain <KEYCHAIN>	<KEYCHAIN> – идентификатор связки ключей, задается строкой длиной до 16 символов.

7.6.6 Пример конфигурации UDP-теста с аутентификацией по ключ-строке

Задача:

Установить нестандартные порты отправки и получения запросов аутентификации, а для аутентификации использовать ключ-строку. Базовый UDP-тест уже настроен.

Решение:

Конфигурация активного UDP-теста:

```
R-sender# show running-config sla
ip sla
ip sla logging error
ip sla logging status
ip sla test 1
  udp-jitter 10.0.0.1 20001 source-ip 10.0.0.2 source-port 20002
  enable
exit
ip sla schedule 1 life forever start-time now
```

```
R-responder# show running-config sla
interface gigabitethernet 1/0/3
  ip sla responder eltex
exit
```

Изменим порты отправки и получения запросов аутентификации (пакетов контрольной фазы). Для аутентификации будем использовать порт отправки – 50000 и порт получения – 49500. Для этого укажем их в параметрах SLA-теста:

```
R-sender# configure
R-sender(config)# ip sla test 1
R-sender(config)# ip sla test 1
R-sender(config-sla-test)# control-phase destination-port 49500
R-sender(config-sla-test)# control-phase source-port 50000
```

Таким образом, при каждом новом запуске SLA-теста первая пара запрос-ответ будет происходить по адресам 10.0.0.2:50000 ↔ 10.0.0.1:49500, а последующий тестовый трафик – 10.0.0.2:20002 ↔ 10.0.0.1:20001.

Здесь же укажем алгоритм для хеширования ключа и сам ключ:

```
R-sender(config-sla-test)# control-phase authentication algorithm sha-256
R-sender(config-sla-test)# control-phase authentication key-string ascii-text sla_password
R-sender(config-sla-test)# end
R-sender# commit
```

Далее необходимо продублировать эти параметры на ответной стороне. Для этого перейдем в режим конфигурирования интерфейса, который выступает SLA-Responder, и укажем порт прослушивания запросов аутентификации:

```
R-responder# configure
R-responder(config)# interface gigabitethernet 1/0/3
R-responder(config-if-gi)# ip sla responder eltex port 49500
R-responder(config-if-gi)# exit
R-responder(config)#
```

После этого необходимо перейти в параметры SLA-Responder и указать там тот же алгоритм хеширования и ключ-пароль:

```
R-responder(config)# ip sla responder
R-responder(config-sla-responder)# authentication algorithm sha-256
R-responder(config-sla-responder)# authentication key-string ascii-text sla_password
R-responder(config-sla-responder)# end
R-responder# commit
```

Таким образом конфигурации R-sender и R-responder:

```
R-sender# show running-config sla
ip sla
ip sla logging error
ip sla logging status
ip sla test 1
  control-phase destination-port 49500
  control-phase source-port 50000
  control-phase authentication algorithm sha-256
  control-phase authentication key-string ascii-text encrypted 8CB5107EA7005AFF2D
  udp-jitter 10.0.0.1 20001 source-ip 10.0.0.2 source-port 20002
  enable
exit
ip sla schedule 1 life forever start-time now
```

```
R-responder# show running-config sla
interface gigabitethernet 1/0/3
  ip sla responder eltex port 49500
  ip sla responder eltex
exit

ip sla responder
  authentication algorithm sha-256
  authentication key-string ascii-text encrypted 8CB5107EA7005AFF2D
exit
```

7.6.7 Пример конфигурации UDP-теста с аутентификацией по связке ключей

Задача:

Изменить конфигурацию, приведенную в примере выше, используя при этом связки ключей.

Решение:

После указания портов аутентификации, создадим связку ключей и новый ключ:

```
R-sender(config)# key-chain SLA_CHAIN
R-sender(config-key-chain)# key 1
R-sender(config-key-chain-key)# key-string ascii-text sla_password
R-sender(config-key-chain-key)# exit
R-sender(config-key-chain)# exit
R-sender(config)#
```

Привяжем созданную связку к SLA-agent, а ключ из связки привяжем к SLA-тесту:

```
R-sender(config)# ip sla key-chain SLA_CHAIN
R-sender(config)# ip sla test 1
R-sender(config-sla-test)# control-phase authentication key-id 1
R-sender(config-sla-test)# end
R-sender# commit
```

Аналогичные действия произведем на R-responder. Создадим связку ключей с необходимым ключом и привяжем связку к SLA-Responder:

```
R-responder(config)# key-chain SLA
R-responder(config-key-chain)# key 1
R-responder(config-key-chain-key)# key-string ascii-text sla_password
R-responder(config-key-chain-key)# exit
R-responder(config-key-chain)# exit
R-responder(config)# ip sla responder
R-responder(config-sla-responder)# authentication key-chain SLA
R-responder(config-sla-responder)# end
R-responder# commit
```

Таким образом конфигурации R-sender и R-responder:

```
R-sender# show running-config
key-chain SLA_CHAIN
  key 1
    key-string ascii-text encrypted 8FB80252A00E5BE802FA0217
  exit
exit

ip sla key-chain SLA_CHAIN
ip sla
ip sla logging error
ip sla logging status
ip sla test 1
  control-phase destination-port 49500
  control-phase source-port 50000
  control-phase authentication algorithm sha-256
  control-phase authentication key-id 1
  udp-jitter 10.0.0.1 20001 source-ip 10.0.0.2 source-port 20002
  enable
exit
ip sla schedule 1 life forever start-time now
```

```
R-responder# show running-config
key-chain SLA
  key 1
    key-string ascii-text encrypted 8FB80252A00E5BE802FA0217
  exit
exit

interface gigabitethernet 1/0/3
  ***
  ip sla responder eltex port 49500
  ip sla responder eltex
exit

ip sla responder
  authentication algorithm sha-256
  authentication key-chain SLA
exit
```

Использование связок ключей позволяет комбинировать различные уникальные пароли для аутентификации между SLA-agent и SLA-Responder.

7.6.8 Настройка пороговых значений

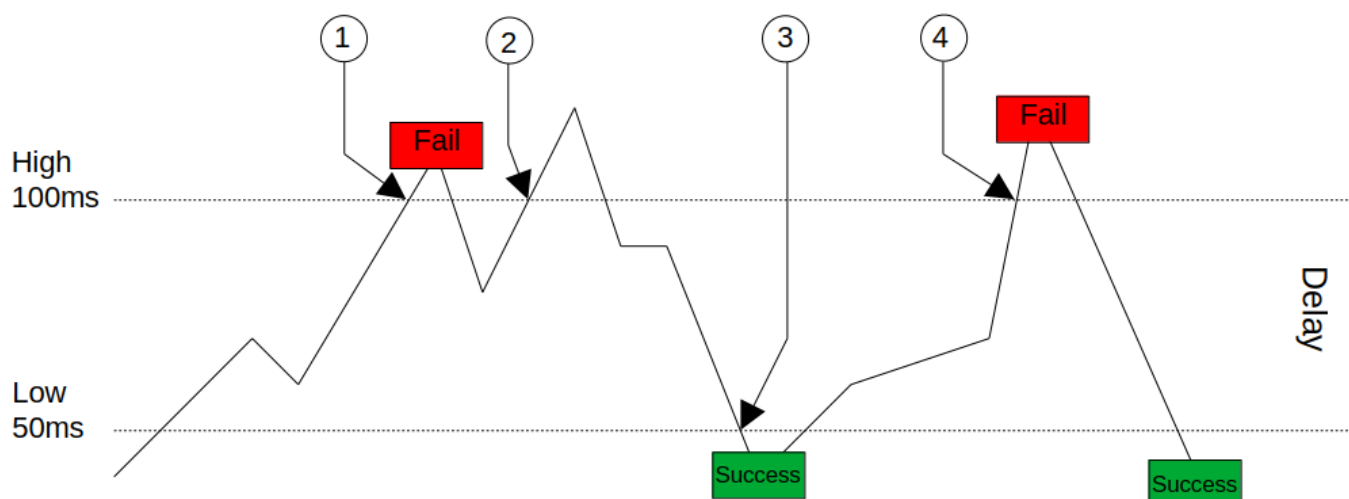
Для настройки реакции SLA-теста на определенные характеристики канала связи предусмотрен механизм активного реагирования на параметры thresholds.

Реагирование на качество канала связи может осуществляться по трём основным параметрам:

- Delay – измерение задержки между эталонным показателем интервала передачи очередного тестового пакета;
- Losses – измерение количества утерянных тестовых пакетов среди общего количества переданных пакетов;
- Jitter – измерение «дрожания» в канале, т. е. разброса во времени прохождения тестовых пакетов.

Для конфигурирования доступна настройка верхнего (high) и нижнего (low) пороговых значений для каждого из представленных параметров. Каждый из параметров может быть установлен как для одностороннего направления (forward/reverse), так и для двухстороннего (two-way).

Механизм активного изменения состояния SLA-теста при установленных пороговых значениях представлен на примере отслеживания показателя Delay с графиком значений величины во времени:



Событие	Описание
1	Первичное превышение верхнего порогового значения. Иницируется смена состояния SLA-теста на «Fail», отображается информационное сообщение о превышении установленного порога.
2	Повторное превышение верхнего порогового значения. Состояние SLA-теста неизменно (Fail), информационных сообщений не отображается. Для восстановления состояния теста ожидается снижение величины до значений меньших, чем установленный порог Low.
3	Понижение отслеживаемой величины до значений ниже установленного порога Low. Иницируется смена состояния SLA-теста на «Success», отображается информационное сообщение о нормализации показателя.
4	Очередная смена состояния SLA-теста, вызванная пересечением значения верхнего порога и предварительно нормализованным пересечением нижнего порога.

Пример конфигурации icmp-jitter SLA-теста с thresholds по показателю delay:

```

R-sender# show running-config sla
ip sla
ip sla logging delay
ip sla logging error
ip sla logging status
ip sla test 1
  icmp-jitter 198.18.0.100 source-ip 198.18.0.1 num-packets 150
  thresholds delay high 15
  thresholds delay low 8
  thresholds delay forward high 10
  thresholds delay forward low 5
  thresholds delay reverse high 10
  thresholds delay reverse low 5
  enable
exit
ip sla schedule all life forever start-time now

```

 Нижний порог (low) допускается не устанавливать. В таком случае он принимается равным верхнему, и нормализация характеристики будет засчитываться при снижении значений до показателей ниже установленного уровня.

7.6.9 Измерение характеристик канала связи

Механизм IP-SLA позволяет производить замеры как двухсторонних (two-way/round), так и односторонних (forward/reverse) характеристик канала связи.

После первичной настройки IP-SLA-тестов и запроса статистики замеров может возникнуть ситуация, в которой односторонние характеристики в прямом и обратном направлениях равны друг другу, а также являются половиной от двухсторонних характеристик. Причиной такого поведения чаще всего является несоответствие вычисленной односторонней характеристики критериям проверки механизма IP-SLA.

Для корректного измерения односторонних параметров существует несколько обязательных критериев:

- Оба узла (SLA-пробер и ответчик) **должны быть синхронизованы по NTP**;
- Суммарное отклонение от NTP на обоих узлах не должно превышать значение двухсторонней характеристики;
- Значение односторонней характеристики не должно быть меньше 0, а также превышать значение двухсторонней характеристики.

Только при соблюдении данных критериев можно ожидать корректное вычисление всех характеристик канала передачи данных.

```
R-sender# show ntp peers
Clock is synchronized, stratum 5, reference is 192.168.32.1
  remote      vrf      refid      st      t
when poll reach delay offset jitter -----
* 192.168.32.1 16 255 0.183 -2.314 0.711 172.16.5.63 4 s 10

R-sender# show ip sla test statistics 2
Test number: 2
Description: --
Test status: Successful
Transmitted packets: 100
Lost packets: 1 (1.00%)
Lost packets in forward direction: 1 (1.00%)
Lost packets in reverse direction: 0 (0.00%)
One-way delay forward min/avg/max: 23.19/24.61/30.57 milliseconds
One-way delay reverse min/avg/max: 46.26/47.25/55.28 milliseconds
One-way jitter forward: 2.77 milliseconds
One-way jitter reverse: 0.92 milliseconds
Two-way delay min/avg/max: 70.26/71.85/80.03 milliseconds
Two-way jitter min/avg/max: 2.01/3.02/3.92 milliseconds
Duplicate packets: 0
Out of sequence packets in forward direction: 0
Out of sequence packets in reverse direction: 0
Number of successes: 3 (100.00%)
Number of failures: 0 (0.00%)
```

8 Часто задаваемые вопросы

Не удалось получить маршруты по BGP и/или OSPF, сконфигурированных в VRF. Соседство успешно устанавливается, но в записи маршрутов в RIB отказано

%ROUTING-W-KERNEL: Can not install route. Reached the maximum number of BGP routes in the RIB

Необходимо выделить ресурс RIB для VRF, по умолчанию он равен нулю. Делает это в режиме конфигурирования VRF:

```
evt(config)# ip vrf <NAME>
evt(config-vrf)# ip protocols ospf max-routes 12000
evt(config-vrf)# ip protocols bgp max-routes 1200000
evt(config-vrf)# end
```

Закрываются сессии SSH/Telnet, проходящие через маршрутизатор EVT/EVS

Для поддержания сессии активной необходимо настроить передачу keepalive-пакетов. Опция отправки keepalive настраивается в клиенте SSH, например, для клиента PuTTY раздел «Соединение».

В свою очередь, на маршрутизаторе можно выставить время ожидания до закрытия неактивных сессий TCP (в примере выставлен 1 час):

```
evt(config)# ip firewall sessions tcp-established-timeout 3600
```

На интерфейсе был отключен firewall (ip firewall disable). После внесения этого интерфейса в security zone, удаления из конфигурации ip firewall disable и применения изменений – доступ для активных сессий с данного порта не закрылся согласно правилам security zone-pair

Изменения в конфигурации Firewall будут действовать только для новых сессий, сброса активных сессий в Firewall не происходит. Отчистить активные сессии в firewall можно командой:

```
evt# clear ip firewall session
```

Как полностью очистить конфигурация EVT/EVS и как сбросить на заводскую конфигурацию?

Очистка конфигурации происходит путем копирования пустой конфигурации в candidate-config и применения его в running-config.

```
evt# copy system:default-config system:candidate-config
```

Процесс сброса на заводскую конфигурацию аналогичен.

```
evt# copy system:factory-config system:candidate-config
```

В случае невозможности аутентификации на маршрутизаторе (неизвестен логин/пароль) конфигурацию можно сбросить к заводской следующим образом:

1. дождаться полной загрузки маршрутизатора
2. зажать функциональную кнопку «F» на 15 секунд
3. отпустить функциональную кнопку «F»
4. дождаться полной загрузки маршрутизатора с заводской конфигурацией

Как привязать subinterface к созданным VLAN?

При создании саб-интерфейса VLAN создается и привязывается автоматически (прямая зависимость индекс sub – VID).

```
evt(config)# interface gigabitethernet 1/0/1.100
```

После применения можно наблюдать информационные сообщения:

```
2016-07-14T012:46:24+00:00 %VLAN: creating VLAN 100
```

Есть ли функционал в маршрутизаторах серии EVT/EVS для анализа трафика?

В маршрутизаторах серии EVT/EVS реализована возможность анализировать трафик на интерфейсах из CLI. Сниффер запускается командой monitor.

```
evt# monitor gigabitethernet 1/0/1
```

Как настроить ip prefix-list 0.0.0.0/0?

Ниже приведен пример конфигурации префикс-листа, разрешающего прием маршрута по умолчанию.

```
evt(config)# ip prefix-list eltex
evt(config-pl)# permit 0.0.0.0/0
```

Проблема прохождения асинхронного трафика

В случае организации сети с асинхронной маршрутизацией, Firewall будет запрещать «неправильный (ошибочный)» входящий трафик (не открывающий новое соединение и не принадлежащий никакому установленному соединению) из соображений безопасности.

Разрешающее правило в Firewall не решит поставленную задачу для подобных схем.

Решить задачу можно, отключив Firewall на входном интерфейсе:

```
evt(config-if-gi)# ip firewall disable
```

Как можно сохранить локальную копию конфигурации маршрутизатора?

Если необходимо скопировать текущую running или candidate – конфигурацию на самом маршрутизаторе – можно воспользоваться командой copy с указанием в качестве источника копирования «system:running-config» или «system:candidate-config», а в качестве назначения – файл в разделе «flash:data/».

```
evt# copy system:candidate-config flash:data/temp.txt
```

Также существует возможность копирования ранее сохраненных конфигурационных файлов (автоматически из раздела flash:backup/ или вручную из раздела flash:data/) в candidate-конфигурацию:

```
evt# copy flash:data/temp.txt system:candidate-config
evt# copy flash:backup/config_20190918_164455 system:candidate-config
```

9 Приложение A. Packet Flow

- Порядок обработки входящего/исходящего трафика сетевыми службами маршрутизаторов EVT/EVS
- Порядок обработки транзитного трафика сетевыми службами маршрутизаторов EVT/EVS

9.1 Порядок обработки входящего/исходящего трафика сетевыми службами маршрутизаторов EVT/EVS

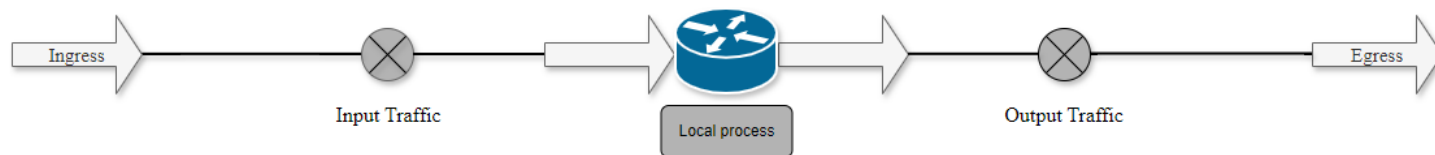


Таблица 1 – Порядок обработки входящего трафика

Шаг	Описание
1	Выполнение функций ACL на входящем трафике
2	Выполнение функций QoS (ограничение полосы пропускания, классификация и т. д.)
3	Отключение функций Firewall командой ip firewall disable. Разрешение трафика исключает проверки на этапах 4, 8
4	Выполнение правил между зонами any/self
5	Выполнение дефрагментации пакета
6	Функции Destination NAT ¹
7	Routing Decision (FIB)
8	Выполнение правил между пользовательскими зонами / self
9	Передача пакета в Netflow ¹
10	IPsec (decode) ¹ . После выполнения этого шага происходит переход к п.3

Таблица 2 – Порядок обработки исходящего трафика

Шаг	Описание
1	Local Policy Based Routing ¹
2	Route Decision
3	tcp adjust-mss ¹
4	Netflow (Egress) ¹

Шаг	Описание
5	Выполнение функций Source NAT ¹
6	IPsec (encode) ¹
7	Выполнение фрагментации пакетов
8	Выполнение функций QoS (ограничение полосы пропускания, классификация и т. д.)

 ¹ Данная функция выполняется только при наличии необходимых настроек.

9.2 Порядок обработки транзитного трафика сетевыми службами маршрутизаторов EVT/EVS



Таблица 3 – Порядок обработки транзитного трафика

Шаг	Описание
1	Выполнение функций ACL на входящем трафике
2	Выполнение функций QoS (ограничение полосы пропускания, классификация и т. д.)
3	Отключение функций Firewall командой ip firewall disable. Разрешение трафика исключает проверки на этапах 4, 10
4	Выполнение правил между пользовательскими зонами / any
5	Выполнение дефрагментации пакета
6	Функции Destination NAT ¹
7	Policy Based Routing
8	Routing Decision (FIB)
Если пакет перед передачей необходимо обработать протоколом более высокого уровня, выполняются следующие действия:	
9.1	Передача пакета в Netflow (Ingress) ¹
9.2	IPsec (decode) ¹ . После выполнения этого шага происходит переход к п.3
10	tcp adjust-mss ¹

Шаг	Описание
11	Выполнение правил между специальными зонами, any/any
12	Netflow (Egress) ¹
13	Выполнение функций Source NAT ¹
14	IPsec (encode) ¹
Если необходимо шифрование, то после этого процесса, выполняются следующие операции:	
15.1	tcp adjust-mss ¹
15.2	Netflow (Egress) ¹
15.3	Выполнение функций Source NAT ¹
16	Выполнение фрагментации пакетов
17	Выполнение функций QoS (ограничение полосы пропускания, классификация и т. д.)

 ¹ Данная функция выполняется только при наличии необходимых настроек.

10 Управление лицензированием

- ### 10.1
- Общие сведения
 - Типы лицензий и поддерживаемые устройства
 - Влияние лицензий на конфигурацию
 - Базовые лицензии (SCPC, MCPC-TERMINAL, MCPC-HUB)
 - Дополнительные лицензии (OQPSK)
 - Смена режима работы спутникового модема
 - Установка лицензий
 - Установка корректной даты
 - Установка лицензий через USB-накопитель
 - Установка лицензии через TFTP

10.2 Общие сведения

Для активации функциональных возможностей **SCPC**, **MCPC-HUB**, **MCPC-TERMINAL** и **OQPSK**, устройства EVT-101 и EVS-101 требуют наличия соответствующих лицензий.

Без установленной лицензии в выводе команды `show running-config/candidate-config` будет отображаться строка `# no licence inactive`:

```

evt-101# sh running-config
# no licence, inactive
interface satellite-modulator 1/1/1
  frame-length short
  frequency 980000.0
  output-level -20.00
  rolloff 0.15
  symrate 2000000
exit
# no licence, inactive
interface satellite-demodulator 1/1/1
  frame-length normal
  frequency 970000.0
  rolloff 0.15
  symrate 2000000
exit

```

После успешной загрузки лицензии эта строка исчезает, и соответствующий функционал становится доступным.

10.3 Типы лицензий и поддерживаемые устройства

Коммерческое название лицензии для заказа	Название лицензии (режима/опции)	Поддерживаемое устройство	Базовая/Дополнительная
EV-SC-101	SCPC	EVT-101	Базовая
EV-MC-101	MCPC-TERMINAL	EVT-101	Базовая
EV-HMC	MCPC-HUB	EVS-101	Базовая
EV-OQPSK	OQPSK	EVT-101	Дополнительная

⚠ Важно: Попытка установить неподдерживаемую лицензию (например, MCPC-HUB на EVT-101) приведёт к ошибке:

```
%LICENCE-W-EVENT: Received licence feature 'MCPC-HUB' not supported on device. Skipping
```

10.4 Влияние лицензий на конфигурацию

10.4.1 Базовые лицензии (SCPC, MCPC-TERMINAL, MCPC-HUB)

Если лицензия не установлена — в `sh run/can` отображается `# no licence inactive`.

После установки — строка исчезает, и функционал активируется.

10.4.2 Дополнительные лицензии (OQPSK)

Если на (де)модуляторе настроен `phase-mode oqpsk`, но лицензия не установлена — в `sh run/can` отображается `# no licence inactive`.

После установки лицензии:

- Конфигурация (де)модуляторов с `phase-mode oqpsk` обновляется;
- Строка `# no licence inactive` удаляется из вывода.

10.5 Смена режима работы спутникового модема

Перед установкой лицензии необходимо корректно выбрать режим работы спутникового модема.

⚠ Если на устройстве уже активированы несколько лицензий, например, SCPC и MCPC-TERMINAL, необходимо вручную выбрать соответствующий режим работы спутникового модема.

Для этого используется команда:

```
evt-101# set satellite-modem mode
Select satellite-modem mode:
mcpc-terminal
scpc
```

Система предложит выбрать один из доступных режимов:

- `mcpc-terminal` — режим терминала MCPC;
- `scpc` — режим SCPC.

Пример выбора режима MCPC-TERMINAL:

```
evt-101# set satellite-modem mode mcpc-terminal
```

Система выведет предупреждение:

```
Warning: factory configuration will be applied after system reboot
Do you still want to change satellite-modem mode? (y/N): y
```

Подтвердите действие, введя «у», если уверены в необходимости смены режима. После подтверждения необходимо перезагрузить устройство для применения изменений.

 После переключения режима модема и перезагрузки текущая конфигурация сбрасывается до заводских настроек.

10.6 Установка лицензий

10.6.1 Установка корректной даты

Перед загрузкой лицензии необходимо убедиться, что на устройстве установлена корректная дата и время.

1. Установка корректной даты и время:

```
evt-101# set date YYYY-MM-DD HH:MM:SS
```

2. Проверить текущую дату и время командой:

```
evt-101# show date
"2026-01-27 21:05:49"
```

10.6.2 Установка лицензий через USB-накопитель

1. Определить метку тома подключенного USB-накопителя.

```
evs-101# show storage-devices usb
```

Name	Filesystem	Total, MB	Used, MB	Free, MB
<USB_DISK>	vfat	29544.55	383.50	29161.05

 При выполнении команд копирования с USB-накопителей необходимо вместо полей <USB_DISK> использовать настоящие метки тома, определенные выше.

2. Скопировать файл на используемый USB-накопитель:

```
evs-101# copy usb://<USB_DISK>:<VS0000000120_MCPC-HUB.lic> system:licence
|*****| 100% (1993B) Licence loaded successfully.
```

3. Проверка установки лицензии:

```
evs-101# show licence
```

Feature	Expiries	Source	State	Value
Valid from	-----	-----	-----	-----
-----	-----	-----	-----	-----
MCPC-HUB		File (v2)	Active	true
--	--			

10.6.3 Установка лицензии через TFTP

1. Необходимо настроить сетевой интерфейс для доступа к TFTP-серверу:

```
interface gigabitethernet 1/0/4
ip firewall disable
ip address 192.168.32.21/24
exit
```

Убедитесь, что устройство имеет IP-соединение с TFTP-сервером (например, ping 192.168.32.85).

2. Используйте команду copy для загрузки файла лицензии с TFTP-сервера:

```
evs-101# copy tftp://192.168.32.85:/<VS00000000120_MCPC-HUB.lic> system:licence
|*****| 100% (1998B) Licence loaded successfully.
```

3. Проверка установки лицензии:

```
evs-101# sh licence
```

Feature	Expiries	Source	State	Value
Valid from	-----	-----	-----	-----
-----	-----	-----	-----	-----
MCPC-HUB		File (v2)	Active	true
--	--			

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения технической консультации по вопросам эксплуатации оборудования ООО «Предприятие «ЭЛТЕКС» вы можете обратиться в Сервисный центр компании:

Форма обратной связи на сайте: <https://eltex.ru/support/>

Servicedesk: <https://servicedesk.eltex-co.ru>

На официальном сайте компании вы можете найти техническую документацию и программное обеспечение для продукции ООО «Предприятие «ЭЛТЕКС», обратиться к базе знаний, оставить интерактивную заявку:

Официальный сайт компании: <https://eltex.ru>

База знаний: <https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base>

Центр загрузок: <https://eltex.ru/support/downloads>