Контроллер беспроводного доступа

WLC-30

Руководство по эксплуатации
Версия ПО 1.19.0

Содержание

1 Quickstart 3
2 Введение 5
3 Описание изделий 7
4 Установка и подключение 81
5 Интерфейсы управления 85
6 Начальная настройка устройств 91
7 Обновление программного обеспечения 99
8 Рекомендации по безопасной настройке 105
9 Управление контроллером WLC-30 113
10 Управление интерфейсами 142
11 Управление туннелированием 198
12 Управление QoS 262
13 Управление маршрутизацией 276
14 Управление технологией MPLS 362
15 Управление безопасностью 488
16 Управление резервированием 577
17 Управление удаленным доступом 601
18 Управление сервисами 631
19 Мониторинг 660
20 Управление BRAS (Broadband Remote Access Server) 688
21 Статьи 706
22 Управление VoIP 711
23 Часто задаваемые вопросы 728

1 Quickstart

Заводская конфигурация WLC-30 преднастроена таким образом, чтобы от пользователя потребовалось минимум настроек для получения первой работоспособной Wi-Fi сети. Если Вы впервые работаете с WLC-30 и хотите в кратчайшие сроки собрать работоспособный стенд, то Вам необходимо сделать несколько простых шагов.

1. Убедиться, что WLC-30 и подключаемая к нему точка доступа сброшены до заводских настроек. Если есть сомнения в том, что конфигурация устройств заводская, нужно сбросить их в дефолт, путем "зажатия" кнопки "F", расположенной на передней или задней панели, на 20 секунд. После этого произойдет перезагрузка устройства и оно загрузится с заводской конфигурацией.
2. Подключить точку доступа напрямую в порт gi1/0/2. Разумеется, если для питания точки доступа используется PoE инжектор, то подключить точку в порт gi1/0/2 нужно через PoE инжектор. Если для питания точки доступа используется PoE коммутатор, то точка включается в access-порт коммутатора, а коммутатор включается в порт gi1/0/2 WLC-30 другим access-портом.
3. Порт gi1/0/1 WLC-30 нужно включить в любой access-порт вышестоящей сети, где имеется доступ в интернет и выдается IP адрес с DHCP сервера. Интерфейс gi1/0/1 является аплинком в заводской конфигурации и получает адрес по DHCP. Интерфейс, получивший адрес по DHCP используется в WLC-30 для NAT.
4. После подключения к WLC-30 аплинка и точки доступа точка доступа автоматически получит с WLC-30 адрес по DHCP из сети 192.168.0.1/24, зарегистрируется на встроенном Wi-Fi контроллере, получит конфигурацию, включая SSID, построит GRE-тоннель до WLC-30 для передачи абонентского трафика и будет готова для подключения enterprise-клиентов.
5. Для успешной авторизации клиента необходимо создать для него учетную запись в БД локального RADIUS-сервера, встроенного в WLC-30. Создать ее можно следующими командами:

```
Логин для авторизации в WLC-30: "admin", пароль: "password".
После авторизации необходимо поменять пароль:
wlc-30(change-expired-password)# password newpassword
wlc-30(change-expired-password)# commit
wlc-30(change-expired-password)# confirm
wlc-30# configure
wlc-30(config)# radius-server local
wlc-30(config-radius)# domain default

#Создаем учетную запись пользователя Wi-Fi для подключения к Enterprise SSID:
wlc-30(config-radius-domain)# user name1
wlc-30(config-radius-user)# password ascii-text password1
wlc-30(config-radius-user)# end
wlc-30# commit
wlc-30# confirm
```

После этого можно подключиться к SSID "default_ssid" с логином "name1" и паролем "password1" и получить услугу Интернет.
Посмотреть статус точки досупа на контроллере можно командой:

```
wlc-30# show wlc ap
```

Полная конфигурация WLC-30 описана в разделе: Управление контроллером WLC-30. При этом нужно понимать, что вся приведенная в разделе Управление контроллером WLC-30 конфигурация уже содержится в заводской конфигурации WLC-30, кроме настроек учетной записи пользователя Wi-Fi, которые мы привели выше. Изучение полной конфигурации WLC-30 дает понимание, за что отвечают различные объекты в этой конфигурации и каким образом они между собой связаны.

2 Введение

- Аннотация
- Целевая аудитория
- Условные обозначения
- Примечания и предупреждения

⚠ Функционал WLC можно активировать на сервисном маршрутизаторе ESR-15.

2.1 Аннотация

WLC-30 — это программно-аппаратный комплекс для самостоятельного управления беспроводными сетями корпоративного уровня для малого и среднего бизнеса. Устройство позволяет оперативно конфигурировать сеть Wi-Fi и добавлять в нее точки доступа ЭЛТЕКС разной производительности и назначения.

В данном руководстве по эксплуатации изложены назначение, технические характеристики, порядок установки, рекомендации по начальной настройке и обновлению программного обеспечения контроллера беспроводного доступа WLC-30 (далее "контроллер" или "устройство").

2.2 Целевая аудитория

Данное руководство пользователя предназначено для технического персонала, выполняющего установку, настройку и мониторинг устройства посредством интерфейса командной строки (CLI), а также процедуры по обслуживанию системы и обновлению ПО. Квалификация технического персонала предполагает знание основ работы стеков протоколов TCP/IP, принципов построения Ethernet-сетей.

2.3 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 шрифтом выделены примечания, предупреждения или информация.
<Полужирный курсив>	Полужирным курсивом в угловых скобках указываются названия клавиш на клавиатуре.

Обозначение	Описание
`Текст в рамке`	В рамках с текстом указаны примеры и результаты выполнения команд.

2.4 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.

3 Описание изделий

- Назначение
- Функции
  - 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
- Основные технические характеристики
- Конструктивное исполнение
  - Конструктивное исполнение WLC-30
  - Конструктивное исполнение ESR-3200
  - Конструктивное исполнение ESR-3100
  - Конструктивное исполнение ESR-1700
  - Конструктивное исполнение ESR-1511, ESR-1500
  - Конструктивное исполнение ESR-1200, ESR-1000
  - Конструктивное исполнение ESR-200, ESR-100
  - Конструктивное исполнение ESR-21
  - Конструктивное исполнение ESR-30, ESR-20
  - Конструктивное исполнение ESR-15
  - Конструктивное исполнение ESR-14VF, ESR-12VF
  - Конструктивное исполнение ESR-12V
  - Конструктивное исполнение ESR-10
  - Световая индикация
- Комплект поставки

3.1 Назначение

Контроллер беспроводного доступа WLC-30 предназначен для управления беспроводными сетями. Устройство позволяет самостоятельно конфигурировать сеть Wi-Fi и добавлять в нее точки доступа ЭЛТЕКС разной производительности и назначения.

Enterprise-авторизация (WPA/WPA2 Enterprise, WPA/WPA2 Personal) пользователей с шифрованием трафика происходит по логину/паролю. В зависимости от задач и схемы сети данное решение позволяет подключать до 150 точек доступа.

Устройство обеспечивает мониторинг всех точек доступа, анализирует статистику трафика и время сессий, выполняет индивидуальные настройки Wi-Fi.

Устройства серии ESR являются высокопроизводительными многоцелевыми сетевыми маршрутизаторами. Устройство объединяет в себе традиционные сетевые функции и комплексный многоуровневый подход к безопасности маршрутизации, что позволяет обеспечить надежную защиту для корпоративной среды.

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

Устройство содержит в себе средства для программной и аппаратной обработки данных. За счет оптимального распределения функций обработки данных между частями достигается максимальная производительность.

3.2 Функции

3.2.1 Функции интерфейсов

В таблице 1 приведен список функций интерфейсов устройства.

Таблица 1 – Функции интерфейсов устройства

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.
Управление потоком (IEEE 802.3X)	Управление потоком позволяет соединять низкоскоростное устройство с высокоскоростным. Для предотвращения переполнения буфера низкоскоростное устройство имеет возможность отправлять пакет PAUSE, тем самым информируя высокоскоростное устройство о необходимости сделать паузу при передаче пакетов.
Агрегирование каналов (LAG, Link aggregation)	Агрегирование (объединение) каналов позволяет увеличить пропускную способность канала связи и повысить его надежность. Маршрутизатор поддерживает статическое и динамическое агрегирование каналов. При динамическом агрегировании используется протокол LACP для управления группой каналов.

3.2.2 Функции при работе с MAC-адресами

В таблице 2 приведены функции устройства при работе с MAC-адресами.

Таблица 2 – 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.

3.2.3 Функции второго уровня сетевой модели OSI

В таблице 3 приведены функции и особенности второго уровня (уровень 2 OSI).

Таблица 3 – Описание функций второго уровня (уровень 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).
Протокол связующего дерева (Spanning Tree Protocol)	Задачей протокола Spanning Tree является исключение избыточных сетевых соединений и приведение топологии сети к древовидной. Основные применения протокола связаны с предотвращением зацикливания сетевого трафика и с организацией резервных каналов связи.

3.2.4 Функции третьего уровня сетевой модели OSI

В таблице 4 приведены функции третьего уровня (уровень 3 OSI).

Таблица 4 – Описание функций третьего уровня (Layer 3)

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, RIPng, 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. Как правило, 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	Функционал DHCP Relay предназначен 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).

3.2.5 Функции туннелирования трафика

Таблица 5 – 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; • **IPv4-IPv4** – туннель, использующий инкапсуляцию исходных IP-пакетов в IP-пакеты с другими сетевыми параметрами; • **L2TPv3** – туннель для передачи L2-трафика с помощью IP-пакетов; • **IPsec** – туннель с шифрованием передаваемых данных; • **L2TP, PPTP, PPPoE, OpenVPN** – туннели, использующиеся для организации удаленного доступа клиент-сервер.

3.2.6 Функции управления и конфигурирования

Таблица 6 – 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.

3.2.7 Функции сетевой защиты

В таблице 7 приведены функции сетевой защиты, выполняемые устройством.

Таблица 7 − 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.

3.3 Основные технические характеристики

Основные технические параметры маршрутизатора приведены в таблице 8.

Таблица 8 – Основные технические характеристики

Общие параметры		
Интерфейсы	WLC-30	4 × Ethernet 10/100/1000BASE-T 2 × 10GBASE-R (SFP+)/1000BASE-X 1 × Консольный порт RJ-45 1 × USB 3.0 1 × USB 2.0 1 × Разъем для установки жесткого диска 1 × Слот для microSD-карты
	ESR-3200	12 × 1000BASE-X/10GBASE-R/25GBASE-R 1 × Console RS-232 (RJ-45) 1 × Порт OOB 1 × USB 2.0 1 × Слот для microSD-карты
	ESR-3100	8 × Combo Ethernet 10/100/1000BASE-T/1000BASE-X 8 × 10GBASE-R/1000BASE-X (SFP+/SFP) 1 × Console RS-232 (RJ-45) 2 × USB 3.0 1 × Слот для SD-карты
	ESR-1700	4 × Combo Ethernet 10/100/1000BASE-T/1000BASE-X 8 × 10GBASE-R/1000BASE-X (SFP+/SFP) 2 × Разъем для установки жесткого диска 1 × Console RS-232 (RJ-45) 1 × Порт OOB 2 × USB 2.0

ESR-1511	4 × Combo Ethernet 10/100/1000BASE-T/1000BASE-X 4 × Ethernet 10/100/1000BASE-T (RJ-45) 4 × 10GBASE-R/1000BASE-X (SFP+/SFP) 2 × 40GBASE-X (QSFP+) 1 × Console RS-232 (RJ-45) 1 × Порт OOB 2 × USB 2.0 1 × Слот для SD-карты
ESR-1500	4 × Combo Ethernet 10/100/1000BASE-T/1000BASE-X 4 × Ethernet 10/100/1000BASE-T (RJ-45) 4 × 10GBASE-R/1000BASE-X (SFP+/SFP) 1 × Console RS-232 (RJ-45) 1 × Порт OOB 2 × USB 2.0 1 × Слот для SD-карты
ESR-1200	4 × Combo Ethernet 10/100/1000BASE-T/1000BASE-X 12 × Ethernet 10/100/1000BASE-T (RJ-45) 8 × 10GBASE-R/1000BASE-X (SFP+/SFP) 1 × Console RS-232 (RJ-45) 2 × USB 2.0 1 × Слот для SD-карты
ESR-1000	24 × Ethernet 10/100/1000BASE-T (RJ-45) 2 × 10GBASE-R/1000BASE-X (SFP+/SFP) 1 × Console RS-232 (RJ-45) 2 × USB 2.0 1 × Слот для SD-карты

ESR-200	4 × Combo Ethernet 10/100/1000BASE-T/1000BASE-X 4 × Ethernet 10/100/1000BASE-T (RJ-45) 1 × Console RS-232 (RJ-45) 1 × USB 3.0 1 × USB 2.0 1 × Слот для SD-карты
ESR-100	4 × Combo Ethernet 10/100/1000BASE-T/1000BASE-X 1 × Console RS-232 (RJ-45) 1 × USB 3.0 1 × USB 2.0 1 × Слот для SD-карты
ESR-30	4 × Ethernet 10/100/1000BASE-T (RJ-45) 2 × 10GBASE-R/1000BASE-X (SFP+/SFP) 1 × Console RS-232 (RJ-45) 1 × USB 3.0 1 × USB 2.0 1 × Слот для microSD-карты
ESR-21	8 × Ethernet 10/100/1000BASE-T (RJ-45) 4 × 1000BASE-X (SFP) 3 × Последовательный порт RS-232 1 × Console RS-232 (RJ-45) 1 × USB 3.0 1 × USB 2.0 1 × Слот для SD-карты

ESR-20	2 × Combo Ethernet 10/100/1000BASE-T/1000BASE-X 2 × Ethernet 10/100/1000BASE-T (RJ-45) 1 × Console RS-232 (RJ-45) 1 × USB 3.0 1 × USB 2.0 1 × Слот для SD-карты
ESR-15	4 × Ethernet 10/100/1000BASE-T (RJ-45) 2 × 1000BASE-X (SFP) 1 × Console RS-232 (RJ-45) 2 × USB 2.0
ESR-14VF	8 × Ethernet 10/100/1000BASE-T (RJ-45) 1 × 1000BASE-X (SFP) 1 × Console RS-232 (RJ-45) 4 × FXS 2 × USB 2.0
ESR-12VF	8 × Ethernet 10/100/1000BASE-T (RJ-45) 1 × 1000BASE-X (SFP) 1 × Console RS-232 (RJ-45) 3 × FXS 1 × FXO 2 × USB 2.0
ESR-12V	8 × Ethernet 10/100/1000BASE-T (RJ-45) 1 × Console RS-232 (RJ-45) 3 × FXS 1 × FXO 2 × USB 2.0

	ESR-10	4 × Ethernet 10/100/1000BASE-T (RJ-45) 2 × 1000BASE-X (SFP) 1 × Console RS-232 (RJ-45) 2 × USB 2.0
Типы оптических трансиверов	WLC-30	1000BASE-X SFP 10GBASE-R SFP+
	ESR-3200	1000BASE-X SFP 10GBASE-R SFP+ 25GBASE-R SFP28
	ESR-1511	1000BASE-X SFP 10GBASE-R SFP+ 40GBASE-X QSFP+
	ESR-3100 ESR-1700 ESR-1500 ESR-1200 ESR-1000 ESR-30	1000BASE-X SFP 10GBASE-R SFP+
	ESR-200 ESR-100 ESR-21 ESR-20 ESR-15 ESR-14VF ESR-12VF ESR-10	1000BASE-X SFP
	ESR-15	1000BASE-R SFP+

Дуплексный и полудуплексный режимы интерфейсов		• дуплексный и полудуплексный режим для электрических портов • дуплексный режим для оптических портов
Максимальная пропускная способность маршрутизатора в L2-режиме (при аппаратной коммутации)	ESR-1700 ESR-1511 ESR-1500 ESR-1200	160 Гбит/с
	ESR-1000	88 Гбит/с
Скорость передачи данных	WLC-30	• электрические интерфейсы 10/100/1000 Мбит/с • оптические интерфейсы 1/10 Гбит/с
	ESR-3200	• оптические интерфейсы 1/10/25 Гбит/с
	ESR-1511	• электрические интерфейсы 10/100/1000 Мбит/с • оптические интерфейсы 1/10/40 Гбит/с
	ESR-3100 ESR-1700 ESR-1500 ESR-1200 ESR-1000 ESR-30	• электрические интерфейсы 10/100/1000 Мбит/с • оптические интерфейсы 1/10 Гбит/с
	ESR-200 ESR-100 ESR-21 ESR-20 ESR-15 ESR-14VF ESR-12V(F) ESR-10	• электрические интерфейсы 10/100/1000 Мбит/с • оптические интерфейсы 1 Гбит/с

Количество VPN-туннелей	ESR-3200 ESR-3100 ESR-1700 ESR-1511 ESR-1500 ESR-1200 ESR-1000	500
	WLC-30 ESR-200 ESR-100 ESR-30 ESR-21 ESR-20	250
	ESR-15 ESR-14VF ESR-12V(F) ESR-10	10

Количество статических маршрутов	WLC-30 ESR-3200 ESR-3100 ESR-1700 ESR-1511 ESR-1500 ESR-1200 ESR-1000 ESR-200 ESR-100 ESR-30 ESR-21 ESR-20	11k
	ESR-15 ESR-14VF ESR-12V(F) ESR-10	1k
Количество конкурентных сессий	ESR-3200 ESR-3100 ESR-1700 ESR-1511 ESR-1500 ESR-1200 ESR-1000	512k

	WLC-30 ESR-200 ESR-100 ESR-30 ESR-21 ESR-20	256k
	ESR-15 ESR-14VF ESR-12V(F) ESR-10	4k
Поддержка VLAN		до 4k активных VLAN в соответствии с 802.1Q
Количество маршрутов BGPv4/BGPv6	ESR-3200 ESR-3100 ESR-1700 ESR-1511 ESR-1500 ESR-1200 ESR-1000	5M
	WLC-30 ESR-200 ESR-100 ESR-30 ESR-21 ESR-20	2,5M

	ESR-15 ESR-14VF ESR-12V(F) ESR-10	1M
Количество маршрутов OSPFv2/OSPFv3/IS-IS	ESR-3200 ESR-3100 ESR-1700 ESR-1511 ESR-1500 ESR-1200 ESR-1000	500k
	WLC-30 ESR-200 ESR-100	300k
	ESR-30 ESR-21 ESR-20 ESR-15 ESR-14VF ESR-12V(F) ESR-10	30k

Количество маршрутов RIP/RIPng	WLC-30 ESR-3200 ESR-3100 ESR-1700 ESR-1511 ESR-1500 ESR-1200 ESR-1000 ESR-200 ESR-100 ESR-30 ESR-21 ESR-20	10k
	ESR-15 ESR-14VF ESR-12V(F) ESR-10	1k
Таблица MAC-адресов	ESR-1700 ESR-1511 ESR-1500 ESR-1200	128k записей
	ESR-3200 ESR-1000	16k записей

	WLC-30 ESR-3100 ESR-200 ESR-100 ESR-30 ESR-21 ESR-20 ESR-15 ESR-14VF ESR-12V(F) ESR-10	2k записей на бридж
Размер базы FIB	ESR-1700	3,0M
	ESR-3200 ESR-3100 ESR-1511 ESR-1500 ESR-1200 ESR-1000	1,7M
	WLC-30 ESR-200 ESR-100 ESR-30 ESR-21 ESR-20	1,4M
	ESR-15 ESR-14VF ESR-12V(F) ESR-10	800k

VRF		32
Количество L3-интерфейсов	WLC-30 ESR-3200 ESR-3100 ESR-1700 ESR-1500 ESR-1511 ESR-1200 ESR-1000 ESR-200 ESR-100 ESR-30 ESR-21 ESR-20	4000
	ESR-15 ESR-14VF ESR-12V(F) ESR-10	200

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 802.3ba 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
Физические характеристики и условия окружающей среды		
Источники питания	ESR-1700	Сеть переменного тока: 176–264 В, 50–60 Гц Сеть постоянного тока: 36–72 В Варианты питания: • один источник питания постоянного или переменного тока; • два источника питания постоянного или переменного тока, с возможностью горячей замены.

	ESR-3200 ESR-3100 ESR-1511 ESR-1500 ESR-1200 ESR-1000	Сеть переменного тока: 100–240 В, 50–60 Гц Сеть постоянного тока: 36–72 В Варианты питания: • один источник питания постоянного или переменного тока; • два источника питания постоянного или переменного тока, с возможностью горячей замены.
	WLC-30 ESR-200 ESR-100 ESR-30 ESR-21 ESR-20 ESR-14VF ESR-12V(F)	Сеть переменного тока: 100–264 В, 50–60 Гц
	ESR-15	Адаптер питания постоянного тока 220 В/12 В, 2 А
	ESR-10	Адаптер питания постоянного тока 220 В/12 В, 1,5 А
Максимальная потребляемая мощность	ESR-3200	118 Вт
	ESR-3100	123 Вт
	ESR-1700	250 Вт
	ESR-1511	128 Вт
	ESR-1500	125 Вт
	ESR-1200	85 Вт
	ESR-1000	75 Вт
	ESR-200	25 Вт
	ESR-100	20 Вт
	WLC-30 ESR-30	26 Вт
	ESR-21	32 Вт
	ESR-20	25 Вт
	ESR-15	18 Вт

	ESR-14VF ESR-12V(F)	22 Вт
	ESR-10	9 Вт
Масса	WLC-30	2,9 кг
	ESR-3200	5 кг
	ESR-3100	4,34 кг
	ESR-1700	12 кг
	ESR-1511 ESR-1500	7 кг
	ESR-1200	5,5 кг
	ESR-1000	3,6 кг
	ESR-200 ESR-100	2,5 кг
	ESR-30	1,8 кг
	ESR-21	3,15 кг
	ESR-20	2 кг
	ESR-15	0,325 кг
	ESR-14VF ESR-12V(F)	1 кг
	ESR-10	0,3 кг
Габаритные размеры (Ш × В × Г)	WLC-30	430 × 40 × 225 мм
	ESR-1700	440 × 88 × 490 мм
	ESR-3200 ESR-3100	430 × 44 × 330 мм
	ESR-1511 ESR-1500	430 × 44 × 425 мм
	ESR-1200 ESR-1000	430 × 44 × 352 мм

	ESR-200 ESR-100	310 × 44 × 240 мм
	ESR-21	430 × 44 × 225 мм
	ESR-30 ESR-20	267 × 44 × 212 мм
	ESR-15	230 × 32 × 133 мм
	ESR-14VF ESR-12V(F)	267 × 43,6 × 160,5 мм
	ESR-10	185 × 32 × 118 мм
Интервал рабочих температур	ESR-3200 ESR-3100 ESR-1700 ESR-1511 ESR-1500 ESR-1200 ESR-1000 ESR-200 ESR-100 ESR-30 ESR-21 ESR-20	от -10 до +45 °C
	ESR-15 ESR-14VF ESR-12V(F) ESR-10	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 15 лет

3.4 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.

3.4.1 Конструктивное исполнение WLC-30

Передняя панель устройства WLC-30

Внешний вид передней панели показан на рисунке 1.

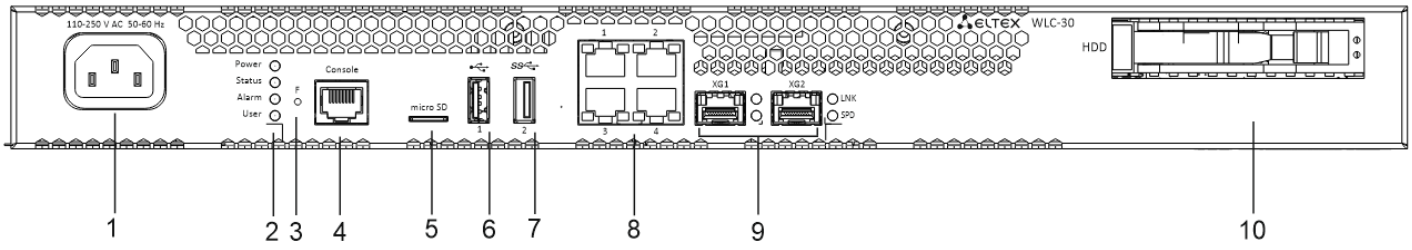


Рисунок 1 – Передняя панель WLC-30

Таблица 9 – Описание разъемов, индикаторов и органов управления передней панели WLC-30

№	Элемент передней панели	Описание
1	110-250 VAC	Источник питания.
2	Power	Индикатор питания устройства.
	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	User	Индикатор, использущийся для пользовательских сценариев, которые можно назначить в режиме конфигурирования устройства.

№	Элемент передней панели	Описание
3	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.
4	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
5	SD	Разъем для установки SD-карт памяти.
6	USB1	Разъем USB 2.0 для подключения внешних USB-устройств.
7	USB2	Разъем USB 3.0 для подключения внешних USB-устройств.
8	[1 .. 4]	4 порта Ethernet 10/100/1000BASE-T.
9	1, 2	2 порта 10GBASE-R (SFP+)1000BASE-X.
10	HDD	Разъем для установки жесткого диска памяти.

Задняя панель устройства WLC-30

Внешний вид задней панели устройства WLC-30 приведен на рисунке ниже.

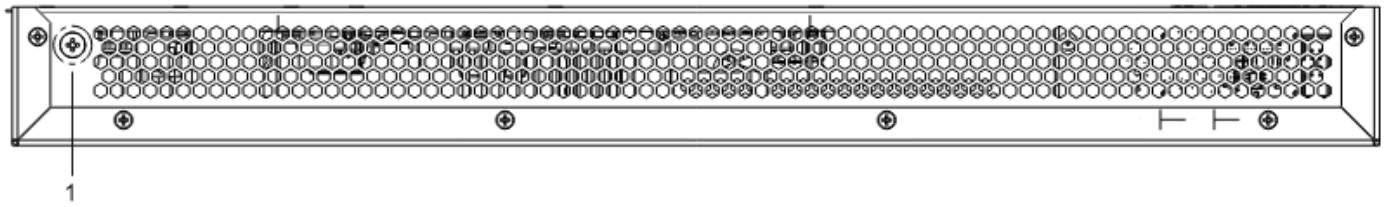


Рисунок 2 – Задняя панель WLC-30

Таблица 10 – Описание разъемов задней панели контроллера WLC-30

№	Описание
1	Клемма для заземления устройства.

Боковые панели устройства WLC-30

Внешний вид боковых панелей устройства WLC-30 приведен на рисунках ниже.

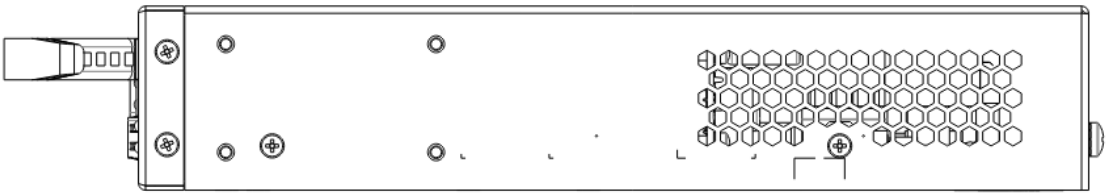


Рисунок 3 – Правая боковая панель WLC-30

Рисунок 4 – Левая боковая панель WLC-30

3.4.2 Конструктивное исполнение ESR-3200

Передняя панель устройства ESR-3200

Внешний вид передней панели показан на рисунке 5.

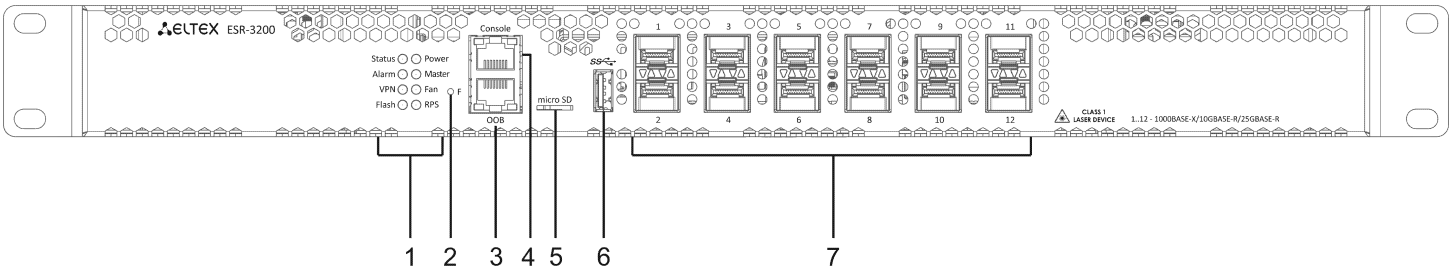


Рисунок 5 – Передняя панель ESR-3200

Таблица 11 – Описание разъемов, индикаторов и органов управления передней панели ESR-3200

№	Элемент передней панели	Описание
1	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	VPN	Индикатор режима работы в режиме VPN-шлюза (не используется в текущей версии).

№	Элемент передней панели	Описание
	Flash	Индикатор активности обмена с накопителем данных – microSD-картой или USB Flash.
	Power	Индикатор питания устройства.
	Master	Индикатор работы устройства в failover-режимах (не используется в текущей версии).
	Fan	Индикатор аварии вентиляторов.
	RPS	Индикатор резервного источника электропитания.
2	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.
3	OOB	Ethernet-порт используется только для обновления программного обеспечения через загрузчик U-Boot. Данный порт не используется для удаленного доступа и управления.
4	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
5	microSD	Разъем для установки microSD-карт памяти.
6	USB1	Порт USB 2.0 для подключения USB-устройств.
7	[1 .. 12]	Слоты для установки трансиверов 25G SFP28/10G SFP+/1G SFP.

Задняя панель устройства ESR-3200

Внешний вид задней панели устройств ESR-3200 приведен на рисунке ниже.

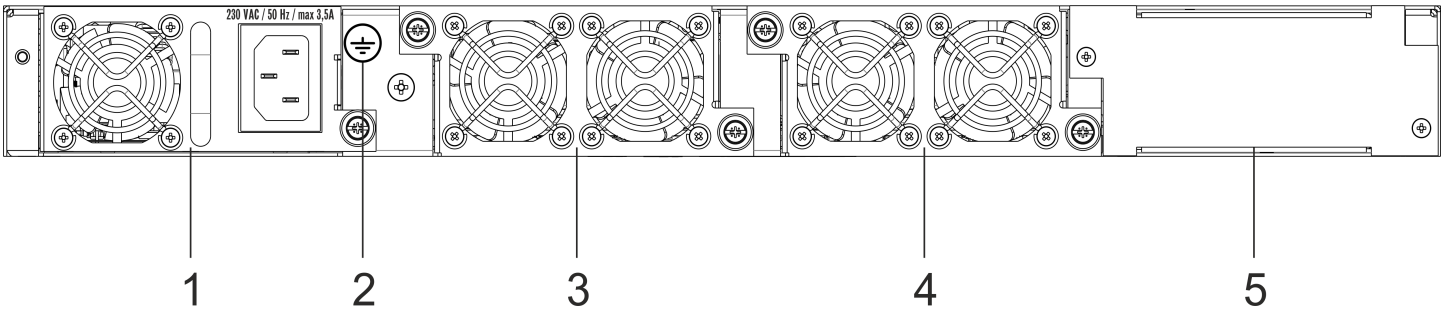


Рисунок 6 – Задняя панель ESR-3200

Таблица 12 – Описание разъемов задней панели маршрутизатора

№	Описание
1	Основной источник питания.
2	Клемма для заземления устройства.
3	Съемные вентиляционные модули с возможностью горячей замены.
4	
5	Место для установки резервного источника питания.

Боковые панели устройства ESR-3200

Внешний вид задней панели устройств ESR-3200 приведен на рисунках ниже.

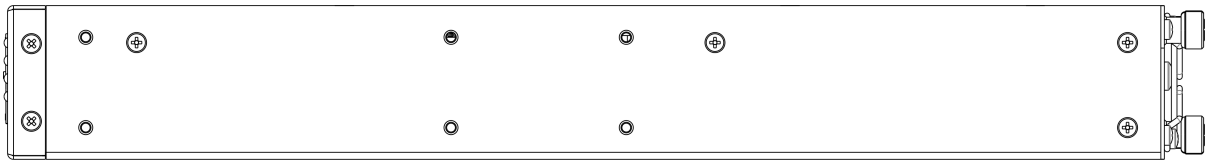


Рисунок 7 – Правая боковая панель ESR-3200

Рисунок 8 – Левая боковая панель ESR-3200

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 разделе Установка и подключение.

3.4.3 Конструктивное исполнение ESR-3100

Передняя панель устройства ESR-3100

Внешний вид передней панели показан на рисунке 9.

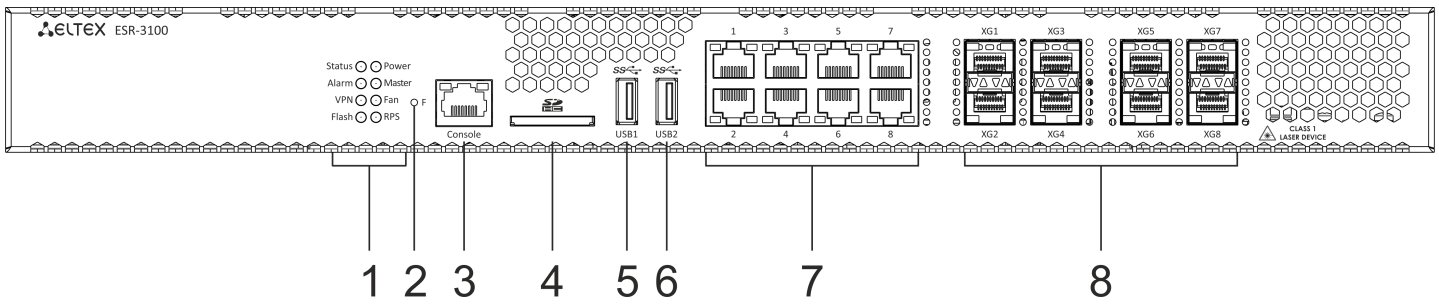


Рисунок 9 – Передняя панель ESR-3100

В таблице 13 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели устройства ESR-3100.

Таблица 13 – Описание разъемов, индикаторов и органов управления передней панели ESR-3100

№	Элемент передней панели	Описание
1	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	VPN	Индикатор режима работы в режиме VPN-шлюза.
	Flash	Индикатор активности обмена с накопителем данных – SD-картой или USB Flash.
	Power	Индикатор питания устройства.
	Master	Индикатор работы устройства в failover-режимах (не используется в текущей версии).
	Fan	Индикатор аварии вентиляторов.
	RPS	Индикатор резервного источника электропитания.
2	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.
3	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
4	SD	Разъем для установки SD-карт памяти.
5	USB1	Порт USB 3.0 для подключения USB-устройств.
6	USB2	Порт USB 3.0 для подключения USB-устройств.
7	[1 .. 8]	8 портов Gigabit Ethernet 10/100/1000BASE-T (RJ-45).
8	XG1 – XG8	Слоты для установки трансиверов 10G SFP+/1G SFP.

Задняя панель устройства ESR-3100

Внешний вид задней панели устройств ESR-3100 приведен на рисунке ниже.

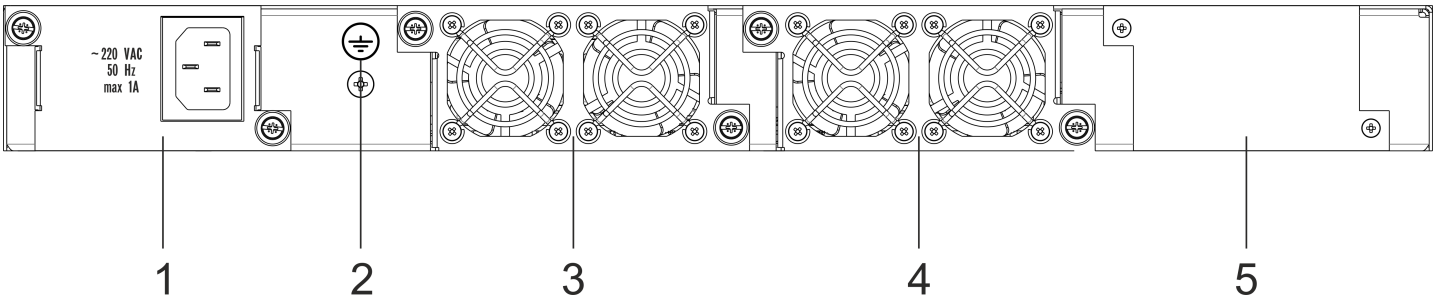


Рисунок 10 – Задняя панель ESR-3100

В таблице 14 приведен перечень разъемов, расположенных на задней панели маршрутизатора.

Таблица 14 – Описание разъемов задней панели ESR-3100

№	Описание
1	Основной источник питания.
2	Клемма для заземления устройства.
3	Съемные вентиляционные модули с возможностью горячей замены.
4	
5	Место для установки резервного источника питания.

Боковые панели устройства ESR-3100

Внешний вид боковых панелей устройства ESR-3100 приведен на рисунках 11 и 12.

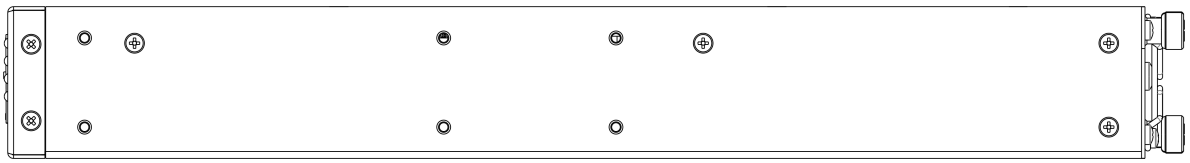


Рисунок 11 – Правая боковая панель ESR-3100

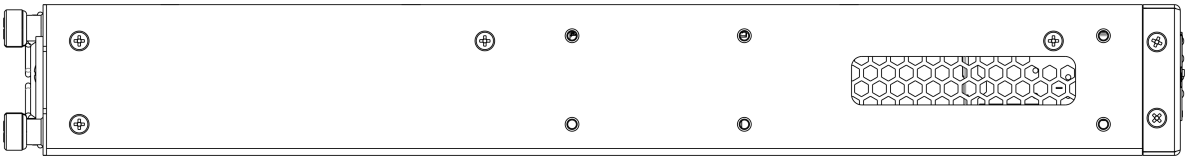


Рисунок 12 – Левая боковая панель ESR-3100

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 разделе Установка и подключение.

3.4.4 Конструктивное исполнение ESR-1700

Передняя панель устройства ESR-1700

Внешний вид передней панели показан на рисунке 13.

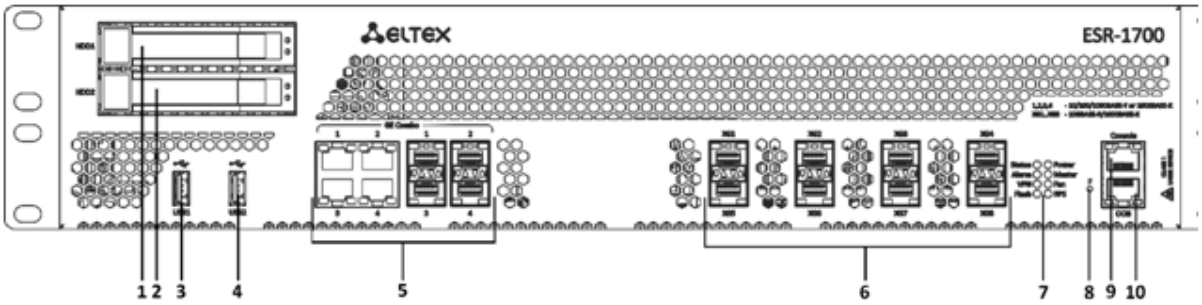


Рисунок 13 – Передняя панель ESR-1700

В таблице 15 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели устройства ESR-1700.

Таблица 15 – Описание разъемов, индикаторов и органов управления передней панели ESR-1700

№	Элемент передней панели	Описание
1	HDD1	Разъем для установки жесткого диска памяти.
2	HDD2	Разъем для установки жесткого диска памяти.
3	USB1	Порт для подключения USB-устройств.
4	USB2	Порт для подключения USB-устройств.
5	Combo Ports [1 .. 4]	4 порта Gigabit Ethernet 10/100/1000BASE-X (SFP).
6	XG1 – XG8	Слоты для установки трансиверов 10G SFP+/1G SFP.
7	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	VPN	Индикатор режима работы в режиме VPN-шлюза (не используется в текущей версии).
	Flash	Индикатор активности обмена с накопителем данных – SD-картой или USB Flash.
	Power	Индикатор питания устройства.

№	Элемент передней панели	Описание
	Master	Индикатор работы устройства в failover-режимах (не используется в текущей версии).
	Fan	Индикатор аварии вентиляторов.
	RPS	Индикатор резервного источника электропитания.
8	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.
9	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
10	OOB	Ethernet-порт используется только для обновления программного обеспечения через загрузчик U-Boot. Данный порт не используется для удаленного доступа и управления.

Задняя панель устройства ESR-1700

Внешний вид задней панели устройства ESR-1700 приведен на рисунке ниже.

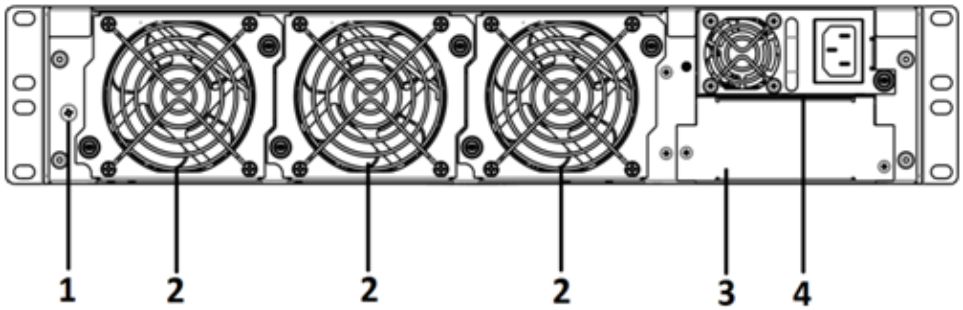


Рисунок 14 – Задняя панель ESR-1700

В таблице 16 приведен перечень разъемов, расположенных на задней панели маршрутизатора.

Таблица 16 – Описание разъемов задней панели ESR-1700

№	Описание
1	Клемма для заземления устройства.
2	Съемные вентиляционные модули с возможностью горячей замены.
3	Основной источник питания.
4	Место для установки резервного источника питания.

Боковые панели устройства ESR-1700

Внешний вид боковых панелей устройства ESR-1700 приведен на рисунках 15 и 16.

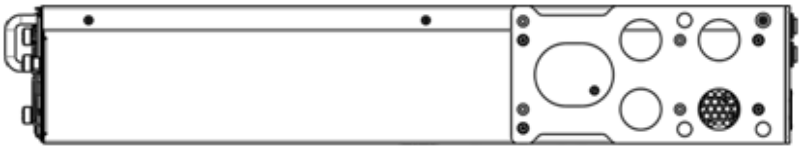


Рисунок 15 – Правая боковая панель ESR-1700

Рисунок 16 – Левая боковая панель ESR-1700

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 разделе Установка и подключение.

3.4.5 Конструктивное исполнение ESR-1511, ESR-1500

Передняя панель устройства ESR-1511

Внешний вид передней панели устройства показан на рисунке 17.

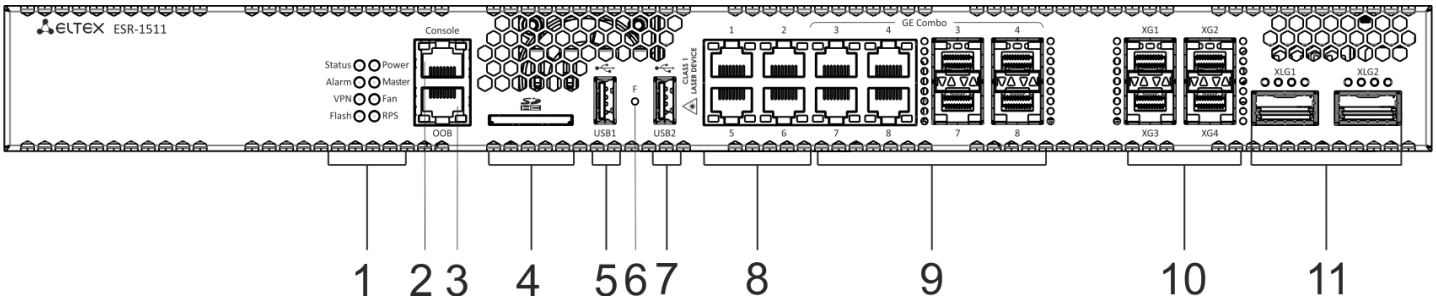


Рисунок 17 – Передняя панель ESR-1511

В таблице 17 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели устройства ESR-1511.

Таблица 17 – Описание разъемов, индикаторов и органов управления передней панели ESR-1511

№	Элемент передней панели	Описание
1	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	VPN	Индикатор режима работы в режиме VPN-шлюза (не используется в текущей версии).

№	Элемент передней панели	Описание
	Flash	Индикатор активности обмена с накопителем данных – SD-картой или USB Flash.
	Power	Индикатор питания устройства.
	Master	Индикатор работы устройства в failover-режимах (не используется в текущей версии).
	Fan	Индикатор аварии вентиляторов.
	RPS	Индикатор резервного источника электропитания.
2	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
3	OOB	Ethernet-порт используется только для обновления программного обеспечения через загрузчик U-Boot. Данный порт не используется для удаленного доступа и управления.
4	SD	Разъем для установки SD-карт памяти.
5	USB1	Порт для подключения USB-устройств.
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.
7	USB2	Порт для подключения USB-устройств.
8	Ethernet	4 порта Ethernet 10/100/1000BASE-T.
9	Combo Ports [1 .. 4]	4 порта Gigabit Ethernet 10/100/1000BASE-X (SFP).
10	XG1 – XG4	Слоты для установки трансиверов 10G SFP+/1G SFP.
11	XLG1 – XLG2	Слоты для установки трансиверов 40G QSFP+.

Передняя панель устройства ESR-1500

Внешний вид передней панели устройства показан на рисунке 18.

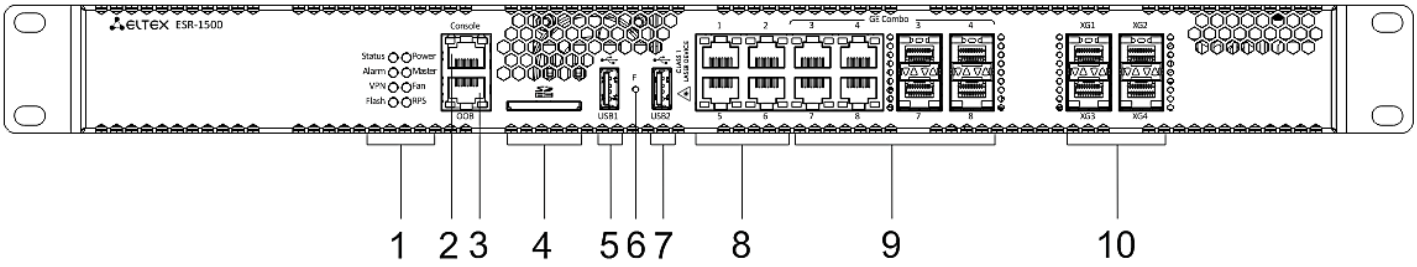


Рисунок 18 – Передняя панель ESR-1500

В таблице 18 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели устройства ESR-1500.

Таблица 18 – Описание разъемов, индикаторов и органов управления передней панели ESR-1500

№	Элемент передней панели	Описание
1	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	VPN	Индикатор режима работы в режиме VPN-шлюза (не используется в текущей версии).
	Flash	Индикатор активности обмена с накопителем данных – SD-картой или USB Flash.
	Power	Индикатор питания устройства.
	Master	Индикатор работы устройства в failover-режимах (не используется в текущей версии).
	Fan	Индикатор аварии вентиляторов.
	RPS	Индикатор резервного источника электропитания.
2	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
3	OOB	Ethernet-порт используется только для обновления программного обеспечения через загрузчик U-Boot. Данный порт не используется для удаленного доступа и управления.
4	SD	Разъем для установки SD-карт памяти.
5	USB1	Порт для подключения USB-устройств.

№	Элемент передней панели	Описание
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.
7	USB2	Порт для подключения USB-устройств.
8	Ethernet	4 порта Ethernet 10/100/1000BASE-T.
9	Combo Ports [1 .. 4]	4 порта Gigabit Ethernet 10/100/1000BASE-X (SFP).
10	XG1 – XG4	Слоты для установки трансиверов 10G SFP+/1G SFP.

Задняя панель устройств ESR-1511, ESR-1500

Внешний вид задней панели устройств ESR-1511, ESR-1500 приведен на рисунке 19.

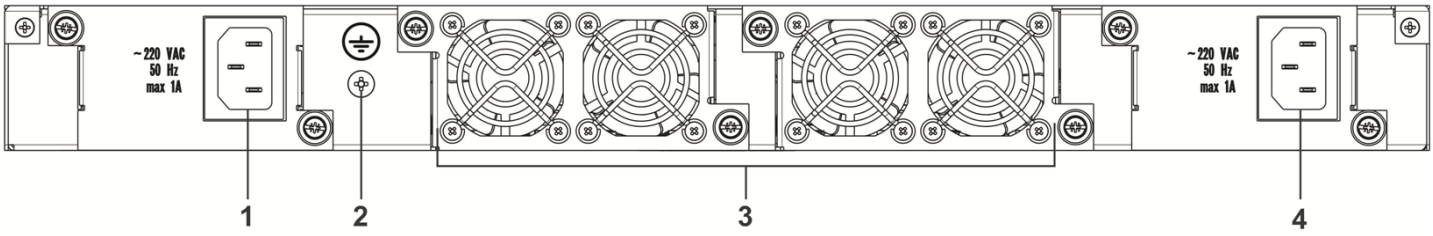


Рисунок 19 – Задняя панель ESR-1511, ESR-1500

В таблице 19 приведен перечень разъемов, расположенных на задней панели маршрутизаторов.

Таблица 19 – Описание разъемов задней панели ESR-1511, ESR-1500

№	Описание
1	Основной источник питания.
2	Клемма для заземления устройства.
3	Съемные вентиляционные модули с возможностью горячей замены.
4	Место для установки резервного источника питания.

Боковые панели устройств ESR-1511, ESR-1500

Внешний вид боковых панелей устройств ESR-1511, ESR-1500 приведен на рисунках 20 и 21.

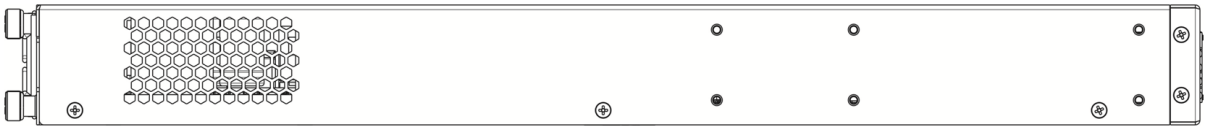


Рисунок 20 – Правая боковая панель ESR-1511, ESR-1500

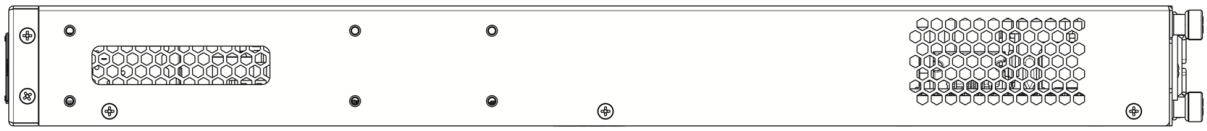


Рисунок 21 – Левая боковая панель ESR-1511, ESR-1500

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 разделе Установка и подключение.

3.4.6 Конструктивное исполнение ESR-1200, ESR-1000

Передняя панель устройства ESR-1200

Внешний вид передней панели показан на рисунке 22.

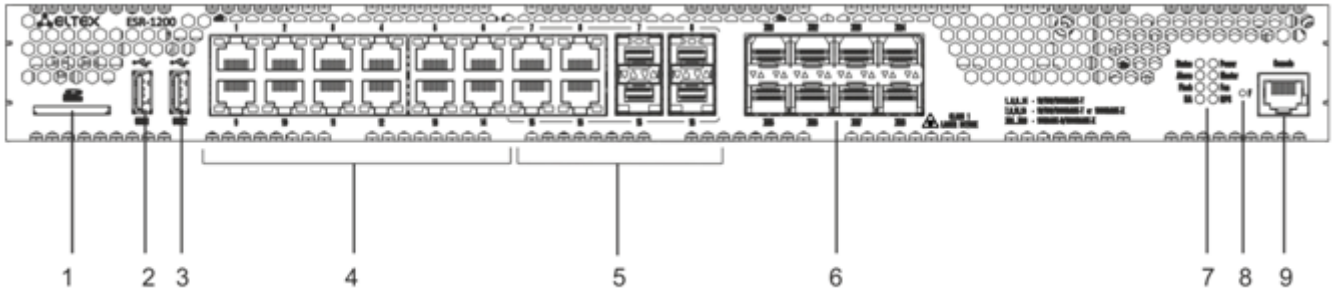


Рисунок 22 – Передняя панель ESR-1200

В таблице 20 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели устройства ESR-1200.

Таблица 20 – Описание разъемов, индикаторов и органов управления передней панели ESR-1200

№	Элемент передней панели	Описание
1	SD	Разъем для установки SD-карт памяти.
2	USB1	Порт для подключения USB-устройств.
3	USB2	Порт для подключения USB-устройств.
4	[1 .. 12]	12 портов Gigabit Ethernet 10/100/1000BASE-T (RJ-45).

№	Элемент передней панели	Описание
5	Combo Ports	4 порта Gigabit Ethernet 10/100/1000BASE-X (SFP).
6	XG1 – XG8	Слоты для установки трансиверов 10G SFP+/1G SFP.
7	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	HA	Индикатор режима работы в режиме HA.
	Flash	Индикатор активности обмена с накопителем данных – SD-картой или USB Flash.
	Power	Индикатор питания устройства.
	Master	Индикатор работы устройства в failover-режимах.
	Fan	Индикатор аварии вентиляторов.
	RPS	Индикатор резервного источника электропитания.
8	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.
9	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.

Передняя панель устройства ESR-1000

Внешний вид передней панели показан на рисунке 23.

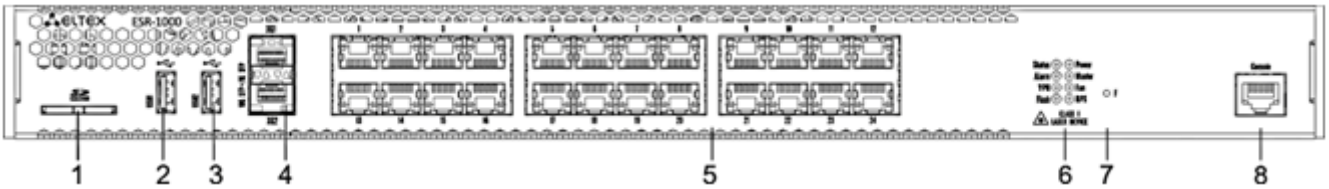


Рисунок 23 – Передняя панель ESR-1000

В таблице 21 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели устройства ESR-1000.

Таблица 21 – Описание разъемов, индикаторов и органов управления передней панели ESR-1000

№	Элемент передней панели	Описание
1	SD	Разъем для установки SD-карт памяти.
2	USB1	Порт для подключения USB-устройств.
3	USB2	Порт для подключения USB-устройств.
4	XG1, XG2	Слоты для установки трансиверов 10G SFP+/1G SFP.
5	[1 .. 24]	24 порта Gigabit Ethernet 10/100/1000BASE-T (RJ-45).
6	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	VPN	Индикатор наличия активных VPN-сессий.
	Flash	Индикатор активности обмена с накопителем данных – SD-картой или USB Flash.
	Power	Индикатор питания устройства.
	Master	Индикатор работы устройства в failover-режимах.
	Fan	Индикатор аварии вентиляторов.
	RPS	Индикатор резервного источника электропитания.
7	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.
8	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.

Задняя панель устройств ESR-1200, ESR-1000

Внешний вид задней панели устройства ESR-1000 приведен на рисунке ниже.

> ⚠ **На рисунке показана комплектация маршрутизатора с одним источником питания переменного тока.**

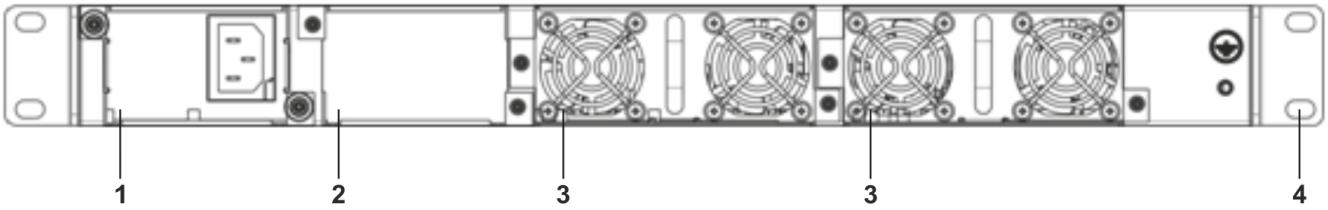


Рисунок 24 – Задняя панель ESR-1000

В таблице 22 приведен перечень разъемов, расположенных на задней панели маршрутизатора.

Таблица 22 – Описание разъемов задней панели ESR-1000

№	Описание
1	Основной источник питания.
2	Место для установки резервного источника питания.
3	Съемные вентиляционные модули с возможностью горячей замены.
4	Клемма для заземления устройства.

Боковые панели устройств ESR-1200, ESR-1000

Внешний вид боковых панелей устройств ESR-1200, ESR-1000 приведен на рисунках 25 и 26.

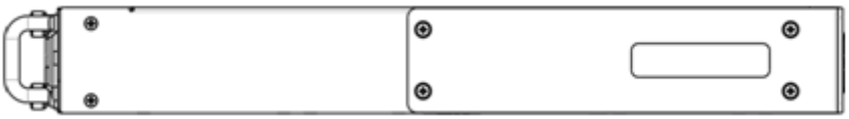


Рисунок 25 – Правая боковая панель маршрутизаторов ESR-1200, ESR-1000

Рисунок 26 – Левая боковая панель маршрутизаторов ESR-1200, ESR-1000

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 разделе Установка и подключение.

3.4.7 Конструктивное исполнение ESR-200, ESR-100

Передняя панель устройств ESR-200, ESR-100

Внешний вид передней панели ESR-200 показан на рисунке 27.

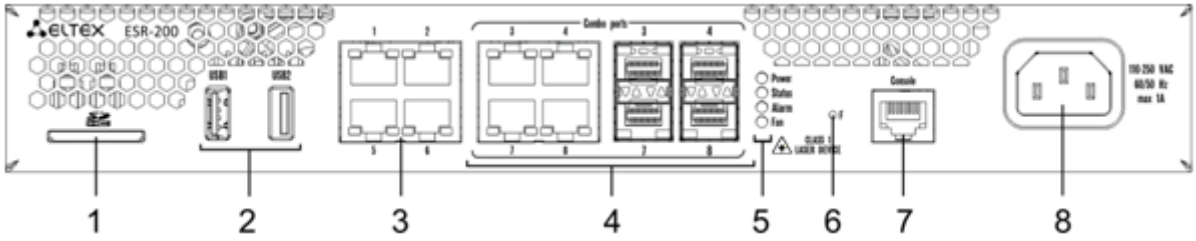


Рисунок 27 – Передняя панель ESR-200

Внешний вид передней панели ESR-100 показан на рисунке 28.

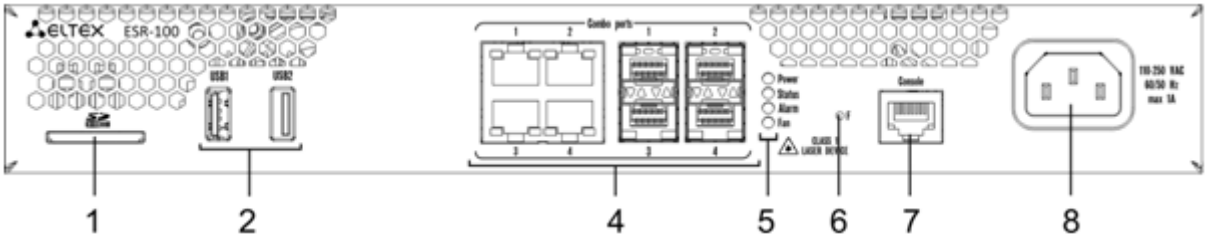


Рисунок 28 – Передняя панель ESR-100

В таблице 23 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели устройств ESR-200, ESR-100.

Таблица 23 – Описание разъемов, индикаторов и органов управления передней панели ESR-200, ESR-100

№	Элемент передней панели	Описание
1	SD	Разъем для установки SD-карт памяти.
2	USB1, USB2	2 порта для подключения USB-устройств.
3	[1 .. 4]	4 порта Gigabit Ethernet 10/100/1000BASE-T (RJ-45).
4	Combo Ports	4 порта Gigabit Ethernet 10/100/1000BASE-X (SFP).
5	Power	Индикатор питания устройства.
	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.

№	Элемент передней панели	Описание
	Fan	Индикатор аварии вентиляторов.
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.
7	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
8	110-250 VAC 60/50 Hz max 1A	Источник питания.

Задняя панель устройств ESR-200, ESR-100

Внешний вид задней панели устройств ESR-200, ESR-100 приведен на рисунке 29.

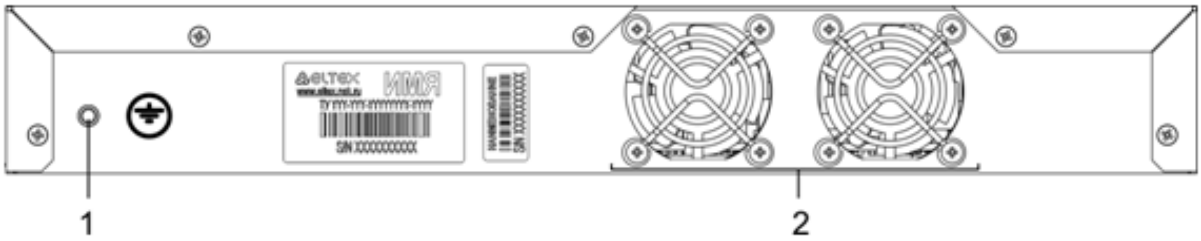


Рисунок 29 – Задняя панель ESR-200, ESR-100

В таблице 24 приведен перечень разъемов, расположенных на задней панели маршрутизатора.

Таблица 24 – Описание разъемов задней панели ESR-200, ESR-100

№	Описание
1	Клемма для заземления устройства.
2	Вентиляционный модуль.

Боковые панели устройств ESR-200, ESR-100

Внешний вид боковых панелей устройств ESR-200, ESR-100 приведен на рисунках 30 и 31.

Рисунок 30 – Правая боковая панель маршрутизатора ESR-200, ESR-100

Рисунок 31 – Левая боковая панель маршрутизатора ESR-200, ESR-100

3.4.8 Конструктивное исполнение ESR-21

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

Передняя панель устройства ESR-21

Внешний вид передней панели ESR-21 показан на рисунке 32.

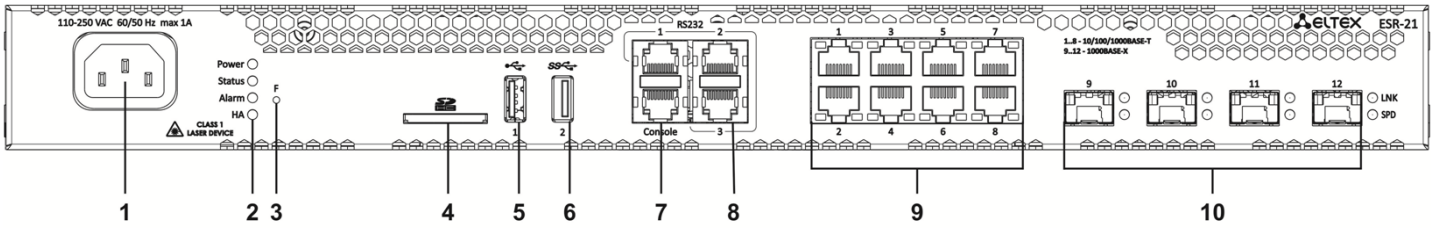


Рисунок 32 – Передняя панель ESR-21

В таблице 25 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели устройства ESR-21.

Таблица 25 – Описание разъемов, индикаторов и органов управления передней панели ESR-21

№	Элемент передней панели	Описание
1	220V AC	Источник питания.
2	Power	Индикатор питания устройства.
	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	HA	Индикатор работы в режиме HA (не используется в текущей версии).

№	Элемент передней панели	Описание
3	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.
4	SD	Разъем для установки SD-карт памяти.
5	USB1	Разъем USB 2.0 для подключения внешних USB-устройств.
6	USB2	Разъем USB 3.0 для подключения внешних USB-устройств.
7	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
8	RS-232	3 последовательных порта.
9	[1 .. 8]	8 портов Gigabit Ethernet 10/100/1000BASE-T (RJ-45).
10	Optical Port	4 порта Gigabit Ethernet 10/100/1000BASE-X (SFP).

Задняя панель устройств ESR-21

Внешний вид задней панели устройства ESR-21 показан на рисунке 33.

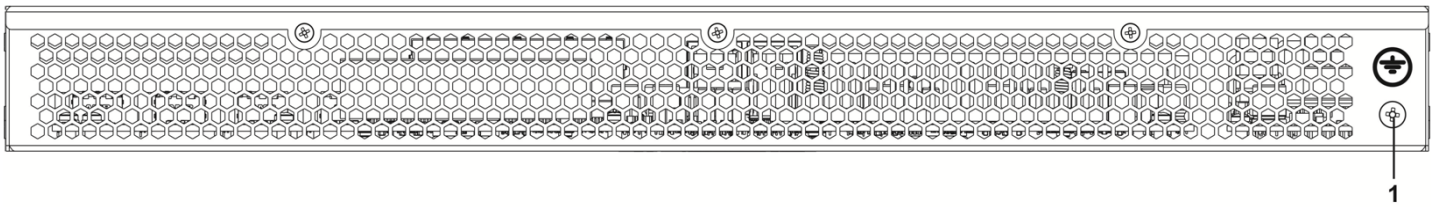


Рисунок 33 – Задняя панель ESR-21

В таблице 26 приведен перечень разъемов, расположенных на задней панели маршрутизатора.

Таблица 26 – Описание разъемов задней панели ESR-21

№	Описание
1	Клемма для заземления устройства.

Боковые панели устройства ESR-21

Внешний вид боковых панелей устройства ESR-21 приведен на рисунках 34 и 35.

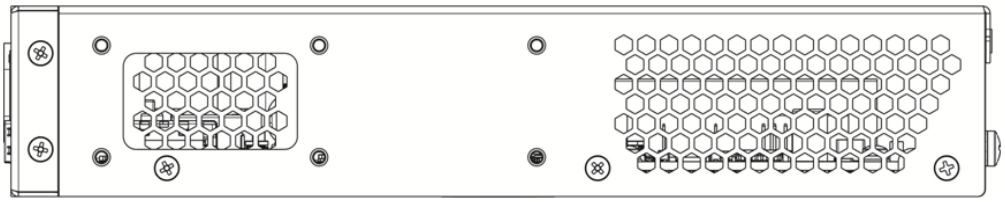


Рисунок 34 – Левая панель ESR-21

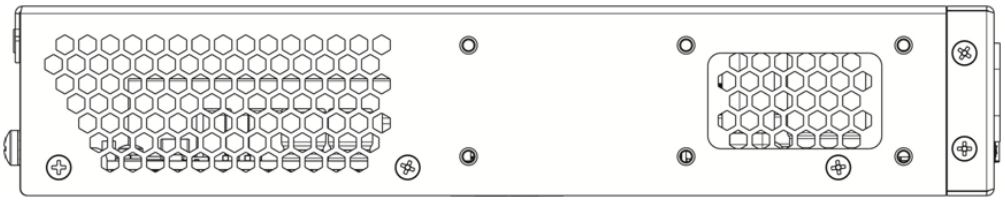


Рисунок 35 – Правая панель ESR-21

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 разделе Установка и подключение.

3.4.9 Конструктивное исполнение ESR-30, ESR-20

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

Передняя панель устройства ESR-30

Внешний вид передней панели показан на рисунке 36.

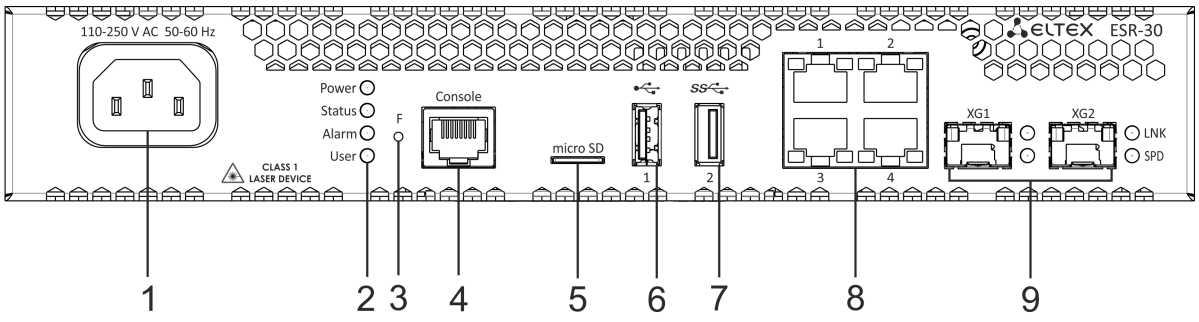


Рисунок 36 – Передняя панель ESR-30

В таблице 27 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели устройства ESR-30.

Таблица 27 – Описание разъемов, индикаторов и органов управления передней панели ESR-30

№	Элемент передней панели	Описание
1	110-250 VAC	Источник питания.
2	Power	Индикатор питания устройства.
	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	User	Индикатор, использующийся для пользовательских сценариев, которые можно назначить в режиме конфигурирования устройства.
3	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.
4	Console	Консольный порт для локального управления устройством.
5	microSD	Разъем для установки microSD-карт памяти.
6	USB1	Разъем USB 2.0 для подключения внешних USB-устройств.
7	USB2	Разъем USB 3.0 для подключения внешних USB-устройств.
8	[1 .. 4]	4 порта Ethernet 10/100/1000BASE-T.
9	1, 2	2 порта 10GBASE-R (SPF+)/1000BASE-X.

Передняя панель устройства ESR-20

Внешний вид передней панели показан на рисунке 37.

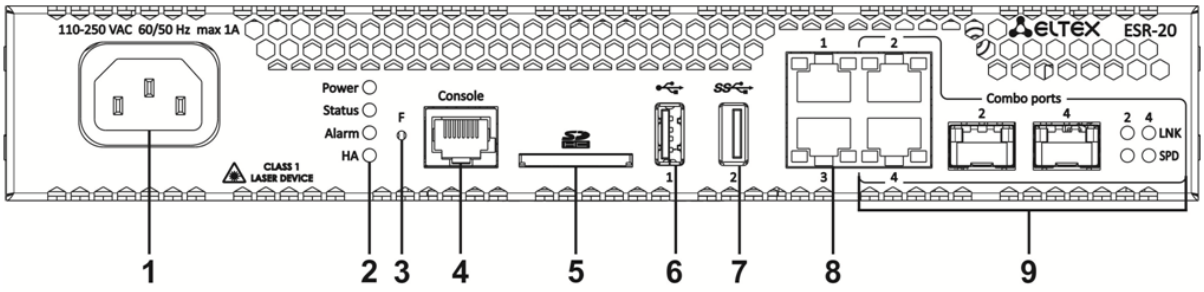


Рисунок 37 – Передняя панель ESR-20

В таблице 28 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели устройства ESR-20.

Таблица 28 – Описание разъемов, индикаторов и органов управления передней панели ESR-20

№	Элемент передней панели	Описание
1	110-250 VAC	Источник питания.
2	Power	Индикатор питания устройства.
	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	HA	Индикатор работы в режиме HA (не используется в текущей версии).
3	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.
4	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
5	SD	Разъем для установки SD-карт памяти.
6	USB1	Разъем USB 2.0 для подключения внешних USB-устройств.
7	USB2	Разъем USB 3.0 для подключения внешних USB-устройств.
8	1, 2	2 порта Gigabit Ethernet 10/100/1000BASE-T (RJ-45).
9	[1 .. 4]	2 Combo-порта Ethernet 10/100/1000BASE-X/10/100/1000BASE-T.

Задняя панель устройств ESR-30, ESR-20

Внешний вид задней панели устройств ESR-30, ESR-20 показан на рисунке 38.

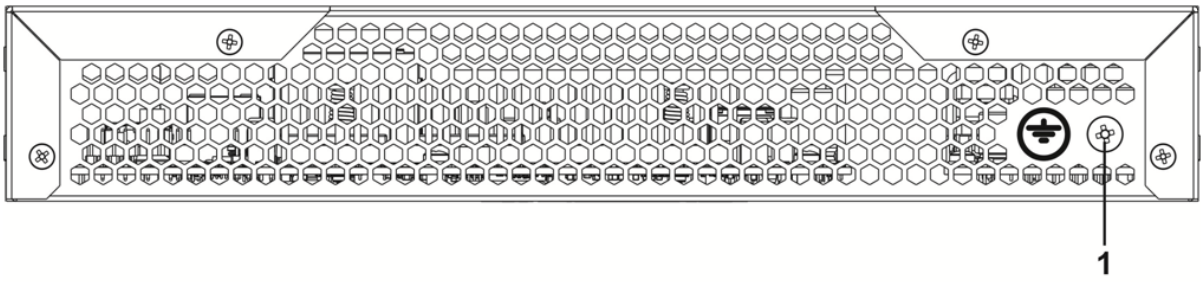


Рисунок 38 – Задняя панель ESR-30, ESR-20

В таблице 29 приведен перечень разъемов, расположенных на задней панели маршрутизатора.

Таблица 29 – Описание разъемов задней панели ESR-20

№	Описание
1	Клемма для заземления устройства.

Боковые панели устройств ESR-30, ESR-20

Внешний вид боковых панелей устройств ESR-30, ESR-20 приведен на рисунках 39 и 40.

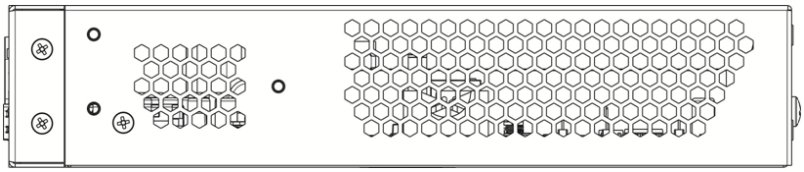


Рисунок 39 – Левая панель ESR-30, ESR-20

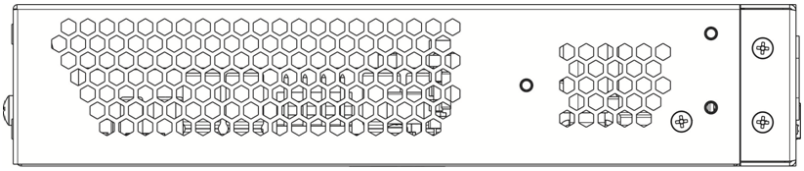


Рисунок 40 – Правая панель ESR-30, ESR-20

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 разделе Установка и подключение.

3.4.10 Конструктивное исполнение ESR-15

Задняя панель устройства ESR-15

Внешний вид задней панели устройства показан на рисунке 41.

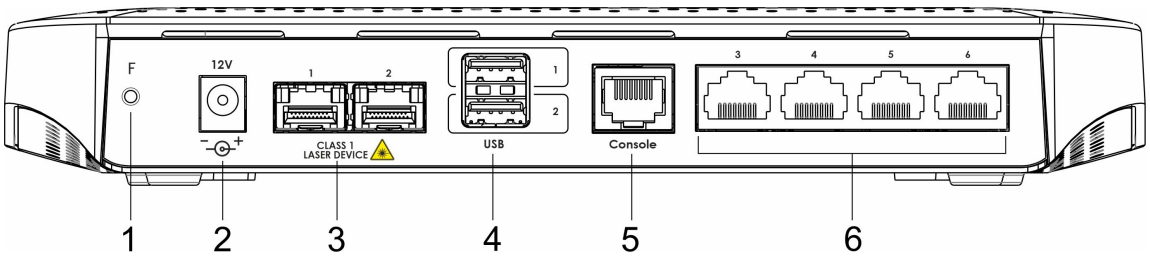


Рисунок 41 – Задняя панель ESR-15

В таблице 30 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на задней панели устройства ESR-15.

Таблица 30 – Описание разъемов, индикаторов и органов управления задней панели ESR-10

№	Элемент передней панели	Описание
1	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при длительности нажатия на кнопку менее 10 секунд происходит перезагрузка устройства; • при длительности нажатия на кнопку более 10 секунд происходит сброс устройства к заводской конфигурации.
2	12V DC	Разъем для подключения адаптера питания.
3	Optical Ports	2 порта Gigabit Ethernet –1000BASE-X (SFP).
4	USB1, USB2	2 разъема для подключения внешних USB-устройств.
5	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
6	[1 .. 4]	4 порта Gigabit Ethernet – 10/100/1000BASE-T (RJ-45)

Верхняя панель устройства ESR-15

Внешний вид верхней панели устройства ESR-15 показан на рисунке 42.

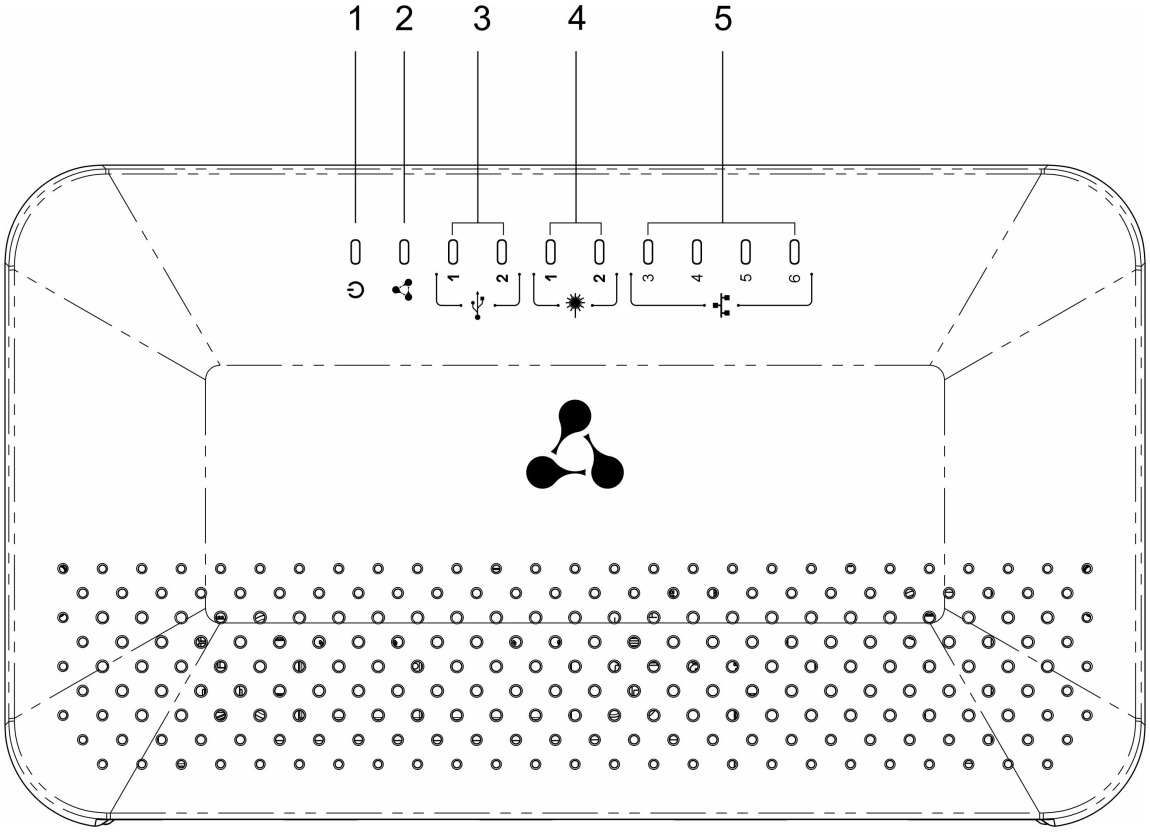


Рисунок 42 – Верхняя панель ESR-15

В таблице 31 приведен перечень светодиодных индикаторов, расположенных на верхней панели устройства ESR-15.

Таблица 31 – Описание индикаторов верхней панели ESR-15

№	Элемент верхней панели	Описание
1	Power	Индикатор питания и статуса работы устройства.
2	-	Индикатор не используется.
3	USB1, USB2	Индикаторы работы внешних USB-устройств.
4	[1 .. 2]	Индикаторы работы оптических интерфейсов.
5	[3 .. 6]	Индикаторы работы Ethernet-портов.

3.4.11 Конструктивное исполнение ESR-14VF, ESR-12VF

Устройства выполнены в металлическом корпусе с возможностью установки в 19” конструктив, высота корпуса 1U.

Передняя панель устройств ESR-14VF, ESR-12VF

Внешний вид передней панели показан на рисунке 43.

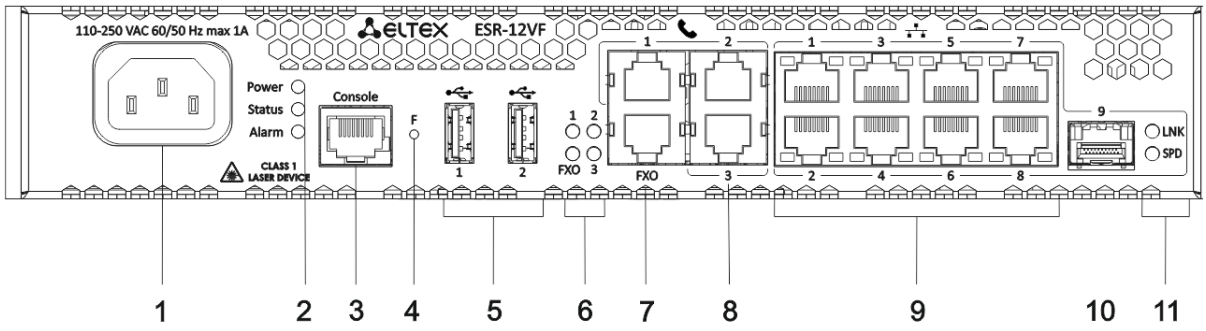


Рисунок 43 – Передняя панель ESR-14VF, ESR-12VF

В таблице 32 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели устройств ESR-14VF, ESR-12VF.

Таблица 32 – Описание разъемов, индикаторов и органов управления передней панели ESR-14VF, ESR-12VF

№	Элемент передней панели	Описание
1	220V AC	Источник питания.
2	Power	Индикатор питания устройства.
3	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
4	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.
5	USB1, USB2	2 разъема USB для подключения внешних USB-устройств.
6	FXO	Индикатор внешней абонентской линии от ТфОП.
	1, 2, 3	Индикатор для внутренних абонентских терминалов.
7	FXO	1 разъем FXO для подключения внешней абонентской линии от ТфОП (только для ESR-12VF).

№	Элемент передней панели	Описание
8	FXS 1, FXS 2, FXS 3	3 разъема для внутренних абонентских терминалов (для ESR-12VF).
	FXS 1, FXS 2, FXS 3	4 разъема для внутренних абонентских терминалов (для ESR-14VF).
9	[1 .. 8]	8 портов Gigabit Ethernet 10/100/1000BASE-T (RJ-45).
10	Optical Port	1 порт Gigabit Ethernet-100/1000BASE-X (SFP).
11	1, 2	Индикаторы работы оптических интерфейсов.

Задняя панель устройств ESR-14VF, ESR-12VF

Внешний вид задней панели устройств ESR-14VF, ESR-12VF показан на рисунке 44.

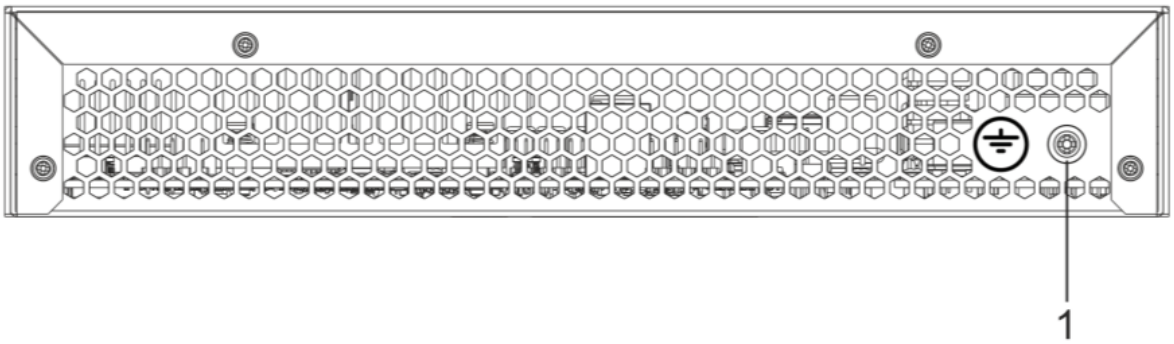


Рисунок 44 – Задняя панель ESR-14VF, ESR-12VF

В таблице 33 приведен перечень разъемов, расположенных на задней панели устройств.

Таблица 33 – Описание разъемов задней панели ESR-14VF, ESR-12VF

№	Описание
1	Клемма для заземления устройства.

Боковые панели устройств ESR-14VF, ESR-12VF

Внешний вид боковых панелей устройств ESR-14VF, ESR-12VF приведен на рисунках 45 и 46.

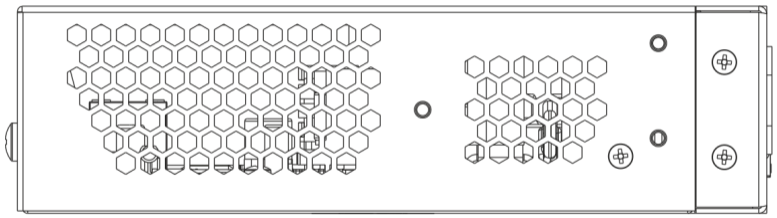


Рисунок 45 – Левая панель ESR-14VF, ESR-12VF

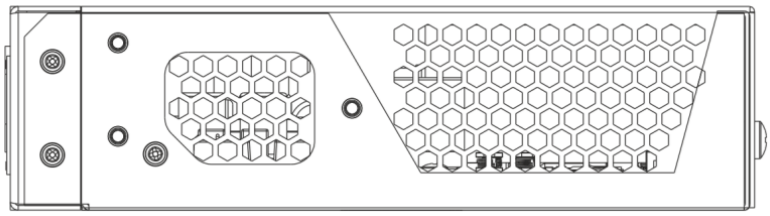


Рисунок 46 – Правая панель ESR-14VF, ESR-12VF

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 разделе Установка и подключение.

3.4.12 Конструктивное исполнение ESR-12V

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

Передняя панель устройства ESR-12V

Внешний вид передней панели показан на рисунке 47.

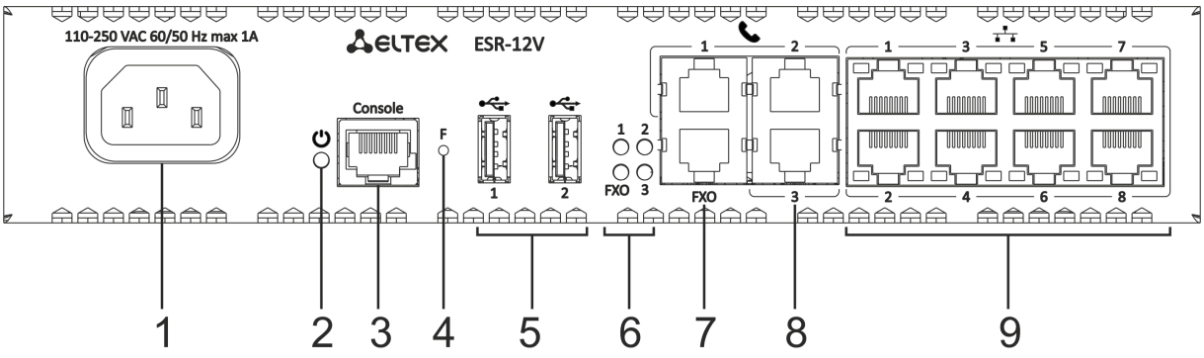


Рисунок 47 – Передняя панель ESR-12V

В таблице 34 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели устройства ESR-12V.

Таблица 34 – Описание разъемов, индикаторов и органов управления передней панели ESR-12V

№	Элемент передней панели	Описание
1	220V AC	Источник питания.
2	Power	Индикатор питания устройства.
3	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
4	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.
5	USB1, USB2	2 разъема USB для подключения внешних USB-устройств.
6	FXO	Индикатор внешней абонентской линии от ТфОП.
	1,2,3	Индикатор для внутренних абонентских терминалов.
7	FXO	1 разъем FXO для подключения внешней абонентской линии от ТфОП.
8	FXS 1, FXS 2, FXS 3	3 разъема для внутренних абонентских терминалов.
9	[1 .. 8]	8 портов Gigabit Ethernet 10/100/1000BASE-T (RJ-45).

Задняя панель устройств ESR-12V

Внешний вид задней панели устройства ESR-12V показан на рисунке 48.

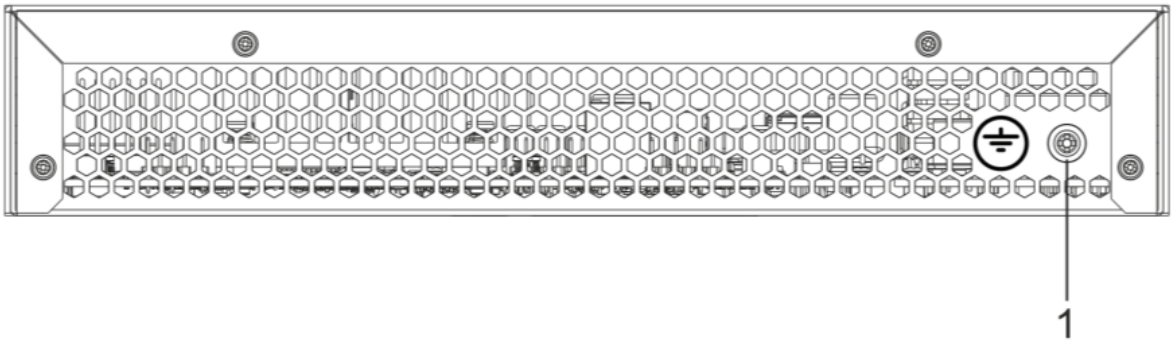


Рисунок 48 – Задняя панель ESR-12V

В таблице 35 приведен перечень разъемов, расположенных на задней панели маршрутизатора.

Таблица 35 – Описание разъемов задней панели ESR-12V

№	Описание
1	Клемма для заземления устройства.

Боковые панели устройства ESR-12V

Внешний вид боковых панелей устройства ESR-12V приведен на рисунках 49 и 50.

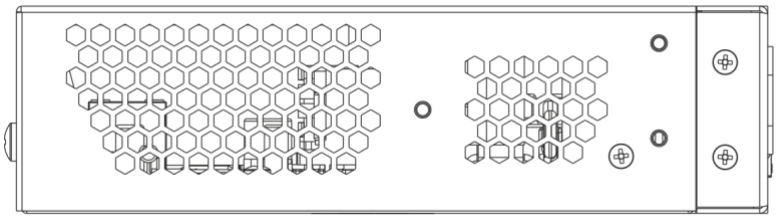


Рисунок 49 – Левая панель ESR-12V

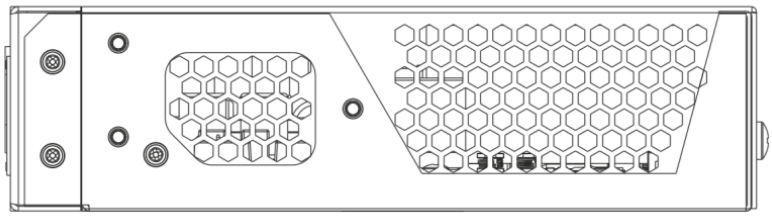


Рисунок 50 – Правая панель ESR-12V

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 разделе Установка и подключение.

3.4.13 Конструктивное исполнение ESR-10

Задняя панель устройства ESR-10

Внешний вид задней панели устройства показан на рисунке 51.

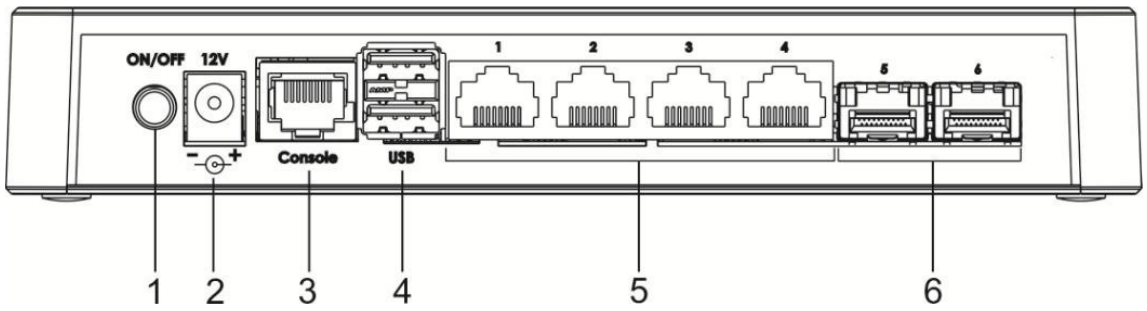


Рисунок 51 – Задняя панель ESR-10

В таблице 36 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на задней панели устройства ESR-10.

Таблица 36 – Описание разъемов, индикаторов и органов управления задней панели ESR-10

№	Элемент передней панели	Описание
1	ON/OFF	Кнопка включения/выключения питания.
2	12V DC	Разъем для подключения адаптера питания.
3	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
4	USB1, USB2	2 разъема для подключения внешних USB-устройств.
5	[1 .. 4]	4 порта Gigabit Ethernet – 10/100/1000BASE-T (RJ-45)
6	Optical Ports	2 порта Gigabit Ethernet –100/1000BASE-X (SFP)

Боковые панели устройства ESR-10

Внешний вид боковой панели устройства ESR-10 показан на рисунке 52.

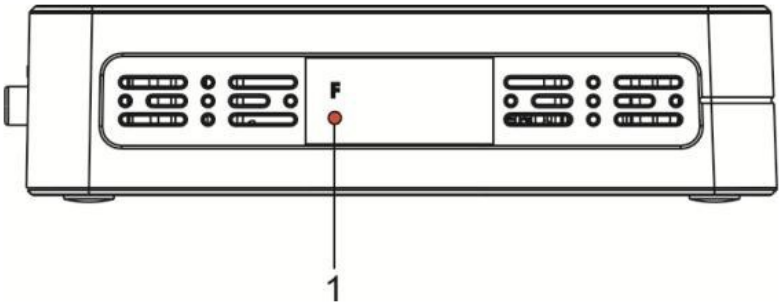


Рисунок 52 – Боковая панель ESR-10

В таблице 37 приведен перечень органов управления, расположенных на правой панели маршрутизатора.

Таблица 37 – Описание разъемов боковой панели ESR-10

№	Элемент боковой панели	Описание
1	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при длительности нажатия на кнопку менее 10 секунд происходит перезагрузка устройства; • при длительности нажатия на кнопку более 10 секунд происходит сброс устройства к заводской конфигурации.

Верхняя панель устройства ESR-10

Внешний вид верхней панели устройства ESR-10 показан на рисунке 53.

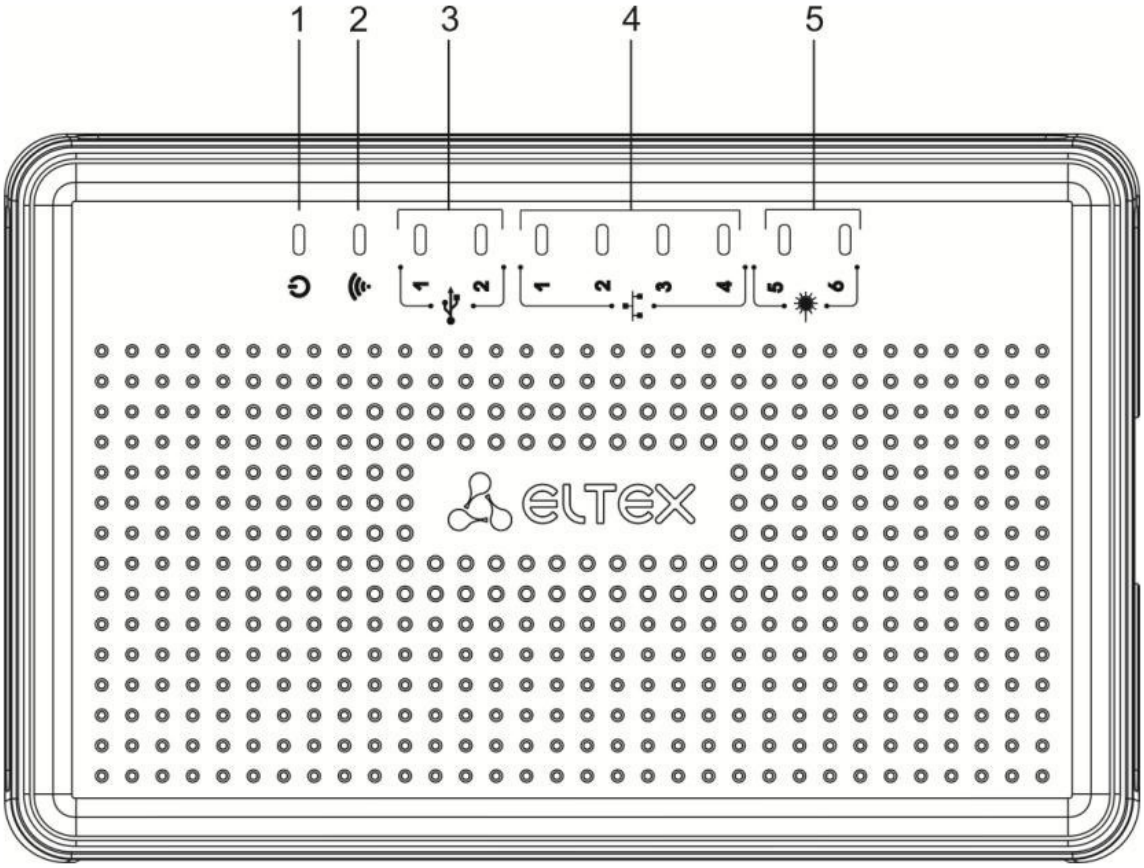


Рисунок 53 – Верхняя панель маршрутизатора ESR-10

В таблице 38 приведен перечень светодиодных индикаторов, расположенных на верхней панели устройства ESR-10.

Таблица 38 – Описание индикаторов верхней панели ESR-10

№	Элемент верхней панели	Описание
1	Power	Индикатор питания и статуса работы устройства.
2	-	Индикатор не используется.
3	USB1, USB2	Индикаторы работы внешних USB-устройств.
4	[1 .. 4]	Индикаторы работы Ethernet-портов.
5	[5 .. 6]	Индикаторы работы оптических интерфейсов.

3.4.14 Световая индикация

Световая индикация ESR-1700, ESR-1200, ESR-1000

Состояние медных интерфейсов Gigabit Ethernet отображается двумя светодиодными индикаторами – *LINK/ACT* зеленого цвета и *SPEED* янтарного цвета. Расположение индикаторов медных интерфейсов показано на рисунке 54. Состояние SFP-интерфейсов отображается двумя индикаторами RX/ACT и TX/ACT и указано на рисунке ниже. Значения световой индикации описаны в таблицах 39 и 40 соответственно.

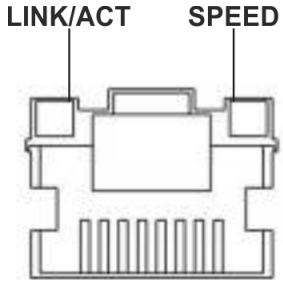


Рисунок 54 – Расположение индикаторов разъема RJ-45

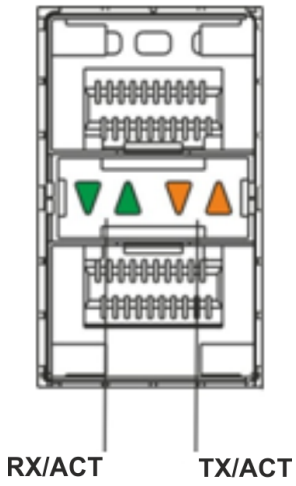


Рисунок 55 – Расположение индикаторов оптических интерфейсов

Таблица 39 – Световая индикация состояния медных интерфейсов

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

Таблица 40 – Световая индикация состояния SFP/SFP+/QSFP+-интерфейсов

Свечение индикатора RX/ACT	Свечение индикатора TX/ ACT	Состояние интерфейса Ethernet
Выключен	Выключен	Порт выключен или соединение не установлено.
Горит постоянно	Горит постоянно	Соединение установлено.
Мигание	X	Идет прием данных.
X	Мигание	Идет передача данных.

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

Таблица 41 – Состояния системных индикаторов

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Status	Индикатор текущего состояния устройства.	Зеленый	Устройство работает нормально.
		Красный	Устройство находится в состоянии загрузки ПО.
Alarm	Индикатор наличия и уровня аварии устройства.	-	-
VPN	Индикатор наличия активных VPN-сессий.	-	-
Flash	Индикатор активности обмена с накопителем данных: SD-картой или USB Flash.	Зеленый	Выполнение операций чтения/ записи по команде «сору».
Power	Индикатор питания устройства.	Зеленый	Питание устройства в норме. Основной источник питания, если он установлен, работает нормально.
		Оранжевый	Неработоспособность основного источника питания, авария или отсутствие первичной сети.
		Выключен	Отказ внутренних источников питания устройства.

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Master	Индикатор работы устройства в failover-режимах.	-	-
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.
RPS	Режим работы резервного источника питания.	Зеленый	Резервный источник установлен и исправен.
		Выключен	Резервный источник не установлен.
		Красный	Отсутствие первичного питания резервного источника или его неисправность.

Световая индикация ESR-3200, ESR-3100, ESR-1511, ESR-1500

Состояние медных интерфейсов Gigabit Ethernet отображается двумя светодиодными индикаторами – *LINK/ACT* зеленого цвета и *SPEED* янтарного цвета. Расположение индикаторов медных интерфейсов показано на рисунке 52. Состояние SFP-интерфейсов отображается двумя индикаторами RX/ACT и TX/ACT и указано на рисунке 57. Значения световой индикации описаны в таблицах 42 и 43 соответственно.

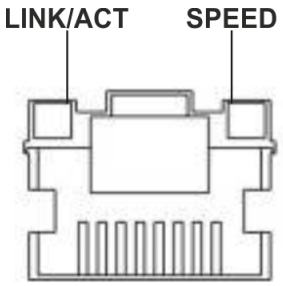


Рисунок 56 – Расположение индикаторов разъема RJ-45

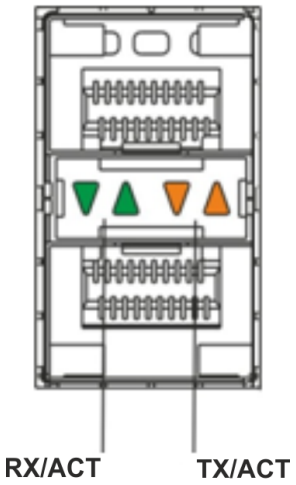


Рисунок 57 – Расположение индикаторов оптических интерфейсов

Таблица 42 – Световая индикация состояния медных интерфейсов

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

Таблица 43 – Световая индикация состояния SFP/SFP+/QSFP+-интерфейсов

Свечение индикатора RX/ACT	Свечение индикатора TX/ ACT	Состояние интерфейса Ethernet
Выключен	Выключен	Порт выключен или соединение не установлено.
Горит постоянно	Горит постоянно	Соединение установлено.
Мигание	X	Идет прием данных.
X	Мигание	Идет передача данных.

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

Таблица 44 – Состояния системных индикаторов

Название индикатора	Функция индикатора	Состояние индикатора	Состояние 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.	-	-
VPN	Индикатор наличия активных VPN-сессий.	-	-
Flash	Индикатор активности обмена с накопителем данных: SD-картой или USB Flash.	Зеленый	Выполнение операций чтения/ записи по команде «сору».
Power	Индикатор питания устройства.	Зеленый	Питание устройства в норме. Основной источник питания, если он установлен, работает нормально.
		Красный	Неработоспособность основного источника питания, авария или отсутствие первичной сети.
		Выключен	Отказ внутренних источников питания устройства.

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Master	Индикатор работы устройства в failover-режимах.	-	-
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.
RPS	Режим работы резервного источника питания.	Зеленый	Резервный источник установлен и исправен.
		Выключен	Резервный источник не установлен.
		Красный	Отсутствие первичного питания резервного источника или его неисправность.

Световая индикация ESR-200/ESR-100

Состояние медных интерфейсов Gigabit Ethernet и SFP-интерфейсов отображается двумя светодиодными индикаторами – *LINK/ACT* зеленого цвета и *SPEED* янтарного цвета. Расположение индикаторов медных интерфейсов показано на рисунке 54. Состояние SFP-интерфейсов указано на рисунке 58. Значения световой индикации описаны в таблице 45.

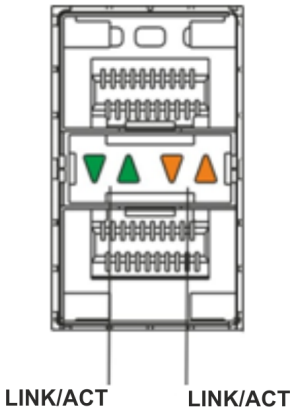


Рисунок 58 – Расположение индикаторов оптических интерфейсов

Таблица 45 – Световая индикация состояния медных интерфейсов и SFP-интерфейсов

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

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

Таблица 46 – Состояния системных индикаторов

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Status	Индикатор текущего состояния устройства.	Зеленый	Устройство работает нормально.
		Красный	Устройство находится в состоянии загрузки ПО.
Alarm	Индикатор наличия и уровня аварии устройства [1] .	-	-
Power	Индикатор питания устройства.	Зеленый	Питание устройства в норме. Основной источник питания, если он установлен, работает нормально.
		Красный	Неработоспособность основного источника питания, авария или отсутствие первичной сети.
		Выключен	Отказ внутренних источников питания устройства.
Fan	Состояние вентилятора охлаждения.	Выключен	Все вентиляторы исправны.

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
		Красный	Отказ одного или более вентиляторов. Причиной возникновения аварии может быть неработоспособность хотя бы одного из вентиляторов – остановка или пониженная частота оборотов.

[1] Не поддерживается в текущей версии ПО.

Световая индикация ESR-21/ESR-20

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

Таблица 47 – Световая индикация состояния медных интерфейсов и SFP-интерфейсов

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

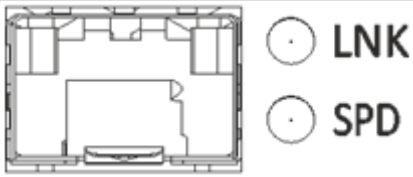


Рисунок 59 – Расположение индикаторов разъема SFP

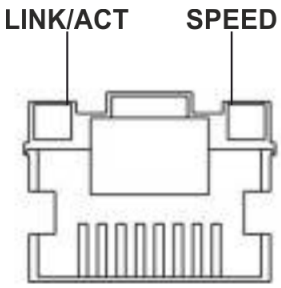


Рисунок 60 – Расположение индикаторов разъема RJ-45

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

Таблица 48 – 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.
		Красный	Устройство находится в состоянии загрузки ПО.
Alarm	Индикатор наличия и уровня аварии устройства.	-	-
HA	Индикатор работы в режиме HA (не используется в текущей версии)	-	-

Световая индикация ESR-30

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

Таблица 49 – Световая индикация состояния медных интерфейсов и SFP-интерфейсов

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

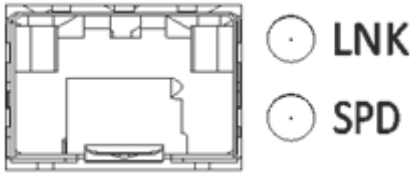


Рисунок 61 – Расположение индикаторов разъема SFP

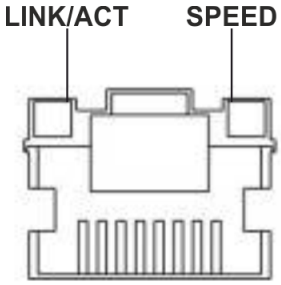


Рисунок 62 – Расположение индикаторов разъема RJ-45

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

Таблица 50 – 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.	-	-
HA	Индикатор работы в режиме HA (не используется в текущей версии).	-	-

Световая индикация ESR-15

Состояние медных интерфейсов Gigabit Ethernet отображается светодиодным индикатором SPEED янтарного/зеленого цвета.

Таблица 51 – Световая индикация состояния медных интерфейсов и SFP-интерфейсов

Свечение индикатора SPEED	Состояние интерфейса Ethernet
Выключен	Порт выключен или соединение не установлено.
Горит постоянно янтарным	Установлено соединение на скорости 1000 Мбит/с.
Горит постоянно зеленым	Установлено соединение на скорости 10 или 100 Мбит/с.
Мигание	Идет передача данных.

В таблице 52 приведено описание состояний системных индикаторов устройства и их значений.

Таблица 52 – 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.
USB1, USB2	Индикаторы работы внешних USB-устройств.	Зеленый	Подключено USB-устройство.
		Мигает зеленым	Выполнение операций чтения/записи.
		Выключен	Нет подключенных устройств или проблемы с подключением.

Световая индикация ESR-12V(F)

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

Таблица 53 – Световая индикация состояния медных интерфейсов и SFP-интерфейсов

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

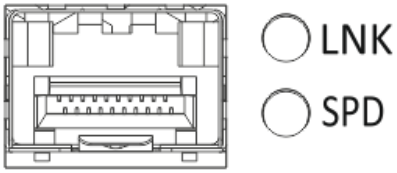


Рисунок 63 – Расположение индикаторов разъема SFP (только для ESR-12VF, ESR-14VF)

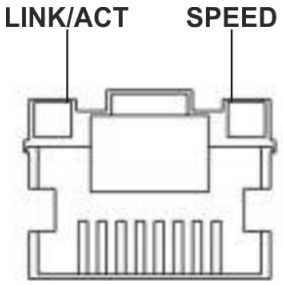


Рисунок 64 – Расположение индикаторов разъема RJ-45

В таблице 54 приведено описание состояний системных индикаторов устройства и их значений.

Таблица 54 – 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.

Световая индикация ESR-10

Состояние медных интерфейсов Gigabit Ethernet отображается светодиодным индикатором SPEED янтарного/зеленого цвета.

Таблица 55 – Световая индикация состояния медных интерфейсов и SFP-интерфейсов

Свечение индикатора SPEED	Состояние интерфейса Ethernet
Выключен	Порт выключен или соединение не установлено.
Горит постоянно янтарным	Установлено соединение на скорости 1000 Мбит/с.
Горит постоянно зеленым	Установлено соединение на скорости 10 или 100 Мбит/с.
Мигание	Идет передача данных.

В таблице 56 приведено описание состояний системных индикаторов устройства и их значений.

Таблица 56 – 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.
		Янтарный	Устройство находится в состоянии загрузки ПО.
		Выключен	Отказ внутренних источников питания устройства.
USB1, USB2	Индикаторы работы внешних USB-устройств.	Зеленый	Подключено USB-устройство
		Мигает зеленым	Выполнение операций чтения/записи
		Выключено	Нет подключенных устройств или проблемы с подключением

3.5 Комплект поставки

В базовый комплект поставки WLC-30 входят:

- контроллер WLC-30;
- кабель питания;
- консольный кабель;
- комплект для крепления устройства в стойку 19";
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки ESR-10 входят:

- маршрутизатор ESR-10;
- адаптер питания 220 В переменного тока/12 В постоянного тока, 1,5 А;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки ESR-12V входят:

- маршрутизатор ESR-12V;
- кабель питания;
- консольный кабель;
- комплект для крепления устройства в стойку 19”;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки ESR-12VF входят:

- маршрутизатор ESR-12VF;
- кабель питания;
- консольный кабель;
- комплект для крепления устройства в стойку 19”;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки ESR-14VF входят:

- маршрутизатор ESR-14VF;
- кабель питания;
- комплект для крепления устройства в стойку 19”;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки ESR-15 входят:

- маршрутизатор ESR-15;
- адаптер питания 220 В переменного тока/12 В постоянного тока, 2 А;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки ESR-20 входят:

- маршрутизатор ESR-20;
- кабель питания;
- консольный кабель;
- комплект для крепления устройства в стойку 19”;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки ESR-21 входят:

- маршрутизатор ESR-21;
- кабель питания;
- консольный кабель;
- комплект для крепления устройства в стойку 19”;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки ESR-30 входят:

- маршрутизатор ESR-30;
- кабель питания;
- консольный кабель;
- комплект для крепления устройства в стойку 19”;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки ESR-100 входят:

- маршрутизатор ESR-100;
- кабель питания;
- консольный кабель;
- комплект для крепления устройства в стойку 19”;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки ESR-200 входят:

- маршрутизатор ESR-200;
- кабель питания;
- консольный кабель;
- комплект для крепления устройства в стойку 19”;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки ESR-1000 входят:

- маршрутизатор ESR-1000;
- консольный кабель;
- комплект для крепления устройства в стойку 19”;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки ESR-1200 входят:

- маршрутизатор ESR-1200;
- консольный кабель;
- комплект для крепления устройства в стойку 19”;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки ESR-1500 входят:

- маршрутизатор ESR-1500;
- консольный кабель;
- комплект для крепления устройства в стойку 19”;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки ESR-1511 входят:

- маршрутизатор ESR-1511;
- консольный кабель;
- комплект для крепления устройства в стойку 19”;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки ESR-1700 входят:

- маршрутизатор ESR-1700;
- консольный кабель;
- комплект для крепления устройства в стойку 19”;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки ESR-3100 входят:

- маршрутизатор ESR-3100;
- консольный кабель;
- комплект для крепления устройства в стойку 19”;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки ESR-3200 входят:

- маршрутизатор ESR-3200;
- консольный кабель;
- комплект для крепления устройства в стойку 19”;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

По заказу покупателя для ESR-1000, ESR-1200 в комплект поставки может быть включен модуль питания (PM160-220/12 или PM100-48/12).
По заказу покупателя для ESR-1500, ESR-1511, ESR-3100, 3200 в комплект поставки может быть включен модуль питания (PM160-220/12).
По заказу покупателя для ESR-1700 в комплект поставки может быть включен модуль питания (PM350-220/12 или PM350-48/12).

По заказу покупателя в комплект поставки могут быть включены SFP/SFP+-трансиверы.

4 Установка и подключение

- Крепление кронштейнов
- Установка устройства в стойку
- Подключение к vESR
- Установка модулей питания ESR-1000, ESR-1200, ESR-1500, ESR-1511, ESR-1700, ESR-3100, ESR-3200
- Подключение питающей сети
- Установка и удаление SFP-трансиверов
    - Установка трансивера
    - Удаление трансивера

В данном разделе описаны процедуры установки устройства в стойку и подключения к питающей сети.

4.1 Крепление кронштейнов

В комплект поставки устройства входят кронштейны для установки в стойку и винты для крепления кронштейнов к корпусу устройства. Для установки кронштейнов:

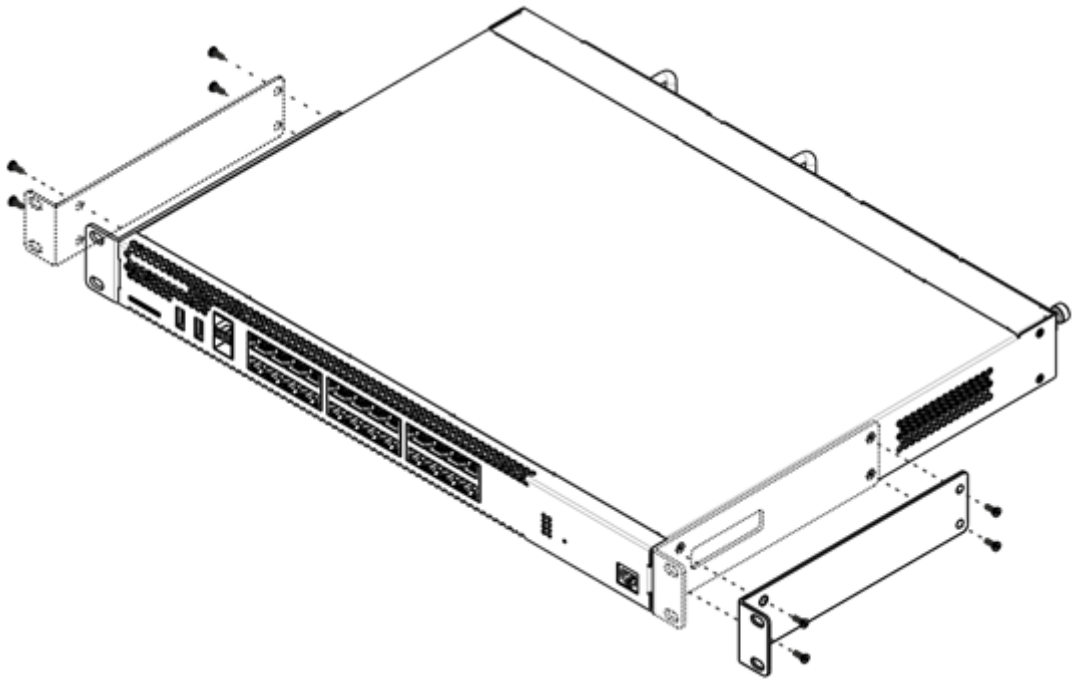


Рисунок 65 – Крепление кронштейнов

1. Совместите четыре отверстия для винтов на кронштейне с такими же отверстиями на боковой панели устройства.
2. С помощью отвертки прикрепите кронштейн винтами к корпусу.
3. Повторите действия 1, 2 для второго кронштейна.

4.2 Установка устройства в стойку

Для установки устройства в стойку:

1. Приложите устройство к вертикальным направляющим стойки.
2. Совместите отверстия кронштейнов с отверстиями на направляющих стойки. Используйте отверстия в направляющих на одном уровне с обеих сторон стойки для того, чтобы устройство располагалось горизонтально.
3. С помощью отвертки прикрепите маршрутизатор к стойке винтами.

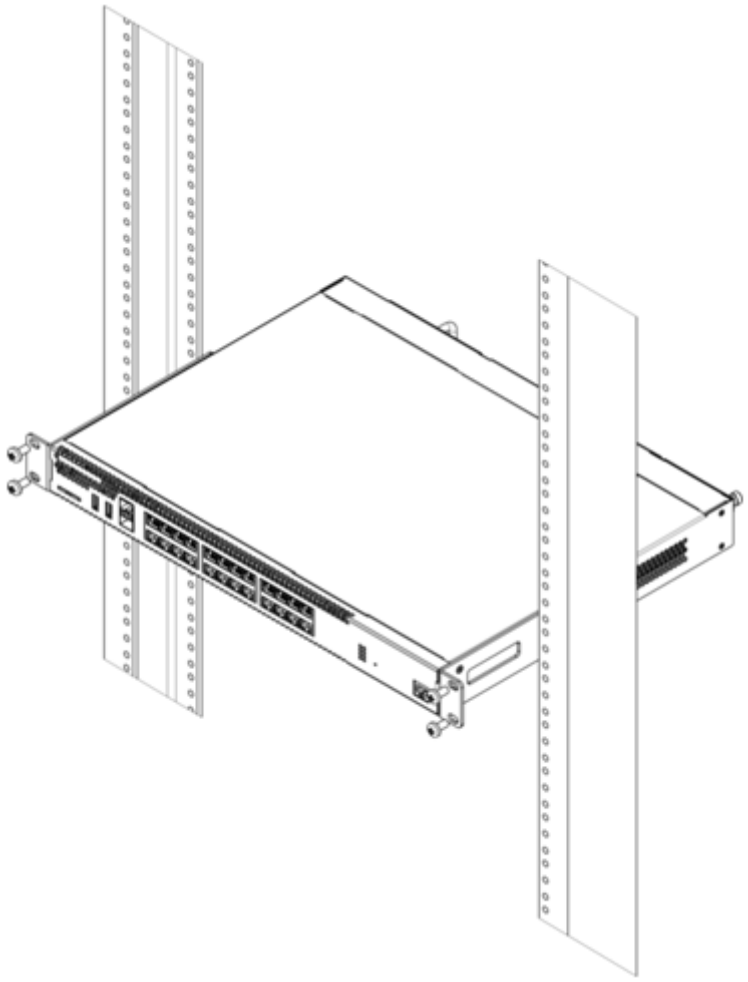


Рисунок 66 – Установка устройства в стойку

Вентиляция устройства организована по схеме фронт-тыл. На передней и боковых панелях устройства расположены вентиляционные отверстия, с задней стороны устройства расположены вентиляционные модули. Не закрывайте входные и выходные вентиляционные отверстия посторонними предметами во избежание перегрева компонентов устройства и нарушения его работы.

4.3 Подключение к vESR

Для установки и подключения к vESR перейдите в раздел документации vESR.

4.4 Установка модулей питания ESR-1000, ESR-1200, ESR-1500, ESR-1511, ESR-1700, ESR-3100, ESR-3200

Маршрутизаторы ESR-1000/1200/1500/1511/1700/3100 могут работать с одним или двумя модулями питания. Установка второго модуля питания необходима в случае использования устройства в условиях, требующих повышенной надежности.

Места для установки модулей питания с электрической точки зрения равноценны. С точки зрения использования устройства, модуль питания может находиться в основном и резервном разъеме, информация о приоритетности находится в таблице "Описание разъемов задней панели маршрутизатора". Модули питания могут устанавливаться и извлекаться без выключения устройства. При установке или извлечении дополнительного модуля питания маршрутизатор продолжает работу без перезапуска.

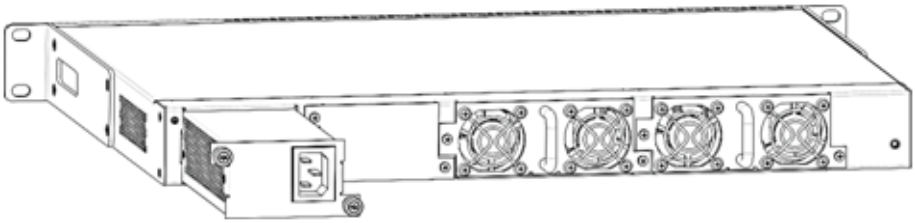


Рисунок 67 – Установка модулей питания

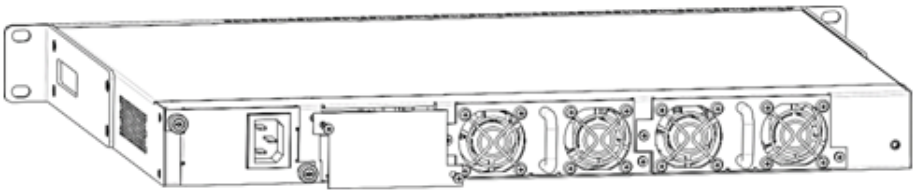


Рисунок 68 – Установка заглушки

Индикация аварии модуля питания может быть вызвана не только отказом модуля, но и отсутствием первичного питания.

Состояние модулей питания может быть проверено по индикации на передней панели маршрутизатора (см. раздел Световая индикация) или по диагностике, доступной через интерфейсы управления маршрутизатором.

4.5 Подключение питающей сети

1. Прежде чем к устройству будет подключена питающая сеть, необходимо заземлить корпус устройства. Заземление необходимо выполнять изолированным многожильным проводом. Устройство заземления и сечение заземляющего провода должны соответствовать требованиями Правил устройства электроустановок (ПУЭ).
2. Если предполагается подключение компьютера или иного оборудования к консольному порту маршрутизатора, это оборудование также должно быть надежно заземлено.
3. Подключите к устройству кабель питания. В зависимости от комплектации устройства, питание может осуществляться от сети переменного тока либо от сети постоянного тока. При подключении сети переменного тока следует использовать кабель, входящий в комплект устройства. Для подключения к сети постоянного тока используйте провод сечением не менее 1 мм^2.
4. Включите питание устройства и убедитесь в отсутствии аварий по состоянию индикаторов на передней панели.

4.6 Установка и удаление SFP-трансиверов

Установка оптических модулей может производиться как при выключенном, так и при включенном устройстве.

4.6.1 Установка трансивера

1. Вставьте верхний SFP-модуль в слот открытой частью разъема вниз, а нижний SFP-модуль – открытой частью разъема вверх.

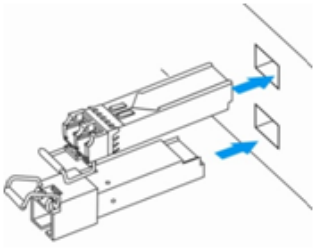


Рисунок 69 – Установка SFP-трансиверов

2. Надавите на модуль по направлению внутрь корпуса устройства до появления характерного щелчка фиксации модуля.

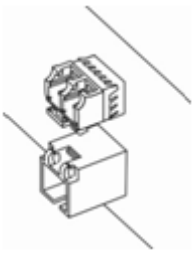


Рисунок 70 – Установленные SFP-трансиверы

4.6.2 Удаление трансивера

1. Откиньте рукоятку модуля, это приведет к разблокированию удерживающей защелки.

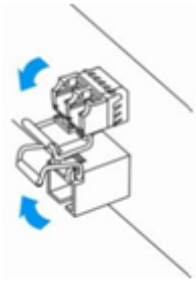


Рисунок 71 – Открытие защелки SFP-трансиверов

2. Извлеките модуль из слота.

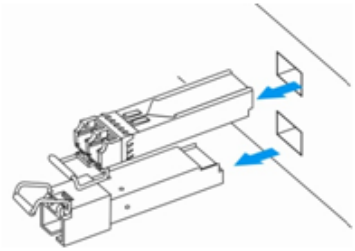


Рисунок 72 – Извлечение SFP-трансиверов

5 Интерфейсы управления

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

Настройка и мониторинг устройства могут осуществляться через различные интерфейсы управления.

Для доступа к устройству может использоваться сетевое подключение по протоколам Telnet и SSH или прямое подключение через консольный порт, соответствующий спецификации RS-232. При доступе по протоколам Telnet, SSH и при подключении через консольный порт для управления устройством используется интерфейс командной строки.

Заводская конфигурация содержит описание доверенной зоны trusted и IP-адрес для доступа к управлению устройством – 192.168.1.1/24.
В доверенную зону входят интерфейсы:

- **для WLC-30: GigabitEthernet 1/0/2-4, TengigabitEthernet 1/0/1-2;**
- **для ESR-10: GigabitEthernet 1/0/2-6;**
- **для ESR-12V(F), ESR-14VF: GigabitEthernet 1/0/2-8;**
- **для ESR-15: GigabitEthernet 1/0/2-5;**
- **для ESR-20: GigabitEthernet 1/0/2-4;**
- **для ESR-21: GigabitEthernet 1/0/2-12;**
- **для ESR-30: GigabitEthernet 1/0/3-4;**
- **для ESR-100: GigabitEthernet 1/0/2-4;**
- **для ESR-200: GigabitEthernet 1/0/2-8;**
- **для ESR-1000: GigabitEthernet 1/0/2-24;**
- **для ESR-1200: GigabitEthernet 1/0/2-16, TengigabitEthernet 1/0/3-8;**
- **для ESR-1500: GigabitEthernet 1/0/2-8, TengigabitEthernet 1/0/2-4;**
- **для ESR-1511: GigabitEthernet 1/0/2-8, TengigabitEthernet 1/0/1-4;**
- **для ESR-1700: GigabitEthernet 1/0/2-4, TengigabitEthernet 1/0/3-12;**
- **для ESR-3100: GigabitEthernet 1/0/2-8, TengigabitEthernet 1/0/3-8;**
- **для ESR-3200: Twentyfivegigabitethernet 1/0/3-12.**

В заводской конфигурации по умолчанию создан пользователь «admin» с паролем «password».

При использовании любого из перечисленных интерфейсов управления действуют единые принципы работы с конфигурацией. Должна соблюдаться определенная, описанная здесь, последовательность изменения и применения конфигурации, позволяющая защитить устройство от некорректного конфигурирования.

5.1 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.

5.2 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 57 – 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.
Порты 1 Гбит/с	**gigabitethernet <UNIT>/<SLOT>/<PORT>** Пример обозначения: **gigabitethernet 1/0/12** ⚠ **Допускается использовать сокращенное наименование, например gi1/0/12.**
Порты 10 Гбит/с	**tengigabitethernet <UNIT>/<SLOT>/<PORT>** Пример обозначения: **tengigabitethernet 1/0/2** ⚠ **Допускается использовать сокращенное наименование, например te1/0/2.**
Порты 40 Гбит/с	**fortygigabitethernet <UNIT>/<SLOT>/<PORT>** Пример обозначения: **fortygigabitethernet 1/0/2** ⚠ **Допускается использовать сокращенное наименование, например fo1/0/2.**

Тип интерфейса	Обозначение
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 1/0/12.100** • **tengigabitethernet 1/0/2.123** • **fortygigabitethernet 1/0/2.1024** • **port-channel 1.6** ⚠ **Идентификатор саб-интерфейса может принимать значения [1..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 1/0/12.100.10** • **tengigabitethernet 1/0/2.45.12** • **fortygigabitethernet 1/0/2.408.507** • **port-channel 1.6.34** ⚠ **Идентификатор сервисного и пользовательского VLAN может принимать значения [1..4094].**
E1-интерфейсы	Обозначение E1-интерфейса включает в себя его тип и идентификатор. Идентификатор E1-интерфейсов имеет вид **<UNIT>/<SLOT>/<STREAM>**, где • **<UNIT>** – номер устройства в группе устройств, • **<SLOT>** – номер E1-модуля в составе устройства, • **<STREAM>** – порядковый номер E1-потока. Пример обозначения: **e1 1/0/1**

Тип интерфейса	Обозначение
Группы агрегации E1-каналов	Обозначение группы агрегации E1-каналов включает в себя его тип и порядковый номер интерфейса: **multilink <CHANNEL_ID>** Пример обозначения: **multilink <CHANNEL_ID>**
Логические интерфейсы	Обозначение логического интерфейса является порядковым номером интерфейса: Примеры обозначений: • **loopback 4** • **bridge 60** • **service-port 1**
Последовательные интерфейсы	Обозначение последовательного интерфейса включает в себя его тип и идентификатор. Идентификатор последовательного интерфейса имеет вид **<UNIT>/<SLOT>/<STREAM>**, где • **<UNIT>** – номер устройства в группе устройств [1..1], • **<SLOT>** – номер модуля в составе устройства или 0 при отсутствии деления устройства на модули, • **<PORT>** – порядковый номер порта. Пример обозначения: **serial 1/0/1**
USB-модемы	Обозначение USB-модема включает в себя его тип и порядковый номер: **modem <MODEM-NUM>** Пример обозначения: **modem 1**
FXS/FXO-порты	Обозначение FXS/FXO-портов включает в себя его тип и порядковый номер: **interface voice-port <NUM>** Пример обозначения: **voice-port 1**

1. Количество интерфейсов каждого типа зависит от модели маршрутизатора.
2. Текущая версия ПО не поддерживает стекирование устройств. Номер устройства в группе устройств unit может принимать только значение 1.
3. 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 1/0/5
interface tengigabitethernet 1/0/1-2
interface fortygigabitethernet 1/0/1-2
interface gi1/0/1-3,gi1/0/7,te1/0/1,fo1/0/1
```

5.3 Типы и порядок именования туннелей маршрутизатора

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

Таблица 58 – Типы и порядок именования туннелей маршрутизатора

Тип туннеля	Обозначение
L2TPv3-туннель	Обозначение L2TPv3-туннеля состоит из обозначения типа и порядкового номера туннеля: **l2tpv3 <L2TPV3_ID>** Пример обозначения: **l2tpv3 1**
GRE-туннель	Обозначение GRE-туннеля состоит из обозначения типа и порядкового номера туннеля: **gre <GRE_ID>** Пример обозначения: **gre 1**
SoftGRE-туннель	Обозначение SoftGRE-туннеля состоит из обозначения типа, порядкового номера туннеля и, опционально, VLAN ID виртуального интерфейса: **softgre <GRE_ID>[.<VLAN>]** Примеры обозначения: **softgre 1, softgre 1.10**
IPv4-over-IPv4-туннель	Обозначение IPv4-over-IPv4-туннеля состоит из обозначения типа и порядкового номера туннеля: **ip4ip4 <IPIP_ID>** Пример обозначения: **ip4ip4 1**

Тип туннеля	Обозначение
IPsec-туннель	Обозначение виртуального IPsec-туннеля состоит из обозначения типа и порядкового номера туннеля: **vti <VTI_ID>** Пример обозначения: **vti 1**
Логический туннель (туннель между VRF)	Обозначение логического туннеля состоит из обозначения типа и порядкового номера туннеля: **lt <LT_ID>** Пример обозначения: **lt 1**

Количество туннелей каждого типа зависит от модели и ПО маршрутизатора.

6 Начальная настройка устройств

- Заводская конфигурация устройств
  - Описание заводской конфигурации
- Подключение и конфигурирование устройства
  - Подключение к устройству
    - Подключение по локальной сети Ethernet
    - Подключение через консольный порт RS-232
  - Применение изменения конфигурации
  - Базовая настройка устройств
    - Изменение пароля пользователя «admin»
    - Создание новых пользователей
    - Назначение имени устройства
    - Настройка параметров публичной сети
    - Настройка удаленного доступа к устройству

6.1 Заводская конфигурация устройств

При отгрузке устройства потребителю на устройство будет загружена заводская конфигурация, которая включает минимально необходимые базовые настройки. Заводская конфигурация позволяет использовать маршрутизаторы серии ESR в качестве шлюза с функцией SNAT без необходимости применять дополнительные настройки. Кроме того, заводская конфигурация содержит настройки, позволяющие получить сетевой доступ к устройству для выполнения расширенного конфигурирования.

6.1.1 Описание заводской конфигурации

Для подключения к сетям в конфигурации описаны 2 зоны безопасности с наименованиями «Trusted» для локальной сети и «Untrusted» для публичной сети. Все интерфейсы разделены между двух зон безопасности:

1. **Зона «Untrusted»** предназначена для подключения к публичной сети (WAN). В этой зоне открыты порты DHCP-протокола для получения динамического IP-адреса от провайдера. Все входящие соединения из данной зоны на маршрутизатор запрещены.
   В данную зону безопасности входят интерфейсы:
   - для WLC-30: GigabitEthernet 1/0/1, TengigabitEthernet 1/0/1-2;
   - для ESR-10/12V: GigabitEthernet 1/0/1;
   - для ESR-12VF/ESR-14VF: GigabitEthernet 1/0/1; GigabitEthernet 1/0/9;
   - для ESR-15: GigabitEthernet1/0/1; GigabitEthernet1/0/6;
   - для ESR-20: GigabitEthernet 1/0/1;
   - для ESR-21: GigabitEthernet 1/0/1;
   - для ESR-30: GigabitEthernet 1/0/1; TengigabitEthernet 1/0/1-2
   - для ESR-100/200: GigabitEthernet 1/0/1;
   - для ESR-1000/1500/3100: GigabitEthernet 1/0/1, TengigabitEthernet 1/0/1-2;
   - для ESR-1200/1700: GigabitEthernet 1/0/1, TengigabitEthernet 1/0/1, TengigabitEthernet 1/0/2;
   - для ESR-1511: GigabitEthernet 1/0/1, FortygigabitEthernet 1/0/1-2;
   - для ESR-3200: Twentyfivegigabitethernet 1/0/1-2.

   Интерфейсы зоны объединены в один L2-сегмент через сетевой мост *Bridge 2*.
2. **Зона «Trusted»** предназначена для подключения к локальной сети (LAN). В этой зоне открыты порты протоколов Telnet и SSH для удаленного доступа, ICMP-протокола для проверки доступности маршрутизатора, DHCP-протокола для получения клиентами IP-адресов от маршрутизатора. Исходящие соединения из данной зоны в зону «Untrusted» разрешены.
   В данную зону безопасности входят интерфейсы:
   - для WLC-30: GigabitEthernet 1/0/2-4;
   - для ESR-10: GigabitEthernet 1/0/2-6;
   - для ESR-12V(F)/ESR-14VF: GigabitEthernet 1/0/2-8;

- для ESR-15: GigabitEthernet 1/0/2-5;
- для ESR-20: GigabitEthernet 1/0/2-4;
- для ESR-21: GigabitEthernet 1/0/2-12;
- для ESR-30: GigabitEthernet 1/0/3-4;
- для ESR-100: GigabitEthernet 1/0/2-4;
- для ESR-200: GigabitEthernet 1/0/2-8;
- для ESR-1000: GigabitEthernet 1/0/2-24;
- для ESR-1200: GigabitEthernet 1/0/2-16, TengigabitEthernet 1/0/3-8;
- для ESR-1500: GigabitEthernet 1/0/2-8, TengigabitEthernet 1/0/3-4;
- для ESR-1511: GigabitEthernet 1/0/2-8, TengigabitEthernet 1/0/1-4;
- для ESR-1700: GigabitEthernet 1/0/2-4, TengigabitEthernet 1/0/3-12;
- для ESR-3100: GigabitEthernet 1/0/2-8, TengigabitEthernet 1/0/3-8;
- для ESR-3200: Twentyfivegigabitethernet 1/0/3-12.

Интерфейсы зоны объединены в один L2-сегмент через сетевой мост *Bridge 1*.

На интерфейсе *Bridge 2* включен DHCP-клиент для получения динамического IP-адреса от провайдера. На интерфейсе *Bridge 1* сконфигурирован статический IP-адрес 192.168.1.1/24. Созданный IP-интерфейс выступает в качестве шлюза для клиентов локальной сети. Для клиентов локальной сети настроен DHCP-пул адресов 192.168.1.2-192.168.1.254 с маской 255.255.255.0. Для получения клиентами локальной сети доступа к Internet на маршрутизаторе включен сервис Source NAT.

Политики зон безопасности настроены следующим образом:

Таблица 59 – Описание политик зон безопасности

Зона, из которой идет трафик	Зона, в которую идет трафик	Тип трафика	Действие
Trusted	Untrusted	TCP, UDP, ICMP	разрешен
Trusted	Trusted	TCP, UDP, ICMP	разрешен
Trusted	self	TCP/22 (SSH), ICMP, UDP/67 (DHCP Server), UDP/123 (NTP)	разрешен
Untrusted	self	UDP/68 (DHCP Client)	разрешен

Для обеспечения возможности конфигурирования устройства при первом включении в конфигурации маршрутизатора создана учётная запись администратора "admin" с паролем "password".
Пользователю будет предложено изменить пароль администратора при начальном конфигурировании маршрутизатора.

Для сетевого доступа к управлению маршрутизатором при первом включении в конфигурации задан статический IP-адрес на интерфейсе Bridge 1 – 192.168.1.1/24.

6.2 Подключение и конфигурирование устройства

Маршрутизаторы серии ESR и контроллер беспроводного доступа WLC предназначены для выполнения функций пограничного шлюза и обеспечения безопасности сети пользователя при подключении ее к публичным сетям передачи данных.

Базовая настройка данных устройств должна включать:

- назначение IP-адресов (статических или динамических) интерфейсам, участвующим в маршрутизации данных;
- создание зон безопасности и распределение интерфейсов по зонам;
- создание политик, регулирующих прохождение данных между зонами;
- настройка сервисов, сопутствующих маршрутизации данных (NAT, Firewall и прочие).

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

6.2.1 Подключение к устройству

Предусмотрены следующие способы подключения к устройству:

Подключение по локальной сети Ethernet

> ⚠ **При первоначальном старте устройство загружается с заводской конфигурацией. Описание заводской конфигурации приведено в разделе** Заводская конфигурация устройств **данного руководства.**

Подключите сетевой кабель передачи данных (патч-корд) к любому порту, входящему в зону «***Trusted***», и к компьютеру, предназначенному для управления.

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.

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
```

6.2.2 Применение изменения конфигурации

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

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

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

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

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

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

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

6.2.3 Базовая настройка устройств

Процедура настройки устройств при первом включении состоит из следующих этапов:

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

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:

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

Создание новых пользователей

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

```
esr(config)# username <name>
esr(config-user)# password <password>
esr(config-user)# privilege <privilege>
esr(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**:

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

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

Назначение имени устройства

Для назначения имени устройства используются следующие команды:

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

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

Настройка параметров публичной сети

Для настройки сетевого интерфейса маршрутизатора или контроллера 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 саб-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.

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

Для того чтобы убедиться, что адрес был назначен интерфейсу, после применения конфигурации введите следующую команду:

```
esr# show ip interfaces
IP address            Interface                          Type
-------------------   --------------------------------   -------
192.168.16.144/24     gigabitethernet 1/0/2.150          static
```

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**:

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

Для того чтобы убедиться, что адрес был назначен интерфейсу, введите следующую команду после применения конфигурации:

```
esr# show ip interfaces
IP address            Interface                          Type
-------------------   --------------------------------   -------
192.168.11.5/25       gigabitethernet 1/0/10             DHCP
```

Настройка удаленного доступа к устройству

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

При конфигурировании доступа к маршрутизатору или контроллеру правила создаются для пары зон:

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

Для создания разрешающего правила используются следующие команды:

```
esr# configure
esr(config)# security zone-pair <source-zone> self
esr(config-zone-pair)# rule <number>
esr(config-zone-rule)# action permit
esr(config-zone-rule)# match protocol tcp
esr(config-zone-rule)# match source-address <network object-group>
esr(config-zone-rule)# match destination-address <network object-group>
esr(config-zone-rule)# match destination-port <service object-group>
esr(config-zone-rule)# enable
esr(config-zone-rule)# exit
esr(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 или контроллеру с IP-адресом **40.13.1.22** по протоколу SSH:

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

7 Обновление программного обеспечения

- Обновление программного обеспечения средствами системы
- Обновление программного обеспечения из начального загрузчика
- Обновление вторичного загрузчика (U-Boot)

7.1 Обновление программного обеспечения средствами системы

Для обновления программного обеспечения понадобится один из следующих серверов: TFTP, FTP, SCP. На сервер должны быть помещены файлы программного обеспечения устройства, полученные от производителя.
На устройстве хранится две копии программного обеспечения. Для обеспечения надежности процедуры обновления программного обеспечения доступна для обновления только копия, которая не была использована для последнего старта устройства.

При обновлении программного обеспечения конфигурация маршрутизатора или контроллера конвертируется в соответствии с новой версией.
При загрузке маршрутизатора или контроллера с более старой версией программного обеспечения, чем загруженная ранее, конфигурация не конвертируется и впоследствии удаляется.

Обновление ПО с более ранних версий можно произвести, воспользовавшись инструкцией, приведенной в разделе Обновление программного обеспечения из начального загрузчика**.**

Обновление программного обеспечения на устройстве, работающем под управлением операционной системы, выполняется в следующем порядке.

1. Подготовьте для работы выбранный сервер. Должен быть известен адрес сервера, на сервере должен быть размещен дистрибутивный файл программного обеспечения.
2. Маршрутизатор/контроллер должен быть подготовлен к работе в соответствии с требованиями документации. Конфигурация маршрутизатора/контроллера должна позволять обмениваться данными по протоколам TFTP/FTP/SCP и ICMP с сервером. При этом должна быть учтена принадлежность сервера к зонам безопасности маршрутизатора/контроллера.
3. Подключитесь к маршрутизатору/контроллеру локально через консольный порт Console или удаленно, используя проколы Telnet или SSH.
   Проверьте доступность сервера для маршрутизатора/контроллера, используя команду *ping*. Если сервер не доступен – проверьте правильность настроек маршрутизатора/контроллера и состояние сетевых интерфейсов сервера.
4. Для обновления программного обеспечения устройства введите следующую команду. В качестве параметра *<server>* должен быть указан IP-адрес используемого сервера. Для обновления с FTP или SCP-сервера потребуется ввести имя пользователя (параметр *<user>*) и пароль (параметр *<password>*). В качестве параметра *<file_name>* укажите имя файла программного обеспечения, помещенного на сервер (при использовании SCP нужно указать полный путь – параметр *<folder>*). После ввода команды устройство скопирует файл во внутреннюю память, проверит целостность данных и сохранит его в энергонезависимую память устройства.
   TFTP:

```
esr# copy tftp://<server>:/<file_name> system:firmware
```

FTP:

```
esr# copy ftp://[<user>[:<password>]@]<server>:/<file_name> system:firmware
```

SCP:

```
esr# copy scp://[<user>[:<password>]@]<server>://<folder>/<file_name>system:firmware
```

SFTP:

```
esr# copy sftp://[<user>[:<password>]@]<server>:/<file_name> system:firmware
```

Для примера обновите основное ПО через SCP:

```
esr# copy scp://adm:password123@192.168.16.168://home/tftp/firmware system:firmware
```

5. Для того чтобы устройство работало под управлением новой версии программного обеспечения, необходимо произвести переключение активного образа. С помощью команды *show bootvar* следует выяснить номер образа, содержащего обновленное ПО.

```
esr# show bootvar
Image   Version                      Date                   Status         After reboot
-----  --------------               --------------------    ------------   ------------
1       1.0.7 build 141[f812808]     date 18/02/2015 time    Active         *
                                     16:12:54

2       1.0.7 build 141[f812808]     date 18/02/2015 time   Not Active
                                     16:12:54
```

Для выбора образа используйте команду:

```
esr# boot system image-[1|2]
```

6. Для обновления вторичного загрузчика (U-Boot) введите следующую команду. В качестве параметра *<server>* должен быть указан IP-адрес используемого сервера. Для обновления с FTP или SCP-сервера потребуется ввести имя пользователя (параметр *<user>*) и пароль (параметр *<password>*). В качестве параметра *<file_name>* укажите имя файла вторичного загрузчика, помещенного на сервер (при использовании SCP нужно указать полный путь – параметр *<folder>*). После ввода команды маршрутизатор скопирует файл во внутреннюю память, проверит целостность данных и сохранит его в энергонезависимую память устройства.
TFTP:

```
esr# copy tftp://<server>:/<file_name> system:boot-2
```

FTP:

```
esr# copy ftp://<server>:/<file_name> system:boot-2
```

SCP:

```
esr# copy scp://[<user>[:<password>]@]<server>://<folder>/<file_name>system:boot-2
```

SFTP:

```
esr# copy sftp://<server>:/<file_name> system:boot-2
```

7.2 Обновление программного обеспечения из начального загрузчика

Программное обеспечение маршрутизатора/контроллера можно обновить из начального загрузчика следующим образом:

1. Остановите загрузку устройства после окончания инициализации устройства загрузчиком U-Boot, нажав клавишу ***<Esc>***.

```
Configuring PoE...
distribution 1 dest_threshold 0xa drop_timer 0x0
Configuring POE in bypass mode
NAE configuration done!
initializing port 0, type 2.
initializing port 1, type 2.
SMC Endian Test:b81fb81f
nae-0, nae-1
  =======Skip: Load SYS UCORE for old 8xxB1/3xxB0 revision on default.
Hit any key to stop autoboot:  2
```

2. Укажите IP-адрес TFTP-сервера:

```
BRCM.XLP316Lite Rev B0.u-boot# serverip 10.100.100.1
```

Для версии 1.5 и выше:

```
BRCM.XLP316Lite Rev B0.u-boot# serverip 10.100.100.1
```

3. Укажите IP-адрес маршрутизатора/контроллера:

```
BRCM.XLP316Lite Rev B0.u-boot# ipaddr 10.100.100.2
```

Для версии 1.5 и выше:

```
BRCM.XLP316Lite Rev B0.u-boot# ipaddr 10.100.100.2
```

4. Укажите имя файла программного обеспечения на TFTP-сервере:

```
BRCM.XLP316Lite Rev B0.u-boot# firmware_file firmware
```

Для версии 1.5 и выше:

```
BRCM.XLP316Lite Rev B0.u-boot# firmware_file firmware
```

5. Можно сохранить окружение командой «saveenv» для будущих обновлений.

6. Запустите процедуру обновления программного обеспечения:

```
BRCM.XLP316Lite Rev B0.u-boot# run tftp_update_image1
Using nae-0-3 device
TFTP from server 10.100.100.1; our IP address is 10.100.100.2
Filename 'esr1000/firmware'.
Load address: 0xa800000060000000
Loading: TftpStart:TftpTimeoutMsecs = 10000, TftpTimeoutCountMax = 6
#################################################################
#################################################################
#################################################################
########################
##################################
done
Bytes transferred = 64453909 (3d77d15 hex)
Device 0: MT29F8G08ABBCAH4 ... is now current device

NAND erase: device 0 offset 0x1440000, size 0x6400000
Bad block table found at page 262080, version 0x01
Bad block table found at page 262016, version 0x01
Erasing at 0x7800000 -- 1895825408% complete..
OK

NAND write: device 0 offset 0x1440000, size 0x6400000
104857600 bytes written: OK
```

7. Установите загруженное программное обеспечение в качестве образа для запуска системы и перезагрузите роутер:

```
BRCM.XLP316Lite Rev B0.u-boot# run set_bootpart_1
```

Для версии 1.5 и выше:

```
BRCM.XLP316Lite Rev B0.u-boot# boot_system image1
BRCM.XLP316Lite Rev B0.u-boot# reset
```

7.3 Обновление вторичного загрузчика (U-Boot)

Вторичный загрузчик занимается инициализацией NAND и маршрутизатора/контроллера. При обновлении новый файл вторичного загрузчика сохраняется на flash на месте старого.

Для просмотра текущей версии загрузочного файла, работающего на устройстве, введите команду «version» в CLI U-Boot, также версия отображается в процессе загрузки устройства:

```
BRCM.XLP316Lite Rev B0.u-boot# version
BRCM.XLP.U-Boot:1.1.0.47 (29/11/2016 - 19:00:24)
```

Процедура обновления ПО:

1. Остановите загрузку устройства после окончания инициализации устройства загрузчиком U-Boot, нажав клавишу ***<Esc>***.

```
Configuring PoE...
distribution 1 dest_threshold 0xa drop_timer 0x0
Configuring POE in bypass mode
NAE configuration done!
initializing port 0, type 2.
initializing port 1, type 2.
SMC Endian Test:b81fb81f
nae-0, nae-1
  =======Skip: Load SYS UCORE for old 8xxB1/3xxB0 revision on default.
Hit any key to stop autoboot:  2
```

2. Укажите IP-адрес TFTP-сервера:

```
BRCM.XLP316Lite Rev B0.u-boot# setenv serverip 10.100.100.1
```

   Для версии 1.5 и выше:

```
BRCM.XLP316Lite Rev B0.u-boot# serverip10.100.100.2
```

3. Укажите IP-адрес маршрутизатора:

```
BRCM.XLP316Lite Rev B0.u-boot# setenv ipaddr 10.100.100.2
```

   Для версии 1.5 и выше:

```
BRCM.XLP316Lite Rev B0.u-boot# ipaddr 10.100.100.2
```

4. Укажите имя файла загрузчика на TFTP-сервере:

```
BRCM.XLP316Lite Rev B0.u-boot# uboot_file u-boot.bin
```

   Для версии 1.5 и выше:

```
BRCM.XLP316Lite Rev B0.u-boot# uboot_file u-boot.bin
```

5. Можно сохранить окружение командой «saveenv» для будущих обновлений.
6. Запустите процедуру обновления программного обеспечения:

```
BRCM.XLP316Lite Rev B0.u-boot# run upd_uboot
```

Для версии 1.5 и выше:

```
BRCM.XLP316LiteRevB0.u-boot# run tftp_update_uboot
Using nae-1 device
TFTP from server 10.100.100.1; our IP address is 10.100.100.2
Filename 'esr1000/u-boot.bin'.
Load address: 0xa800000078020000
Loading: #################################################################
done
Bytes transferred = 852648 (d02a8 hex)
SF: Detected MX25L12805D with page size 256, total 16777216 bytes
16384 KiB MX25L12805D at 0:0 is now current device
```

7. Перезагрузите устройство:

```
BRCM.XLP316Lite Rev B0.u-boot# reset
```

8 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
- Настройка механизмов защиты от сетевых атак
  - 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.

8.1 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.

8.2 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.

8.2.1 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.
- Рекомендуется включать добавление меток timestamp msec к syslog-сообщениям на устройствах ESR-1500 и ESR-1511.

8.2.2 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 устройства.

8.2.3 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:

```
esr(config)# syslog file tmpsys:syslog/default info
```

Настраиваем ограничение размера и ротацию файлов:

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

Настраиваем передачу сообщений на внешний сервер:

```
esr(config)# syslog host mylog 192.168.1.2 info udp 514
```

Включаем нумерацию сообщений syslog:

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

8.3 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.

8.3.1 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.

8.3.2 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:

```
esr(config)# security passwords default-expered
```

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

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

Устанавливаем ограничения на длину пароля:

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

Устанавливаем ограничения по минимальному количеству символов соответствующих типов:

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

8.4 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.

8.4.1 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.

8.4.2 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** перестаёт 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.

8.4.3 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:

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

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

Задаём локальный ENABLE-пароль:

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

Понижаем привилегии пользователя admin:

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

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

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

Настраиваем политику AAA:

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

Настраиваем логирование:

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

8.5 Настройка удалённого управления

Подробная информация о командах настройки удалённого доступа приведена в разделе Настройка доступа SSH, Telnet справочника команд CLI.

8.5.1 Рекомендации

- Рекомендуется отключить 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 перегенерировать ключи шифрования.

8.5.2 Пример настройки

Задача:

Отключить протокол telnet. Сгенерировать новые ключи шифрования. Использовать криптостойкие алгоритмы.

Решение:

Отключаем удаленное управление по протоколу telnet:

```
esr(config)# no ip telnet server
```

Отключаем устаревшие и не криптостойкие алгоритмы:

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

Генерируем новые ключи шифрования:

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

8.6 Настройка механизмов защиты от сетевых атак

Алгоритмы настройки механизмов защиты от сетевых атак приведены в разделе Настройка логирования и защиты от сетевых настоящего руководства.

Подробная информация о командах для настройки политики использования паролей приведена в разделе Управление логированием и защитой от сетевых атак справочника команд CLI.

8.6.1 Рекомендации

- Рекомендуется всегда включать защиту от ip spoofing.
- Рекомендуется всегда включать защиту от TCP-пакетов с неправильно выставленными флагами.
- Рекомендуется всегда включать защиту от фрагментированных TCP-пакетов с выставленным флагом SYN.
- Рекомендуется всегда включать защиту от фрагментированных ICMP-пакетов.
- Рекомендуется всегда включать защиту ICMP-пакетов большого размера.
- Рекомендуется всегда включать защиту от незарегистрированных ip-протоколов.
- Рекомендуется включать логирование механизма защиты от сетевых атак.

8.6.2 Пример настройки

Задача:

Настроить механизм защиты от сетевых атак в соответствии с рекомендациями.

Решение:

Включаем защиту от ip spoofing и логирование механизма защиты:

```
esr(config)# ip firewall screen spy-blocking spoofing
esr(config)# logging firewall screen spy-blocking spoofing
```

Включаем защиту от TCP-пакетов с неправильно выставленными флагами и логирование механизма защиты:

```
esr(config)# ip firewall screen spy-blocking syn-fin
esr(config)# logging firewall screen spy-blocking syn-fin
esr(config)# ip firewall screen spy-blocking fin-no-ack
esr(config)# logging firewall screen spy-blocking fin-no-ack
esr(config)# ip firewall screen spy-blocking tcp-no-flag
esr(config)# logging firewall screen spy-blocking tcp-no-flag
esr(config)# ip firewall screen spy-blocking tcp-all-flags
esr(config)# logging firewall screen spy-blocking tcp-all-flags
```

Включаем защиту от фрагментированных ICMP-пакетов и логирование механизма защиты:

```
esr(config)# ip firewall screen suspicious-packets icmp-fragment
esr(config)# logging firewall screen suspicious-packets icmp-fragment
```

Включаем защиту от ICMP-пакетов большого размера и логирование механизма защиты:

```
esr(config)# ip firewall screen suspicious-packets large-icmp
esr(config)# logging firewall screen suspicious-packets large-icmp
```

Включаем защиту от незарегистрированных IP-протоколов и логирование механизма защиты:

```
esr(config)# ip firewall screen suspicious-packets unknown-protocols
esr(config)# logging firewall screen suspicious-packets unknown-protocols
```

9 Управление контроллером WLC-30

- Настройка WLC
  - Алгоритм настройки
  - Пример настройки
    - Задача
    - Решение
      - Настройка интерфейсов, сетевых параметров и firewall
      - Настройка DHCP-сервера
      - Настройка RADIUS-сервера
      - Настройка модуля управления точками доступа WLC
        - Настройка SSID
        - Настройка профилей конфигурации
        - Настройка локации
        - Определение подсетей обслуживаемых точек доступа
        - Авторегистрация точек доступа
        - Включение функционала WLC
      - Обновление точек доступа
- Настройка AirTune
  - Описание
  - Алгоритм работы
  - Алгоритм настройки
  - Пример настройки

9.1 Настройка WLC

9.1.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Настроить локальный RADIUS-сервер и перейти в режим его конфигурирования.	**wlc(config)# radius-server local** **wlc(config-radius)#**	
2	Активировать работу локального RADIUS-сервера.	**wlc(config-radius)# enable**	
3	Добавить NAS и перейти в режим его конфигурирования.	**wlc(config-radius)# nas <NAME>** **wlc(config-radius-nas)#**	<NAME> – название NAS, задается строкой до 235 символов.
4	Задать ключ аутентификации.	**wlc(config-radius-nas)# key ascii-text { <KEY> | encrypted <ENCRYPTED-KEY> }**	<KEY> – строка из [4..64] ASCII-символов; <ENCRYPTED-KEY> – зашифрованный ключ, задаётся строкой [8..128] символов.

Шаг	Описание	Команда	Ключи
5	Указать сеть.	**wlc(config-radius-nas)# network <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].
6	Создать домен.	**wlc(config-radius)# domain <NAME>**	<NAME> – идентификатор домена, задается строкой до 235 символов.
7	Добавить виртуальный RADIUS-сервер и перейти в режим его конфигурирования.	**wlc(config-radius)# virtual-server <NAME>** **wlc(config-radius-vserver)#**	<NAME> – название виртуального RADIUS-сервера, задается строкой до 235 символов.
8	Активировать работу виртуального RADIUS-сервера.	**wlc(config-radius-vserver)# enable**	
9	Добавить RADIUS-сервер в список используемых серверов и перейти в режим его конфигурирования.	**wlc(config)# radius-server host { <IP-ADDR> | <IPV6-ADDR> } [vrf <VRF>]** **wlc(config-radius-server)#**	<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::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF] <VRF> – имя экземпляра VRF, задается строкой до 31 символа.
10	Задать ключ аутентификации.	**wlc(config-radius-server)# key ascii-text { <KEY> | encrypted <ENCRYPTED-KEY> }**	<KEY> – строка из [4..64] ASCII-символов; <ENCRYPTED-KEY> – зашифрованный ключ, задаётся строкой [8..128] символов.
11	Создать профиль AAA и перейти в режим его конфигурирования.	**wlc(config)# aaa radius-profile <NAME>** **wlc(config-aaa-radius-profile)#**	<NAME> – имя профиля сервера, задается строкой до 31 символа.

Шаг	Описание	Команда	Ключи
12	В профиле AAA указать RADIUS-сервер.	**wlc(config-aaa-radius-profile)# radius-server host { <IP-ADDR> | <IPV6-ADDR> }**	<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::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
13	Перейти в настройки конфигурирования контроллера Wi-Fi.	**wlc(config)# softgre-controller** **wlc(config-softgre)#**	
14	Определить IP-адрес маршрутизатора, который будет использоваться в качестве IP-адреса источника в отправляемых RADIUS-пакетах.	**wlc(config-softgre)# nas-ip-address <ADDR>**	<ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
15	Установить режим конфигурации SoftGRE DATA туннелей.	**wlc(config-softgre)# data-tunnel configuration { local | radius | wlc}**	local – режим конфигурации, при котором параметры SoftGRE DATA туннелей получаются из локальной конфигурации маршрутизатора; radius – режим, при котором параметры SoftGRE DATA туннелей запрашиваются у RADIUS-сервера; wlc – режим, при котором параметры SoftGRE DATA туннелей запрашиваются у WLC.
16	Указать профиль AAA.	**wlc(config-softgre)# aaa radius-profile <NAME>**	<NAME> – имя профиля сервера, задается строкой до 31 символа.
17	Отключить обмен ICMP-сообщениями, которые используются для проверки доступности удаленного шлюза туннелей Wi-Fi контроллера.	**wlc(config-softgre)# keepalive-disable**	
18	Активировать работу контроллера Wi-Fi.	**wlc(config-softgre)# enable**	
19	Перейти в раздел конфигурирования контроллера.	**wlc(config)# wlc** **wlc(config)#**	

Шаг	Описание	Команда	Ключи
20	Создать профиль конфигурирования общих настроек точки доступа.	**wlc(config-wlc)# ap-profile <NAME>** **wlc(config-wlc-ap-profile)#**	<NAME> – название профиля, задается строкой до 235 символов.
21	Задать пароль для подключения к точкам доступа.	**wlc(config-wlc-ap-profile)# password ascii-text { <CLEAR-TEXT> | encrypted <HASH_SHA512> }** **wlc(config-wlc-ap-profile)# exit**	<CLEAR-TEXT> – пароль, задаётся строкой [8-64] символов. <HASH_SHA512> – хеш пароля по алгоритму sha512, задаётся строкой [16-128] символов.
22	Создать профиль конфигурирования для точки доступа конкретного типа.	**wlc(config-wlc)# board-profile <NAME>** **wlc(config-wlc-board-profile)#**	<NAME> – название профиля, задается строкой до 235 символов.
23	Указать тип точки доступа, для которой производится конфигурирование.	**wlc(config-wlc-board-profile)# ap-model <BOARD-TYPE>**	<BOARD-TYPE> – тип точки доступа, доступные значения: • WEP-1L; • WEP-2L; • WEP-3ax; • WOP-2L; • WOP-20L; • WEP-30L.
24	Перейти в настройки конфигурирования радиоинтерфейса.	**wlc(config-wlc-board-profile)# radio <WLAN>** **wlc(config-wlc-board-profile-radio)#**	<WLAN> – радиоинтерфейс, доступные значения: • wlan0 – диапазон 2g; • wlan1 – диапазон 5g.
25	Указать частотный диапазон, в котором работает радиоинтерфейс.	**wlc(config-wlc-board-profile-radio)# band <BAND>**	<BAND> – диапазон частот, доступны значения: • 2g; • 5g.
26	Установить режим работы радиоинтерфейса.	**wlc(config-wlc-board-profile-radio)# work-mode <WORK-MODE>**	<WORK-MODE> – режим работы, доступные значения: WEP-3ax, WEP-30L: • bgn, ax, bgnax – для диапазона 2g; • anac, anacax, a – для диапазона 5g; WEP-1L, WEP-2L, WOP-2L, WOP-20L: • n, bg, bgn – для диапазона 2g; • a, an, ac – для диапазона 5g.

Шаг	Описание	Команда	Ключи
27	Задать список каналов для динамического выбора канала.	**wlc(config-wlc-board-profile-radio)# limit-channels <CHANNEL> <CHANNEL> <CHANNEL>**	<CHANNEL> – номер используемого канала, доступные значения: Для 2g каналы из диапазона: [1.. 13] Для 5g каждый 4 канал из диапазонов: [36.. 64] [100.. 144] [149.. 165]
28	Включить использование созданного списка.	**wlc(config-wlc-board-profile-radio)# use-limit-channels**	
29	Активировать функцию динамического выбора канала.	**wlcconfig-wlc-board-profile-radio)# autochannel**	
30	Настроить ширину канала.	**wlcconfig-wlc-board-profile-radio)# bandwidth <BANDWIDTH>**	<BANDWIDTH> – ширина канала, доступны значения: • 20; • 40L; • 40U; • 80; • 160.
31	Настроить уровень мощности для радиоинтерфейса.	**wlc(config-wlc-board-profile-radio)# tx-power <TX-POWER>**	<TX-POWER> – уровень мощности в дБм, принимает значения в диапазоне [6.. 19].
32	Создать профиль конфигурирования RADIUS-сервера.	**wlc(config-wlc)# radius-profile <RADIUS-ID>** **wlc(config-wlc-radius-profile)#**	<RADIUS-ID> – идентификатор RADIUS-сервера, задается строкой до 235 символов.
33	Указать IP-адрес RADIUS-сервера, который отвечает за аутентификацию.	**wlc(config-wlc-radius-profile)# auth-address <ADDR>**	<ADDR> – IP-адрес RADIUS-сервера, задаётся в виде: AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
34	Указать пароль RADIUS-сервера, который отвечает за аутентификацию.	**wlc(config-wlc-radius-profile)# auth-password ascii-text { <CLEAR-TEXT> | encrypted <HASH_SHA512> }**	<CLEAR-TEXT> – пароль, задаётся строкой [8-64] символа. <HASH_SHA512> – хеш пароля по алгоритму sha512, задаётся строкой [16-128] символов.
35	Указать домен.	**wlc(config-wlc-radius-profile)# domain <NAME>**	<NAME> – идентификатор домена, задается строкой до 235 символов.

Шаг	Описание	Команда	Ключи
36	Создать профиль конфигурирования SSID.	**wlc(config-wlc)# ssid-profile <NAME>** **wlc(config-wlc-ssid-profile)#**	<NAME> – название профиля SSID, задается строкой до 235 символов.
37	Задать описание профиля.	**wlc(config-wlc-ssid-profile)# description <DESCRIPTION>**	<DESCRIPTION> – произвольное описание, задается строкой до 255 символов.
38	Настроить частотный диапазон, в котором будет происходить вещание SSID.	**wlc(config-wlc-ssid-profile)# band <BAND>**	<BAND> – диапазон частот, доступные значения: • 2g; • 5g.
39	Указать пользовательский vlan.	**wlc(config-wlc-ssid-profile)# vlan-id <ID>**	<ID> – идентификатор vlan, принимает значения в диапазоне [0-4094].
40	Установить режим безопасности подключения к SSID.	**wlc(config-wlc-ssid-profile)# security-mode <MODE>**	<MODE> – режим безопасности, доступные значения: • WPA; • WPA2; • WPA2_1X; • WPA3; • WPA_1X; • WPA_WPA2; • WPA_WPA2_1X; • off.
41	Указать профиль RADIUS-сервера.	**wlc(config-wlc-ssid-profile)# radius-profile <RADIUS-ID>**	<RADIUS-ID> – идентификатор RADIUS-сервера, задается строкой до 235 символов.
42	Задать название SSID, который будет вещаться пользователям.	**wlc(config-wlc-ssid-profile)# ssid <NAME>**	<NAME> – название SSID, задается строкой до 32 символов. Названия, содержащие пробел, необходимо заключать в кавычки.
43	Активировать работу SSID.	**wlc(config-wlc-ssid-profile)# enable**	
44	Создать профиль локации.	**wlc(config-wlc)# ap-location <NAME>** **wlc(config-wlc-ap-location)#**	<NAME> – название профиля локального конфигурирования, задается строкой до 235 символов.
45	Задать описание профиля.	**wlc(config-wlc-ap-location)# description <DESCRIPTION>**	<DESCRIPTION> – произвольное описание, задается строкой до 255 символов.

Шаг	Описание	Команда	Ключи
46	Указать для точек доступа существующий профиль настроек.	**wlc(config-wlc-ap-location)# board-profile <BOARD-TYPE> <PROFILE-ID>**	<BOARD-TYPE> – тип точки доступа, доступные значения: • WEP-1L; • WEP-2L; • WEP-3ax; • WOP-2L; • WOP-20L; • WEP-30L. <PROFILE-ID> – идентификатор профиля, задается строкой до 235 символов, и должен совпадать с названием описанного профиля из board-profile.
47	Указать для точек доступа существующий профиль общих настроек.	**wlc(config-wlc-ap-location)# ap-profile <PROFILE-ID>**	<PROFILE-ID> – идентификатор профиля, задается строкой до 235 символов, и должен совпадать с названием описанного профиля из ap-profile.
48	Указать профиль SSID, который будет назначен точкам доступа.	**wlc(config-wlc-ap-location)# ssid-profile <NAME> <LOCATION>**	<NAME> – название профиля SSID, задается строкой до 235 символов. <LOCATION> – bridge location, используется для построения SoftGRE DATA туннеля, должен совпадать с location, указанным в конфигурации бриджа для пользовательского трафика, задается строкой до 220 символов. При использовании схемы L2 параметр не задается.
49	Создать адресное пространство для доступа к контроллеру.	**wlc(config-wlc)# ip-pool <NAME>** **wlc(config-wlc-ip-pool)#**	<NAME> – название адресного пространства, задается строкой до 235 символов.
50	Задать описание адресного пространства.	**wlc(config-wlc-ip-pool)# description <DESCRIPTION>**	<DESCRIPTION> – произвольное описание, задается строкой до 255 символов.
51	Указать название профиля локации, который применяется к заданному адресному пространству.	**wlc(config-wlc-ip-pool)# ap-location <NAME>**	<NAME> – название локации, задается строкой до 235 символов.

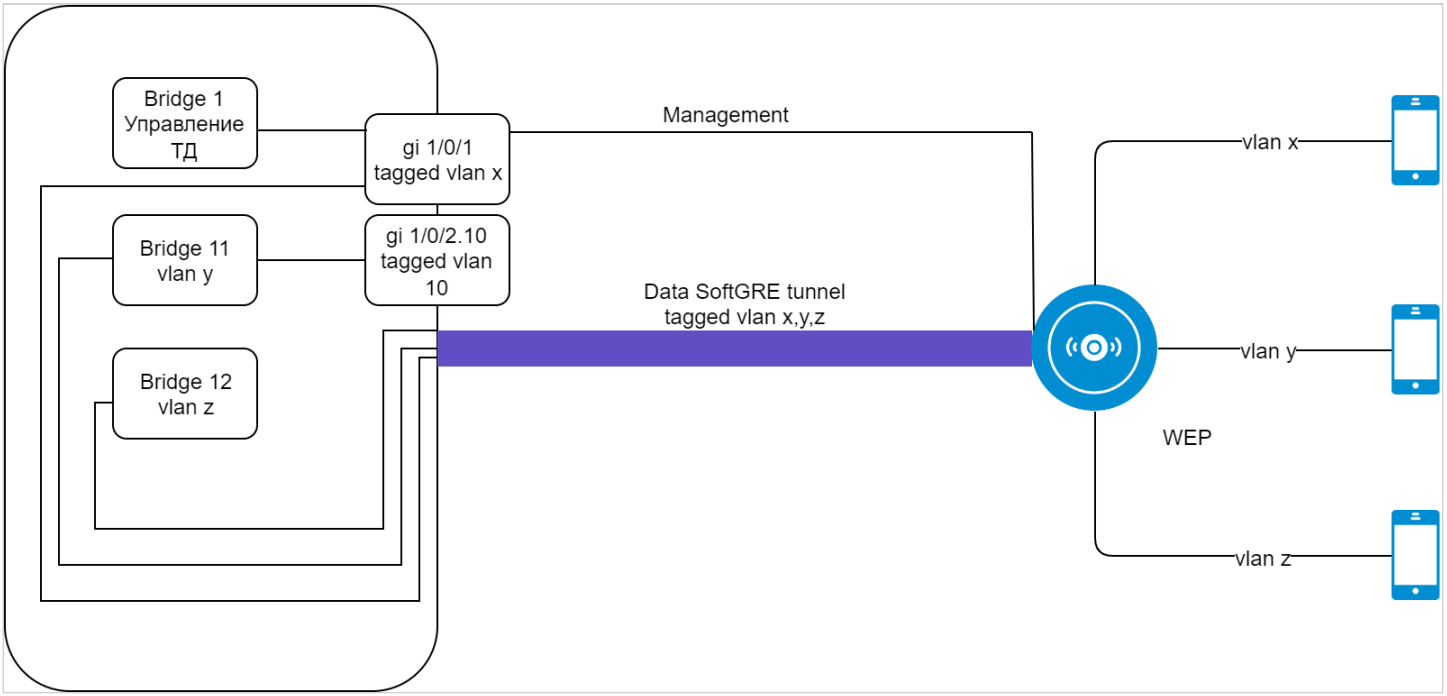
Шаг	Описание	Команда	Ключи
52	Перейти в настройки сервис-активатора.	**wlc(config-wlc)# service-activator** **wlc(config-wlc-service-activator)#**	
53	Настроить автоматическую регистрацию точек доступа на контроллере.	**wlc(config-wlc-service-activator)# aps join auto**	
54	Активировать работу контроллера.	**wlc(config-wlc)# enable**	

9.1.2 Пример настройки

Задача

Организовать управление беспроводными точками доступа с помощью контроллера WLC-30. В частности, необходимо настроить подключение точек доступа, обновить и сконфигурировать их для предоставления доступа до ресурсов Интернет авторизованным пользователям Wi-Fi.

Пример настройки приведен на основе заводской конфигурации для схемы с построением SoftGRE-туннелей.



Решение

Архитектура решения предполагает автоматическое подключение точек доступа к контроллеру WLC-30. При подключении к сети точка доступа запрашивает адрес по DHCP и вместе с ним должна получить URL сервиса инициализации точек доступа в 43 (vendor specific) опции DHCP.

Получив данную опцию, точка доступа приходит на контроллер и появляется в базе обслуживаемых точек доступа (команда для мониторинга списка: show wlc ap). Далее контроллер инициализирует ее в соответствии со своей конфигурацией:

1. Выполняет обновление, если версия ПО на точке доступа не соответствует версии, которая размещена на контроллере.
2. Устанавливает пароль доступа.
3. Выполняет конфигурирование в соответствии с настройками для данной локации (ap-location): выбранным профилем конфигурации для данного типа точек доступа и SSID.

Точки доступа могут быть подключены к контроллеру WLC-30 через L2- или L3-сеть предприятия.

Выделение и настройка VLAN при подключении новых точек доступа может оказаться трудоемкой задачей, особенно если на сети предприятия между точками доступа и контроллером используется большое количество коммутаторов. Поэтому заводская конфигурация WLC-30 предполагает построение SoftGRE DATA туннелей для передачи пользовательского трафика. Такое решение даже в L2-сети позволяет упростить подключение точек доступа, так как отсутствует необходимость прокидывать VLAN для каждого SSID через все коммутаторы.

При организации связи в L3-сети необходимо обеспечить настройку DHCP-relay на оборудовании сети предприятия для перенаправления DHCP-запросов точек доступа на WLC-30, где настроен пул IP-адресов для управления точками доступа, а также выдача 43 опции 15 подопции DHCP, содержащая URL контроллера.

Последовательность настройки контроллера беспроводных сетей WLC-30:

1. Настройка интерфейсов, сетевых параметров и firewall.
2. Настройка контроллера для организации SoftGRE DATA туннелей.
3. Настройка DHCP-сервера.
4. Настройка RADIUS-сервера.
5. Настройка модуля управления точками доступа WLC:
    - Настройка SSID.
    - Настройка профилей конфигурации для каждого типа точек доступа.
    - Создание локации (ap-location) и определение правил конфигурирования точек доступа, входящих в данную локацию.
    - Определение подсетей обслуживаемых точек доступа.
6. Настройка обновления точек доступа.

Настройка интерфейсов, сетевых параметров и firewall

Настроим профили TCP/UDP-портов для необходимых сервисов:

```
wlc-30# configure

wlc-30(config)# object-group service ssh
wlc-30(config-object-group-service)# port-range 22
wlc-30(config-object-group-service)# exit

wlc-30(config)# object-group service dns
wlc-30(config-object-group-service)# port-range 53
wlc-30(config-object-group-service)# exit

wlc-30(config)# object-group service dhcp_server
wlc-30(config-object-group-service)# port-range 67
wlc-30(config-object-group-service)# exit

wlc-30(config)# object-group service dhcp_client
wlc-30(config-object-group-service)# port-range 68
wlc-30(config-object-group-service)# exit

wlc-30(config)# object-group service ntp
wlc-30(config-object-group-service)# port-range 123
wlc-30(config-object-group-service)# exit

wlc-30(config)# object-group service netconf
wlc-30(config-object-group-service)# port-range 830
wlc-30(config-object-group-service)# exit

wlc-30(config)# object-group service radius_auth
wlc-30(config-object-group-service)# port-range 1812
wlc-30(config-object-group-service)# exit

wlc-30(config)# object-group service sa
wlc-30(config-object-group-service)# port-range 8043
wlc-30(config-object-group-service)# exit

wlc-30(config)# object-group service airtune
wlc-30(config-object-group-service)# port-range 8099
wlc-30(config-object-group-service)# exit
```

Создаём три зоны безопасности — зона пользователей (users), доверенная зона для точек доступа (trusted) и недоверенная зона для выхода в Интернет (untrusted):

```
wlc-30(config)# security zone users
wlc-30(config-zone)# exit

wlc-30(config)# security zone trusted
wlc-30(config-zone)# exit

wlc-30(config)# security zone untrusted
wlc-30(config-zone)# exit
```

Настраиваем правила firewall:

```
wlc-30(config)# security zone-pair trusted untrusted
wlc-30(config-zone-pair)# rule 1
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair)# exit
wlc-30(config)# security zone-pair trusted trusted
wlc-30(config-zone-pair)# rule 1
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair)# exit
wlc-30(config)# security zone-pair trusted self
wlc-30(config-zone-pair)# rule 10
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# match protocol tcp
wlc-30(config-zone-pair-rule)# match destination-port ssh
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair)# rule 20
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# match protocol icmp
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair)# rule 30
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# match protocol udp
wlc-30(config-zone-pair-rule)# match source-port dhcp_client
wlc-30(config-zone-pair-rule)# match destination-port dhcp_server
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair)# rule 40
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# match protocol udp
wlc-30(config-zone-pair-rule)# match destination-port ntp
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair)# rule 50
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# match protocol tcp
wlc-30(config-zone-pair-rule)# match destination-port dns
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair)# rule 60
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# match protocol udp
wlc-30(config-zone-pair-rule)# match destination-port dns
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair)# rule 70
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# match protocol tcp
wlc-30(config-zone-pair-rule)# match destination-port netconf
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
```

```
wlc-30(config-zone-pair)# rule 80
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# match protocol tcp
wlc-30(config-zone-pair-rule)# match destination-port sa
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair)# rule 90
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# match protocol udp
wlc-30(config-zone-pair-rule)# match destination-port radius_auth
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair)# rule 100
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# match protocol gre
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair)# exit
wlc-30(config)# security zone-pair users self
wlc-30(config-zone-pair)# rule 10
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# match protocol icmp
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair)# rule 20
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# match protocol udp
wlc-30(config-zone-pair-rule)# match source-port dhcp_client
wlc-30(config-zone-pair-rule)# match destination-port dhcp_server
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair)# rule 30
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# match protocol tcp
wlc-30(config-zone-pair-rule)# match destination-port dns
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair)# rule 40
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# match protocol udp
wlc-30(config-zone-pair-rule)# match destination-port dns
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair)# exit
wlc-30(config)# security zone-pair untrusted self
wlc-30(config-zone-pair)# rule 1
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# match protocol udp
wlc-30(config-zone-pair-rule)# match source-port dhcp_server
wlc-30(config-zone-pair-rule)# match destination-port dhcp_client
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair)# exit
wlc-30(config)# security zone-pair users untrusted
wlc-30(config-zone-pair)# rule 1
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair)# exit
```

Настраиваем NAT:

```
wlc-30(config)# nat source
wlc-30(config-snat)# ruleset factory
wlc-30(config-snat-ruleset)# to zone untrusted
wlc-30(config-snat-ruleset)# rule 10
wlc-30(config-snat-rule)# description "replace 'source ip' by outgoing interface ip address"
wlc-30(config-snat-rule)# action source-nat interface
wlc-30(config-snat-rule)# enable
wlc-30(config-snat-rule)# exit
wlc-30(config-snat-ruleset)# exit
wlc-30(config-snat)# exit
```

Создаем VLAN для uplink:

```
wlc-30(config)# vlan 2
wlc-30(config-vlan)# exit
```

Создаем интерфейсы для взаимодействия с подсетями управления точками доступа, пользователей Wi-Fi и Интернет:

```
#Сконфигурируем параметры интерфейса для точек доступа:
wlc-30(config)# bridge 1
wlc-30(config-bridge)# vlan 1
wlc-30(config-bridge)# security-zone trusted
wlc-30(config-bridge)# ip address 192.168.1.1/24
wlc-30(config-bridge)# enable
wlc-30(config-bridge)# exit

#Сконфигурируем параметры публичного интерфейса:
wlc-30(config)# bridge 2
wlc-30(config-bridge)# vlan 2
wlc-30(config-bridge)# security-zone untrusted
wlc-30(config-bridge)# ip address dhcp
wlc-30(config-bridge)# enable
wlc-30(config-bridge)# exit

#Сконфигурируем параметры интерфейса для пользователей Wi-Fi. Параметр location необходим для
построения SoftGRE-туннелей и должен совпадать с указанным для SSID-профиля в настройках ap-
location:
wlc-30(config)# bridge 3
wlc-30(config-bridge)# security-zone users
wlc-30(config-bridge)# ip address 192.168.2.1/24
wlc-30(config-bridge)# location default
wlc-30(config-bridge)# enable
wlc-30(config-bridge)# exit
```

Настраиваем порты:

```
#Конфигурируем интерфейсы для uplink:
wlc-30(config)# interface gigabitethernet 1/0/1
wlc-30(config-if-gi)# mode switchport
wlc-30(config-if-gi)# switchport access vlan 2
wlc-30(config-if-gi)# exit
wlc-30(config)# interface tengigabitethernet 1/0/1
wlc-30(config-if-te)# mode switchport
wlc-30(config-if-te)# switchport access vlan 2
wlc-30(config-if-te)# exit
wlc-30(config)# interface tengigabitethernet 1/0/2
wlc-30(config-if-te)# mode switchport
wlc-30(config-if-te)# switchport access vlan 2
wlc-30(config-if-te)# exit

#Конфигурируем интерфейсы для подключения точек доступа:
wlc-30(config)# interface gigabitethernet 1/0/2
wlc-30(config-if-gi)# mode switchport
wlc-30(config-if-gi)# exit
wlc-30(config)# interface gigabitethernet 1/0/3
wlc-30(config-if-gi)# mode switchport
wlc-30(config-if-gi)# exit
wlc-30(config)# interface gigabitethernet 1/0/4
wlc-30(config-if-gi)# mode switchport
wlc-30(config-if-gi)# exit
```

Включаем разрешение DNS-имен:

```
wlc-30(config)# domain lookup enable
```

Настраиваем профиль для поднятия туннелей:

```
wlc-30(config)# tunnel softgre 1
wlc-30(config-softgre)# mode data
wlc-30(config-softgre)# local address 192.168.1.1
wlc-30(config-softgre)# default-profile
wlc-30(config-softgre)# enable
wlc-30(config)# exit
```

Настройка DHCP-сервера

> ⚠ Необходимо обязательно указывать NTP-сервер, т.к. корректное время позволяет пройти проверку валидности сертификатов.

Настраиваем адресное пространство для устройств, которые будут подключены к контроллеру:

```
wlc-30(config)# ip dhcp-server pool ap-pool

#Определяем подсеть:
wlc-30(config-dhcp-server)# network 192.168.1.0/24

#Задаем диапазон выдаваемых IP-адресов:
wlc-30(config-dhcp-server)# address-range 192.168.1.2-192.168.1.254

#Шлюз по умолчанию. Им является адрес бриджа управления ТД:
wlc-30(config-dhcp-server)# default-router 192.168.1.1

#Выдаем адрес DNS-сервера:
wlc-30(config-dhcp-server)# dns-server 192.168.1.1

#Необходимо обязательно указывать NTP-сервер, т.к. корректное время позволяет пройти проверку
валидности сертификатов.

#Выдаем 42 опцию DHCP, содержащую адрес NTP-сервера, для синхронизации времени на точках
доступа:
wlc-30(config-dhcp-server)# option 42 ip-address 192.168.1.1

#Выдаем 43 vendor specific опцию DHCP, которая содержит:

- 12 подопцию, необходимую для построения SoftGRE data туннелей. Опция содержит IP-адрес
 softgre-интерфейса контроллера.
wlc-30(config-dhcp-server)# vendor-specific
wlc-30(config-dhcp-server-vendor-specific)# suboption 12 ascii-text "192.168.1.1"

- 15 подопцию, необходимую для того, чтобы точка доступа автоматически пришла на контроллер и
включилась в работу под его управлением. Опция содержит HTTPS URL контроллера.
wlc-30(config-dhcp-server-vendor-specific)# suboption 15 ascii-text "https://192.168.1.1:8043"
wlc-30(config-dhcp-server-vendor-specific)# exit
wlc-30(config-dhcp-server)# exit
```

Настраиваем адресное пространство для пользователей:

```
wlc-30(config)# ip dhcp-server pool users-pool

#Определяем подсеть:
wlc-30(config-dhcp-server)# network 192.168.2.0/24

#Задаем диапазон выдаваемых пользователям Wi-Fi IP-адресов:
wlc-30(config-dhcp-server)# address-range 192.168.2.2-192.168.2.254

#Шлюз по умолчанию:
wlc-30(config-dhcp-server)# default-router 192.168.2.1

#Выдаем адрес DNS-сервера:
wlc-30(config-dhcp-server)# dns-server 192.168.2.1
wlc-30(config-dhcp-server)# exit
```

Настройка RADIUS-сервера

Настраиваем локальный RADIUS-сервер.

```
wlc-30(config)# radius-server local

#Настраиваем NAS ap. Содержит подсети точек доступа, которые будут обслуживаться локальным
 RADIUS-сервером при Enterprise-авторизации пользователей Wi-Fi:
wlc-30(config-radius)# nas ap
wlc-30(config-radius-nas)# key ascii-text password
wlc-30(config-radius-nas)# network 192.168.1.0/24
wlc-30(config-radius-nas)# exit

#Настраиваем NAS local. Используется при обращении WLC к локальному RADIUS-серверу при
построении SoftGRE-туннелей:
wlc-30(config-radius)# nas local
wlc-30(config-radius-nas)# key ascii-text password
wlc-30(config-radius-nas)# network 127.0.0.1/32
wlc-30(config-radius-nas)# exit

#Создаем домен для пользователей:
wlc-30(config-radius)# domain default

#Создаем учетную запись пользователя Wi-Fi для подключения к Enterprise SSID:
wlc-30(config-radius-domain)# user name1
wlc-30(config-radius-user)# password ascii-text password1
wlc-30(config-radius-user)# exit
wlc-30(config-radius-domain)# exit

#Настройки виртуального сервера содержат номера портов для аутентификации и аккаунтинга,
настройки проксирования на внешний RADIUS server. Использование стандартных портов (1812 для
аутентификации и 1813 для аккаунтинга) не требует настройки. В таком случае достаточно просто
включения виртуального сервера (enable).
wlc-30(config-radius)# virtual-server default
wlc-30(config-radius-vserver)# enable
wlc-30(config-radius-vserver)# exit
wlc-30(config-radius)# enable
wlc-30(config)# exit
```

Обратите внимание, что в заводской конфигурации учетная запись пользователя не настроена в целях безопасности, поэтому для подключения к Enterprise SSID в заводской конфигурации необходимо создать учетную запись.

Определим параметры для взаимодействия с RADIUS-сервером: IP-адрес и ключ. Так как RADIUS-сервер находится локально на контроллере, в качестве адреса хоста задаем 127.0.0.1. Ключ должен совпадать с ключом, указанным для nas local.

```
wlc-30(config)# radius-server host 127.0.0.1
wlc-30(config-radius-server)# key ascii-text password
wlc-30(config-radius-server)# exit
```

Добавляем профиль AAA, указываем адрес сервера, который будет использоваться:

```
wlc-30(config)# aaa radius-profile default_radius
wlc-30(config-aaa-radius-profile)# radius-server host 127.0.0.1
wlc-30(config-aaa-radius-profile)# exit
```

Настраиваем и включаем функционал автоматического поднятия SoftGRE-туннелей:

```
wlc-30(config)# softgre-controller

#Так как RADIUS-сервер находится локально на контроллере,указываем nas-ip-address 127.0.0.1:
wlc-30(config-softgre)# nas-ip-address 127.0.0.1

#Выбираем режим создания data SoftGRE туннелей – WLC:
wlc-30(config-softgre)# data-tunnel configuration wlc

#Выбираем созданный ранее AAA-профиль:
wlc-30(config-softgre)# aaa radius-profile default_radius
wlc-30(config-softgre)# keepalive-disable
wlc-30(config-softgre)# enable
wlc-30(config-softgre)# exit
```

Настройка модуля управления точками доступа WLC

Переходим к настройкам модуля управления конфигурацией точек доступа:

```
wlc-30(config)# wlc
wlc-30(config-wlc)#
```

Настраиваем профиль RADIUS-сервера, который будет использоваться для аутентификации беспроводных клиентов Enterprise SSID точек доступа Wi-Fi. Если предполагается аутентификация клиентов на внешнем RADIUS-сервере, то здесь указывается его адрес и ключ. При такой настройке точка доступа будет проводить аутентификацию клиентов без участия WLC.

```
wlc-30(config-wlc)# radius-profile default-radius

#Так как RADIUS-сервер находится локально на контроллере, указываем адрес контроллера в подсети
точек доступа:
wlc-30(config-wlc-radius-profile)# auth-address 192.168.1.1

#Ключ RADIUS-сервера должен совпадать с ключом, указанным для NAS ap:
wlc-30(config-wlc-radius-profile)# auth-password ascii-text password

#Указываем домен RADIUS. Этот домен должен совпадать с доменом, в котором созданы учетные
записи пользователей Enterprise.
wlc-30(config-wlc-radius-profile)# domain default
wlc-30(config-wlc-radius-profile)# exit
```

Настройка SSID

Профиль SSID содержит настройки SSID точки доступа. Для примера настроим Enterprise SSID:

```
wlc-30(config-wlc)# ssid-profile default-ssid

#Description может содержать краткое описание профиля:
wlc-30(config-wlc-ssid-profile)# description default-ssid

#SSID – название беспроводной сети, которое будут видеть пользователи при сканировании эфира:
wlc-30(config-wlc-ssid-profile)# ssid default-ssid

#VLAN ID – номер VLAN для передачи пользовательского трафика. При передаче трафика Wi-Fi
клиентам метка будет сниматься точкой доступа. При прохождении трафика в обратную сторону на
нетегированный трафик от клиентов метка будет навешиваться:
wlc-30(config-wlc-ssid-profile)# vlan-id 1000

#Security mode – режим безопасности доступа к беспроводной сети. Для Enterprise авторизации
выберите режим WPA2_1X:
wlc-30(config-wlc-ssid-profile)# security-mode WPA2_1X

#Указываем профиль настроек RADIUS-сервера, который будет использоваться для авторизации
пользователей Wi-Fi:
wlc-30(config-wlc-ssid-profile)# radius-profile default-radius

#Далее необходимо указать хотя бы один диапазон, в котором будет работать SSID: 2.4/5 ГГц:
wlc-30(config-wlc-ssid-profile)# band 2g
wlc-30(config-wlc-ssid-profile)# band 5g

#Активируем профиль SSID. В случае необходимости отключения SSID на всех локациях, SSID-профиль
можно выключить командой 'no enable':
wlc-30(config-wlc-ssid-profile)# enable
wlc-30(config-wlc-ssid-profile)# exit
```

Настройка профилей конфигурации

Создаем профиль общих настроек точек доступа:

```
wlc-30(config-wlc)# ap-profile default-ap

#Задаем пароль для подключения к точке доступа:
wlc-30(config-wlc-ap-profile)# password ascii-text password

wlc-30(config-wlc-ap-profile)# exit
```

Создаем профили конфигурации точек доступа:

⚠ Для каждой модели подключаемых точек доступа необходимо создать отдельный профиль конфигурации, так как точки доступа различных типов могут иметь особенности конфигурации (например, разные IEEE 802.11 режимы работы радиоинтерфейса). В профиле обязательно указывается тип точки доступа – ap-model.

✓ Подробную информацию о точках доступа можно найти в официальной документации по ссылке.

Создаем профили точек доступа WEP-1L, WEP-2L, WOP-2L, WOP-20L:

```
wlc-30(config-wlc)# board-profile default_wep-1l_profile

#Указываем модель точки доступа, для которой создается профиль:
wlc-30(config-wlc-board-profile)# ap-model WEP-1L

#Выполняем настройки радиоинтерфейсов точки доступа. Заходим в настройки первого
радиоинтерфейса (wlan0):
wlc-30(config-wlc-board-profile)# radio wlan0

#Задаем радиочастотный диапазон 2.4 ГГц:
wlc-30(config-wlc-board-profile-radio)# band 2g

#Выбираем IEEE 802.11 режим работы радиоинтерфейса:
wlc-30(config-wlc-board-profile-radio)# work-mode bgn

#Задаем номер радиоканала, который будет выставлен при выключенной опции автовыбора каналов:
wlc-30(config-wlc-board-profile-radio)# channel 1

#Задаем ширину радиоканала:
wlc-30(config-wlc-board-profile-radio)# bandwidth 20

#Выставляем мощность сигнала передатчика в дБм:
wlc-30(config-wlc-board-profile-radio)# tx-power 16

#Задаем список каналов, из которых точка доступа будет автоматически выбирать наименее
загруженный радиоканал при включенных настройках autochannel и use-limit-channels:
wlc-30(config-wlc-board-profile-radio)# limit-channels 1 6 11

#Включаем использование списка каналов для автовыбора. При выключенной опции use-limit-
channels точка доступа будет выбирать рабочий канал из всех доступных каналов данного диапазона
частот:
wlc-30(config-wlc-board-profile-radio)# use-limit-channels
wlc-30(config-wlc-board-profile-radio)# exit
```

```
#Заходим в настройки второго радиоинтерфейса (wlan1):
wlc-30(config-wlc-board-profile)# radio wlan1

#Задаем радиочастотный диапазон 5 ГГц:
wlc-30(config-wlc-board-profile-radio)# band 5g

#Выбираем IEEE 802.11 режим работы радиоинтерфейса:
wlc-30(config-wlc-board-profile-radio)# work-mode ac

#Задаем номер радиоканала, который будет выставлен при выключенной опции автовыбора каналов:
wlc-30(config-wlc-board-profile-radio)# channel 36

#Задаем ширину радиоканала:
wlc-30(config-wlc-board-profile-radio)# bandwidth 20

#Выставляем мощность сигнала передатчика в дБм:
wlc-30(config-wlc-board-profile-radio)# tx-power 19

#Задаем список каналов, из которых точка доступа будет автоматически выбирать наименее
загруженный радиоканал при включенных настройках autochannel и use-limit-channels:
wlc-30(config-wlc-board-profile-radio)# limit-channels 36 40 44 48
wlc-30(config-wlc-board-profile-radio)# exit
wlc-30(config-wlc-board-profile)# exit
```

Создаем аналогично профили точек доступа WEP-3ax, WEP-30L, учитывая особенности конфигурации:

```
wlc-30(config-wlc)# board-profile default_wep-3ax_profile
wlc-30(config-wlc-board-profile)# ap-model WEP-3ax
wlc-30(config-wlc-board-profile)# radio wlan0
wlc-30(config-wlc-board-profile-radio)# band 2g
wlc-30(config-wlc-board-profile-radio)# work-mode bgn
wlc-30(config-wlc-board-profile-radio)# channel 1
wlc-30(config-wlc-board-profile-radio)# use-limit-channels
wlc-30(config-wlc-board-profile-radio)# bandwidth 20
wlc-30(config-wlc-board-profile-radio)# tx-power 16
wlc-30(config-wlc-board-profile-radio)# limit-channels 1 6 11
wlc-30(config-wlc-board-profile-radio)# exit
wlc-30(config-wlc-board-profile)# radio wlan1
wlc-30(config-wlc-board-profile-radio)# band 5g
wlc-30(config-wlc-board-profile-radio)# work-mode anacax
wlc-30(config-wlc-board-profile-radio)# channel 36
wlc-30(config-wlc-board-profile-radio)# bandwidth 20
wlc-30(config-wlc-board-profile-radio)# tx-power 19
wlc-30(config-wlc-board-profile-radio)# limit-channels 36
wlc-30(config-wlc-board-profile-radio)# limit-channels 40 44 48
wlc-30(config-wlc-board-profile-radio)# exit
wlc-30(config-wlc-board-profile)# exit
```

Настройка локации

Под локацией понимается группа точек доступа, предназначенная для предоставления сервиса внутри топографического и/или логического сегмента сети, которые в общем случае будут конфигурироваться по одним и тем же правилам (профилям). Локация для точки (ap-location) определяется при подключении точки к контроллеру в зависимости от адресного пространства. Исключение составляет переопределение профиля конфигурации и/или ap-location в индивидуально созданном шаблоне для точки доступа по ее MAC-адресу.

Создаем локацию и определяем правила конфигурирования точек доступа, входящих в данную локацию:

```
wlc-30(config-wlc)# ap-location default-location

#Description может содержать краткое описание локации:
wlc-30(config-wlc-ap-location)# description default-location

#Устанавливаем соответствия типа точки доступа и профиля конфигурации, который содержит правила
настройки точек доступа в данной локации:
wlc-30(config-wlc-ap-location)# board-profile WEP-1L default_wep-1l_profile
wlc-30(config-wlc-ap-location)# board-profile WEP-2L default_wep-2l_profile
wlc-30(config-wlc-ap-location)# board-profile WEP-3ax default_wep-3ax_profile
wlc-30(config-wlc-ap-location)# board-profile WOP-20L default_wop-20l_profile
wlc-30(config-wlc-ap-location)# board-profile WOP-2L default_wop-2l_profile
wlc-30(config-wlc-ap-location)# board-profile WEP-30L default_wep-30l_profile

#Указываем профили беспроводных сетей, которые будут предоставлять услуги в данной локации:
wlc-30(config-wlc-ap-location)# ssid-profile default-ssid default

#Так как схема предполагает передачу пользовательского трафика через SoftGRE-туннели, то
необходимо указать, что локация работает в режиме туннелирования:
wlc-30(config-wlc-ap-location)# mode tunnel
wlc-30(config-wlc-ap-location)# exit
```

Определение подсетей обслуживаемых точек доступа

Определяем адресное пространство подключаемых точек доступа:

```
wlc-30(config-wlc)# ip-pool default-ip-pool

#Description может содержать краткое описание пула адресов:
wlc-30(config-wlc-ip-pool)# description default-ip-pool

#Подсеть IP-адресов точек доступа указывается в параметре network. Если данный параметр не
определен, то все точки доступа будут попадать под данное правило.

#Указываем ap-location, которая будет присваиваться точкам доступа данного пула адресов:
wlc-30(config-wlc-ip-pool)# ap-location default-location
wlc-30(config-wlc-ip-pool)# exit
```

Точки доступа, подсети которых не определены в ip-pool, не будут обслуживаться контроллером.

Авторегистрация точек доступа

Активируем авторегистрацию точек доступа на контроллере:

```
wlc-30(config-wlc)# service-activator
wlc-30(config-wlc-service-activator)# aps join auto
```

При подключении новых точек доступа не потребуется дополнительных действий, точки доступа будут зарегистроированы в автоматическом режиме.

Включение функционала WLC

Активируем работу WLC и сохраняем настройки:

```
wlc-30(config-wlc)# enable
wlc-30(config-wlc)# end
wlc-30# commit
wlc-30# confirm
```

Обновление точек доступа

В конфигурации по умолчанию при подключении точка доступа сразу автоматически обновится на прошивку, которая загружена на WLC. Если точка доступа уже находится под управлением WLC, то она обновится на новую прошивку сразу после ее загрузки.

Для загрузки прошивки используйте команду:

```
#IP-адрес TFTP-сервера - 192.168.1.2, WEP-1L-1.2.5_build_16.tar.gz - название файла ПО.
wlc-30# copy tftp://192.168.1.2:/WEP-1L-1.2.5_build_16.tar.gz system:access-points-firmwares
```

Если на WLC загружено несколько файлов ПО, то точка доступа будет обновляться на самую последнюю версию.

9.2 Настройка AirTune

9.2.1 Описание

Одним из приоритетных направлений по развитию точек доступа в области Enterprise&High-Density Wi-Fi является реализация сервиса AirTune, основной функцией которого является Radio Resource Management (RRM).

Radio Resource Management позволяет автоматически оптимизировать характеристики точек доступа в зависимости от текущих условий. **Сервис AirTune не заменяет собой процедуры радиопланирования**, но позволяет провести финальный этап оптимизации сети, а также вести постоянный контроль.

Используемые технологии и алгоритмы:

- Dynamic Channel Assignment (DCA) – алгоритм автоматического распределения частотных каналов каждой точки доступа в сети для избежания интерференции между ними;
- Transmit Power Control (TPC) – алгоритм управления мощностью передатчиков с целью обеспечения оптимальной зоны покрытия сети и минимизации "конфликтных" областей, где клиент находится в зоне уверенного приема нескольких соседних точек доступа;
- Load Balancing – алгоритм автоматического распределения клиентских устройств между точками. В случае перегрузки сервис определит более оптимальную ТД для подключения клиента и выдаст рекомендации на точки доступа, клиент будет видеть в эфире только 1 ТД, рекомендованную для авторизации;
- Roaming – поддержка стандартов бесшовного роуминга 802.11 k/r.

Основными задачами функционала являются:

- Автоматическая настройка рабочих каналов между точками доступа;
- Автоматическая подстройка излучаемой мощности для стабильности зоны покрытия («соты»);
- Оптимизация пропускной способности беспроводной сети;
- Минимизация «конфликтных» областей между точками доступа;
- Равномерное распределение нагрузки между точками доступа;
- Поиск оптимальной точки доступа для клиента находящегося в «неуверенной» зоне приема;

- Минимизация «случайных» переподключений клиентов на границах «сот»;
- Поддержка бесшовного роуминга клиентов между точками доступа.

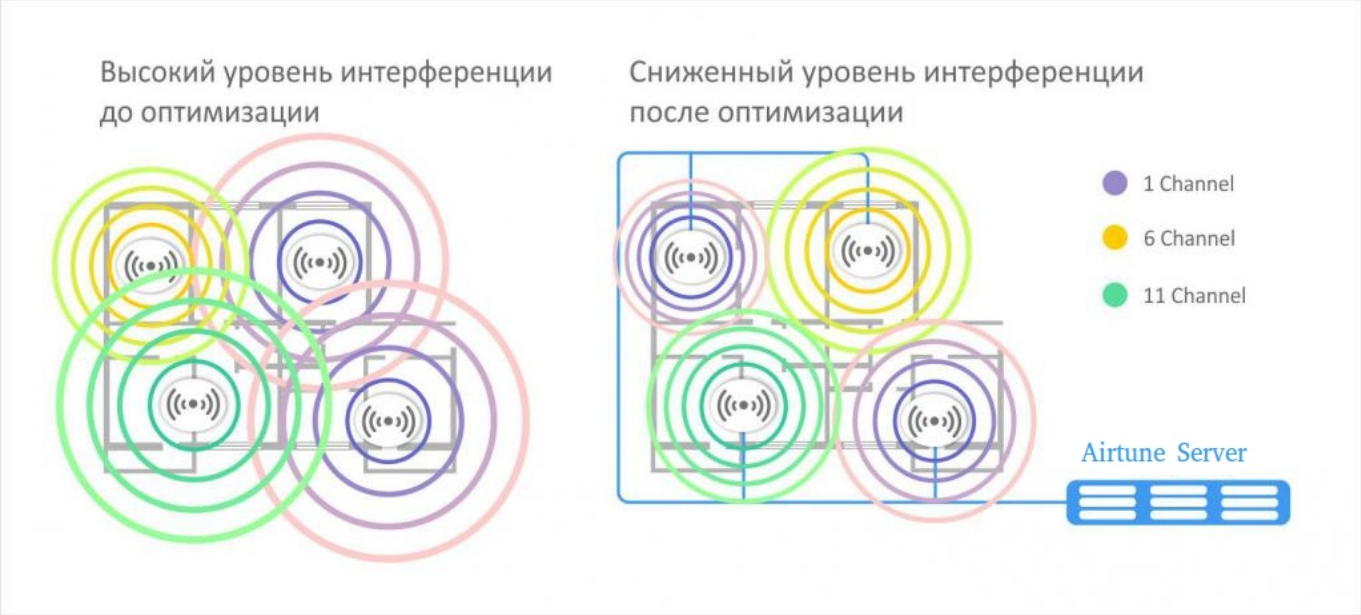
При работе функционала TPC/DCA точки доступа по команде от сервиса с помощью специальных пакетов (Action Frame) собирают информацию о радиосреде в текущий момент времени. Затем передают информацию на сервис, который выполняет анализ "качества радиоэфира" и проводит оптимизацию параметров для каждой точки доступа, что обеспечивает равномерность зоны покрытия и минимизацию интерференции.

Также сервис в себя включает функционал роуминга:

- Синхронизация списков соседних точек доступа стандарта 802.11k, который позволяет клиенту при ослабевании сигнала с текущей точки доступа искать более подходящую точку доступа из рекомендуемого списка, а не анализируя весь эфир.
- Согласование ключей между точками доступа для роуминга стандарта 802.11r, который позволяет значительно ускорять процесс переключения клиента между точками доступа, т.к. клиенту не нужно будет проходить повторную полную авторизацию на встречной точке доступа, только ускоренную.

> ⓘ Для работы роуминга стандартов 802.11k/r необходима поддержка стандарта со стороны клиентов.

Простой пример работы оптимизации сети с помощью сервиса представлен на картинке (функционал DCA+TPC):



9.2.2 Алгоритм работы

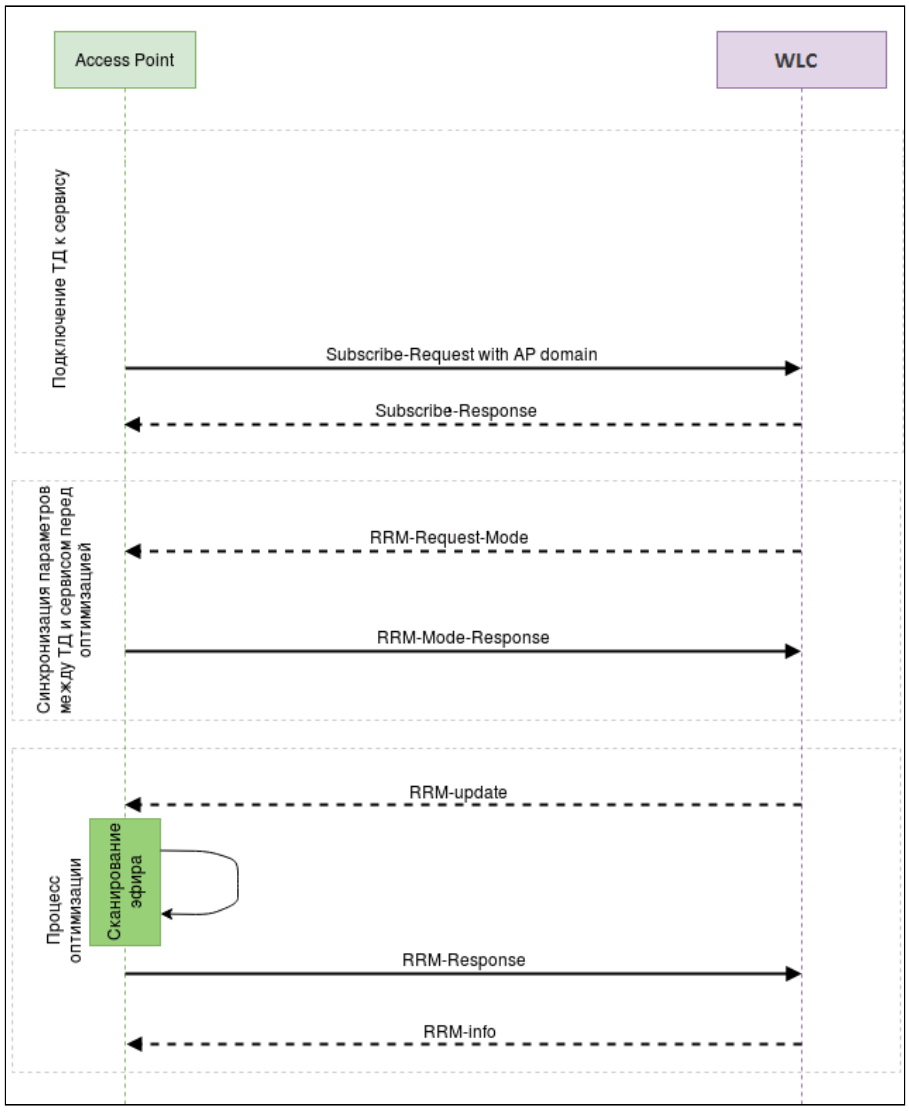
ТД при подключении к серверу (соединение между ТД и сервером осуществляется по протоколу WebSocket) отправляет сообщение "subscribe-request", где передает свои параметры, такие как:

- заводские установочные параметры (серийный номер, тип устройство, MAC-адрес);
- имя локации (географический домен);
- радио настройки (канал, мощность);
- список SSID;
- список подключенных клиентов.

После того как ТД построила сессию с сервисом, на AirTune точки группируются по доменам. Если на сервисе нет домена, которому принадлежит точка, AirTune отправляет отказ в обслуживании.

Если на AirTune домен настроен, то сервер отправляет "subscribe-response" с указанием какие функции (DCA, TPC, Load Balance) настроены для этого домена.

Оптимизация (DCA, TPC) проходит внутри домена по следующему сценарию:



1) Первым этапом происходит авторизация ТД на сервисе AirTune, для этого система управления посредством SNMP-set запроса конфигурирует на точках доступа URL сервиса AirTune;

2) ТД поднимают сессию с сервисом, обменявшись пакетами Subscribe-Request/Subscribe-Response, в которых ТД информирует сервис о текущей конфигурации. В случае если на сервисе не существует

географический домен, переданный в сообщении от точки, сервис будет игнорировать запросы. Если домен найден, подключение происходит успешно;

3) Далее сервер отправляет на точки запрос "rrm-request-mode", чтобы актуализировать текущую информацию о них, т.к. оптимизация может начаться не только после подключения точки, а планово либо по команде администратора спустя долгое время после первичного подключения;

4) Точки доступа отвечают "rrm-response-mode", в котором передают свои текущие радио параметры;

5) Сервер отправляет запрос на сканирование окружения "rrm-update". В зависимости от опции eltex-rrm-scan сканирование может быть "обычным" (точка перебирает доступные каналы и детектирует все видимые точки) либо специальным, когда только точки из домена передают специальные action пакеты в один, заранее определенный, момент времени;

6) Точки отправляют результат сканирования на сервер сообщением "rrm-response";

7) Получив результаты от всех ТД в домене, сервер в зависимости от настроек определяет для каждой точки оптимальную мощность, оптимальный канал, список соседей и отправляет сообщение "rrm-info";

8) После этого ТД применяют рекомендованные настройки, и оптимизация считается завершенной.

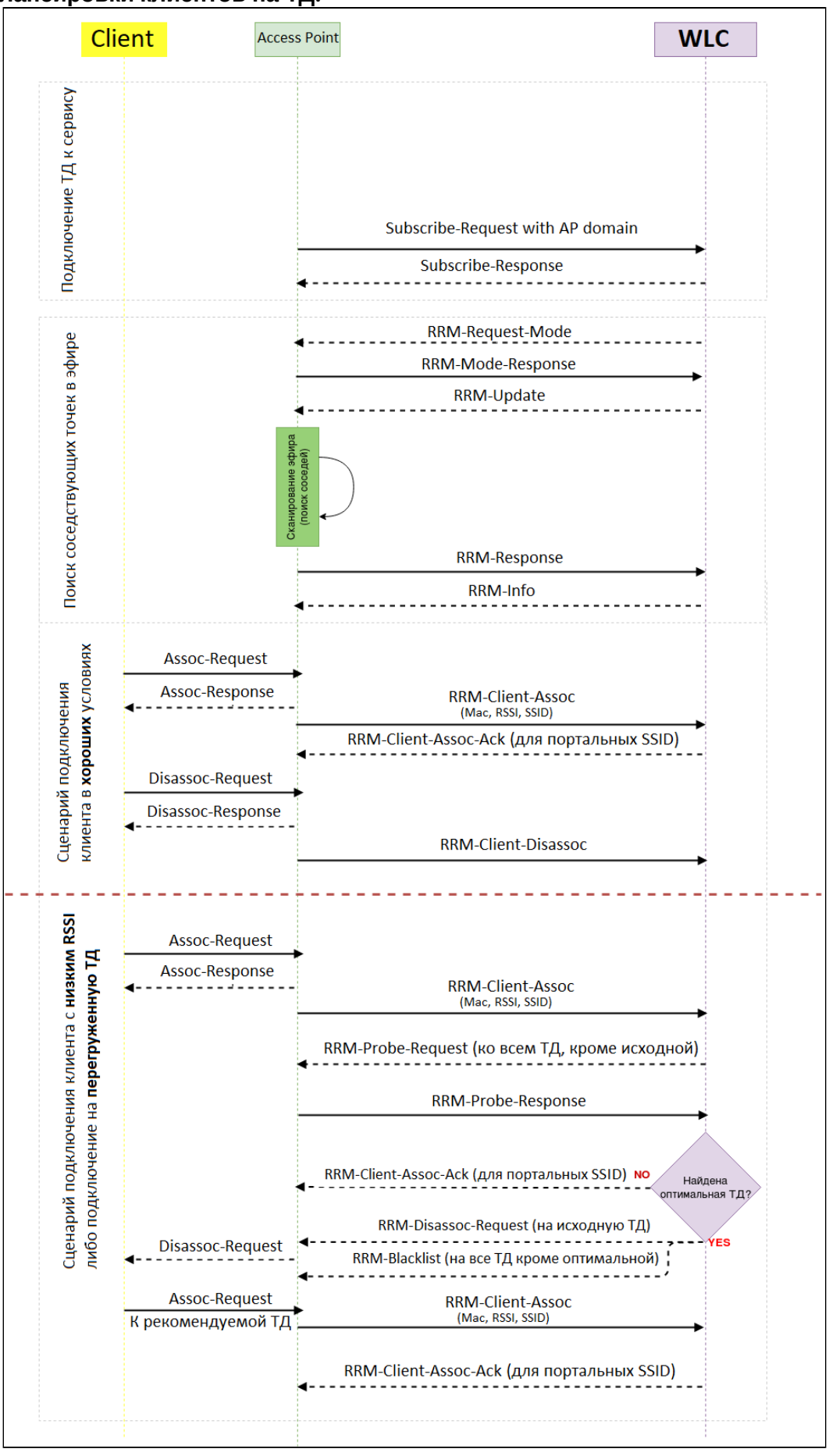
Оптимизация происходит в следующих случаях:

- новая точка добавилась в домен;
- одна из ТД была отключена;
- на одной из точек были изменены радио параметры;
- по таймеру (Optimization interval);
- по нажатию администратором соответствующей кнопки.

Оптимизация не происходит в случае:

- перезапуска ТД;
- короткого пропадания связи между ТД и сервисом;
- обновления ТД.

Сценарий балансировки клиентов на ТД:



1) В случае если алгоритмы TPC/DCA включены вместе с балансировщиком либо отключена опция "Use all AP for Balance", то первым этапом происходит поиск соседствующих точек в эфире;

> В случае если стоит флаг "Use all AP for Balance" в конфигурации AirTune, то пункт Поиск соседствующих точек в эфире будет пропущен, рассылка будет осуществляться всем ТД, находящимся в одном домене;

2) Далее начинаются сценарии работы балансировщика. При подключении нового клиента с ТД на сервер отправляется сообщение "rrm-client-assoc", в котором содержится MAC-адрес клиента, SSID к которому клиент подключился. В случае если подключенный клиент находится в зоне уверенного приема и ТД не является загруженной, сервисом никаких действий не предпринимается, отправляется только сообщение "RRM-Client-Assoc-Ack" для портальных клиентов, после него ТД разблокирует клиентов для доступа в интернет (если пользователь уже авторизовался на портале);

3) Если при подключении клиента данная точка является загруженной (превышен лимит клиентов) или клиент имеет сигнал ниже установленного уровня, сервер инициирует процесс балансировки этого клиента;

4) Сервис отправляет "соседним" ТД, на которых настроен такой же SSID сообщение "rrm-probe-request", чтобы определить с каким уровнем сигнала ТД "видят" данного клиента;

5) ТД отвечают сообщением "rrm-probe-response", в котором указывают уровень сигнала RSSI;

6) Если сервер не нашел подходящей точки для клиента, он оставляет его на текущей. Если оптимальная точка найдена, клиента отключаем от текущей ТД командой "rrm-disassoc-request", на всех остальных, кроме оптимальной, блокируем клиента командой "rrm-blacklist", таким образом клиент видит в эфире только 1 целевую ТД и произойдет переключение клиента (роуминг).

> Балансировка клиентов между точками доступа происходит в рамках одного интерфейса (2.4 ГГц или 5 ГГц).
> Если клиент подключился в 2.4 ГГц к загруженной ТД, то его балансировка на свободный интерфейс 5 ГГц второй точки доступа происходить не будет, только на аналогичный интерфейс (2.4 ГГц).

> Если клиентское устройство поддерживает функционал рандомизации MAC-адреса в Probe Request, то для таких клиентов функционал работать не будет, т.к. анализ уровня сигнала от клиента на соседних точках доступа основывается на менеджмент-пакетах от клиента (Probe request).

9.2.3 Алгоритм настройки

По умолчанию все необходимые настройки для работы сервиса настроены, нужно только указать IP-адрес контроллера, который виден точкам доступа, включить сервис, создать профиль и привязать его к локации.

Настройки производятся в режиме конфигурирования (config) раздела настройки контроллера WLC (config-wlc).

Шаг	Описание	Команда	Ключи
1	Перейти в раздел конфигурирования WLC.	**wlc-30# configure** **wlc-30(config)# wlc** **wlc-30(config-wlc)#**	
2	Создать профиль AirTune.	**wlc-30(config-wlc)# airtune-profile <NAME>** **wlc-30(config-airtune-profile)#exit** **wlc-30(config-wlc)#**	<NAME> – название профиля, задается строкой до 235 символов.
3	Перейти в локацию, для которой требуется автоматическая оптимизация настроек точек доступа.	**wlc-30(config-wlc)# ap-location <NAME>** **wlc-30(config-wlc-ap-location)#**	<NAME> – название профиля локации, задается строкой до 235 символов.
4	Привязать созданный профиль к локации.	**wlc-30(config-wlc-ap-location)# airtune-profile <NAME>** **wlc-30(config-wlc-ap-location)#exit** **wlc-30(config-wlc)#**	<NAME> – название профиля локации, задается строкой до 235 символов.
5	Перейти в раздел общих настроек сервиса.	**wlc-30(config-wlc)# airtune** **wlc-30(config-airtune)#**	
6	Активировать работу сервиса.	**wlc-30(config-airtune)# enable** **wlc-30(config-airtune)#end**	
7	Указать IP-адрес контроллера, который виден точкам доступа.	**wlc-30(config-wlc)# outside-address <ADDR>**	<ADDR> – IP-адрес контроллера, задаётся в виде: AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

9.2.4 Пример настройки

```
wlc-30# configure
wlc-30(config)# wlc
wlc-30(config-wlc)# airtune-profile default_airtune
wlc-30(config-airtune-profile)#exit

wlc-30(config-wlc)#
wlc-30(config-wlc)# ap-location default-location
wlc-30(config-wlc-ap-location)# airtune-profile default_airtune
wlc-30(config-wlc-ap-location)#exit

wlc-30(config-wlc)# airtune
wlc-30(config-airtune)# enable
wlc-30(config-airtune)#exit

wlc-30(config-wlc)# outside-address 192.168.1.1
wlc-30(config-wlc)# end

wlc-30# commit
wlc-30# confirm
```

10 Управление интерфейсами

- Настройка VLAN
  - Алгоритм настройки
  - Пример настройки 1. Удаление VLAN с интерфейса
  - Пример настройки 2. Разрешение обработки VLAN в тегированном режиме
  - Пример настройки 3. Разрешение обработки VLAN в тегированном и не тегированном режиме
- Настройка LLDP
  - Алгоритм настройки
  - Пример настройки
- Настройка LLDP MED
  - Алгоритм настройки
  - Пример настройки Voice VLAN
- Настройка терминации на саб-интерфейсе
  - Алгоритм настройки
  - Пример настройки саб-интерфейса
- Настройка терминации на Q-in-Q интерфейсе
  - Алгоритм настройки
  - Пример настройки Q-in-Q интерфейса
- Настройка USB-модемов
  - Алгоритм настройки USB-модемов
  - Пример настройки
- Настройка STP/RSTP
  - Алгоритм настройки Spanning Tree
  - Пример настройки
- Настройка PPP через E1
  - Алгоритм настройки
  - Пример конфигурации
- Настройка MLPPP
  - Алгоритм настройки
  - Пример настройки
- Настройка Bridge
  - Алгоритм настройки
  - Пример настройки bridge для VLAN и L2TPv3-туннеля
  - Пример настройки bridge для VLAN
  - Пример настройки добавления/удаления второго VLAN-тега
- Настройка Dual-Homing
  - Алгоритм настройки
  - Пример настройки
- Настройка зеркалирования (SPAN/RSPAN)
  - Алгоритм настройки
  - Пример настройки
- Настройка LACP
  - Алгоритм настройки
  - Пример настройки
- Настройка AUX
  - Алгоритм настройки
  - Примеры настроек
  - Схемы распайки переходников

10.1 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.

10.1.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать VLAN.	**esr(config)# vlan <VID>**	<VID> – идентификатор VLAN, задаётся в диапазоне [2..4094]. Также есть возможность создания нескольких vlan (через запятую), диапазона vlan (через дефис) или комбинированная запись содержащая запятые и дефисы.
2	Задать имя vlan (не обязательно).	**esr(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).	**esr(config-vlan)# force-up**	
4	Отключить обработку входящих не тегированных Ethernet-фреймов на основе таблицы коммутации VLAN'а по умолчанию (VLAN-ID – 1) (не обязательно).	**esr(config-if-gi)# switchport forbidden default-vlan**	
5	Установить режим работы физического интерфейса в L2-режим.	**esr(config-if-gi)# mode switchport**	
6	Установить комбинированный режим работы физического интерфейса.	**esr(config-if-gi)# mode hybrid**	Допустимо только для ESR-1000/1200/1500/1511 /1700.
7	Задать режим работы L2-интерфейса.	**esr(config-if-gi)# switchport access**	Только для ESR-10/12V(F)/ 14VF/ 15/20/21/30/100/200/3100/ 3200 и WLC-30. Данный режим является режимом по умолчанию и не отображается в конфигурации.

Шаг	Описание	Команда	Ключи
		esr(config-if-gi)# switchport trunk	Только для ESR-10/12V(F)/ 14VF/ 15/20/21/30/100/200/3100/ 3200 и WLC-30.
		esr(config-gi)# switchport general	Только для ESR-1000/1200/1500/1511 /1700. Данный режим является режимом по умолчанию и не отображается в конфигурации.
8	Настроить список VLAN на интерфейсе в тегированном режиме.	**esr(config-if-gi)# switchport trunk allowed vlan add <VID>**	Для ESR-10/12V(F)/14VF/ 15/20/21/30/100/200/3100/ 3200. <VID> – идентификатор VLAN, задаётся в диапазоне [2..4094]. Также есть возможность создания нескольких vlan (через запятую) или диапазона vlan (через дефис).
		esr(config-if-gi)# switchport general allowed vlan add <VID> tagged	Для ESR-1000/1200/1500/1511 /1700. <VID> – идентификатор VLAN, задаётся в диапазоне [2..4094]. Также есть возможность создания нескольких vlan (через запятую) или диапазона vlan (через дефис).
9	Настроить VLAN на интерфейсе в нетегированном режиме (не обязательно).	**esr(config-if-gi)# switchport trunk native-vlan <VID>**	Для ESR-10/12V(F)/14VF/ 15/20/21/30/100/200/3100/ 3200 и WLC-30. <VID> – идентификатор VLAN, задаётся в диапазоне [2..4094].

Шаг	Описание	Команда	Ключи
		esr(config-if-gi)# switchport general allowed vlan add <VID> untagged	Для ESR-1000/1200/1500/1511 /1700. <VID> – идентификатор VLAN, задаётся в диапазоне [2..4094].
10	Разрешить на интерфейсе обработку Ethernet-фреймов всех созданных на маршрутизаторе VLAN (не обязательно).	**esr(config-if-gi)# switchport trunk allowed vlan auto-all**	Только для ESR-10/12V(F)/ 14VF/ 15/20/21/30/100/200/3100/ 3200 и WLC-30.
		esr(config-if-gi)# switchport general allowed vlan auto-all	Только для ESR-1000/1200/1500/1511 /1700.
11	Устанавливается идентификатор VLAN-порта (PVID) для входящего нетегированного трафика (не обязательно).	**esr(config-if-gi)# switchport general pvid <PVID>**	Только для ESR-1000/1200/1500/1511 /1700.

10.1.2 Пример настройки 1. Удаление VLAN с интерфейса

Задача:

На основе заводской конфигурации удалить из VLAN 2 порт gi1/0/1.

Решение:

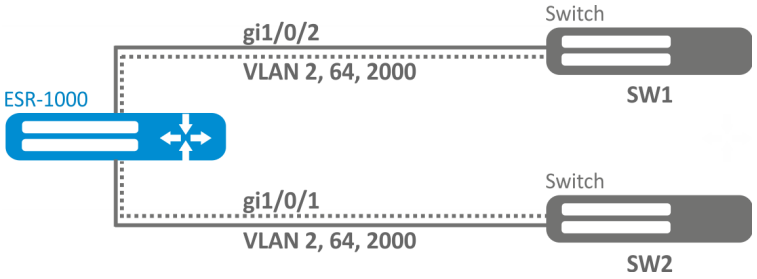
Удалим VLAN 2 с порта gi1/0/1:

```
esr(config)# interface gi 1/0/1
esr(config-if-gi)# switchport general allowed vlan remove 2 untagged
esr(config-if-gi)# no switchport general pvid
```

10.1.3 Пример настройки 2. Разрешение обработки VLAN в тегированном режиме

Задача:

Настроить порты gi1/0/1 и gi1/0/2 для передачи и приема пакетов в VLAN 2, VLAN 64, VLAN 2000.



Решение:

Создадим VLAN 2, VLAN 64, VLAN 2000 на ESR-1000:

```
esr-1000(config)# vlan 2,64,2000
```

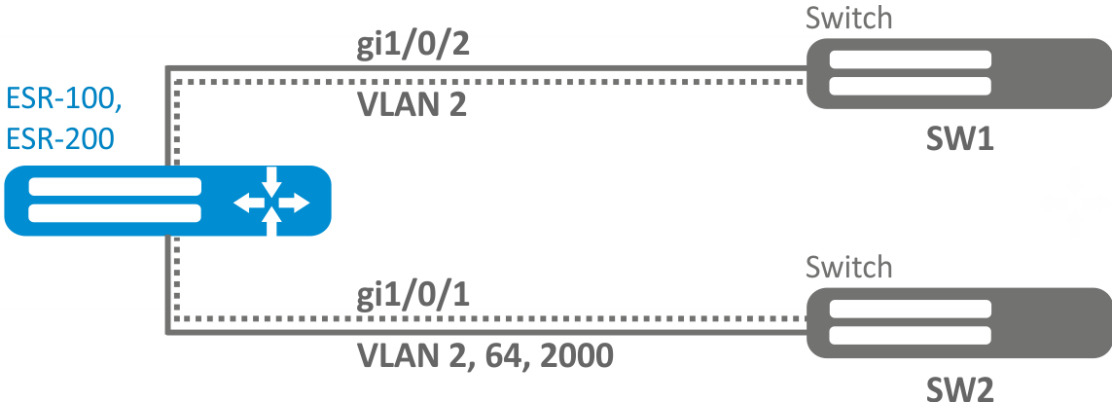
Пропишем VLAN 2, VLAN 64, VLAN 2000 на порт gi1/0/1-2:

```
esr-1000(config)# interface gi1/0/1
esr-1000(config-if-gi)# mode switchport
esr-1000(config-if-gi)# switchport forbidden default-vlan
esr-1000(config-if-gi)# switchport general allowed vlan add 2,64,2000 tagged
```

10.1.4 Пример настройки 3. Разрешение обработки VLAN в тегированном и не тегированном режиме

Задача:

Настроить порты gi1/0/1 для передачи и приема пакетов в VLAN 2, VLAN 64, VLAN 2000 в режиме trunk, настроить порт gi1/0/2 в режиме access для VLAN 2 на ESR-100/ESR-200.



Решение:

Создадим VLAN 2, VLAN 64, VLAN 2000 на ESR-100/ESR-200:

```
esr(config)# vlan 2,64,2000
```

Пропишем VLAN 2, VLAN 64, VLAN 2000 на порт gi1/0/1:

```
esr(config)# interface gi1/0/1
esr(config-if-gi)# mode switchport
esr(config-if-gi)# switchport forbidden default-vlan
esr(config-if-gi)# switchport mode trunk
esr(config-if-gi)# switchport trunk allowed vlan add 2,64,2000
```

Пропишем VLAN 2 на порт gi1/0/2:

```
esr(config)# interface gi1/0/2
esr(config-if-gi)# mode switchport
esr(config-if-gi)# switchport access vlan 2
```

10.2 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.

10.2.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Активировать LLDP на маршрутизаторе/контроллере.	**esr(config)# lldp enable**	
2	Включить прием и обработку LLDPDU на физическом интерфейсе.	**esr(config-if-gi)# lldp receive**	
3	Включить отправку LLDPDU на физическом интерфейсе.	**esr(config-if-gi)# lldp transmit**	
8	Установить период отправки LLDPDU (не обязательно).	**esr(config)# lldp timer <SEC>**	<SEC> – период времени в секундах, принимает значение [1..32768]. Значение по умолчанию: 30.
4	Установить период, в течение которого маршрутизатор/контроллер хранит информацию, полученную по LLDP (не обязательно).	**esr(config)# lldp hold-multiplier <SEC>**	<SEC> – период времени в секундах, принимает значение [1..10]. Значение по умолчанию: 4.

Шаг	Описание	Команда	Ключи
5	Установить IP-адрес, который будет передаваться в LLDP TLV в качестве management-address (не обязательно).	**esr(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.
6	Установить поле system-description, которое будет передаваться в LLDP TLV в качестве system-description (не обязательно).	**esr(config)# lldp system-description <DESCRIPTION>**	<DESCRIPION> – описание системы, задаётся строкой до 255 символов. По умолчанию содержит информацию о модели и версии ПО маршрутизатора.
7	Установить поле system-name, которое будет передаваться в LLDP TLV в качестве system-name (не обязательно).	**esr(config)# lldp system-name <NAME>**	<NAME> – имя системы, задается строкой до 255 символов. По умолчанию совпадает с заданным hostname.

10.2.2 Пример настройки

Задача:

Организовать обмен и обработку LLDPDU между маршрутизаторами ESR-1 и ESR-2 или между двумя контроллерами.

Решение:

1. Конфигурирование R1
   Включим LLDP глобально на маршрутизаторе/контроллере:

```
esr(config)# lldp enable
```

Включим прием и отправку LLDPDU на интерфейсе gi 1/0/1.

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# lldp receive
esr(config-if-gi)# lldp transmit
```

2. Конфигурирование R2
   Включим LLDP глобально на маршрутизаторе/контроллере:

```
esr(config)# lldp enable
```

Включим прием и отправку LLDPDU на интерфейсе gi 1/0/1.

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# lldp receive
esr(config-if-gi)# lldp transmit
```

Общую информацию по LLDP соседям можно посмотреть командой:

```
esr# show lldp neighbors
```

Подробную информацию по соседу конкретного интерфейса можно посмотреть командой:

```
esr# show lldp neighbors gigabitethernet 1/0/1
```

Общую статистику по LLDP можно посмотреть командой:

```
esr# show lldp statistics
```

10.3 Настройка LLDP MED

LLDP MED — расширение стандарта LLDP, которое позволяет передавать сетевые политики: VLAN ID, DSCP, priority.

10.3.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Активировать LLDP на маршрутизаторе.	**esr(config)# lldp enable**	
2	Включить отправку LLDPDU на физическом интерфейсе.	**esr(config-if-gi)# lldp transmit**	
3	Активировать расширение MED LLDP на маршрутизаторе.	**esr(config)# lldp med fast-start enable**	
4	Создать сетевую политику.	**esr(config)# network-policy <NAME>**	<NAME> – имя network-policy, задается строкой до 31 символа.

Шаг	Описание	Команда	Ключи
5	Указать тип приложения.	**esr(config-net-policy)# application <APP_TYPE>**	<APP-TYPE> – тип приложения, для которого будет срабатывать network-policy. Принимает значения: • voice; • voice-signaling; • guest-voice; • guest-voice-signaling; • softphone-voice; • video-conferencing; • streaming-video; • video-signaling.
6	Установить значение DSCP (не обязательно).	**esr(config-net-policy)# dscp <DSCP>**	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].
7	Установить значение COS (не обязательно).	**esr(config-net-policy)# priority <PRIORITY>**	<COS> – значение приоритета, принимает значения: • best-effort – COS0; • background – COS1; • excellent-effort – COS2; • critical-applications – COS3; • video – COS4; • voice – COS5; • internetwork-control – COS6; • network-control – COS7.
8	Установить значение VLAN ID.	**esr(config-net-policy)# vlan <VID> [tagged]**	<VID> – идентификационный номер VLAN, принимает значения [1…4094]; • **tagged** – ключ, при установке которого абонентское устройство будет отправлять Ethernet-фреймы указанного приложения в тегированном виде.
9	Установить сетевую политику на интерфейс.	**esr(config-if-gi)# lldp network-policy <NAME>**	<NAME> – имя network-policy, задается строкой до 31 символа.

10.3.2 Пример настройки Voice VLAN

Voice VLAN — VLAN ID, при получении которого IP-телефон переходит в режим trunk с заданным VLAN ID для приема и отправки VoIP-трафика. Передача VLAN ID осуществляется посредством расширения MED протокола LLDP.

Задача:

Необходимо разделить трафик телефонии и данных по разным VLAN, vid 10 для данных и vid 20 для телефонии и настроить отправку Voice VLAN с порта gi 1/0/1 ESR. При этом на IP-телефоне должен поддерживаться и быть включен Voice VLAN.

Решение:

Предварительно необходимо создать VLAN 10 и 20 и настроить интерфейс gi 1/0/1 в режиме trunk:

```
esr(config)# vlan 10,20
esr(config-vlan)# exit
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# mode switchport
esr(config-if-gi)# switchport mode trunk
esr(config-if-gi)# switchport trunk allowed vlan add 10,20
esr(config-if-gi)# exit
```

Включим LLDP и поддержку MED в LLDP глобально на маршрутизаторе:

```
esr(config)# lldp enable
esr(config)# lldp med fast-start enable
```

Создадим и настроим сетевую политику таким образом, чтобы для приложения voice указывался VLAN ID 20:

```
esr(config)# network-policy VOICE_VLAN
esr(config-net-policy)# application voice
esr(config-net-policy)# vlan 20 tagged
esr(config-net-policy)# exit
```

Настроим LLDP на интерфейсе и установим на него сетевую политику:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# lldp transmit
esr(config-if-gi)# lldp receive
esr(config-if-gi)# lldp network-policy VOICE_VLAN
esr(config-if-gi)# exit
```

10.4 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.

10.4.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать саб-интерфейс физического интерфейса (возможно только если физический интерфейс в режиме routeport или hybrid).	**esr(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 (не обязательно).	**esr(config-subif)# description <DESCRIPTION>**	<DESCRIPTION> – описание интерфейса, задаётся строкой до 255 символов.
3	Указать экземпляр VRF, в котором будет работать данный саб-интерфейс (не обязательно).	**esr(config-subif)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.
4	Указать IPv4/IPv6-адрес и маску подсети для конфигурируемого интерфейса или включить получение IP-адреса динамически.	**esr(config-subif)# ip address <ADDR/LEN>**	<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]. Дополнительные функции IPv4-адресации см. в разделе Настройка IP-адресации.

Шаг	Описание	Команда	Ключи
		esr(config-subif)# 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 UIPv4/IPv6-адресов перечислением через запятую. Может быть назначено до 8 IPv4/IPv6-адресов на интерфейс.
		esr(config-subif)# 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).	**esr(config-subif)# ip firewall disable**	
		esr(config-subif)# security-zone <NAME>	<NAME> – имя зоны безопасности, задаётся строкой до 31 символа.
6	Установить интервал времени, в течение которого собирается статистика о нагрузке на саб-интерфейс (не обязательно).	**esr(config-subif)# 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 (не обязательно).	**esr(config-subif)# ip arp reachable-time <TIME>** или **esr(config-subif)# 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>.

Шаг	Описание	Команда	Ключи
8	Изменить размер MTU (MaximumTransmitionUnit). MTU более 1500 будет активно только если применена команда "system jumbo-frames" (не обязательно).	**esr(config-subif)# mtu <MTU>**	<MTU> – значение MTU в байтах. Значение по умолчанию: 1500.
9	Включить запись статистики использования текущего интерфейса (не обязательно).	**esr(config-subif)# history statistics**	
10	Переопределить значение поля MSS (Maximum segment size) во входящих TCP-пакетах (не обязательно).	**esr(config-subif)# ip tcp adjust-mss <MSS>** **esr(config-subif)# 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); • proxy (см. раздел Проксирование HTTP/HTTPS-трафика); • мониторинг траффика (см. разделы Настройка Netflow и Настройка sFlow); • функционал протоколов маршрутизации (см. раздел Управление маршрутизацией); • протокол VRRF (см. раздел Управление резервированием); • функционал BRAS (см. раздел Управление BRAS (Broadband Remote Access Server)); • функционал IDS/IPS (см. раздел Настройка IPS/IDS).			

10.4.2 Пример настройки саб-интерфейса

Задача:

Настроить терминацию подсети 192.168.3.1/24 в VLAN: 828 на физическом интерфейсе gigabitethernet 1/0/1.

Решение:

Создадим саб-интерфейс для VLAN: 828

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

Настроим IP-адрес из необходимой подсети:

```
esr(config)# interface gigabitethernet 1/0/1.828
esr(config-subif)# ip address 192.168.3.1/24
esr(config-subif)# exit
```

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

10.5 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. Так же внутренний тег называют C-VLAN (Customer VLAN). Внешний тег (OuterTag) — это 802.1q-заголовок, добавленный к изначальному 802.1q-пакетом, так же называется S-VLAN (Service VLAN). Использование двойных меток в Ethernet-фреймах описывается протоколом 802.1ad.

10.5.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать саб-интерфейс физического интерфейса (возможно только если физический интерфейс в режиме routeport или hybrid).	**esr(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	Создать Q-in-Q интерфейс.	**esr(config)# interface gigabitethernet <PORT>.<S-VLAN>.<C-VLAN>** или **esr(config)# interface tengigabitethernet <PORT>.<S-VLAN>.<C-VLAN>** или **esr(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.

Шаг	Описание	Команда	Ключи
3	Задать описание Q-in-Q интерфейс (не обязательно).	**esr(config-qinq-if)# description <DESCRIPTION>**	<DESCRIPTION> – описание интерфейса, задаётся строкой до 255 символов.
4	Указать экземпляр VRF, в котором будет работать данный Q-in-Q интерфейс (не обязательно).	**esr(config-qinq-if) # 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.	**esr(config-qinq-if)# ip address <ADDR/LEN>**	<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]. Дополнительные функции IPv4-адресации см. в разделе Настройка IP-адресации.
		esr(config-qinq-if)# 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 UIPv4/IPv6-адресов перечислением через запятую. Может быть назначено до 8 IPv4/IPv6-адресов на интерфейс.
		esr(config-qinq-if)# 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).	**esr(config-qinq-if)# ip firewall disable**	

Шаг	Описание	Команда	Ключи
		esr(config-qinq-if)# 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 (не обязательно).	**esr(config-subif)# 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 (не обязательно).	**esr(config-subif)# ip arp reachable-time <TIME>** или **esr(config-subif)# 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 (MaximumTransmitionUnit). MTU более 1500 будет активно только если применена команда "system jumbo-frames" (не обязательно).	**esr(config-subif)# mtu <MTU>**	<MTU> – значение MTU в байтах. Значение по умолчанию: 1500.
10	Включить запись статистики использования текущего интерфейса (не обязательно).	**esr(config-subif)# history statistics**	
11	Переопределить значение поля MSS (Maximum segment size) во входящих TCP-пакетах (не обязательно).	**esr(config-subif)# ip tcp adjust-mss <MSS>** **esr(config-subif)# 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);
- proxy (см. раздел Проксирование HTTP/HTTPS-трафика);
- мониторинг траффика (см. разделы Настройка Netflow и Настройка sFlow);
- функционал протоколов маршрутизации (см. раздел Управление маршрутизацией);
- протокол VRRF (см. раздел Управление резервированием);
- функционал BRAS (см. раздел Управление BRAS (Broadband Remote Access Server));
- функционал IDS/IPS (см. раздел Настройка IPS/IDS).

10.5.2 Пример настройки Q-in-Q интерфейса

Задача:

Настроить терминацию подсети 192.168.1.1/24 комбинации C-VLAN: 741, S-VLAN: 828 на физическом интерфейсе gigabitethernet 1/0/1.

Решение:

Создадим саб-интерфейс для S-VLAN: 828:

```
esr(config)# interface gigabitethernet 1/0/1.828
esr(config-subif)# exit
```

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

```
esr(config)# interface gigabitethernet 1/0/1.828.741
esr(config-qinq-if)# ip address 192.168.1.1/24
esr(config-qinq-if)# exit
```

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

10.6 Настройка USB-модемов

Использование USB-модемов позволяет организовать дополнительный канал связи для работы маршрутизатора. При подключении USB-модемов возможно использовать USB-концентраторы. Одновременно в системе может быть сконфигурировано до 10 USB-модемов.

10.6.1 Алгоритм настройки USB-модемов

Шаг	Описание	Команда	Ключи
1	После подключения USB-модема дождаться, когда система обнаружит подключенное устройство.		
2	Определить, какой номер устройства назначен на подключенный USB-модем.	**esr# show cellulars status modem**	В поле "USB port" будет указан идентификатор подключенного устройства.
3	Создать профиль настроек для USB-модема и перейти в режим конфигурирования профиля.	**esr(config)# cellular profile <ID>**	<ID> – идентификатор профиля настроек для USB-модема в системе [1..10].
4	Задать описание профиля настроек (не обязательно).	**esr(config-cellular-profile)# description <DESCRIPTION>**	<DESCRIPTION> – описание профиля, задаётся строкой до 255 символов.

Шаг	Описание	Команда	Ключи
5	Задать точку доступа мобильной сети.	**esr(config-cellular-profile)# apn <NAME>**	<NAME> – точка доступа мобильной сети, задаётся строкой до 31 символа.
6	Задать имя пользователя мобильной сети (если мобильный оператор требует аутентификации по логину/паролю).	**esr(config-cellular-profile)# user <NAME>**	<NAME> – имя пользователя, задаётся строкой до 31 символа.
7	Установить парол для пользователя мобильной сети (если мобильный оператор требует аутентификации по логину/паролю).	**esr(config-user)# password ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<CLEAR-TEXT> – пароль в открытой форме, задаётся строкой [1 .. 64] символов, может включать символы [0-9a-fA-F]; <ENCRYPTED-TEXT> – пароль в зашифрованной форме, задаётся строкой [2..128] символов.
8	Активировать пользователя (если мобильный оператор требует аутентификации по логину/паролю).	**esr(config-user)# enable**	
9	Установить номер дозвона для подключения к мобильной сети.	**esr(config-cellular-profile)# number <WORD>**	<WORD> – номер дозвона для подключения к мобильной сети, задаётся строкой до 15 символов.
10	Задать метод аутентификации пользователя в мобильной сети (не обязательно).	**esr(config-cellular-profile)# allowed-auth <TYPE>**	<TYPE> – метод аутентификации пользователя в мобильной сети [none, PAP, CHAP, MSCHAP, MSCHAPv2, EAP]. Значение по умолчанию: PAP.
11	Ограничить возможность использования семейств IP-адресов в мобильной сети.	**esr(config-cellular-profile)# ip-version { ipv4 | ipv6 }**	• **ipv4** – семейство IPv4; • **ipv6** – семейство IPv6;
12	Создать USB-модем в конфигурации маршрутизатора и перейти в режим конфигурирования модема.	**esr(config)# cellular modem <ID>**	<ID> – идентификатор USB-модема в системе [1..10].
13	Задать описание модема (не обязательно).	**esr(config-cellular-modem)# description <DESCRIPTION>**	<DESCRIPTION> – описание модема, задаётся строкой до 255 символов.

Шаг	Описание	Команда	Ключи
14	Указать экземпляр VRF, в котором будет работать данный модем (не обязательно).	**esr(config-cellular-modem)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.
15	Задать идентификатор USB-модема, назначенного системой (определен в пункте 2).	**esr(config-cellular-modem)# device <WORD>**	<WORD> – идентификатор USB-порта подключенного модема [1..12].
16	Назначить ранее созданный профиль настроек для USB-модема.	**esr(config-cellular-modem)# profile <ID>**	<ID> – идентификатор профиля настроек для USB-модема в системе [1..10].
17	Задать код разблокировки SIM-карты (в случае необходимости).	**esr(config-cellular-modem)# pin <WORD>**	<WORD> – код разблокировки SIM-карты [4..8]. Возможно использование только цифр.
18	Разрешить использование того или иного режима работы USB-модема (не обязательно).	**esr(config-cellular-modem)# allowed-mode <MODE>**	<MODE> – допустимый режим работы USB-модема [2g, 3g, 4g]. По умолчанию: разрешены все режимы, поддерживаемые модемом.
19	Задать размер максимального принимаемого пакета (не обязательно).	**esr(config-cellular-modem)# mru { <MRU> }**	<MRU> – значение MRU, принимает значения в диапазоне [128..16383]. Значение по умолчанию: 1500.
20	Изменить максимальный размер обрабатываемых пакетов MTU (MaximumTransmitionUnit). MTU более 1500 будет активно только если применена команда "system jumbo-frames" (не обязательно).	**esr(config-cellular-modem)# mtu <MTU>**	<MTU> – значение MTU в байтах. Значение по умолчанию: 1500.
21	Задать предпочтительный режим работы USB-модема в мобильной сети (не обязательно).	**esr(config-cellular-modem)# preferred-mode { <MODE> }**	<MODE> – предпочтительный режим работы USB-модема [2g, 3g, 4g].
22	Отключить на интерфейсе функции Firewall или включить интерфейс в зону безопасности (см. раздел Конфигурирование Firewall).	**esr(config-subif)# ip firewall disable**	

Шаг	Описание	Команда	Ключи
		esr(config-subif)# security-zone <NAME>	<NAME>-имя зоны безопасности, задаётся строкой до 31 символа.
23	Активировать USB-модем.	**esr(config-cellular-modem)# enable**	

Также для модема сотовой сети возможно настроить:

- QoS в базовом или расширенном режимах (см. раздел Управление QoS);
- proxy (см. раздел Проксирование HTTP/HTTPS-трафика);
- мониторинг траффика (см. разделы Настройка Netflow и Настройка sFlow);
- функционал протоколов маршрутизации (см. разделы Policy-based routing и MultiWAN).

Для полноценного функционирования модема мобильной сети необходимо дополнительно настроить маршрутизацию и функционал NAT.

10.6.2 Пример настройки

Задача:

Настроить подключение к сети Интернет, используя USB-модем.

Решение:

Для примера разберём подключение к сотовому оператору МТС.

После подключения модема необходимо дождаться, когда система обнаружит устройство. Определим порт устройства, который был назначен на подключённый USB-модем:

```
esr# show cellular status modem
Number
device  USB port    Manufacturer    Model   Current state   Interface   Link    state
1       1-2         huawei          E3372   Disabled        --          Down
```

Создадим профиль настроек для USB-модема:

```
esr(config)# cellular profile 1
```

Зададим APN, который требует провайдер, или иной необходимый адрес. Ниже показан пример подключения к APN МТС:

```
esr(config-cellular-profile)# apn internet.mts.ru
```

При необходимости задаём имя пользователя, пароль, номер дозвона и метод аутентификации:

```
esr(config-cellular-profile)# user mts
esr(config-ppp-user)# password ascii-text mts
esr(config-cellular-profile)# number *99#
esr(config-cellular-profile)# allowed-auth PAP
```

Перейдём к конфигурированию USB-модема и зададим идентификатор, соответствующий порту устройства, который был определён в начале:

```
esr(config)# cellular modem 1
esr(config-cellular-modem)# device 1-2
```

Назначим соответствующий профиль настроек и активируем модем:

```
esr(config-cellular-modem)# profile 1
esr(config-cellular-modem)# enable
```

10.7 Настройка STP/RSTP

Spanning Tree Protocol – сетевой протокол, основной задачей которого является приведение сети Ethernet с избыточными соединениями к древовидной топологии, исключающей петли. Сетевые устройства обмениваются конфигурационными сообщениями, используя кадры специального формата, и выборочно включают и отключают передачу на порты.

Rapid (быстрый) STP (RSTP) – является усовершенствованием протокола STP, характеризуется меньшим временем приведения сети к древовидной топологии и имеет более высокую устойчивость.

10.7.1 Алгоритм настройки Spanning Tree

Шаг	Описание	Команда	Ключи
1	Включить spanning-tree в режиме vlan-aware.	**esr(config)# spanning-tree**	
2	Установить интервал времени, затрачиваемый на прослушивание и изучение состояний перед переключением в состояние передачи.	**esr(config)# spanning-tree forward-time <TIME>**	<TIME> – время в секундах, принимает значения [4..30]. Значение по умолчанию: 15 секунд.
3	Установить интервал времени между отправкой BPDU-пакетов.	**esr(config)# spanning-tree hello-time <TIME>**	<TIME> – время в секундах, принимает значения [1..10]. Значение по умолчанию: 2 секунды.
4	Установить время жизни связующего дерева STP.	**esr(config)# spanning-tree max-age <TIME>**	<TIME> – время в секундах, принимает значения [6..40]. Значение по умолчанию: 20 секунд.

Шаг	Описание	Команда	Ключи
5	Выбрать поддерживаемый протокол из семейства STP.	**esr(config)# spanning-tree mode <MODE>**	<MODE> – протокол семейства STP: • STP – IEEE 802.1D Spanning Tree Protocol; • RSTP – IEEE 802.1W Rapid Spanning Tree Protocol; • MSTP – IEEE 802.1s Multiple Spanning Trees. Значение по умолчанию: RSTP.
6	Установить метод определения ценности пути.	**esr(config)# spanning-tree pathcost method <short | long>**	long – значение ценности в диапазоне [1..200000000]; short – значение ценности в диапазоне [1..65535]. Значение по умолчанию: short.
7	Настроить приоритет связующего дерева STP.	**esr(config)# spanning-tree priority <PRIORITY>**	<PRIORITY> – приоритет, указывается в диапазоне с шагом 4096 [0..61440]. Значение по умолчанию: 32768.
8	Перейти в режим конфигурирования интерфейса/туннеля/сетевого моста.	**esr(config)# interface <IF-TYPE><IF-NUM>**	<IF-TYPE> тип интерфейса; <IF-NUM> – F/S/P – F-фрейм (1), S – слот (0), P – порт.
		esr(config)# tunnel <TUN-TYPE><TUN-NUM>	<TUN-TYPE> тип туннеля; <TUN-NUM> номер туннеля.
		esr(config)# bridge <BR-NUM>	<BR-NUM> – номер bridge.
9	Включить spanning-tree.	**esr(config-bridge)# spanning-tree**	
10	Установить интервал времени, затрачиваемый на прослушивание и изучение состояний перед переключением в состояние передачи.	**esr(config-bridge)# spanning-tree forward-time <TIME>**	<TIME> – время в секундах, принимает значения [4..30]. Значение по умолчанию: 15 секунд.

Шаг	Описание	Команда	Ключи
11	Установить интервал времени между отправкой BPDU-пакетов.	**esr(config-bridge)# spanning-tree hello-time <TIME>**	<TIME> – время в секундах, принимает значения [1..10]. Значение по умолчанию: 2 секунды.
12	Установить время жизни связующего дерева STP.	**esr(config-bridge)# spanning-tree max-age <TIME>**	<TIME> – время в секундах, принимает значения [6..40]. Значение по умолчанию: 20 секунд.
13	Выбрать поддерживаемый протокол из семейства STP.	**esr(config-bridge)# spanning-tree mode <MODE>**	<MODE> – протокол семейства STP: • STP – IEEE 802.1D Spanning Tree Protocol; • RSTP – IEEE 802.1W Rapid Spanning Tree Protocol; Значение по умолчанию: RSTP.
14	Настроить приоритет связующего дерева STP.	**esr(config-bridge)# spanning-tree priority <PRIORITY>**	<PRIORITY> – приоритет, указывается в диапазоне с шагом 4096 [0..61440]. Значение по умолчанию: 32768.
15	Запретить работу протокола STP на конфигурируемом интерфейсе.	**esr(config-if-gi)# spanning-tree disable**	
16	Установить метод определения ценности пути.	**esr(config-if-gi)# spanning-tree cost**	<COST> – стоимость пути, устанавливается в диапазоне [1..20000000]. Значение по умолчанию: 4.
17	Разрешить установить этот порт в качестве root.	**esr(config-if-gi)# spanning-tree guard root**	

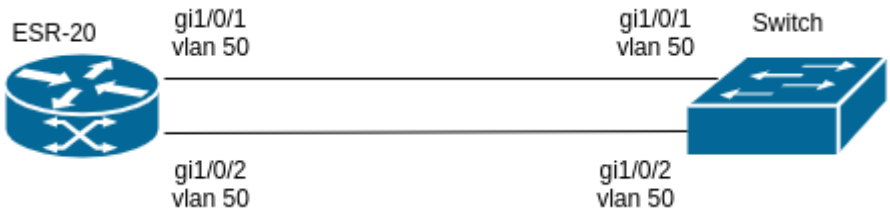
Шаг	Описание	Команда	Ключи
18	Установить протокол RSTP в передающее состояние и определить тип связи для выбранного порта – «точка-точка», «разветвлённый».	**esr(config-if-gi)# spanning-tree link-type {point-to-point|shared}**	point-to-point – команда определяет интерфейс как «точка-точка»; shared – команда определяет интерфейс как «разветвленный». Значение по умолчанию: point-to-point.
19	Установить приоритет интерфейса в связующем дереве STP.	**esr(config-if-gi)# spanning-tree port-priority <PRIORITY>**	<PRIORITY> – приоритет, указывается в диапазоне с шагом 16 [0..240].
20	Включается режим, в котором порт, при поднятии на нем линка, сразу переходит в состояние передачи, не дожидаясь истечения таймера.	**esr(config-if-gi)# spanning-tree portfast**	

⚠ Протокол MSTP на данный момент поддержан только на ESR-1000, соответственно команды для настройки MSTP есть только на нем.

10.7.2 Пример настройки

Задача:

Настроить на маршрутизаторе протокол STP для предотвращения петли с интервалом прослушивания и изучения сети 10 секунд и временем жизни связующего дерева 15 секунд.



Решение:

Для примера разберём схему с маршрутизатором и коммутатором соединенных двумя линками.

По умолчанию на ESR включен протокол RSTP.

Перейдём в режим конфигурирования:

```
esr-20# configure
```

Зададим протокол по умолчанию STP:

```
esr-20(config)# spanning-tree mode stp
```

Установим время жизни связующего дерева – 15 секунд и интервал прослушивания и изучения сети – 10 секунд:

```
esr-20(config)# spanning-tree max-age 15
esr-20(config)# spanning-tree forward-time 10
```

Вывод команды show spanning-tree active:

```
esr-20# show spanning-tree active
Protocol version: STP
          Root ID: [32768] a8:f9:4b:ad:5a:00
                    Root port: [128] gi1/0/1
                    Pathcost 32768
                    Message Age 300
                    Hello time: 2 Max age time: 20 Forward delay: 15
         Bridge ID: [32768] a8:f9:4b:ad:8e:5d
                    Hello time: 2 Max age time: 15 Forward delay: 10
                    Transmit hold count: 6 Topology change: 0
                    Time since topology change: 16 Topology change count: 2
Name            State    Prio.Num    Cost         Status      Role        PortFast    Type
-------------   -----    --------    ----------   --------    --------    --------
---------------------
gi1/0/1         en       128.2       32768        FRW         Root        No          STP
gi1/0/2         en       128.3       32768        BLK         Altr        No          STP
```

10.8 Настройка PPP через E1

PPP (англ. *Point-to-Point Protocol*) — двухточечный протокол канального уровня, используется для установления прямой связи между двумя узлами сети. Может обеспечить аутентификацию соединения, шифрование и сжатие данных.

Для установления PPP-соединения через поток E1 необходимо наличие медиаконвертера TOPGATE-WAN-E1 в маршрутизаторе или контроллере.

10.8.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
Предварительная настройка:			
1	Необходимо включить поддержку Jumbo-фреймов. Для вступления изменений в силу требуется перезагрузка устройства.	**esr(config)# system jumbo-frames**	
Настройка физического интерфейса:			
2	Необходимо выбрать интерфейс, в котором установлен TOPGATE-WAN-E1.	**esr(config)# interface gigabitethernet 1/0/3**	

Шаг	Описание	Команда	Ключи
3	Перевести физический интерфейс в режим коммутации.	**esr(config-if-gi)# mode switchport**	
4	Задать режим работы интерфейса E1.	**esr(config-if-gi)# switchport mode e1**	
5	Задать источник синхронизации (не обязательно).	**esr(config-if-gi)# switchport e1 clock source <SOURCE>**	<SOURCE> – источник синхронизации: • **internal** (по умолчанию) – синхронизироваться с внутренним источником; • **line** – синхронизироваться с линейным сигналом.
6	Указать размер MTU (Maximum Transmition Unit) для физических интерфейсов.	**esr(config-if-gi)# mtu <MTU>**	<MTU> – значение MTU, для E1 и Multilink интерфейсов необходимо указать значения в диапазоне [1510..9600].
7	Задать хэш-алгоритм проверки кадра (не обязательно).	**esr(config-if-gi)# switchport e1 crc <FCS>**	<FCS> – последовательность проверки кадра: • **16** (по умолчанию) – FCS16; • **32** – FCS32.
8	Задать проверку на наличие ошибок при передаче (не обязательно).	**esr(config-if-gi)# switchport e1 framing <CRC>**	<CRC> – проверка циклической избыточности: • **crc-4** – использовать алгоритм CRC-4; • **no-crc4** (по умолчанию) – не использовать проверку.
9	Задать инвертирование передаваемых бит (не обязательно).	**esr(config-if-gi)# switchport e1 invert data**	
10	Задать тип линейного кодирования (не обязательно).	**esr(config-if-gi)# switchport e1 linecode <CODE>**	<CODE> – тип линейного кодирования; • **ami** – чередующейся полярностью импульсов; • **hdb3** (по умолчанию) – двухполярный код высокой плотности порядка 3.

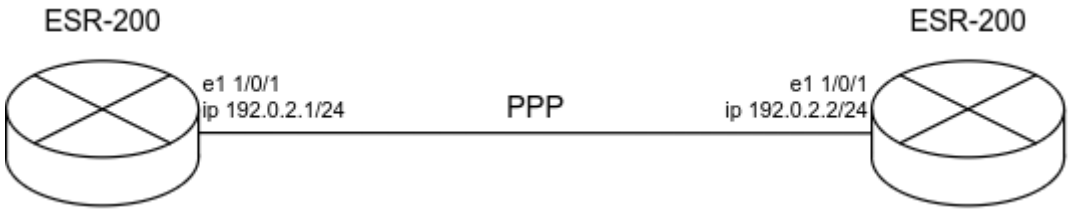
Шаг	Описание	Команда	Ключи
11	Задать количество тайм-слотов.	**esr(config-if-gi)# switchport e1 timeslots <RANGE>**	<RANGE> – количество тайм-слотов.
12	Использовать E1 как единую сущность, без таймслотов (не обязательно).	**esr(config-if-gi)# switchport e1 unframed**	
Настройка интерфейса E1:			
13	Необходимо выбрать интерфейс E1.	**esr(config)# interface e1 1/<SLOT>/1**	<SLOT> – номер слота.
14	Указать IPv4 и маску подсети для конфигурируемого интерфейса.	**esr(config-e1)# ip address <ADDR/LEN>**	<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].
15	Отключить на интерфейсе функции Firewall или включить интерфейс в зону безопасности (см. раздел Конфигурирование Firewall).	**esr(config-e1)# ip firewall disable**	
		esr(config-e1)# security-zone <NAME>	<NAME>-имя зоны безопасности, задаётся строкой до 31 символа.
Дополнительные настройки PPP для E1:			
16	Включить CHAP-аутентификацию для PPP (не обязательно).	**esr(config-e1)# ppp authentication chap**	
17	Задать имя маршрутизатора, которое отправляется удаленной стороне для прохождения CHAP-аутентификации (не обязательно).	**esr(config-e1)# ppp chap hostname <NAME>**	<NAME> – имя маршрутизатора.
18	Задать пароль для аутентификации (не обязательно).	**esr(config-e1)# ppp chap password ascii-text <CLEAR-TEXT>**	<CLEAR-TEXT> – пароль в открытой форме, задаётся строкой [1 .. 64] символов, может включать символы [0-9a-fA-F].
19	Включить игнорирование аутентификации (не обязательно).	**esr(config-e1)# ppp chap refuse**	
20	Задать имя пользователя для аутентификации (не обязательно).	**esr(config-e1)# ppp chap username <NAME>**	<NAME> – имя пользователя.

Шаг	Описание	Команда	Ключи
21	Разрешается принимать от соседа любой ненулевой IP-адрес в качестве локального IP-адреса (не обязательно).	**esr(config-e1)# ppp ipcp accept-address**	
22	Задать IP-адрес, который отправляется удаленной стороне для последующего его присвоения (не обязательно).	**esr(config-e1)# ppp ipcp remote-address <ADDR>**	<ADDR> – IP-адрес удаленного шлюза.
23	Задать количество попыток отправки Configure-Request пакетов, прежде чем удаленный пир будет признан неспособным ответить (не обязательно).	**esr(config-e1)# ppp max-configure <VALUE>**	<VALUE> – количество попыток.
24	Задать количество попыток отправки Configure-NAK пакетов, прежде чем будут подтверждены все опции (не обязательно).	**esr(config-e1)# ppp max-failure <VALUE>**	<VALUE> – количество попыток.
25	Задать количество попыток отправки Terminate-Request пакетов, прежде чем сессия будет прервана (не обязательно).	**esr(config-e1)# ppp max-terminate <VALUE>**	<VALUE> – количество попыток.
26	Задать размер MRU (Maximum Receive Unit) для интерфейса (не обязательно).	**esr(config-e1)# ppp mru <MRU>**	<MRU> – значение MRU.
27	Задается интервал времени в секундах, по истечении которого маршрутизатор отправляет keepalive-сообщение (не обязательно).	**esr(config-e1)# ppp timeout keepalive <TIME>**	<TIME> – время в секундах.
28	Задается интервал, по истечении которого маршрутизатор повторяет запрос на установление сессии (не обязательно).	**esr(config-e1)# ppp timeout retry <TIME>**	<TIME> – время в секундах.
Включение интерфейса E1 в Multilink PPP:			
29	Добавить в MLPPP-группу (не обязательно).	**esr(config-e1)# ppp multilink-group <GROUP-ID>**	<GROUP-ID> – номер группы.
30	Включение режима MLPPP (не обязательно).	**esr(config-e1)# ppp multilink**	

10.8.2 Пример конфигурации

Задача:

Настроить PPP-соединение со встречной стороной с IP-адресом 192.0.2.2/24 через TOPGATE-WAN-E1, используя 1-8 канальные интервалы для передачи данных.



Решение:

Предварительно необходимо настроить system jumbo-frames, сохранить изменения в конфигурации и перезагрузить маршрутизатор:

```
esr(config)# system jumbo-frames
esr(config)# exit
esr# commit
esr# confirm
esr# reload system
Do you really want to reload system ? (y/N): y
```

Настроим физический интерфейс gigabitethernet 1/0/3, в котором установлен TOPGATE-WAN-E1:

- Укажем mtu не менее 1510.
- Переведем интерфейс в режим работы e1.
- Укажем канал e1 – 0.
- Укажем интервал каналов e1 – 1-8.

```
esr# configure
esr(config)# interface gigabitethernet 1/0/3
esr(config-if-gi)# mode switchport
esr(config-if-gi)# mtu 1510
esr(config-if-gi)# switchport mode e1
esr(config-if-gi)# switchport e1 slot 0
esr(config-if-gi)# switchport e1 timeslots 1-8
esr(config-if-gi)# exit
```

Настроим интерфейс e1:

```
esr(config)# interface e1 1/0/1
esr(config-e1)# ip address 192.0.2.1/24
esr(config-e1)# security-zone trusted
esr(config-e1)# exit
```

Информацию о физическом состоянии e1 можно узнать с помощью следующей команды:

```
esr# show controllers e1 gigabitethernet 1/0/3
Interface 'gi1/0/3':
 SFP present:     Yes
 SFP Vendor name: --
 is te:    No
 SFP Vendor PN:   --
 SFP SW Version:  LPOS 1.0.9.4SR42 (20.12.2017) [
 Line code:       HDB3
 Clock source:    Internal
 Timeslot:        1-8
 Invert Data:     No
 Framing CRC4:    No
 Loopback:        --
 CRC algorithm:   FCS16
 E1 Link:         Up
 E1 Synced:       Yes
 E1 RX AIS:       No
 E1 RX RAI:       No
 E1 TX AIS:       No
```

Информацию о состоянии e1-интерфейса можно узнать с помощью следующей команды:

```
esr# show interfaces status e1 1/0/1
Interface 'e1 1/0/1' status information:
 Description:          --
 Operational state:    Up
 Administrative state: Up
 Track ID:             0
 Supports broadcast:   No
 Supports multicast:   Yes
 MTU:                  1492
 MAC address:          none
 Last change:          1 minute and 3 seconds
 Mode:                 routerport
```

10.9 Настройка MLPPP

Multilink PPP (MLPPP) предоставляет собой агрегированный канал, включающий в себя методы для распространения трафика через несколько физических каналов, имея одно логическое соединение. Этот вариант позволяет расширить пропускную способность и обеспечивает балансировку нагрузки.

10.9.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Настроить группу агрегации.	**esr(config)# interface multilink <IF>**	<IF> – наименование интерфейса.
2	Указать описание конфигурируемой группы агрегации (не обязательно).	**esr(config-multilink)# description <DESCRIPTION>**	<DESCRIPTION> – описание группы агрегации, задаётся строкой до 255 символов.
3	Задать интервал времени, за который усредняется статистика о нагрузке на группе агрегации (не обязательно).	**esr(config-multilink)# load-average <TIME>**	<TIME> – интервал в секундах, принимает значения [5..150]. Значение по умолчанию: 5.
4	Указать размер MTU (Maximum Transmition Unit) для группы агрегации (не обязательно). MTU более 1500 будет активно только в случае применения команды "system jumbo-frames".	**esr(config-multilink)# mtu <MTU>**	<MTU> – значение MTU, принимает значения в диапазоне [1280..1500]. Значение по умолчанию: 1500.
5	Включить CHAP-аутентификацию.	**esr(config-multilink)# ppp authentication chap**	
6	Включить игнорирование аутентификации (не обязательно).	**esr(config-multilink)# ppp chap refuse**	
7	Указать имя маршрутизатора/ контроллера, которое отправляется удаленной стороне для прохождения CHAP-аутентификации.	**esr(config-multilink)# ppp chap hostname <NAME>**	<NAME> – имя маршрутизатора/ контроллера, задаётся строкой до 31 символа
8	Указать пароль, который отправляется удаленной стороне вместе с именем маршрутизатора/ контроллера для прохождения CHAP-аутентификации.	**esr(config-multilink)# ppp chap password ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<CLEAR-TEXT> – пароль в открытой форме, задаётся строкой [8 .. 64] символов, может включать символы [0-9a-fA-F]. <ENCRYPTED-TEXT> – пароль в зашифрованной форме, задаётся строкой [16..128] символов.

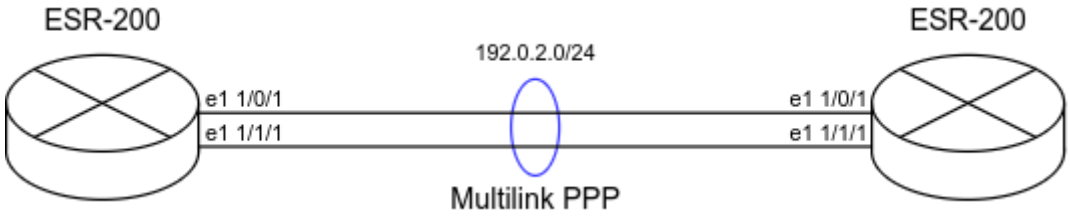
Шаг	Описание	Команда	Ключи
9	Разрешить принимать от соседа любой ненулевой IP-адрес в качестве локального IP-адреса (не обязательно).	**esr(config-multilink)# ppp ipcp accept-address**	
10	Установить IP-адрес, который отправляется удаленной стороне для последующего его присвоения.	**esr(config-multilink)# ppp iccp remote-address <ADDR>**	<ADDR> – IP-адрес удаленного шлюза.
11	Указать пользователя для аутентификации удаленной стороны и перейти в режим конфигурирования указанного пользователя.	**esr(config-multilink)# chap username <NAME>**	<NAME> – имя пользователя, задаётся строкой до 31 символа.
12	Установить пароль в открытой или зашифрованной форме определенному пользователю для аутентификации удаленной стороны.	**esr(config-ppp-user)# password ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<CLEAR-TEXT> – пароль в открытой форме, задаётся строкой [8 .. 64] символов, может включать символы [0-9a-fA-F]. <ENCRYPTED-TEXT> – пароль в зашифрованной форме, задаётся строкой [16..128] символов.
13	Установить количество попыток отправки Configure-Request пакетов, прежде чем удаленный пир будет признан неспособным ответить (не обязательно).	**esr(config-multilink)# ppp max-configure <VALUE>**	<VALUE> – время в секундах, принимает значения [1..255]. Значение по умолчанию: 10.
14	Установить количество попыток выслать Configure-NAK пакеты, прежде чем будут подтверждены все опции (не обязательно).	**esr(config-multilink)# ppp max-failure <VALUE>**	<VALUE> – время в секундах, принимает значения [1..255].
15	Установить количество попыток выслать Terminate-Request пакеты, прежде чем сессия будет прервана (не обязательно).	**esr(config-multilink)# ppp max-terminate <VALUE>**	<VALUE> – время в секундах, принимает значения [1..255]. Значение по умолчанию: 2.
16	Указать размер MRU (Maximum Receive Unit) для интерфейса.	**esr(config-multilink)# ppp mru <MRU>**	<MRU> – значение MRU, принимает значения в диапазоне [128..1485]. Значение по умолчанию: 1500.
17	Указать интервал времени в секундах, по истечении которого маршрутизатор/контроллер отправляет keepalive-сообщение (не обязательно).	**esr(config-multilink)# ppp timeout keepalive <TIME>**	<TIME> – время в секундах, принимает значения [1..32767]. Значение по умолчанию: 10.

Шаг	Описание	Команда	Ключи
18	Установить интервал времени в секундах, по истечении которого маршрутизатор/контроллер повторяет запрос на установление сессии (не обязательно).	**esr(config-multilink)# ppp timeout retry <TIME>**	<TIME> – время в секундах, принимает значения [1..255]. Значение по умолчанию: 3.
19	Определить максимальный размер пакета для MLPP-интерфейса.	**esr(config-multilink)# mrru <MRRU>**	<MRRU> – максимальный размер принимаемого пакета для MLPP-интерфейса, принимает значение в диапазоне [1500..10000].
20	Привязать порт e1 к физическому интерфейсу.	**esr(config-if-gi)# switchport e1 <SLOT>**	<SLOT> – идентификатор слота, принимает значение в диапазоне [0..3].
21	Перевести физический порт в режим работы с SFPe1-модулем.	**esr(config-if-gi)# switchport mode e1**	
22	Включить режим MLPPP на E1-интерфейсе.	**esr(config-e1)# ppp multilink**	
23	Включить E1-интерфейс в группу агрегации.	**esr(config-e1)# ppp multilink-group <GROUP-ID>**	<GROUP-ID> – идентификатор группы, принимает значение [1..4].

10.9.2 Пример настройки

Задача:

Настроить MLPPP-соединение с встречной стороной с IP-адресом 192.0.2.2/24 через интерфейсы e1 1/0/1 и e1 1/1/1. Для построения агрегированного канала PPP используются интерфейсы gi 1/0/3 и gi 1/0/4, в которые вставлены TOPGATE-WAN-E1.



Решение:

Предварительно необходимо настроить system jumbo-frames, сохранить изменения в конфигурации и перезагрузить маршрутизатор:

```
esr# configure
esr(config)# system jumbo-frames
esr(config)# exit
esr# commit
esr# confirm
esr# reload system
Do you really want to reload system ? (y/N): y
```

Настроим физические интерфейсы gigabitethernet 1/0/3-4, в которых установлены TOPGATE-WAN-E1. При настройке физических интерфейсов укажем mtu не менее 1510, переведем интерфейс в режим работы e1, укажем канал e1:

```
esr# configure
esr(config)# interface gigabitethernet 1/0/3
esr(config-if-gi)# mode switchport
esr(config-if-gi)# mtu 1510
esr(config-if-gi)# switchport mode e1
esr(config-if-gi)# switchport e1 slot 0
esr(config-if-gi)# switchport e1 timeslots 1-31
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/4
esr(config-if-gi)# mode switchport
esr(config-if-gi)# mtu 1510
esr(config-if-gi)# switchport mode e1
esr(config-if-gi)# switchport e1 slot 1
esr(config-if-gi)# switchport e1 timeslots 1-31
esr(config-if-gi)# exit
```

Настроим интерфейс multilink:

```
esr(config)# interface multilink 3
esr(config-multilink)# ip address 192.0.2.1/24
esr(config-multilink)# security-zone trusted
esr(config-multilink)# exit
```

Привяжем интерфейсы E1 к Multilink PPP. При настройке e1-интерфейса необходимо указать multilink-group и включить multilink:

```
esr(config)# interface e1 1/0/1
esr(config-e1)# ppp multilink-group 3
esr(config-e1)# ppp multilink
esr(config-e1)# exit
esr(config)# interface e1 1/1/1
esr(config-e1)# ppp multilink-group 3
esr(config-e1)# ppp multilink
esr(config-e1)# exit
```

Информацию о состоянии multilink интерфейса есть возможность узнать с помощью следующей команды:

```
esr# show interfaces status multilink 3
Interface 'mu1' status information:
 Description:          --
 Operational state:    Up
 Administrative state: Up
 Track ID:             0
 Supports broadcast:   No
 Supports multicast:   Yes
 MTU:                  1492
 MAC address:          none
 Last change:          6 seconds
 Mode:                 routerport
```

10.10 Настройка Bridge

Bridge (мост) — это способ соединения двух 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.

10.10.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Добавить сетевой мост (bridge) в систему и перейти в режим настройки его параметров.	**esr(config)# bridge <BRIDGE-ID>**	<BRIDGE-ID> – идентификационный номер моста, принимает значения в диапазоне: • для ESR-10/12V(F)/ 14VF/15 – [1..50]; • для ESR-20/21/30/100/200 – [1..250]; • для ESR-1000/1200/1500 /1511/1700/3100/3200 – [1..500].
2	Активировать сетевой мост.	**esr(config-bridge)# enable**	
3	Указать экземпляр VRF, в котором будет работать данный интерфейс (не обязательно).	**esr(config-bridge)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.
4	Назначить описание конфигурируемому сетевому мосту (не обязательно).	**esr(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).	**esr(config-if-gi)# bridge-group <BRIDGE-ID>** **esr(config-if-l2tpv3)# bridge-group <BRIDGE-ID>**	<BRIDGE-ID> – идентификационный номер моста, принимает значения в диапазоне: • для ESR-10/12V(F)/ 14VF/15 – [1..50]; • для ESR-20/21/30/100/200 и WLC-30 – [1..250]; • для ESR-1000/1200/1500 /1511/1700/3100/3200 – [1..500].

Шаг	Описание	Команда	Ключи
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).	**esr(config-bridge)# vlan <VID>**	<VID> – идентификатор VLAN, задаётся в диапазоне [1..4094].
7	Указать размер MTU (Maximum Transmition 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"	**esr(config-bridge)# mtu <MTU>**	<MTU> – значение MTU, принимает значения в диапазоне: • для ESR-10/12V(F)/ 14VF/15 – [552..9600]; • для ESR-20/21/30 и WLC-30 – [552..9500]; • для ESR-100/200/1000/1200/1500/1511/1700 – [552..10000] • для ESR-1500/1511/1700 /3100/3200 – [552..9190]. Значение по умолчанию: 1500.
8	Указать IPv4/IPv6-адрес и маску подсети для конфигурируемого интерфейса или включить получение IP-адреса динамически.	**esr(config-bridge)# ip address <ADDR/LEN>**	<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]. Дополнительные функции IPv4-адресации см. в разделе Настройка IP-адресации.

Шаг	Описание	Команда	Ключи
		esr(config-bridge)# 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 UIPv4/IPv6-адресов перечислением через запятую. Может быть назначено до 8 IPv4/IPv6-адресов на интерфейс.
		esr(config-bridge)# ip address dhcp	Дополнительные функции при работе DHCP-клиента см. в разделе Управление DHCP-клиентом.
9	Отключить на интерфейсе функции Firewall или включить интерфейс в зону безопасности (см. раздел Конфигурирование Firewall).	**esr(config-bridge)# ip firewall disable**	
		esr(config-bridge)# security-zone <NAME>	<NAME>-имя зоны безопасности, задаётся строкой до 31 символа.
10	Включить запись статистики использования текущего интерфейса (не обязательно).	**esr(config-bridge)# history statistics**	
11	Задать интервал времени, за который усредняется статистика о нагрузке на bridge (не обязательно).	**esr(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).	**esr(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; применимо только на ESR-1000/1200/1500/1511/1700 /3100).	**esr(config-bridge)# protected-ports [exclude vlan]**	exclude vlan – при указании данного ключа, VLAN (связанный с bridge) исключается из списка изолируемых интерфейсов.
14	Запретить коммутацию трафика unknown-unicast (когда MAC-адрес назначения не содержится в таблице коммутации) в данном bridge. (не обязательно; применимо только на ESR-1000/1200/1500/1511/1700 /3100).	**esr(config-bridge)# unknown-unicast-forwarding disable**	
15	Установить время жизни IPv4/IPv6-записей в ARP-таблице, изученных на данном bridge (не обязательно).	**esr(config-bridge)# ip arp reachable-time <TIME>** или **esr(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);
- proxy (см. раздел Проксирование HTTP/HTTPS-трафика);
- мониторинг траффика (см. разделы Настройка Netflow и Настройка sFlow);
- функционал протоколов маршрутизации (см. раздел Управление маршрутизацией);
- протокол VRRF (см. раздел Управление резервированием);
- функционал BRAS (см. раздел Управление BRAS (Broadband Remote Access Server));
- функционал IDS/IPS (см. раздел Настройка IPS/IDS).

10.10.2 Пример настройки bridge для VLAN и L2TPv3-туннеля

Задача:

Объединить в единый L2-домен интерфейсы устройства, относящиеся к локальной сети, и L2TPv3-туннель, проходящий по публичной сети. Для объединения использовать VLAN 333.

Решение:

Создадим VLAN 333:

```
esr(config)# vlan 333
esr(config-vlan)# exit
```

Создадим зону безопасности «trusted»:

```
esr(config)# security-zone trusted
esr(config-zone)# exit
```

Добавим интерфейсы gi1/0/11, gi1/0/12 в VLAN 333:

```
esr(config)# interface gigabitethernet 1/0/11-12
esr(config-if)# mode switchport
esr(config-if)# switchport general allowed vlan add 333 tagged
```

Создадим bridge 333, привяжем к нему VLAN 333 и укажем членство в зоне «trusted»:

```
esr(config)# bridge 333
esr(config-bridge)# vlan 333
esr(config-bridge)# security-zone trusted
esr(config-bridge)# enable
```

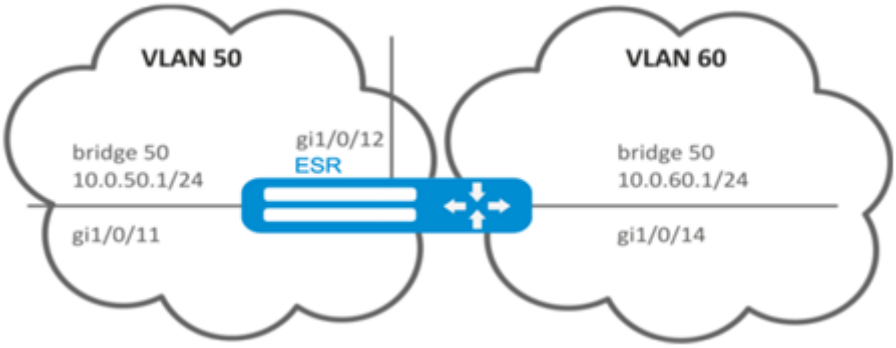
Установим принадлежность L2TPv3-туннеля к мосту, который связан с локальной сетью (настройка L2TPv3-туннеля рассматривается в разделе Настройка L2TPv3-туннелей). В общем случае идентификаторы моста и туннеля не должны совпадать с VID как в данном примере.

```
esr(config)# tunnel l2tpv3 333
esr(config-l2tpv3)# bridge-group 333
```

10.10.3 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», разрешить свободную передачу трафика между зонами.



Решение:

Создадим VLAN 50, 60:

```
esr(config)# vlan 50,60
esr(config-vlan)# exit
```

Создадим зоны безопасности «LAN1» и «LAN2»:

```
esr(config)# security-zone LAN1
esr(config-zone)# exit
esr(config)# security-zone LAN2
esr(config-zone)# exit
```

Назначим интерфейсам gi1/0/11, gi1/0/12 VLAN 50:

```
esr(config)# interface gigabitethernet 1/0/11-12
esr(config-if-gi)# switchport general allowed vlan add 50 tagged
```

Назначим интерфейсу gi1/0/14 VLAN 60:

```
esr(config)# interface gigabitethernet 1/0/14
esr(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»:

```
esr(config)# bridge 50
esr(config-bridge)# vlan 50
esr(config-bridge)# ip address 10.0.50.1/24
esr(config-bridge)# security-zone LAN1
esr(config-bridge)# enable
```

Создадим bridge 60, привяжем VLAN 60, укажем IP-адрес 10.0.60.1/24 и членство в зоне «LAN2»:

```
esr(config)# bridge 60
esr(config-bridge)# vlan 60
esr(config-bridge)# ip address 10.0.60.1/24
esr(config-bridge)# security-zone LAN2
esr(config-bridge)# enable
```

Создадим правила в Firewall, разрешающие свободное прохождение трафика между зонами:

```
esr(config)# security zone-pair LAN1 LAN2
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# security zone-pair LAN2 LAN1
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# exit
```

Посмотреть членство интерфейсов в мосте можно командой:

```
esr# show interfaces bridge
```

10.10.4 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:

```
esr(config)# bridge 1
esr(config-bridge)# enable
esr(config-bridge)# exit
```

Включим интерфейс gigabitethernet 1/0/1 в bridge 1:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# bridge-group 1
esr(config-if-gi)# exit
```

Включим саб-интерфейс gigabitethernet 1/0/2.828 в bridge 1:

```
esr(config)# interface gigabitethernet 1/0/2.828
esr(config-subif)# bridge-group 1
esr(config-subif)# 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.

10.11 Настройка Dual-Homing

В текущей версии ПО данный функционал поддерживается только на маршрутизаторе ESR-1000.

Dual-Homing – технология резервирования соединений, позволяет организовать надежное соединение ключевых ресурсов сети на основе наличия резервных линков.

10.11.1 Алгоритм настройки

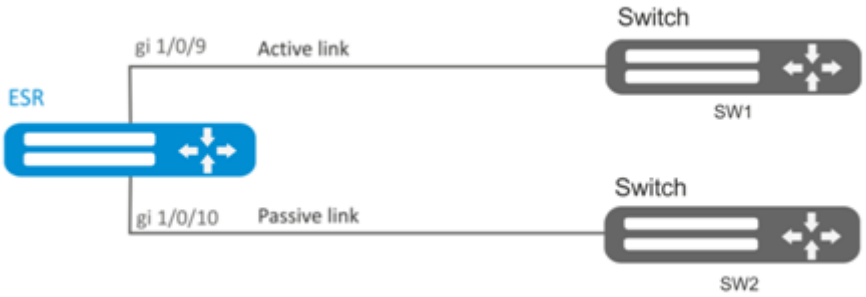
Шаг	Описание	Команда	Ключи
1	Указать резервный интерфейс, на который будет происходить переключение при потере связи на основном.	**esr(config-if-gi)# backup interface<IF> vlan <VID>**	<IF> – интерфейс, на который будет происходить переключение. <VID> – идентификационный номер VLAN, задаётся в диапазоне [2…4094]. Можно также задать диапазоном через «-» или перечислением через «,».
2	Указать количество копий пакетов с одним и тем же MAC-адресом, которые будут отправлены в активный интерфейс при переключении (не обязательно).	**esr(config)# backup-interface mac-duplicate <COUNT>**	<COUNT> – количество копий пакетов, принимает значение [1..4].
3	Указать количество пакетов в секунду, которое будет отправлено в активный интерфейс при переключении (не обязательно).	**esr(config)# backup-interfacemac-per-second<COUNT>**	<COUNT> – количество MAC-адресов в секунду, принимает значение [50..400].

Шаг	Описание	Команда	Ключи
4	Указать, что необходимо осуществить переключение на основной интерфейс при восстановлении связи (не обязательно).	**esr(config)# backup-interface preemption**	

10.11.2 Пример настройки

Задача:

Организовать резервирование L2-соединений маршрутизатора ESR для VLAN 50-55 через устройства SW1 и SW2.



Решение:

Предварительно нужно выполнить следующие действия:

Создадим VLAN 50-55:

```
esr(config)# vlan 50-55
```

Необходимо отключить STP на интерфейсах gigabitethernet 1/0/9 и gigabitethernet 1/0/10, так как совместная работа данных протоколов невозможна:

```
esr(config)# interface gigabitethernet 1/0/9-10
esr(config-if-gi)# spanning-tree disable
```

Интерфейсы gigabitethernet 1/0/9 и gigabitethernet 1/0/10 добавим в VLAN 50-55 в режиме general:

```
esr(config-if-gi)# switchport general allowed vlan add 50-55
esr(config-if-gi)# exit
```

Основной этап конфигурирования:
Сделаем интерфейс gigabitethernet 1/0/10 резервным для gigabitethernet 1/0/9:

```
esr(config)# interface gigabitethernet 1/0/9
esr(config-if-gi)# backup interface gigabitethernet 1/0/10 vlan 50-55
```

Просмотреть информацию о резервных интерфейсах можно командой:

```
esr# show interfaces backup
```

10.12 Настройка зеркалирования (SPAN/RSPAN)

> ⚠ **В текущей версии ПО функциональность удаленного зеркалирования (RSPAN) поддерживается только на маршрутизаторах ESR-1000/1200/1500/1511/1700.**

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).

10.12.1 Алгоритм настройки

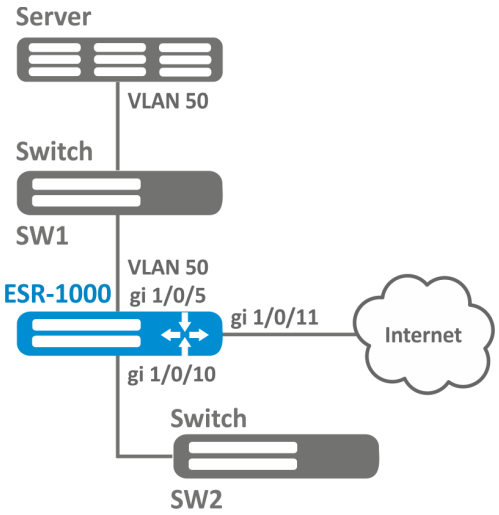
Шаг	Описание	Команда	Ключи
1	Определить VLAN, по которому будет передаваться отзеркалированный трафик (в случае использования удаленного зеркалирования).	**esr(config)# port monitor remote vlan <VID> <DIRECTION>**	<VID> – идентификационный номер VLAN, задаётся в диапазоне [2…4094]; <DIRECTION> – направление 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).	**esr(config)# port monitor remote**	
3	Определить режим порта передающего отзеркалированный трафик (не обязательно).	**esr(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.	**esr(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.

10.12.2 Пример настройки

Задача:

Организовать удаленное зеркалирование трафика по VLAN 50 с интерфейса gi1/0/11 для передачи на сервер для обработки.



Решение:

Предварительно нужно выполнить следующие действия:

- Создать VLAN 50;
- На интерфейсе gi 1/0/5 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 1/0/5 укажем порт для зеркалирования:

```
esr1000(config)# interface gigabitethernet 1/0/5
esr1000(config-if-gi)# port monitor interface gigabitethernet 1/0/11
```

Укажем на интерфейсе gi 1/0/5 режим удаленного зеркалирования:

```
esr1000(config-if-gi)# port monitor remote
```

10.13 Настройка LACP

LACP — протокол для агрегирования каналов, позволяет объединить несколько физических каналов в один логический. Такое объединение позволяет увеличивать пропускную способность и надежность канала.

10.13.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Установить приоритет системы для протокола LACP.	**esr(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.	**esr(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.

Шаг	Описание	Команда	Ключи
3	Установить административный таймаут протокола LACP.	**esr(config)# lacp timeout {short | long }**	• **long** – длительное время таймаута; • **short** – короткое время таймаута. Значение по умолчанию: long.
4	Создать и перейти в режим конфигурирования агрегированного интерфейса.	**esr(config)# interface port-channel <ID>**	<ID> – порядковый номер группы агрегации каналов, принимает значения [1..12].
5	Настроить необходимые параметры агрегированного канала.		
6	Перейти в режим конфигурирования физического интерфейса.	**esr(config)# interface <IF-TYPE><IF-NUM>**	<IF-TYPE> тип интерфейса (gigabitethernet или tengigabitethernet). <IF-NUM> – F/S/P – F-фрейм (1), S – слот (0), P – порт.
7	Включить физический интерфейс в группу агрегации каналов с указанием режима формирования группы агрегации каналов.	**esr(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.
8	Установить LACP-приоритет интерфейса Ethernet.	**esr(config-if-gi)# lacp port-priority <PRIORITY>**	<PRIORITY> – приоритет, указывается в диапазоне [1..65535]. Значение по умолчанию: 1.
9	Установить интервал времени, в течение которого собирается статистика о нагрузке на саб-интерфейс (не обязательно).	**esr(config-subif)# load-average <TIME>**	<TIME> – интервал в секундах, принимает значения [5..150].

Шаг	Описание	Команда	Ключи
10	Установить время жизни IPv4/IPv6 записей в ARP-таблице, изученных на данном интерфейсе (не обязательно).	**esr(config-subif)# ip arp reachable-time <TIME>** или **esr(config-subif)# 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>.
11	Изменить размер MTU (MaximumTransmitionUnit). MTU более 1500 будет активно только если применена команда "system jumbo-frames" (не обязательно).	**esr(config-subif)# mtu <MTU>**	<MTU> – значение MTU в байтах. Значение по умолчанию: 1500.
12	Включить запись статистики использования текущего интерфейса (не обязательно).	**esr(config-subif)# history statistics**	
13	Переопределить значение поля MSS (Maximum segment size) во входящих TCP-пакетах (не обязательно).	**esr(config-subif)# ip tcp adjust-mss <MSS>** **esr(config-subif)# ipv6 tcp adjust-mss <MSS>**	<MSS> – значение MSS, принимает значения в диапазоне [500..1460]. Значение по умолчанию: 1460.

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);
- proxy (см. раздел Проксирование HTTP/HTTPS-трафика);
- мониторинг траффика (см. разделы Настройка Netflow и Настройка sFlow);
- функционал протоколов маршрутизации (см. раздел Управление маршрутизацией);
- протокол VRRF (см. раздел Управление резервированием)
- функционал BRAS (см. раздел Управление BRAS (Broadband Remote Access Server));
- функционал IDS/IPS (см. раздел Настройка IPS/IDS).

10.13.2 Пример настройки

Задача:

Настроить агрегированный канал между маршрутизатором ESR/контроллером WLC и коммутатором.

Решение:

Предварительно необходимо выполнить следующие настройки:

На интерфейсах gi1/0/1, gi1/0/2 отключить зону безопасности командой «no security-zone».

Основной этап конфигурирования:

Создадим интерфейс port-channel 2:

```
esr(config)# interface port-channel 2
```

Включим физические интерфейсы gi1/0/1, gi1/0/2 в созданную группу агрегации каналов:

```
esr(config)# interface gigabitethernet 1/0/1-2
esr(config-if-gi)# channel-group 2 mode auto
```

Дальнейшая конфигурация port-channel проводится как на обычном физическом интерфейсе.

10.14 Настройка AUX

> ⚠ **Для моделей ESR-21.**

Настройка AUX используется для указания параметров взаимодействия с внешними устройствами, подключенными через последовательные интерфейсы к ESR.

10.14.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим конфигурирования последовательного интерфейса.	**esr(config)# line aux <NUM>**	<NUM> – номер последовательного интерфейса, задается в диапазоне [1..3].

Шаг	Описание	Команда	Ключи
2	Установить необходимые параметры последовательного интерфейса для взаимодействия с подключенным устройством (не обязательно). Данные параметры, как правило, указаны в инструкции подключаемого устройства. По умолчанию будут использовать стандартные значения.	**esr(config-line-aux) databits <BITS>** **esr(config-line-aux) flowcontrol <FMODE>** **esr(config-line-aux) parity <PMODE>** **esr(config-line-aux) speed <SPEED>** **esr(config-line-aux) stopbits <STOP-BITS>**	<BITS> - количество бит данных в посылке [7..8]; Значение по умолчанию "8", <FMODE> – режим управления потоком. Принимает значения: • software – программное управление потоком; • hardware – аппаратное управление потоком; • disabled – управление потоком отключено; Значение по умолчанию "disabled", <PMODE> – режим установки бита четности. Принимает значения: • odd – проверка на нечетность; • even – проверка на четность; • none – бит четности не выставляется; Значение по умолчанию "none", <SPEED> – скорость работы последовательного интерфейса в бит/с. Принимает значения: 300; 1200; 2400; 4800; 9600; 19200; 38400; 57600; 115200; Значение по умолчанию "115200", <STOP-BITS> - количество стоповых битов в посылке [1..2]; Значение по умолчанию "1".
3	Задать описание последовательного интерфейса (не обязательно).	**esr(config-line-aux)# description <DESCRIPTION>**	<DESCRIPTION> – описание интерфейса, задаётся строкой до 255 символов.

Шаг	Описание	Команда	Ключи
4	При использовании подключаемого устройства в качестве модема, перевести последовательный интерфейс в режим работы с модемом (не обязательно). Примечание: невозможно использовать совместно с командой "transport telnet port".	**esr(config-line-aux)# modem inout**	
5	При использовании ESR в качестве терминального сервера для управления подключенным устройством к последовательному интерфейсу установить номер TCP-порта, который будет использоваться в качестве номера TCP-порта для подключения к ESR по протоколу telnet (не обязательно). Примечание: невозможно использовать совместно с командой "modem inout".	**esr(config-line-aux)# transport telnet port <PORT>**	<PORT> – номер TCP-порта для режима консольного сервера. Принимает значения [1..65535].

10.14.2 Примеры настроек

Задача 1:

Настроить IP-связность между двумя ESR на Serial-порту, используя модемы в режиме Leased line (автоматический режим модемов), соединенных между собой телефонным кабелем.

Модемы должны быть предварительно введены в режим автоматической установки соединения.

Проверена совместимость с модемами Modem Zyxel U-336E Plus.

Решение:

Сконфигурировать первый ESR-21

Настроим параметры согласования:

```
esr-21-1(config)# line aux 2
esr-21-1(config-line-aux)# flowcontrol hardware
esr-21-1(config-line-aux)# exit
esr-21-1(config)#
```

Сконфигурируем необходимые RS-232 интерфейсы:

```
esr-21-1(config)# interface serial 1/0/2
esr-21-1(config-serial)# ip address 1.1.1.1/24
esr-21-1(config-serial)# exit
esr-21-1(config)#
```

Сконфигурируем firewall для зон безопасности:

```
esr-21-1(config)# security zone xx
esr-21-1(config-zone)# exit
esr-21-1(config)# security zone-pair xx self
esr-21-1(config-zone-pair)#   rule 1
esr-21-1(config-zone-pair-rule)# action permit
esr-21-1(config-zone-pair-rule)# enable
esr-21-1(config-zone-pair-rule)# exit
esr-21-1(config-zone-pair)# exit
esr-21-1(config)#
```

И укажем принадлежность интерфейсов к зоне безопасности:

```
esr-21-1(config)# interface serial 1/0/2
esr-21-1(config-serial)# security-zone xx
esr-21-1(config-serial)# exit
esr-21-1(config)#
```

Сконфигурировать второй ESR-21

Настроим параметры согласования:

```
esr-21-2(config)# line aux 2
esr-21-2(config-line-aux)# flowcontrol hardware
esr-21-2(config-line-aux)# exit
esr-21-2(config)#
```

Сконфигурируем необходимые RS-232 интерфейсы:

```
esr-21-2(config)# interface serial 1/0/2
esr-21-2(config-serial)# ip address 1.1.1.2/24
esr-21-2(config-serial)# exit
esr-21-2(config)#
```

Сконфигурируем firewall для зон безопасности:

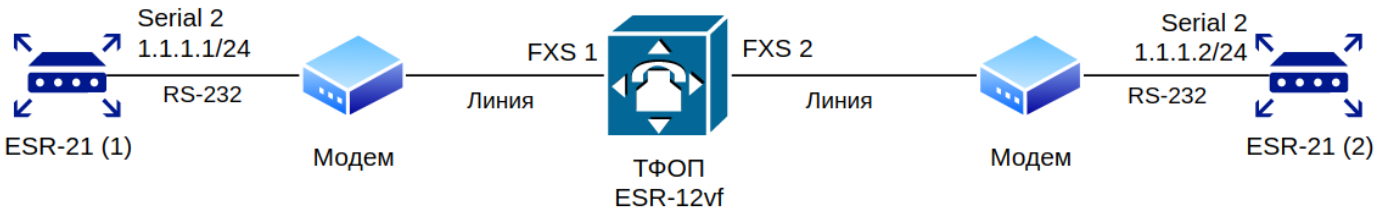
```
esr-21-2(config)# security zone xx
esr-21-2(config-zone)# exit
esr-21-2(config)# security zone-pair xx self
esr-21-2(config-zone-pair)#   rule 1
esr-21-2(config-zone-pair-rule)# action permit
esr-21-2(config-zone-pair-rule)# enable
esr-21-2(config-zone-pair-rule)# exit
esr-21-2(config-zone-pair)# exit
esr-21-2(config)#
```

И укажем принадлежность интерфейсов к зоне безопасности:

```
esr-21-2(config)# interface serial 1/0/2
esr-21-2(config-serial)# security-zone xx
esr-21-2(config-serial)# exit
esr-21-2(config)#
```

Задача 2:

Настроить IP-связность между двумя ESR на Serial-порту, используя модемы в режиме Dial-Up и телефонную сеть общего пользования (ТфОП).



В качестве эмуляции ТфОП используется ESR-12VF с нижеприведенной настройкой:

```
dialplan pattern factory_test
  description "dialplan for factory test"
  pattern "S5, L5 (00[1-3]@{local} | [xABCD*#].S)"
  enable
exit
sip profile 1
  dialplan pattern "factory_test"
  enable
  proxy primary
    enable
    ip address proxy-server 192.0.2.5
    registration
    ip address registration-server 192.0.2.5
  exit
exit
interface voice-port 1
  sip user phone 001
  profile sip 1
exit
interface voice-port 2
  sip user phone 002
  profile sip 1
  caller-id mode fsk-bell
exit
```

Проверена совместимость с модемами
- **Modem ZyXEL OMNI 56K (MINI).**
- **Modem Acorp-M56SCD.**

Решение:

Сконфигурировать первый ESR-21

Настроим параметры согласования с модемом:

```
esr-21-1(config)# line aux 2
esr-21-1(config-line-aux)# flowcontrol hardware
esr-21-1(config-line-aux)# modem inout
esr-21-1(config-line-aux)# exit
esr-21-1(config)#
```

Сконфигурируем необходимые RS-232 интерфейсы:

```
esr-21-1(config)# interface serial 1/0/2
esr-21-1(config-serial)# ip address 1.1.1.1/24
esr-21-1(config-serial)# exit
esr-21-1(config)#
```

Сконфигурируем firewall для зон безопасности:

```
esr-21-1(config)# security zone xx
esr-21-1(config-zone)# exit
esr-21-1(config)# security zone-pair xx self
esr-21-1(config-zone-pair)#   rule 1
esr-21-1(config-zone-pair-rule)# action permit
esr-21-1(config-zone-pair-rule)# enable
esr-21-1(config-zone-pair-rule)# exit
esr-21-1(config-zone-pair)# exit
esr-21-1(config)#
```

И укажем принадлежность интерфейсов к зоне безопасности:

```
esr-21-1(config)# interface serial 1/0/2
esr-21-1(config-serial)# security-zone xx
esr-21-1(config-serial)# exit
esr-21-1(config)#
```

Включим дозвон по номеру:

```
esr-21-1(config)# interface serial 1/0/2
esr-21-1(config-serial)# dialer string 002
esr-21-1(config-serial)# dialer
esr-21-1(config-serial)# exit
esr-21-1(config)#
```

Сконфигурировать второй ESR-21
Настроим параметры согласования:

```
esr-21-2(config)# line aux 2
esr-21-2(config-line-aux)# flowcontrol hardware
esr-21-2(config-line-aux)# modem inout
esr-21-2(config-line-aux)# exit
esr-21-2(config)#
```

Сконфигурируем необходимые RS-232 интерфейсы:

```
esr-21-2(config)# interface serial 1/0/2
esr-21-2(config-serial)# ip address 1.1.1.2/24
esr-21-2(config-serial)# exit
esr-21-2(config)#
```

Сконфигурируем firewall для зон безопасности:

```
esr-21-2(config)# security zone xx
esr-21-2(config-zone)# exit
esr-21-2(config)# security zone-pair xx self
esr-21-2(config-zone-pair)#   rule 1
esr-21-2(config-zone-pair-rule)# action permit
esr-21-2(config-zone-pair-rule)# enable
esr-21-2(config-zone-pair-rule)# exit
esr-21-2(config-zone-pair)# exit
esr-21-2(config)#
```

И укажем принадлежность интерфейсов к зоне безопасности:

```
esr-21-2(config)# interface serial 1/0/2
esr-21-2(config-serial)# security-zone xx
esr-21-2(config-serial)# exit
esr-21-2(config)#
```

Задача 3:

Использовать дополнительные параметры настройки модемов для задачи 2:

- для модема 1 включение протокола V.22bis,
- отключение динамиков на обоих модемах.

Решение

Создадим строку с дополнительными параметрами инициализации модема для первого ESR-21, где:

- AT&N1 – включение режима V.22bis на модеме,
- ATM0L0 – отключение динамика модема.

```
esr-21-1(config)# chat-script dial_test "ABORT 'BUSY' ABORT 'NO CARRIER' ABORT ERROR '' AT OK
AT&F OK AT&N14 OK ATM0L0 OK ATD\\T CONNECT '"
esr-21-1(config)#
```

Включим использование строки инициализации модема:

```
esr-21-1(config)# interface serial 1/0/2
esr-21-1(config-serial)# dialer string 001 modem-script dial_test
esr-21-1(config-serial)# exit
esr-21-1(config)#
```

Создадим строку с дополнительными параметрами инициализации модема для второго ESR-21:

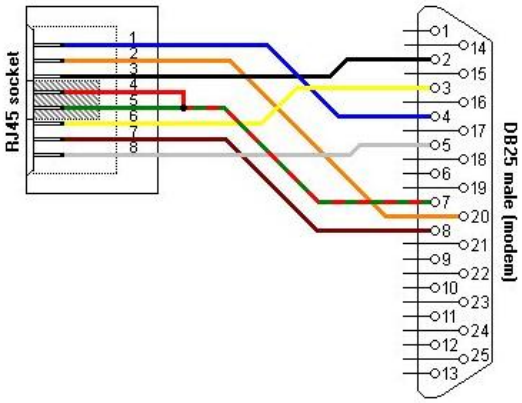
```
esr-21-2(config)# chat-script answer_test "ABORT 'BUSY' ABORT 'NO CARRIER' '' AT OK AT&F OK
ATM0L0 RING ATAr CONNECT ''"
esr-21-2(config)#
```

Включим использование строки инициализации модема:

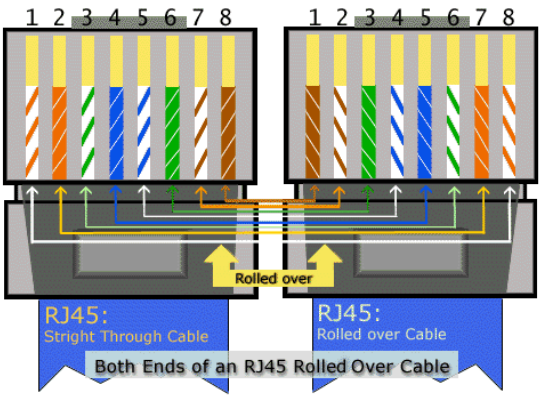
```
esr-21-2(config)# interface serial 1/0/2
esr-21-2(config-serial)# dialer string 000 modem-script answer_test
esr-21-2(config-serial)# exit
esr-21-2(config)#
```

10.14.3 Схемы распайки переходников

RJ-45 <--> DB-25 pinout



RJ-45 <--> RJ-45 pinout (rolled over cable)



11 Управление туннелированием

- Настройка GRE-туннелей
  - Алгоритм настройки
  - Пример настройки IP-GRE-туннеля
- Настройка DMVPN
  - Алгоритм настройки
  - Пример настройки 1
  - Пример настройки 2
- Настройка L2TPv3-туннелей
  - Алгоритм настройки
  - Пример настройки L2TPv3-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

11.1 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 ESR и контроллере WLC 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.

11.1.1 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.	**esr(config)# tunnel gre <INDEX>**	<INDEX> – идентификатор туннеля в диапазоне: • для ESR-10/12V(F)/ 14VF/15 – [1..10]; • для ESR-20/21/30/100/200 – [1..250]; • для ESR-1000/1200/ 1500/1511/1700/3100/ 3200 – [1..500].

Шаг	Описание	Команда	Ключи
3	Указать экземпляр VRF, в котором будет работать данный GRE-туннель (не обязательно).	**esr(config-gre)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.
4	Указать описание конфигурируемого туннеля (не обязательно).	**esr(config-gre)# description <DESCRIPTION>**	<DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов.
5	Установить локальный IP-адрес для установки туннеля.	**esr(config-gre)# local address <ADDR>**	<ADDR> – IP-адрес локального шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
		esr(config-gre)# local interface <IF>	<IF> – интерфейс, от IP-адреса которого устанавливается туннель.
6	Установить удаленный IP-адрес для установки туннеля.	**esr(config-gre)# remote address <ADDR>**	<ADDR> – IP-адрес локального шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
7	Указать режим инкапсуляции для GRE-туннеля.	**esr(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
8	Установить IP-адрес локальной стороны туннеля (только в режиме ip).	**esr(config-gre)# ip address <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]. Можно указать до 8 IP-адресов перечислением через запятую. Дополнительные функции IPv4-адресации см. в разделе Настройка IP-адресации.

Шаг	Описание	Команда	Ключи
9	Назначить широковещательный домен для инкапсуляции в GRE-пакеты данного туннеля (только в режиме ethernet).	**esr(config-gre)# bridge-group <BRIDGE-ID>**	<BRIDGE-ID> – идентификационный номер моста, принимает значения в диапазоне: • для ESR-10/12V(F)/ 14VF/15 – [1..50]; • для ESR-20/21/30/100/200 – [1..250]; • для ESR-1000/1200/ 1500/1511/1700/3100/ 3200 – [1..500].
10	Включить GRE-туннель в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall (см. раздел Конфигурирование Firewall).	**esr(config-gre)# security-zone<NAME>**	<NAME> – имя зоны безопасности, задаётся строкой до 12 символов.
		esr(config-gre)# ip firewall disable	
11	Указать размер MTU (Maximum Transmition Unit) для туннеля (не обязательно). MTU более 1500 будет активно только если применена команда "system jumbo-frames".	**esr(config-gre)# mtu <MTU>**	<MTU> – значение MTU, принимает значения в диапазоне: • для ESR-10/12V(F)/ 14VF/15 – [1280..9600]; • для ESR-20/21/30 – [1280..9500]; • для ESR-100/200/1000/ 1200/1500/1511/1700/ 3100/3200 – [1280..10000]. Значение по умолчанию: 1500.
12	Указать значение времени жизни TTL для туннельных пакетов (не обязательно).	**esr(config-gre)# ttl <TTL>**	<TTL> – значение TTL, принимает значения в диапазоне [1..255]. Значение по умолчанию: Наследуется от инкапсулируемого пакета.
13	Указать DSCP для использования в IP-заголовке инкапсулирующего пакета (не обязательно).	**esr(config-gre)# dscp <DSCP>**	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: наследуется от инкапсулируемого пакета.

Шаг	Описание	Команда	Ключи
14	Разрешить передачу ключа (Key) в туннельном заголовке GRE (в соответствии с RFC 2890) и установить значение ключа. Настраивается только с обеих сторон туннеля. (не обязательно).	**esr(config-gre)# key <KEY>**	<KEY> – значение KEY, принимает значения в диапазоне [1..2000000]. Значение по умолчанию: ключ не передаётся.
15	Включить вычисление контрольной суммы и занесение её в GRE-заголовок отправляемых пакетов. При этом на удаленной стороне необходимо включить проверку контрольной суммы. (не обязательно)	**esr(config-gre)# local checksum**	
16	Включить проверку наличия и соответствия значений контрольной суммы в заголовках принимаемых GRE-пакетов. При этом на удаленной стороне необходимо включить вычисление контрольной суммы (не обязательно).	**esr(config-gre)# remote checksum**	
17	Включить проверку доступности удаленного шлюза туннеля (не обязательно).	**esr(config-gre)# keepalive enable**	
18	Изменить время ожидания keepalive пакетов от встречной стороны (не обязательно).	**esr(config-gre)# keepalive timeout <TIME>**	<TIME> – время в секундах, принимает значения в диапазоне [1..32767]. Значение по умолчанию: 10.
19	Изменить количество попыток проверки доступности удаленного шлюза туннеля (не обязательно).	**esr(config-gre)# keepalive retries <VALUE>**	<VALUE> – количество попыток, принимает значения в диапазоне [1..255]. Значение по умолчанию: 5.
20	Указать IP-адрес для работы механизма keepalive (обязательно в режиме ethernet).	**esr(config-gre)# keepalive dst-address <ADDR>**	<ADDR> – IP-адрес для проверки работоспособности GRE-туннеля.
21	Изменить интервал времени, за который усредняется статистика о нагрузке на туннеле (не обязательно).	**esr(config-gre)# load-average <TIME>**	<TIME> – интервал в секундах, принимает значения [5..150]. Значение по умолчанию: 5.

Шаг	Описание	Команда	Ключи
22	Включить отправку snmp-trap о включении/отключении туннеля.	**esr(config-gre)# snmp init-trap**	
23	Включить механизм перезапроса IP-адресов по протоколу DHCP на указанных интерфейсах при отключении GRE-туннеля по keepalive (не обязательно).	**esr(config-gre)# keepalive dhcp dependent-interface <IF>**	<IF> – физический/ логический интерфейс, на котором включено получение IP-адреса по DHCP.
24	Задать интервал времени между отключением GRE-туннеля и перезапросом IP-адреса на интерфейсе/интерфейсах, указанных командой keepalive dhcp dependent-interface (не обязательно).	**esr(config-gre)# keepalive dhcp link-timeout <SEC>**	<SEC> – интервал между отключением GRE-туннеля и перезапросом IP-адреса по DHCP на интерфейсах.
25	Переопределить значение поля MSS (Maximum segment size) во входящих TCP-пакетах (не обязательно).	**esr(config-gre)# ip tcp adjust-mss <MSS>**	<MSS> – значение MSS, принимает значения в диапазоне [500..1460]. Значение по умолчанию: 1460.
26	Включить запись статистики использования текущего туннеля (не обязательно).	**esr(config-gre)# history statistics**	
27	Активировать туннель.	**esr(config-gre)# enable**	

Также для GRE-туннеля возможно настроить:

- QoS в базовом или расширенном режимах (см. раздел Управление QoS);
- proxy (см. раздел Проксирование HTTP/HTTPS-трафика);
- мониторинг траффика (см. разделы Настройка Netflow и Настройка sFlow);
- функционал протоколов маршрутизации (см. раздел Управление маршрутизацией);
- функционал BRAS (см. раздел Управление BRAS (Broadband Remote Access Server));

11.1.2 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 устройствах 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:

```
esr(config)# tunnel gre 10
```

Укажем локальный и удаленный шлюз (IP-адреса интерфейсов, граничащих с WAN):

```
esr(config-gre)# local address 115.0.0.1
esr(config-gre)# remote address 114.0.0.10
```

Укажем IP-адрес туннеля 25.0.0.1/24:

```
esr(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:

```
esr(config-gre)# security-zone untrusted
```

Включим туннель:

```
esr(config-gre)# enable
esr(config-gre)# exit
```

На маршрутизаторе или контроллере должен быть создан маршрут до локальной сети партнера. В качестве интерфейса назначения указываем ранее созданный туннель GRE:

```
esr(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:

```
esr(config-gre)# local checksum
```

- Включить проверку наличия и корректности контрольной суммы GRE для входящего трафика:

```
esr(config-gre)# remote checksum
```

- Указать уникальный идентификатор:

```
esr(config-gre)# key 15808
```

- Указать значение DSCP, MTU, TTL:

```
esr(config-gre)# dscp 44
esr(config-gre)# mtu 1426
esr(config-gre)# ttl 18
```

- Включить и настроить механизм keepalive:

```
esr(config-gre)# keepalive enable
esr(config-gre)# keepalive timeout <TIME>
esr(config-gre)# keepalive retries <VALUE>
```

Состояние туннеля можно посмотреть командой:

```
esr# show tunnels status gre 10
```

Счетчики входящих и отправленных пакетов можно посмотреть командой:

```
esr# show tunnels counters gre 10
```

Конфигурацию туннеля можно посмотреть командой:

```
esr# show tunnels configuration gre 10
```

Настройка туннеля IPv4-over-IPv4 производится аналогичным образом.

При создании туннеля необходимо в firewall разрешить протокол GRE (47).

11.2 Настройка DMVPN

DMVPN (*Dynamic Multipoint Virtual Private Network*) — технология для создания виртуальных частных сетей, с возможностью динамического создания туннелей между узлами. Преимуществом данного решения является высокая масштабируемость и легкость настройки при подключении филиалов к головному офису. DMVPN используется в топологии Hub-and-Spoke, и позволяет строить прямые VPN-туннели Spoke-to-Spoke в дополнение к обычным Spoke-to-Hub туннелям. Это означает, что филиалы смогут общаться друг с другом напрямую, без необходимости прохождения трафика через Hub.

Чтобы установить такое соединение, клиенты (NHC) по шифрованному IPsec-туннелю отправляют соответствие своего внутреннего (туннельного) адреса и внешнего (NBMA) адреса на NHRP-сервер (NHS). Когда клиент захочет соединиться с другим NHC, он посылает на сервер запрос, чтобы узнать его внешний адрес. Получив ответ от сервера, клиент теперь самостоятельно может устанавливать соединение с удалённым филиалом.

11.2.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Проверить доступность “внешних” IP-адресов, находящихся на физических интерфейсах.		
2	Подготовить IPsec-туннели для работы совместно с динамическими GRE-туннелями.		См. раздел Настройка Policy-based IPsec VPN.
2	Создать GRE-туннель и перейти в режим его конфигурирования.	**esr(config)# tunnel gre <INDEX>**	<INDEX> – идентификатор туннеля.
3	Перевести GRE-туннель в режим multipoint.	**esr(config-gre)# multipoint**	
4	Установить открытый пароль для NHRP пакетов (не обязательно).	**esr(config-gre)# ip nhrp authentication <WORD>**	<WORD> – пароль в открытой форме, задается строкой [1..8] символов, может включать символы [0-9a-fA-F].
5	Указать время, в течение которого на NHS будет существовать запись о данном клиенте (не обязательно).	**esr(config-gre)# ip nhrp holding-time <TIME>**	<TIME> – время в секундах, в течение которого на сервере будет существовать запись о данном клиенте, принимает значения [1..65535]. Значение по умолчанию: 7200.
6	Задать «логический(туннельный)» адрес NHRP-сервера.	**esr(config-gre)# ip nhrp nhs <ADDR> [no-registration]**	<ADDR/LEN> – адрес, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]; • **no-registration** – не регистрироваться на NHRP сервере.

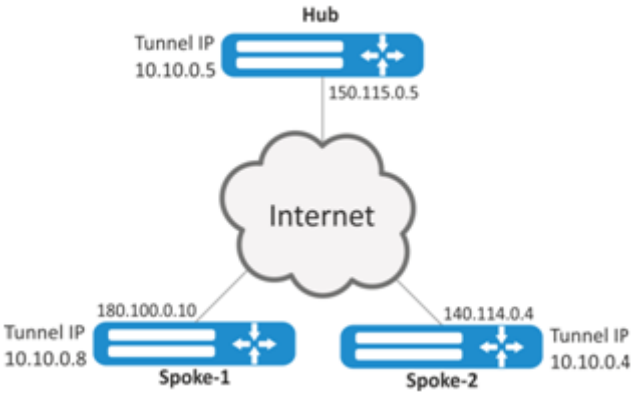
Шаг	Описание	Команда	Ключи
7	Задать соответствие «внутреннего» туннельного адреса с «внешним» NBMA-адресом.	**esr(config-gre)# ip nhrp map <ADDR> <ADDR>**	<ADDR> – IP-адрес задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
8	Определить адресата мультикастного трафика.	**esr(config-gre)# ip nhrp multicast { dynamic | nhs | <ADDR> }**	• **dynamic** – отправлять на все пиры, с которыми есть соединение; • **nhs** – отправлять на все статические сконфигурированные сервера; <ADDR> – отправлять на специфически сконфигурированный адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
9	Включить возможность отправки NHRP Traffic Indication пакетов. Выполняется на NHS (не обязательно).	**esr(config-gre)# ip nhrp redirect**	
10	Включить возможность создания кратчайших маршрутов. Выполняется на NHC (не обязательно).	**esr(config-gre)# ip nhrp shortcut**	
11	Привязать IPsec-VPN к mGRE-туннелю (не обязательно).	**esr(config-gre)# ip nhrp ipsec <WORD> { static | dynamic }**	<WORD> – имя VPN, задаётся строкой до 31 символа; • **static** – статическое соединение, применятся для связи с NHS; • **dynamic** – динамически устанавливающееся соединение, конфигурируется для связи между NHC.
12	Включить передачу группового атрибута (не обязательно).	**esr(config-gre)# ip nhrp attribute group <WORD>**	<WORD> – имя nhrp-группы, задаётся строкой [1..40] символов, не принимает символы [^#].
13	Включить работу протокола NHRP.	**esr(config-gre)# ip nhrp enable**	

Шаг	Описание	Команда	Ключи
14	Организовать IP-связность посредством протокола динамической маршрутизации.		
Остальные настройки – аналогичны настройкам статичного GRE-туннеля (см. раздел Настройка GRE-туннелей).			

11.2.2 Пример настройки 1

Задача:

Организовать DMVPN между офисами компании, используя mGRE-туннели, NHRP (Next Hop Resolution Protocol), протокол динамической маршрутизации (BGP), IPsec. В нашем примере у нас будет HUB-устройство и два филиала. HUB – это DMVPN-сервер (NHS), а филиалы – DMPVN-клиенты (NHC).



Hub внешний IP-адрес — 150.115.0.5;

Spoke-1 внешний IP-адрес — 180.100.0.10;

Spoke-2 внешний IP-адрес — 140.114.0.4.

Параметры IPsec VPN:

IKE:

- группа Диффи-Хэллмана: 2;
- алгоритм шифрования: AES128;
- алгоритм аутентификации: SHA1.

IPsec:

- алгоритм шифрования: AES128;
- алгоритм аутентификации: SHA1.

Решение:

1. Конфигурирование Hub.
   Создадим туннель GRE:

   ```
   esr# configure
   esr(config)# tunnel gre 5
   ```

   Укажем IP-адрес интерфейса, граничащего с ISP:

   ```
   esr(config-gre)# local address 150.115.0.5
   ```

Зададим значение MTU:

```
esr(config-gre)# mtu 1416
```

Установим значение ttl:

```
esr(config-gre)# ttl 16
```

Зададим IP-адрес GRE-туннеля:

```
esr(config-gre)# ip address 10.10.0.5/24
```

Переведём GRE-туннель в mutipoint режим для возможности соединения с несколькими точками:

```
esr(config-gre)# multipoint
```

Перейдём к настройке NHRP. Настроим отправку мультикастовых рассылок в динамически узнаваемые адреса:

```
esr(config-gre)# ip nhrp multicast dynamic
```

Произведём настройку протокола динамической маршрутизации для Hub. В нашем примере это будет BGP:

```
esr(config)# router bgp 65005
esr(config-bgp)# address-family ipv4
esr(config-bgp-af)# neighbor 10.10.0.8
esr(config-bgp-neighbor)# remote-as 65008
esr(config-bgp-neighbor)# enable
esr(config-bgp-neighbor)# exit
esr(config-bgp-af)# neighbor 10.10.0.4
esr(config-bgp-neighbor)# remote-as 65004
esr(config-bgp-neighbor)# enable
esr(config-bgp-neighbor)# exit
esr(config-bgp-af)# enable
```

Произведём настройку IPsec для Hub:

```
esr(config)# security ike proposal IKEPROP
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# exit
```

```
esr(config)# security ike policy IKEPOLICY
esr(config-ike-policy)# pre-shared-key ascii-text encrypted 8CB5107EA7005AFF
esr(config-ike-policy)# proposal IKEPROP
esr(config-ike-policy)# exit
```

```
esr(config)# security ike gateway IKEGW
esr(config-ike-gw)# ike-policy IKEPOLICY
esr(config-ike-gw)# local address 150.115.0.5
esr(config-ike-gw)# local network 150.115.0.5/32 protocol gre
esr(config-ike-gw)# remote address any
esr(config-ike-gw)# remote network any
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

```
esr(config)# security ipsec proposal IPSECPROP
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

```
esr(config)# security ipsec policy IPSECPOLICY
esr(config-ipsec-policy)# proposal IPSECPROP
esr(config-ipsec-policy)# exit
```

```
esr(config)# security ipsec vpn IPSECVPN
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway IKEGW
esr(config-ipsec-vpn)# ike ipsec-policy IPSECPOLICY
esr(config-ipsec-vpn)# enable
```

Привяжем IPsec к GRE-туннелю, чтобы клиенты могли устанавливать шифрованное соединение:

```
esr(config-gre)# ip nhrp ipsec IPSECVPN dynamic
```

Включим работу NHRP и сам туннель:

```
esr(config-gre)# ip nhrp enable
esr(config-gre)# enable
```

2. Конфигурирование Spoke
   Проведём стандартную настройку DMVPN на туннеле:

```
esr# configure
esr(config-gre)# tunnel gre 8
esr(config-gre)# mtu 1416
esr(config-gre)# ttl 16
esr(config-gre)# multipoint
esr(config-gre)# local address 180.100.0.10
esr(config-gre)# ip address 10.10.0.8/24
```

Указываем сколько времени будет храниться запись о клиенте на сервере:

```
esr(config-gre)# ip nhrp holding-time 300
```

Указываем туннельный адрес NHS:

```
esr(config-gre)# ip nhrp nhs 10.10.0.5/24
```

Зададим соответствие туннельному адресу – реальный:

```
esr(config-gre)# ip nhrp map 10.10.0.5 150.115.0.5
```

Настроим мультикастовую рассылку на NHRP-сервер:

```
esr(config)# ip nhrp multicast nhs
```

Произведём настройку BGP для spoke:

```
esr(config)# router bgp 65008
esr(config-bgp)# address-family ipv4
esr(config-bgp-af)# neighbor 10.10.0.5
esr(config-bgp-neighbor)# remote-as 65005
esr(config-bgp-neighbor)# enable
esr(config-bgp-neighbor)# exit
esr(config-bgp-af)# enable
```

Произведём настройку IPsec. При создании шлюза протокола IKE для NHS, укажем конкретные адреса назначения. А при создании шлюза IKE для NHC – адрес назначения будет any:

```
esr(config)# security ike proposal IKEPROP
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# exit
```

```
esr(config)# security ike policy IKEPOLICY
esr(config-ike-policy)# pre-shared-key ascii-text encrypted 8CB5107EA7005AFF
esr(config-ike-policy)# proposal IKEPROP
esr(config-ike-policy)# exit
```

```
esr(config)# security ike gateway IKEGW_HUB
esr(config-ike-gw)# ike-policy IKEPOLICY
esr(config-ike-gw)# local address 180.100.0.10
esr(config-ike-gw)# local network 180.100.0.10/32 protocol gre
esr(config-ike-gw)# remote address 150.115.0.5
esr(config-ike-gw)# remote network 150.115.0.5/32 protocol gre
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

```
esr(config)# security ike gateway IKEGW_SPOKE
esr(config-ike-gw)# ike-policy IKEPOLICY
esr(config-ike-gw)# local address 180.100.0.10
esr(config-ike-gw)# local network 180.100.0.10/32 protocol gre
esr(config-ike-gw)# remote address any
esr(config-ike-gw)# remote network any
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

```
esr(config)# security ipsec proposal IPSECPROP
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

```
esr(config)# security ipsec policy IPSECPOLICY
esr(config-ipsec-policy)# proposal IPSECPROP
esr(config-ipsec-policy)# exit
```

```
esr(config)# security ipsec vpn IPSECVPN_HUB
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway IKEGW_HUB
esr(config-ipsec-vpn)# ike ipsec-policy IPSECPOLICY
esr(config-ipsec-vpn)# enable
```

```
esr(config)# security ipsec vpn IPSECVPN_SPOKE
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway IKEGW_SPOKE
esr(config-ipsec-vpn)# ike ipsec-policy IPSECPOLICY
esr(config-ipsec-vpn)# enable
```

Привяжем IPsec к GRE-туннелю для возможности установления шифрованного соединения с сервером и с другими клиентами сети:

```
esr(config-gre)# ip nhrp ipsec IPSECVPN_HUB static
esr(config-gre)# ip nhrp ipsec IPSECVPN_SPOKE dynamic
```

Включим работу NHRP и сам туннель:

```
esr(config-gre)# ip nhrp enable
esr(config-gre)# enable
```

Состояние NHRP-записей можно посмотреть командой:

```
esr# show ip nhrp
```

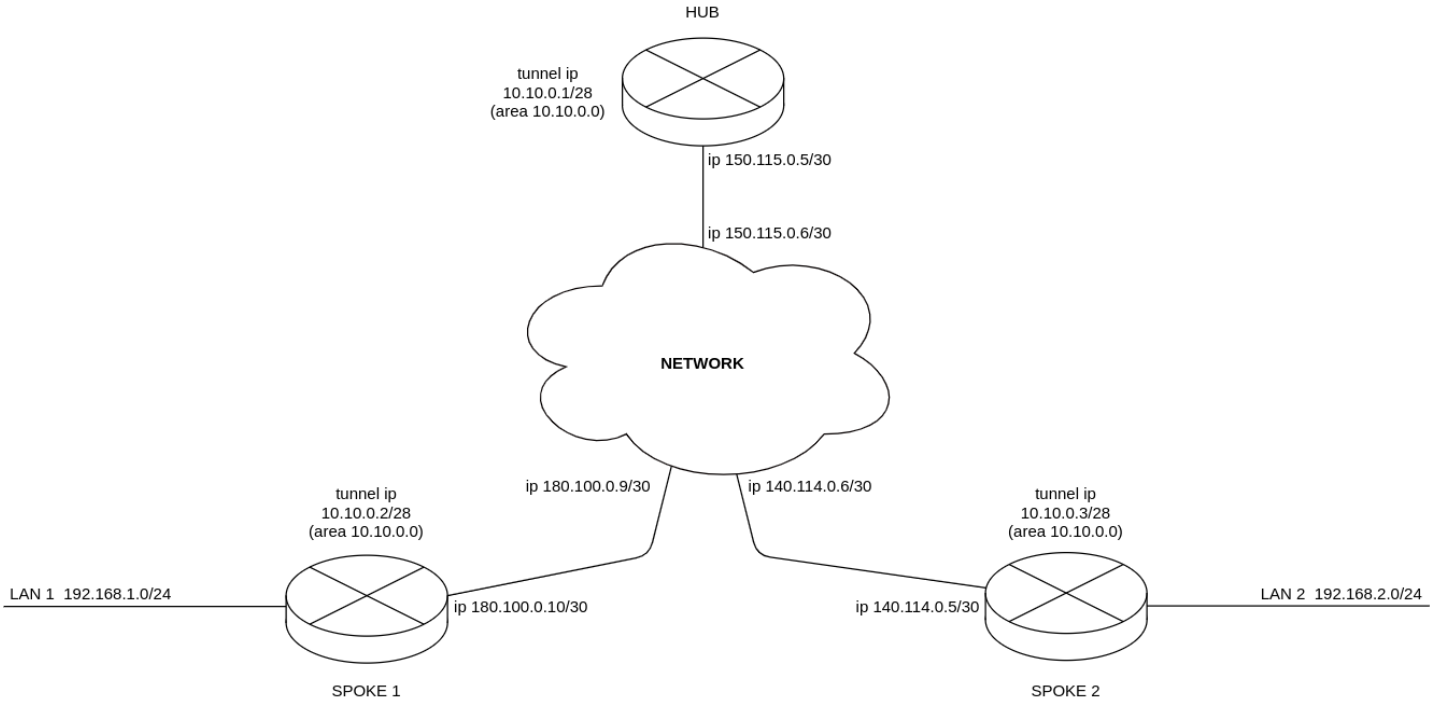
Очистить NHRP-записи можно командой:

```
esr# clear ip nhrp
```

11.2.3 Пример настройки 2

Задача:

Организовать DMVPN между офисами компании с соответствующими подсетями LAN1 и LAN2, используя mGRE-туннели, NHRP (Next Hop Resolution Protocol), протокол динамической маршрутизации (OSPF), IPsec. В нашем примере у нас будет HUB-устройство и два филиала. HUB – это DMVPN-сервер (NHS), а филиалы – DMPVN-клиенты (NHC).



При использовании схемы DMVPN необходимо, чтобы HUB являлся DR-маршрутизатором. Таким образом, маршруты локальных подсетей spoke 1 и spoke 2 будут ретранслироваться через hub.

HUB внешний IP-адрес — 150.115.0.5;
SPOKE-1 внешний IP-адрес — 180.100.0.10;
SPOKE-2 внешний IP-адрес — 140.114.0.4.

Параметры IPsec VPN:

IKE:

- группа Диффи-Хэллмана: 2;
- алгоритм шифрования: AES128;
- алгоритм аутентификации: MD5.

IPsec:

- группа Диффи-Хэллмана: 2;
- алгоритм шифрования: AES128;
- алгоритм аутентификации: MD5.

Решение:

1. Конфигурирование HUB:
   Предварительно настроим протокол OSPF:

```
esr(config)# router ospf log-adjacency-changes
esr(config)# router ospf 1
esr(config-ospf)# router-id 77.77.77.77
esr(config-ospf)# area 10.10.0.0
esr(config-ospf-area)# enable
esr(config-ospf-area)# exit
esr(config-ospf)# enable
esr(config-ospf)# exit
```

Настроим интерфейс и определим принадлежность к зоне безопасности:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# security-zone untrusted
esr(config-if-gi)# ip address 150.115.0.5/30
esr(config-if-gi)# exit
```

Настроим GRE-туннель, определим принадлежность к зоне безопасности, настроим OSPF на GRE-туннеле, настроим NHRP и включим туннель и NHRP командой enable. Чтобы HUB стал DR, необходимо выставить максимальный приоритет:

```
esr(config)# tunnel gre 1
esr(config-gre)# ttl 16
esr(config-gre)# mtu 1416
esr(config-gre)# multipoint
esr(config-gre)# security-zone untrusted
esr(config-gre)# local address 150.115.0.5
esr(config-gre)# ip address 10.10.0.1/28
esr(config-gre)# ip ospf instance 1
esr(config-gre)# ip ospf area 10.10.0.0
esr(config-gre)# ip ospf priority 255
esr(config-gre)# ip ospf
esr(config-gre)# ip nhrp multicast dynamic
esr(config-gre)# ip nhrp enable
esr(config-gre)# enable
esr(config-gre)# exit
```

Создадим статические маршруты для подсетей интерфейсов spoke 180.100.0.8/30 и 140.114.0.4/30:

```
esr(config)# ip route 180.100.0.8/30 150.115.0.6
esr(config)# ip route 140.114.0.4/30 150.115.0.6
```

Произведём настройку IPsec для HUB:

```
esr(config)# security ike proposal ike_prop1
esr(config-ike-proposal)# authentication algorithm md5
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# exit
```

```
esr(config)# security ike policy ike_pol1
esr(config-ike-policy)# pre-shared-key ascii-text password
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit
```

```
esr(config)# security ike gateway ike_spoke
esr(config-ike-gw)# ike-policy ike_pol1
esr(config-ike-gw)# local address 150.115.0.5
esr(config-ike-gw)# local network 150.115.0.5/32 protocol gre
esr(config-ike-gw)# remote address any
esr(config-ike-gw)# remote network any
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

```
esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# pfs dh-group 2
esr(config-ipsec-proposal)# exit
```

```
esr(config)# security ipsec policy ipsec_pol1
esr(config-ipsec-policy)# proposal ipsec_prop1
esr(config-ipsec-policy)# exit
```

```
esr(config)# security ipsec vpn ipsec_spoke
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway ike_spoke
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
```

Привяжем IPsec к GRE-туннелю, чтобы клиенты могли устанавливать шифрованное соединение:

```
esr(config)# tunnel gre 1
esr(config-gre)# ip nhrp ipsec ipsec_spoke dynamic
esr(config-gre)# exit
```

2. Конфигурирование SPOKE:
   Предварительно настроим протокол OSPF с анонсированием подсети LAN1:

```
esr(config)# router ospf log-adjacency-changes
esr(config)# router ospf 1
esr(config-ospf)# router-id 1.1.1.1
esr(config-ospf)# area 10.10.0.0
esr(config-ospf-area)# network 192.168.1.0/24
esr(config-ospf-area)# enable
esr(config-ospf-area)# exit
esr(config-ospf)# enable
esr(config-ospf)# exit
```

Настроим интерфейс и определим принадлежность к зоне безопасности:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# security-zone untrusted
esr(config-if-gi)# ip address 180.100.0.10/30
esr(config-if-gi)# exit
```

Настроим GRE-туннель, определим принадлежность к зоне безопасности, настроим OSPF на GRE-туннеле, настроим NHRP и включим туннель и NHRP командой enable. Чтобы HUB стал DR, необходимо выставить минимальный приоритет на spoke:

```
esr(config)# tunnel gre 1
esr(config-gre)# ttl 16
esr(config-gre)# mtu 1416
esr(config-gre)# multipoint
esr(config-gre)# ip firewall disable
esr(config-gre)# local address 180.100.0.10
esr(config-gre)# ip address 10.10.0.2/28
esr(config-gre)# ip ospf instance 1
esr(config-gre)# ip ospf area 10.10.0.0
esr(config-gre)# ip ospf priority 0
esr(config-gre)# ip ospf
esr(config-gre)# ip nhrp holding-time 300
esr(config-gre)# ip nhrp map 10.10.0.1 150.115.0.5
esr(config-gre)# ip nhrp nhs 10.10.0.1/28
esr(config-gre)# ip nhrp multicast nhs
esr(config-gre)# ip nhrp enable
esr(config-gre)# enable
esr(config-gre)# exit
```

Создадим статические маршруты для подсетей интерфейсов spoke 180.100.0.8/30 и 140.114.0.4/30:

```
esr(config)# ip route 150.115.0.4/30 180.100.0.9
esr(config)# ip route 140.114.0.4/30 180.100.0.9
```

Произведём настройку IPsec для SPOKE:

```
esr(config)# security ike proposal ike_prop1
esr(config-ike-proposal)# authentication algorithm md5
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# exit
```

```
esr(config)# security ike policy ike_pol1
esr(config-ike-policy)# pre-shared-key ascii-text password
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit
```

```
esr(config)# security ike gateway ike_spoke
esr(config-ike-gw)# ike-policy ike_pol1
esr(config-ike-gw)# local address 180.100.0.10
esr(config-ike-gw)# local network 180.100.0.10/32 protocol gre
esr(config-ike-gw)# remote address any
esr(config-ike-gw)# remote network any
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
esr(config)# security ike gateway ike_hub
esr(config-ike-gw)# ike-policy ike_pol1
esr(config-ike-gw)# local address 180.100.0.10
esr(config-ike-gw)# local network 180.100.0.10/32 protocol gre
esr(config-ike-gw)# remote address 150.115.0.5
esr(config-ike-gw)# remote network 150.115.0.5/32 protocol gre
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

```
esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# pfs dh-group 2
esr(config-ipsec-proposal)# exit
```

```
esr(config)# security ipsec policy ipsec_pol1
esr(config-ipsec-policy)# proposal ipsec_prop1
esr(config-ipsec-policy)# exit
```

```
esr(config)# security ipsec vpn ipsec_spoke
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway ike_spoke
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
esr(config)# security ipsec vpn ipsec_hub
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway ike_hub
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
```

Привяжем IPsec к GRE-туннелю, для возможности установления шифрованного соединения с сервером и с другими клиентами сети:

```
esr(config)# tunnel gre 1
esr(config-gre)# ip nhrp ipsec ipsec_hub static
esr(config-gre)# ip nhrp ipsec ipsec_spoke dynamic
esr(config-gre)# exit
```

3. Состояние NHRP-записей можно посмотреть командой:

```
esr# show ip nhrp
```

4. Дополнительно в security zone-pair untrusted self необходимо разрешить протоколы для GRE over IPSec-туннеля:

```
esr(config)# object-group service ISAKMP_PORT
esr(config-object-group-service)# port-range 500
esr(config-object-group-service)# poRt-range 4500
esr(config-object-group-service)# exit
esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol udp
esr(config-zone-pair-rule)# match destination-port ISAKMP_PORT
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# rule 2
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol gre
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# rule 3
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol esp
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# rule 4
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol ah
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
```

11.3 Настройка L2TPv3-туннелей

L2TPv3 (Layer 2 Tunneling Protocol Version 3) — протокол для туннелирования пакетов 2 уровня модели OSI между двумя IP-узлами. В качестве инкапсулирующего протокола используется IP или UDP. L2TPv3 может использоваться как альтернатива MPLS P2P L2VPN (VLL) для организации VPN уровня L2. В устройствах реализованы статические неуправляемые L2TPv3-туннели, то есть туннели создаются вручную путем конфигурирования на локальном и удаленном узлах. Параметры туннеля на каждой из сторон должны быть взаимосогласованными или переносимые данные не будут декапсулироваться партнером.

11.3.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Сконфигурировать L3-интерфейс, от которого будет строиться L2TPv3-туннель.		

Шаг	Описание	Команда	Ключи
2	Создать L2TPv3-туннель и перейти в режим его конфигурирования.	**esr(config)# tunnel l2tpv3 <INDEX>**	<INDEX> – идентификатор туннеля в диапазоне: • для ESR-10/12V(F)/ 14VF/15 – [1..10]; • для ESR-20/21/30/100/200 – [1..250]; • для ESR-1000/1200/1500/ 1511/1700/3100/3200 – [1..500].
3	Указать описание конфигурируемого туннеля (не обязательно).	**esr(config-l2tpv3)# description <DESCRIPTION>**	<DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов.
4	Установить локальный IP-адрес для установки туннеля.	**esr(config-l2tpv3)# local address <ADDR>**	<ADDR> – IP-адрес локального шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
5	Установить удаленный IP-адрес для установки туннеля.	**esr(config-l2tpv3)# remote address <ADDR>**	<ADDR> – IP-адрес локального шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
6	Выбрать метод инкапсуляции для туннеля L2TPv3.	**esr(config-l2tpv3)# protocol <TYPE>**	<TYPE> – тип инкапсуляции, возможные значения: • **ip** - инкапсуляция в IP-пакет; • **udp** - инкапсуляция в UDP-дейтаграммы.
7	Установить локальный идентификатор сессии.	**esr(config-l2tpv3)# local session-id <SESSION-ID>**	<SESSION-ID> – идентификатор сессии, принимает значения [1..200000].
8	Установить удаленный идентификатор сессии.	**esr(config-l2tpv3)# remote session-id <SESSION-ID>**	<SESSION-ID> – идентификатор сессии, принимает значения [1..200000].
9	Определить локальный UDP-порт (если в качестве метода инкапсуляции был выбран UDP протокол).	**esr(config-l2tpv3)# local port <UDP>**	<UDP> – номер UDP-порта в диапазоне [1..65535].

Шаг	Описание	Команда	Ключи
10	Определить удаленный UDP-порт (если в качестве метода инкапсуляции был выбран UDP протокол).	**esr(config-l2tpv3)# remote port <UDP>**	<UDP> – номер UDP-порта в диапазоне [1..65535].
11	Назначить широковещательный домен для инкапсуляции в L2TPV3-пакеты данного туннеля.	**esr(config-l2tpv3)# bridge-group <BRIDGE-ID>**	<BRIDGE-ID> – идентификационный номер моста, принимает значения в диапазоне: • для ESR-10/12V(F)/ 14VF/15 – [1..50]; • для ESR-20/21/30/100/200 – [1..250]; • для ESR-1000/1200/1500 – /1511/1700/3100/3200 – [1..500].
12	Активировать туннель.	**esr(config-l2tpv3)# enable**	
13	Указать размер MTU (MaximumTransmitionUnit) для туннелей (не обязательно). MTU более 1500 будет активно только в случае применения команды "system jumbo-frames".	**esr(config-l2tpv3)# mtu <MTU>**	<MTU> – значение MTU, принимает значения в диапазоне: • для ESR-10/12V(F)/ 14VF/15 – [1280..9600]; • для ESR-20/21/30 – [1280..9500]; • для ESR-100/200/1000/ 1200/1500/1511/1700/ 3100/3200 – [1280..10000]. Значение по умолчанию: 1500.
14	Определить локальное значение cookie для дополнительной проверки соответствия между передаваемыми данными и сессией (не обязательно).	**esr(config-l2tpv3)# local cookie <COOKIE>**	<COOKIE> – значение COOKIE, параметр принимает значения длиной восемь или шестнадцать символов в шестнадцатеричном виде.
15	Определить удаленное значение cookie для дополнительной проверки соответствия между передаваемыми данными и сессией (не обязательно).	**esr(config-l2tpv3)# remote cookie <COOKIE>**	<COOKIE> – значение COOKIE, параметр принимает значения длиной восемь или шестнадцать символов в шестнадцатеричном виде.

Шаг	Описание	Команда	Ключи
16	Задать интервал времени, за который усредняется статистика о нагрузке на туннеле (не обязательно).	**esr(config-l2tpv3)# load-average <TIME>**	<TIME> – интервал в секундах, принимает значения [5..150]. Значение по умолчанию: 5.
17	Включить запись статистики использования текущего туннеля (не обязательно).	**esr(config-subif)# history statistics**	
Также для L2TPv3-туннеля возможно настроить: • QoS в базовом или расширенном режимах (см. раздел Управление QoS); • функционал BRAS (см. раздел Управление BRAS (Broadband Remote Access Server)).			

11.3.2 Пример настройки L2TPv3-туннеля

Задача:

Организовать L2 VPN между офисами компании через IP-сеть, используя для туннелирования трафика протокол L2TPv3.

- в качестве инкапсулирующего протокола используется UDP, номер порта на локальной стороне и номер порта на стороне партнера 519;
- в качестве локального шлюза для туннеля используется IP-адрес 21.0.0.1;
- в качестве удаленного шлюза для туннеля используется IP-адрес 183.0.0.10;
- идентификатор туннеля на локальной стороне равен 2, на стороне партнера 3;
- идентификатор сессии внутри туннеля равен 100, на стороне партнера 200;
- в туннель направим трафик из bridge с идентификатором 333.

Решение:

Создадим туннель L2TPv3 333:

```
esr# configure
esr(config)# tunnel l2tpv3 333
```

Укажем локальный и удаленный шлюз (IP-адреса интерфейсов, граничащих с WAN):

```
esr(config-l2tpv3)# local address 21.0.0.1
esr(config-l2tpv3)# remote address 183.0.0.10
```

Укажем тип инкапсулирующего протокола и номера UDP-портов:

```
esr(config-l2tpv3)# protocol udp
esr(config-l2tpv3)# local port 519
esr(config-l2tpv3)# remote port 519
```

Укажем идентификаторы сессии внутри туннеля для локальной и удаленной сторон:

```
esr(config-l2tpv3)# local session-id 100
esr(config-l2tpv3)# remote session-id 200
```

Установим принадлежность L2TPv3-туннеля к мосту, который должен быть связан с сетью удаленного офиса (настройка моста рассматривается в пункте Пример настройки bridge для VLAN и L2TPv3-туннеля):

```
esr(config-l2tpv3)# bridge-group 333
```

Включим ранее созданный туннель и выйдем:

```
esr(config-l2tpv3)# enable
esr(config-l2tpv3)# exit
```

Создадим саб-интерфейс для коммутации трафика, поступающего из туннеля, в локальную сеть с тегом VLAN id 333:

```
esr(config)# interface gi 1/0/2.333
```

Установим принадлежность саб-интерфейса к мосту, который должен быть связан с локальной сетью (настройка моста рассматривается в пункте Настройка PPP через E1):

```
esr(config-subif)# bridge-group 333
esr(config-subif)# exit
```

После применения настроек трафик будет инкапсулироваться в туннель и отправляться партнеру, независимо от наличия L2TPv3-туннеля и правильности настроек с его стороны.

Настройки туннеля в удаленном офисе должны быть зеркальными локальным. В качестве локального шлюза должен использоваться IP-адрес 183.0.0.10. В качестве удаленного шлюза должен использоваться IP-адрес 21.0.0.1. Номер порта инкапсулирующего протокола на локальной стороне и

стороне партнера 519. Идентификатор сессии внутри туннеля должен быть равным 200, на стороне партнера 100. Также туннель должен принадлежать мосту, который необходимо соединить с сетью партнера.

Состояние туннеля можно посмотреть командой:

```
esr# show tunnels status l2tpv3 333
```

Счетчики входящих и отправленных пакетов можно посмотреть командой:

```
esr# show tunnels counters l2tpv3 333
```

Конфигурацию туннеля можно посмотреть командой:

```
esr# show tunnels configuration l2tpv3 333
```

Помимо создания туннеля необходимо в firewall разрешить входящий трафик по протоколу UDP с портом отправителя 519 и портом назначения 519.

11.4 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.

11.4.1 Алгоритм настройки Route-based IPsec VPN

Шаг	Описание	Команда	Ключи
1	Создать VTI-туннель и перейти в режим его конфигурирования.	**esr(config)# tunnel vti <TUN>**	<TUN> – имя туннеля устройства.
2	Указать локальный IP-адрес VTI-туннеля.	**esr(config-vti)#local address <ADDR>**	<ADDR> – IP-адрес локального шлюза.
3	Указать удаленный IP-адрес VTI-туннеля.	**esr(config-vti)#remote address <ADDR>**	<ADDR> – IP-адрес удаленного шлюза.
4	Установить IP-адрес локальной стороны VTI-туннеля.	**esr(config-vti)# ip address <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].
5	Включить VTI-туннель в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall для VTI-туннеля.	**esr(config-vti)# security-zone<NAME>** **esr(config-vti)# ip firewall disable**	<NAME> – имя зоны безопасности, задаётся строкой до 12 символов.

Шаг	Описание	Команда	Ключи
6	Включить туннель.	**esr(config-vti)#enable**	
7	Создать IKE-профиль и перейти в режим его конфигурирования.	**esr(config)# security ike proposal <NAME>**	<NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа.
8	Указать описание конфигурируемого IKE-профиля (не обязательно).	**esr(config-ike-proposal)# description<DESCRIPTION>**	<DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов.
9	Определить алгоритм аутентификации для IKE (не обязательно).	**esr(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 (не обязательно).	**esr(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 (не обязательно).	**esr(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.

Шаг	Описание	Команда	Ключи
12	Определить режим аутентификации IKE (не обязательно).	**esr(config-ike-proposal)# 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.
13	Создать ike-политику и перейти в режим её конфигурирования.	**esr(config)# security ike policy <NAME>**	<NAME> – имя политики IKE, задаётся строкой до 31 символа.
14	Задать время жизни соединения протокола IKE (не обязательно).	**esr(config-ike-proposal)# lifetime seconds <SEC>**	<SEC> – период времени, принимает значения [4 .. 86400] секунд. Значение по умолчанию: 3600.
15	Привязать IKE-профиль к IKE-политике.	**esr(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)	**esr(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.	**esr(config)# security ike gateway <NAME>**	<NAME> – имя шлюза протокола IKE, задаётся строкой до 31 символа.
18	Привязать IKE-политику к IKE-шлюзу.	**esr(config-ike-gw)# ike-policy <NAME>**	<NAME> – имя политики протокола IKE, задаётся строкой до 31 символа.
19	Указать версию IKE (не обязательно).	**esr(config-ike-gw)# version <VERSION>**	<version> – версия IKE-протокола: v1-only или v2-only. Значение по умолчанию: v1-only.

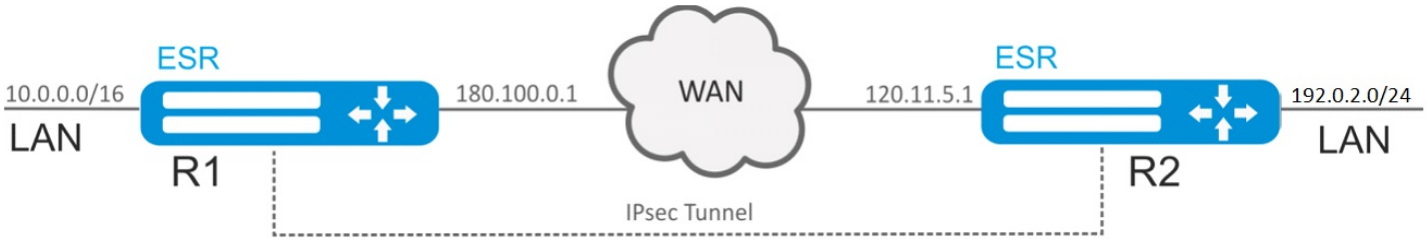
Шаг	Описание	Команда	Ключи
20	Установить режим перенаправления трафика в туннель – route-based.	**esr(config-ike-gw)# mode route-based**	
21	Указать действие для DPD (не обязательно).	**esr(config-ike-gw)# dead-peer-detection action <MODE>**	<MODE> – режим работы DPD: • **restart** – соединение переустанавливается; • **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 (не обязательно).	**esr(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 для ответа на сообщения механизма DPD (не обязательно).	**esr(config-ike-gw)# dead-peer-detection timeout <SEC>**	<SEC> – период времени для ответа на сообщения механизма DPD, принимает значения [1..180] секунд. Значение по умолчанию: 30 секунд.
24	Привязать VTI-туннель к IKE-шлюзу.	**esr(config-ike-gw)# bind-interface vti <VTI>**	<VTI> – идентификационный номер интерфейса VTI.
25	Создать в IPsec-профиль.	**esr(config)# security ipsec proposal <NAME>**	<NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа.
26	Определить алгоритм аутентификации для IPsec (не обязательно).	**esr(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
27	Определить алгоритм шифрования для IPsec (не обязательно).	**esr(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.
28	Указать протокол инкапсуляции для IPsec (не обязательно).	**esr(config-ipsec-proposal)# protocol <PROTOCOL>**	<PROTOCOL> – инкапсулирующий протокол, принимает значения Значение по умолчанию: esp.
29	Создать IPsec-политику и перейти в режим её конфигурирования.	**esr(config)# security ipsec policy <NAME>**	<NAME> – имя политики IPsec, задаётся строкой до 31 символа.
30	Привязать IPsec-профиль к IPsec-политике.	**esr(config-ipsec-policy)# proposal <NAME>**	<NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа.
31	Задать время жизни IPsec-туннеля (не обязательно).	**esr(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..86400] секунд. Значение по умолчанию: 28800 секунд.

Шаг	Описание	Команда	Ключи
32	Создать IPsec VPN и перейти в режим конфигурирования.	**esr(config)# security ipsec vpn <NAME>**	<NAME> – имя VPN, задаётся строкой до 31 символа.
33	Определить режим согласования данных, необходимых для активации VPN.	**esr(config-ipsec-vpn)# mode <MODE>**	<MODE> – режим работы VPN.
34	Привязать IPsec-политику к IPsec-VPN.	**esr(config-ipsec-vpn)# ike ipsec-policy <NAME>**	<NAME> – имя IPsec-политики, задаётся строка до 31 символа.
35	Задать значение DSCP для использования в IP-заголовке исходящих пакетов IKE-протокола (не обязательно).	**esr(config-ipsec-vpn)# ike dscp <DSCP>**	DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 63.
36	Установить режим активации VPN.	**esr(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.
37	Осуществить привязку IKE-шлюза к IPsec-VPN.	**esr(config-ipsec-vpn)# ike gateway <NAME>**	<NAME> – имя IKE-шлюза, задаётся строкой до 31 символа.
38	Установить значение временного интервала в секундах, по истечению которого соединение закрывается, если не было принято или передано ни одного пакета через SA (не обязательно).	**esr(config-ipsec-vpn)# ike idle-time <TIME>**	<TIME> – интервал в секундах, принимает значения [4..86400].
39	Отключить пересогласование ключей до разрыва IKE-соединения по истечению времени, количеству переданных пакетов или байт (не обязательно).	**esr(config-ipsec-vpn)# ike rekey disable**	

Шаг	Описание	Команда	Ключи
40	Настроить начало пересогласования ключей IKE-соединения до истечения времени жизни (не обязательно).	**esr(config-ipsec-vpn)# ike rekey margin { seconds <SEC> | packets <PACKETS> | kilobytes <KB> }**	<SEC> – интервал времени в секундах, оставшийся до закрытия соединения (задается командой lifetimeseconds, см. 22.2.13). Принимает значения [4..86400]. <PACKETS> – количество пакетов, оставшихся до закрытия соединения (задается командой lifetimepackets). Принимает значения [4..86400] <KB> – объем трафика в килобайтах, оставшийся до закрытия соединения (задается командой lifetimekilobytes). 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.
41	Установить уровень случайного разброса значений параметров margin seconds, margin packets, margin kilobytes (не обязательно).	**esr(config-ipsec-vpn)# ike rekey randomization <VALUE>**	<VALUE> – максимальный процент разброса значений, принимает значения [1..100]. Значение по умолчанию: 100%
42	Указать описание для IPsec-VPN (не обязательно).	**esr(config-ipsec-vpn)# description <DESCRIPTION>**	<DESCRIPTION> – описание профиля, задаётся строкой до 255 символов.
43	Активировать IPsec VPN.	**esr(config-ipsec-vpn)# enable**	

11.4.2 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:

1. Конфигурирование R1
   Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```
esr# configure
esr(config)# interface gi 1/0/1
esr(config-if-gi)# ip address 180.100.0.1/24
esr(config-if-gi)# security-zone untrusted
esr(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:

```
esr(config)# tunnel vti 1
esr(config-vti)# local address 180.100.0.1
esr(config-vti)# remote address 120.11.5.1
esr(config-vti)# enable
esr(config-vti)# exit
```

   Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```
esr(config)# object-group service ISAKMP
esr(config-object-group-service)# port-range 500
esr(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:

```
esr(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:

```
esr(config)# security ike proposal ike_prop1
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm md5
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# exit
```

Создадим политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы и ключ аутентификации:

```
esr(config)# security ike policy ike_pol1
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit
```

Создадим шлюз протокола IKE. В данном профиле указывается VTI-туннель, политика, версия протокола и режим перенаправления трафика в туннель:

```
esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_pol1
esr(config-ike-gw)# mode route-based
esr(config-ike-gw)# bind-interface vti 1
esr(config-ike-gw)# version v2-only
esr(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:

```
esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы.

```
esr(config)# security ipsec policy ipsec_pol1
esr(config-ipsec-policy)# proposal ipsec_prop1
esr(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*.

```
esr(config)# security ipsec vpn ipsec1
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway ike_gw1
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
esr(config)# exit
```

2. Конфигурирование R2

Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```
esr# configure
esr(config)# interface gi 1/0/1
esr(config-if)# ip address 120.11.5.1/24
esr(config-if)# security-zone untrusted
esr(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:

```
esr(config)# tunnel vti 1
esr(config-vti)# remote address 180.100.0.1
esr(config-vti)# local address 120.11.5.1
esr(config-vti)# enable
esr(config-vti)# exit
```

Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```
esr(config)# object-group service ISAKMP
esr(config-object-group-service)# port-range 500
esr(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:

```
esr(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:

```
esr(config)# security ike proposal ike_prop1
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm md5
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# exit
esr(config)#
```

Создадим политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы и ключ аутентификации:

```
esr(config)# security ike policy ike_pol1
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit
```

Создадим шлюз протокола IKE. В данном профиле указывается VTI-туннель, политика, версия протокола и режим перенаправления трафика в туннель:

```
esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_pol1
esr(config-ike-gw)# mode route-based
esr(config-ike-gw)# bind-interface vti 1
esr(config-ike-gw)# version v2-only
esr(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:

```
esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы.

```
esr(config)# security ipsec policy ipsec_pol1
esr(config-ipsec-policy)# proposal ipsec_prop1
esr(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*.

```
esr(config)# security ipsec vpn ipsec1
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway ike_gw1
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
esr(config)# exit
```

Состояние туннеля можно посмотреть командой:

```
esr# show security ipsec vpn status ipsec1
```

Конфигурацию туннеля можно посмотреть командой:

```
esr# show security ipsec vpn configuration ipsec1
```

В firewall необходимо разрешить протокол ESP и ISAKMP (UDP-порт 500).

11.4.3 Алгоритм настройки Policy-based IPsec VPN

Шаг	Описание	Команда	Ключи
1	Создать IKE-экземпляр и перейти в режим его конфигурирования.	**esr(config)# security ike proposal <NAME>**	<NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа.
2	Указать описание конфигурируемого туннеля (не обязательно).	**esr(config-ike-proposal)# description<DESCRIPTION>**	<DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов.
3	Определить алгоритм аутентификации для IKE.	**esr(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.	**esr(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.
5	Определить номер группы Диффи-Хэллмана.	**esr(config-ike-proposal)# dh-group <DH-GROUP>**	<DH-GROUP> – номер группы Диффи-Хэллмана, принимает значения [1, 2, 5, 14, 15, 16, 17, 18].
6	Определить режим аутентификации.	**esr(config-ike-proposal)# 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.
7	Создать политику для профиля IKE и перейти в режим её конфигурирования.	**esr(config)# security ike policy <NAME>**	<NAME> – имя политики IKE, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
8	Задать время жизни соединения протокола IKE (не обязательно).	**esr(config-ike-proposal)# lifetime seconds <SEC>**	<SEC> – период времени, принимает значения [4 .. 86400] секунд.
9	Привязать политику к профилю.	**esr(config-ike-policy)# proposal <NAME>**	<NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа.
10	Указать ключ аутентификации.	**esr(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.	**esr(config)# security ike gateway <NAME>**	<NAME> – имя шлюза протокола IKE, задаётся строкой до 31 символа.
12	Привязать политику IKE.	**esr(config-ike-gw)# ike-policy <NAME>**	<NAME> – имя политики протокола IKE, задаётся строкой до 31 символа.
13	Указать версию IKE (не обязательно).	**esr(config-ike-gw)# version <VERSION>**	<version> – версия IKE-протокола: **v1-only** или **v2-only**.
14	Установить режим перенаправления трафика в туннель.	**esr(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 (не обязательно).	**esr(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 (не обязательно).	**esr(config-ike-gw)#dead-peer-detection interval <SEC>**	<SEC> – интервал между отправкой сообщений механизмом DPD, принимает значения [1..180] секунд.

Шаг	Описание	Команда	Ключи
17	Указать период времени для ответа на сообщения механизма DPD (не обязательно).	**esr(config-ike-gw)# dead-peer-detection timeout <SEC>**	<SEC> – период времени для ответа на сообщения механизма DPD, принимает значения [1..180] секунд.
18	Указать версию IKE (не обязательно).	**esr(config-ike-gw)# version <VERSION>**	<version> – версия IKE-протокола: **v1-only** или **v2-only**.
19	Установить IP подсети отправителя.	**esr(config-ike-gw)# local 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].
20	Установить IP-адрес локального шлюза IPsec-туннеля.	**esr(config-ike-gw)#local address <ADDR>**	<ADDR> – IP-адрес локального шлюза.
21	Установить IP-адрес удаленного шлюза IPsec-туннеля.	**esr(config-ike-gw)#remote address <ADDR>**	<ADDR> – IP-адрес удаленного шлюза.

Шаг	Описание	Команда	Ключи
22	Установить IP-адрес подсети получателя, а также IP-протокол и порт.	**esr(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].
23	Создать в профиль IPsec.	**esr(config)# security ipsec proposal <NAME>**	<NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа.
24	Определить алгоритм аутентификации для IPsec.	**esr(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.	**esr(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.
26	Указать протокол (не обязательно).	**esr(config-ipsec-proposal)#protocol <PROTOCOL>**	<PROTOCOL> – инкапсулирующий протокол, принимает значения
27	Создать политику для профиля IPsec и перейти в режим её конфигурирования.	**esr(config)# security ipsec policy <NAME>**	<NAME> – имя политики IPsec, задаётся строкой до 31 символа.

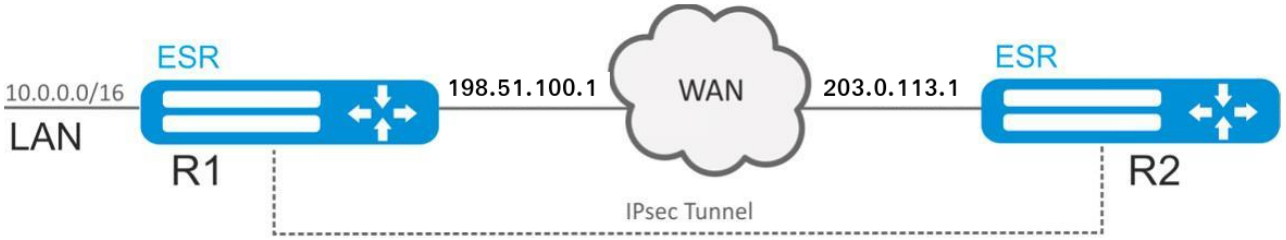
Шаг	Описание	Команда	Ключи
28	Привязать политику к профилю.	**esr(config-ipsec-policy)# proposal <NAME>**	<NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа.
29	Задать время жизни IPsec туннеля (не обязательно).	**esr(config-ipsec-policy)# lifetime { seconds <SEC> | packets <PACKETS> | 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..86400] секунд.
30	Создать IPsec VPN и перейти в режим конфигурирования.	**esr(config)# security ipsecvpn <NAME>**	<NAME> – имя VPN, задаётся строкой до 31 символа.
31	Определить режим согласования данных, необходимых для активации VPN.	**esr(config-ipsec-vpn)# mode <MODE>**	<MODE> – режим работы VPN.
32	Привязать IPsec политику к VPN.	**esr(config-ipsec-vpn)#ike ipsec-policy <NAME>**	<NAME> – имя IPsec-политики, задаётся строка до 31 символа.
33	Задать значение DSCP для использования в IP-заголовке исходящих пакетов IKE-протокола (не обязательно).	**esr(config-ipsec-vpn)#ike dscp <DSCP>**	DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].

Шаг	Описание	Команда	Ключи
34	Установить режим активации VPN.	**esr(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.
35	Осуществить привязка IKE-шлюза к VPN.	**esr(config-ipsec-vpn)# ike gateway <NAME>**	<NAME> – имя IKE-шлюза, задаётся строкой до 31 символа.
36	Установить значение временного интервала в секундах, по истечению которого соединение закрывается, если не было принято или передано ни одного пакета через SA (не обязательно).	**esr(config-ipsec-vpn)# ike idle-time <TIME>**	<TIME> – интервал в секундах, принимает значения [4..86400].
37	Отключить пересогласование ключей до разрыва IKE-соединения по истечению времени, количеству переданных пакетов или байт (не обязательно).	**esr(config-ipsec-vpn)#ike rekey disable**	

Шаг	Описание	Команда	Ключи
38	Настроить начало пересогласования ключей IKE-соединения до истечения времени жизни (не обязательно).	**esr(config-ipsec-vpn)# Ike rekey margin { seconds <SEC> | packets <PACKETS> | kilobytes <KB> }**	<SEC> – интервал времени в секундах, оставшийся до закрытия соединения (задается командой lifetimeseconds) . Принимает значения [4..86400]. <PACKETS> – количество пакетов, оставшихся до закрытия соединения (задается командой lifetimepackets). Принимает значения [4..86400]. <KB> – объем трафика в килобайтах, оставшийся до закрытия соединения (задается командой lifetimekilobytes). Принимает значения [4..86400]
39	Установить уровень случайного разброса значений параметров marginseconds, marginpackets, marginkilobytes (не обязательно).	**esr(config-ipsec-vpn)# ike rekey randomization <VALUE>**	<VALUE> – максимальный процент разброса значений, принимает значения [1..100].
40	Описать VPN (не обязательно).	**esr(config-ipsec-vpn)# description <DESCRIPTION>**	<DESCRIPTION> – описание профиля, задаётся строкой до 255 символов.
41	Активировать IPsec VPN.	**esr(config-ipsec-vpn)# enable**	

11.4.4 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:

1. Конфигурирование R1
   Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```
esr# configure
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 198.51.100.1/24
esr(config-if-gi)# security-zone untrusted
esr(config-if-gi)# exit
```

   Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```
esr(config)# object-group service ISAKMP
esr(config-object-group-service)# port-range 500
esr(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:

```
esr(config)# security ike proposal ike_prop1
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm md5
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# exit
```

   Создадим политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы и ключ аутентификации:

```
esr(config)# security ike policy ike_pol1
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit
```

Создадим шлюз протокола IKE. В данном профиле указывается VTI-туннель, политика, версия протокола и режим перенаправления трафика в туннель:

```
esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_pol1
esr(config-ike-gw)# local address 198.51.100.1
esr(config-ike-gw)# local network 10.0.0.0/16
esr(config-ike-gw)# remote address 203.0.113.1
esr(config-ike-gw)# remote network 192.0.2.0/24
esr(config-ike-gw)# mode policy-based
esr(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:

```
esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы.

```
esr(config)# security ipsec policy ipsec_pol1
esr(config-ipsec-policy)# proposal ipsec_prop1
esr(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*.

```
esr(config)# security ipsec vpn ipsec1
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway ike_gw1
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
esr(config)# exit
```

2. Конфигурирование R2
   Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```
esr# configure
esr(config)# interface gi 1/0/1
esr(config-if)# ip address 203.0.113.1/24
esr(config-if)# security-zone untrusted
esr(config-if)# exit
```

Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```
esr(config)# object-group service ISAKMP
esr(config-addr-set)# port-range 500
esr(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:

```
esr(config)# security ike proposal ike_prop1
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm md5
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# exit
esr(config)#
```

Создадим политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы и ключ аутентификации:

```
esr(config)# security ike policy ike_pol1
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit
```

Создадим шлюз протокола IKE. В данном профиле указывается VTI-туннель, политика, версия протокола и режим перенаправления трафика в туннель:

```
esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_pol1
esr(config-ike-gw)# remote address 198.51.100.1
esr(config-ike-gw)# remote network 10.0.0.0/16
esr(config-ike-gw)# local address 203.0.113.1
esr(config-ike-gw)# local network 192.0.2.0/24
esr(config-ike-gw)# mode policy-based
esr(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:

```
esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы.

```
esr(config)# security ipsec policy ipsec_pol1
esr(config-ipsec-policy)# proposal ipsec_prop1
esr(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*.

```
esr(config)# security ipsec vpn ipsec1
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway ike_gw1
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
esr(config)# exit
```

Состояние туннеля можно посмотреть командой:

```
esr# show security ipsec vpn status ipsec1
```

Конфигурацию туннеля можно посмотреть командой:

```
esr# show security ipsec vpn configuration ipsec1
```

В firewall необходимо разрешить протокол ESP и ISAKMP (UDP-порт 500).

11.4.5 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 второго фактора аутентификации IPsec – Extended Authentication (XAUTH), 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.	**esr(config)# security ike proposal <NAME>**	<NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа.
2	Указать описание конфигурируемого туннеля (не обязательно).	**esr(config-ike-proposal)# description <DESCRIPTION>**	<DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов.
3	Определить алгоритм аутентификации для IKE (не обязательно).	**esr(config-ike-proposal)# authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2_384, sha2-512. Значение по умолчанию: sha1.
4	Установить IP-адрес локальной стороны VTI-туннеля (не обязательно).	**esr(config-vti)# ip address <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..31].

Шаг	Описание	Команда	Ключи
5	Определить номер группы Диффи-Хэллмана (не обязательно).	**esr(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.	**esr(config)# security ike policy <NAME>**	<NAME> – имя политики IKE, задаётся строкой до 31 символа.
7	Определить режим аутентификации.	**esr(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.
8	Задать режим клиента (только для клиента).	**esr(config-ike- policy)# authentication mode client**	
9	Задать время жизни соединения протокола IKE (не обязательно).	**esr(config-ike- policy)# lifetime seconds <SEC>**	<SEC> – период времени, принимает значения [4 .. 86400] секунд. Значение по умолчанию: 3600.
10	Привязать политику к профилю.	**esr(config-ike-policy)# proposal <NAME>**	<NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа.
11	Указать ключ аутентификации.	**esr(config-ike-policy)#pre-shared-key ascii-text <TEXT>**	<TEXT> – строка [1..64] ASCII символов.
12	Создать профиль доступа.	**esr(config)# access profile <NAME>**	<NAME> – имя профиля доступа, задаётся строкой до 31 символа.
13	Создать имя пользователя.	**esr(config-access-profile)# user <LOGIN>**	<LOGIN> – логин клиента, задаётся строкой до 31 символа.
14	Задать пароль пользователя.	**esr(config-profile)# password ascii-text <TEXT>**	<TEXT> – строка [8..32] ASCII символов.

Шаг	Описание	Команда	Ключи
15	Создать пул адресов назначения (только для сервера).	**esr(config)# address-assignment pool <NAME>**	<NAME> – имя пула адресов назначения, задаётся строкой до 31 символа.
16	Задать подсеть, из которой будут выдаваться IP клиентам (только для сервера).	**esr(config-pool)# ip prefix <ADDR/LEN>**	<ADDR/LEN> – адрес подсети и префикс.
17	Создать шлюз для IKE и перейти в режим его конфигурирования.	**esr(config)# security ike gateway <NAME>**	<NAME> – имя шлюза протокола IKE, задаётся строкой до 31 символа.
18	Привязать политику IKE.	**esr(config-ike-gw)# ike-policy <NAME>**	<NAME> – имя политики протокола IKE, задаётся строкой до 31 символа.
19	Установить режим перенаправления трафика в туннель.	**esr(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.
20	Указать действие для DPD (не обязательно).	**esr(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.
21	Указать интервал между отправкой сообщений механизмом DPD (не обязательно).	**esr(config-ike-gw)#dead-peer-detection interval <SEC>**	<SEC> – интервал между отправкой сообщений механизмом DPD, принимает значения [1..180] секунд. Значение по умолчанию: 2.
22	Указать период времени для ответа на сообщения механизма DPD (не обязательно).	**esr(config-ike-gw)# dead-peer-detection timeout <SEC>**	<SEC> – период времени для ответа на сообщения механизма DPD, принимает значения [1..180] секунд. Значение по умолчанию: 30.

Шаг	Описание	Команда	Ключи
23	Указать версию IKE (не обязательно).	**esr(config-ike-gw)# version <VERSION>**	<VERSION> – версия IKE-протокола: **v1-only** или **v2-only**. Значение по умолчанию: v1-only
24	Установить IP подсети отправителя (только для сервера).	**esr(config-ike-gw)# local 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].
25	Установить IP-адрес локального шлюза IPsec-туннеля.	**esr(config-ike-gw)#local address <ADDR>**	<ADDR> – IP-адрес локального шлюза.
26	Установить IP-адрес удаленного шлюза IPsec-туннеля.	**esr(config-ike-gw)#remote address [any | <ADDR/LEN> [protocol { <TYPE> | <ID> } [port <PORT>]]**	Any – установить в качестве удаленного адреса – любой адрес клиента, в конфигурации сервера; <ADDR/LEN> – IP-адрес и маска подсети сервера, в конфигурации клиента.
27	Задать пул динамического выделения IP-адресов клиентам (только для сервера).	**esr(config-ike-gw)# remote network dynamic pool <NAME>**	<NAME> – имя пула адресов назначения, задаётся строкой до 31 символа.
28	Задать режим динамического установления удаленной подсети (только для клиента).	**esr(config-ike-gw)# remote network dynamic client**	
29	Задать профиль доступа для XAUTH-параметров (только для сервера).	**esr(config-ike-gw)# xauth access-profile <NAME>**	<NAME> – имя профиля доступа, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
30	Задать профиль доступа и логин для XAUTH-параметров (только для клиента).	**esr(config-ike-gw)# xauth access-profile <NAME> client <LOGIN>**	<NAME> – имя профиля доступа, задаётся строкой до 31имвола; <LOGIN> – логин клиента, задаётся строкой до 31 символа.
31	Задать интерфейс терминации выделенного IP для построения IPsec VPN (только для клиента).	**esr(config-ike-gw)# assign-interface loopback <INDEX>**	<INDEX> – индекс интерфейса, принимает значения [1..65535].
32	Создать профиль IPsec.	**esr(config)# security ipsec proposal <NAME>**	<NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа.
33	Определить алгоритм аутентификации для IPsec (не обязательно).	**esr(config-ipsec-proposal)# authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2_384, sha2-512. Значение по умолчанию: sha1.
34	Определить алгоритм шифрования для IPsec (не обязательно).	**esr(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.
35	Указать протокол (не обязательно).	**esr(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.

Шаг	Описание	Команда	Ключи
36	config-ipsec-proposal конфигурирования	**esr(config)# security ipsec policy <NAME>**	<NAME> – имя политики IPsec, задаётся строкой до 31 символа.
37	Привяжем политику к профилю	**esr(config-ipsec-policy)# proposal <NAME>**	<NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа.
38	Задать время жизни IPsec-туннеля (не обязательно).	**esr(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..86400] секунд. Значение по умолчанию: отключено.
39	Создать IPsec VPN и перейти в режим конфигурирования.	**esr(config)# security ipsec vpn <NAME>**	<NAME> – имя VPN, задаётся строкой до 31 символа.
40	Определить режим согласования данных, необходимых для активации VPN.	**esr(config-ipsec-vpn)# mode <MODE>**	<MODE> – режим работы VPN, принимает значения: ike, manual.
41	Привязать IPsec политику к VPN.	**esr(config-ipsec-vpn)#ike ipsec-policy <NAME>**	<NAME> – имя IPsec-политики, задаётся строка до 31 символа.

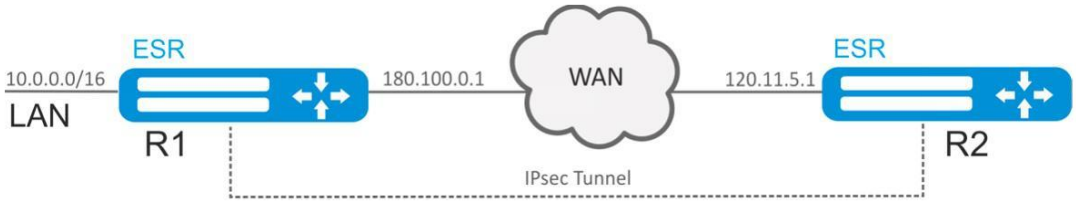
Шаг	Описание	Команда	Ключи
42	Задать значение DSCP для использования в IP-заголовке исходящих пакетов IKE-протокола (не обязательно).	**esr(config-ipsec-vpn)#ike dscp <DSCP>**	DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 63.
43	Устанавливается режим активации VPN.	**esr(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.
44	Осуществить привязка IKE-шлюза к VPN.	**esr(config-ipsec-vpn)# ike gateway <NAME>**	<NAME> – имя IKE-шлюза, задаётся строкой до 31 символа.
45	Установить значение временного интервала в секундах, по истечению которого соединение закрывается, если не было принято или передано ни одного пакета через SA (не обязательно).	**esr(config-ipsec-vpn)# ike idle-time <TIME>**	<TIME> – интервал в секундах, принимает значения [4..86400]. Значение по умолчанию: 0.
46	Отключить пересогласование ключей до разрыва IKE-соединения по истечению времени, количеству переданных пакетов или байт (не обязательно).	**esr(config-ipsec-vpn)#ike rekey disable**	Значение по умолчанию: включено.

Шаг	Описание	Команда	Ключи
47	Настроить начало пересогласования ключей IKE-соединения до истечения времени жизни (не обязательно).	**esr(config-ipsec-vpn)# ike rekey margin { seconds <SEC> | packets <PACKETS> | kilobytes <KB> }**	<SEC> – интервал времени в секундах, оставшийся до закрытия соединения (задается командой lifetimeseconds) . Принимает значения [4..86400]. Значение по умолчанию: 540 <PACKETS> – количество пакетов, оставшихся до закрытия соединения (задается командой lifetimepackets). Принимает значения [4..86400]. Значение по умолчанию: отключено. <KB> – объем трафика в килобайтах, оставшийся до закрытия соединения (задается командой lifetimekilobytes). Принимает значения [4..86400] Значение по умолчанию: отключено.
48	Установить уровень случайного разброса значений параметров marginseconds, marginpackets, marginkilobytes (не обязательно).	**esr(config-ipsec-vpn)# ike rekey randomization <VALUE>**	<VALUE> – максимальный процент разброса значений, принимает значения [1..100]. Значение по умолчанию: 100.
49	Описать VPN (не обязательно).	**esr(config-ipsec-vpn)# description <DESCRIPTION>**	<DESCRIPTION> – описание профиля, задаётся строкой до 255 символов.
50	Активировать IPsec VPN.	**esr(config-ipsec-vpn)# enable**	

Шаг	Описание	Команда	Ключи
51	Включить режим переподключения клиентов XAUTH с одним логином/паролем (только для сервера) (не обязательно).	**esr(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.

11.4.6 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 устройство R1, а устройство 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:

1. Конфигурирование R1
   Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```
esr# configure
esr(config)# security zone untrusted
esr(config-zone)# exit
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# security-zone untrusted
esr(config-if-gi)# ip address 180.100.0.1/24
esr(config-if-gi)# exit
```

   Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```
esr(config)# object-group service ISAKMP
esr(config-object-group-service)# port-range 500,4500
esr(config-object-group-service)# 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:

```
esr(config)# security ike proposal IKEPROP
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm sha1
esr(config-ike-proposal)# encryption algorithm 3des
esr(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:

```
esr(config)# security ike policy IKEPOLICY
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# authentication method xauth-psk-key
esr(config-ike-policy)# proposal IKEPROP
esr(config-ike-policy)# exit
```

Создадим профиль доступа и заведем в нем пару логин и пароль для клиента IPsec VPN:

```
esr(config)# access profile XAUTH
esr(config-access-profile)# user client1
esr(config-profile)# password ascii-text password123
esr(config-profile)# exit
esr(config-access-profile)# exit
```

Создадим пул адресов назначения, из которого будут выдаваться IP клиентам IPsec VPN:

```
esr-1000(config)# address-assignment pool CLIENT_POOL
esr-1000(config-pool)# ip prefix 192.0.2.0/24
esr-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:

```
esr(config)# security ike gateway IKEGW
esr(config-ike-gw)# ike-policy IKEPOLICY
esr(config-ike-gw)# local address 180.100.0.1
esr(config-ike-gw)# local network 10.0.0.0/16
esr(config-ike-gw)# remote address any
esr(config-ike-gw)# remote network dynamic pool CLIENT_POOL
esr(config-ike-gw)# dead-peer-detection action clear
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# xauth access-profile XAUTH
esr(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:

```
esr(config)# security ipsec proposal IPSECPROP
esr(config-ipsec-proposal)# authentication algorithm sha1
esr(config-ipsec-proposal)# encryption algorithm 3des
esr(config-ipsec-proposal)# exit
```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы.

```
esr(config)# security ipsec policy IPSECPOLICY
esr(config-ipsec-policy)# proposal IPSECPROP
esr(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*.

```
esr(config)# security ipsec IPSECVPN
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel by-request
esr(config-ipsec-vpn)# ike gateway IKEGW
esr(config-ipsec-vpn)# ike ipsec-policy IPSECPOLICY
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
```

Разрешим протокол esp и udp порты 500, 4500 в конфигурации firewall для установления IPsec VPN:

```
esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol udp
esr(config-zone-pair-rule)# match destination-port ISAKMP
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)#   rule 2
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol esp
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# end
```

2. Конфигурирование R2
   Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```
esr# configure
esr(config)# interface gi 1/0/1
esr(config-if)# ip address 120.11.5.1/24
esr(config-if)# security-zone untrusted
esr(config-if)# exit
```

Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```
esr(config)# object-group service ISAKMP
esr(config-addr-set)# port-range 500,4500
esr(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:

```
esr(config)# security ike proposal IKEPROP
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm sha1
esr(config-ike-proposal)# encryption algorithm 3des
esr(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:

```
esr(config)# security ike policy IKEPOLICY
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# authentication method xauth-psk-key
esr(config-ike-policy)# authentication mode client
esr(config-ike-policy)# proposal IKEPROP
esr(config-ike-policy)# exit
```

Создадим профиль доступа и заведем в нем пару логин и пароль:

```
esr(config)# access profile XAUTH
esr(config-access-profile)# user client1
esr(config-profile)# password ascii-text password123
esr(config-profile)# exit
esr(config-access-profile)# exit
```

Создадим интерфейс loopback для терминации IP-адреса, полученного от IPsec VPN сервера:

```
esr(config)# interface loopback 8
esr(config-loopback)# exit
```

Создадим шлюз протокола IKE. В данном профиле указывается политика, интерфейс терминации, режим динамического установления удаленной подсети, выбор профиля доступа для XAUTH и режим перенаправления трафика в туннель по политике:

```
esr(config)# security ike gateway IKEGW
esr(config-ike-gw)# ike-policy IKEPOLICY
esr(config-ike-gw)# assign-interface loopback 8
esr(config-ike-gw)# local address 120.11.5.1
esr(config-ike-gw)# remote address 180.100.0.1
esr(config-ike-gw)# remote network dynamic client
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# xauth access-profile xauth client client1
esr(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:

```
esr(config)# security ipsec proposal IPSECPROP
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы:

```
esr(config)# security ipsec policy IPSECPOLICY
esr(config-ipsec-policy)# proposal IPSECPROP
esr(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:*

```
esr(config)# security ipsec vpn IPSECVPN
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway IKEGW
esr(config-ipsec-vpn)# ike ipsec-policy IPSECPOLICY
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
```

Разрешим протокол esp и udp порты 500,4500 в конфигурации firewall для установления IPsec VPN:

```
esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol udp
esr(config-zone-pair-rule)# match destination-port ISAKMP
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)#   rule 2
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol esp
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# end
```

Состояние туннеля можно посмотреть командой:

```
esr# show security ipsec vpn status IPSECVPN
```

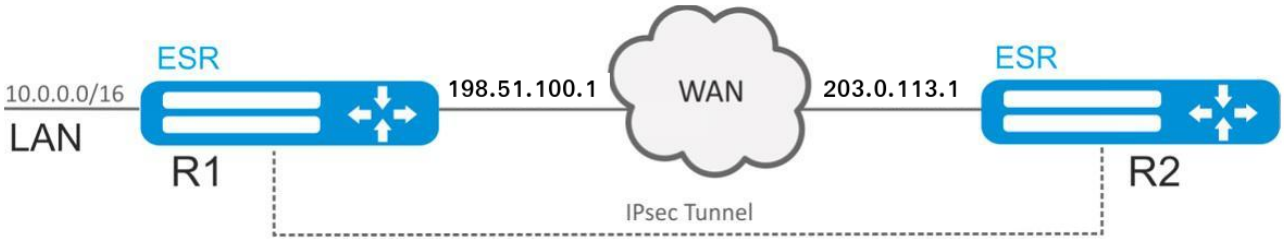
Конфигурацию туннеля можно посмотреть командой:

```
esr# show security ipsec vpn configuration IPSECVPN
```

В firewall необходимо разрешить протокол ESP и ISAKMP (UDP-порт 500, 4500).

11.4.7 Пример настройки DPD (Dead Peer Detection)

Задача:



Настроить Dead Peed 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:

```
esr# configure
esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# dead-peer-detection action restart
esr(config-ike-gw)# dead-peer-detection interval 1
esr(config-ike-gw)# dead-peer-detection timeout 4
esr(config-ike-gw)# exit
```

Состояние туннеля можно посмотреть командой:

```
esr# show security ipsec vpn status ipsec1
```

Конфигурацию туннеля можно посмотреть командой:

```
esr# show security ipsec vpn configuration ipsec1
```

После разрыва соединения между R1 и R2 на R1 IPsec-туннель начнет перестраиваться спустя 4 секунды после разрыва.

```
esr# 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
esr# 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
```

11.5 Настройка LT-туннелей

LT (англ. Logical Tunnel – логический туннель) – тип туннелей, предназначенный для передачи маршрутной информации и трафика между различными виртуальными устройствами (VRF), сконфигурированными на одном аппаратном устройстве. LT-туннель может использоваться для организации взаимодействия между двумя или более VRF с применением ограничений firewall.

11.5.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать LT-туннели для каждого из существующих VRF.	**esr(config)# tunnel lt <ID>**	<ID> – идентификатор туннеля в диапазоне [1..128].
2	Указать описание конфигурируемых туннелей (не обязательно).	**esr(config-lt)# description <DESCRIPTION>**	<DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов.
3	Включить каждый LT-туннель в соответствующий VFR.	**esr(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.	**esr(config-lt)# security-zone<NAME>**	<NAME> – имя зоны безопасности, задаётся строкой до 12 символов.
		esr(config-lt)# ip firewall disable	
5	Для каждого LT-туннеля задать номер противоположный LT туннель (в другом VRF).	**esr(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.	**esr(config-lt)# ip address <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].
7	Включить туннели.	**esr(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 (не обязательно).	**esr(config-lt)# load-average <TIME>**	<TIME> – интервал в секундах, принимает значения [5..150]. Значение по умолчанию: 5.
10	Указать размер MTU (Maximum Transmition 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".	**esr(config-lt)# mtu <MTU>**	<MTU> – значение MTU, принимает значения в диапазоне: • для ESR-10/12V(F)/14VF/15 – [1280..9600]; • для ESR-20/21/30 – [1280..9500]; • для ESR-100/200/1000/1200/1500/1511/1700/3100/3200 – [1280..10000]. Значение по умолчанию: 1500.

11.5.2 Пример настройки

Задача:

Организовать взаимодействие между хостами, терминированными в двух VRF vrf_1 и vrf_2.

Исходная конфигурация:

```
hostname esr
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:

```
esr(config)# tunnel lt 1
esr(config-lt)# ip vrf forwarding vrf_1
esr(config-lt)# ip firewall disable
esr(config-lt)# ip address 192.168.0.1/30
esr(config-lt)# exit
esr(config)# tunnel lt 2
esr(config-lt)# ip vrf forwarding vrf_2
esr(config-lt)# ip firewall disable
esr(config-lt)# ip address 192.168.0.2/30
esr(config-lt)# exit
```

Укажем для каждого LT-туннеля LT-туннель из VRF, с которым необходимо установить связь, и активируем их:

```
esr(config)# tunnel lt 1
esr(config-lt)# peer lt 2
esr(config-lt)# enable
esr(config-lt)# exit
esr(config)# tunnel lt 2
esr(config-lt)# peer lt 1
esr(config-lt)# enable
esr(config-lt)# exit
```

Если в VRF не сконфигурирован ни один из протоколов динамической маршрутизации, то необходимо указать статические маршруты для каждого VRF:

```
esr(config)# ip route vrf vrf_1 0.0.0.0/0 192.168.0.2
esr(config)# ip route vrf vrf_2 0.0.0.0/0 192.168.0.1
```

12 Управление QoS

- Базовый QoS
  - Алгоритм настройки
  - Пример настройки
- Расширенный QoS
  - Алгоритм настройки
  - Пример настройки

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.

12.1 Базовый QoS

В базовом режиме на маршрутизаторах ESR и контроллере WLC классификация (направление трафика в очередь) и перемаркировка работает только на входе (на интерфейсе через который поступает трафик должен быть включен QoS).

12.1.1 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.	**esr(config-if-gi)# qos enable**	
2	Установить режим доверия к значениям кодов 802.1p и DSCP во входящих пакетах (не обязательно).	**esr(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.

Шаг	Описание	Команда	Ключи
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).	**esr(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
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).	**esr(config)# qos map cos-queue <COS> to <QUEUE>**	<COS> – классификатор обслуживания в теге 802.1q 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.	**esr(config)# qos map dscp-queue <DSCP> to <DSCP>**	<DSCP> – классификатор обслуживания в IP-заголовке пакета, принимает значения [0..63].

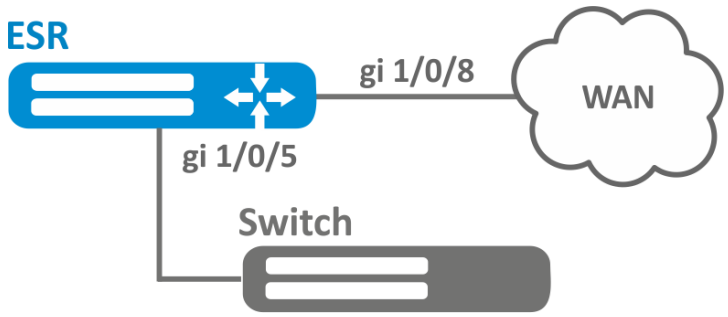
Шаг	Описание	Команда	Ключи
6	Включить изменения кодов DSCP в соответствии с таблицей DSCP-Mutation (в случае необходимости перемаркировки).	**esr(config)# qos dscp mutation**	
7	Установить номер очереди по умолчанию, в которую попадает весь трафик кроме IP в режиме доверия DSCP-приоритетам.	**esr(config)# qos queue default <QUEUE>**	<QUEUE> – идентификатор очереди, принимает значения [1..8].
8	Задать количество приоритетных очередей. Оставшиеся очереди являются взвешенными (не обязательно).	**esr(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-й, в сторону уменьшения номера очереди. Значение по умолчанию: 8.
9	Определить вес для соответствующих взвешенных очередей.	**esr(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.

Шаг	Описание	Команда	Ключи
10	Установить ограничение скорости исходящего трафика для определенной очереди или интерфейса в целом. Команда актуальна только для BasicQoS-режима интерфейса. Ели трафик на входе был классифицирован при помощи расширенного QoS, ограничение не сработает (в случае необходимости ограничения скорости входящего потока).	**esr(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 TengigabitEthernet 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.
11	Установить ограничение скорости входящего трафика (в случае необходимости ограничения скорости исходящего потока).	**esr(config-if-gi)# rate-limit <BANDWIDTH> [BURST]**	<BANDWIDTH> – средняя скорость трафика в Кбит/с, принимает значение [3000..10000000] для TengigabitEthernet 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.

12.1.2 Пример настройки

Задача:

Настроить следующие ограничения на интерфейсе gigabitethernet 1/0/8: 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:

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

Перенаправим трафик с DSCP 22 в первую приоритетную очередь:

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

Перенаправим трафик с DSCP 14 в седьмую взвешенную очередь:

```
esr(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:

```
esr(config)# interface gigabitethernet 1/0/5
esr(config-if-gi)# qos enable
esr(config-if-gi)# exit
```

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

```
esr(config)# interface gigabitethernet 1/0/8
esr(config-if-gi)# qos enable
```

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

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

Просмотреть статистику по QoS можно командой:

```
esr# show qos statistics gigabitethernet 1/0/8
```

12.2 Расширенный QoS

12.2.1 Алгоритм настройки

В расширенном режиме на маршрутизаторах ESR 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.	**esr(config)# class-map <NAME>**	<NAME> – имя создаваемого класса, задается строкой до 31 символа.
3	Задать описание класса QoS (не обязательно).	**esr(config-class-map)# description <description>**	<description> – до 255 символов.
4	Определить трафик, относящийся к конфигурируемому классу по списку контроля доступа (ACL).	**esr(config-class-map)# match access-group <NAME>**	<NAME> – имя списка контроля доступа, задаётся строкой до 31 символа.
5	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).	**esr(config-class-map)# set dscp <DSCP>**	<DSCP> – значение кода DSCP, принимает значения [0..63].
6	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).	**esr(config-class-map)# set ip-precedence <IPP>**	<IPP> – значение кода IP Precedence, принимает значения [0..7].

Шаг	Описание	Команда	Ключи
7	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).	**esr(config-class-map)# set cos <COS>**	<COS> – значение 802.1p приоритета, принимает значения [0..7].
8	Создать политику QoS и осуществить переход в режим настройки параметров политики.	**esr(config)# policy-map <NAME>** **esr(config-policy-map)#**	<NAME> – имя создаваемой политики, задается строкой до 31 символа.
9	Задать описание политики QoS (не обязательно).	**esr(config-policy-map)# description <description>**	<description> – до 255 символов.
10	Установить гарантированную полосу пропускания исходящего трафика для политики в целом.	**esr(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.
11	Включить автоматическое распределение полосы пропускания между классами, в которых нет настройки полосы пропускания, включая класс по умолчанию (в случае необходимости).	**esr(config-policy-map)# shape auto-distribution**	

Шаг	Описание	Команда	Ключи
12	Включить указанный QoS-класс в политику и осуществить переход в режим настройки параметров класса в рамках политики.	**esr(config-policy-map)# class <NAME>** **esr(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.
13	Включить политику QoS в класс QoS для создания иерархического QoS.	**esr(config-class-policy-map)# service-policy <NAME>**	<NAME> – имя политики, задается строкой до 31 символа. Вкладываемая политика должна быть уже создана.
14	Установить гарантированную полосу пропускания исходящего трафика для класса в рамках политики (при необходимости).	**esr(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
15	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).	**esr(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.
16	Определить режим работы класса (не обязательно).	**esr(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**.

Шаг	Описание	Команда	Ключи
17	Задать приоритет класса в WRR-процессе (при необходимости).	**esr(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.
18	Перевести класс в режим StrictPriority и задать приоритет класса (при необходимости).	**esr(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.
19	Определить предельное количество виртуальных очередей (не обязательно).	**esr(config-class-policy-map)# fair-queue <QUEUE-LIMIT>**	<QUEUE-LIMIT> – предельное количество виртуальных очередей, принимает значения в диапазоне [16..4096]. Значение по умолчанию: 16.
20	Определить предельное количество пакетов для виртуальной очереди (не обязательно).	**esr(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
21	Определить параметры RED (Random Early Detection) (при необходимости).	**esr(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>

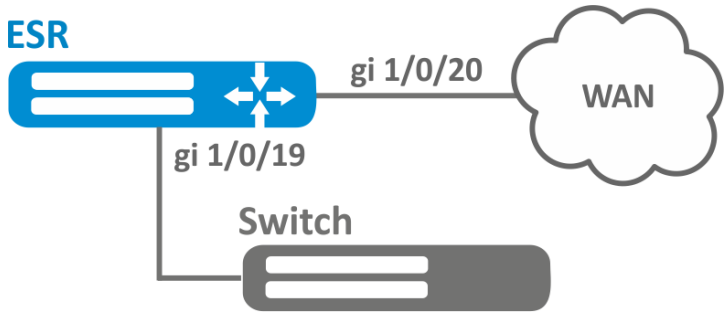
Шаг	Описание	Команда	Ключи
22	Определить параметры GRED (Generalized Random Early Detection) (при необходимости).	**esr(config-class-policy-map)# random-detect queue <QUEUE-NUM> [dscp <DSCP> | precedence <IPP>] <LIMIT> <MIN> <MAX> <APS> <APS-NUM> <PROBABILITY>**	<QUEUE-NUM> – номер очереди [1..16]; <DSCP> – классификатор обслуживания в IP-заголовке пакета, принимает значения [0..63]; <IPP> – значение кода IP Precedence, принимает значения [0..7]; <PRECEDENCE> – значение IP Precendence [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 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>
23	Включить протокол компрессии tcp-заголовков для трафика отдельного класса (при необходимости).	**esr(config-class-policy-map)# compression header ip tcp**	
24	Включить сервис QoS на интерфейсе /туннеле/сетевом мосту.	**esr(config-if-gi)# qos enable**	

Шаг	Описание	Команда	Ключи
25	Назначить политику QoS на сконфигурируемом интерфейсе/ туннеле/сетевом мосту для классификации входящего (input) или приоритизации исходящего (output) трафика.	**esr(config-if-gi)# service-policy { input | output } <NAME>**	<NAME> – имя QoS-политики, задаётся строкой до 31 символа.

12.2.2 Пример настройки

Задача:

Классифицировать приходящий трафик по подсетям (10.0.11.0/24, 10.0.12.0/24), произвести маркировку по DSCP (38 и 42) и произвести 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:

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

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

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

Создаём политику и определяем ограничение общей полосы пропускания:

```
esr(config)# policy-map fl
esr(config-policy-map)# shape average 250000
```

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

```
esr(config-policy-map)# class fl1
esr(config-class-policy-map)# shape average 40000
esr(config-class-policy-map)# exit
esr(config-policy-map)# class fl2
esr(config-class-policy-map)# shape average 60000
esr(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:

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

Включаем QoS на интерфейсах, политику на входе интерфейса gi 1/0/19 для классификации и на выходе gi1/0/20 для применения ограничений и режима SFQ для класса по умолчанию:

```
esr(config)# interface gigabitethernet 1/0/19
esr(config-if-gi)# qos enable
esr(config-if-gi)# service-policy input fl
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/20
esr(config-if-gi)# qos enable
esr(config-if-gi)# service-policy output fl
esr(config-if-gi)# exit
```

Для просмотра статистики используется команда:

```
esr# do show qos policy statistics gigabitethernet 1/0/20
```

13 Управление маршрутизацией

- Политика анонсирования маршрутной информации
  - Протокол RIP
  - Протокол OSPF
  - Протокол IS-IS
  - Протокол iBGP
  - Протокол eBGP
- Конфигурирование статических маршрутов
  - Алгоритм настройки
  - Пример настройки статических маршрутов
- Настройка RIP
  - Алгоритм настройки
  - Пример настройки RIP
- Настройка OSPF
  - Алгоритм настройки
  - Пример настройки OSPF
  - Пример настройки OSPF stub area
  - Пример настройки Virtual link
- Настройка BGP
  - Алгоритм настройки
  - Пример настройки
  - Политика выбора лучшего маршрута в протоколе BGP
- Настройка BFD
  - Настройка таймеров
  - Алгоритм настройки
  - Пример настройки BFD с BGP
- Настройка политики маршрутизации PBR
  - Алгоритм настройки Route-map для BGP
  - Пример настройки 1. Route-map для BGP
  - Пример настройки 2. 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
- Настройка IS-IS
  - Алгоритм настройки
  - Пример настройки

13.1 Политика анонсирования маршрутной информации

13.1.1 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 запрещает все, что явно не разрешено предыдущими правилами. Prefix-list — последнее (неявное) правило запрещает все, что явно не разрешено предыдущими правилами.	Процесс RIP
Export	Без отдельных команд анонсирования маршрутизатор или контроллер не отправляет маршрутную информацию		Prefix-list — последнее (неявное) правило разрешает все, что явно не запрещено предыдущими правилами. Prefix-list — последнее (неявное) правило разрешает все, что явно не запрещено предыдущими правилами.	

13.1.2 Протокол OSPF

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 запрещает все, что явно не разрешено предыдущими правилами. Prefix-list — последнее (неявное) правило запрещает все, что явно не разрешено предыдущими правилами.	Процесс OSPF

in/ out	Политика по умолчанию	Способы Анонсирования	Способы фильтрации	Уровни применения политик фильтрации
Export	Анонсируется информация о интерфейсах, на которых включен протокол OSPF		Route-map — последнее (неявное) правило разрешает все, что явно не запрещено предыдущими правилами. Prefix-list — последнее (неявное) правило разрешает все, что явно не запрещено предыдущими правилами. *Фильтрация анонсируемой маршрутной информации возможна для следующих типов OSPF-маршрутов: E2, E1.*	

13.1.3 Протокол IS-IS

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 запрещает все, что явно не разрешено предыдущими правилами. Prefix-list — последнее (неявное) правило запрещает все, что явно не разрешено предыдущими правилами.	Процесс IS-IS
Export	Анонсируется информация о интерфейсах, на которых включен протокол IS-IS		Route-map — последнее (неявное) правило разрешает все, что явно не запрещено предыдущими правилами. Prefix-list — последнее (неявное) правило разрешает все, что явно не запрещено предыдущими правилами.	

13.1.4 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 запрещает все, что явно не разрешено предыдущими правилами. Prefix-list — последнее (неявное) правило запрещает 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 разрешает все, что явно не разрешено предыдущими правилами. Prefix-list — последнее (неявное) правило разрешает все, что явно не разрешено предыдущими правилами.	

13.1.5 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 запрещает все, что явно не разрешено предыдущими правилами. Prefix-list — последнее (неявное) правило запрещает все, что явно не разрешено предыдущими правилами.	address-family, peer-group, neighbor

in/ out	Политика по умолчанию	Способы Анонсирования	Способы фильтрации	Уровни применения политик фильтрации
Export	Анонсирование маршрутов запрещено до применения разрешающего route-map или prefix-list		Route-map — последнее (неявное) правило запрещает все, что явно не разрешено предыдущими правилами. Prefix-list — последнее (неявное) правило запрещает все, что явно не разрешено предыдущими правилами.	

13.2 Конфигурирование статических маршрутов

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

13.2.1 Алгоритм настройки

Добавить статический маршрут возможно командой в режиме глобальной конфигурации:

```
esr(config)# ip route [ vrf <VRF> ] <SUBNET> { <NEXTHOP> | interface <IF> | tunnel <TUN> | wan load-balance rule <RULE> [<METRIC>] | blackhole | unreachable | prohibit } [ <METRIC> ] [ track <TRACK-ID> ] [ bfd ]
```

- <VRF> – имя экземпляра VRF, задается строкой до 31 символа;
- <SUBNET> – адрес назначения, может быть задан в следующем формате:
  - 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];
- <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;
- 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);
- bfd – при указании данного ключа активируется удаление статического маршрута в случае недоступности next-hop.

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

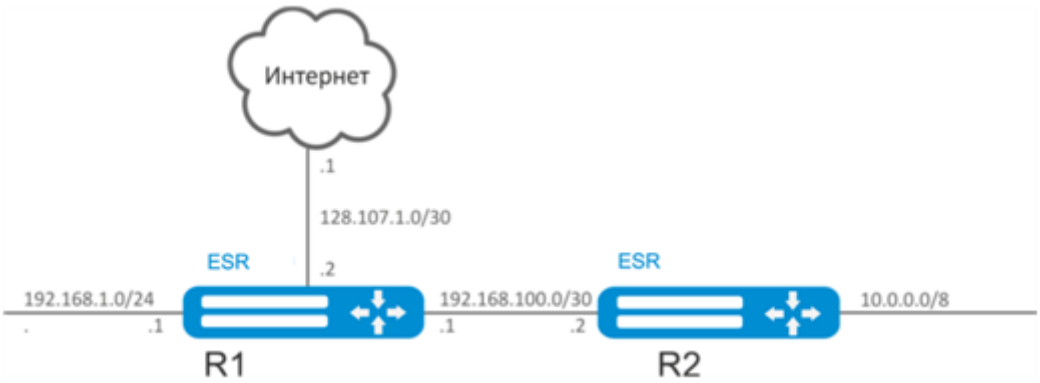
```
ipv6 route [ vrf <VRF> ] <SUBNET> { <NEXTHOP> [ resolve ] | interface <IF> | wan load-balance rule <RULE> | blackhole | unreachable | prohibit } [ <METRIC> ] [ bfd ]
```

- <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].
- <NEXTHOP> – IPv6-адрес шлюза, задаётся в виде X: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;
- <IF> – имя IP-интерфейса, задаётся 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].
- bfd – при указании данного ключа активируется удаление статического маршрута в случае недоступности next-hop.

13.2.2 Пример настройки статических маршрутов

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 R1:

```
esr# 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:

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

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

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

```
esr(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):

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

Зададим имя устройства для R2:

```
esr# 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:

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

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

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

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

Проверить таблицу маршрутов можно командой:

```
esr# show ip route
```

13.3 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. Каждое RIP-устройство по умолчанию вещает в сеть свою полную таблицу маршрутизации один раз в 30 секунд. RIP работает на 3-м уровне стека TCP/IP, используя UDP-порт 520.

13.3.1 Алгоритм настройки

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

Шаг	Описание	Команда	Ключи
3	Создать списки IP-подсетей, которые в дальнейшем будут использоваться для фильтрации анонсируемых и получаемых IP-маршрутов.	**esr(config)# ip prefix-list <NAME>**	<NAME> – имя конфигурируемого списка подсетей, задаётся строкой до 31 символа.
4	Разрешить (permit) или запретить (deny) списки префиксов.	**esr(config-pl)# permit {object-group <OBJ-GROUP-NETWORK-NAME > <ADDR/LEN> | <IPV6-ADDR/LEN> } [{ eq <LEN> | le <LEN> | ge <LEN> [le <LEN>] }]** **esr(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.	**esr(config)# router rip** **esr(config-rip)#**	
6	Включить RIP-протокол.	**esr(config-rip)# enable**	
7	Определить алгоритм аутентификации протокола RIP (не обязательно).	**esr(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).	**esr(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).	**esr(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).	**esr(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).	**esr(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).	**esr(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 производиться удаление маршрута (не обязательно).	**esr(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.	**esr(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).	**esr(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).	**esr(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.
		esr(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.

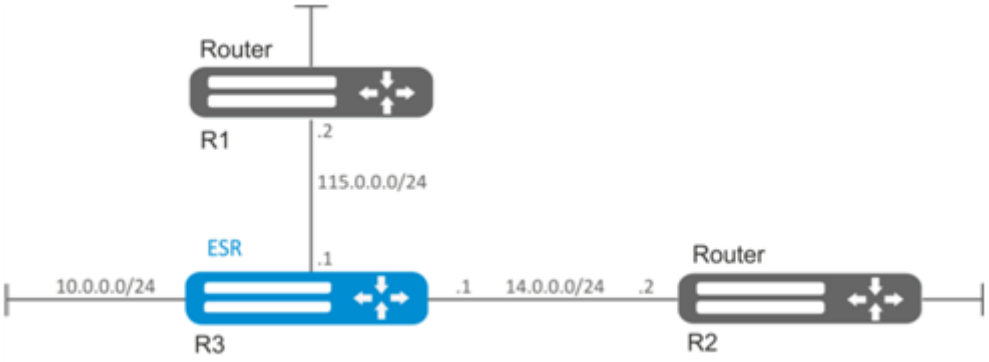
Шаг	Описание	Команда	Ключи
		esr(config-rip)# redistribute ospf <ID><ROUTE-TYPE> [route-map <NAME>]	<ID> – номер процесса, может принимать значение [1..65535]; <ROUTE-TYPE> – тип маршрута: • **intra - area** – анонсирование маршрутов OSPF-процесса в пределах зоны; • **inter - area** – анонсирование маршрутов 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.
		esr(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.	**esr(config)# interface <IF-TYPE><IF-NUM>**	<IF-TYPE> тип интерфейса; <IF-NUM> – F/S/P – F-фрейм (1), S – слот (0), P – порт.

Шаг	Описание	Команда	Ключи
		esr(config)# tunnel <TUN-TYPE><TUN-NUM>	<TUN-TYPE> тип туннеля; <TUN-NUM> номер туннеля.
		esr(config)# bridge <BR-NUM>	<BR-NUM> – номер bridge.
18	Установить величину метрики RIP-маршрутов на интерфейсе (не обязательно).	**esr(config-if-gi)# ip rip metric <VALUE>**	<VALUE> – величина метрики, задаётся в размере [0..32767]. Значение по умолчанию: 5.
19	Установить режим анонсирования маршрутов по протоколу RIP (не обязательно).	**esr(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).	**esr(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).	**esr(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].

13.3.2 Пример настройки RIP

Задача:

Настроить на устройстве протокол RIP для обмена маршрутной информацией с соседними устройствами. Маршрутизатор/контроллер 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 выше.

Перейдём в режим конфигурирования протокола RIP:

```
esr(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:

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

Для анонсирования протоколом статических маршрутов выполним команду:

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

Настроим таймер, отвечающий за отправку маршрутной информации:

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

После установки всех требуемых настроек включаем протокол:

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

Для того чтобы просмотреть таблицу маршрутов RIP, воспользуемся командой:

```
esr# show ip rip
```

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

13.4 Настройка OSPF

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

13.4.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Настроить приоритетность протокола OSPF-маршрутизации для основной таблицы маршрутизации (не обязательно).	**esr(config)# ip protocols ospf preference <VALUE>** **esr(config-vrf)# ip protocols ospf preference <VALUE>**	<VALUE> – приоритетность протокола, принимает значения в диапазоне [1..255]. Значение по умолчанию: 150.
2	Настроить емкость таблиц маршрутизации протокола OSPF (не обязательно).	**esr(config)# ip protocols ospf max-routes <VALUE>** **esr(config)# ipv6 protocols ospf max-routes <VALUE>**	<VALUE> – количество маршрутов протокола OSPF в маршрутной таблице, принимает значения в диапазоне: • для ESR-1000/1200/1500/1511/1700/3100/3200 – [1..500000]; • для ESR-20/21/30/100/200 – [1..300000]; • для ESR-10/12V(F)/14VF/15 – [1..30000] Значение по умолчанию для глобального режима: • для ESR-1000/1200/1500/1511/1700/3100/3200 – (500000); • для ESR-20/21/30/100/200 – (300000); • для ESR-10/12V(F)/14VF/15 – (30000). Значение по умолчанию для VRF: 0.
3	Включить вывод информации о состоянии отношений с соседями для протокола маршрутизации OSPF (не обязательно).	**esr(config)# router ospf log-adjacency-changes** **esr(config)# ipv6 router ospf log-adjacency-changes**	

Шаг	Описание	Команда	Ключи
4	Создать списки IP-подсетей, которые в дальнейшем будут использоваться для фильтрации анонсируемых и получаемых IP-маршрутов (не обязательно).	**esr(config)# ip prefix-list <NAME>** **esr(config)# ipv6 prefix-list <NAME>**	<NAME> – имя конфигурируемого списка подсетей, задаётся строкой до 31 символа.
5	Разрешить (permit) или запретить (deny) списки префиксов (не обязательно).	**esr(config-pl)# permit [{ object-group <OBJ-GROUP-NETWORK-NAME> | <ADDR/LEN> | <IPV6-ADDR/LEN> }] [{ eq <LEN> | le <LEN> | ge <LEN> [le <LEN>] }]** **esr(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 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.
6	Добавить OSPF-процесс в систему и осуществить переход в режим настройки параметров OSPF-процесса.	**esr(config)# router ospf <ID> [vrf <VRF>]** **esr(config)# ipv6 router ospf <ID> [vrf <VRF>]**	<ID> – номер автономной системы процесса, принимает значения [1..65535] <VRF> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет работать протокол маршрутизации.

Шаг	Описание	Команда	Ключи
7	Установить идентификатор устройства для данного OSPF-процесса.	**esr(config-ospf)# router-id { <ID> | <IF> | <TUN> }** **esr(config-ipv6-ospf)# router-id { <ID> | <IF> | <TUN> }**	<ID> – идентификатор устрйоства, 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	Определить приоритетность маршрутов процесса OSPF (не обязательно).	**esr(config-ospf)# preference <VALUE>** **esr(config-ipv6-ospf)# preference <VALUE>**	<VALUE> – приоритетность маршрутов процесса OSPF, принимает значения в диапазоне [1..255].
9	Определить максимальное количество равнозначных маршрутов до цели (не обязательно).	**esr(config-ospf)# maximum-path <PATHS>** **esr(config-ipv6-ospf)# maximum-path <PATHS>**	<PATHS> – количество равноценных маршрутов до цели, принимает значения в диапазоне [1..32]. Значение по умолчанию: 16.
10	Включить совместимость с RFC 1583 (не обязательно).	**esr(config-ospf)# compatible rfc1583** **esr(config-ipv6-ospf)# compatible rfc1583**	
11	Добавить фильтрацию подсетей во входящих или исходящих обновлениях (не обязательно).	**esr(config-ospf)# prefix-list <PREFIX-LIST-NAME> { in | out }** **esr(config-ipv6-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.

Шаг	Описание	Команда	Ключи
12	Включить анонсирование маршрутов, полученных альтернативным способом (не обязательно).	**esr(config-ospf)# redistribute static [route-map <NAME>]**	<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых статических маршрутов, задаётся строкой до 31 символа.
		esr(config-ipv6-ospf)# redistribute static [route-map <NAME>]	
		esr(config-ospf)# 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.
		esr(config-ipv6-ospf)# redistribute connected [route-map <NAME>]	
		esr(config-ospf)# redistribute rip [route-map <NAME>]	<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых RIP-маршрутов, задаётся строкой до 31 символа.
		esr(config-ospf)# 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.
		esr(config-ipv6-ospf)# redistribute bgp <AS> [route-map <NAME>]	
13	Активировать OSPF-процесс.	**esr(config-ospf)# enable**	
		esr(config-ipv6-ospf)# enable	
14	Создать OSPF-область и перейти в режим конфигурирования области.	**esr(config-ospf)# area <AREA_ID>**	<AREA_ID> – идентификатор области, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
		esr(config-ipv6-ospf)# area <AREA_ID>	

Шаг	Описание	Команда	Ключи
15	Включить анонсирование подсетей (не обязательно).	**esr(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].
		esr(config-ipv6-ospf-area)# 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].
16	Определить тип области (не обязательно).	**esr(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).
		esr(config-ipv6-ospf-area)# area-type <TYPE> [no-summary]	
17	Включить генерацию маршрута по умолчанию для NSSA-области и анонсирование его в качестве NSSA-LSA (не обязательно).	**esr(config-ospf-area)# default-information-originate**	
		esr(config-ipv6-ospf-area)# default-information-originate	

Шаг	Описание	Команда	Ключи
18	Включить суммаризацию или скрытие подсетей (не обязательно).	**esr(config-ospf-area)# summary-address <ADDR/LEN> { advertise | not-advertise }**	<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]; • **advertise** – при указании команды вместо указанных подсетей будет анонсироваться суммарная подсеть; • **not - advertise** – при указании команды подсети, входящие в указанную подсеть, анонсироваться не будут.
		esr(config-ipv6-ospf-area)# summary-address <IPV6-ADDR/LEN> { advertise | not-advertise }	<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]; • **advertise** – при указании команды вместо подсетей, входящих в указанную подсеть, будет анонсироваться суммарная подсеть; • **not-advertise** – подсети входящие в указанную подсеть анонсироваться не будут.
19	Активировать OSPF-область.	**esr(config-ospf-area)# enable**	
		esr(config-ipv6-ospf-area)# enable	

Шаг	Описание	Команда	Ключи
20	Установить виртуальное соединение между основной и удаленными областями, имеющими между ними несколько областей (не обязательно).	**esr(config-ospf-area)# virtual-link <ID>** **esr(config-ipv6-ospf-area)# virtual-link <ID>**	<ID> – идентификатор маршрутизатора/ контроллера, с которым устанавливается виртуальное соединение, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
21	Установить интервал времени в секундах, по истечении которого маршрутизатор/контроллер повторно отправит пакет, который не получил подтверждения о получении (не обязательно).	**esr(config-ospf- vlink)# restransmit-interval <TIME>** **esr(config-ipv6-ospf- vlink)# restransmit-interval <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 5 секунд.
22	Установить интервал времени в секундах, по истечении которого маршрутизатор/контроллер отправляет следующий hello-пакет (не обязательно).	**esr(config-ospf- vlink)# hello-interval <TIME>** **esr(config-ipv6-ospf- vlink)# hello-interval <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 10 секунд.
23	Установить интервал времени в секундах, по истечении которого сосед будет считаться неактивным (не обязательно). Этот интервал должен быть кратным значению «hello-interval».	**esr(config-ospf- vlink)# dead-interval <TIME>** **esr(config-ipv6-ospf- vlink)# dead-interval <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 40 секунд.
24	Определяется интервал времени в секундах, по истечении которого маршрутизатор/контроллер выберет DR в сети (не обязательно).	**esr(config-ospf- vlink)# wait-interval <TIME>** **esr(config-ipv6-ospf- vlink)# wait-interval <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 40 секунд
25	Определить алгоритм аутентификации (не обязательно).	**esr(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.

Шаг	Описание	Команда	Ключи
26	Установить пароль для аутентификации с соседом (не обязательно).	**esr(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...).
27	Определить список паролей для аутентификации через алгоритм хеширования md5 (не обязательно).	**esr(config-ospf- vlink)# authentication key chain <KEYCHAIN>**	<KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов.
28	Активировать виртуальное соединение (не обязательно).	**esr(config-ospf- vlink)# enable**	
29	Перейти в режим конфигурирования интерфейса/туннеля/сетевого моста.	**esr(config)# interface <IF-TYPE><IF-NUM>**	<IF-TYPE> тип интерфейса; <IF-NUM> – F/S/P – F-фрейм (1), S – слот (0), P – порт.
		esr(config)# tunnel <TUN-TYPE><TUN-NUM>	<TUN-TYPE> тип туннеля; <TUN-NUM> номер туннеля.
		esr(config)# bridge <BR-NUM>	<BR-NUM> – номер bridge.
30	Определить принадлежность интерфейса/туннеля/сетевого моста к определенному OSPF-процессу.	**esr(config-if-gi)# ip ospf instance <ID>**	<ID> – номер процесса, принимает значения [1..65535].
		esr(config-if-gi)# ipv6 ospf instance <ID>	
31	Определить принадлежность интерфейса к определенной области OSPF-процесса.	**esr(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].
		esr(config-if-gi)# ipv6 ospf area <AREA_ID>	
32	Включить маршрутизацию по протоколу OSPF на интерфейсе.	**esr(config-if-gi)# ip ospf**	
		esr(config-if-gi)# ipv6 ospf	

Шаг	Описание	Команда	Ключи
33	Включить режим, в котором OSPF-процесс будет игнорировать значение MTU интерфейса во входящих Database Description-пакетах (не обязательно).	**esr(config-if-gi)# ip ospf mtu-ignore** **esr(config-if-gi)# ipv6 ospf mtu-ignore**	
34	Определить алгоритм аутентификации протокола OSPF (не обязательно).	**esr(config-if-gi)# ip ospf authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм аутентификации: • **cleartext** – пароль, передается открытым текстом; • **md 5** – пароль хешируется по алгоритму md5.
35	Установить пароль для аутентификации с OSPF-соседом при передаче пароля открытым текстом (не обязательно).	**esr(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...).
36	Определить список паролей для аутентификации по алгоритму хеширования md5 с соседом (не обязательно).	**esr(config-if-gi)# ip ospf authentication key-chain <KEYCHAIN>**	<KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов.
37	Определить интервал времени в секундах, по истечении которого маршрутизатор/контроллер выберет DR в сети (не обязательно).	**esr(config-if-gi)# ip ospf wait-interval <TIME>** **esr(config-if-gi)# ipv6 ospf wait-interval <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 40 секунд.
38	Установить интервал времени в секундах, по истечении которого маршрутизатор/контроллер повторно отправит пакет, на который не получил подтверждения о получении (не обязательно).	**esr(config-if-gi)# ip ospf restransmit-interval <TIME>** **esr(config-if-gi)# ipv6 ospf restransmit-interval <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 5 секунд.

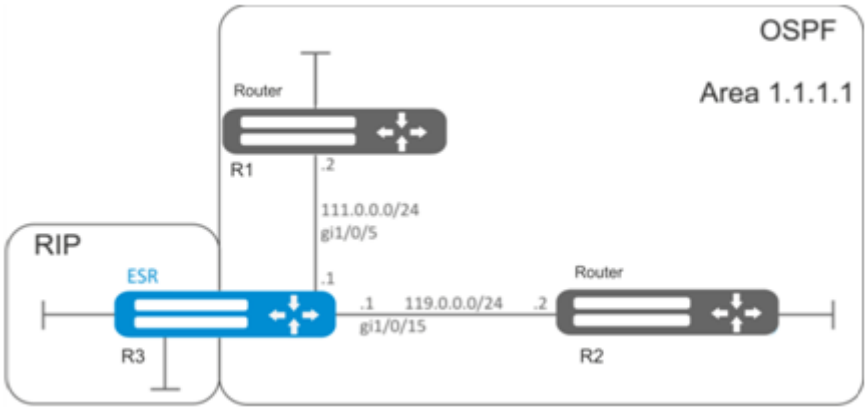
Шаг	Описание	Команда	Ключи
39	Установить интервал времени в секундах, по истечении которого маршрутизатор/контроллер отправляет следующий hello-пакет (не обязательно).	**esr(config-if-gi)# ip ospf hello-interval <TIME>** **esr(config-if-gi)# ipv6 ospf hello-interval <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 10 секунд.
40	Установить интервал времени в секундах, по истечении которого сосед будет считаться неактивным (не обязательно). Этот интервал должен быть кратным значению hello-interval.	**esr(config-if-gi)# ip dead-interval <TIME>** **esr(config-if-gi)# ipv6 dead-interval <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 40 секунд.
41	Установить интервал времени, в течение которого NBMA-интерфейс ждет, прежде чем отправить HELLO-пакет соседу, даже в случае, если сосед неактивен (не обязательно).	**esr(config-if-gi)# ip poll-interval <TIME>** **esr(config-if-gi)# ipv6 poll-interval <TIME>**	<TIME> – время в секундах, принимает значения [1 .. 65535]. Значение по умолчанию: 120 секунд.
42	Задать статический IP-адрес соседа для установления отношения в NMBA и P2MP (Point-to-MultiPoint) сетях (не обязательно).	**esr(config-if-gi)# ip ospf neighbor <IP> [eligible]**	<IP> – IP-адрес соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. **eligible** – опциональный параметр, позволяет устройству участвовать в процессе выбора DR в NBMA-сетях. Приоритет интерфейса должен быть больше нуля.
		esr(config-if-gi)# ip ospf neighbor <IP> [eligible]	<IPV6-ADDR> – IPv6-адрес соседа, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; **eligible** – опциональный параметр, позволяет устройству участвовать в процессе выбора DR в NBMA-сетях. Приоритет интерфейса должен быть больше нуля.

Шаг	Описание	Команда	Ключи
43	Определить тип сети для установления OSPF-соседства (не обязательно).	**esr(config-if-gi)# ip ospf network <TYPE>** **esr(config-if-gi)# ipv6 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.
44	Установить приоритет маршрутизатора/контроллера, который используется для выбора DR и BDR (не обязательно).	**esr(config-if-gi)# ip ospf priority <VALUE>** **esr(config-if-gi)# ipv6 ospf priority <VALUE>**	<VALUE> – приоритет интерфейса, принимает значения [1..65535]. Значение по умолчанию: 120.
45	Установить величину метрики на интерфейсе или туннеле (не обязательно).	**esr(config-if-gi)# ip ospf cost <VALUE>** **esr(config-if-gi)# ipv6 ospf cost <VALUE>**	<VALUE> – величина метрики, задаётся в размере [0..32767]. Значение по умолчанию: 10.
46	Включить протокол BFD для протокола OSPF (не обязательно).	**esr(config-if-gi)# ip ospf bfd-enable** **esr(config-if-gi)# ipv6 ospf bfd-enable**	

13.4.2 Пример настройки OSPF

Задача:

Настроить протокол OSPF на устройстве для обмена маршрутной информацией с соседними устройствами. Устройство 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 выше.

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

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

Создадим и включим требуемую область:

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

Включим анонсирование маршрутной информации из протокола RIP:

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

Включим OSPF-процесс:

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

Соседние устройства подключены к интерфейсам gi1/0/5 и gi1/0/15. Для установления соседства с другими устройствами привяжем их к OSPF-процессу и области. Далее включим на интерфейсе маршрутизацию по протоколу OSPF:

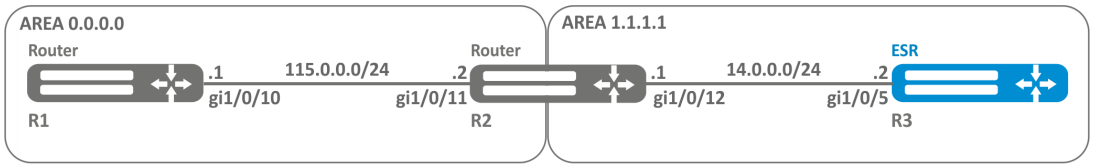
```
esr(config)# interface gigabitethernet 1/0/5
esr(config-if-gi)# ip ospf instance 10
esr(config-if-gi)# ip ospf area 1.1.1.1
esr(config-if-gi)# ip ospf
esr(config-if-gi)# exit
```

```
esr(config)# interface gigabitethernet 1/0/15
esr(config-if-gi)# ip ospf instance 10
esr(config-if-gi)# ip ospf area 1.1.1.1
esr(config-if-gi)# ip ospf
esr(config-if-gi)# exit
esr(config)# exit
```

13.4.3 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 выше.

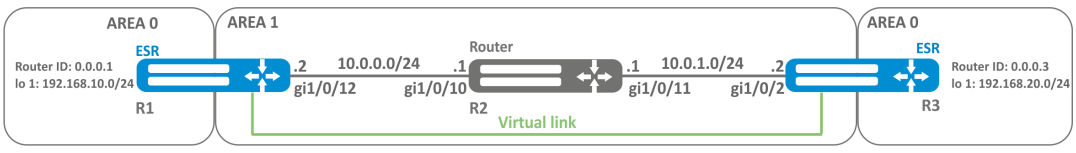
Изменим тип области на тупиковый. На R2 и R3 из области 1.1.1.1 в режиме конфигурирования области выполним команду:

```
esr(config-ospf-area)# area-type stub
```

13.4.4 Пример настройки Virtual link

Задача:

Объединить две магистральные области в одну с помощью virtual link.



Решение:

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

Предварительно нужно настроить протокол OSPF и IP-адреса на интерфейсах согласно схеме, приведенной на рисунке выше.

На устройстве R1 перейдем в режим конфигурирования области 1.1.1.1:

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

Создадим virtual link с идентификатором 0.0.0.3 и включим его:

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

На устройстве R3 перейдем в режим конфигурирования области 1.1.1.1:

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

Создадим virtual link с идентификатором 0.0.0.1 и включим его:

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

Рассмотрим таблицу маршрутизации на R1:

```
esr# show ip route
C     * 10.0.0.0/24        [0/0]   dev gi1/0/12,                  [direct 00:49:34]
O     * 10.0.1.0/24        [150/20] via 10.0.0.1 on gi1/0/12,     [ospf1 00:49:53]  (0.0.0.3)
O     * 192.168.20.0/24    [150/30] via 10.0.0.1 on gi1/0/12,     [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 R3:

```
esr# show ip route
O     * 10.0.0.0/24        [150/20] via 10.0.1.1 on gi1/0/12,     [ospf1 14:38:35]  (0.0.0.2)
C     * 10.0.1.0/24        [0/0]   dev gi1/0/12,                  [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 gi1/0/12,     [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:

```
esr# show ip ospf neighbors 10
```

Таблицу маршрутов протокола OSPF можно просмотреть командой:

```
esr# show ip ospf 10
```

В firewall необходимо разрешить протокол OSPF (89).

13.5 Настройка BGP

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

13.5.1 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).	**esr(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).	**esr(config)# ip protocols bgp max-routes <VALUE>**	<VALUE> – количество маршрутов протокола BGP в маршрутной таблице, принимает значения в диапазоне: • для ESR-1000/1200/1500/1511/1700/3100/3200 – [1..5000000]; • для ESR-20/21/30/100/200 – [1..2500000]; • для ESR-10/12V(F)/14VF/15 – [1..1000000]. Значение по умолчанию для глобальной таблицы маршрутизации: • для ESR-1000/1200/1500/1511/1700/3100/3200 – [5000000]; • для ESR-20/21/30/100/200 – [2500000]; • для ESR-10/12V/12VF/14VF/15 – [1000000]. Значение по умолчанию для VRF: 0.
		esr(config)# ipv6 protocols bgp max-routes <VALUE>	
		esr(config-vrf)# ip protocols bgp max-routes <VALUE>	
		esr(config-vrf)# ipv6 protocols bgp max-routes <VALUE>	
3	Включить вывод информации о состоянии отношений с соседями для протокола маршрутизации BGP (не обязательно).	**esr(config)# router bgp log-neighbor-changes**	
		esr(config)# ipv6 router bgp log-neighbor-changes	
4	Включить ECMP и определяется максимальное количество равноценных маршрутов до цели.	**esr(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).		

Шаг	Описание	Команда	Ключи
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.	**esr(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.	**esr(config-route-map-rule)#match ip address { <ADDR/LEN> | object-group <OBJ-GRP-NETNAME> } [{ eq <LEN> | le <LEN> | ge <LEN 1> [le <LEN 2>] }]**	<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, задаётся строкой до 31 символа*; <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
		esr(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>] }]	⚠ При использовании фильтрации по object-group, их необходимо создать заранее.
5.1.4	Разрешить (permit) или запретить (deny) действие для указанных подсетей в правиле.	**esr(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.	**esr(config)# ip prefix-list <NAME>** **esr(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.	**esr(config-pl)# permit { <ADDR/LEN> | object-group <OBJ-GRP-NETNAME>} [{ eq <LEN> | le <LEN> | ge <LEN 1> [le <LEN 2>] }]**	<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, 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]; <OBJ-GRP-NETNAME> – имя профиля IP -адресов, задаётся строкой до 31 символа*; <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
		esr(config-pl)# deny {<ADDR/LEN> | object-group <OBJ-GRP-NETNAME>} [{ eq <LEN> | le <LEN> | ge <LEN 1> [le <LEN 2>] }]	⚠ При использовании фильтрации по object-group, их необходимо создать заранее.
		esr(config-ipv6-pl)# permit { <IPV6-ADDR/LEN> | object-group <OBJ-GRP-NETNAME>} [{ eq <LEN> | le <LEN> | ge <LEN 1> [le <LEN 2>] }]	
		esr(config-ipv6-pl)# deny {<IPV6-ADDR/LEN> | object-group <OBJ-GRP-NETNAME> } [{ eq <LEN> | le <LEN> | ge <LEN 1> [le <LEN 2>] }]	
6	Добавить BGP-процесс в систему и осуществить переход в режим настройки параметров BGP-процесса.	**esr(config)# router bgp <AS>**	<AS> – номер автономной системы процесса, принимает значения [1..4294967295].
7	Установить идентификатор устройства.	**esr(config-bgp)# router-id { <ID> | <IF> | <TUN> }**	<ID> – идентификатор устройства, 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 устройсва (при необходимости).	**esr(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).	**esr(config-bgp)# default-information-originate**	

Шаг	Описание	Команда	Ключи
10	Установить временной интервал, по истечении которого идет проверка соединения со встречной стороной (не обязательно).	**esr(config-bgp-af)# timers keeaplive <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 60 секунд.
11	Установить временной интервал, по истечении которого встречная сторона считается недоступной (не обязательно).	**esr(config-bgp-af)# timers holdtime <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 180 секунд.
12	Установить время минимальной и максимальной задержки, в течение которого запрещено устанавливать соединение, в целях защиты от частых разрывов соединения (не обязательно).	**esr(config-bgp-af)# 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).	**esr(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").	**esr(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.	**esr(config-bgp)# enable**	
16	Определить тип конфигурируемой маршрутной информации и перейти в данный режим настройки.	**esr(config-bgp)# address-family { ipv4 | ipv6 } unicast**	**ipv 4** – семейство IPv4; **ipv 6** – семейство IPv6;

Шаг	Описание	Команда	Ключи
17	Включить анонсирование маршрутов процессом BGP полученных альтернативным образом (при необходимости).	**esr(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.
		esr(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.
		esr(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.

Шаг	Описание	Команда	Ключи
		esr(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.
		esr(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.	**esr(config-bgp-af)# network <ADDR/LEN>**	<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].
19	Осуществить выход из режима глобального конфигурирования анонсов маршрутной информации процесса BGP	**esr(config-bgp-af)# exit**	
20	Добавить BGP-соседа и осуществить переход в режим настройки параметров BGP-соседа.	**esr(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).	**esr(config-bgp-neighbor)# description <DESCRIPTION>**	<DESCRIPTION> – описание соседа, задаётся строкой до 255 символов.
22	Установить временной интервал, по истечении которого идет проверка соединения со встречной стороной (не обязательно).	**esr(config-bgp-neighbor)# timers keepalive <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 60 секунд.

Шаг	Описание	Команда	Ключи
23	Установить временной интервал, по истечении которого встречная сторона считается недоступной (не обязательно).	**esr(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).	**esr(config-bgp-af)# 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.	**esr(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).	**esr(config-bgp-neighbor)# ebgp-multihop <NUM>**	<NUM> – максимальное количество хопов при установке EBGP (используется для TTL).
27	Указать, что BGP-сосед является Route-Reflector клиентом (не обязательно).	**esr(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).	**esr(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::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).	**esr(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).	**esr(config-bgp-neighbor)# bfd-enable**	
31	Определить алгоритм аутентификации с соседом (не обязательно).	**esr(config-bgp-neighbor)# authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм шифрования: md5 – пароль шифруется по алгоритму md5.

Шаг	Описание	Команда	Ключи
32	Установить пароль для аутентификации с соседом (не обязательно).	**esr(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...).
33	Сделать соседство активным.	**esr(config-bgp-neighbor)# enable**	
34	Определить тип конфигурируемой маршрутной информации соседа и перейти в данный режим настройки.	**esr(config-bgp-neighbor)# address-family { ipv4 | ipv6 | vpnv4 } unicast**	**ipv 4** – семейство IPv4; **ipv 6** – семейство IPv6; **vpnv4** – семейство VPNv4;
35	При выборе режима фильтрации на основе префикс-листов добавить фильтрацию подсетей во входящих или исходящих обновлениях (обязательно при конфигурировании eBGP для анонсирования подсетей).	**esr(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.
36	Задать режим, в котором BGP-соседу в обновлении на ряду с другими маршрутами всегда отправляется маршрут по умолчанию. (не обязательно, отсутствует для vpnv4).	**esr(config-bgp-neighbor-af)# default-originate**	
37	Задать режим, в котором все обновления отправляются BGP-соседу с указанием в качестве next-hop IP-адреса исходящего интерфейса локального устройства (не обязательно, отсутствует для vpnv4).	**esr(config-bgp-neighbor-af)# next-hop-self**	
38	Определить приоритетность маршрутов, получаемых от соседа (не обязательно).	**esr(config-bgp-neighbor-af)# preference <VALUE>**	<VALUE> – приоритетность маршрутов соседа, принимает значения в диапазоне [1..255]. Значение по умолчанию: 170.

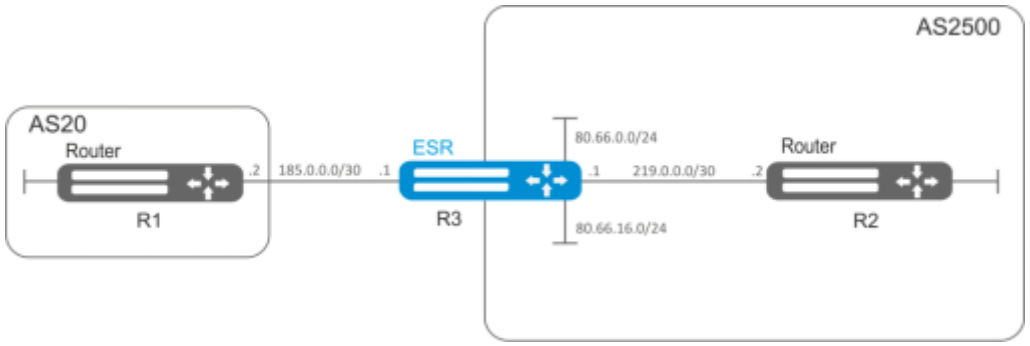
Шаг	Описание	Команда	Ключи
39	Задать режим, в котором перед отправлением обновления из BGP-атрибута AS Path маршрутов удаляются приватные номера автономных систем (в соответствии с RFC 6996) (не обязательно, отсутствует для vpnv4).	**esr(config-bgp-neighbor-af)# remove-private-as [{ all | nearest | replace }]**	**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.
40	Включить обмен маршрутной информацией.	**esr(config-bgp-neighbor-af)# enable**	

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.

13.5.2 Пример настройки

Задача:

Настроить BGP-протокол на устройстве 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:

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

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

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

И укажем принадлежность интерфейсов к зоне безопасности:

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

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

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

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

```
esr(config)# router bgp 2500
```

Сконфигурируем анонсирование подсетей, подключенных напрямую:

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

Создадим соседство с роутером R2 по iBGP:

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

И включим обмен IPv4-маршрутами:

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

Создадим соседство с роутером R1 по eBGP:

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

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

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

Включим работу протокола:

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

Информацию о BGP-пирах можно посмотреть командой:

```
esr# show bgp neighbors
```

Таблицу маршрутов протокола BGP можно просмотреть с помощью команды:

```
esr# show bgp ipv4 unicast
```

13.5.3 Политика выбора лучшего маршрута в протоколе BGP

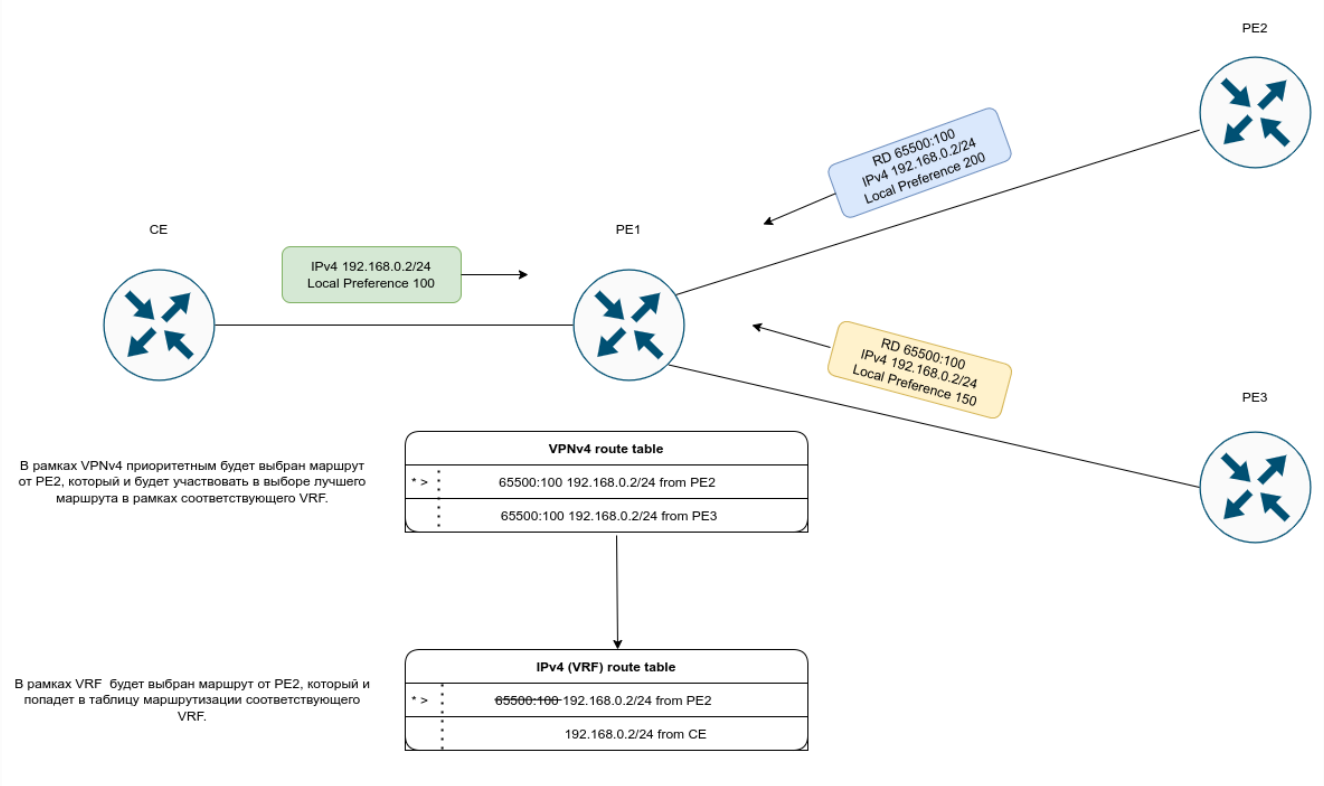
В процессе работы BGP, обычно, вычисляет один лучший маршрут до каждой полученной подсети. Если нет более приоритетного маршрута, полученного при помощи другого протокола маршрутизации до этой подсети, то маршрут устанавливается в таблицу маршрутизации.

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.

Для VPNv4 маршрутов выбор лучшего маршрута происходит следующим образом: Сначала выбор лучшего маршрута происходит в рамках своего RD. Далее, в рамках VRF, куда он попадет в соответствии своего 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 (Подробнее);
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 "хопов" становится лучшим;
5. Сравнивается значение атрибута Origin – IGP является самым приоритетным. EGP приоритетнее, чем Incomplete;
6. 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;
   7.1 Если включен ECMP, то дальнейших сравнений не производится и маршрут (multipath) попадет в таблицу маршрутизации;
8. Сравнивается параметр Router-Id – маршрут, полученный от BGP-соседа с наименьшим Router-Id, является приоритетным;
9. Сравнивается количество адресов в Cluster list – маршрут, имеющий наименьшее количество адресов становится лучшим;
10. Сравниваются адрес 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":

```
ESR# show bgp ipv4 unicast 192.0.2.0/24
192.0.2.0/24 via 100.64.28.1 on gi1/0/1.2800   [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)
(3356:2065)
                             (12389:6) (65000:64990)
    Weight:                  0
    Valid
192.0.2.0/24 via 101.7.0.1 on gi1/0/1.2800   [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)
(3356:2065)
                             (12389:6) (65000:64990)
    Weight:                  0
    Valid,Best
```

13.6 Настройка BFD

BFD (Bidirectional Forwarding Detection) — это протокол, работающий поверх других протоколов, позволяющий сократить время обнаружения проблемы до 50 мс. BFD является двусторонним протоколом, т.е. требует настройки обоих маршрутизаторов или контроллеров (оба устройства 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

Для изменения поведения (режима) необходимо в ручную переопределить параметры сессии, указав необходимый режим. Рассмотрим на примере:
Допустим, мы установили eBGP-соседство и включили для него BFD:

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

ESR# 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:

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

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

```
esr-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
```

13.6.1 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.

```
ESR(config)# ip bfd min-tx-interval 1000
ESR(config)# ip bfd min-rx-interval 1000
ESR(config)# do commmit

ESR# 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 наибольшее значение из локального Tx Interval и удаленного RX Interval. Detection Interval вычисляется по следующей формуле: Detection Interval = remoteMultiplier * MAX(RxLocal || 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:

```
esr-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            <----
```

13.6.2 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Активировать BFD для протокола OSPF на интерфейсе.	**esr(config-if-gi)# ip ospf bfd-enable**	
2	Активировать BFD для протокола BGP neighbor на интерфейсе.	**esr(config-bgp-neighbor)# bfd-enable**	
3	Задать интервал, по истечении которого происходит отправка BFD-сообщения соседу. Глобально (не обязательно).	**esr(config)# ip bfd idle-tx-interval <TIMEOUT>**	<TIMEOUT> – интервал, по истечении которого происходит отправка BFD-пакета, принимает значение в миллисекундах в диапазоне [200..65535] для ESR-1000/1200/1500/1511 /1700/3100/32000 и [300..65535] для ESR-10/12V(F)/14VF/ 15/20/21/30/100/200 По умолчанию 1 секунда.

Шаг	Описание	Команда	Ключи
4	Включить логирование изменений состояния BFD-протокола (не обязательно).	**esr(config)# ip bfd log-adjacency-changes**	
5	Задать минимальный интервал, по истечении которого сосед должен сгенерировать BFD-сообщение. Глобально (не обязательно).	**esr(config)# ip bfd min-rx-interval <TIMEOUT>**	<TIMEOUT> – интервал, по истечении которого должна происходить отправка BFD-сообщения соседом, принимает значение в миллисекундах в диапазоне [200..65535] для ESR-1000/1200/1500/1511 /1700/3100/3200 и [300..65535] для ESR-10/12V(F)/14VF/ 15/20/21/30/100/200 По умолчанию: • 300 миллисекунд на ESR-10/12V(F)/14VF/ 15/20/21/30/100/200, • 200 миллисекунд на ESR-1000/1200/1500 /1511/1700/3100/3200.
6	Задать минимальный интервал, по истечении которого происходит отправка BFD-сообщения соседу. Глобально (не обязательно).	**esr(config)# ip bfd min-tx-interval <TIMEOUT>**	<TIMEOUT> – интервал, по истечении которого должна происходить отправка BFD-сообщения соседом, принимает значение в миллисекундах в диапазоне [200..65535] для ESR-1000/1200/1500/1511 /1700/3100/3200 и [300..65535] для ESR-10/12V(F)/14VF/ 15/20/21/30/100/200 По умолчанию: • 300 миллисекунд на ESR-10/12V(F)/14VF/ 15/20/21/30/100/200, • 200 миллисекунд на ESR-1000/1200/1500 /1511/1700/3100/3200.

Шаг	Описание	Команда	Ключи
7	Задать число пропущенных пакетов, после достижения которого BFD-сосед считается недоступным. Глобально.	**esr(config)# ip bfd multiplier <COUNT>**	<COUNT> – число пропущенных пакетов, после достижения которого сосед считается недоступным, принимает значение в диапазоне [1..100]. По умолчанию: 5.
8	Запустить работу механизма BFD с определенным IP-адресом.	**esr(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.
9	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).	**esr(config)# ip bfd passive**	
10	Задать интервал, по истечении которого происходит отправка BFD-сообщения соседу. На интерфейсе (не обязательно).	**esr(config-if-gi)# ip bfd idle-tx-interval <TIMEOUT>**	<TIMEOUT> – интервал, по истечении которого происходит отправка BFD-пакета, принимает значение в миллисекундах в диапазоне [200..65535] для ESR-1000/1200/1500/1511 /1700/3100/3200 и [300..65535] для ESR-10/12V(F)/14VF/ 15/20/21/30/100/200. По умолчанию: 1 секунда.

Шаг	Описание	Команда	Ключи
11	Задать минимальный интервал, по истечении которого сосед должен сгенерировать BFD-сообщение. На интерфейсе (не обязательно).	**esr(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 [200..65535] для ESR-1000/1200/1500/1511 /1700/3100/3200 и [300..65535] для ESR-10/12V(F)/14VF/ 15/20/21/30/100/200 По умолчанию: • 300 миллисекунд на ESR-10/12V(F)/14VF/ 15/20/21/30/100/200, • 200 миллисекунд на ESR-1000/1200/1500 /1511/1700/3100/3200.
12	Задать минимальный интервал, по истечении которого происходит отправка BFD-сообщения соседу. На интерфейсе (не обязательно).	**esr(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 [200..65535] для ESR-1000/1200/1500/1511 /1700/3100/3200 и [300..65535] для ESR-10/12V(F)/14VF/ 15/20/21/30/100/200 По умолчанию: • 300 миллисекунд на ESR-10/12V(F)/14VF/ 15/20/21/30/100/200, • 200 миллисекунд на ESR-1000/1200/1500 /1511/1700/3100/3200.
13	Задать число пропущенных пакетов, после достижения которого BFD-сосед считается недоступным. На интерфейсе (не обязательно).	**esr(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.

Шаг	Описание	Команда	Ключи
14	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).	**esr(config-if-gi)# ip bfd passive**	
15	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.		

13.6.3 Пример настройки BFD с BGP

Задача:

Необходимо настроить eBGP между ESR R1 и R2 и включить BFD.

Решение:

1. Конфигурирование R1
   Предварительно необходимо настроить интерфейс Gi1/0/1:

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

   Настроим eBGP с BFD:

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

2. Конфигурирование R2
   Предварительно необходимо настроить интерфейс Gi1/0/1:

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

Настроим eBGP с BFD:

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

13.7 Настройка политики маршрутизации PBR

13.7.1 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.	**esr(config)# route-map <NAME>**	<NAME> – имя маршрутной карты, задается строкой до 31 символа.
2	Создать правило маршрутной карты.	**esr(config-route-map)# rule <ORDER>**	<ORDER> – номер правила, принимает значения [1 .. 10000].
3	Указать действие, которое должно быть применено для маршрутной информации.	**esr(config-route-map-rule)# action <ACT>**	<ACT> – назначаемое действие: • **permit** – прием или анонсирование маршрутной информации разрешено; • **deny** – запрещено.
4	Задать значение атрибута BGPAS-Path в маршруте, для которого должно срабатывать правило (не обязательно).	**esr(config-route-map-rule)# match as-path [begin | end | contain] <AS-PATH>**	<AS-PATH> – список номеров автономных систем, задается в виде AS,AS,AS, принимает значения [1..4294967295]. Опциональные параметры: • **begin** – значение атрибута начинается с указанных номеров AS; • **end** – значение атрибута заканчивается указанными номерами AS; • **contain** – значение атрибута содержит указанный список номеров AS.

Шаг	Описание	Команда	Ключи
5	Задать значение атрибута BGPCommunity, для которого должно срабатывать правило (не обязательно).	**esr(config-route-map-rule)# match community <COMMUNITY-LIST>**	<COMMUNITY-LIST> – список community, задается в виде AS:N,AS:N, принимает значения [1..4294967295]. Можно указать до 64 community.
6	Задать значение атрибута BGPExtendedCommunity, для которого должно срабатывать правило (не обязательно).	**esr(config-route-map-rule)# match 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].
7	Задать профиль IP-адресов, содержащий значения подсетей назначения в маршруте (не обязательно).	**esr(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.
		esr(config-route-map-rule)# match ipv6 address object-group <OBJ-GROUP-NETWORK-NAME>	
8	Задать профиль IP-адресов, содержащий значения атрибута BGPNext-Hop в маршруте для которого должно срабатывать правило (не обязательно).	**esr(config-route-map-rule)# match ip 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.
		esr(config-route-map-rule)# match ipv6 next-hop object-group <OBJ-GROUP-NETWORK-NAME>	
9	Задать профиль, содержащий IP-адреса устройства, анонсировавшего маршрут, для которого должно срабатывать правило (не обязательно).	**esr(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.
		esr(config-route-map-rule)# match ipv6 route-source object-group <OBJ-GROUP-NETWORK-NAME>	

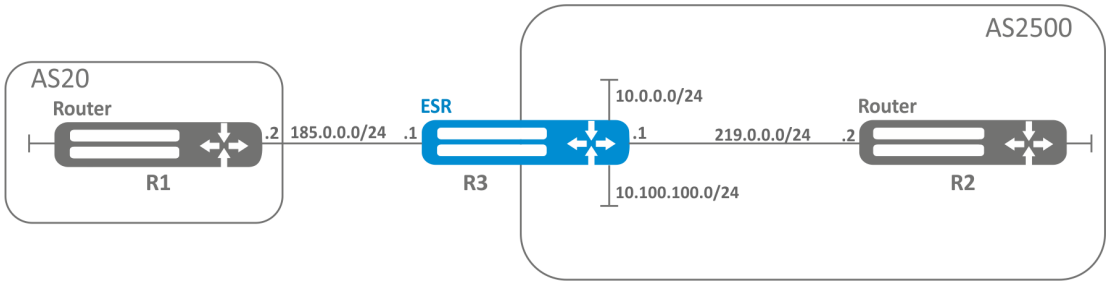
Шаг	Описание	Команда	Ключи
10	Задать ACL-группу, для которой должно срабатывать правило (не обязательно).	**esr(config-route-map-rule)# match access-group <NAME>**	<NAME> – имя списка контроля доступа, задается строкой до 31 символа.
11	Задать значение атрибута BGP MED в маршруте для которого должно срабатывать правило (не обязательно).	**esr(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.	**esr(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.	**esr(config-route-map-rule)# match metric rip <METRIC>**	<METRIC> – значение атрибута RIP Metric, принимает значения [0..16].
14	Задать значение атрибута OSPF Tag в маршруте, для которого должно срабатывать правило.	**esr(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.	**esr(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).	**esr(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]. <TCACK-ID> – идентификатор vrrp-tracking, при котором будет исполняться указанное действие. Изменяется в диапазоне [1..60].

Шаг	Описание	Команда	Ключи
17	Задать значение атрибута BGP Community, которое будет установлено в маршруте (не обязательно).	**esr(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).	**esr(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].
19	Задать атрибут BGP Next-Hop, который будет установлен в маршруте при анонсировании (не обязательно).	**esr(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].
		esr(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].

Шаг	Описание	Команда	Ключи
20	Задать значение Next-Hop, которое будет установлено в маршруте, полученном по BGP (не обязательно).	**esr(config-route-map-rule)# action set ip next-hop {NEXTHOP> | blackhole | unreachable | prohibit}**	<NEXTHOP> – IP-адрес шлюза задаётся 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 ICMPDestinationunreachable (Communication administratively prohibited code 13).
		esr(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).	**esr(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).	**esr(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).	**esr(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.	**esr(config-bgp-neighbor)# route-map <NAME><DIRECTION>** **esr(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.

13.7.2 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 ESR или контроллере WLC;
- Установить соседство с AS20.

Решение:

Создаем политику:

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

Создаем правило 1:

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

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

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

В BGP процессе AS2500 заходим в настройки параметров соседа:

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

Привязываем политику к принимаемой маршрутной информации:

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

13.7.3 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 ESR

Решение:

Создаем политику:

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

Создаем правило:

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

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

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

В BGP процессе AS2500 заходим в настройки параметров соседа:

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

Привязываем политику к анонсируемой маршрутной информации:

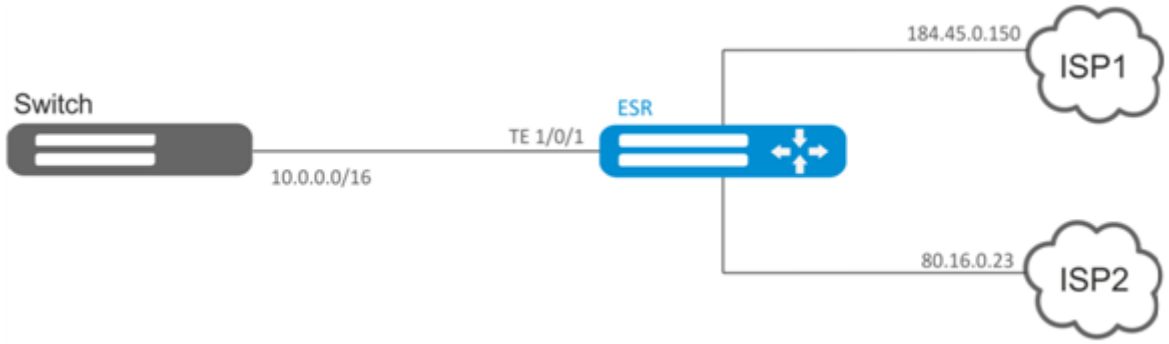
```
esr(config-bgp-neighbor-af)# route-map to-as20 out
esr(config-bgp-neighbor-af)# exit
esr(config-bgp-neighbor)# exit
esr(config-bgp)# exit
```

13.7.4 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.	**esr(config)# route-map <NAME>**	<NAME> – имя маршрутной карты, задаётся строкой до 31 символа.
2	Создать правило маршрутной карты.	**esr(c onfig-route-map)# rule <ORDER>**	<ORDER> – номер правила, принимает значения [1 .. 10000].
3	Указать действие, которое должно быть применено для маршрутной информации.	**esr(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).	**esr(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).	**esr(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].

Шаг	Описание	Команда	Ключи
6	Назначить политику маршрутизации на основе списков доступа (ACL).	**esr(config-if-gi)# ip policy route-map <NAME>**	<NAME> – имя сконфигурированной политики маршрутизации, строка до 31 символа.
7	Разрешить фильтрацию и модификацию локального трафика на основе политики маршрутизации.	**esr(config)# ip local policy [vrf <VRF>] route-map <NAME>**	<NAME> – имя сконфигурированной политики маршрутизации, строка до 31 символа.

13.7.5 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:

```
esr# configure
esr(config)# ip access-list extended sub20
esr(config-acl)# rule 1
esr(config-acl-rule)# match source-address 10.0.20.0 255.255.255.0
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# action permit
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit
esr(config)# ip access-list extended sub30
esr(config-acl)# rule 1
esr(config-acl-rule)# match source-address 10.0.30.0 255.255.255.0
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# action permit
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit
```

Создаем политику:

```
esr(config)# route-map PBR
```

Создаем правило 1:

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

Указываем список доступа (ACL) в качестве фильтра:

```
esr(config-route-map-rule)# match ip access-group sub20
```

Указываем next-hop для sub20:

```
esr(config-route-map-rule)# action set ip next-hop verify-availability 184.45.0.150 10
esr(config-route-map-rule)# action set ip next-hop verify-availability 80.16.0.23 30
esr(config-route-map-rule)# exit
esr(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:

```
esr(config-route-map)# rule 2
```

Указываем список доступа (ACL) в качестве фильтра:

```
esr(config-route-map-rule)# match ip access-group sub30
```

Указываем nexthop для sub30 и выходим:

```
esr(config-route-map-rule)# action set ip next-hop verify-availability 80.16.0.23 10
esr(config-route-map-rule)# action set ip next-hop verify-availability 184.45.0.150 30
esr(config-route-map-rule)# exit
esr(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:

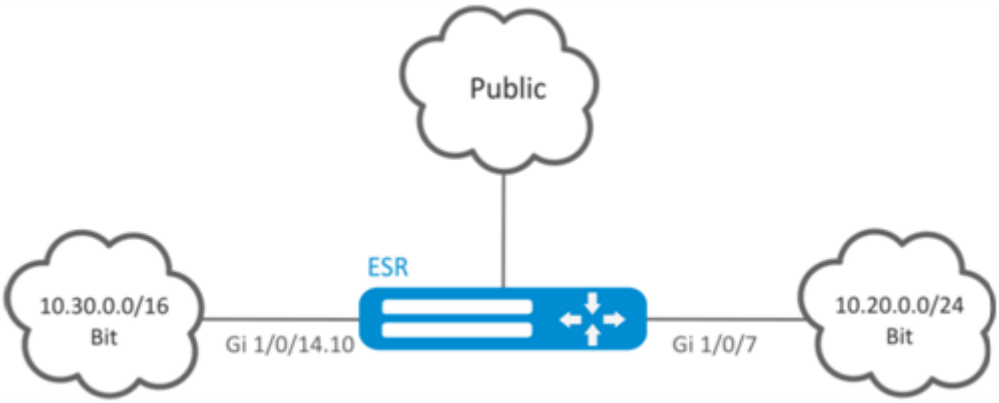
```
esr(config)# interface tengigabitethernet 1/0/1
```

Привязываем политику на соответствующий интерфейс:

```
esr(config-if-te)# ip policy route-map PBR
```

13.8 Настройка VRF

VRF (Virtual Routing and Forwarding) – технология, которая позволяет изолировать маршрутную информацию, принадлежащую различным классам (например, маршруты одного клиента).



13.8.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать экземпляр VRF и перейти в режим настройки параметров экземпляра VRF.	**esr(config)# ip vrf <VRF>**	<VRF> – имя экземпляра VRF, задается строкой до 31 символа.
2	Назначить описание конфигурируемого экземпляра VRF.	**esr(config-vrf)# description <DESCRIPTION>**	<DESCRIPTION> – описание экземпляра VRF, задаётся строкой до 255 символов.

Шаг	Описание	Команда	Ключи
3	Настроить емкость таблиц маршрутизации в конфигурируемом VRF для IPv4/IPv6 протоколов маршрутизации (не обязательно).	**esr(config-vrf)# ip protocols <PROTOCOL> max-routes <VALUE>** **esr(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 ESR-1000/1200/1500/1511/1700/3100/3200 – [1..500000], ESR-20/21/30/100/200 – [1..300000], ESR-10/12V(F)/14VF/15 – [1..30000] • BGP ESR-1000/1200/1500/1511/1700/3100/3200 – [1..5000000], ESR-20/21/30/100/200 – [1..2500000], ESR-10/12V(F)/14VF – [1..1000000]. 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.		
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).	**esr(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.

13.8.2 Пример настройки

Задача:

К маршрутизатору серии ESR подключены 2 сети, которые необходимо изолировать от остальных сетей.

Решение:

Создадим VRF:

```
esr(config)# ip vrf bit
esr(config-vrf)# exit
```

Создадим зону безопасности:

```
esr(config)# security zone vrf-sec
esr(config-zone)# ip vrf forwarding bit
esr(config-zone)# exit
```

Создадим правило для пары зон и разрешим любой TCP/UDP-трафик:

```
esr(config)# security zone-pair vrf-sec vrf-sec
esr(config-zone-pair)# rule 1
esr(config-zone-rule)# match source-address any
esr(config-zone-rule)# match destination-address any
esr(config-zone-rule)# match protocol udp
esr(config-zone-rule)# match source-port any
esr(config-zone-rule)# match destination-port any
esr(config-zone-rule)# action permit
esr(config-zone-rule)# enable
esr(config-zone-rule)# exit
esr(config-zone-pair)# rule 2
esr(config-zone-rule)# match source-address any
esr(config-zone-rule)# match destination-address any
esr(config-zone-rule)# match protocol tcp
esr(config-zone-rule)# match source-port any
esr(config-zone-rule)# match destination-port any
esr(config-zone-rule)# action permit
esr(config-zone-rule)# enable
esr(config-zone-rule)# exit
```

Создадим привязку интерфейсов, назначим IP-адреса, укажем принадлежность к зоне:

```
esr(config)# interface gigabitethernet 1/0/7
esr(config-if-gi)# ip vrf forwarding bit
esr(config-if-gi)# ip address 10.20.0.1/24
esr(config-if-gi)# security-zone vrf-sec
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/14.10
esr(config-subif)# ip vrf forwarding bit
esr(config-subif)# ip address 10.30.0.1/16
esr(config-subif)# security-zone vrf-sec
esr(config-subif)# exit
esr(config)# exit
```

Информацию об интерфейсах, привязанных к VRF, можно посмотреть командой:

```
esr# show ip vrf
```

Таблицу маршрутов VRF можно просмотреть с помощью команды:

```
esr# show ip route vrf bit
```

13.9 Настройка MultiWAN

Технология MultiWAN позволяет организовать отказоустойчивое соединение с резервированием линков от нескольких провайдеров, а также решает проблему балансировки трафика между резервными линками.

13.9.1 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).	**esr(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.	**esr(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.	**esr(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).	**esr(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).	**esr(config-wan-rule)# failover**	
7	Включить wan-правило.	**esr(config-wan-rule)# enable**	
8	Создать список IP-адресов для проверки целостности соединения и осуществить переход в режим настройки параметров списка.	**esr(config)# wan load-balance target-list <NAME>**	<NAME> – название списка, задается строкой до 31 символа.
9	Задать цель проверки и перейти в режим настройки параметров цели.	**esr(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.
10	Описать target (не обязательно).	**esr(config-wan-target)# description <DESCRIPTION>**	<DESCRIPTION> – описание target, задаётся строкой до 255 символов.
11	Указать время ожидания ответа на запрос по протоколу ICMP (не обязательно).	**esr(config-wan-target)# resp-time <TIME>**	<TIME> – время ожидания, определяется в секундах [1..30].
12	Указать IP-адрес проверки.	**esr(config-wan-target)# ip address <ADDR>**	<ADDR> – IP-адрес назначения, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

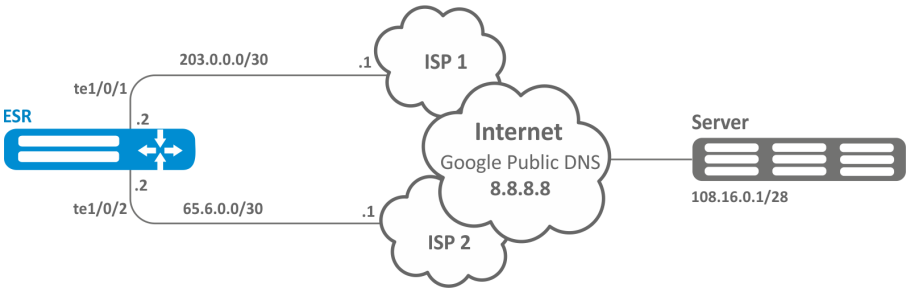
Шаг	Описание	Команда	Ключи
		esr(config-wan-target)# ipv6 address <IPV6-ADDR>	<IPV6-ADDR> – IPv6-адрес назначения, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
13	Включить проверку цели.	**esr(config-wan-target)# enable**	
Команды для пунктов 14–17 необходимо применить на интерфейсах/туннелях в MultiWAN.			
14	Включить WAN режим на интерфейсе для IPv4/IPv6-стека.	**esr(config-if-gi)# wan load-balance enable**	
		esr(config-if-gi)# ipv6 wan load-balance enable	
15	Задать количество неудачных попыток проверки соединения, после которых, при отсутствии ответа от встречной стороны, соединение будет считается неактивным (не обязательно).	**esr(config-if-gi)# wan load-balance failure-count <VALUE>**	<VALUE> – количество попыток, определяется в диапазоне [1..10]. Значение по умолчанию 1.
		esr(config-if-gi)# ipv6 wan load-balance failure-count <VALUE>	
16	Задать количество успешных попыток проверки соединения, после которых, в случае успеха, соединение считается вновь активным (не обязательно).	**esr(config-if-gi)# wan load-balance success-count <VALUE>**	<VALUE> – количество попыток, определяется в диапазоне [1..10]. Значение по умолчанию 1.
		esr(config-if-gi)# ipv6 wan load-balance success-count <VALUE>	
17	Задать IP-адрес соседа, который будет указан в качестве одного из шлюзов в статическом маршруте, создаваемом службой MultiWAN.	**esr(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.

Шаг	Описание	Команда	Ключи
		esr(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].
18	Данной командой будут проверяться IP-адреса из списка проверки целостности. В случае недоступности всех (по умолчанию)/хотя бы одной (с использованием ключа chack-all) из проверяемых узлов, шлюз будет считаться недоступным.	**esr(config-if-gi)# wan load-balance target-list { check-all | <NAME> }**	<NAME> – проверку производить на основании конкретного target листа (заданного в п.7). check-all – проверку производить на основании всех target листа.
		esr(config-if-gi)# ipv6 wan load-balance target-list { check-all | <NAME> }	
19	Прописать статические маршруты через WAN.	**esr(config)# ip route <SUBNET> wan load-balance rule <ID> [<METRIC>]**	<ID> – идентификатор создаваемого правила из п.2. [METRIC] – метрика маршрута, принимает значения [0..255].
		esr(config)# ipv6 route <SUBNET> wan load-balance rule <ID [<METRIC>]	

13.9.2 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 te1/0/2;
- указать IP-адреса для интерфейсов te1/0/1 и te1/0/2.

Основной этап конфигурирования:

Настроим маршрутизацию:

```
esr(config)# ip route 108.16.0.0/28 wan load-balance rule 1
```

Создадим правило WAN:

```
esr(config)# wan load-balance rule 1
```

Укажем участвующие интерфейсы:

```
esr(config-wan-rule)# outbound interface tengigabitethernet 1/0/2
esr(config-wan-rule)# outbound interface tengigabitethernet 1/0/1
```

Включим созданное правило балансировки и выйдем из режима конфигурирования правила:

```
esr(config-wan-rule)# enable
esr(config-wan-rule)# exit
```

Создадим список для проверки целостности соединения:

```
esr(config)# wan load-balance target-list google
```

Создадим цель проверки целостности:

```
esr(config-target-list)# target 1
```

Зададим адрес для проверки, включим проверку указанного адреса и выйдем:

```
esr(config-wan-target)# ip address 8.8.8.8
esr(config-wan-target)# enable
esr(config-wan-target)# exit
```

Настроим интерфейсы. В режиме конфигурирования интерфейса te1/0/1 указываем nexthop:

```
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if)# wan load-balance nexthop 203.0.0.1
```

В режиме конфигурирования интерфейса te1/0/1 указываем список целей для проверки соединения:

```
esr(config-if)# wan load-balance target-list google
```

В режиме конфигурирования интерфейса te1/0/1 включаем WAN-режим и выходим:

```
esr(config-if)# wan load-balance enable
esr(config-if)# exit
```

В режиме конфигурирования интерфейса te1/0/2 указываем nexthop:

```
esr(config)# interface tengigabitethernet 1/0/2
esr(config-if)# wan load-balance nexthop 65.6.0.1
```

В режиме конфигурирования интерфейса te1/0/2 указываем список целей для проверки соединения:

```
esr(config-if)# wan load-balance target-list google
```

В режиме конфигурирования интерфейса te1/0/2 включаем WAN-режим и выходим:

```
esr(config-if)# wan load-balance enable
esr(config-if)# exit
```

Для переключения в режим резервирования настроим следующее:

Заходим в режим настройки правила WAN:

```
esr(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:

```
esr(config-wan-rule)# failover
```

13.10 Настройка IS-IS

IS-IS — протокол динамической маршрутизации, стандартизированный ISO, основанный на состояниях линков (link-state). Он обеспечивает быструю сходимость и отличную масштабируемость, экономно использует пропускную способность сетей, использует Алгоритм Дейкстры для просчёта наилучших маршрутов. Отличительной особенностью протокола IS-IS является работа поверх канального уровня модели OSI, поэтому он не привязан к конкретному протоколу сетевого уровня.

13.10.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать IS-IS процесс и перейти в режим настройки параметров этого процесса.	**esr(config)# router isis <ID> [vrf <VRF>]**	<ID> – номер процесса, принимает значения [1..65535]; <VRF> – имя экземпляра VRF, задается строкой до 31 символа.
2	Установить NET-адрес.	**esr(config-isis)# net {<NET>}**	<NET> – NET адрес, формат: ff[.ffff.ffff.ffff.ffff.ffff.ffff].ffff.ffff.ffff.00.
3	Включить IS-IS процесс.	**esr(config-isis)# enable**	
4	Установить алгоритм аутентификации для L2-уровня (не обязательно).	**esr(config-isis)# authentication domain algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм аутентификации: • cleartext – пароль, передается открытым текстом; • md5 – пароль хешируется по алгоритму md5.
5	Установить пароль аутентификации для L2-уровня (не обязательно).	**esr(config-isis)# authentication domain key ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<CLEAR-TEXT> – пароль, задаётся строкой 8 символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером 8 байт (16 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).
6	Установить список ключей для аутентификации (не обязательно).	**esr(config-isis)# authentication domain key chain <KEYCHAIN>**	<KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов.
7	Выбрать алгоритм аутентификации для L1-уровня (не обязательно).	**esr(config-isis)# authentication area algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм аутентификации: • cleartext – пароль, передается открытым текстом; • md5 – пароль хешируется по алгоритму md5.

Шаг	Описание	Команда	Ключи
8	Установить пароль аутентификации для L1-уровня (не обязательно).	**esr(config-isis)# authentication area key ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<CLEAR-TEXT> – пароль, задаётся строкой 8 символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером 8 байт (16 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).
9	Установить список ключей для аутентификации (не обязательно).	**esr(config-isis)# authentication area key chain <KEYCHAIN>**	<KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов.
10	Включить передачу имени устройства в LSP (не обязательно).	**esr(config-isis)# hostname dynamic**	
11	Установить уровень работы IS-IS процесса (не обязательно).	**esr(config-isis)# is-type {<LEVEL>}**	<LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-1-2 – работа производится и на 1, и на 2 уровне; • level-2 – работа производится только на 2 уровне.
12	Установить тип метрики, который будет использоваться в работе IS-IS процесса (не обязательно).	**esr(config-isis)# metric-style { narrow | wide | transition } [<LEVEL>]**	narrow — принимает и генерирует TLV (о достижимости сетей) старого типа; wide — принимает и генерирует TLV (о достижимости сетей) нового типа; transition — принимает и генерирует TLV (о достижимости сетей) нового и старого типа; <LEVEL> — уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
13	Установить приоритетность маршрутов для данного IS-IS процесса (не обязательно).	**esr(config-isis)# preference {<VALUE>}**	<VALUE> – принимает значения [1..255].

Шаг	Описание	Команда	Ключи
14	Включить работу IS-IS с IPv4 и/или IPv6 адресами (не обязательно).	**esr(config-isis)# address-family { ipv4 | ipv6 }**	ipv4 – семейство адресов IPv4; ipv6 – семейство адресов IPv6.
15	Установить интервал обновления собственных LSP (не обязательно).	**esr(config-isis)# lsp-refresh-interval { min | max } <TIME> [<LEVEL>]**	min — минимальный интервал обновления/генерации; max — максимальный интервал обновления/генерации; <TIME> — время в секундах, принимает значения [1..65535]; <LEVEL> — уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
16	Установить время жизни собственных LSP (не обязательно).	**esr(config-isis)# max-lsp-lifetime <TIME> [<LEVEL>]**	<TIME> – время в секундах, принимает значения [1..65535]; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
17	Установить таймаут перед следующим расчётом SPF (не обязательно).	**esr(config-isis)# spf-timeout <TIME> [<LEVEL>]**	<TIME> – время в миллисекундах, принимает значения [1..10000]; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.

Шаг	Описание	Команда	Ключи
18	Включить анонсирование маршрутов, полученных альтернативным способом (не обязательно).	**esr(config-isis)# redistribute bgp <AS> [route-map <NAME>] [is-type <LEVEL>]**	<AS> – номер автономной системы, может принимать значения [1..4294967295]; <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых маршрутов, задаётся строкой до 31 символа; <LEVEL> — уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
		esr(config-isis)# redistribute ipv6 bgp <AS> [route-map <NAME>] [is-type <LEVEL>]	
		esr(config-isis)# redistribute ospf <ID> <ROUTE-TYPE> [route-map <NAME>] [is-type <LEVEL>]	<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; • external1 – анонсирование внешних маршрутов OSPF-формата 1; • external2 – 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; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
		esr(config-isis)# redistribute ipv6 ospf <ID> <ROUTE-TYPE> [route-map <NAME>] [is-type <LEVEL>]	

Шаг	Описание	Команда	Ключи
		esr(config-isis)# redistribute isis <ID> <ROUTE-TYPE> [route-map <NAME>] [is-type <LEVEL>]	<ID> – номер процесса, может принимать значение [1..65535]; <ROUTE-TYPE> – тип маршрута: • level-1 – анонсирование маршрутов 1 уровня; • level-2 – анонсирование маршрутов 1 уровня; • inter-area – анонсирование маршрутов IS-IS-процесса между зонами; <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых IS-IS-маршрутов, задаётся строкой до 31 символа; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
		esr(config-isis)# redistribute rip [route-map <NAME>] [is-type <LEVEL>]	<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых RIP-маршрутов, задаётся строкой до 31 символа; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.

Шаг	Описание	Команда	Ключи
		esr(config-isis)# redistribute static [route-map <NAME>] [is-type <LEVEL>]	<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых статических маршрутов, задаётся строкой до 31 символа; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
		esr(config-isis)# redistribute connected [route-map <NAME>] [is-type <LEVEL>]	<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых подключённых маршрутов, задаётся строкой до 31 символа; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
19	Добавить фильтрацию подсетей во входящих или исходящих обновлениях (не обязательно).	**esr(config-isis)# prefix-list { ipv6 <LIST_NAME> | <LIST_NAME> } {in|out}**	<LIST-NAME> – имя сконфигурированного списка подсетей, задаётся строкой до 31 символа. in – фильтрация входящих маршрутов; out – фильтрация анонсируемых маршрутов.
20	Добавить фильтрацию подсетей во входящих или исходящих обновлениях (не обязательно).	**esr(config-isis)# route-map <NAME> {in|out}**	<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых маршрутов, задаётся строкой до 31 символа.
21	Установить принадлежность интерфейса к определенному IS-IS процессу.	**esr(config-if-gi)# isis instance <ID>**	<ID> – номер процесса, принимает значения [1..65535].

Шаг	Описание	Команда	Ключи
22	Включить работу протокола IS-IS на интерфейсе.	**esr(config-if-gi)# isis enable**	
23	Включить использование TLV#8 в hello-пакетах (не обязательно).	**esr(config-if-gi)# isis hello-padding**	
24	Установить приоритет при выборе DIS (не обязательно).	**esr(config-if-gi)# isis priority <VALUE> [<LEVEL>]**	<VALUE> – число, принимающее значения [0..127]; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
25	Установить значение метрики для интерфейса (не обязательно).	**esr(config-if-gi)# isis metric <VALUE> [<LEVEL>]**	<VALUE> – число, принимающее значения [1..16777215]; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
26	Установить на каком уровне маршрутизации будет работать текущий процесс IS-IS на конкретном интерфейсе (не обязательно).	**esr(config-if-gi)# isis circuit-type {<LEVEL>}**	<LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-1-2 – работа производится и на 1, и на 2 уровне; • level-2 – работа производится только на 2 уровне.

Шаг	Описание	Команда	Ключи
27	Установить интервал отправки hello-пакетов (не обязательно).	**esr(config-if-gi)# isis hello-interval <TIME> [<LEVEL>]**	<TIME> – время в секундах, принимает значения [1..65535]; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
28	Установить множитель для вычисления и отправки Hold Time (не обязательно).	**esr(config-if-gi)# isis hello-multiplier <VALUE> [<LEVEL>]**	<VALUE> – число, принимающее значения [3..1000]; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
29	Перевести интерфейс в режим работы point-to-point протокола IS-IS (не обязательно).	**esr(config-if-gi)# isis network point-to-point**	
30	Установить интервал генерации и отправки CSNP (не обязательно).	**esr(config-if-gi)# isis csnp-interval <TIME> [<LEVEL>]**	<TIME> – время в секундах, принимает значения [1..65535]; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
31	Установить интервал генерации и отправки PSNP (не обязательно).	**esr(config-if-gi)# isis psnp-interval <TIME> [<LEVEL>]**	<TIME> – время в секундах, принимает значения [1..65535]; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.

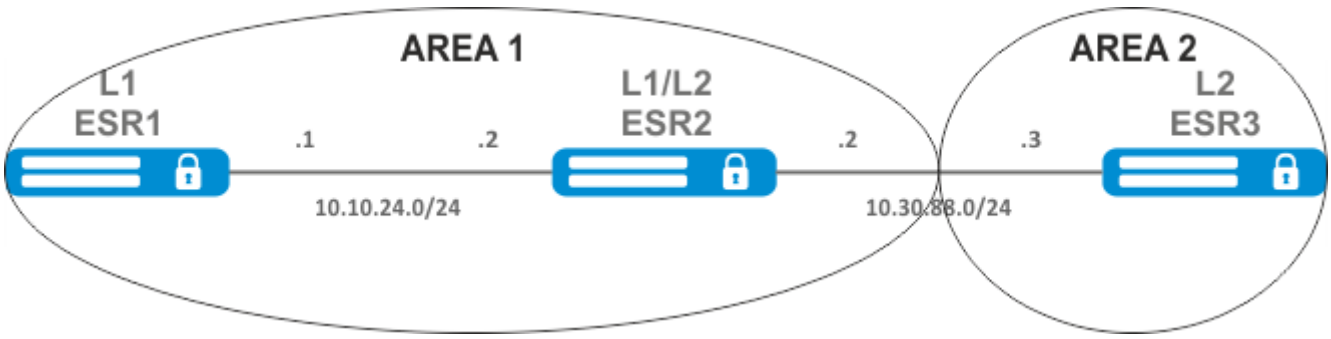
Шаг	Описание	Команда	Ключи
32	Установить интервал между передачами LSP в Broadcast-сети (не обязательно).	**esr(config-if-gi)# isis lsp-interval <TIME> [<LEVEL>]**	<TIME> – время в миллисекундах, принимает значения [1-10000]; <LEVEL> - уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
33	Установить интервал повторного распространения LSP в PtP-сети (не обязательно).	**esr(config-if-gi)# isis lsp-retransmit-interval <TIME> [<LEVEL>]**	<TIME> – время в секундах, принимает значения [1..65535]; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
34	Установить алгоритм аутентификации для hello-пакетов (не обязательно).	**esr(config-if-gi)# isis authentication algorithm <ALGORITHM> [<LEVEL>]**	<ALGORITHM> – алгоритм аутентификации: • cleartext – пароль, передается открытым текстом; • md5 – пароль хешируется по алгоритму md5; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.

Шаг	Описание	Команда	Ключи
35	Установить пароль для аутентификации hello-пакетов (не обязательно).	**esr(config-if-gi)# isis authentication key ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> } [<LEVEL>]**	<CLEAR-TEXT> – пароль, задаётся строкой 8 символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером 8 байт (16 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...); <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
36	Установить список ключей для аутентификации hello-пакетов (не обязательно).	**esr(config-if-gi)# isis authentication key chain <KEYCHAIN> [<LEVEL>]**	<KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.

13.10.2 Пример настройки

Задача:

Настроить протокол IS-IS на устройствах для обмена маршрутной информацией с соседями. Маршрутизатор ESR1 будет L1-only, ESR2 - L1/L2, ESR3 - L2-only, который также будет находится в другой area.



Решение:

Предварительно нужно настроить IP-адреса на интерфейсах согласно схеме, приведенной на рисунке выше.

Перейдём к настройке маршрутизатора ESR1. Создадим IS-IS процесс с идентификатором 1 и перейдём в режим конфигурирования протокола:

```
ESR1(config)# router isis 1
```

Зададим номер зоны, в которой будет работать маршрутизатор и его системный идентификатор:

```
ESR1(config-isis)# net 49.0001.1111.1111.1111.00
```

Настроим работу маршрутизатора только на первом уровне протокола IS-IS:

```
ESR1(config-isis)# is-type level-1
```

Зададим работу маршрутизатора с узкой метрикой на первом уровне:

```
ESR1(config-isis)# metric-style narrow level-1
```

Включим работу процесса IS-IS на маршрутизаторе:

```
ESR1(config-isis)# enable
```

Перейдём к конфигурированию интерфейсов. Нужно задать номер процесса IS-IS, который будет работать на интерфейсе и включить работу самого протокола на нём:

```
ESR1(config-if-gi)# isis instance 1
ESR1(config-if-gi)# isis enable
```

Перейдём к настройке маршрутизатора ESR2:

```
ESR2(config)# router isis 2
```

Зададим номер зоны, такой же как на ESR1, а также уникальный системный идентификатор:

```
ESR2(config-isis)# net 49.0001.2222.2222.2222.00
```

Зададим работу маршрутизатора с узкой метрикой на первом уровне и с широкой метрикой на втором, и включим работу данного процесса IS-IS:

```
ESR2(config-isis)# metric-style narrow level-1
ESR2(config-isis)# metric-style wide level-2
ESR2(config-isis)# enable
```

Настроим работу интерфейсов на маршрутизаторе. На обоих интерфейсах настройка будет одинаковая:

```
ESR2(config-if-gi)# isis instance 2
ESR2(config-if-gi)# isis enable
```

Перейдём к настройке маршрутизатора ESR3:

```
ESR3(config)# router isis 3
ESR3(config-isis)# net 49.0002.3333.3333.3333.00
ESR3(config-isis)# is-type level-2
ESR3(config-isis)# metric-style wide level-2
ESR3(config-isis)# enable
ESR3(config-if-gi)# isis instance 3
ESR3(config-if-gi)# isis enable
```

Установление соседства можно посмотреть командой show isis neighbors. Выполним её на ESR2:

```
ESR2# show isis neighbors
IS-IS 2
IS-IS Level 1 Neighbors
System ID                Hostname          Interface         State         Holdtime  SNPA
1111.1111.1111  ESR1                      gi1/0/2            Up              25
a8f9.4baa.1d42
IS-IS Level 2 Neighbors
System ID              Hostname          Interface         State         Holdtime  SNPA
3333.3333.3333  ESR3                     gi1/0/1            Up              8
a8f9.4bab.813a
```

14 Управление технологией MPLS

- Настройка протокола LDP
  - Алгоритм настройки
  - Пример настройки
- Конфигурирование параметров сессии в протоколе LDP
  - Алгоритм настройки параметров Hello holdtime и Hello interval в глобальной конфигурации LDP
  - Алгоритм настройки параметров Hello holdtime и Hello interval для address family
  - Алгоритм настройки параметра Keepalive holdtime в глобальной конфигурации LDP
  - Алгоритм настройки параметра Keepalive holdtime для определенного соседа
  - Пример настройки
- Конфигурирование параметров сессии в протоколе targeted-LDP
  - Алгоритм настройки параметров Hello holdtime, Hello interval и Keepalive holdtime для процесса LDP
  - Алгоритм настройки параметров Hello holdtime, Hello interval и Keepalive holdtime для определенного соседа
  - Пример настройки
- Настройка фильтрации LDP-меток
  - Алгоритм настройки
  - Пример настройки
- Настройка сервиса L2VPN Martini mode
  - Алгоритм настройки L2VPN VPWS
  - Пример настройки L2VPN VPWS
  - Алгоритм настройки L2VPN VPLS
  - Пример настройки L2VPN VPLS
- Настройка сервиса L2VPN Kompella mode
  - Алгоритм настройки L2VPN VPLS
  - Пример настройки L2VPN VPLS
- Настройка сервиса L3VPN
  - Алгоритм настройки
  - Пример настройки
- Балансировка трафика MPLS
  - Пример настройки
- Работа с бридж-доменом в рамках MPLS
- Назначение MTU при работе с MPLS
- Inter-AS Option A
  - L2VPN
  - L3VPN
- Inter-AS Option B
  - L3VPN
- MPLS over GRE
  - L2VPN
  - L3VPN

14.1 Настройка протокола LDP

LDP — протокол распределения меток. Для нахождения соседей используется рассылка hello-сообщений на мультикастный адрес 224.0.0.2. При обмене hello-сообщениями маршрутизаторы узнают транспортные адреса друг друга. Маршрутизатор с большим адресом инициализирует TCP-сессию. После проверки параметров LDP-сессия считается установленной.

В маршрутизаторах ESR поддержаны следующие режимы работы LDP:

- Режим обмена информации о метках — Downstream Unsolicited;
- Механизм контроля за распространением меток — Independent Label Distribution Control;
- Режим сохранения меток — Liberal Label Retention;

На интерфейсах, где включены протокол LDP и MPLS-коммутация, firewall должен быть отключен.

В текущей реализации протокол LDP работает только с IPv4-адресами.

14.1.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	В контексте настройки параметров MPLS указать интерфейсы, участвующие в процессе MPLS-коммутации.	**esr(config-mpls)# forwarding 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.
2	Задать router-id для LDP (не обязательно, если указан transport-address).	**esr(config-ldp)# 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.

Шаг	Описание	Команда	Ключи
3	В контексте настройки address family ipv4 указать transport-address (не обязательно, если указан router-id).	**esr(config-ldp-af-ipv4)# transport-address <ADDR>**	<ADDR> – задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
4	В контексте настройки address family ipv4 указать интерфейсы для включения на них процесса LDP.	**esr(config-ldp-af-ipv4)# 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.
5	Включить процесс LDP.	**esr(config-ldp)# enable**	
6	Включить функционал explicit-null (не обязательно).	**esr(config-ldp)# egress-label-type explicit-null**	
7	В режиме конфигурирования соседа LDP задать пароль командой password (не обязательно).	**esr(config-ldp-neig)# password {<TEXT> | ENCRYPTED-TEXT>}**	<CLEAR-TEXT> – пароль, задаётся строкой длиной [8..16] символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером [8..16] байт ([16..32] символа) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).

В рамках настройки протокола LDP также доступен следующий функционал:

- Настройка фильтрации LDP-меток (см. Настройка фильтрации LDP-меток);
- Настройка параметров LDP-сессии (см. Конфигурирование параметров сессии в протоколе LDP);
- Настройка параметров tLDP-сессии (см. Конфигурирование параметров сессии в протоколе targeted-LDP).

Если изменить значение router-id, то новое значение будет применено только после рестарта данного протокола. Для рестарта mpls ldp используется команда clear mpls ldp.

14.1.2 Пример настройки

Задача:

Настроить взаимодействие по протоколу LDP между пирами.

Решение:

Предварительная конфигурация ESR:

Предварительно на интерфейсы должны быть назначены IP-адреса, отключен межсетевой экран и настроен один из протоков внутренней маршрутизации.

Предварительная конфигурация ESR:

```
hostname ESR
router ospf 1
  area 0.0.0.0
    enable
  exit
  enable
exit


interface gigabitethernet 1/0/1
  ip firewall disable
  ip address 10.10.10.1/30
  ip ospf instance 1
  ip ospf
exit


interface loopback 1
  ip address 1.1.1.1/32
  ip ospf instance 1
  ip ospf
exit
```

Предварительная конфигурация ESR1:

```
hostname ESR1
router ospf 1
  area 0.0.0.0
    enable
  exit
  enable
exit


interface gigabitethernet 1/0/1
  ip firewall disable
  ip address 10.10.10.2/30
  ip ospf instance 1
  ip ospf
exit


interface loopback 1
  ip address 4.4.4.4/32
  ip ospf instance 1
  ip ospf
exit
```

Настройка на ESR:

ESR

```
ESR# config
ESR(config)# mpls
ESR(config-mpls)# forwarding interface gigabitethernet 1/0/1
ESR(config-mpls)# ldp
ESR(config-ldp)# router-id 1.1.1.1
ESR(config-ldp)# enable
ESR(config-ldp)# address-family ipv4
ESR(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1
ESR(config-ldp-af-ipv4-if)# end
ESR#
```

Настройка на ESR1:

ESR1

```
ESR1# configure
ESR1(config)# mpls
ESR1(config-mpls)# forwarding interface gigabitethernet 1/0/1
ESR1(config-mpls)# ldp
ESR1(config-ldp)# router-id 4.4.4.4
ESR1(config-ldp)# enable
ESR1(config-ldp)# address-family ipv4
ESR1(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1
ESR1(config-ldp-af-ipv4-if)# end
ESR1#
```

Проверка:

На одном из пиров ввести следующие команды:

```
ESR# show mpls ldp discovery detailed
Local LDP ID: 1.1.1.1
Discovery sources:
    Interfaces:
        gigabitethernet 1/0/1:
                 Hello interval: 5 seconds
        Transport IP address: 1.1.1.1
        LDP ID: 4.4.4.4
            Source IP address: 10.10.10.2
            Transport IP address: 4.4.4.4
                         Hold time: 15 seconds
                         Proposed hold time: 90/15 (local/peer) seconds
```

Вывод покажет параметры соседнего пира, полученные из мультикастовых hello-сообщений.

Сессия LDP должна находиться в статусе "Operational".

```
ESR1# show mpls ldp neighbor
Peer LDP ID: 4.4.4.4; Local LDP ID 1.1.1.1
    State: Operational
    TCP connection: 4.4.4.4:40245 - 1.1.1.1:646
    Messages sent/received: 10/11
    Uptime: 00:00:58
    LDP discovery sources:
        gigabitethernet 1/0/1
```

14.2 Конфигурирование параметров сессии в протоколе LDP

По умолчанию в рассылаемых hello-сообщениях установлены следующие значения:

Параметр	LDP
Hello interval	5 секунд
Hold timer	15 секунд
Keepalive holdtime	180 секунд

Hold timer является согласуемым параметром – выбирается наименьший. В данном примере показано, что на ESR после согласования Hold timer равен 10 секундам.

```
ESR# sh mpls ldp discovery detailed
Local LDP ID: 4.4.4.4
Discovery sources:
    Interfaces:
        gigabitethernet 1/0/4:
            Hello interval: 5 seconds
            Transport IP address: 4.4.4.4
            LDP ID: 1.1.1.1
                Source IP address: 10.10.10.1
                Transport IP address: 1.1.1.1
                                    Hold time: 10 seconds
                                    Proposed hold time: 15/10 (local/peer) seconds
```

Если после согласования Hello interval стал больше, чем Hold timer, то Hello interval будет равным Hold timer/3.

На маршрутизаторах ESR реализована возможность гибкой настройки параметров Hello holdtime, Hello interval и Keepalive holdtime. Рассмотрим пример настройки Hello holdtime для LDP-сессии:

```
ESR# show run mpls
mpls
  ldp
  router-id 4.4.4.4
     discovery hello holdtime 40
    address-family ipv4
      interface gigabitethernet 1/0/4
             discovery hello holdtime 60
    exit
  exit
  enable
exit
```

Если параметры Hello Holdtime и Hello Interval не указаны, то используются значения по умолчанию. Если параметры указаны, то приоритет значений для address-family будет выше, чем для значений, сконфигурированных глобально.

```
ESR# show mpls ldp discovery detailed
Local LDP ID: 4.4.4.4
Discovery sources:
    Interfaces:
        gigabitethernet 1/0/4:
            Hello interval: 5 seconds
            Transport IP address: 4.4.4.4
            LDP ID: 1.1.1.1
                Source IP address: 10.10.10.1
                Transport IP address: 1.1.1.1
                Hold time: 15 seconds
                                    Proposed hold time: 60 /15 (local/peer) seconds
```

Параметры, сконфигурированные в address-family, могут быть настроены на каждый отдельный интерфейс, участвующий в процессе LDP.

```
ESR# show running-config mpls
mpls
  ldp
    router-id 4.4.4.4
    discovery hello holdtime 50
    discovery hello interval 10
    address-family ipv4
             interface gigabitethernet 1/0/1
                 discovery hello holdtime 60
                 discovery hello interval 20
      exit
             interface gigabitethernet 1/0/4
                 discovery hello holdtime 30
                 discovery hello interval 10
      exit
    exit
  enable
exit
```

Для TCP-сессии Keepalive holdtime является также согласуемым параметром по аналогии с Hold timer. Keepalive interval рассчитывается автоматически и равен Keepalive holdtime/3. Keepalive holdtime можно задать как глобально, так и для каждого соседа. Таймер, заданный для определенного соседа, является более приоритетным.

```
ESR# show running-config mpls
mpls
  ldp
  router-id 4.4.4.4
     keepalive 30 // установлен в глобальной конфигурации LDP
  neighbor 1.1.1.1
     keepalive 55// установлен в соседа с адресом 1.1.1.1
  exit
exit
```

```
ESR# sh mpls ldp neighbor 1.1.1.1
Peer LDP ID: 1.1.1.1; Local LDP ID 4.4.4.4
    State: Operational
    TCP connection: 1.1.1.1:646 - 4.4.4.4:56668
    Messages sent/received: 401/401
    Uptime: 02:00:24
    Peer holdtime: 55
    Keepalive interval: 18
    LDP discovery sources:
```

14.2.1 Алгоритм настройки параметров Hello holdtime и Hello interval в глобальной конфигурации LDP

Шаг	Описание	Команда	Ключи
1	Настроить протокол LDP (см. раздел Конфигурирование протокола LDP)		
2	В режиме конфигурации протокола LDP задать Hello holdtime	**esr(config-ldp)# discovery hello holdtime <TIME>**	<TIME> – время в секундах в интервале [3..65535] Значение по умолчанию: 15
3	В режиме конфигурации протокола LDP задать Hello interval	**esr(config-ldp)# discovery hello interval <TIME>**	<TIME> – время в секундах в интервале [3..65535] Значение по умолчанию: 5

14.2.2 Алгоритм настройки параметров Hello holdtime и Hello interval для address family

Шаг	Описание	Команда	Ключи
1	Настроить протокол LDP (см. раздел Конфигурирование протокола LDP)		
2	В режиме конфигурации address famillly протокола LDP установить Hello holdtime на нужном интерфейсе	**esr(config-ldp-af-ipv4-if)# discovery hello holdtime <TIME>**	<TIME> – время в секундах в интервале [3..65535] Значение по умолчанию: 15
3	В режиме конфигурации address famillly протокола LDP установить Hello interval на нужном интерфейсе	**esr(config-ldp-af-ipv4-if)# discovery hello interval <TIME>**	<TIME> – время в секундах в интервале [3..65535] Значение по умолчанию: 5

14.2.3 Алгоритм настройки параметра Keepalive holdtime в глобальной конфигурации LDP

Шаг	Описание	Команда	Ключи
1	Настроить протокол LDP (см. раздел Конфигурирование протокола LDP)		
2	В режиме конфигурации LDP задать параметр Keepalive	**esr(config-ldp)# keepalive <TIME>**	<TIME> – время в секундах в интервале [3..65535] Значение по умолчанию: 180

14.2.4 Алгоритм настройки параметра Keepalive holdtime для определенного соседа

Шаг	Описание	Команда	Ключи
1	Настроить протокол LDP (см. раздел Конфигурирование протокола LDP)		
2	В режиме конфигурации соседа задать параметр Keepalive holdtime	**esr(config-ldp-neig)# keepalive <TIME>**	<TIME> – время в секундах в интервале [3..65535] Значение по умолчанию: 180

14.2.5 Пример настройки

Задача:

Переопределить параметры Hello holdtime (40 секунд) и Hello interval (10 секунд) для всего процесса LDP. Для соседа с адресом 1.1.1.1 установить Keepalive holdtime равным 150 секунд.

Решение:

ESR

```
ESR(config)# mpls
ESR(config-mpls)# ldp
ESR(config-ldp)# discovery hello holdtime 40
ESR(config-ldp)# discovery hello interval 10
ESR(config-ldp)# neighbor 1.1.1.1
ESR(config-ldp-neig)# keepalive 150
```

Проверка:

Для просмотра hello-параметров:

ESR

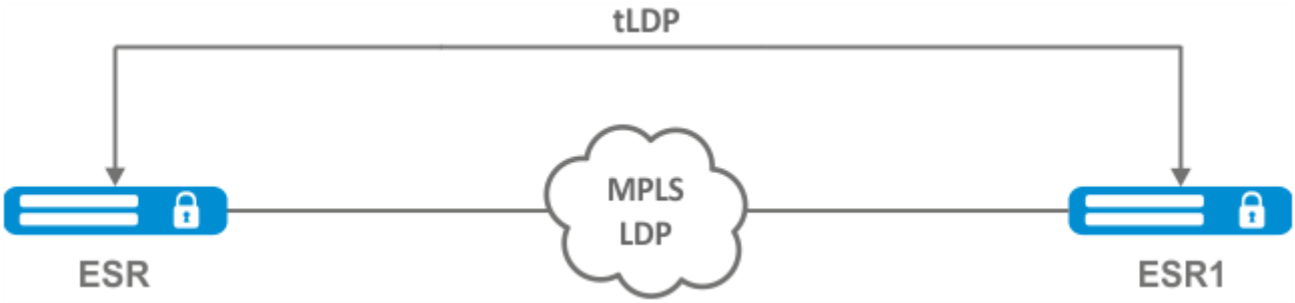
```
ESR# sh mpls ldp discovery detailed
Local LDP ID: 4.4.4.4
Discovery sources:
    Interfaces:
        gigabitethernet 1/0/4:
            Hello interval:       10 seconds
            Transport IP address: 4.4.4.4
            LDP ID:               1.1.1.1
                Source IP address:    10.10.10.1
                Transport IP address: 1.1.1.1
                Hold time:            15 seconds
                Proposed hold time:   40/15 (local/peer) seconds
```

Для просмотра параметров установленной TCP-сессии:

ESR

```
ESR# sh mpls ldp neighbor 1.1.1.1
Peer LDP ID: 1.1.1.1; Local LDP ID 4.4.4.4
    State:                  Operational
    TCP connection:         1.1.1.1:646 - 4.4.4.4:45414
    Messages sent/received: 15/15
    Uptime:                 00:06:31
    Peer holdtime:          150
    Keepalive interval:     50
    LDP discovery sources:
```

14.3 Конфигурирование параметров сессии в протоколе targeted-LDP



По умолчанию для targeted LDP-сессии установлены следующие значения:

Параметр	targeted-LDP
Hello interval	5 секунд
Hold timer	45 секунд
Keepalive holdtime	180 секунд

Hold timer является согласуемым параметром – выбирается наименьший. В данном примере показано, что ESR после согласования установил 30 секунд:

```
ESR1# sh mpls ldp discovery detailed

...
Targeted hellos:
1.1.1.1 -> 4.4.4.4:
Hello interval: 2 seconds
Transport IP address: 1.1.1.1
LDP ID: 4.4.4.4
Source IP address: 4.4.4.4
Transport IP address: 4.4.4.4
Hold time: 30 seconds
Proposed hold time: 30/45 (local/peer) seconds
```

Если после согласования Hello interval стал больше, чем Hold timer, то Hello interval будет равным Hold timer/3.

На маршрутизаторах ESR реализована возможность гибкой настройки параметров Hello holdtime, Hello interval и Keepalive holdtime: параметры можно задать как для всего процесса LDP, так и на соответствующего соседа.

Пример вывода для процесса LDP:

```
ESR# sh running-config mpls
mpls
  ldp
    router-id 1.1.1.1
         keepalive 160
         discovery targeted-hello holdtime 30
         discovery targeted-hello interval 10
  exit
exit
```

Пример вывода для targeted-LDP-сессии для определенного соседа:

```
ESR# sh running-config mpls
mpls
  ldp
    router-id 1.1.1.1
    neighbor 4.4.4.4
      keepalive 160
      targeted
      discovery targeted-hello holdtime 30
      discovery targeted-hello interval 45
    exit
  exit
exit
```

Если параметры установлены и для процесса LDP, и на определенного соседа, приоритетом будут считаться настройки, установленные для соседа.

```
ESR# sh running-config mpls
mpls
  ldp
    router-id 1.1.1.1
    keepalive  160
    discovery hello holdtime 90
    discovery targeted-hello interval 30
    neighbor 4.4.4.4
      keepalive 140
      targeted
      discovery targeted-hello holdtime 45
      discovery targeted-hello interval 15
    exit
  exit
exit
```

```
ESR# show mpls ldp discovery detailed
...
Targeted hellos:
1.1.1.1 -> 4.4.4.4:
Hello interval: 15 seconds
Transport IP address: 1.1.1.1
LDP ID: 4.4.4.4
Source IP address: 4.4.4.4
Transport IP address: 4.4.4.4
Hold time: 45 seconds
Proposed hold time: 45/45 (local/peer) seconds


ESR# show mpls ldp neighbor 4.4.4.4
Peer LDP ID: 4.4.4.4; Local LDP ID 1.1.1.1
     State: Operational
      TCP connection: 4.4.4.4:51861 - 1.1.1.1:646
      Messages sent/received: 10/10
      Uptime: 00:00:09
      Peer holdtime: 140
      Keepalive interval: 46
      LDP discovery sources:
            1.1.1.1 -> 4.4.4.4:
```

14.3.1 Алгоритм настройки параметров Hello holdtime, Hello interval и Keepalive holdtime для процесса LDP

1	Настроить протокол LDP (см. раздел Конфигурирование протокола LDP)		
2	В режиме конфигурации протокола LDP задать Hello holdtime	**esr(config-ldp)# discovery targeted-hello holdtime <TIME>**	<TIME> – время в секундах в интервале [3..65535] Значение по умолчанию: 45

3	В режиме конфигурации протокола LDP задать Hello interval	**esr(config-ldp)# discovery targeted- hello interval <TIME>**	<TIME> – время в секундах в интервале [1..65535] Значение по умолчанию: 5
4	В режиме конфигурации протокола LDP задать Keepalive holdtime	**esr(config-ldp)# keepalive <TIME>**	<TIME> – время в секундах в интервале [3..65535] Значение по умолчанию: 180

14.3.2 Алгоритм настройки параметров Hello holdtime, Hello interval и Keepalive holdtime для определенного соседа

1	Настроить протокол LDP (см. раздел Конфигурирование протокола LDP)		
2	В режиме конфигурации LDP-соседа задать Hello holdtime	**esr(config-ldp-neig)# discovery targeted-hello holdtime <TIME>**	<TIME> – время в секундах в интервале [3..65535] Значение по умолчанию: 45
3	В режиме конфигурации LDP-соседа задать Hello interval	**esr(config-ldp-neig)# discovery targeted- hello interval <TIME>**	<TIME> – время в секундах в интервале [1..65535] Значение по умолчанию: 5
4	В режиме конфигурации LDP-соседа задать Keepalive holdtime	**esr(config-ldp-neig)# keepalive <TIME>**	<TIME> – время в секундах в интервале [3..65535] Значение по умолчанию: 180

14.3.3 Пример настройки

Задача:

Переопределить параметры Hello holdtime (120 секунд) и Hello interval (30 секунд) для всего процесса targeted-LDP. Для соседа с адресом 4.4.4.4 установить Keepalive holdtime равным 150 секунд.

Решение:

ESR

```
ESR(config)# mpls
ESR(config-mpls)# ldp
ESR(config-ldp)# discovery targeted-hello holdtime 40
ESR(config-ldp)# discovery targeted-hello interval 10
ESR(config-ldp)# neighbor 4.4.4.4
ESR(config-ldp-neig)# keepalive 150
```

Проверка:

Для просмотра hello-параметров targeted LDP-сессии:

ESR

```
ESR1# sh mpls ldp discovery detailed
...
    Targeted hellos:
         1.1.1.1 -> 4.4.4.4:
            Hello interval:       10 seconds
            Transport IP address: 1.1.1.1
            LDP ID:               4.4.4.4
                Source IP address:    4.4.4.4
                Transport IP address: 4.4.4.4
                Hold time:            40 seconds
                Proposed hold time:   40/45 (local/peer) seconds
```

Для просмотра параметров установленной TCP-сессии:

ESR

```
ESR# sh mpls ldp neighbor 4.4.4.4
Peer LDP ID: 4.4.4.4; Local LDP ID 1.1.1.1
    State:                  Operational
    TCP connection:         4.4.4.4:34879 - 1.1.1.1:646
    Messages sent/received: 11/11
    Uptime:                 00:01:05
    Peer holdtime:          150
    Keepalive interval:     50
    LDP discovery sources:
         1.1.1.1 -> 4.4.4.4:
            Hello interval: 10 seconds
            Holdtime:       40 seconds
  ...
```

14.4 Настройка фильтрации LDP-меток

По умолчанию маршрутизаторы выделяют на каждый FEC отдельную метку. Существуют сценарии, когда необходимо выделять MPLS-метки только для определенных FEC.

14.4.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Настроить протокол LDP (см. раздел Конфигурирование протокола LDP).		
2	Создать object-group типа network.	**esr(config)# object-group network <NAME>**	<NAME> – имя конфигурируемого списка подсетей, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
3	Описать префиксы, для которых будут назначаться метки.	**esr(config-object-group-network)# ip prefix <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].
4	В контексте настройки LDP применить созданную object-group.	**esr(config-ldp)# advertise-labels <NAME>**	<NAME> – имя конфигурируемого списка подсетей, задаётся строкой до 31 символа.

Метки будут выделяться ТОЛЬКО на описанные в object-group подсети, независимо от того, как они были изучены (connected, local, IGP и т.д.).

В object-group необходимо описывать префиксы.
Префикс должен иметь точное совпадение с маршрутом из FIB.

Данный функционал поддержан для протокола IPv4.

14.4.2 Пример настройки

Задача:

Назначить MPLS-метки только FEC 10.10.0.2/32 и 10.10.0.1/32.

Решение:

На ESR_A и ESR_B создадим object-group ADV_LABELS типа network и добавим в нее префиксы 10.10.0.1/32 и 10.10.0.2/32 соответственно:

ESR_A

```
esr(config)# object-group network ADV_LABELS
esr(config-object-group-network)# ip prefix 10.10.0.1/32
esr(config-object-group-network)# ip prefix 10.10.0.2/32
```

ESR_B

```
esr(config)# object-group network ADV_LABELS
esr(config-object-group-network)# ip prefix 10.10.0.1/32
esr(config-object-group-network)# ip prefix 10.10.0.2/32
```

Применим созданную object-group на обоих маршрутизаторах:

ESR_A и ESR_B

```
esr(config)# mpls
esr(config-ldp)# ldp
esr(config-ldp)# advertise-labels ADV_LABELS
```

Проверка:

На ESR_B убедимся, что метка назначена для соответствующих префиксов:

```
esr# sh mpls ldp bindings 10.10.0.1/32
10.10.0.1/32
local label: exp-null
remote label: 75 lsr: 172.16.0.1
```

И не назначена для 192.168.2.0/24:

```
esr# sh mpls ldp bindings 192.168.2.0/24
esr#
```

14.5 Настройка сервиса L2VPN Martini mode

L2VPN позволяет организовать передачу ethernet-фреймов через MPLS-домен. Выделение и распространение туннельных меток в данном режиме осуществляется по средствам протокола LDP. В реализации L2VPN можно условно выделить два случая:

1. P2P – туннель, создаваемый по схеме "точка-точка".
2. VPLS – туннель, создаваемый по схеме "точка-многоточка".

В обоих случаях для передачи ethernet-фреймов между маршрутизаторами создается виртуальный канал (далее pseudo-wire). Для согласования параметров pseudo-wire, а также для выделения и передачи туннельных меток между маршрутизаторами, устанавливается LDP-сессия в targeted-режиме.

14.5.1 Алгоритм настройки L2VPN VPWS

Шаг	Описание	Команда	Ключи
1	Настроить протокол LDP (см. раздел Конфигурирование протокола LDP).		
2	Создать pw-class в системе и осуществить переход в режим настройки параметров pw-class.	**esr(config-l2vpn)# pw-class <WORD>**	<WORD> – имя pw-class длиной [1..31] символов.
3	Добавить описание для pw-class (не обязательно).	**esr(config-l2vpn-pw-class)# description <LINE>**	<LINE> – описание. Задается в виде строки длиной [1..255] символов.

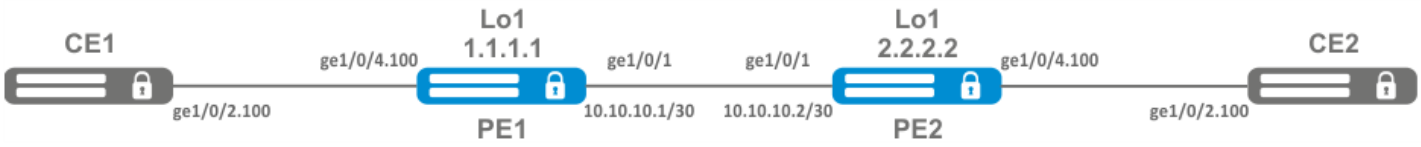
Шаг	Описание	Команда	Ключи
4	Установить значение MTU для pseudo-wire входящих в pw-class (не обязательно).	**esr(config-l2vpn-pw-class)# encapsulation mpls mtu <MTU>**	<MTU> – значение MTU, принимает значение в диапазоне [552..10000] Значение по умолчанию: 1500.
5	Отключить обмен status-tlv сообщениями (не обязательно).	**esr(config-l2vpn-pw-class)# encapsulation mpls status-tlv disable**	Значение по умолчанию: status-tlv enable.
6	Создать p2p-туннель в системе и осуществить переход в режим настройки параметров p2p-туннеля.	**esr(config-l2vpn)# p2p <NAME>**	<NAME> – имя p2p-сервиса, задается строкой до 31 символа.
7	Задать Attached Circuit интерфейс.	**esr(config-l2vpn-p2p)# 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.
8	Включить p2p-туннель.	**esr(config-l2vpn-p2p)# enable**	
9	Задать транспортный режим (не обязательно).	**esr(config-l2vpn-p2p)# transport-mode { ethenet | vlan }**	<ethernet> – режим, при котором при входе в pseudo-wire из заголовка удаляется 802.1Q тег ; <vlan> – режим, при котором 802.1Q тег может быть сохранен при передаче через pseudo-wire. Значение по умолчанию: ethernet.

Шаг	Описание	Команда	Ключи
10	Создать pseudo-wire и осуществить переход в режим настройки его параметров.	**esr(config-l2vpn-p2p)# pw <PW_ID> <LSR_ID>**	<PW_ID> – идентификатор psewdowire, задается в виде числа в диапазоне [1..4294967295] <LSR_ID> – идентификатор LSR, до которого строится pseudo-wire, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]
11	Добавить описание для pseudo-wire (не обязательно).	**esr(config-l2vpn-pw)# description <LINE>**	<LINE> – описание. Задается в виде строки длиной [1..255] символов.
12	Задать pw-class для pseudo-wire.	**esr(config-l2vpn-pw)# pw-class <WORD>**	<WORD> – имя pw-class длиной [1..31] символов.
13	Задать адрес LSR до которого устанавливается pseudo-wire (не обязательно, если neighbor address совпадает с LSR_ID).	**esr(config-l2vpn-pw)# neighbor-address <ADDR>**	<ADDR> – IP-адрес маршрутизатора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
14	Включить pseudo-wire.	**esr(config-l2vpn-pw)# enable**	
	В случае если необходимо изменить параметры по умолчанию для targeted LDP-сессии, обратитесь к разделу Конфигурирование параметров сессии в протоколе targeted-LDP.		

14.5.2 Пример настройки L2VPN VPWS

Задача:

Настроить l2vpn таким образом, чтобы интерфейс ge1/0/2.100 маршрутизатора CE1 и интерфейс ge1/0/2.100 маршрутизатора CE2 работали в рамках одного широковещательного домена.



Решение:

Предварительно нужно:

- Включить поддержку Jumbo-фреймов с помощью команды "system jumbo-frames" (для вступления изменений в силу требуется перезагрузка устройства);
- Настроить IP-адреса на интерфейсах согласно схеме сети, приведенной на рисунке выше;
- Организовать обмен маршрутами между PE1 и PE2 при помощи IGP-протокола (OSPF, IS-IS, RIP).

На маршрутизаторе PE1 создадим саб-интерфейс, на который будем принимать трафик от CE1:

```
PE1# configure
PE1(config)# interface gigabitethernet 1/0/4.100
PE1(config-subif)# exit
```

Выставим на интерфейсе в сторону PE2 значение MTU равным 9600, для того чтобы избежать ситуации с превышением MTU после инкапсуляции MPLS-заголовка, а также отключим межсетевой экран:

```
PE1#(config)# interface gigabitethernet 1/0/1
PE1(config-if-gi)# mtu 9600
PE1(config-if-gi)# ip firewall disable
PE1(config-if-gi)# exit
```

Разрешим прием пакетов с MPLS-заголовком на интерфейсе в сторону MPLS-сети (в данном примере интерфейс в сторону PE2):

```
PE1(config)# mpls
PE1(config-mpls)# forwarding interface gigabitethernet 1/0/1
```

Настроим протокол LDP и включим обнаружение соседей на интерфейсе в сторону PE2:

```
PE1(config-mpls)# ldp
PE1(config-ldp)# router-id 1.1.1.1
PE1(config-ldp)# address-family ipv4
PE1(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1
PE1(config-ldp-af-ipv4-if)# exit
PE1(config-ldp-af-ipv4)# transport-address 1.1.1.1
PE1(config-ldp-af-ipv4)# exit
PE1(config-ldp)# enable
PE1(config-ldp)# exit
```

Создадим pw-class, на основе которого в дальнейшем будет создан виртуальный канал (pw). Так как в данном примере на pw будут применяться параметры по умолчанию, достаточно будет указать имя класса:

```
PE1(config-mpls)# l2vpn
PE1(config-l2vpn)# pw-class for_p2p_VLAN100
PE1(config-l2vpn-pw-class)# exit
```

Создадим новый l2vpn типа p2p и добавим pw до маршрутизатора PE3, идентификатор pw для удобства возьмем равным VID (в данном случае равным 100):

```
PE1(config-l2vpn)# p2p to_PE2_VLAN100
PE1(config-l2vpn-p2p)# interface gigabitethernet 1/0/4.100
PE1(config-l2vpn-p2p)# pw 100 3.3.3.3
PE1(config-l2vpn-pw)# pw-class for_p2p_VLAN100
PE1(config-l2vpn-pw)# enable
PE1(config-l2vpn-pw)# exit
PE1(config-l2vpn-p2p)# enable
PE1(config-l2vpn-p2p)# end
```

Применим конфигурацию:

```
PE1# commit
PE1# confirm
```

Проведем настройку маршрутизатора PE2 по аналогии с PE1:

```
PE2# configure
PE2(config)# interface gigabitethernet 1/0/4.100
PE2(config-subif)# exit
PE2#(config)# interface gigabitethernet 1/0/1
PE2(config-if-gi)# mtu 9600
PE1(config-if-gi)# ip firewall disable
PE1(config-if-gi)# exit
PE2(config)# mpls
PE2(config-mpls)# forwarding interface gigabitethernet 1/0/1
PE2(config-mpls)# ldp
PE2(config-ldp)# router-id 2.2.2.2
PE2(config-ldp)# address-family ipv4
PE2(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1
PE2(config-ldp-af-ipv4-if)# exit
PE2(config-ldp-af-ipv4)# transport-address 2.2.2.2
PE2(config-ldp-af-ipv4)# exit
PE2(config-ldp)# enable
PE2(config-ldp)# exit
PE2(config-mpls)# l2vpn
PE2(config-l2vpn)# pw-class for_p2p_VLAN100
PE2(config-l2vpn-pw-class)# exit
PE2(config-l2vpn)# p2p to_PE1_VLAN100
PE2(config-l2vpn-p2p)# interface gigabitethernet 1/0/4.100
PE2(config-l2vpn-p2p)# pw 100 1.1.1.1
PE2(config-l2vpn-pw)# pw-class for_p2p_VLAN100
PE2(config-l2vpn-pw)# enable
PE2(config-l2vpn-pw)# exit
PE2(config-l2vpn-p2p)# enable
PE2(config-l2vpn-p2p)# end
PE2# commit
PE2# confirm
```

Убедимся в установлении соседства по протоколу LDP и выведем информацию по статусу виртуального канала (pseudowire) между PE1 и PE2:

```
PE2# show mpls ldp neighbor
Peer LDP ID: 1.1.1.1; Local LDP ID 2.2.2.2
    State: Operational
    TCP connection: 1.1.1.1:646 - 2.2.2.2:34625
    Messages sent/received: 12/12
    Uptime: 00:03:50
    LDP discovery sources:
        2.2.2.2 -> 1.1.1.1
```

```
PE2# show mpls l2vpn pseudowire
Neighbor                                PW ID           Type          Status
--------------------------------------- ----------      ----------    ------
1.1.1.1                                   100           Ethernet        Up
```

Соседство по протоколу LDP установлено, pseudowire перешел в статус 'UP'. Настройка l2vpn типа p2p завершена.

14.5.3 Алгоритм настройки L2VPN VPLS

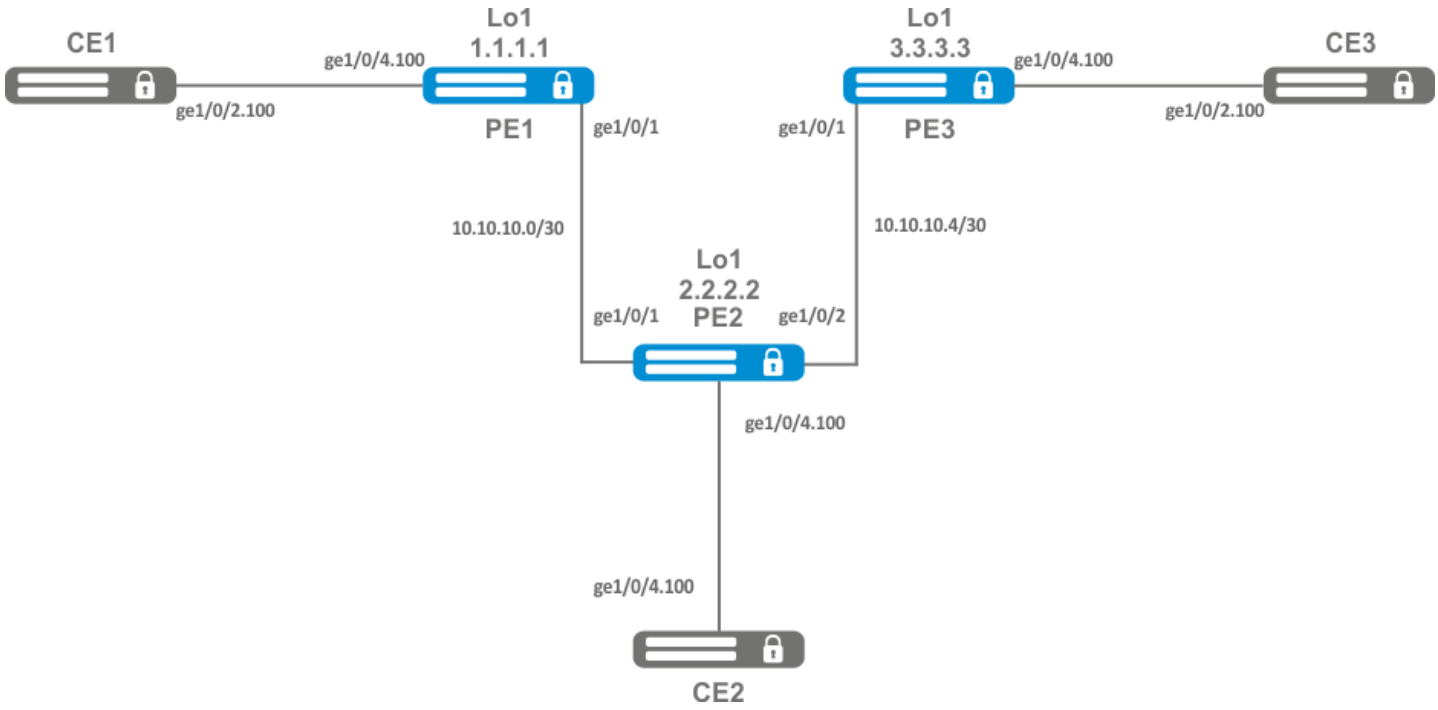
Шаг	Описание	Команда	Ключи
1	Настроить протокол LDP (см. раздел Конфигурирование протокола LDP).		
2	Создать сетевой мост в системе без указания IP-адреса (см. раздел Настройка Bridge).		
3	Создать pw-class в системе и осуществить переход в режим настройки параметров pw-class.	**esr(config-l2vpn)# pw-class <WORD>**	<WORD> – имя pw-class длинной [1..31] символов.
4	Добавить описание для pw-class (не обязательно).	**esr(config-l2vpn-pw-class)# description <LINE>**	<LINE> – описание. Задается в виде строки длинной [1..255] символов
5	Установить значение MTU для pseudo-wire входящих в pw-class (не обязательно).	**esr(config-l2vpn-pw-class)# encapsulation mpls mtu <MTU>**	<MTU> – значение MTU, принимает значение в диапазоне [552..10000] Значение по умолчанию: 1500.
6	Отключить обмен status-tlv сообщениями (не обязательно).	**esr(config-l2vpn-pw-class)# encapsulation mpls status-tlv disable**	Значение по умолчанию: status-tlv enable.
7	Создать VPLS-домен в системе и осуществить переход в режим настройки параметров VPLS-домена.	**esr(config-l2vpn)# vpls <NAME>**	<NAME> – имя p2p-сервиса, задается строкой до 31 символа.
8	Включить VPLS-туннель.	**esr(config-l2vpn-vpls)# enable**	
9	Добавить бридж-домен.	**esr (config-l2vpn-vpls)# bridge-group <ID>**	<ID> – идентификатор бридж-домена, задается в виде числа в диапазоне [1..250].
10	Задать транспортный режим (не обязательно).	**esr(config-l2vpn-vpls)# transport-mode { ethenet | vlan }**	<ethernet> – режим при котором при входе в pseudo-wire из заголовка удаляется 802.1Q тег; <vlan> – режим при котором 802.1Q тег может быть сохранен при передаче через pseudo-wire. Значение по умолчанию: ethernet.

Шаг	Описание	Команда	Ключи
11	Создать pseudo-wire и осуществить переход в режим настройки его параметров.	**esr(config-l2vpn-vpls)# pw <PW_ID> <LSR_ID>**	<PW_ID> – идентификатор psewdowire, задается в виде числа в диапазоне [1..4294967295] <LSR_ID> – идентификатор LSR до которого строится pseudo-wire, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
12	Добавить описание для pseudo-wire (не обязательно).	**esr(config-l2vpn-pw)# description <LINE>**	<LINE> – описание. Задается в виде строки длинной [1..255] символов.
13	Задать pw-class для pseudo-wire.	**esr(config-l2vpn-pw)# pw-class <WORD>**	<WORD> – имя pw-class длинной [1..31] символов.
14	Задать адрес LSR до которого устанавливается pseudo-wire (не обязательно, если neighbor address совпадает с LSR_ID).	**esr(config-l2vpn-pw)# neighbor-address <ADDR>**	<ADDR> – IP-адрес маршрутизатора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
15	Включить pseudo-wire.	**esr(config-l2vpn-pw)# enable**	
16	В случае если топология создаваемого VPLS-домена требует установить более одного pseudo-wire, повторить шаги с 10 по 14.		
17	В случае если необходимо изменить параметры по умолчанию для targeted LDP-сессии, обратитесь к разделу Конфигурирование параметров сессии в протоколе targeted-LDP.		

14.5.4 Пример настройки L2VPN VPLS

Задача:

Настроить l2vpn таким образом, чтобы маршрутизаторы CE1, CE2, CE3 имели L2-связность через интерфейсы gi1/0/2.100 и gi1/0/4 (CE2).



Решение:

Предварительно необходимо:

- Включить поддержку Jumbo-фреймов с помощью команды "system jumbo-frames" (для вступления изменений в силу требуется перезагрузка устройства);
- Настроить IP-адреса на интерфейсах согласно схеме сети, приведенной на рисунке выше;
- Организовать обмен маршрутами между PE1, PE2 и PE3 при помощи IGP протокола (OSPF, IS-IS).

На маршрутизаторе PE1 создадим бридж-группу и включим ее:

```
PE1# configure
PE1(config)# bridge 10
PE1(config-bridge)# enable
PE1(config-bridge)# exit
```

Интерфейсе в сторону CE1 включим в созданную бридж-группу:

```
PE1(config)# interface gigabitethernet 1/0/4.100
PE1(config-subif)# bridge-group 10
PE1(config-subif)# exit
```

Выставим на интерфейсе в сторону PE2 значение MTU равным 9600, для того чтобы избежать ситуации с превышением MTU после инкапсуляции MPLS-заголовка, а также отключим межсетевой экран:

```
PE1#(config)# interface gigabitethernet 1/0/1
PE1(config-if-gi)# mtu 9600
PE1(config-if-gi)# ip firewall disable
PE1(config-if-gi)# exit
```

Разрешим прием пакетов с MPLS-заголовком на интерфейсе в сторону MPLS-сети (в данном примере интерфейс в сторону PE2):

```
PE1(config)# mpls
PE1(config-mpls)# forwarding interface gigabitethernet 1/0/1
```

Настроим протокол LDP и включим обнаружение соседей на интерфейсе в сторону PE2:

```
PE1(config-mpls)# ldp
PE1(config-ldp)# router-id 1.1.1.1
PE1(config-ldp)# address-family ipv4
PE1(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1
PE1(config-ldp-af-ipv4-if)# exit
PE1(config-ldp-af-ipv4)# transport-address 1.1.1.1
PE1(config-ldp-af-ipv4)# exit
PE1(config-ldp)# enable
PE1(config-ldp)# exit
```

Создадим pw-class, на основе которого в дальнейшем будет созданы виртуальные каналы (pw). Так как в данном примере на pw будут применяться параметры по умолчанию, достаточно будет указать имя класса:

```
PE1(config-mpls)# l2vpn
PE1(config-l2vpn)# pw-class for_vpls1
PE1(config-l2vpn-pw-class)# exit
```

Создадим новый l2vpn типа vpls и добавим pw до маршрутизаторов PE2 и PE3, идентификатор pw для удобства возьмем равным VID (в данном случае равным 100):

```
PE1(config-l2vpn)# vpls vpls1
PE1(config-l2vpn-vpls)# bridge-group 10
PE1(config-l2vpn-vpls)# pw 100 2.2.2.2
PE1(config-l2vpn-pw)# pw-class for_vpls1
PE1(config-l2vpn-pw)# enable
PE1(config-l2vpn-pw)# exit
PE1(config-l2vpn-vpls)# pw 100 3.3.3.3
PE1(config-l2vpn-pw)# pw-class for_vpls1
PE1(config-l2vpn-pw)# enable
PE1(config-l2vpn-pw)# exit
PE1(config-l2vpn-vpls)# enable
PE1(config-l2vpn-vpls)# end
```

Применим созданную конфигурацию:

```
PE1# commit
PE1# confirm
```

Проведем настройку маршрутизатора PE2 и PE3 по аналогии с PE1:

```
PE2# configure
PE2(config)# bridge 10
PE2(config-bridge)# enable
PE2(config-bridge)# exit
PE2(config)# interface gigabitethernet 1/0/4.100
PE2(config-subif)# bridge-group 10
PE2(config-subif)# exit
PE2(config)# interface gigabitethernet 1/0/2
PE2(config-if-gi)# mtu 9600
PE2(config-if-gi)# ip firewall disable
PE2(config-if-gi)# exit
PE2(config)# mpls
PE2(config-mpls)# forwarding interface gigabitethernet 1/0/1
PE2(config-mpls)# forwarding interface gigabitethernet 1/0/2
PE2(config-mpls)# ldp
PE2(config-ldp)# enable
PE2(config-ldp)# router-id 2.2.2.2
PE2(config-ldp)# address-family ipv4
PE2(config-ldp-af-ipv4)# transport-address 2.2.2.2
PE2(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1
PE2(config-ldp-af-ipv4-if)# exit
PE2(config-ldp-af-ipv4)# interface gigabitethernet 1/0/2
PE2(config-ldp-af-ipv4-if)# exit
PE2(config-ldp-af-ipv4)# exit
PE2(config-ldp)# exit
PE2(config-mpls)# l2vpn
PE2(config-l2vpn)# pw-class for_vpls1
PE2(config-l2vpn-pw-class)# exit
PE2(config-l2vpn)# vpls vpls1
PE2(config-l2vpn-vpls)# enable
PE2(config-l2vpn-vpls)# bridge-group 10
PE2(config-l2vpn-vpls)# pw 100 1.1.1.1
PE2(config-l2vpn-pw)# pw-class for_vpls1
PE2(config-l2vpn-pw)# enable
PE2(config-l2vpn-pw)# exit
PE2(config-l2vpn-vpls)# pw 100 3.3.3.3
PE2(config-l2vpn-pw)# pw-class for_vpls1
PE2(config-l2vpn-pw)# enable
PE2(config-l2vpn-pw)# end
PE2# commit
PE2# confirm
PE3(config)# bridge 10
PE3(config-bridge)# enable
PE3(config-bridge)# exit
PE3(config)# interface gigabitethernet 1/0/4.100
PE3(config-subif)# bridge-group 10
PE3(config-subif)# exit
PE3(config)# interface gigabitethernet 1/0/1
PE3(config-if-gi)# mtu 9600
PE3(config-if-gi)# ip firewall disable
PE3(config-if-gi)# exit
PE3(config)# mpls
PE3(config-mpls)# forwarding interface gigabitethernet 1/0/1
PE3(config-mpls)# exit
PE3(config)# mpls
PE3(config-mpls)# ldp
```

```
PE3(config-ldp)# enable
PE3(config-ldp)# router-id 3.3.3.3
PE3(config-ldp)# address-family ipv4
PE3(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1
PE3(config-ldp-af-ipv4-if)# exit
PE3(config-ldp-af-ipv4)# transport-address 3.3.3.3
PE3(config-ldp-af-ipv4)# exit
PE3(config-ldp)# exit
PE3(config-mpls)# l2vpn
PE3(config-l2vpn)# pw-class for_vpls
PE3(config-l2vpn-pw-class)# exit
PE3(config-l2vpn)# vpls vpls1
PE3(config-l2vpn-vpls)# enable
PE3(config-l2vpn-vpls)# bridge-group 10
PE3(config-l2vpn-vpls)# pw 100 2.2.2.2
PE3(config-l2vpn-pw)# pw-class for_vpls
PE3(config-l2vpn-pw)# enable
PE3(config-l2vpn-pw)# exit
PE3(config-l2vpn-vpls)# pw 100 1.1.1.1
PE3(config-l2vpn-pw)# pw-class for_vpls
PE3(config-l2vpn-pw)# enable
PE3(config-l2vpn-pw)# end
PE3# commit
PE3# confirm
```

Убедимся в установлении соседства по протоколу LDP и выведем информацию по статусу виртуального канала (pseudowire) между PE1, PE2 и PE3:

```
PE3# show mpls ldp neighbor
Peer LDP ID: 1.1.1.1; Local LDP ID 3.3.3.3
    State: Operational
    TCP connection: 1.1.1.1:646 - 3.3.3.3:45979
    Messages sent/received: 22/22
    Uptime: 00:13:16
    LDP discovery sources:
        3.3.3.3 -> 1.1.1.1
Peer LDP ID: 2.2.2.2; Local LDP ID 3.3.3.3
    State: Operational
    TCP connection: 2.2.2.2:646 - 3.3.3.3:59627
    Messages sent/received: 22/22
    Uptime: 00:13:20
    LDP discovery sources:
        3.3.3.3 -> 2.2.2.2
        gigabitethernet 1/0/1
```

```
PE3# show mpls l2vpn pseudowire
Neighbor                                  PW ID    Type          Status
----------------------------------------- ----------      ----------       ------
1.1.1.1                                     100        Ethernet     Up
2.2.2.2                                     100        Ethernet     Up
```

Соседство по протоколу LDP установлено, pseudowire перешел в статус 'UP'. Настройка l2vpn завершена.

14.6 Настройка сервиса L2VPN Kompella mode

В отличии от Martini mode, где вся работа ложится на LDP, в данном режиме LDP отводится только работа с транспортными метками. Автообнаружение и построение псевдо-провода возложено на протокол BGP.

14.6.1 Алгоритм настройки L2VPN VPLS

Шаг	Описание	Команда	Ключи
1	Настроить протокол LDP (см. раздел Конфигурирование протокола LDP).		
2	Создать сетевой мост в системе без указания IP-адреса (см. раздел Настройка Bridge).		
3	Создать VPLS-домен в системе и осуществить переход в режим настройки параметров VPLS-домена.	**esr(config-l2vpn)# vpls <NAME>**	<NAME> – имя p2p-сервиса, задается строкой до 31 символа.
4	Включить VPLS-туннель.	**esr(config-l2vpn-vpls)# enable**	
5	Добавить бридж-домен.	**esr(config-l2vpn-vpls)# bridge-group <ID>**	<ID> – идентификатор бридж-домена, задается в виде числа в диапазоне [1..250].
6	Перейти в контекст настройки autodiscovery bgp.	**esr(config-l2vpn-vpls)# autodiscovery bgp**	
7	Указать route distinguisher для данного экземпляра VPLS.	**esr(config-bgp)# rd <RD>**	<RD> – значение Route distinguisher, задается в одном из следующем виде: • <ASN>:<nn> – где <ASN> – принимает значение [1..65535], nn – принимает значение [1..65535]; • <ADDR>:<nn> – где <ADDR> имеет вид – AAA.BBB.CCC.DDD/EE и AAA-DDD принимают значения [0..255], а nn – принимает значение [1..65535]; • <4ASN>:<nn> – где <4ASN> – принимает значение [1..4294967295], nn – принимает значение [1..65535];

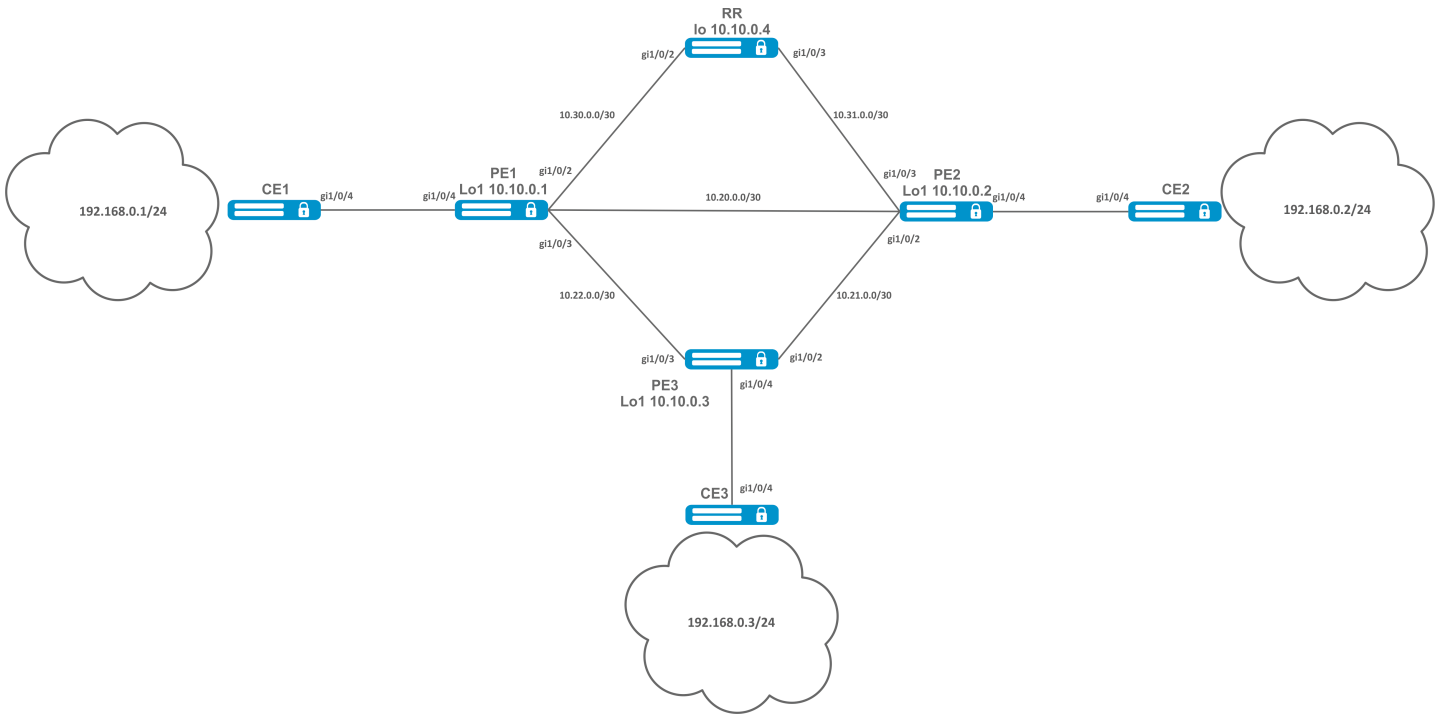
Шаг	Описание	Команда	Ключи
8	Указать route target import для данного экземпляра VPLS.	**esr(config-bgp)# route-target import <RT>**	<RT> – значение route-target, задается в одном из следующих видов: • <ASN>:<nn> – где <ASN> – принимает значение [1..65535], nn – принимает значение [1..65535]; • <ADDR>:<nn> – где <ADDR> имеет вид – AAA.BBB.CCC.DDD/EE и AAA-DDD принимают значения [0..255], а nn – принимает значение [1..65535]; • <4BASN>:<nn> – где <4ASN> – принимает значение [1..4294967295], nn – принимает значение [1..65535];
9	Указать route target export для данного экземпляра VPLS.	**esr(config-bgp)# route-target export <RT>**	<RT> – значение route-target, задается в одном из следующих видов: • <ASN>:<nn> – где <ASN> – принимает значение [1..65535], nn – принимает значение [1..65535]; • <ADDR>:<nn> – где <ADDR> имеет вид – AAA.BBB.CCC.DDD/EE и AAA-DDD принимают значения [0..255], а nn – принимает значение [1..65535]; • <4BASN>:<nn> – где <4ASN> – принимает значение [1..4294967295], nn – принимает значение [1..65535];
10	Указать ve id.	**esr(config-bgp)# ve id <ID>**	<ID> – идентификатор экземпляра VPLS, задается в виде числа в диапазоне [1..16384].
11	Указать vpn id.	**esr (config-bgp)# vpn id <ID>**	<ID> – идентификатор VPN, задается в виде числа в диапазоне [1..4294967295].
12	Указать ve range (не обязательно).	**esr (config-bgp)# ve range <RANGE>**	<RANGE> – диапазон идентификаторов пограничных устройств VPLS [8..100].

Шаг	Описание	Команда	Ключи
13	Указать mtu (не обязательно).	**esr (config-bgp)# mtu <VALUE>**	<VALUE> – значение MTU [552..10000].
14	Включить игнорирование типа инкапсуляции (не обязательно).	**esr(config-bgp)# ignore encapsulation-mismatch**	
15	Включить игнорирование значений MTU (не обязательно).	**esr(config-bgp)# ignore mtu-mismatch**	
16	В контексте настройки address-family l2vpn vpls протокола BGP включить передачу расширенных атрибутов.	**esr(config-bgp-neighbor-af)# send-community extended**	

14.6.2 Пример настройки L2VPN VPLS

Задача:

Настроить L2VPN-сервис: все CE-устройства должны работать в рамках одного широковещательного домена.



Решение:

Предварительно необходимо:

- Включить поддержку Jumbo-фреймов с помощью команды "system jumbo-frames" (для вступления изменений в силу требуется перезагрузка устройства);
- Настроить IP-адреса на интерфейсах согласно схеме сети, приведенной на рисунке выше;
- Организовать обмен маршрутами между PE1, PE2, PE3 и RR при помощи IGP-протокола (OSPF, IS-IS).

Настроим маршрутизатор RR:

```
hostname RR

system jumbo-frames

router ospf 1
area 0.0.0.0
enable
exit
enable
exit

interface gigabitethernet 1/0/2
mtu 9500
ip firewall disable
ip address 10.30.0.2/30
ip ospf instance 1
ip ospf
exit
interface gigabitethernet 1/0/3
mtu 9500
ip firewall disable
ip address 10.31.0.2/30
ip ospf instance 1
ip ospf
exit
interface loopback 1
ip address 10.10.0.4/32
ip ospf instance 1
ip ospf
exit
mpls
ldp
router-id 10.10.0.4
address-family ipv4
interface gigabitethernet 1/0/2
exit
interface gigabitethernet 1/0/3
exit
exit
enable
exit
forwarding interface gigabitethernet 1/0/2
forwarding interface gigabitethernet 1/0/3
exit
```

Настроим BGP Route Reflector для address family l2vpn:

```
RR(config)# router bgp 65500
RR(config-bgp)#   router-id 10.10.0.4
RR(config-bgp)#   neighbor 10.10.0.1
RR(config-bgp-neighbor)#     remote-as 65500
RR(config-bgp-neighbor)#     route-reflector-client
RR(config-bgp-neighbor)#     update-source 10.10.0.4
RR(config-bgp-neighbor)#     address-family l2vpn vpls
RR(config-bgp-neighbor-af)#       send-community extended
RR(config-bgp-neighbor-af)#       enable
RR(config-bgp-neighbor-af)#     exit
RR(config-bgp-neighbor)#     enable
RR(config-bgp-neighbor)#   exit
RR(config-bgp)#   neighbor 10.10.0.2
RR(config-bgp-neighbor)#     remote-as 65500
RR(config-bgp-neighbor)#     route-reflector-client
RR(config-bgp-neighbor)#     update-source 10.10.0.4
RR(config-bgp-neighbor)#     address-family l2vpn vpls
RR(config-bgp-neighbor-af)#       send-community extended
RR(config-bgp-neighbor-af)#       enable
RR(config-bgp-neighbor-af)#     exit
RR(config-bgp-neighbor)#     enable
RR(config-bgp-neighbor)#   exit
RR(config-bgp)#   neighbor 10.10.0.3
RR(config-bgp-neighbor)#     remote-as 65500
RR(config-bgp-neighbor)#     route-reflector-client
RR(config-bgp-neighbor)#     update-source 10.10.0.4
RR(config-bgp-neighbor)#     address-family l2vpn vpls
RR(config-bgp-neighbor-af)#       send-community extended
RR(config-bgp-neighbor-af)#       enable
RR(config-bgp-neighbor-af)#     exit
RR(config-bgp-neighbor)#     enable
RR(config-bgp-neighbor)#   exit
RR(config-bgp)#   enable
```

Настройка протокола BGP на PE-маршрутизаторах:

Предварительная конфигурация

```
hostname PE1

system jumbo-frames

router ospf 1
area 0.0.0.0
enable
exit
enable
exit

interface gigabitethernet 1/0/1
mtu 9500
```

Предварительная конфигурация

```
ip firewall disable
ip address 10.20.0.1/30
ip ospf instance 1
ip ospfexit
interface gigabitethernet 1/0/2
mtu 9500
ip firewall disable
ip address 10.30.0.1/30
ip ospf instance 1
ip ospf
exitinterface gigabitethernet 1/0/3
mtu 9500
ip firewall disable
ip address 10.22.0.1/30
ip ospf instance 1
ip ospf
exit
interface loopback 1
ip address 10.10.0.1/32
ip ospf instance 1
ip ospf
exit
mpls
ldp
router-id 10.10.0.1
address-family ipv4
interface gigabitethernet 1/0/1
exit
interface gigabitethernet 1/0/2
exit
interface gigabitethernet 1/0/3
exit

exit

enable

exit
forwarding interface gigabitethernet 1/0/1
forwarding interface gigabitethernet 1/0/2
forwarding interface gigabitethernet 1/0/3
exit
```

Настройка протокола BGP:

```
PE1(config)# router bgp 65500
PE1(config-bgp)#   neighbor 10.10.0.4
PE2(config-bgp)#   router-id 10.10.0.1
PE1(config-bgp-neighbor)#     remote-as 65500
PE1(config-bgp-neighbor)#     update-source 10.10.0.1
PE1(config-bgp-neighbor)#     address-family l2vpn vpls
PE1(config-bgp-neighbor-af)#       send-community extended
PE1(config-bgp-neighbor-af)#       enable
PE1(config-bgp-neighbor-af)#     exit
PE1(config-bgp-neighbor)#     enable
PE1(config-bgp-neighbor)#   exit
PE1(config-bgp)#   enable
PE1(config-bgp)# exit
```

Проверим, что BGP-сессия успешно установлена с RR:

```
PE1# show bgp neighbors
BGP neighbor is 10.10.0.4
BGP state: Established
Neighbor address: 10.10.0.4
Neighbor AS: 65500
Neighbor ID: 10.10.0.4
Neighbor caps: refresh enhanced-refresh restart-aware AS4
Session: internal multihop AS4
Source address: 10.10.0.1
Weight: 0
Hold timer: 110/180
Keepalive timer: 21/60
Uptime: 7375 s
```

Настройка BGP на PE2:

Предварительная конфигурация

```
hostname PE2

system jumbo-frames

router ospf 1
area 0.0.0.0
enable
exit
enable
exit
```

Предварительная конфигурация

```
interface gigabitethernet 1/0/1
mtu 9500
ip firewall disable
ip address 10.20.0.2/30
ip ospf instance 1
ip ospf
exit
interface gigabitethernet 1/0/2
mtu 9500
ip firewall disable
ip address 10.21.0.1/30
ip ospf instance 1
ip ospf
exit
interface gigabitethernet 1/0/3
mtu 9500
ip firewall disable
ip address 10.31.0.1/30
ip ospf instance 1
ip ospf
exit
interface loopback 1
ip address 10.10.0.2/32
ip ospf instance 1
ip ospf
exit
mpls
ldp
router-id 10.10.0.2
address-family ipv4
interface gigabitethernet 1/0/1
exit
interface gigabitethernet 1/0/2
exit
interface gigabitethernet 1/0/3
exit
exit

enable

exit
forwarding interface gigabitethernet 1/0/1
forwarding interface gigabitethernet 1/0/2
forwarding interface gigabitethernet 1/0/3
exit
```

```
PE2(config)# router bgp 65500
PE2(config-bgp)#   router-id 10.10.0.2
PE2(config-bgp)#   neighbor 10.10.0.4
PE2(config-bgp-neighbor)#     remote-as 65500
PE2(config-bgp-neighbor)#     update-source 10.10.0.2
PE2(config-bgp-neighbor)#     address-family l2vpn vpls
PE2(config-bgp-neighbor-af)#       send-community extended
PE2(config-bgp-neighbor-af)#       enable
PE2(config-bgp-neighbor-af)#     exit
PE2(config-bgp-neighbor)#     enable
PE2(config-bgp-neighbor)#   exit
PE2(config-bgp)#   enable
PE2(config-bgp)# exit
```

Убедимся, что сессия с RR поднялась успешно:

```
PE2# show bgp neighbors
BGP neighbor is 10.10.0.4
BGP state: Established
Neighbor address: 10.10.0.4
Neighbor AS: 65500
Neighbor ID: 10.10.0.4
Neighbor caps: refresh enhanced-refresh restart-aware AS4
Session: internal multihop AS4
Source address: 10.10.0.2
Weight: 0
Hold timer: 113/180
Keepalive timer: 56/60
Uptime: 47 s
```

Настройка BGP на PE3:

Предварительная конфигурация

```
hostname PE3

system jumbo-frames

router ospf 1
area 0.0.0.0
enable
exit
enable
exit

interface gigabitethernet 1/0/2
mtu 9500
ip firewall disable
ip address 10.21.0.2/30
ip ospf instance 1
ip ospf
exit
interface gigabitethernet 1/0/3
mtu 9500
ip firewall disable
ip address 10.22.0.2/30
ip ospf instance 1
ip ospf
exit
interface loopback 1
ip address 10.10.0.3/24
ip ospf instance 1
ip ospf
exit
mpls
ldp
router-id 10.10.0.3
address-family ipv4
interface gigabitethernet 1/0/2
exit
interface gigabitethernet 1/0/3
exit
exit
enable
exit
forwarding interface gigabitethernet 1/0/2
forwarding interface gigabitethernet 1/0/3
exit
```

```
PE3(config)# router bgp 65500
PE3(config-bgp)#   router-id 10.10.0.3
PE3(config-bgp)#   neighbor 10.10.0.4
PE3(config-bgp-neighbor)#     remote-as 65500
PE3(config-bgp-neighbor)#     update-source 10.10.0.3
PE3(config-bgp-neighbor)#     address-family l2vpn vpls
PE3(config-bgp-neighbor-af)#       send-community extended
PE3(config-bgp-neighbor-af)#       enable
PE3(config-bgp-neighbor-af)#     exit
PE3(config-bgp-neighbor)#     enable
PE3(config-bgp-neighbor)#   exit
PE3(config-bgp)#   enable
PE3(config-bgp)# exit
```

Проверим, что сессия BGP установлена успешно:

```
PE3# show bgp neighbors
BGP neighbor is 10.10.0.4
BGP state: Established
Neighbor address: 10.10.0.4
Neighbor AS: 65500
Neighbor ID: 10.10.0.4
Neighbor caps: refresh enhanced-refresh restart-aware AS4
Session: internal multihop AS4
Source address: 10.10.0.3
Weight: 0
Hold timer: 141/180
Keepalive timer: 27/60
Uptime: 77 s
```

Следующим этапом на каждом PE-маршрутизаторе создадим бридж-домен и включим в него интерфейс (Attachment circuit, AC), смотрящий в сторону CE:

PE1:

```
PE1(config)# bridge 1
PE1(config-bridge)# enable
PE1(config-bridge)# exit
PE1(config)# interface gigabitethernet 1/0/4
PE1(config-if-gi)# mode switchport
PE1(config-if-gi)# bridge-group 1
```

Проверим, что интерфейс включен в бридж-домен:

```
PE1# show interfaces bridge
Bridges      Interfaces
----------   ------------------------------------------------------------
bridge 1     gi1/0/4

PE1# sh interfaces status bridge 1
Interface 'bridge 1' status information:
 Description:          --
 Operational state:    Up
 Administrative state: Up
 Supports broadcast:   Yes
 Supports multicast:   Yes
 MTU:                  1500
 MAC address:          a8:f9:4b:ac:4d:15
 Last change:          4 minutes and 22 seconds
 Mode:                 Routerport
```

PE2:

```
PE2(config)# bridge 1
PE2(config-bridge)# enable
PE2(config-bridge)# exit
PE2(config)# interface gigabitethernet 1/0/4
PE2(config-if-gi)# mode switchport
PE2(config-if-gi)# bridge-group 1
```

```
PE2# show interfaces bridge 1
Bridges      Interfaces
----------   ------------------------------------------------------------
bridge 1     gi1/0/4

PE2# sh interfaces status bridge 1
Interface 'bridge 1' status information:
 Description:          --
 Operational state:    Up
 Administrative state: Up
 Supports broadcast:   Yes
 Supports multicast:   Yes
 MTU:                  1500
 MAC address:          a8:f9:4b:ad:f2:45
 Last change:          10 seconds
 Mode:                 routerport
```

PE3:

```
PE3(config)# bridge 1
PE3(config-bridge)# enable
PE3(config-bridge)# exit
PE3(config)# interface gigabitethernet 1/0/4
PE3(config-if-gi)# mode switchport
PE3(config-if-gi)# bridge-group 1
```

```
PE3# show interfaces bridge
Bridges      Interfaces
----------   ------------------------------------------------------------
bridge 1     gi1/0/4
PE3# sh interfaces status bridge
Interface            Admin   Link    MTU      MAC address          Last change
Mode
                     state   state
------------------   -----   -----   ------   ------------------   -------------------------
----------
bridge 1             Up      Up      1500     a8:f9:4b:ac:df:f0    1 minute and 21 seconds
Routerport

PE3# sh interfaces status bridge 1
Interface 'bridge 1' status information:
 Description:          --
 Operational state:    Up
 Administrative state: Up
 Supports broadcast:   Yes
 Supports multicast:   Yes
 MTU:                  1500
 MAC address:          a8:f9:4b:ac:df:f0
 Last change:          1 minute and 24 seconds
 Mode:                 Routerport
```

Далее выполним настройку VPLS:

PE1:

Переходим в контекст настройки L2VPN и включим в него заранее созданный бридж-домен.

```
PE1(config)# mpls
PE1(config-mpls)# l2vpn
PE1(config-l2vpn)# vpls l2vpn
PE1(config-l2vpn-vpls)# bridge-group 1
```

Укажем RD, RT, VE-ID, VPN ID согласно схеме сети и активируем сервис:

В некоторых случаях можно отказаться от ввода таких параметров, как RD и RT: если указать только VPN ID, то они будут сформированы следующим образом: <номер AS> : <vpn-id>.
Например, есть номер автономной системы AS 65550, vpn-id указан 10, тогда сгенерируются следующие параметры:
RD - 65550: 10.
RT import/export - 65550:10.

```
PE1(config-l2vpn-vpls)# autodiscovery bgp
PE1(config-bgp)# rd 65500:100
PE1(config-bgp)# route-target import 65500:100
PE1(config-bgp)# route-target export 65500:100
PE1(config-bgp)# ve id 1
PE1(config-bgp)# vpn id 1
PE1(config-bgp)# exit
PE1(config-l2vpn-vpls)# enable
```

После активации сервиса проверим, что в таблице l2vpn появилась маршрутная информация и она анонсируется на RR:

```
PE1# show bgp l2vpn vpls all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes Route Distinguisher   VID   VBO   VBS   Next hop        Metric     LocPrf     Weight Path
----- --------------------- ----- ----- ----- --------------- ---------- ---------- ------
-------------------
*>    65500:100             1     1     10    --              --         --         --


PE1# show bgp l2vpn vpls all neighbor 10.10.0.4 advertise-routes
Origin codes: i - IGP, e - EGP, ? - incomplete

Route Distinguisher   VID   VBO   VBS   Next hop        Metric     LocPrf     Path
--------------------- ----- ----- ----- --------------- ---------- ----------
----------------------
65500:100             1     1     10    10.10.0.1       --         100        i


* Подробный вывод анонсированного маршрута *

PE1# show bgp l2vpn vpls all neighbor 10.10.0.4 advertise-routes  ve-id 1 block
-offset 1
BGP routing table entry for 65500:100 VE ID 1 VE Block Offset 1
    VE Block Size:      10
    Label Base:         86
    Next hop:           10.10.0.1
    AS path:            --
    Origin:             IGP
    Local preference:   100
    Extended Community: RT:65500:100
    Layer2-info:        encaps (VPLS), control flags(0x00), MTU (1500)
```

Переходим к настройке PE2:

```
PE2(config-mpls)# l2vpn
PE2(config-l2vpn)# vpls l2vpn
PE2(config-l2vpn-vpls)# bridge-group 1
PE2(config-l2vpn-vpls)# autodiscovery bgp
PE2(config-bgp)# rd 65500:100
```

```
PE2(config-bgp)# route-target export 65500:100
PE2(config-bgp)# route-target import  65500:100
PE2(config-bgp)# vpn id 2
PE2(config-bgp)# ve id 2
PE2(config-bgp)# exit
PE2(config-l2vpn-vpls)# enable
```

Проверяем, что PE2 анонсирует маршрутную информацию на RR:

```
PE2# show bgp l2vpn vpls all  neighbor 10.10.0.4 advertise-routes
Origin codes: i - IGP, e - EGP, ? - incomplete

Route Distinguisher   VID   VBO   VBS   Next hop        Metric     LocPrf     Path
--------------------- ----- ----- ----- --------------- ---------- ----------
----------------------
65500:100             2     1     10    10.10.0.2       --         100        i
```

В таблице l2vpn видны как и свои маршруты, так и от PE1:

```
PE2# show bgp l2vpn vpls all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes Route Distinguisher   VID   VBO   VBS   Next hop        Metric     LocPrf     Weight Path
----- --------------------- ----- ----- ----- --------------- ---------- ---------- ------
-------------------
*>    65500:100             2     1     10    --              --         --         --
*>i   65500:100             1     1     10    10.10.0.1       --         100        0      i
```

Просмотреть вычисленные сервисные метки можно следующим образом:

1)

```
PE2# show mpls l2vpn bindings
Neighbor: 10.10.0.1, PW ID: 2, VE ID: 1
Local label: 45
Encasulation Type: VPLS
Control flags: 0x00
MTU: 1500
Remote label: 87
Encasulation Type: VPLS
Control flags: 0x00
MTU: 1500
```

2)

```
PE2# show mpls forwarding-table
Local       Outgoing          Prefix              Outgoing                Next Hop
label       label             or tunnel ID        Interface
--------    --------          ------------------  -----------------
-----------------------------------

45          87                PW ID 2                   --                10.10.0.1
```

Проверим состояние сервиса:

```
PE2# show mpls l2vpn vpls l2vpn
VPLS: l2vpn
    bridge 1:
        MTU:    1500
        Status: Up
    ACs:
      gigabitethernet 1/0/4:
        MTU:    1500
        Status: Up
    PWs:
      PW ID 2, Neighbor 10.10.0.1:
        MTU:         1500
        Last change: 00:21:33
        Status:      Up
```

Переходим к настройке PE3:

```
PE3#    config
PE3(config)# mpls
PE3(config-mpls)# l2vpn
PE3(config-l2vpn)# vpls l2vpn
PE3(config-l2vpn-vpls)# bridge-group 1
PE3(config-l2vpn-vpls)# autodiscovery bgp
PE3(config-bgp)# rd 65500:100
PE3(config-bgp)# route-target export 65500:100
PE3(config-bgp)# route-target import  65500:100
PE3(config-bgp)# ve id 3
PE3(config-bgp)# vpn id 3
PE3(config-bgp)# exit
PE3(config-l2vpn-vpls)# enable
```

Проверяем маршрутную информацию на PE3:

```
PE3# show bgp l2vpn vpls all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes Route Distinguisher   VID   VBO   VBS   Next hop        Metric     LocPrf     Weight Path
----- --------------------- ----- ----- ----- --------------- ---------- ---------- ------
-------------------
*>    65500:100             3     1     10    --              --         --         --
*>i   65500:100             2     1     10    10.10.0.2       --         100        0      i
*>i   65500:100             1     1     10    10.10.0.1       --         100        0      i
```

Убедимся, что PE3 анонсирует маршрутную информацию на RR:

```
PE3# show bgp l2vpn vpls all neighbor 10.10.0.4 advertise-routes
Origin codes: i - IGP, e - EGP, ? - incomplete

Route Distinguisher   VID   VBO   VBS   Next hop        Metric     LocPrf     Path
--------------------- ----- ----- ----- --------------- ---------- ----------
----------------------
65500:100             3     1     10    10.10.0.3       --         100        i
```

Проверим, что псевдо-провод построен до обеих PE и находится в статусе "UP":

```
PE3# show mpls l2vpn vpls l2vpn
VPLS: l2vpn
    bridge 1:
        MTU:    1500
        Status: Up
    ACs:
      gigabitethernet 1/0/4:
        MTU:    1500
        Status: Up
    PWs:
      PW ID 3, Neighbor 10.10.0.2:
        MTU:         1500
        Last change: 00:06:08
        Status:      Up
      PW ID 3, Neighbor 10.10.0.1:
        MTU:         1500
        Last change: 00:06:08
        Status:      Up
```

Проверим сетевую доступность клиентских устройств (CE):

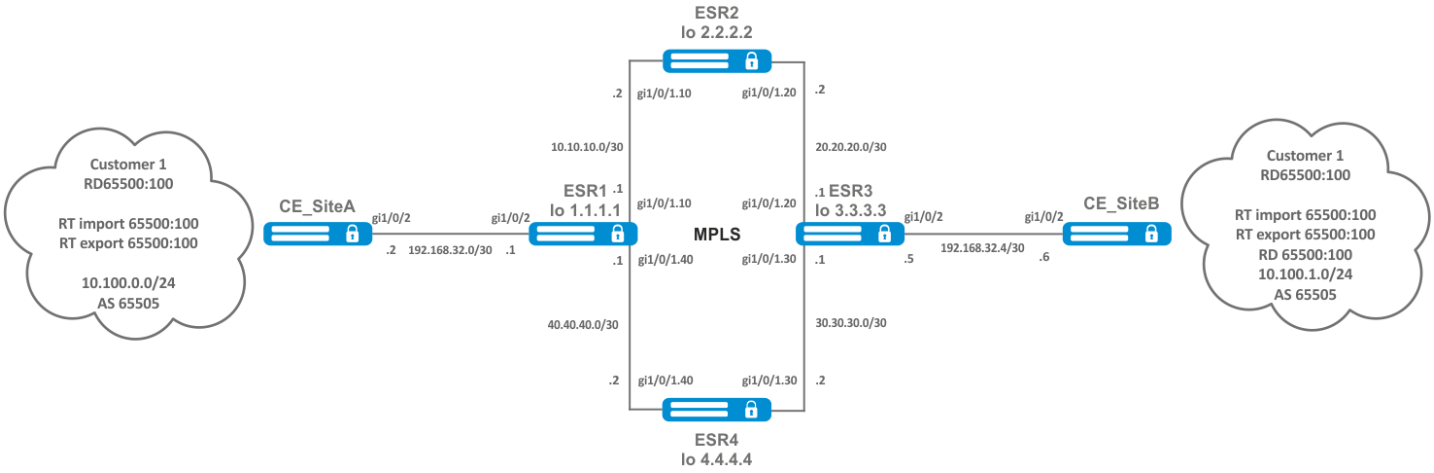
```
CE3# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
!!!!!
--- 192.168.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 0.173/0.208/0.290/0.045 ms
CE3# ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
!!!!!
--- 192.168.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 0.158/0.204/0.255/0.032 ms

PE3# sh mac address-table bridge 1
VID     MAC Address          Interface                       Type
-----   ------------------   -----------------------------   -------
--      a8:f9:4b:aa:11:08    gigabitethernet 1/0/4           Dynamic
--      a8:f9:4b:aa:11:06    dypseudowire 3_10.10.0.1        Dynamic
--      a8:f9:4b:aa:11:07    dypseudowire 3_10.10.0.2        Dynamic
3 valid mac entries
```

Настройка L2VPN-сервиса завершена.

14.7 Настройка сервиса L3VPN

Сервис L3VPN позволяет объединить распределенные клиентские IP-сети и обеспечить передачу трафика между ними с рамках единой VRF.

В текущей реализации протокола MP-BGP поддержана передача только VPN-IPv4 маршрутов (AFI = 1, SAFI = 128).



14.7.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Настроить адресацию и один из протоколов IGP на всех P и PE-маршрутизаторах.		
2	Настроить распространение транспортных меток по протоколу LDP.		
3	Создать VRF.	**esr(config)# ip vrf <VRF>**	<VRF> – имя экземпляра VRF, задается строкой до 31 символа.
4	Указать route distinguisher для данного VRF.	**esr(config-vrf)# rd <RD>**	<RD> – значение Route distinguisher, задается в одном из следующем виде: • <ASN>:<nn> – где <ASN> – принимает значение [1..65535], nn – принимает значение [1..65535]; • <ADDR>:<nn> – где <ADDR> имеет вид – AAA.BBB.CCC.DDD/EE и AAA-DDD принимают значения [0..255], а nn – принимает значение [1..65535]; • <4ASN>:<nn> – где <4ASN> – принимает значение [1..4294967295], nn – принимает значение [1..65535];

Шаг	Описание	Команда	Ключи
5	Указать route target import для данного VRF.	**esr(config-vrf)# route-target import <RT>**	<RT> – значение route-target, задается в одном из следующих видов: • <ASN>:<nn> – где <ASN> - принимает значение [1..65535], nn – принимает значение [1..65535]; • <ADDR>:<nn> – где <ADDR> имеет вид – AAA.BBB.CCC.DDD/EE и AAA-DDD принимают значения [0..255], а nn – принимает значение [1..65535]; • <4BASN>:<nn> – где <4ASN> – принимает значение [1..4294967295], nn – принимает значение [1..65535];
6	Указать route target export для данного VRF.	**esr(config-vrf)# route-target export <RT>**	<RT> – значение route-target, задается в одном из следующем виде: • <ASN>:<nn> – где <ASN> – принимает значение [1..65535], nn – принимает значение [1..65535]; • <ADDR>:<nn> – где <ADDR> имеет вид – AAA.BBB.CCC.DDD/EE и AAA-DDD принимают значения [0..255], а nn – принимает значение [1..65535]; • <4BASN>:<nn> – где <4ASN> – принимает значение [1..4294967295], nn – принимает значение [1..65535];

Шаг	Описание	Команда	Ключи

7	Указать разрешенное количество маршрутов для данного VRF.	**esr(config-vrf)# ip protocols <PROTOCOLS> max-routes <VALUE>**	<PROTOCOL> – вид протокола, принимает значения: rip (только в глобальном режиме), ospf, isis, bgp;
			
			<VALUE> – количество маршрутов в маршрутной таблице, принимает значения в диапазоне:
			
			• BGP
			  • ESR-1000/1200/1500/1511/3100/3200/1700 – [1..5000000];
			  • ESR-20/21/30/100/200 – [1..2500000],
			  • ESR-10/12V/12VF/14VF/15 – [1.. 1000000].
			• OSPF и IS-IS
			  • ESR-1000/1200/1500/1511/1700/3100/3200 – [1..500000];
			  • ESR-20/21/30/100/200 – [1..300000];
			  • ESR-10/12V/12VF/14VF/15 – [1..30000].

8	В рамках настройки address-family VPNv4 протокола BGP включить передачу расширенных атрибутов.	**esr(config-bgp-neighbor-af)# send-community extended**	

14.7.2 Пример настройки

Задача:

Настроить L3VPN на базе технологии MPLS между ESR1 и ESR3. Конечным результатом настройки является появление связности между узлами, подключенными к VRF на различных маршрутизаторах сети (то есть объединение VRF на разных маршрутизаторах через MPLS-транспорт). При этом должна быть обеспечена передача сервисных MPLS-меток для сервиса L3VPN посредством MP-BGP и передача транспортных меток для достижения nexthop-адресов полученных BGP-маршрутов.

Решение:

Настройка адресации и включение IGP на P/PE-маршрутизаторах

ESR1

```
ESR1(config)# router ospf log-adjacency-changes
ESR1(config)# router ospf 1
ESR1(config-ospf)# router-id 1.1.1.1
ESR1(config-ospf)# area 0.0.0.0
ESR1(config-ospf-area)# enable
ESR1(config-ospf-area)# exit
ESR1(config-ospf)# enable
ESR1(config-ospf)# exit
ESR1(config)#
ESR1(config)# interface loopback 1
ESR1(config-loopback)# ip address 1.1.1.1/32
ESR1(config-loopback)# ip ospf instance 1
ESR1(config-loopback)# ip ospf
ESR1(config-loopback)# exit
ESR1(config)#
ESR1(config)# interface gigabitethernet 1/0/1.10
ESR1(config-subif)# ip firewall disable
ESR1(config-subif)# ip address 10.10.10.1/30
ESR1(config-subif)# ip ospf instance 1
ESR1(config-subif)# ip ospf
ESR1(config-subif)# exit
ESR1(config)#
ESR1(config)# interface gigabitethernet 1/0/1.40
ESR1(config-subif)# ip firewall disable
ESR1(config-subif)# ip address 40.40.40.1/30
ESR1(config-subif)# ip ospf instance 1
ESR1(config-subif)# ip ospf
ESR1(config-subif)# exit
ESR1(config)#
ESR1(config)# system jumbo-frames
ESR1(config)# do commit
ESR1(config)# do confirm
```

ESR2

```
ESR2(config)# router ospf log-adjacency-changes
ESR2(config)# router ospf 1
ESR2(config-ospf)# router-id 2.2.2.2
ESR2(config-ospf)# area 0.0.0.0
ESR2(config-ospf-area)# enable
ESR2(config-ospf-area)# exit
ESR2(config-ospf)# enable
ESR2(config-ospf)# exit
ESR2(config)#
ESR2(config)# interface loopback 1
ESR2(config-loopback)# ip address 2.2.2.2/32
ESR2(config-loopback)# ip ospf instance 1
ESR2(config-loopback)# ip ospf
ESR2(config-loopback)# exit
ESR2(config)#
ESR2(config)# interface gigabitethernet 1/0/1.10
ESR2(config-subif)# ip firewall disable
ESR2(config-subif)# ip address 10.10.10.2/30
ESR2(config-subif)# ip ospf instance 1
ESR2(config-subif)# ip ospf
ESR2(config-subif)# exit
ESR2(config)#
ESR2(config)# interface gigabitethernet 1/0/1.20
ESR2(config-subif)# ip firewall disable
ESR2(config-subif)# ip address 20.20.20.2/30
ESR2(config-subif)# ip ospf instance 1
ESR2(config-subif)# ip ospf
ESR2(config-subif)# exit
ESR2(config)#
ESR2(config)# system jumbo-frames
ESR2(config)# do commit
ESR2(config)# do confirm
```

ESR3

```
ESR3(config)# router ospf log-adjacency-changes
ESR3(config)# router ospf 1
ESR3(config-ospf)# router-id 3.3.3.3
ESR3(config-ospf)# area 0.0.0.0
ESR3(config-ospf-area)# enable
ESR3(config-ospf-area)# exit
ESR3(config-ospf)# enable
ESR3(config-ospf)# exit
ESR3(config)#
ESR3(config)# interface loopback 1
ESR3(config-loopback)# ip address 3.3.3.3/32
ESR3(config-loopback)# ip ospf instance 1
ESR3(config-loopback)# ip ospf
ESR3(config-loopback)# exit
ESR3(config)#
ESR3(config)# interface gigabitethernet 1/0/1.20
ESR3(config-subif)# ip firewall disable
ESR3(config-subif)# ip address 20.20.20.1/30
ESR3(config-subif)# ip ospf instance 1
ESR3(config-subif)# ip ospf
ESR3(config-subif)# exit
ESR3(config)#
ESR3(config)# interface gigabitethernet 1/0/1.30
ESR3(config-subif)# ip firewall disable
ESR3(config-subif)# ip address 30.30.30.1/30
ESR3(config-subif)# ip ospf instance 1
ESR3(config-subif)# ip ospf
ESR3(config-subif)# exit
ESR3(config)#
ESR3(config)# system jumbo-frames
ESR3(config)# do commit
ESR3(config)# do confirm
```

ESR4

```
ESR4(config)# router ospf log-adjacency-changes
ESR4(config)# router ospf 1
ESR4(config-ospf)# router-id 4.4.4.4
ESR4(config-ospf)# area 0.0.0.0
ESR4(config-ospf-area)# enable
ESR4(config-ospf-area)# exit
ESR4(config-ospf)# enable
ESR4(config-ospf)# exit
ESR4(config)#
ESR4(config)# interface loopback 1
ESR4(config-loopback)# ip address 4.4.4.4/32
ESR4(config-loopback)# ip ospf instance 1
ESR4(config-loopback)# ip ospf
ESR4(config-loopback)# exit
ESR4(config)#
ESR4(config)# interface gigabitethernet 1/0/1.40
ESR4(config-subif)# ip firewall disable
ESR4(config-subif)# ip address 40.40.40.2/30
ESR4(config-subif)# ip ospf instance 1
ESR4(config-subif)# ip ospf
ESR4(config-subif)# exit
ESR4(config)#
ESR4(config)# interface gigabitethernet 1/0/1.30
ESR4(config-subif)# ip firewall disable
ESR4(config-subif)# ip address 30.30.30.2/30
ESR4(config-subif)# ip ospf instance 1
ESR4(config-subif)# ip ospf
ESR4(config-subif)# exit
ESR4(config)#
ESR4(config)# system jumbo-frames
ESR4(config)# do commit
ESR4(config)# do confirm
```

Необходимо убедиться, что протокол OSPF запущен на каждом маршрутизаторе:

```
ESR1# show ip ospf neighbors


Router ID        Pri  State          DTime  Interface      Router IP
---------        ---  -----          -----  -------------  ---------
2.2.2.2          128  Full/BDR       00:39  gi1/0/1.10     10.10.10.2
4.4.4.4          128  Full/BDR       00:32  gi1/0/1.40     40.40.40.2


ESR1# show ip ospf
O       40.40.40.0/30       [150/10]          dev gi1/0/1.40                    [ospf1 1970-01-0
8]  (1.1.1.1)
O     * 30.30.30.0/30       [150/20]          via 40.40.40.2 on gi1/0/1.40      [ospf1 1970-01-0
8]  (3.3.3.3)
O       1.1.1.1/32          [150/0]           dev lo1                           [ospf1 1970-01-0
8]  (1.1.1.1)
O     * 4.4.4.4/32          [150/10]          via 40.40.40.2 on gi1/0/1.40      [ospf1 1970-01-0
8]  (4.4.4.4)
O     * 20.20.20.0/30       [150/20]          via 10.10.10.2 on gi1/0/1.10      [ospf1 22:05:45]
    (3.3.3.3)
O       10.10.10.0/30       [150/10]          dev gi1/0/1.10                    [ospf1 22:05:33]
    (1.1.1.1)
O     * 3.3.3.3/32          [150/20]          multipath                         [ospf1 22:05:45]
    (3.3.3.3)
                                              via 40.40.40.2 on gi1/0/1.40 weight 1
O     * 2.2.2.2/32          [150/10]          via 10.10.10.2 on gi1/0/1.10      [ospf1 22:05:45]
    (2.2.2.2)
```

Настройка LDP на P/PE-маршрутизаторах

ESR1

```
ESR1# config
ESR1(config)# mpls
ESR1(config-mpls)# ldp
ESR1(config-ldp)# address-family ipv4
ESR1(config-ldp-af-ipv4)# transport-address 1.1.1.1
ESR1(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1.10
ESR1(config-ldp-af-ipv4-if)# exit
ESR1(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1.40
ESR1(config-ldp-af-ipv4-if)# exit
ESR1(config-ldp-af-ipv4)# exit
ESR1(config-ldp)# enable
ESR1(config-ldp)# exit
ESR1(config-mpls)# forwarding interface gigabitethernet 1/0/1.10
ESR1(config-mpls)# forwarding interface gigabitethernet 1/0/1.40
ESR1(config-mpls)# exit
ESR1(config)# do commit
ESR1(config)# do confirm
```

ESR2

```
ESR2# config
ESR2(config)# mpls
ESR2(config-mpls)# ldp
ESR2(config-ldp)# address-family ipv4
ESR2(config-ldp-af-ipv4)# transport-address 2.2.2.2
ESR2(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1.10
ESR2(config-ldp-af-ipv4-if)# exit
ESR2(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1.20
ESR2(config-ldp-af-ipv4-if)# exit
ESR2(config-ldp-af-ipv4)# exit
ESR2(config-ldp)# enable
ESR2(config-ldp)# exit
ESR2(config-mpls)# forwarding interface gigabitethernet 1/0/1.10
ESR2(config-mpls)# forwarding interface gigabitethernet 1/0/1.20
ESR2(config-mpls)# exit
ESR2(config)# do commit
ESR2(config)# do confirm
```

ESR3

```
ESR3# config
ESR3(config)# mpls
ESR3(config-mpls)# ldp
ESR3(config-ldp)# address-family ipv4
ESR3(config-ldp-af-ipv4)# transport-address 3.3.3.3
ESR3(config-ldp-af-ipv4)#  interface gigabitethernet 1/0/1.20
ESR3(config-ldp-af-ipv4-if)# exit
ESR3(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1.30
ESR3(config-ldp-af-ipv4-if)# exit
ESR3(config-ldp-af-ipv4)# exit
ESR3(config-ldp)# enable
ESR3(config-ldp)# exit
ESR3(config-mpls)# forwarding interface gigabitethernet 1/0/1.20
ESR3(config-mpls)# forwarding interface gigabitethernet 1/0/1.30
ESR3(config-mpls)# exit
ESR3(config)# do commit
ESR3(config)# do confirm
```

ESR4

```
ESR4# config
ESR4(config)# mpls
ESR4(config-mpls)# ldp
ESR4(config-ldp)# address-family ipv4
ESR4(config-ldp-af-ipv4)# transport-address 4.4.4.4
ESR4(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1.30
ESR4(config-ldp-af-ipv4-if)# exit
ESR4(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1.40
ESR4(config-ldp-af-ipv4-if)# exit
ESR4(config-ldp-af-ipv4)# exit
ESR4(config-ldp)# enable
ESR4(config-ldp)# exit
ESR4(config-mpls)# forwarding interface gigabitethernet 1/0/1.30
ESR4(config-mpls)# forwarding interface gigabitethernet 1/0/1.40
ESR4(config-mpls)# exit
ESR4(config)# do commit
ESR4(config)# do confirm
```

Для проверки сходимости LDP можно воспользоваться одной из следующих команд:

```
ESR1# show mpls ldp neighbor
Peer LDP ID: 2.2.2.2; Local LDP ID 1.1.1.1
    State: Operational
    TCP connection: 2.2.2.2:33933 - 1.1.1.1:646
    Messages sent/received: 1059/1070
    Uptime: 17:32:07
    LDP discovery sources:
        gigabitethernet 1/0/1.10
Peer LDP ID: 4.4.4.4; Local LDP ID 1.1.1.1
    State: Operational
    TCP connection: 4.4.4.4:40894 - 1.1.1.1:646
    Messages sent/received: 1376/1386
    Uptime: 22:38:38
    LDP discovery sources:
        gigabitethernet 1/0/1.40
```

Настройка MP-BGP

Создадим VRF на ESR1 и ESR3 соответственно. Укажем RD, rt-export/import в соответствии со схемой, настроим интерфейс для взаимодействия с CE (CE-SiteA и CE-SiteB). Дополнительно создадим route-map для разрешения анонсирования маршрутов по протоколу BGP:

⚠ **Без указания атрибутов RD и RT маршрутная информация не попадет в таблицу VPNv4.**

ESR1

```
ESR1(config)# ip vrf Customer1
ESR1(config-vrf)# ip protocols bgp max-routes 1000
ESR1(config-vrf)# rd 65500:100
ESR1(config-vrf)# route-target import 65500:100
ESR1(config-vrf)# route-target export 65500:100
ESR1(config-vrf)# exit
ESR1(config)# interface gigabitethernet 1/0/2
ESR1(config-if-gi)# ip vrf forwarding Customer1
ESR1(config-if-gi)# description "Customer1"
ESR1(config-if-gi)# ip firewall disable
ESR1(config-if-gi)# ip address 192.168.32.1/30
ESR1(config-if-gi)# exit
ESR1(config)# route-map OUTPUT
ESR1(config-route-map)# rule 1
ESR1(config-route-map-rule)# action permit
ESR1(config-route-map-rule)# exit
ESR1(config-route-map)# exit
ESR1(config)# do commit
ESR1(config)# do confirm
```

ESR3

```
ESR3(config)# ip vrf Customer1
ESR3(config-vrf)# ip protocols bgp max-routes 1000
ESR3(config-vrf)# rd 65500:100
ESR3(config-vrf)# route-target export 65500:100
ESR3(config-vrf)# route-target import 65500:100
ESR3(config-vrf)# exit
ESR3(config)# interface gigabitethernet 1/0/2
ESR3(config-if-gi)# ip vrf forwarding Customer1
ESR3(config-if-gi)# description "Customer1"
ESR3(config-if-gi)# ip firewall disable
ESR3(config-if-gi)# ip address 192.168.32.5/30
ESR3(config-if-gi)# exit
ESR3(config)# route-map OUTPUT
ESR3(config-route-map)# rule 1
ESR3(config-route-map-rule)# action permit
ESR3(config-route-map-rule)# exit
ESR3(config-route-map)# exit
ESR3(config)# do commit
ESR3(config)# do confirm
```

Настроим iBGP между ESR1 и ESR3. Включим отправку extended community на обоих устройствах:

ESR1

```
ESR1(config)# router bgp log-neighbor-changes
ESR1(config)# router bgp 65500
ESR1(config-bgp)# router-id 1.1.1.1
ESR1(config-bgp)# enable
ESR1(config-bgp)# neighbor 3.3.3.3
ESR1(config-bgp-neighbor)# remote-as 65500
ESR1(config-bgp-neighbor)# update-source 1.1.1.1
ESR1(config-bgp-neighbor)# enable
ESR1(config-bgp-neighbor)# address-family vpnv4 unicast
ESR1(config-bgp-neighbor-af)# send-community extended
ESR1(config-bgp-neighbor-af)# enable
ESR1(config-bgp-neighbor-af)# exit
ESR1(config-bgp-neighbor)# exit
ESR1(config-bgp)# exit
ESR1(config)# do commit
ESR1(config)# do confirm
```

ESR3

```
ESR3(config)# router bgp log-neighbor-changes
ESR3(config)# router bgp 65500
ESR3(config-bgp)# router-id 3.3.3.3
ESR3(config-bgp)# enable
ESR3(config-bgp)# neighbor 1.1.1.1
ESR3(config-bgp-neighbor)# remote-as 65500
ESR3(config-bgp-neighbor)# update-source 3.3.3.3
ESR3(config-bgp-neighbor)# enable
ESR3(config-bgp-neighbor)# address-family vpnv4 unicast
ESR3(config-bgp-neighbor-af)# send-community extended
ESR3(config-bgp-neighbor-af)# enable
ESR3(config-bgp-neighbor-af)# exit
ESR3(config-bgp-neighbor)# exit
ESR3(config-bgp)# exit
ESR3(config)# do commit
ESR3(config)# do confirm
```

Необходимо убедиться, что BGP-сессия успешно установлена:

```
ESR1# show bgp neighbors
BGP neighbor is 3.3.3.3
    BGP state: Established
    Neighbor address: 3.3.3.3
    Neighbor AS: 65500
    Neighbor ID: 3.3.3.3
    Neighbor caps: refresh enhanced-refresh restart-aware AS4
    Session: internal multihop AS4
    Source address: 1.1.1.1
    Weight: 0
    Hold timer: 126/180
    Keepalive timer: 40/60
    Address family ipv4 unicast:
    Default originate: No
    Default information originate: No
    Uptime: 88495 s
```

Настройка маршрутизации PE-CE

Согласно топологии, Customer1 анонсирует по BGP (AS65505) подсеть 10.100.0.0/24. Необходимо настроить соответствующие интерфейсы, eBGP между ESR1 и CE_SiteA. Также необходимо разрешить анонсирование маршрутов в сторону PE.

По умолчанию для eBGP анонсирование маршрутов запрещено, необходимо настроить разрешающее правило. Для iBGP анонсирование маршрутов разрешено.

Необходимая конфигурация на маршрутизаторе CE-SiteA:

CE _SiteA

```
CE-SiteA(config)# interface gigabitethernet 1/0/2
CE-SiteA(config-if-gi)# ip firewall disable
CE-SiteA(config-if-gi)# ip address 192.168.32.2/30
CE-SiteA(config-if-gi)# exit
CE-SiteA(config)# interface loopback 1
CE-SiteA(config-loopback)# ip address 10.100.0.1/24
CE-SiteA(config-loopback)# exit
CE-SiteA(config)# route-map OUTPUT
CE-SiteA(config-route-map)# rule 1
CE-SiteA(config-route-map-rule)# match ip address 10.100.0.0/24
CE-SiteA(config-route-map-rule)# action permit
CE-SiteA(config-route-map-rule)# exit
CE-SiteA(config-route-map)# exit
CE-SiteA(config)# router bgp log-neighbor-changes
CE-SiteA(config)# router bgp 65505
CE-SiteA(config-bgp)# router-id 192.168.32.1
CE-SiteA(config-bgp)# neighbor 192.168.32.1
CE-SiteA(config-bgp-neighbor)# remote-as 65500
CE-SiteA(config-bgp-neighbor)# allow-local-as 1
CE-SiteA(config-bgp-neighbor)# update-source 192.168.32.2
CE-SiteA(config-bgp-neighbor)# address-family ipv4 unicast
CE-SiteA(config-bgp-neighbor-af)# route-map OUTPUT out
CE-SiteA(config-bgp-neighbor-af)# enable
CE-SiteA(config-bgp-neighbor-af)# exit
CE-SiteA(config-bgp-neighbor)# enable
CE-SiteA(config-bgp-neighbor)# exit
CE-SiteA(config-bgp)# address-family ipv4 unicast
CE-SiteA(config-bgp-af)# network 10.100.0.0/24
CE-SiteA(config-bgp-af)# exit
CE-SiteA(config-bgp)# enable
CE-SiteA(config-bgp)# exit
CE-SiteA(config)# do commit
CE-SiteA(config)# do confirm
```

Переходим к настройке eBGP на маршрутизаторе ESR1.
Создадим eBGP-сессию с CE_SiteA и разрешим передачу маршрутов BGP-пиру:

ESR1

```
ESR1(config)# router bgp 65500
ESR1(config-bgp)# vrf Customer1
ESR1(config-bgp-vrf)# router-id 192.168.32.1
ESR1(config-bgp-vrf)# neighbor 192.168.32.2
ESR1(config-bgp-vrf-neighbor)# remote-as 65505
ESR1(config-bgp-vrf-neighbor)# update-source 192.168.32.1
ESR1(config-bgp-vrf-neighbor)# address-family ipv4 unicast
ESR1(config-bgp-neighbor-af-vrf)# route-map OUTPUT out
ESR1(config-bgp-neighbor-af-vrf)# enable
ESR1(config-bgp-neighbor-af-vrf)# exit
ESR1(config-bgp-vrf-neighbor)# enable
ESR1(config-bgp-vrf-neighbor)# exit
ESR1(config-bgp-vrf)# address-family ipv4 unicast
ESR1(config-bgp-vrf-af)# redistribute connected
ESR1(config-bgp-vrf-af)# redistribute bgp 65500
ESR1(config-bgp-vrf-af)# exit
ESR1(config-bgp-vrf)# enable
ESR1(config-bgp-vrf)# exit
ESR1(config-bgp)# exit
ESR1(config)# do commit
ESR1(config)# do confirm
```

При передаче маршрутов из VRF в таблицу VPNv4 ТОЛЬКО connected- и/или static-сетей указывать команду enable не нужно. Включение необходимо только при наличии BGP пиров в VRF.
Пример конфигурации передачи в VPNv4 таблицу connected- и static-сетей:

```
ESR1(config)# router bgp 65500
ESR1(config-bgp)# router-id 1.1.1.1
ESR1(config-bgp)# neighbor 3.3.3.3
ESR1(config-bgp-neighbor)# remote-as 65500
ESR1(config-bgp-neighbor)# update-source 1.1.1.1
ESR1(config-bgp-neighbor)# enable
ESR1(config-bgp-neighbor)# address-family vpnv4 unicast
ESR1(config-bgp-neighbor-af)# send-community extended
ESR1(config-bgp-neighbor-af)# enable
ESR1(config-bgp-neighbor-af)# exit
ESR1(config-bgp-neighbor)# exit
ESR1(config-bgp)# enable
EESR1(config-bgp)# vrf Customer1
ESR1(config-bgp-vrf)# address-family ipv4 unicast
ESR1(config-bgp-vrf-af)# redistribute connected
ESR1(config-bgp-vrf-af)# redistribute static
ESR1(config-bgp-vrf-af)# exit
ESR1(config-bgp-vrf)# exit
ESR1(config-bgp)# exit
ESR1(config)# do commit
ESR1(config)# do confirm
```

Для проверки принятых и анонсированных маршрутов можно воспользоваться следующими командами:

```
ESR1# show bgp vpnv4 unicast vrf Customer1 neighbors 192.168.32.2 advertise-routes
Status codes: u - unicast, b - broadcast, m - multicast, a - anycast
              * - valid, > - best
Origin codes: i - IGP, e - EGP, ? - incomplete


     Network              Next Hop            Metric  LocPrf      Weight Path
*> u 10.100.1.0/24        192.168.32.1                100                 65500 i
*> u 192.168.32.4/30      192.168.32.1                100                 65500 i
```

Вывод анонсируемых маршрутов для определенного пира. Маршрутная информация отображается после применения фильтрации:

```
ESR1# show bgp vpnv4 unicast vrf Customer1 neighbors 192.168.32.2 routes
Status codes: u - unicast, b - broadcast, m - multicast, a - anycast
              * - valid, > - best
Origin codes: i - IGP, e - EGP, ? - incomplete


     Network              Next Hop            Metric  LocPrf      Weight Path
*> u 10.100.0.0/24        192.168.32.2                100         0      65505
```

Вывод принятой маршрутной информации от определенного пира. Маршрутная информация отображается после применения фильтрации.

CE-SiteB

Необходимо проделать схожие операции между маршрутизаторами ESR3 и CE_SiteB.

Произвести настройку соответствующих интерфейсов и создать eBGP-сессию между ESR3 и CE_SiteB:

CE-SiteB

```
CE-SiteB(config)# interface gigabitethernet 1/0/2
CE-SiteB(config-if-gi)# ip firewall disable
CE-SiteB(config-if-gi)# ip address 192.168.32.6/30
CE-SiteB(config-if-gi)# exit
CE-SiteB(config)#
CE-SiteB(config)# interface loopback 1
CE-SiteB(config-loopback)# ip address 10.100.1.1/24
CE-SiteB(config-loopback)# exit
CE-SiteB(config)#
CE-SiteB(config)# route-map OUTPUT
CE-SiteB(config-route-map)# rule 1
CE-SiteB(config-route-map-rule)# match ip address 10.100.1.0/24
CE-SiteB(config-route-map-rule)# action permit
CE-SiteB(config-route-map-rule)# exit
CE-SiteB(config-route-map)# exit
CE-SiteB(config)#
CE-SiteB(config)# router bgp 65505
CE-SiteB(config-bgp)# router-id 192.168.32.6
CE-SiteB(config-bgp)# neighbor 192.168.32.5
CE-SiteB(config-bgp-neighbor)# remote-as 65500
CE-SiteB(config-bgp-neighbor)# allow-local-as 1
CE-SiteB(config-bgp-neighbor)# update-source 192.168.32.6
CE-SiteB(config-bgp-neighbor)# address-family ipv4 unicast
CE-SiteB(config-bgp-neighbor-af)# route-map OUTPUT out
CE-SiteB(config-bgp-neighbor-af)# enable
CE-SiteB(config-bgp-neighbor-af)# exit
CE-SiteB(config-bgp-neighbor)# enable
CE-SiteB(config-bgp-neighbor)# exit
CE-SiteB(config-bgp)# address-family ipv4 unicast
CE-SiteB(config-bgp-af)# network 10.100.1.0/24
CE-SiteB(config-bgp-af)# exit
CE-SiteB(config-bgp)# enable
CE-SiteB(config-bgp)# exit
CE-SiteB(config)# do commit
CE-SiteB(config)# do confirm
```

Со стороны ESR3 также настроить eBGP и разрешить передачу маршрутной информации из VRF в таблицу VPNv4:

ESR3

```
router bgp 65500
ESR3(config)# router bgp 65500
ESR3(config-bgp)# vrf Customer1
ESR3(config-bgp-vrf)# router-id 192.168.32.5
ESR3(config-bgp-vrf)# neighbor 192.168.32.6
ESR3(config-bgp-vrf-neighbor)# remote-as 65505
ESR3(config-bgp-vrf-neighbor)# update-source 192.168.32.5
ESR3(config-bgp-vrf-neighbor)# address-family ipv4 unicast
ESR3(config-bgp-neighbor-af-vrf)# route-map OUTPUT out
ESR3(config-bgp-neighbor-af-vrf)# enable
ESR3(config-bgp-neighbor-af-vrf)# exit
ESR3(config-bgp-vrf-neighbor)# enable
ESR3(config-bgp-vrf-neighbor)# exit
ESR3(config-bgp-vrf)# address-family ipv4 unicast
ESR3(config-bgp-vrf-af)# redistribute connected
ESR3(config-bgp-vrf-af)# redistribute bgp 65500
ESR3(config-bgp-vrf-af)# exit
ESR3(config-bgp-vrf)# enable
ESR3(config-bgp-vrf)# exit
ESR3(config-bgp)# exit
ESR3(config)# do commit
ESR3(config)# do confirm
```

Для просмотра VPNv4-таблицы воспользоваться командой:

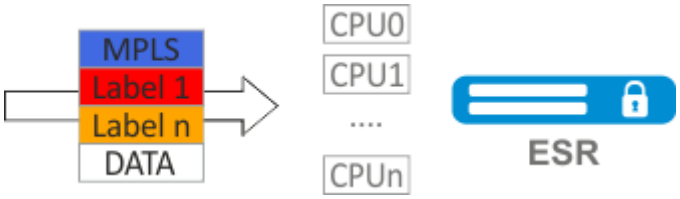
```
ESR1# show bgp vpnv4 unicast all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete


Codes Route Distinguisher   IP Prefix          Next hop        Metric     Label   LocPrf
    Weight Path
----- --------------------- ------------------ --------------- ---------- ------- ----------
------ ----------------
*>    65500:100             10.100.0.0/24      --              --         23      --         --
    ?
*>i   65500:100             192.168.32.4/30    3.3.3.3         --         84      100        0
      i
*>i   65500:100             10.100.1.0/24      3.3.3.3         --         84      100        0
      i
```

Данная команда выводит все принятые VPNv4-маршруты после применения фильтрации.

14.8 Балансировка трафика MPLS

Маршрутизаторы ESR имеют многоядерную архитектуру. Одним из первых звеньев обработки поступающего трафика является load balancer daemon (lbd), который выполняет две основных функции:

1. Равномерно распределяет нагрузку между всеми CPU маршрутизатора.
2. Выявляет аномальные ситуации с высокой нагрузкой на отдельные CPU и перераспределяет обработку с этих CPU на менее загруженные.



По умолчанию lbd использует только MPLS-метки для вычисления хеша и дальнейшего распределения нагрузки на различные CPU. Данное поведение не всегда дает преимущество, особенно когда существуют "большие" однородные потоки MPLS-трафика. Для добавления энтропии в хеш можно включить дополнительный функционал:

cpu load-balance mpls passenger ip
Включает возможность "заглядывать" дальше MPLS-заголовка для поиска IP-заголовка и добавления ip-src и ip-dst в расчет хеша:
Для L3VPN: идет поиск пары ip-src и ip-dst в ip-заголовке, находящимся за mpls заголовком.

Для L2VPN: ESR попытается "заглянуть" в ethernet-фрейм (который находится за mpls-заголовком) и получить ip-src и ip-dst в ip-заголовке для добавления в расчет хеша.

cpu load-balance mpls passenger ip-over-ethernet-pseudowire-with-cw
cpu load-balance mpls passenger ip-over-ethernet-pseudowire-without-cw
Позволяет явно указать, используется ли при построении L2VPN функционал Control Word. Это позволяет исключить возникновение ошибки, когда пакет с наличием Control word может быть ошибочно распознан как пакет без него.

При хешировании MPLS-меток действуют следующие ограничения:

- В расчет не добавляются метки 0-15 (Special-Purpose Labels) – см. RFC 7274;
- В расчет не добавляется метка, если непосредственно перед ней следует метка 15 (Extension Label) – см. RFC 7274;
- В расчет хеша добавляется не более трёх меток.

Во избежание падения LDP-сессии при большой нагрузке на CPU маршрутизатора на моделях ESR-200, ESR-1000, ESR-1200, ESR-1500, ESR-1700 после включения функционала все пакеты протокола LDP будут обрабатываться управляющими CPU (Management CPU), которые не участвуют в обработке трафика. Для ESR-200, ESR-1000, ESR-1200, ESR-1500 – это CPU 0, ESR-1700 – CPU 0-1.

14.8.1 Пример настройки

Задача:

Включить балансировку L2VPN-трафика без использования функционала Control Word.

Решение:

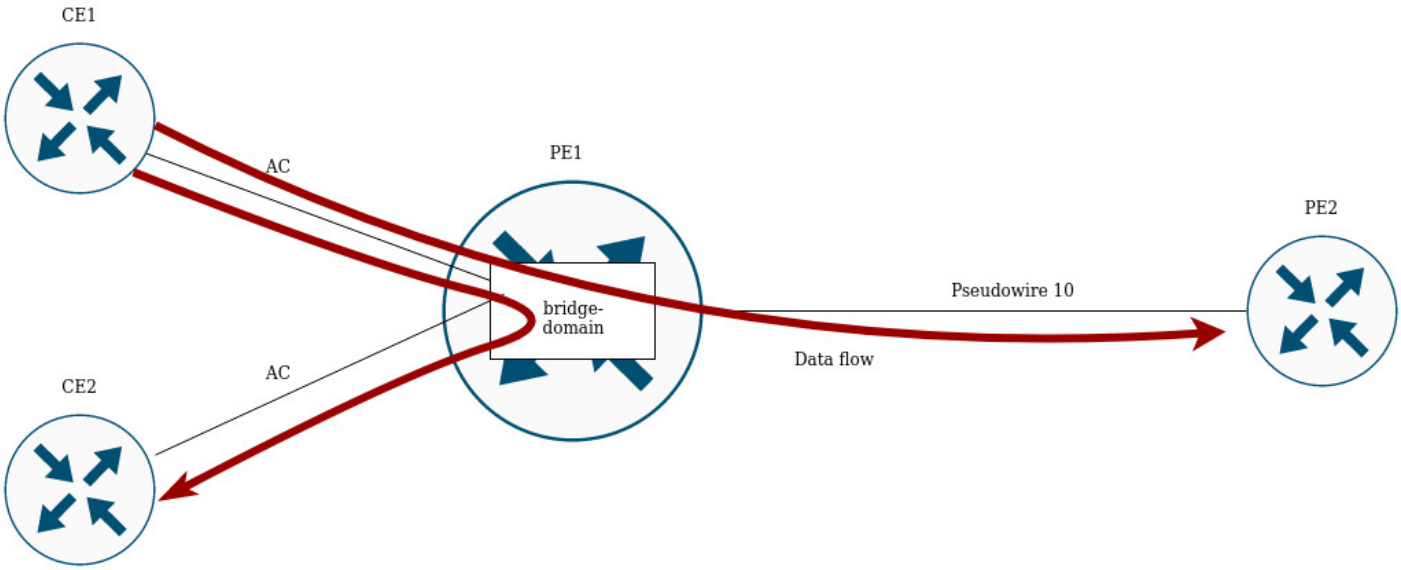
ESR

```
ESR(config)# system cpu load-balance mpls passenger ip
ESR(config)# system cpu load-balance mpls passenger ipoe-pw-without-cw
```

14.9 Работа с бридж-доменом в рамках MPLS

Для организации L2VPN-сервиса необходимо настроить на устройстве бридж-домен, создать требуемые AC, PW (LDP-signaling) и связать все данные элементы с бридж-доменом.

Для point-to-point бридж-домен создается автоматически.



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

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

В текущей реализации бридж-домен не пропускает трафик протоколов канального уровня, таких так: STP, LLDP, CDP и т.д.

Бридж-домен может работать в двух транспортных режимах: ethernet или vlan. Транспортных режим задает правила обработки трафика на входе и выходе с бридж-домена.

В LDP signaling по умолчанию используется ethernet mode (Raw mode, type 5). Для каждого отдельного экземпляра VPLS можно задать транспортный режим.

В BGP signaling бридж-домен работает только в ethernet mode.

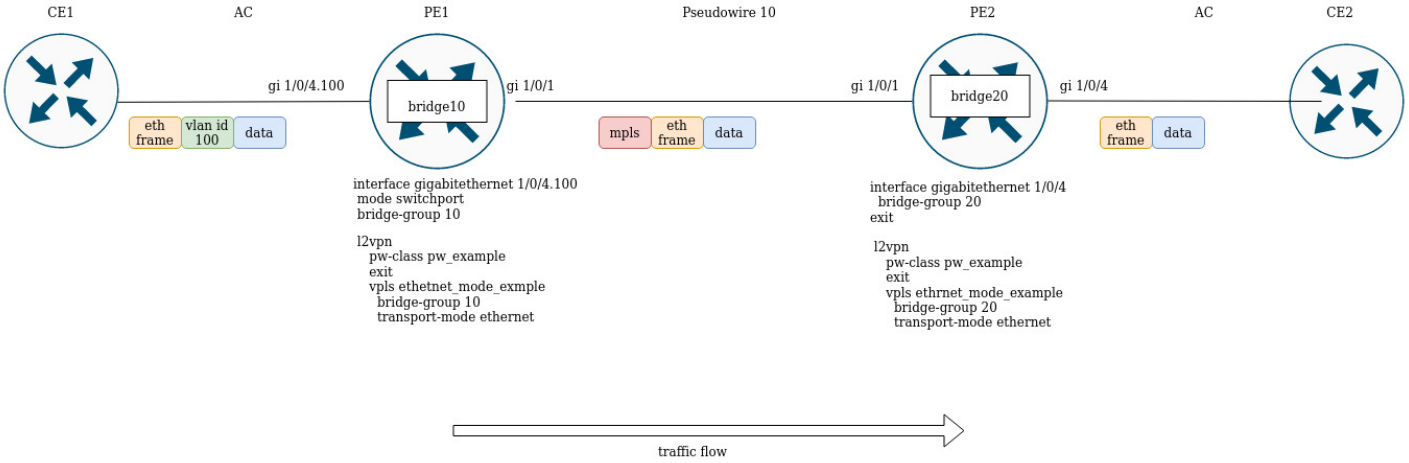
```
PE1# config
PE1(config)# mpls
PE1(config-mpls)# l2vpn
PE1(config-l2vpn)# vpls MARTINI_br
PE1(config-l2vpn-vpls)# transport-mode vlan

PE1# sh mpls l2vpn pseudowire
Neighbor                                PW ID      Sig Type       Status
--------------------------------------- ---------- --- ---------- ------
10.10.0.2                               200        LDP Eth Tagged Up
```

В LDP signaling транспортный режим согласуется между PE в процессе создания псевдо-провода, поэтому он должен совпадать на обоих PE.

Рассмотрим правила обработки трафика:

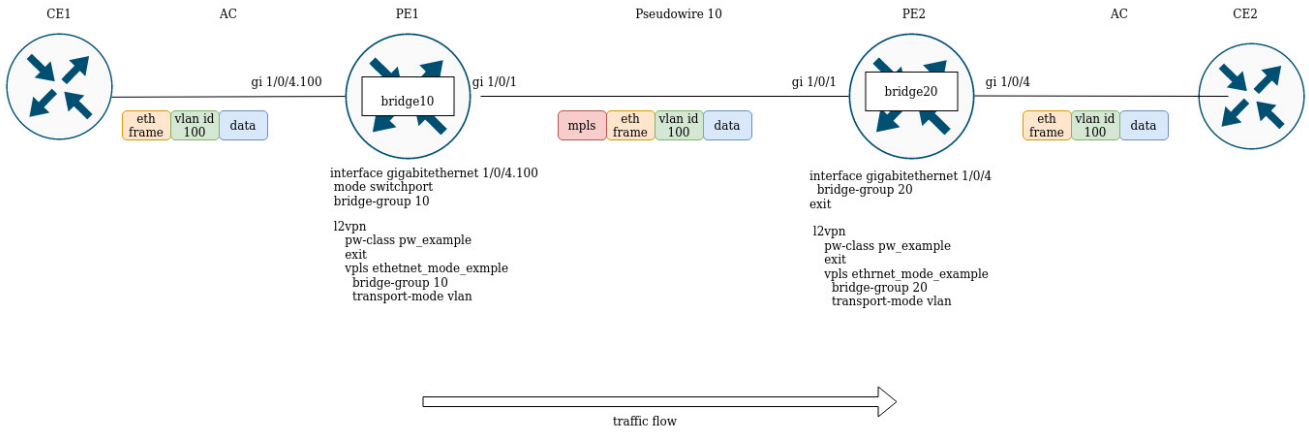
1. Ethernet (Raw) mode:

- Если AC является саб-интерфейсом, то vlan-тег перед помещение в бридж снимается. При выходе из бриджа vlan-тег восстанавливается.
- Если AC является интерфейсом, то тегированный и нетегированный трафик проходит в обоих направлениях без модификаций.



Предположим, PE1 и PE2 сконфигурированы в ethernet mode. Со стороны PE1 в бридж-домен включен саб-интерфейс gigabitethernet 1/0/4.100, поэтому vlan-тег (vlan id 100) с входящего трафика будет удален перед помещением в Pseudowire 10 (соответственно, восстановлен при трафике в сторону AC). С другой стороны, AC на PE2 является интерфейсом, значит трафик будет проходить без модификаций в обоих направлениях.

2. Vlan (Tagged) mode:
   - Если AC является саб-интерфейсом, то vlan-тег перед помещением в бридж сохраняется. При выходе из бриджа vlan-тег может быть сохранен или перезаписан в зависимости от конфигурации.
   - Если AC является интерфейсом, то модификация тегов не происходит в обоих направлениях.



14.10 Назначение MTU при работе с MPLS

Очень важно правильно настроить MTU на интерфейсах, участвующих в передаче трафика. Отметим два ключевых момента:

1. Размер Ethernet-заголовка (18 байт), inner tag (4 байта), outer tag (4 байта) не учитываются на AC-интерфейсах;
2. На интерфейсах, принимающих участие в пересылке MPLS-трафика, необходимо увеличить MTU на количество меток (каждая метка равна 4 байтам).

Значение MTU также участвует в сигнализации при построении псевдо-провода как в LDP-signaling, так и в BGP-signaling. Рассмотрим примеры настройки для обоих случаев:

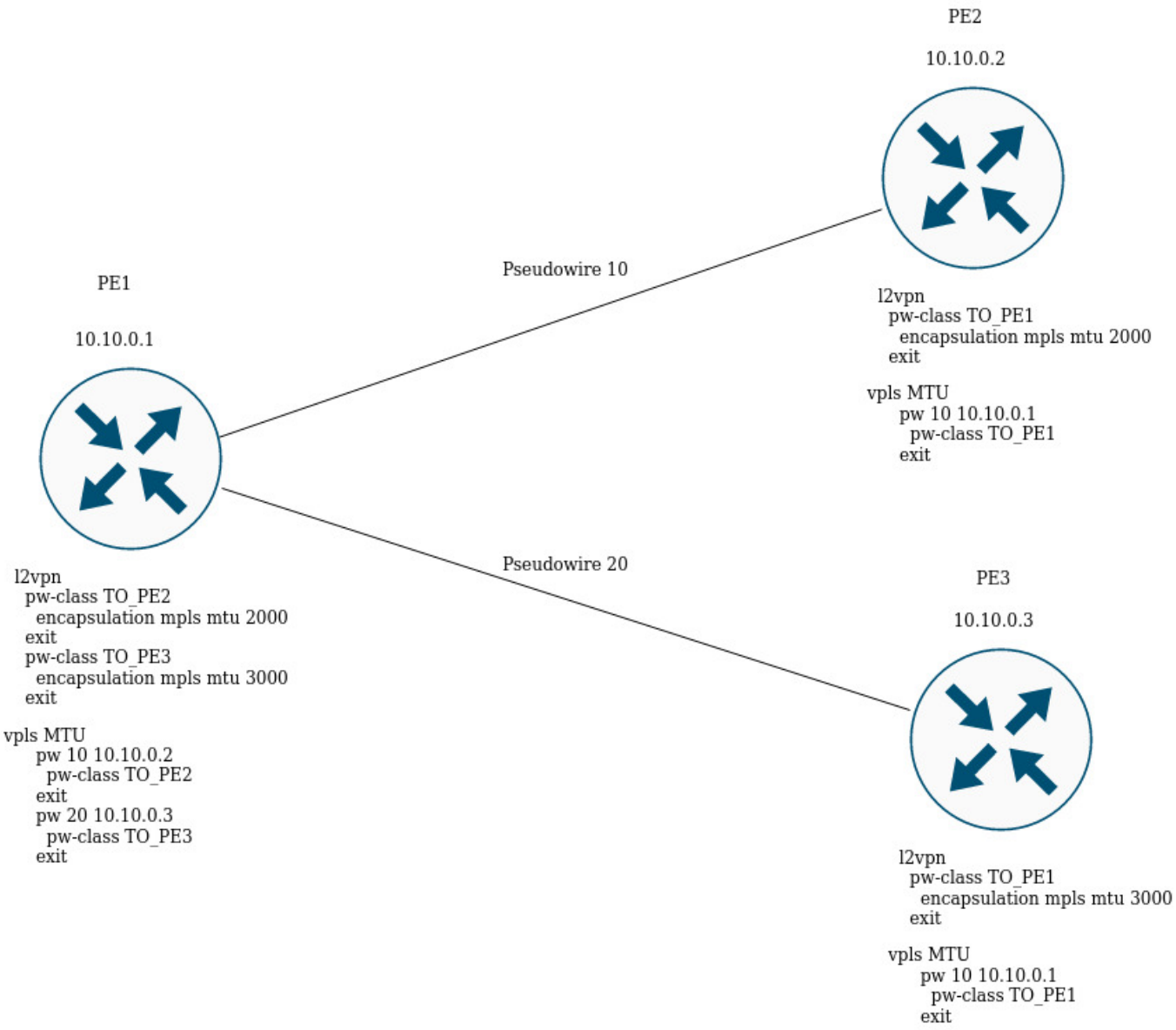
Для сигнализации (LDP, BGP) значение MTU по умолчанию – 1500.

Значения MTU, участвующие в сигнализации, не влияют на фактический размер пакета, проходящего по псевдо-проводу.

В LDP-signaling MTU задается в рамках настройки pw − class:

LDP-signaling. Настройка MTU для согласования

```
PE2(config)# mpls
PE2(config-mpls)# l2vpn
PE2(config-l2vpn)# pw-class MTU_example
PE2(config-l2vpn-pw-class)# encapsulation mpls mtu 9000
PE2(config-l2vpn-pw-class)# exit
PE2(config-mpls)# l2vpn
PE2(config-l2vpn)# vpls MTU_Example_PW
PE2(config-l2vpn-vpls)# pw 200 10.10.0.1
PE2(config-l2vpn-pw)# pw-class
PE2(config-l2vpn-pw)# pw-class MTU_example

*Просмотр созданных pw-class'ов*
PE2#  sh mpls l2vpn pw-class
PW-class                        Neighbor   PW ID      Status Status-tlv MTU
------------------------------- ---------- ---------- ------ ---------- ------
MTU_example                      10.10.0.1  200         Up     Enable     9000


PE2# sh mpls l2vpn vpls  MTU_Example_PW
VPLS:  MTU_Example_PW
...
    PWs:
      PW ID 2, Neighbor 10.10.0.1:
        MTU:         9000
        Last change: 01:27:42
        Status:      Up

* Для сигнализации PW 2 данного VPLS выбрано MTU 9000*
```



На рисунке выше PE1 поднимает два псевдо-провода: pseudowire 10 до PE2, и pseudowire 20 до PE3 соответственно. Для сигнализации с PE2 MTU будет равным 2000 (pw-class TO_PE2), для PE3 – MTU будет равным 3000 (pw-class TO_PE3).

Для BGP-signaling MTU указывается в рамках конфигурации l2vpn-сервиса:

BGP -signaling. Настройка MTU для согласования

```
PE1(config)# mpls
PE1(config-mpls)# l2vpn
PE1(config-l2vpn)# vpls l2vpn_MTU
PE1(config-l2vpn-vpls)# autodiscovery bgp
PE1(config-bgp)# mtu 1500

PE2# sh mpls l2vpn vpls  l2vpn_MTU
VPLS: l2vpn_MTU
...
    PWs:
      PW ID 2, Neighbor 10.10.0.1:
        MTU:          1500
        Last change: 01:27:42
        Status:      Up

* Для сигнализации всех псевдо-проводов данного VPLS будет выбрано MTU 1500 *
```

Если при согласовании значение MTU не совпадает, то статус псевдо-провода будет – "DOWN", " Reason: MTU mismatch":

```
PE1(config-l2vpn)# vpls l2vpn_MTU
PE1(config-l2vpn-vpls)# autodiscovery bgp
PE1(config-bgp)# mtu 2000

PE2# sh mpls l2vpn vpls l2vpn_MTU
...
    PWs:
      PW ID 2, Neighbor 10.10.0.1:
        MTU:          2000
        Last change: 00:00:10
        Status:      Down
        Reason:      MTU mismatch
```

В BGP-signaling можно отключить проверку MTU для сервиса:

```
PE1(config)# mpls
PE1(config-mpls)# l2vpn
PE1(config-l2vpn)# vpls l2vpn _MTU
PE1(config-l2vpn-vpls)# autodiscovery bgp
PE1(config-bgp)# ignore mtu-mismatch
```

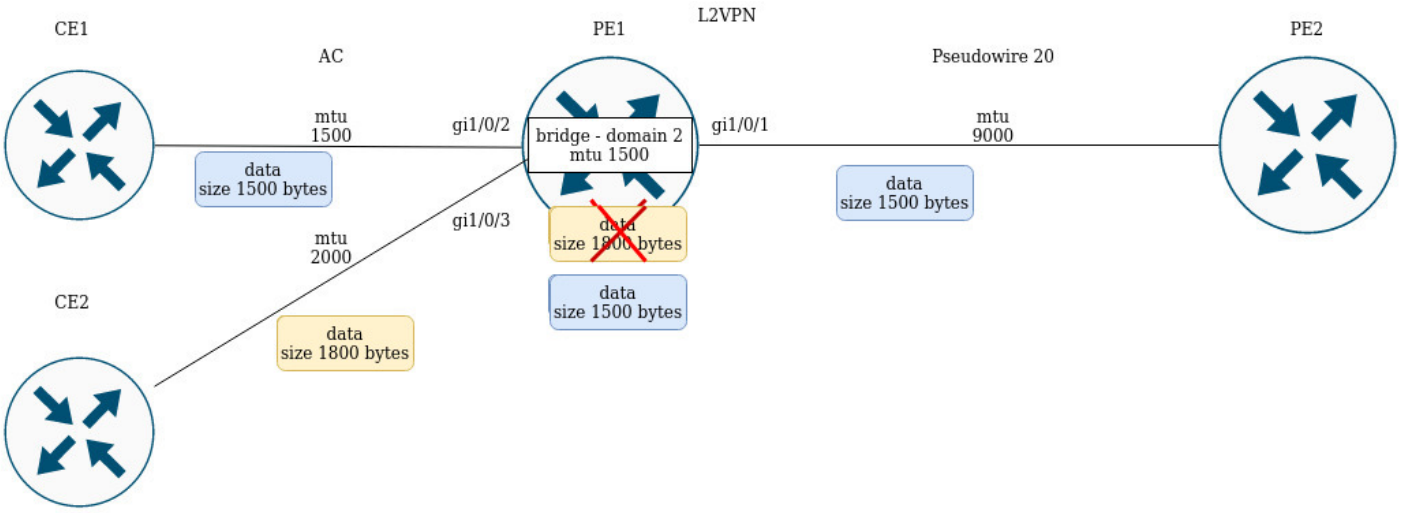
Теперь при согласовании значение MTU будет игнорироваться.

По умолчанию бридж-домен имеет MTU равным 1500 байт. Стоит отметить, что бридж-домен автоматически выбирает наименьшее значение MTU, исходя из собственного MTU и MTU-интерфейсов, включенных в бридж-домен.

```
* Например, имеем бридж-домен 100, в который включены интерфейсы gi1/0/1 со значением MTU 2000,
и gi1/0/2 со значением MTU 3000 *
CE3(config)# bridge 100
CE3(config-bridge)# enable
CE3(config-bridge)# exit
CE3(config)# interface gigabitethernet 1/0/1
CE3(config-if-gi)# mtu 2000
CE3(config-if-gi)# bridge-group 100
CE3(config-if-gi)# exit
CE3(config)# interface gigabitethernet 1/0/2
CE3(config-if-gi)# mtu 3000
CE3(config-if-gi)# bridge-group 100
CE3(config-if-gi)# do com

* MTU бридж-домена будет равным 1500, так как по умолчанию сам бридж имеет MTU 1500 (значение
по умолчанию), которое и стало наименьшим:
 MTU bridge 100 = 1500  <-- Наименьшее значение MTU
 MTU gi1/0/1  = 2000
 MTU gi1/0/2 = 3000
*


CE3# sh interfaces bridge
Bridges      Interfaces
----------   ------------------------------------------------------------
bridge 100   gi1/0/1-2

CE3# sh interfaces status bridge 100
Interface 'bridge 100' status information:
 Description:          --
 Operational state:    UP
 Administrative state: Up
 Supports broadcast:   Yes
 Supports multicast:   Yes
 MTU:                  1500
 MAC address:          a8:f9:4b:aa:11:00
 Last change:          1 minute and 46 seconds
 Mode:                 Routerport

* Изменим MTU на самом бридж-домене:  *

CE3(config)# bridge 100
CE3(config-bridge)# mtu 6000
CE3(config-bridge)# do com

* MTU бридж-домена стало равным 2000 байт, так как gi1/0/2 имеет наименьшее MTU:
 MTU bridge 100 = 6000
 MTU gi1/0/1 = 2000 <-- Наименьшее значение MTU
 MTU gi1/0/2 = 3000
*

CE3# sh interfaces bridge
Bridges      Interfaces
----------   ------------------------------------------------------------
bridge 100   gi1/0/1-2

CE3# sh interfaces status bridge 100
Interface 'bridge 100' status information:
 Description:          --
 Operational state:    Up
```

```
Administrative state: Up
Supports broadcast:   Yes
Supports multicast:   Yes
MTU:                  2000
MAC address:          a8:f9:4b:aa:11:00
Last change:          6 minutes and 42 seconds
Mode:                 Routerport
```

Рассмотрим пример прохождения трафика в L2VPN-сервисе:

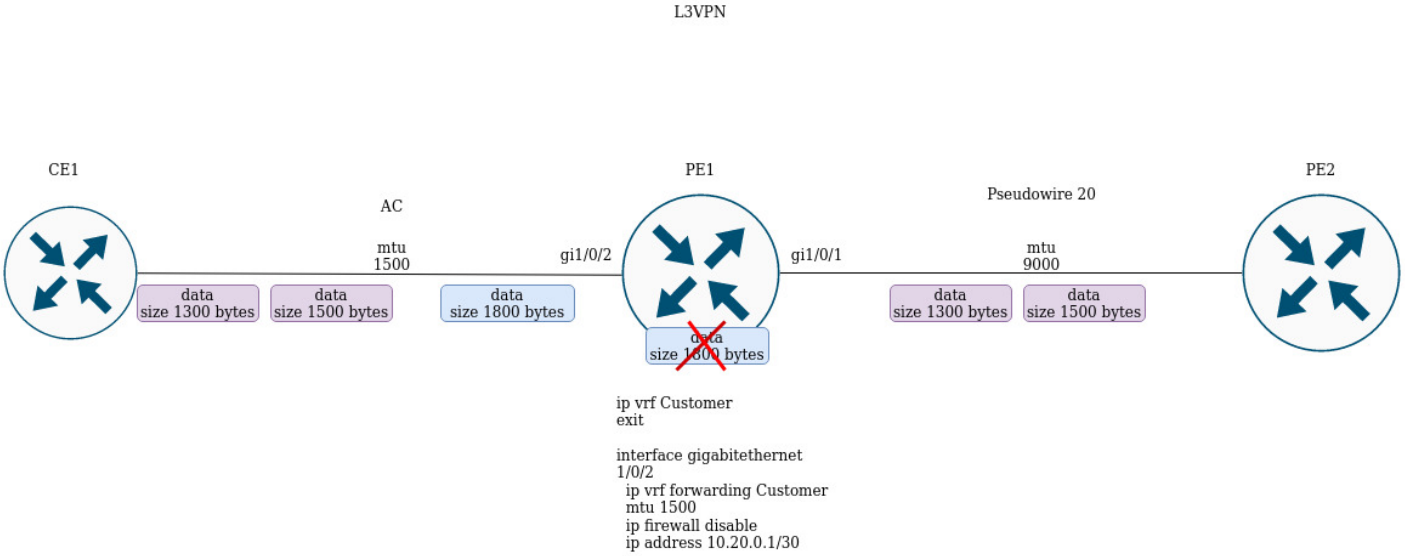


PE1 имеет следующие значения MTU на интерфейсах:

```
PE1# sh interfaces status
Interface            Admin   Link    MTU      MAC address          Last change
Mode
                     state   state
-------------------  -----   -----   ------   -------------------  --------------------------
----------
gi1/0/1              Up      Up      9000     a8:f9:4b:ac:4d:16    5 hours, 25 minutes and 2
Routerport
                                                                   seconds
gi1/0/2              Up      Up      1500     a8:f9:4b:ac:4d:17    4 days, 4 hours, 49
Switchport
                                                                   minutes and 40 seconds
gi1/0/3              Up      Up      1800     a8:f9:4b:ac:4d:18    4 days, 1 hour, 49
Switchport
                                                                   minutes and 38 seconds
bridge 2             Up      Up      1500     a8:f9:4b:ac:4d:15    1 day, 1 hour, 27 minutes
Routerport
                                                                   and 28 seconds
```

CE1 посылает пакеты размером 1500 байт, CE2 – 1800 байт соответственно. Так как MTU бридж-домена меньше, чем MTU пакета от CE2, то пакет от CE2 будет отброшен перед попаданием в бридж-домен. Аналогичные действия будут, если MTU-интерфейса, смотрящего в сторону mpls-core (gi1/0/1), меньше чем MTU, приходящих от CE-пакетов (с учетом mpls-заголовка).

Схожее поведение и при прохождении трафика в L3VPN-сервисе:

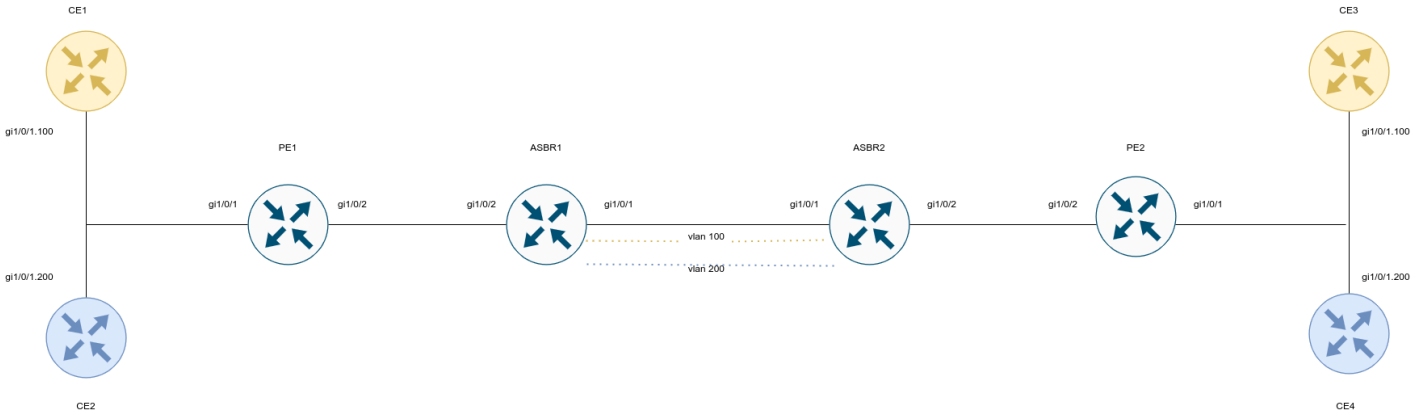


Если CE1 пошлет пакет с большим MTU, чем на интерфейсе, смотрящим в сторону клиента (gi1/0/2) или в сторону mpls-core (gi1/0/1), то пакет будет отброшен.

14.11 Inter-AS Option A

Рассмотрим примеры настройки на базе построения сервисов l3vpn и l2vpn. Главная особенность inter-AS Option A – отсутствие mpls-меток в трафике при передаче между ABSR. Для разделения трафика клиентских сервисов между ASBR обычно используют VRF для l3vpn или тегирование (dot1q, q-in-q) для сервисов l2vpn.

14.11.1 L2VPN



Настроим CE:

CE1

```
ESR# config
ESR(config)# hostname CE1
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-if-gi)# ip firewall disable
ESR(config-if-gi)# ip address 192.168.1.1/24
ESR(config-if-gi)# do com
ESR(config-if-gi)# do conf
```

CE2

```
ESR# config
ESR(config)# hostname CE2
ESR(config)# interface gigabitethernet 1/0/1.200
ESR(config-if-gi)# ip firewall disable
ESR(config-if-gi)# ip address 192.168.2.1/24
ESR(config-if-gi)# do com
ESR(config-if-gi)# do conf
```

CE3

```
ESR# config
ESR(config)# hostname CE3
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-if-gi)# ip firewall disable
ESR(config-if-gi)# ip address 192.168.1.2/24
ESR(config-if-gi)# do com
ESR(config-if-gi)# do conf
```

CE4

```
ESR# config
ESR(config)# hostname CE4
ESR(config)# interface gigabitethernet 1/0/1.200
ESR(config-if-gi)# ip firewall disable
ESR(config-if-gi)# ip address 192.168.2.2/24
ESR(config-if-gi)# do com
ESR(config-if-gi)# do conf
```

Произведем настройку PE1 и PE2. Анонсирование сервисных меток возложим на протокол BGP (Kompella mode):

PE1

```
ESR(config)# hostname PE1
ESR(config)# system jumbo-frames
ESR(config)# router bgp log-neighbor-changes
ESR(config)# router bgp 65500
ESR(config-bgp)# neighbor 10.10.1.2
ESR(config-bgp-neighbor)# remote-as 65500
ESR(config-bgp-neighbor)# update-source 10.10.1.1
ESR(config-bgp-neighbor)# address-family l2vpn vpls
ESR(config-bgp-neighbor-af)# send-community extended
ESR(config-bgp-neighbor-af)# enable
ESR(config-bgp-neighbor-af)# exit
ESR(config-bgp-neighbor)# enable
ESR(config-bgp-neighbor)# exit
ESR(config-bgp)# enable
ESR(config-bgp)# exit
ESR(config)#
ESR(config)# router ospf 1
ESR(config-ospf)# area 0.0.0.0
ESR(config-ospf-area)# enable
ESR(config-ospf-area)# exit
ESR(config-ospf)# enable
ESR(config-ospf)# exit
ESR(config)#
ESR(config)# bridge 100
ESR(config-bridge)# enable
ESR(config-bridge)# exit
ESR(config)# bridge 200
ESR(config-bridge)# enable
ESR(config-bridge)# exit
ESR(config)#
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-subif)# description "to CE1"
ESR(config-subif)# bridge-group 100
ESR(config-subif)# exit
ESR(config)# interface gigabitethernet 1/0/1.200
ESR(config-subif)# description "to CE2"
ESR(config-subif)# bridge-group 200
ESR(config-subif)# exit
ESR(config)# interface gigabitethernet 1/0/2
ESR(config-if-gi)# mtu 1522
ESR(config-if-gi)# ip firewall disable
ESR(config-if-gi)# ip address 10.100.0.1/30
ESR(config-if-gi)# ip ospf instance 1
ESR(config-if-gi)# ip ospf
ESR(config-if-gi)# exit
ESR(config)# interface loopback 1
ESR(config-loopback)# ip address 10.10.1.1/32
ESR(config-loopback)# ip ospf instance 1
ESR(config-loopback)# ip ospf
ESR(config-loopback)# exit
ESR(config)# mpls
ESR(config-mpls)# ldp
ESR(config-ldp)# router-id 10.10.1.1
ESR(config-ldp)# address-family ipv4
ESR(config-ldp-af-ipv4)# interface gigabitethernet 1/0/2
ESR(config-ldp-af-ipv4-if)# exit
ESR(config-ldp-af-ipv4)# exit
ESR(config-ldp)# enable
```

```
ESR(config-ldp)# exit
ESR(config-mpls)# l2vpn
ESR(config-l2vpn)# vpls CE1
ESR(config-l2vpn-vpls)# bridge-group 100
ESR(config-l2vpn-vpls)# autodiscovery bgp
ESR(config-bgp)# vpn id 1
ESR(config-bgp)# ve id 2
ESR(config-bgp)# rd 65500:1
ESR(config-bgp)# route-target export 65500:1
ESR(config-bgp)# route-target import 65500:1
ESR(config-bgp)# exit
ESR(config-l2vpn-vpls)# enable
ESR(config-l2vpn-vpls)# exit
ESR(config-l2vpn)# vpls CE2
ESR(config-l2vpn-vpls)# bridge-group 200
ESR(config-l2vpn-vpls)# autodiscovery bgp
ESR(config-bgp)# vpn id 2
ESR(config-bgp)# ve id 2
ESR(config-bgp)# rd 65500:2
ESR(config-bgp)# route-target export 65500:2
ESR(config-bgp)# route-target import 65500:2
ESR(config-bgp)# exit
ESR(config-l2vpn-vpls)# enable
ESR(config-l2vpn-vpls)# exit
ESR(config-l2vpn)# exit
ESR(config-mpls)# forwarding interface gigabitethernet 1/0/2
ESR(config-mpls)# exit
ESR(config)# do com
ESR(config)# do conf
```

PE2

```
ESR(config)# hostname ESR
ESR(config)# system jumbo-frames
ESR(config)#
ESR(config)# router bgp log-neighbor-changes
ESR(config)# router bgp 65500
ESR(config-bgp)# router-id 10.11.1.1
ESR(config-bgp)# neighbor 10.11.1.2
ESR(config-bgp-neighbor)# remote-as 65500
ESR(config-bgp-neighbor)# update-source 10.11.1.1
ESR(config-bgp-neighbor)# address-family l2vpn vpls
ESR(config-bgp-neighbor-af)# send-community extended
ESR(config-bgp-neighbor-af)# enable
ESR(config-bgp-neighbor-af)# exit
ESR(config-bgp-neighbor)# enable
ESR(config-bgp-neighbor)# exit
ESR(config-bgp)# enable
ESR(config-bgp)# exit
ESR(config)#
ESR(config)# router ospf 1
ESR(config-ospf)# area 0.0.0.0
ESR(config-ospf-area)# enable
ESR(config-ospf-area)# exit
ESR(config-ospf)# enable
ESR(config-ospf)# exit
ESR(config)#
ESR(config)# bridge 100
ESR(config-bridge)# enable
ESR(config-bridge)# exit
ESR(config)# bridge 200
ESR(config-bridge)# enable
ESR(config-bridge)# exit
ESR(config)#
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-subif)# description "to CE3"
ESR(config-subif)# bridge-group 100
ESR(config-subif)# exit
ESR(config)# interface gigabitethernet 1/0/1.200
ESR(config-subif)# description "to CE4"
ESR(config-subif)# bridge-group 200
ESR(config-subif)# exit
ESR(config)# interface gigabitethernet 1/0/2
ESR(config-if-gi)# mtu 1522
ESR(config-if-gi)# ip firewall disable
ESR(config-if-gi)# ip address 10.101.0.1/30
ESR(config-if-gi)# ip ospf instance 1
ESR(config-if-gi)# ip ospf
ESR(config-if-gi)# exit
ESR(config)# interface loopback 1
ESR(config-loopback)# ip address 10.11.1.1/32
ESR(config-loopback)# ip ospf instance 1
ESR(config-loopback)# ip ospf
ESR(config-loopback)# exit
ESR(config)# mpls
ESR(config-mpls)# ldp
ESR(config-ldp)# router-id 10.11.1.1
ESR(config-ldp)# address-family ipv4
ESR(config-ldp-af-ipv4)# interface gigabitethernet 1/0/2
ESR(config-ldp-af-ipv4-if)# exit
```

```
ESR(config-ldp-af-ipv4)# exit
ESR(config-ldp)# enable
ESR(config-ldp)# exit
ESR(config-mpls)# l2vpn
ESR(config-l2vpn)# vpls CE1
ESR(config-l2vpn-vpls)# bridge-group 100
ESR(config-l2vpn-vpls)# autodiscovery bgp
ESR(config-bgp)# vpn id 1
ESR(config-bgp)# ve id 2
ESR(config-bgp)# rd 65500:1
ESR(config-bgp)# route-target export 65500:1
ESR(config-bgp)# route-target import 65500:1
ESR(config-bgp)# exit
ESR(config-l2vpn-vpls)# enable
ESR(config-l2vpn-vpls)# exit
ESR(config-l2vpn)# vpls CE2
ESR(config-l2vpn-vpls)# bridge-group 200
ESR(config-l2vpn-vpls)# autodiscovery bgp
ESR(config-bgp)# vpn id 2
ESR(config-bgp)# ve id 2
ESR(config-bgp)# rd 65500:2
ESR(config-bgp)# route-target export 65500:2
ESR(config-bgp)# route-target import 65500:2
ESR(config-bgp)# exit
ESR(config-l2vpn-vpls)# enable
ESR(config-l2vpn-vpls)# exit
ESR(config-l2vpn)# exit
ESR(config-mpls)# forwarding interface gigabitethernet 1/0/2
ESR(config-mpls)# exit
ESR(config)# do com
ESR(config)# do conf
```

Настроим ASBR1 и ASBR2. Для разделения трафика от CE1 и CE2 в сторону ASBR2 сделаем интерфейс gi1/0/1 транковым. Vlan 100 и 200 будут предназначены для трафика от CE1 и CE2 соответственно:

ASBR1

```
ESR(config)# hostname ASBR1
ESR(config)#
ESR(config)# system jumbo-frames
ESR(config)#
ESR(config)# vlan 100,200
ESR(config-vlan)# exit
ESR(config)#
ESR(config)# router bgp 65500
ESR(config-bgp)# router-id 10.10.1.2
ESR(config-bgp)# neighbor 10.10.1.1
ESR(config-bgp-neighbor)# remote-as 65500
ESR(config-bgp-neighbor)# update-source 10.10.1.2
ESR(config-bgp-neighbor)# address-family l2vpn vpls
ESR(config-bgp-neighbor-af)# send-community extended
ESR(config-bgp-neighbor-af)# enable
ESR(config-bgp-neighbor-af)# exit
ESR(config-bgp-neighbor)# enable
ESR(config-bgp-neighbor)# exit
ESR(config-bgp)# enable
ESR(config-bgp)# exit
ESR(config)#
ESR(config)# router ospf 1
ESR(config-ospf)# area 0.0.0.0
ESR(config-ospf-area)# enable
ESR(config-ospf-area)# exit
ESR(config-ospf)# enable
ESR(config-ospf)# exit
ESR(config)#
ESR(config)# bridge 10
ESR(config-bridge)# vlan 100
ESR(config-bridge)# enable
ESR(config-bridge)# exit
ESR(config)# bridge 20
ESR(config-bridge)# vlan 200
ESR(config-bridge)# enable
ESR(config-bridge)# exit
ESR(config)#
ESR(config)# interface gigabitethernet 1/0/1
ESR(config-if-gi)# description "to ASBR2"
ESR(config-if-gi)# mode switchport
ESR(config-if-gi)# spanning-tree disable
ESR(config-if-gi)# switchport forbidden default-vlan
ESR(config-if-gi)# switchport mode trunk
ESR(config-if-gi)# switchport trunk allowed vlan add 100,200
ESR(config-if-gi)# exit
ESR(config)# interface gigabitethernet 1/0/2
ESR(config-if-gi)# description "to PE1"
ESR(config-if-gi)# mtu 1522
ESR(config-if-gi)# ip firewall disable
ESR(config-if-gi)# ip address 10.100.0.2/30
ESR(config-if-gi)# ip ospf instance 1
ESR(config-if-gi)# ip ospf
ESR(config-if-gi)# exit
ESR(config)# interface loopback 1
ESR(config-loopback)# ip address 10.10.1.2/32
ESR(config-loopback)# ip ospf instance 1
ESR(config-loopback)# ip ospf
ESR(config-loopback)# exit
```

```
ESR(config)# mpls
ESR(config-mpls)# ldp
ESR(config-ldp)# router-id 10.10.1.2
ESR(config-ldp)# address-family ipv4
ESR(config-ldp-af-ipv4)# interface gigabitethernet 1/0/2
ESR(config-ldp-af-ipv4-if)# exit
ESR(config-ldp-af-ipv4)# exit
ESR(config-ldp)# enable
ESR(config-ldp)# exit
ESR(config-mpls)# l2vpn
ESR(config-l2vpn)# vpls CE1
ESR(config-l2vpn-vpls)# bridge-group 10
ESR(config-l2vpn-vpls)# autodiscovery bgp
ESR(config-bgp)# vpn id 1
ESR(config-bgp)# ve id 1
ESR(config-bgp)# rd 65500:1
ESR(config-bgp)# route-target export 65500:1
ESR(config-bgp)# route-target import 65500:1
ESR(config-bgp)# exit
ESR(config-l2vpn-vpls)# enable
ESR(config-l2vpn-vpls)# exit
ESR(config-l2vpn)# vpls CE2
ESR(config-l2vpn-vpls)# bridge-group 20
ESR(config-l2vpn-vpls)# autodiscovery bgp
ESR(config-bgp)# vpn id 2
ESR(config-bgp)# ve id 1
ESR(config-bgp)# rd 65500:2
ESR(config-bgp)# route-target export 65500:2
ESR(config-bgp)# route-target import 65500:2
ESR(config-bgp)# exit
ESR(config-l2vpn-vpls)# enable
ESR(config-l2vpn-vpls)# exit
ESR(config-l2vpn)# exit
ESR(config-mpls)# forwarding interface gigabitethernet 1/0/2
ESR(config-mpls)# exit
ESR(config)# do com
ESR(config)# do conf
```

ASBR2

```
ESR(config)# hostname ASBR2
ESR(config)#
ESR(config)# system jumbo-frames
ESR(config)#
ESR(config)# vlan 100,200
ESR(config-vlan)# exit
ESR(config)#
ESR(config)# router bgp 65500
ESR(config-bgp)# router-id 10.10.1.2
ESR(config-bgp)# neighbor 10.10.1.1
ESR(config-bgp-neighbor)# remote-as 65500
ESR(config-bgp-neighbor)# update-source 10.10.1.2
ESR(config-bgp-neighbor)# address-family l2vpn vpls
ESR(config-bgp-neighbor-af)# send-community extended
ESR(config-bgp-neighbor-af)# enable
ESR(config-bgp-neighbor-af)# exit
ESR(config-bgp-neighbor)# enable
ESR(config-bgp-neighbor)# exit
ESR(config-bgp)# enable
ESR(config-bgp)# exit
ESR(config)#
ESR(config)# router ospf 1
ESR(config-ospf)# area 0.0.0.0
ESR(config-ospf-area)# enable
ESR(config-ospf-area)# exit
ESR(config-ospf)# enable
ESR(config-ospf)# exit
ESR(config)#
ESR(config)# bridge 10
ESR(config-bridge)# vlan 100
ESR(config-bridge)# enable
ESR(config-bridge)# exit
ESR(config)# bridge 20
ESR(config-bridge)# vlan 200
ESR(config-bridge)# enable
ESR(config-bridge)# exit
ESR(config)#
ESR(config)# interface gigabitethernet 1/0/1
ESR(config-if-gi)# description "to ASBR1"
ESR(config-if-gi)# mode switchport
ESR(config-if-gi)# spanning-tree disable
ESR(config-if-gi)# switchport forbidden default-vlan
ESR(config-if-gi)# switchport mode trunk
ESR(config-if-gi)# switchport trunk allowed vlan add 100,200
ESR(config-if-gi)# exit
ESR(config)# interface gigabitethernet 1/0/2
ESR(config-if-gi)# description "to PE1"
ESR(config-if-gi)# mtu 1522
ESR(config-if-gi)# ip firewall disable
ESR(config-if-gi)# ip address 10.100.0.2/30
ESR(config-if-gi)# ip ospf instance 1
ESR(config-if-gi)# ip ospf
ESR(config-if-gi)# exit
ESR(config)# interface loopback 1
ESR(config-loopback)# ip address 10.10.1.2/32
ESR(config-loopback)# ip ospf instance 1
ESR(config-loopback)# ip ospf
ESR(config-loopback)# exit
```

```
ESR(config)# mpls
ESR(config-mpls)# ldp
ESR(config-ldp)# router-id 10.10.1.2
ESR(config-ldp)# address-family ipv4
ESR(config-ldp-af-ipv4)# interface gigabitethernet 1/0/2
ESR(config-ldp-af-ipv4-if)# exit
ESR(config-ldp-af-ipv4)# exit
ESR(config-ldp)# enable
ESR(config-ldp)# exit
ESR(config-mpls)# l2vpn
ESR(config-l2vpn)# vpls CE1
ESR(config-l2vpn-vpls)# bridge-group 10
ESR(config-l2vpn-vpls)# autodiscovery bgp
ESR(config-bgp)# vpn id 1
ESR(config-bgp)# ve id 1
ESR(config-bgp)# rd 65500:1
ESR(config-bgp)# route-target export 65500:1
ESR(config-bgp)# route-target import 65500:1
ESR(config-bgp)# exit
ESR(config-l2vpn-vpls)# enable
ESR(config-l2vpn-vpls)# exit
ESR(config-l2vpn)# vpls CE2
ESR(config-l2vpn-vpls)# bridge-group 20
ESR(config-l2vpn-vpls)# autodiscovery bgp
ESR(config-bgp)# vpn id 2
ESR(config-bgp)# ve id 1
ESR(config-bgp)# rd 65500:2
ESR(config-bgp)# route-target export 65500:2
ESR(config-bgp)# route-target import 65500:2
ESR(config-bgp)# exit
ESR(config-l2vpn-vpls)# enable
ESR(config-l2vpn-vpls)# exit
ESR(config-l2vpn)# exit
ESR(config-mpls)# forwarding interface gigabitethernet 1/0/2
ESR(config-mpls)# exit
ESR(config)# do com
ESR(config)# do conf
```

Проверим назначение меток, статус сервисов, а также сетевую доступность между CE:

Информация о метках

```
ASBR2# sh bgp l2vpn vpls all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes Route Distinguisher   VID   VBO   VBS   Next hop        Metric     LocPrf     Weight Path
----- --------------------- ----- ----- ----- --------------- ---------- ---------- ------
-------------------
*>i   65500:1               2     1     10    10.11.1.1       --         100        0      i
*>i   65500:2               2     1     10    10.11.1.1       --         100        0      i
*>    65500:1               1     1     10    --              --         --         --
*>    65500:2               1     1     10    --              --         --         --

ASBR2# sh mpls forwarding-table
Local    Outgoing Prefix                                    Outgoing         Next Hop
label    label    or tunnel ID                              Interface
-------- -------- ----------------------------------------- ----------------
---------------------------------------
56       imp-null 10.11.1.1/32                              gi1/0/2          10.101.0.1
47       37       PW ID 1                                   --               10.11.1.1
37       47       PW ID 2                                   --               10.11.1.1
```

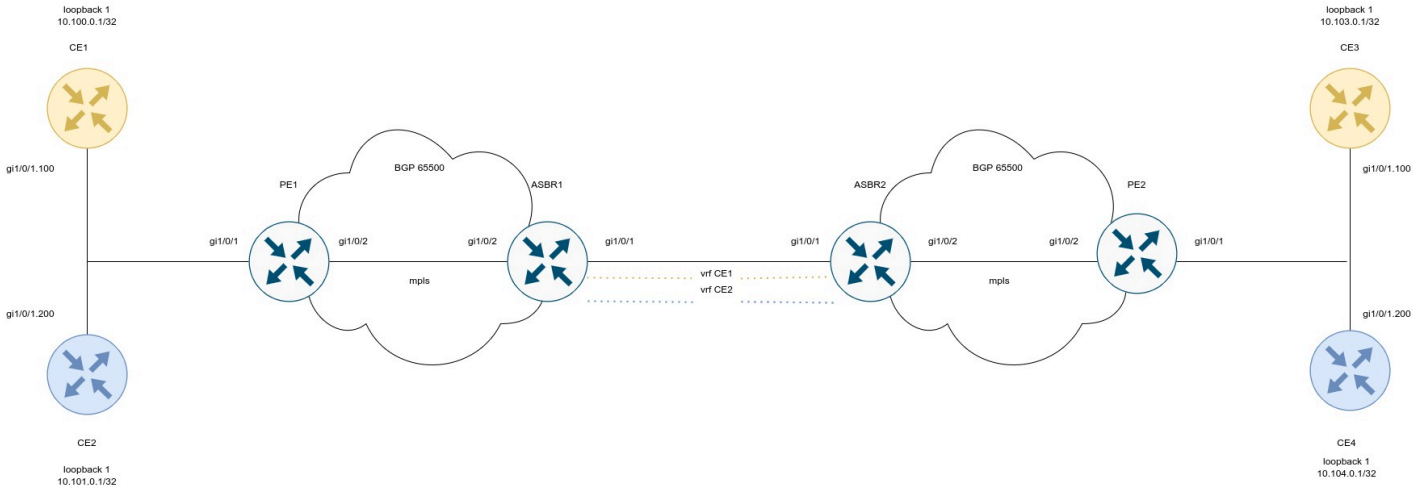
Статус сервисов

```
ASBR2# sh mpls l2vpn vpls
VPLS: CE1
    bridge 10:
        MTU:    1500
        Status: Up
    PWs:
      PW ID 1, Neighbor 10.11.1.1:
        MTU:         1500
        Last change: 00:16:59
        Status:      Up
VPLS: CE2
    bridge 20:
        MTU:    1500
        Status: Up
    PWs:
      PW ID 2, Neighbor 10.11.1.1:
        MTU:         1500
        Last change: 00:16:59
        Status:      Up
```

Проверка сетевой доступности

```
CE1# ping 192.168.1.2 detailed
PING 192.168.1.2 (192.168.1.2) 56 bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=0 time=1.08 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=0 time=1.06 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=0 time=1.01 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=0 time=0.971 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=0 time=0.972 ms

CE2# ping 192.168.2.2 detailed  packets
PING 192.168.2.2 (192.168.2.2) 56 bytes of data.
64 bytes from 192.168.2.2: icmp_seq=1 ttl=0 time=1.17 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=0 time=0.972 ms
64 bytes from 192.168.2.2: icmp_seq=3 ttl=0 time=0.960 ms
64 bytes from 192.168.2.2: icmp_seq=4 ttl=0 time=1.04 ms
64 bytes from 192.168.2.2: icmp_seq=5 ttl=0 time=0.976 ms

ASBR2# sh mac address-table bridge 10
VID     MAC Address          Interface                       Type
-----   ------------------   -----------------------------   -------
--      e4:5a:d4:01:b9:73    vlan 100                        Dynamic
--      e4:5a:d4:a1:34:61    dypseudowire 1_10.11.1.1        Dynamic
2 valid mac entries
ASBR2# sh mac address-table bridge 20
VID     MAC Address          Interface                       Type
-----   ------------------   -----------------------------   -------
--      e4:5a:d4:01:c1:80    vlan 200                        Dynamic
--      e4:5a:d4:a1:34:61    dypseudowire 2_10.11.1.1        Dynamic
2 valid mac entries
```

14.11.2 L3VPN



Настроим CE:

CE1

```
ESR(config)# hostname CE1
ESR(config)#
ESR(config)# route-map BGP
ESR(config-route-map)# rule 1
ESR(config-route-map-rule)# exit
ESR(config-route-map)# exit
ESR(config)# router bgp 65501
ESR(config-bgp)# neighbor 192.168.1.2
ESR(config-bgp-neighbor)# remote-as 65500
ESR(config-bgp-neighbor)# address-family ipv4 unicast
ESR(config-bgp-neighbor-af)# route-map BGP out
ESR(config-bgp-neighbor-af)# enable
ESR(config-bgp-neighbor-af)# exit
ESR(config-bgp-neighbor)# enable
ESR(config-bgp-neighbor)# exit
ESR(config-bgp)# address-family ipv4 unicast
ESR(config-bgp-af)# network 10.110.0.1/32
ESR(config-bgp-af)# exit
ESR(config-bgp)# enable
ESR(config-bgp)# exit
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-subif)# ip firewall disable
ESR(config-subif)# ip address 192.168.1.1/30
ESR(config-subif)# exit
ESR(config)# interface loopback 1
ESR(config-loopback)# ip address 10.110.0.1/32
ESR(config-loopback)# exit
ESR(config)# do com
ESR(config)# do conf
```

CE2

```
ESR(config)# hostname CE2
ESR(config)#
ESR(config)# route-map BGP
ESR(config-route-map)# rule 1
ESR(config-route-map-rule)# exit
ESR(config-route-map)# exit
ESR(config)# router bgp 65501
ESR(config-bgp)# neighbor 192.168.2.2
ESR(config-bgp-neighbor)# remote-as 65500
ESR(config-bgp-neighbor)# address-family ipv4 unicast
ESR(config-bgp-neighbor-af)# route-map BGP out
ESR(config-bgp-neighbor-af)# enable
ESR(config-bgp-neighbor-af)# exit
ESR(config-bgp-neighbor)# enable
ESR(config-bgp-neighbor)# exit
ESR(config-bgp)# address-family ipv4 unicast
ESR(config-bgp-af)# network 10.112.0.1/32
ESR(config-bgp-af)# exit
ESR(config-bgp)# enable
ESR(config-bgp)# exit
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-subif)# ip firewall disable
ESR(config-subif)# ip address 192.168.2.1/30
ESR(config-subif)# exit
ESR(config)#
ESR(config)# interface loopback 1
ESR(config-loopback)# ip address 10.112.0.1/32
ESR(config-loopback)# exit
ESR(config)# do com
ESR(config)# do conf
```

CE3

```
ESR(config)# hostname CE3
ESR(config)#
ESR(config)# route-map BGP
ESR(config-route-map)#   rule 1
ESR(config-route-map-rule)#   exit
ESR(config-route-map)# exit
ESR(config)# router bgp 65501
ESR(config-bgp)# neighbor 192.168.3.2
ESR(config-bgp-neighbor)# remote-as 65500
ESR(config-bgp-neighbor)# address-family ipv4 unicast
ESR(config-bgp-neighbor-af)# route-map BGP out
ESR(config-bgp-neighbor-af)# enable
ESR(config-bgp-neighbor-af)# exit
ESR(config-bgp-neighbor)# enable
ESR(config-bgp-neighbor)# exit
ESR(config-bgp)# address-family ipv4 unicast
ESR(config-bgp-af)# network 10.113.0.1/32
ESR(config-bgp-af)# exit
ESR(config-bgp)# enable
ESR(config-bgp)# exit
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-subif)# ip firewall disable
ESR(config-subif)# ip address 192.168.3.1/30
ESR(config-subif)# exit
ESR(config)#
ESR(config)# interface loopback 1
ESR(config-loopback)# ip address 10.113.0.1/32
ESR(config-loopback)# exit
ESR(config)# do com
ESR(config)# do conf
```

CE4

```
ESR(config)# hostname CE4
ESR(config)#
ESR(config)# route-map BGP
ESR(config-route-map)# rule 1
ESR(config-route-map-rule)# exit
ESR(config-route-map)# exit
ESR(config)# router bgp 65501
ESR(config-bgp)# neighbor 192.168.4.2
ESR(config-bgp-neighbor)# remote-as 65500
ESR(config-bgp-neighbor)# address-family ipv4 unicast
ESR(config-bgp-neighbor-af)# route-map BGP out
ESR(config-bgp-neighbor-af)# enable
ESR(config-bgp-neighbor-af)# exit
ESR(config-bgp-neighbor)# enable
ESR(config-bgp-neighbor)# exit
ESR(config-bgp)# address-family ipv4 unicast
ESR(config-bgp-af)# network 10.114.0.1/32
ESR(config-bgp-af)# exit
ESR(config-bgp)# enable
ESR(config-bgp)# exit
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-subif)# ip firewall disable
ESR(config-subif)# ip address 192.168.4.1/30
ESR(config-subif)# exit
ESR(config)#
ESR(config)# interface loopback 1
ESR(config-loopback)# ip address 10.114.0.1/32
ESR(config-loopback)# exit
ESR(config)# do com
ESR(config)# do conf
```

Произведем настройку PE1 и PE2:

PE1

```
ESR(config)# hostname PE1
ESR(config)#
ESR(config)# ip vrf CE1
ESR(config-vrf)# ip protocols bgp max-routes 100
ESR(config-vrf)# rd 65500:1
ESR(config-vrf)# route-target export 65500:1
ESR(config-vrf)# route-target import 65500:1
ESR(config-vrf)# exit
ESR(config)# ip vrf CE2
ESR(config-vrf)# ip protocols bgp max-routes 100
ESR(config-vrf)# rd 65500:2
ESR(config-vrf)# route-target export 65500:2
ESR(config-vrf)# route-target import 65500:2
ESR(config-vrf)# exit
ESR(config)#
ESR(config)# system jumbo-frames
ESR(config)#
ESR(config)# route-map BGP
ESR(config-route-map)# rule 1
ESR(config-route-map-rule)# exit
ESR(config-route-map)# exit
ESR(config)# router bgp log-neighbor-changes
ESR(config)# router bgp 65500
ESR(config-bgp)# neighbor 10.10.1.2
ESR(config-bgp-neighbor)# remote-as 65500
ESR(config-bgp-neighbor)# update-source 10.10.1.1
ESR(config-bgp-neighbor)# address-family vpnv4 unicast
ESR(config-bgp-neighbor-af)# send-community extended
ESR(config-bgp-neighbor-af)# enable
ESR(config-bgp-neighbor-af)# exit
ESR(config-bgp-neighbor)# enable
ESR(config-bgp-neighbor)# exit
ESR(config-bgp)# enable
ESR(config-bgp)# vrf CE1
ESR(config-bgp-vrf)# neighbor 192.168.1.1
ESR(config-bgp-vrf-neighbor)# remote-as 65501
ESR(config-bgp-vrf-neighbor)# address-family ipv4 unicast
ESR(config-bgp-neighbor-af-vrf)# route-map BGP out
ESR(config-bgp-neighbor-af-vrf)# enable
ESR(config-bgp-neighbor-af-vrf)# exit
ESR(config-bgp-vrf-neighbor)# enable
ESR(config-bgp-vrf-neighbor)# exit
ESR(config-bgp-vrf)# address-family ipv4 unicast
ESR(config-bgp-vrf-af)# redistribute bgp 65500 route-map BGP
ESR(config-bgp-vrf-af)# exit
ESR(config-bgp-vrf)# enable
ESR(config-bgp-vrf)# exit
ESR(config-bgp)# vrf CE2
ESR(config-bgp-vrf)# neighbor 192.168.2.1
ESR(config-bgp-vrf-neighbor)# remote-as 65501
ESR(config-bgp-vrf-neighbor)# address-family ipv4 unicast
ESR(config-bgp-neighbor-af-vrf)# route-map BGP out
ESR(config-bgp-neighbor-af-vrf)# enable
ESR(config-bgp-neighbor-af-vrf)# exit
ESR(config-bgp-vrf-neighbor)# enable
ESR(config-bgp-vrf-neighbor)# exit
ESR(config-bgp-vrf)# address-family ipv4 unicast
ESR(config-bgp-vrf-af)# redistribute bgp 65500 route-map BGP
```

```
ESR(config-bgp-vrf-af)# exit
ESR(config-bgp-vrf)# enable
ESR(config-bgp-vrf)# exit
ESR(config-bgp)# exit
ESR(config)#
ESR(config)# router ospf 1
ESR(config-ospf)# area 0.0.0.0
ESR(config-ospf-area)# enable
ESR(config-ospf-area)# exit
ESR(config-ospf)# enable
ESR(config-ospf)# exit
ESR(config)#
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-subif)# ip vrf forwarding CE1
ESR(config-subif)# description "to CE1"
ESR(config-subif)# ip firewall disable
ESR(config-subif)# ip address 192.168.1.2/30
ESR(config-subif)# exit
ESR(config)# interface gigabitethernet 1/0/1.200
ESR(config-subif)# ip vrf forwarding CE2
ESR(config-subif)# description "to CE2"
ESR(config-subif)# ip firewall disable
ESR(config-subif)# ip address 192.168.2.2/30
ESR(config-subif)# exit
ESR(config)# interface gigabitethernet 1/0/2
ESR(config-if-gi)# mtu 1522
ESR(config-if-gi)# ip firewall disable
ESR(config-if-gi)# ip address 10.100.0.1/30
ESR(config-if-gi)# ip ospf instance 1
ESR(config-if-gi)# ip ospf
ESR(config-if-gi)# exit
ESR(config)# interface loopback 1
ESR(config-loopback)# ip address 10.10.1.1/32
ESR(config-loopback)# ip ospf instance 1
ESR(config-loopback)# ip ospf
ESR(config-loopback)# exit
ESR(config)# mpls
ESR(config-mpls)# ldp
ESR(config-ldp)# router-id 10.10.1.1
ESR(config-ldp)# address-family ipv4
ESR(config-ldp-af-ipv4)# interface gigabitethernet 1/0/2
ESR(config-ldp-af-ipv4-if)# exit
ESR(config-ldp-af-ipv4)# exit
ESR(config-ldp)# enable
ESR(config-ldp)# exit
ESR(config-mpls)# forwarding interface gigabitethernet 1/0/2
ESR(config-mpls)# exit
ESR(config)# do com
ESR(config)# do conf
```

PE2

```
ESR(config)# hostname PE2
ESR(config)#
ESR(config)# ip vrf CE1
ESR(config-vrf)# ip protocols bgp max-routes 100
ESR(config-vrf)# rd 65500:1
ESR(config-vrf)# route-target export 65500:1
ESR(config-vrf)# route-target import 65500:1
ESR(config-vrf)# exit
ESR(config)# ip vrf CE2
ESR(config-vrf)# ip protocols bgp max-routes 100
ESR(config-vrf)# rd 65500:2
ESR(config-vrf)# route-target export 65500:2
ESR(config-vrf)# route-target import 65500:2
ESR(config-vrf)# exit
ESR(config)#
ESR(config)# system jumbo-frames
ESR(config)#
ESR(config)# route-map BGP
ESR(config-route-map)# rule 1
ESR(config-route-map-rule)# exit
ESR(config-route-map)# exit
ESR(config)# router bgp log-neighbor-changes
ESR(config)# router bgp 65500
ESR(config-bgp)# router-id 10.11.1.1
ESR(config-bgp)# neighbor 10.11.1.2
ESR(config-bgp-neighbor)# remote-as 65500
ESR(config-bgp-neighbor)# update-source 10.11.1.1
ESR(config-bgp-neighbor)# address-family vpnv4 unicast
ESR(config-bgp-neighbor-af)# send-community extended
ESR(config-bgp-neighbor-af)# enable
ESR(config-bgp-neighbor-af)# exit
ESR(config-bgp-neighbor)# enable
ESR(config-bgp-neighbor)# exit
ESR(config-bgp)# enable
ESR(config-bgp)# vrf CE1
ESR(config-bgp-vrf)# neighbor 192.168.3.1
ESR(config-bgp-vrf-neighbor)# remote-as 65501
ESR(config-bgp-vrf-neighbor)# address-family ipv4 unicast
ESR(config-bgp-neighbor-af-vrf)# route-map BGP out
ESR(config-bgp-neighbor-af-vrf)# enable
ESR(config-bgp-neighbor-af-vrf)# exit
ESR(config-bgp-vrf-neighbor)# enable
ESR(config-bgp-vrf-neighbor)# exit
ESR(config-bgp-vrf)# address-family ipv4 unicast
ESR(config-bgp-vrf-af)# redistribute bgp 65500 route-map BGP
ESR(config-bgp-vrf-af)# exit
ESR(config-bgp-vrf)# enable
ESR(config-bgp-vrf)# exit
ESR(config-bgp)# vrf CE2
ESR(config-bgp-vrf)# neighbor 192.168.4.1
ESR(config-bgp-vrf-neighbor)# remote-as 65501
ESR(config-bgp-vrf-neighbor)# address-family ipv4 unicast
ESR(config-bgp-neighbor-af-vrf)# route-map BGP out
ESR(config-bgp-neighbor-af-vrf)# enable
ESR(config-bgp-neighbor-af-vrf)# exit
ESR(config-bgp-vrf-neighbor)# enable
ESR(config-bgp-vrf-neighbor)# exit
ESR(config-bgp-vrf)# address-family ipv4 unicast
```

```
ESR(config-bgp-vrf-af)# redistribute bgp 65500 route-map BGP
ESR(config-bgp-vrf-af)# exit
ESR(config-bgp-vrf)# enable
ESR(config-bgp-vrf)#exit
ESR(config-bgp)# exit
ESR(config)#
ESR(config)# router ospf 1
ESR(config-ospf)# area 0.0.0.0
ESR(config-ospf-area)# enable
ESR(config-ospf-area)# exit
ESR(config-ospf)# enable
ESR(config-ospf)# exit
ESR(config)#
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-subif)# ip vrf forwarding CE1
ESR(config-subif)# description "to CE3"
ESR(config-subif)# ip firewall disable
ESR(config-subif)# ip address 192.168.3.2/30
ESR(config-subif)# exit
ESR(config)# interface gigabitethernet 1/0/1.200
ESR(config-subif)# ip vrf forwarding CE2
ESR(config-subif)# description "to CE4"
ESR(config-subif)# ip firewall disable
ESR(config-subif)# ip address 192.168.4.2/30
ESR(config-subif)# exit
ESR(config)# interface gigabitethernet 1/0/2
ESR(config-if-gi)# mtu 1522
ESR(config-if-gi)# ip firewall disable
ESR(config-if-gi)# ip address 10.101.0.1/30
ESR(config-if-gi)# ip ospf instance 1
ESR(config-if-gi)# ip ospf
ESR(config-if-gi)# exit
ESR(config)# interface loopback 1
ESR(config-loopback)# ip address 10.11.1.1/32
ESR(config-loopback)# ip ospf instance 1
ESR(config-loopback)# ip ospf
ESR(config-loopback)# exit
ESR(config)# mpls
ESR(config-mpls)# ldp
ESR(config-ldp)# router-id 10.11.1.1
ESR(config-ldp)# address-family ipv4
ESR(config-ldp-af-ipv4)# interface gigabitethernet 1/0/2
ESR(config-ldp-af-ipv4-if)# exit
ESR(config-ldp-af-ipv4)# exit
ESR(config-ldp)# enable
ESR(config-ldp)# exit
ESR(config-mpls)# forwarding interface gigabitethernet 1/0/2
ESR(config-mpls)# exit
ESR(config)# do com
ESR(config)# do conf
```

Настроим ASBR1 и ASBR2. Для передачи маршрутной информации между ними воспользуемся протоколом OSPF в соответствующих VRF:

ASBR1

```
ESR(config)# hostname ASBR1
ESR(config)#
ESR(config)# ip vrf CE1
ESR(config-vrf)# ip protocols ospf max-routes 100
ESR(config-vrf)# rd 65500:1
ESR(config-vrf)# route-target export 65500:1
ESR(config-vrf)# route-target import 65500:1
ESR(config-vrf)# exit
ESR(config)# ip vrf CE2
ESR(config-vrf)# ip protocols ospf max-routes 100
ESR(config-vrf)# rd 65500:2
ESR(config-vrf)# route-target export 65500:2
ESR(config-vrf)# route-target import 65500:2
ESR(config-vrf)# exit
ESR(config)#
ESR(config)# system jumbo-frames
ESR(config)#
ESR(config)# vlan 100,200
ESR(config-vlan)# exit
ESR(config)#
ESR(config)# router bgp 65500
ESR(config-bgp)# router-id 10.10.1.2
ESR(config-bgp)# neighbor 10.10.1.1
ESR(config-bgp-neighbor)# remote-as 65500
ESR(config-bgp-neighbor)# update-source 10.10.1.2
ESR(config-bgp-neighbor)# address-family vpnv4 unicast
ESR(config-bgp-neighbor-af)# send-community extended
ESR(config-bgp-neighbor-af)# enable
ESR(config-bgp-neighbor-af)# exit
ESR(config-bgp-neighbor)# enable
ESR(config-bgp-neighbor)# exit
ESR(config-bgp)# enable
ESR(config-bgp)# vrf CE1
ESR(config-bgp-vrf)# address-family ipv4 unicast
ESR(config-bgp-vrf-af)# redistribute ospf 1 intra-area inter-area external1 external2
ESR(config-bgp-vrf-af)# exit
ESR(config-bgp-vrf)# exit
ESR(config-bgp)# vrf CE2
ESR(config-bgp-vrf)# address-family ipv4 unicast
ESR(config-bgp-vrf-af)# redistribute ospf 1 intra-area inter-area external1 external2
ESR(config-bgp-vrf-af)# exit
ESR(config-bgp-vrf)# exit
ESR(config-bgp)# exit
ESR(config)#
ESR(config)# router ospf log-adjacency-changes
ESR(config)# router ospf 1
ESR(config-ospf)#   area 0.0.0.0
ESR(config-ospf-area)# enable
ESR(config-ospf-area)# exit
ESR(config-ospf)# enable
ESR(config-ospf)# exit
ESR(config)# router ospf 1 vrf CE1
ESR(config-ospf)# redistribute bgp 65500
ESR(config-ospf)# area 0.0.0.0
ESR(config-ospf-area)# enable
ESR(config-ospf-area)# exit
ESR(config-ospf)#   enable
ESR(config-ospf)# exit
```

```
ESR(config)# router ospf 1 vrf CE2
ESR(config-ospf)# area 0.0.0.0
ESR(config-ospf-area)# enable
ESR(config-ospf-area)# exit
ESR(config-ospf)# enable
ESR(config-ospf)# exit
ESR(config)#
ESR(config)# bridge 10
ESR(config-bridge)# ip vrf forwarding CE1
ESR(config-bridge)# vlan 100
ESR(config-bridge)# ip firewall disable
ESR(config-bridge)# ip address 172.16.32.1/30
ESR(config-bridge)# ip ospf instance 1
ESR(config-bridge)# ip ospf
ESR(config-bridge)# enable
ESR(config-bridge)# exit
ESR(config)# bridge 20
ESR(config-bridge)# ip vrf forwarding CE2
ESR(config-bridge)# vlan 200
ESR(config-bridge)# ip firewall disable
ESR(config-bridge)# ip address 172.16.32.5/30
ESR(config-bridge)# ip ospf instance 1
ESR(config-bridge)# ip ospf
ESR(config-bridge)# enable
ESR(config-bridge)# exit
ESR(config)#
ESR(config)# interface gigabitethernet 1/0/1
ESR(config-if-gi)# description "to ASBR2"
ESR(config-if-gi)# mode switchport
ESR(config-if-gi)# mtu 1522
ESR(config-if-gi)# spanning-tree disable
ESR(config-if-gi)# switchport forbidden default-vlan
ESR(config-if-gi)# switchport mode trunk
ESR(config-if-gi)# switchport trunk allowed vlan add 100,200
ESR(config-if-gi)# exit
ESR(config)# interface gigabitethernet 1/0/2
ESR(config-if-gi)# description "to PE1"
ESR(config-if-gi)# mtu 1522
ESR(config-if-gi)# ip firewall disable
ESR(config-if-gi)# ip address 10.100.0.2/30
ESR(config-if-gi)# ip ospf instance 1
ESR(config-if-gi)# ip ospf
ESR(config-if-gi)# exit
ESR(config)# interface loopback 1
ESR(config-loopback)# ip address 10.10.1.2/32
ESR(config-loopback)# ip ospf instance 1
ESR(config-loopback)# ip ospf
ESR(config-loopback)# exit
ESR(config)# mpls
ESR(config-mpls)# ldp
ESR(config-ldp)# router-id 10.10.1.2
ESR(config-ldp)# address-family ipv4
ESR(config-ldp-af-ipv4)# interface gigabitethernet 1/0/2
ESR(config-ldp-af-ipv4-if)# exit
ESR(config-ldp-af-ipv4)# exit
ESR(config-ldp)# enable
ESR(config-ldp)# exit
ESR(config-mpls)# forwarding interface gigabitethernet 1/0/2
ESR(config-mpls)# exit
ESR(config)# do com
ESR(config)# do conf
```

ASBR2

```
ESR(config)# hostname ASBR2
ESR(config)#
ESR(config)# ip vrf CE1
ESR(config-vrf)# ip protocols ospf max-routes 100
ESR(config-vrf)# rd 65500:1
ESR(config-vrf)# route-target export 65500:1
ESR(config-vrf)# route-target import 65500:1
ESR(config-vrf)# exit
ESR(config)# ip vrf CE2
ESR(config-vrf)# ip protocols ospf max-routes 100
ESR(config-vrf)# rd 65500:2
ESR(config-vrf)# route-target export 65500:2
ESR(config-vrf)# route-target import 65500:2
ESR(config-vrf)# exit
ESR(config)#
ESR(config)# system jumbo-frames
ESR(config)#
ESR(config)# vlan 100,200
ESR(config-vlan)# exit
ESR(config)#
ESR(config)# router bgp 65500
ESR(config-bgp)# router-id 10.11.1.2
ESR(config-bgp)# neighbor 10.11.1.1
ESR(config-bgp-neighbor)# remote-as 65500
ESR(config-bgp-neighbor)# update-source 10.11.1.2
ESR(config-bgp-neighbor)# address-family vpnv4 unicast
ESR(config-bgp-neighbor-af)# send-community extended
ESR(config-bgp-neighbor-af)# enable
ESR(config-bgp-neighbor-af)# exit
ESR(config-bgp-neighbor)# enable
ESR(config-bgp-neighbor)# exit
ESR(config-bgp)# enable
ESR(config-bgp)# vrf CE1
ESR(config-bgp-vrf)# address-family ipv4 unicast
ESR(config-bgp-vrf-af)# redistribute ospf 1 intra-area inter-area external1 external2
ESR(config-bgp-vrf-af)# exit
ESR(config-bgp-vrf)# exit
ESR(config-bgp)# vrf CE2
ESR(config-bgp-vrf)# address-family ipv4 unicast
ESR(config-bgp-vrf-af)# redistribute ospf 1 intra-area inter-area external1 external2
ESR(config-bgp-vrf-af)# exit
ESR(config-bgp-vrf)# exit
ESR(config-bgp)# exit
ESR(config)#
ESR(config)# router ospf log-adjacency-changes
ESR(config)# router ospf 1
ESR(config-ospf)# area 0.0.0.0
ESR(config-ospf-area)# enable
ESR(config-ospf-area)# exit
ESR(config-ospf)# enable
ESR(config-ospf)# exit
ESR(config)# router ospf 1 vrf CE1
ESR(config-ospf)# redistribute bgp 65500
ESR(config-ospf)# area 0.0.0.0
ESR(config-ospf-area)# enable
ESR(config-ospf-area)# exit
ESR(config-ospf)# enable
ESR(config-ospf)# exit
```

```
ESR(config)# router ospf 1 vrf CE2
ESR(config-ospf)# redistribute bgp 65500
ESR(config-ospf)# area 0.0.0.0
ESR(config-ospf-area)# enable
ESR(config-ospf-area)# exit
ESR(config-ospf)# enable
ESR(config-ospf)# exit
ESR(config)#
ESR(config)# bridge 10
ESR(config-bridge)# ip vrf forwarding CE1
ESR(config-bridge)# vlan 100
ESR(config-bridge)# ip firewall disable
ESR(config-bridge)# ip address 172.16.32.2/30
ESR(config-bridge)# ip ospf instance 1
ESR(config-bridge)# ip ospf
ESR(config-bridge)# enable
ESR(config-bridge)# exit
ESR(config)# bridge 20
ESR(config-bridge)# ip vrf forwarding CE2
ESR(config-bridge)# vlan 200
ESR(config-bridge)# ip firewall disable
ESR(config-bridge)# ip address 172.16.32.6/30
ESR(config-bridge)# ip ospf instance 1
ESR(config-bridge)# ip ospf
ESR(config-bridge)# enable
ESR(config-bridge)# exit
ESR(config)#
ESR(config)# interface gigabitethernet 1/0/1
ESR(config-if-gi)# description "to ASBR1"
ESR(config-if-gi)# mode switchport
ESR(config-if-gi)# mtu 1522
ESR(config-if-gi)# spanning-tree disable
ESR(config-if-gi)# switchport forbidden default-vlan
ESR(config-if-gi)# switchport mode trunk
ESR(config-if-gi)#  switchport trunk allowed vlan add 100,200
ESR(config-if-gi)# exit
ESR(config)# interface gigabitethernet 1/0/2
ESR(config-if-gi)# description "to PE2"
ESR(config-if-gi)# mtu 1522
ESR(config-if-gi)# ip firewall disable
ESR(config-if-gi)# ip address 10.101.0.2/30
ESR(config-if-gi)# ip ospf instance 1
ESR(config-if-gi)# ip ospf
ESR(config-if-gi)# exit
ESR(config)# interface loopback 1
ESR(config-loopback)# ip address 10.11.1.2/32
ESR(config-loopback)# ip ospf instance 1
ESR(config-loopback)# ip ospf
ESR(config-loopback)# exit
ESR(config)# mpls
ESR(config-mpls)# ldp
ESR(config-ldp)# router-id 10.11.1.2
ESR(config-ldp)# address-family ipv4
ESR(config-ldp-af-ipv4)# interface gigabitethernet 1/0/2
ESR(config-ldp-af-ipv4-if)# exit
ESR(config-ldp-af-ipv4)# exit
ESR(config-ldp)# enable
ESR(config-ldp)# exit
ESR(config-mpls)# forwarding interface gigabitethernet 1/0/2
ESR(config-mpls)# exit
ESR(config)# do com
```

```
ESR(config)# do conf
```

Настройка завершена. Проверим распространение маршрутной информации и сетевую доступность узлов:

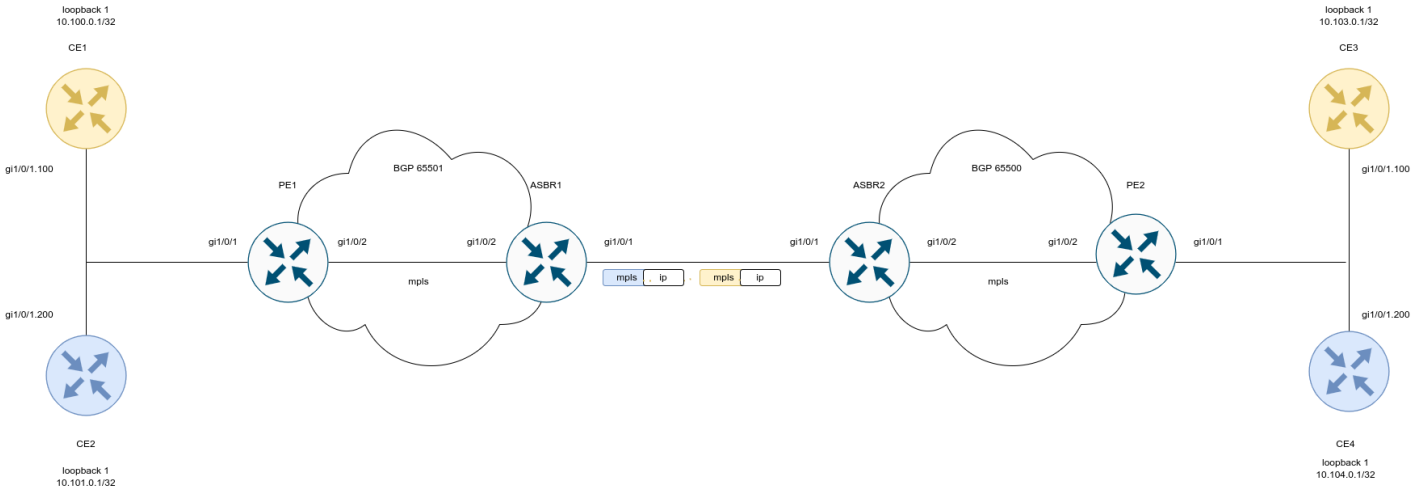
```
PE1# sh bgp vpnv4 unicast all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes Route Distinguisher   IP Prefix          Next hop        Metric     Label   LocPrf
Weight Path
----- --------------------- ------------------ --------------- ---------- ------- ----------
------ -----------------
*>    65500:1               10.110.0.1/32      --              --         37      100        --
65501 i
*>    65500:1               10.111.0.1/32      --              --         35      100        --
65501 i
*>i   65500:1               10.113.0.1/32      10.10.1.2       --         43      100        0
     ?
*>i   65500:1               10.114.0.1/32      10.10.1.2       --         48      100        0
     ?

CE1# ping 10.113.0.1 source ip 10.110.0.1 detailed
PING 10.113.0.1 (10.113.0.1) from 10.110.0.1 : 56 bytes of data.
64 bytes from 10.113.0.1: icmp_seq=1 ttl=0 time=1.31 ms
64 bytes from 10.113.0.1: icmp_seq=2 ttl=0 time=1.14 ms
64 bytes from 10.113.0.1: icmp_seq=3 ttl=0 time=1.08 ms
64 bytes from 10.113.0.1: icmp_seq=4 ttl=0 time=1.06 ms
64 bytes from 10.113.0.1: icmp_seq=5 ttl=0 time=1.16 ms
```

14.12 Inter-AS Option B

В отличие от Option A, между ASBR нет необходимости использовать VRF: при передаче трафика между ASBR будет навешиваться mpls-метка. Данная схема имеет лучшую масштабируемость.

> **В текущей реализации Option B поддержана только для VPN-IPv4 маршрутов (AFI = 1, SAFI = 128).**

14.12.1 L3VPN



Настроим CE:

CE1

```
ESR(config)# hostname CE1
ESR(config)#
ESR(config)# route-map BGP
ESR(config-route-map)# rule 1
ESR(config-route-map-rule)# exit
ESR(config-route-map)# exit
ESR(config)# router bgp 65501
ESR(config-bgp)# neighbor 192.168.1.2
ESR(config-bgp-neighbor)# remote-as 65500
ESR(config-bgp-neighbor)# address-family ipv4 unicast
ESR(config-bgp-neighbor-af)# route-map BGP out
ESR(config-bgp-neighbor-af)# enable
ESR(config-bgp-neighbor-af)# exit
ESR(config-bgp-neighbor)# enable
ESR(config-bgp-neighbor)# exit
ESR(config-bgp)# address-family ipv4 unicast
ESR(config-bgp-af)# network 10.110.0.1/32
ESR(config-bgp-af)# exit
ESR(config-bgp)# enable
ESR(config-bgp)# exit
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-subif)# ip firewall disable
ESR(config-subif)# ip address 192.168.1.1/30
ESR(config-subif)# exit
ESR(config)# interface loopback 1
ESR(config-loopback)# ip address 10.110.0.1/32
ESR(config-loopback)# exit
ESR(config)# do com
ESR(config)# do conf
```

CE2

```
ESR(config)# hostname CE2
ESR(config)#
ESR(config)# route-map BGP
ESR(config-route-map)# rule 1
ESR(config-route-map-rule)# exit
ESR(config-route-map)# exit
ESR(config)# router bgp 65501
ESR(config-bgp)# neighbor 192.168.2.2
ESR(config-bgp-neighbor)# remote-as 65500
ESR(config-bgp-neighbor)# address-family ipv4 unicast
ESR(config-bgp-neighbor-af)# route-map BGP out
ESR(config-bgp-neighbor-af)# enable
ESR(config-bgp-neighbor-af)# exit
ESR(config-bgp-neighbor)# enable
ESR(config-bgp-neighbor)# exit
ESR(config-bgp)# address-family ipv4 unicast
ESR(config-bgp-af)# network 10.112.0.1/32
ESR(config-bgp-af)# exit
ESR(config-bgp)# enable
ESR(config-bgp)# exit
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-subif)# ip firewall disable
ESR(config-subif)# ip address 192.168.2.1/30
ESR(config-subif)# exit
ESR(config)#
ESR(config)# interface loopback 1
ESR(config-loopback)# ip address 10.112.0.1/32
ESR(config-loopback)# exit
ESR(config)# do com
ESR(config)# do conf
```

CE3

```
ESR(config)# hostname CE3
ESR(config)#
ESR(config)# route-map BGP
ESR(config-route-map)# rule 1
ESR(config-route-map-rule)# exit
ESR(config-route-map)# exit
ESR(config)# router bgp 65501
ESR(config-bgp)# neighbor 192.168.3.2
ESR(config-bgp-neighbor)# remote-as 65500
ESR(config-bgp-neighbor)# address-family ipv4 unicast
ESR(config-bgp-neighbor-af)# route-map BGP out
ESR(config-bgp-neighbor-af)# enable
ESR(config-bgp-neighbor-af)# exit
ESR(config-bgp-neighbor)# enable
ESR(config-bgp-neighbor)# exit
ESR(config-bgp)# address-family ipv4 unicast
ESR(config-bgp-af)# network 10.113.0.1/32
ESR(config-bgp-af)# exit
ESR(config-bgp)# enable
ESR(config-bgp)# exit
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-subif)# ip firewall disable
ESR(config-subif)# ip address 192.168.3.1/30
ESR(config-subif)# exit
ESR(config)#
ESR(config)# interface loopback 1
ESR(config-loopback)# ip address 10.113.0.1/32
ESR(config-loopback)# exit
ESR(config)# do com
ESR(config)# do conf
```

CE4

```
ESR(config)# hostname CE4
ESR(config)#
ESR(config)# route-map BGP
ESR(config-route-map)# rule 1
ESR(config-route-map-rule)# exit
ESR(config-route-map)# exit
ESR(config)# router bgp 65501
ESR(config-bgp)# neighbor 192.168.4.2
ESR(config-bgp-neighbor)# remote-as 65500
ESR(config-bgp-neighbor)# address-family ipv4 unicast
ESR(config-bgp-neighbor-af)# route-map BGP out
ESR(config-bgp-neighbor-af)# enable
ESR(config-bgp-neighbor-af)# exit
ESR(config-bgp-neighbor)# enable
ESR(config-bgp-neighbor)# exit
ESR(config-bgp)# address-family ipv4 unicast
ESR(config-bgp-af)# network 10.114.0.1/32
ESR(config-bgp-af)# exit
ESR(config-bgp)# enable
ESR(config-bgp)# exit
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-subif)# ip firewall disable
ESR(config-subif)# ip address 192.168.4.1/30
ESR(config-subif)# exit
ESR(config)#
ESR(config)# interface loopback 1
ESR(config-loopback)# ip address 10.114.0.1/32
ESR(config-loopback)# exit
ESR(config)# do com
ESR(config)# do conf
```

Произведем настройку PE1 и PE2:

PE1

```
PE1(config)# hostname PE1
PE1(config)#
PE1(config)# ip vrf CE1
PE1(config-vrf)# ip protocols bgp max-routes 100
PE1(config-vrf)# rd 65501:1
PE1(config-vrf)# route-target export 65501:1
PE1(config-vrf)# route-target import 65501:1
PE1(config-vrf)# exit
PE1(config)# ip vrf CE2
PE1(config-vrf)# ip protocols bgp max-routes 100
PE1(config-vrf)# rd 65501:2
PE1(config-vrf)# route-target export 65501:2
PE1(config-vrf)# route-target import 65501:2
PE1(config-vrf)# exit
PE1(config)#
PE1(config)# system jumbo-frames
PE1(config)#
PE1(config)# route-map BGP_OUT
PE1(config-route-map)# rule 1
PE1(config-route-map-rule)# exit
PE1(config-route-map)# exit
PE1(config)# router bgp 65501
PE1(config-bgp)# neighbor 10.10.1.2
PE1(config-bgp-neighbor)# remote-as 65501
PE1(config-bgp-neighbor)# update-source 10.10.1.1
PE1(config-bgp-neighbor)# address-family vpnv4 unicast
PE1(config-bgp-neighbor-af)# send-community extended
PE1(config-bgp-neighbor-af)# enable
PE1(config-bgp-neighbor-af)# exit
PE1(config-bgp-neighbor)# enable
PE1(config-bgp-neighbor)# exit
PE1(config-bgp)# enable
PE1(config-bgp)# vrf CE1
PE1(config-bgp-vrf)# neighbor 192.168.1.1
PE1(config-bgp-vrf-neighbor)# remote-as 65510
PE1(config-bgp-vrf-neighbor)# address-family ipv4 unicast
PE1(config-bgp-neighbor-af-vrf)# route-map BGP_OUT out
PE1(config-bgp-neighbor-af-vrf)# enable
PE1(config-bgp-neighbor-af-vrf)# exit
PE1(config-bgp-vrf-neighbor)# enable
PE1(config-bgp-vrf-neighbor)# exit
PE1(config-bgp-vrf)# address-family ipv4 unicast
PE1(config-bgp-vrf-af)# redistribute bgp 65501 route-map BGP_OUT
PE1(config-bgp-vrf-af)# exit
PE1(config-bgp-vrf)# enable
PE1(config-bgp-vrf)# exit
PE1(config-bgp)# vrf CE2
PE1(config-bgp-vrf)# neighbor 192.168.2.1
PE1(config-bgp-vrf-neighbor)# remote-as 65511
PE1(config-bgp-vrf-neighbor)# address-family ipv4 unicast
PE1(config-bgp-neighbor-af-vrf)# route-map BGP_OUT out
PE1(config-bgp-neighbor-af-vrf)# enable
PE1(config-bgp-neighbor-af-vrf)# exit
PE1(config-bgp-vrf-neighbor)# enable
PE1(config-bgp-vrf-neighbor)# exit
PE1(config-bgp-vrf)# address-family ipv4 unicast
PE1(config-bgp-vrf-af)# redistribute bgp 65501 route-map BGP_OUT
PE1(config-bgp-vrf-af)# exit
```

```
PE1(config-bgp-vrf)# enable
PE1(config-bgp-vrf)# exit
PE1(config-bgp)# exit
PE1(config)#
PE1(config)# router ospf 1
PE1(config-ospf)# area 0.0.0.0
PE1(config-ospf-area)# enable
PE1(config-ospf-area)# exit
PE1(config-ospf)# enable
PE1(config-ospf)# exit
PE1(config)#
PE1(config)# interface gigabitethernet 1/0/1.100
PE1(config-subif)# ip vrf forwarding CE1
PE1(config-subif)# description "to CE1"
PE1(config-subif)# ip firewall disable
PE1(config-subif)# ip address 192.168.1.2/30
PE1(config-subif)# exit
PE1(config)# interface gigabitethernet 1/0/1.200
PE1(config-subif)# ip vrf forwarding CE2
PE1(config-subif)# description "to CE2"
PE1(config-subif)# ip firewall disable
PE1(config-subif)# ip address 192.168.2.2/30
PE1(config-subif)# exit
PE1(config)# interface gigabitethernet 1/0/2
PE1(config-if-gi)# description "to ASBR1"
PE1(config-if-gi)# mtu 1522
PE1(config-if-gi)# ip firewall disable
PE1(config-if-gi)# ip address 10.100.0.1/30
PE1(config-if-gi)# ip ospf instance 1
PE1(config-if-gi)# ip ospf
PE1(config-if-gi)# exit
PE1(config)# interface loopback 1
PE1(config-loopback)# ip address 10.10.1.1/32
PE1(config-loopback)# ip ospf instance 1
PE1(config-loopback)# ip ospf
PE1(config-loopback)# exit
PE1(config)# mpls
PE1(config-mpls)# ldp
PE1(config-ldp)# router-id 10.10.1.1
PE1(config-ldp)# address-family ipv4
PE1(config-ldp-af-ipv4)# interface gigabitethernet 1/0/2
PE1(config-ldp-af-ipv4-if)# exit
PE1(config-ldp-af-ipv4)# exit
PE1(config-ldp)# enable
PE1(config-ldp)# exit
PE1(config-mpls)# forwarding interface gigabitethernet 1/0/2
PE1(config-mpls)# exit
PE1(config)# do com
PE1(config)# do conf
```

PE2

```
PE2(config)# hostname PE2
PE2(config)#
PE2(config)# ip vrf CE1
PE2(config-vrf)# ip protocols bgp max-routes 100
PE2(config-vrf)# rd 65501:1
PE2(config-vrf)# route-target export 65501:1
PE2(config-vrf)# route-target import 65501:1
PE2(config-vrf)# exit
PE2(config)# ip vrf CE2
PE2(config-vrf)# ip protocols bgp max-routes 100
PE2(config-vrf)# rd 65501:2
PE2(config-vrf)# route-target export 65501:2
PE2(config-vrf)# route-target import 65501:2
PE2(config-vrf)# exit
PE2(config)#
PE2(config)# system jumbo-frames
PE2(config)#
PE2(config)# route-map BGP_OUT
PE2(config-route-map)# rule 1
PE2(config-route-map-rule)# exit
PE2(config-route-map)# exit
PE2(config)# router bgp 65500
PE2(config-bgp)# neighbor 10.11.1.2
PE2(config-bgp-neighbor)# remote-as 65500
PE2(config-bgp-neighbor)# update-source 10.11.1.1
PE2(config-bgp-neighbor)# address-family vpnv4 unicast
PE2(config-bgp-neighbor-af)# send-community extended
PE2(config-bgp-neighbor-af)# enable
PE2(config-bgp-neighbor-af)# exit
PE2(config-bgp-neighbor)# enable
PE2(config-bgp-neighbor)# exit
PE2(config-bgp)# enable
PE2(config-bgp)# vrf CE1
PE2(config-bgp-vrf)# neighbor 192.168.3.1
PE2(config-bgp-vrf-neighbor)# remote-as 65512
PE2(config-bgp-vrf-neighbor)# address-family ipv4 unicast
PE2(config-bgp-neighbor-af-vrf)# route-map BGP_OUT out
PE2(config-bgp-neighbor-af-vrf)# enable
PE2(config-bgp-neighbor-af-vrf)# exit
PE2(config-bgp-vrf-neighbor)# enable
PE2(config-bgp-vrf-neighbor)# exit
PE2(config-bgp-vrf)# address-family ipv4 unicast
PE2(config-bgp-vrf-af)# redistribute bgp 65500 route-map BGP_OUT
PE2(config-bgp-vrf-af)# exit
PE2(config-bgp-vrf)# enable
PE2(config-bgp-vrf)# exit
PE2(config-bgp)# vrf CE2
PE2(config-bgp-vrf)# neighbor 192.168.4.1
PE2(config-bgp-vrf-neighbor)# remote-as 65513
PE2(config-bgp-vrf-neighbor)# address-family ipv4 unicast
PE2(config-bgp-neighbor-af-vrf)# route-map BGP_OUT out
PE2(config-bgp-neighbor-af-vrf)# enable
PE2(config-bgp-neighbor-af-vrf)# exit
PE2(config-bgp-vrf-neighbor)# enable
PE2(config-bgp-vrf-neighbor)# exit
PE2(config-bgp-vrf)# address-family ipv4 unicast
PE2(config-bgp-vrf-af)# redistribute bgp 65500 route-map BGP_OUT
PE2(config-bgp-vrf-af)# exit
```

```
PE2(config-bgp-vrf)# enable
PE2(config-bgp-vrf)# exit
PE2(config-bgp)# exit
PE2(config)#
PE2(config)# router ospf 1
PE2(config-ospf)# router-id 10.11.1.1
PE2(config-ospf)# area 0.0.0.0
PE2(config-ospf-area)# enable
PE2(config-ospf-area)# exit
PE2(config-ospf)# enable
PE2(config-ospf)# exit
PE2(config)#
PE2(config)# interface gigabitethernet 1/0/1.100
PE2(config-subif)# ip vrf forwarding CE1
PE2(config-subif)# description "to CE3"
PE2(config-subif)# ip firewall disable
PE2(config-subif)# ip address 192.168.3.2/30
PE2(config-subif)# exit
PE2(config)# interface gigabitethernet 1/0/1.200
PE2(config-subif)# ip vrf forwarding CE2
PE2(config-subif)# description "CE4"
PE2(config-subif)# ip firewall disable
PE2(config-subif)# ip address 192.168.4.2/30
PE2(config-subif)# exit
PE2(config)# interface gigabitethernet 1/0/2
PE2(config-if-gi)# description "to ASBR2"
PE2(config-if-gi)# mtu 1522
PE2(config-if-gi)# ip firewall disable
PE2(config-if-gi)# ip address 10.102.0.1/30
PE2(config-if-gi)# ip ospf instance 1
PE2(config-if-gi)# ip ospf
PE2(config-if-gi)# exit
PE2(config)# interface loopback 1
PE2(config-loopback)# ip address 10.11.1.1/32
PE2(config-loopback)# ip ospf instance 1
PE2(config-loopback)# ip ospf
PE2(config-loopback)# exit
PE2(config)# mpls
PE2(config-mpls)# ldp
PE2(config-ldp)# router-id 10.11.1.1
PE2(config-ldp)# address-family ipv4
PE2(config-ldp-af-ipv4)# interface gigabitethernet 1/0/2
PE2(config-ldp-af-ipv4-if)# exit
PE2(config-ldp-af-ipv4)# exit
PE2(config-ldp)# enable
PE2(config-ldp)# exit
PE2(config-mpls)# forwarding interface gigabitethernet 1/0/2
PE2(config-mpls)# exit
PE2(config)# do com
PE2(config)# do conf
```

Настроим ASBR1 и ASBR2:

ASBR1

```
ASBR1(config)# hostname ASBR1
ASBR1(config)#
ASBR1(config)# system jumbo-frames
ASBR1(config)#
ASBR1(config)# route-map VPNv4
ASBR1(config-route-map)# rule 1
ASBR1(config-route-map-rule)# exit
ASBR1(config-route-map)# exit
ASBR1(config)# router bgp 65501
ASBR1(config-bgp)# router-id 10.10.1.2
ASBR1(config-bgp)# neighbor 10.10.1.1
ASBR1(config-bgp-neighbor)# remote-as 65501
ASBR1(config-bgp-neighbor)# update-source 10.10.1.2
ASBR1(config-bgp-neighbor)# address-family vpnv4 unicast
ASBR1(config-bgp-neighbor-af)# next-hop-self
ASBR1(config-bgp-neighbor-af)# send-community extended
ASBR1(config-bgp-neighbor-af)# enable
ASBR1(config-bgp-neighbor-af)# exit
ASBR1(config-bgp-neighbor)# enable
ASBR1(config-bgp-neighbor)# exit
ASBR1(config-bgp)# neighbor 10.101.0.1
ASBR1(config-bgp-neighbor)# remote-as 65500
ASBR1(config-bgp-neighbor)# address-family vpnv4 unicast
ASBR1(config-bgp-neighbor-af)# route-map VPNv4 out
ASBR1(config-bgp-neighbor-af)# send-community extended
ASBR1(config-bgp-neighbor-af)# enable
ASBR1(config-bgp-neighbor-af)# exit
ASBR1(config-bgp-neighbor)# enable
ASBR1(config-bgp-neighbor)# exit
ASBR1(config-bgp)# enable
ASBR1(config-bgp)# exit
ASBR1(config)#
ASBR1(config)# router ospf 1
ASBR1(config-ospf)# area 0.0.0.0
ASBR1(config-ospf-area)# enable
ASBR1(config-ospf-area)# exit
ASBR1(config-ospf)# enable
ASBR1(config-ospf)# exit
ASBR1(config)#
ASBR1(config)# interface gigabitethernet 1/0/1
ASBR1(config-if-gi)# description "to ASBR2"
ASBR1(config-if-gi)# ip firewall disable
ASBR1(config-if-gi)# ip address 10.101.0.2/30
ASBR1(config-if-gi)# exit
ASBR1(config)# interface gigabitethernet 1/0/2
ASBR1(config-if-gi)# description "to PE1"
ASBR1(config-if-gi)# mtu 1522
ASBR1(config-if-gi)# ip firewall disable
ASBR1(config-if-gi)# ip address 10.100.0.2/30
ASBR1(config-if-gi)# ip ospf instance 1
ASBR1(config-if-gi)# ip ospf
ASBR1(config-if-gi)# exit
ASBR1(config)# interface loopback 1
ASBR1(config-loopback)# ip address 10.10.1.2/32
ASBR1(config-loopback)# ip ospf instance 1
ASBR1(config-loopback)# ip ospf
ASBR1(config-loopback)# exit
ASBR1(config)# mpls
```

```
ASBR1(config-mpls)# ldp
ASBR1(config-ldp)# router-id 10.10.1.2
ASBR1(config-ldp)# address-family ipv4
ASBR1(config-ldp-af-ipv4)# interface gigabitethernet 1/0/2
ASBR1(config-ldp-af-ipv4-if)# exit
ASBR1(config-ldp-af-ipv4)# exit
ASBR1(config-ldp)# enable
ASBR1(config-ldp)# exit
ASBR1(config-mpls)# forwarding interface gigabitethernet 1/0/1
ASBR1(config-mpls)# forwarding interface gigabitethernet 1/0/2
ASBR1(config-mpls)# exit
ASBR1(config)# do com
ASBR1(config)# do conf
```

ASBR2

```
ASBR2(config)# hostname ASBR2
ASBR2(config)#
ASBR2(config)# system jumbo-frames
ASBR2(config)#
ASBR2(config)# route-map VPNv4
ASBR2(config-route-map)# rule 1
ASBR2(config-route-map-rule)# exit
ASBR2(config-route-map)# exit
ASBR2(config)# router bgp 65500
ASBR2(config-bgp)# router-id 10.11.1.2
ASBR2(config-bgp)# neighbor 10.101.0.2
ASBR2(config-bgp-neighbor)# remote-as 65501
ASBR2(config-bgp-neighbor)# address-family vpnv4 unicast
ASBR2(config-bgp-neighbor-af)# route-map VPNv4 out
ASBR2(config-bgp-neighbor-af)# send-community extended
ASBR2(config-bgp-neighbor-af)# enable
ASBR2(config-bgp-neighbor-af)# exit
ASBR2(config-bgp-neighbor)# enable
ASBR2(config-bgp-neighbor)# exit
ASBR2(config-bgp)# neighbor 10.11.1.1
ASBR2(config-bgp-neighbor)# remote-as 65500
ASBR2(config-bgp-neighbor)# update-source 10.11.1.2
ASBR2(config-bgp-neighbor)# address-family vpnv4 unicast
ASBR2(config-bgp-neighbor-af)# next-hop-self
ASBR2(config-bgp-neighbor-af)# send-community extended
ASBR2(config-bgp-neighbor-af)# enable
ASBR2(config-bgp-neighbor-af)# exit
ASBR2(config-bgp-neighbor)# enable
ASBR2(config-bgp-neighbor)# exit
ASBR2(config-bgp)# enable
ASBR2(config-bgp)# exit
ASBR2(config)#
ASBR2(config)# router ospf 1
ASBR2(config-ospf)# router-id 10.11.1.2
ASBR2(config-ospf)# area 0.0.0.0
ASBR2(config-ospf-area)# enable
ASBR2(config-ospf-area)# exit
ASBR2(config-ospf)# enable
ASBR2(config-ospf)# exit
ASBR2(config)#
ASBR2(config)# interface gigabitethernet 1/0/1
ASBR2(config-if-gi)# description "to ASBR1"
ASBR2(config-if-gi)# ip firewall disable
ASBR2(config-if-gi)# ip address 10.101.0.1/30
ASBR2(config-if-gi)# exit
ASBR2(config)# interface gigabitethernet 1/0/2
ASBR2(config-if-gi)# description "to PE2"
ASBR2(config-if-gi)# mtu 1522
ASBR2(config-if-gi)# ip firewall disable
ASBR2(config-if-gi)# ip address 10.102.0.2/30
ASBR2(config-if-gi)# ip ospf instance 1
ASBR2(config-if-gi)# ip ospf
ASBR2(config-if-gi)# exit
ASBR2(config)# interface loopback 1
ASBR2(config-loopback)# ip address 10.11.1.2/32
ASBR2(config-loopback)# ip ospf instance 1
ASBR2(config-loopback)# ip ospf
ASBR2(config-loopback)# exit
```

```
ASBR2(config)# mpls
ASBR2(config-mpls)# ldp
ASBR2(config-ldp)# router-id 10.11.1.2
ASBR2(config-ldp)# address-family ipv4
ASBR2(config-ldp-af-ipv4)# interface gigabitethernet 1/0/2
ASBR2(config-ldp-af-ipv4-if)# exit
ASBR2(config-ldp-af-ipv4)# exit
ASBR2(config-ldp)# enable
ASBR2(config-ldp)# exit
ASBR2(config-mpls)# forwarding interface gigabitethernet 1/0/1
ASBR2(config-mpls)# forwarding interface gigabitethernet 1/0/2
ASBR2(config-mpls)# exit
ASBR2(config)# do com
ASBR2(config)# do conf
```

После завершения настройки проверим распространение маршрутной информации и сетевую доступность узлов:

```
PE1# sh bgp vpnv4 unicast all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes Route Distinguisher   IP Prefix          Next hop        Metric     Label   LocPrf
Weight Path
----- --------------------- ------------------ --------------- ---------- ------- ----------
------ ----------------
*>i   65501:2               10.104.0.1/32      10.10.1.2       --         23      100        0
65500 65513 i
*>i   65501:1               10.103.0.1/32      10.10.1.2       --         19      100        0
65500 65512 i
*>    65501:2               10.101.0.1/32      --              --         29      100        --
65511 i
*>    65501:1               10.100.0.1/32      --              --         28      100        --
65510 i
ASBR1#    sh bgp vpnv4 unicast all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes Route Distinguisher   IP Prefix          Next hop        Metric     Label   LocPrf
Weight Path
----- --------------------- ------------------ --------------- ---------- ------- ----------
------ ----------------
*>    65501:2               10.104.0.1/32      10.101.0.1      --         24      100        0
65500 65513 i
*>    65501:1               10.103.0.1/32      10.101.0.1      --         20      100        0
65500 65512 i
*>i   65501:2               10.101.0.1/32      10.10.1.1       --         29      100        0
65511 i
*>i   65501:1               10.100.0.1/32      10.10.1.1       --         28      100        0
65510 i

ASBR2# sh bgp vpnv4 unicast all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes Route Distinguisher   IP Prefix          Next hop        Metric     Label   LocPrf
Weight Path
----- --------------------- ------------------ --------------- ---------- ------- ----------
------ ----------------
*>i   65501:2               10.104.0.1/32      10.11.1.1       --         19      100        0
65513 i
*>i   65501:1               10.103.0.1/32      10.11.1.1       --         18      100        0
65512 i
*>    65501:2               10.101.0.1/32      10.101.0.2      --         30      100        0
65501 65511 i
*>    65501:1               10.100.0.1/32      10.101.0.2      --         31      100        0
65501 65510 i

PE2# sh bgp vpnv4 unicast all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes Route Distinguisher   IP Prefix          Next hop        Metric     Label   LocPrf
Weight Path
----- --------------------- ------------------ --------------- ---------- ------- ----------
------ ----------------
*>    65501:2               10.104.0.1/32      --              --         19      100        --
65513 i
```

```
*>    65501:1              10.103.0.1/32      --              --          18      100        --
65512 i
*>i   65501:2              10.101.0.1/32      10.11.1.2       --          29      100        0
65501 65511 i
*>i   65501:1              10.100.0.1/32      10.11.1.2       --          30      100        0
65501 65510 i

CE4# ping 10.104.0.1 source ip 10.101.0.1  detailed
PING 10.104.0.1 (10.104.0.1) from 10.101.0.1 : 56 bytes of data.
64 bytes from 10.104.0.1: icmp_seq=1 ttl=0 time=2.25 ms
64 bytes from 10.104.0.1: icmp_seq=2 ttl=0 time=2.08 ms
64 bytes from 10.104.0.1: icmp_seq=3 ttl=0 time=2.15 ms
64 bytes from 10.104.0.1: icmp_seq=4 ttl=0 time=2.12 ms
64 bytes from 10.104.0.1: icmp_seq=5 ttl=0 time=2.09 ms

CE1# ping 10.103.0.1 source ip 10.100.0.1 detailed
PING 10.103.0.1 (10.103.0.1) from 10.100.0.1 : 56 bytes of data.
64 bytes from 10.103.0.1: icmp_seq=1 ttl=0 time=2.22 ms
64 bytes from 10.103.0.1: icmp_seq=2 ttl=0 time=2.11 ms
64 bytes from 10.103.0.1: icmp_seq=3 ttl=0 time=2.09 ms
64 bytes from 10.103.0.1: icmp_seq=4 ttl=0 time=2.09 ms
64 bytes from 10.103.0.1: icmp_seq=5 ttl=0 time=2.11 ms
```

14.13 MPLS over GRE

В этом разделе приведен пример настройки сервисов VPN, построенных через GRE-туннель.

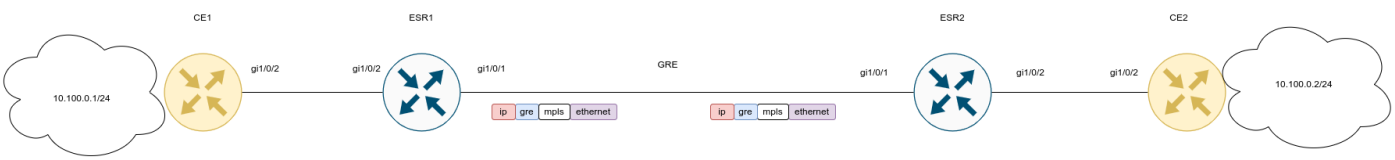
14.13.1 L2VPN

В качестве сервиса l2vpn произведем настройку EoMPLS over GRE. Также возможно построение VPLS over GRE (BGP или LDP signaling).

При настройке MTU на туннеле необходимо учитывать следующее:

- **По крайней мере одна mpls-метка будет присутствовать при передаче через туннель. В учет стоит включать все метки в стеке, например, explicit null или entropy label;**
- **Необходимо учитывать vlan, q-in-q заголовки (если они имеются);**
- **При превышении MTU исходящего интерфейса пакет будет отброшен (если не включена безусловная фрагментация GRE-трафика);**
- **Control world не поддержан;**
- **DF-бит будет выставлен в единицу.**

Ниже представлена примерная структура пакета:



Настройки CE1 и CE2:

CE1

```
hostname CE1

interface gigabitethernet 1/0/2
  ip firewall disable
  ip address 10.100.0.1/24
exit
```

CE2

```
hostname CE2

interface gigabitethernet 1/0/2
  ip firewall disable
  ip address 10.100.0.2/24
exit
```

Конфигурация ESR1 и ESR2:

ESR1

```
ESR1(config)# hostname ESR1
ESR1(config)#
ESR1(config)# system cpu load-balance mpls passenger ip
ESR1(config)# system cpu load-balance mpls passenger ipoe-pw-without-cw
ESR1(config)# security zone trusted
ESR1(config-zone)# exit
ESR1(config)# security zone untrusted
ESR1(config-zone)# exit
ESR1(config)#
ESR1(config)# router ospf 1
ESR1(config-ospf)# area 0.0.0.0
ESR1(config-ospf-area)# enable
ESR1(config-ospf-area)# exit
ESR1(config-ospf)# enable
ESR1(config-ospf)# exit
ESR1(config)#
ESR1(config)# interface gigabitethernet 1/0/1
ESR1(config-if-gi)# security-zone untrusted
ESR1(config-if-gi)# ip address 192.0.2.1/30
ESR1(config-if-gi)# exit
ESR1(config)# interface gigabitethernet 1/0/2
ESR1(config-if-gi)# description "From CE1"
ESR1(config-if-gi)# mode switchport
ESR1(config-if-gi)# exit
ESR1(config)# interface loopback 1
ESR1(config-loopback)# ip address 10.100.0.1/32
ESR1(config-loopback)# ip ospf instance 1
ESR1(config-loopback)# ip ospf
ESR1(config-loopback)# exit
ESR1(config)# tunnel gre 1
ESR1(config-gre)# key 60
ESR1(config-gre)# ttl 64
ESR1(config-gre)# mtu 1458
ESR1(config-gre)# ip firewall disable
ESR1(config-gre)# local address 192.0.2.1
ESR1(config-gre)# remote address 192.0.2.2
ESR1(config-gre)# ip address 10.0.0.1/30
ESR1(config-gre)# ip ospf instance 1
ESR1(config-gre)# ip ospf network point-to-point
ESR1(config-gre)# ip ospf
ESR1(config-gre)# enable
ESR1(config-gre)# exit
ESR1(config)#
ESR1(config)# mpls
ESR1(config-mpls)# ldp
ESR1(config-ldp)# router-id 10.100.0.1
ESR1(config-ldp)# address-family ipv4
ESR1(config-ldp-af-ipv4)# interface gre 1
ESR1(config-ldp-af-ipv4-if)# exit
ESR1(config-ldp-af-ipv4)# exit
ESR1(config-ldp)# enable
ESR1(config-ldp)# exit
ESR1(config-mpls)# l2vpn
ESR1(config-l2vpn)# pw-class VPWS
ESR1(config-l2vpn-pw-class)# exit
ESR1(config-l2vpn)# p2p EoMPLS
ESR1(config-l2vpn-p2p)# interface gigabitethernet 1/0/2
ESR1(config-l2vpn-p2p)# pw 100 10.100.0.2
```

```
ESR1(config-l2vpn-pw)# pw-class VPWS
ESR1(config-l2vpn-pw)# enable
ESR1(config-l2vpn-pw)# exit
ESR1(config-l2vpn-p2p)# enable
ESR1(config-l2vpn-p2p)# exit
ESR1(config-l2vpn)# exit
ESR1(config-mpls)# forwarding interface gre 1
ESR1(config-mpls)# exit
ESR1(config)# security zone-pair untrusted self
ESR1(config-zone-pair)# rule 1
ESR1(config-zone-pair-rule)# action permit
ESR1(config-zone-pair-rule)# match protocol gre
ESR1(config-zone-pair-rule)# enable
ESR1(config-zone-pair-rule)# exit
ESR1(config-zone-pair)# exit
ESR1(config)# do com
ESR1(config)# do conf
```

ESR2

```
ESR2(config)# hostname ESR2
ESR2(config)#
ESR2(config)# system cpu load-balance mpls passenger ip
ESR2(config)# system cpu load-balance mpls passenger ipoe-pw-without-cw
ESR2(config)# security zone trusted
ESR2(config-zone)# exit
ESR2(config)# security zone untrusted
ESR2(config-zone)# exit
ESR2(config)#
ESR2(config)# router ospf 1
ESR2(config-ospf)# area 0.0.0.0
ESR2(config-ospf-area)# enable
ESR2(config-ospf-area)# exit
ESR2(config-ospf)# enable
ESR2(config-ospf)# exit
ESR2(config)#
ESR2(config)# interface gigabitethernet 1/0/1
ESR2(config-if-gi)# security-zone untrusted
ESR2(config-if-gi)# ip address 192.0.2.2/30
ESR2(config-if-gi)# exit
ESR2(config)# interface gigabitethernet 1/0/2
ESR2(config-if-gi)# description "From CE2"
ESR2(config-if-gi)# mode switchport
ESR2(config-if-gi)# exit
ESR2(config)# interface loopback 1
ESR2(config-loopback)# ip address 10.100.0.2/32
ESR2(config-loopback)# ip ospf instance 1
ESR2(config-loopback)# ip ospf
ESR2(config-loopback)# exit
ESR2(config)# tunnel gre 1
ESR2(config-gre)# key 60
ESR2(config-gre)# ttl 64
ESR2(config-gre)# mtu 1458
ESR2(config-gre)# ip firewall disable
ESR2(config-gre)# local address 192.0.2.2
ESR2(config-gre)# remote address 192.0.2.1
ESR2(config-gre)# ip address 10.0.0.2/30
ESR2(config-gre)# ip ospf instance 1
ESR2(config-gre)# ip ospf network point-to-point
ESR2(config-gre)# ip ospf
ESR2(config-gre)# enable
ESR2(config-gre)# exit
ESR2(config)#
ESR2(config)# mpls
ESR2(config-mpls)# ldp
ESR2(config-ldp)# router-id 10.100.0.2
ESR2(config-ldp)# address-family ipv4
ESR2(config-ldp-af-ipv4)# interface gre 1
ESR2(config-ldp-af-ipv4-if)# exit
ESR2(config-ldp-af-ipv4)# exit
ESR2(config-ldp)# enable
ESR2(config-ldp)# exit
ESR2(config-mpls)# l2vpn
ESR2(config-l2vpn)# pw-class VPWS
ESR2(config-l2vpn-pw-class)# exit
ESR2(config-l2vpn)# p2p EoMPLS
ESR2(config-l2vpn-p2p)# interface gigabitethernet 1/0/2
ESR2(config-l2vpn-p2p)# pw 100 10.100.0.1
```

```
ESR2(config-l2vpn-pw)#  pw-class VPWS
ESR2(config-l2vpn-pw)# enable
ESR2(config-l2vpn-pw)# exit
ESR2(config-l2vpn-p2p)# enable
ESR2(config-l2vpn-p2p)# exit
ESR2(config-l2vpn)# exit
ESR2(config-mpls)# forwarding interface gre 1
ESR2(config-mpls)# exit
ESR2(config)# security zone-pair untrusted self
ESR2(config-zone-pair)# rule 1
ESR2(config-zone-pair-rule)# action deny
ESR2(config-zone-pair-rule)# match protocol gre
ESR2(config-zone-pair-rule)# enable
ESR2(config-zone-pair-rule)# exit
ESR2(config-zone-pair)# exit
ESR2(config)# do com
ESR2(config)# do conf
```

Настройка завершена. Проверим состояние сервиса и доступность узлов:

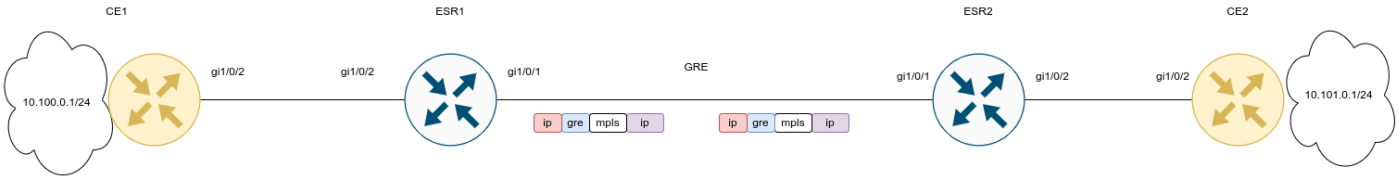
```
* Конфигурация туннеля*
ESR2# sh tunnels configuration gre 1
State:                                          Enabled
Description:                                    --
Mode:                                           ip
Bridge group:                                   --
VRF:                                            --
Local address:                                  192.0.2.2
Remote address:                                 192.0.2.1
Calculates checksums for outgoing GRE packets:  No
Requires that all input GRE packets were checksum: No
key:                                            60
TTL:                                            64
DSCP:                                           Inherit
MTU:                                            1458
Path MTU discovery:                             Enabled
Don't fragment bit suppression:                 Disabled
Security zone:                                  --
Multipoint mode:                                Disabled
Keepalive:
    State:                                          Disabled
    Timeout:                                        10
    Retries:                                        6
    Destination address:                            --

*Статус сервиса и выделенные метки*
sh mpls l2vpn p2p
P2P: EoMPLS
    gigabitethernet 1/0/2:
        MTU:    1500
        Status: Up
    PW ID 100, Neighbor 10.100.0.1:
        MTU:         1500
        Status TLV:  Enable
        Last change: 00:14:27
        Status:      Up

ESR2# sh mpls forwarding-table
Local    Outgoing Prefix                                    Outgoing         Next Hop
label    label    or tunnel ID                              Interface
-------- -------- ----------------------------------------- ----------------
---------------------------------------
17       imp-null 10.100.0.1/32                             gre 1            10.0.0.1
16       16       PW ID 100                                 --               10.100.0.1

*Доступность*CE1# ping 10.100.0.2 detailed
PING 10.100.0.2 (10.100.0.2) 56 bytes of data.
64 bytes from 10.100.0.2: icmp_seq=1 ttl=0 time=1.38 ms
64 bytes from 10.100.0.2: icmp_seq=2 ttl=0 time=1.22 ms
64 bytes from 10.100.0.2: icmp_seq=3 ttl=0 time=1.33 ms
64 bytes from 10.100.0.2: icmp_seq=4 ttl=0 time=1.26 ms
64 bytes from 10.100.0.2: icmp_seq=5 ttl=0 time=1.17 ms
```

14.13.2 L3VPN

При настройке MTU на туннеле необходимо учитывать следующее:

- **По крайне мере одна mpls-метка будет присутствовать при передаче через туннель. В учет стоит включать все метки в стеке, например, explicit null и/или entropy label;**
- **При превышении MTU исходящего интерфейса пакет будет отброшен (если не включена безусловная фрагментация GRE-трафика);**
- **Control world не поддержан;**
- **DFбит будет выставлен в единицу.**

Ниже представлена примерная структура пакета:



Настройки CE1 и CE2:

CE1

```
CE1(config)# hostname CE1
CE1(config)#
CE1(config)# route-map BGP_OUT
CE1(config-route-map)# rule 1
CE1(config-route-map-rule)# exit
CE1(config-route-map)# exit
CE1(config)# router bgp 65501
CE1(config-bgp)# neighbor 10.10.0.2
CE1(config-bgp-neighbor)# remote-as 65500
CE1(config-bgp-neighbor)# address-family ipv4 unicast
CE1(config-bgp-neighbor-af)# route-map BGP_OUT out
CE1(config-bgp-neighbor-af)# enable
CE1(config-bgp-neighbor-af)# exit
CE1(config-bgp-neighbor)# enable
CE1(config-bgp-neighbor)# exit
CE1(config-bgp)# address-family ipv4 unicast
CE1(config-bgp-af)# network 10.100.0.0/24
CE1(config-bgp-af)# exit
CE1(config-bgp)# enable
CE1(config-bgp)# exit
CE1(config)#
CE1(config)#
CE1(config)# interface gigabitethernet 1/0/2
CE1(config-if-gi)# description "to ESR1"
CE1(config-if-gi)# ip firewall disable
CE1(config-if-gi)# ip address 10.10.0.1/30
CE1(config-if-gi)# exit
CE1(config)# interface loopback 1
CE1(config-loopback)# ip address 10.100.0.1/24
CE1(config-loopback)# exit
```

CE2

```
CE2(config)# hostname CE2
CE2(config)#
CE2(config)# route-map BGP_OUT
CE2(config-route-map)# rule 1
CE2(config-route-map-rule)# exit
CE2(config-route-map)# exit
CE2(config)# router bgp 65502
CE2(config-bgp)# neighbor 10.10.0.5
CE2(config-bgp-neighbor)# remote-as 65500
CE2(config-bgp-neighbor)# address-family ipv4 unicast
CE2(config-bgp-neighbor-af)# route-map BGP_OUT out
CE2(config-bgp-neighbor-af)# enable
CE2(config-bgp-neighbor-af)# exit
CE2(config-bgp-neighbor)# enable
CE2(config-bgp-neighbor)# exit
CE2(config-bgp)# address-family ipv4 unicast
CE2(config-bgp-af)# network 10.101.0.0/24
CE2(config-bgp-af)# exit
CE2(config-bgp)# enable
CE2(config-bgp)# exit
CE2(config)#
CE2(config)#
CE2(config)# interface gigabitethernet 1/0/2
CE2(config-if-gi)# description "to ESR2"
CE2(config-if-gi)# ip firewall disable
CE2(config-if-gi)# ip address 10.10.0.6/30
CE2(config-if-gi)# exit
CE2(config)# interface loopback 1
CE2(config-loopback)# ip address 10.101.0.1/24
CE2(config-loopback)# exit
```

Конфигурация ESR1 и ESR2:

ESR1

```
ESR1(config)# hostname ESR1
ESR1(config)#
ESR1(config)# ip vrf l3vpn_service
ESR1(config-vrf)# ip protocols bgp max-routes 100
ESR1(config-vrf)# rd 65500:1
ESR1(config-vrf)# route-target export 65500:1
ESR1(config-vrf)# route-target import 65500:1
ESR1(config-vrf)# exit
ESR1(config)#
ESR1(config)#
ESR1(config)# system cpu load-balance mpls passenger ip
ESR1(config)# security zone untrusted
ESR1(config-zone)# exit
ESR1(config)# security zone trusted
ESR1(config-zone)# exit
ESR1(config)#
ESR1(config)# route-map BGP_OUT
ESR1(config-route-map)# rule 1
ESR1(config-route-map-rule)#   exit
ESR1(config-route-map)# exit
ESR1(config)# router bgp 65500
ESR1(config-bgp)# router-id 10.12.0.1
ESR1(config-bgp)# neighbor 10.12.0.2
ESR1(config-bgp-neighbor)# remote-as 65500
ESR1(config-bgp-neighbor)# update-source 10.12.0.1
ESR1(config-bgp-neighbor)# address-family vpnv4 unicast
ESR1(config-bgp-neighbor-af)# send-community extended
ESR1(config-bgp-neighbor-af)# enable
ESR1(config-bgp-neighbor-af)# exit
ESR1(config-bgp-neighbor)# enable
ESR1(config-bgp-neighbor)# exit
ESR1(config-bgp)# enable
ESR1(config-bgp)# vrf l3vpn_service
ESR1(config-bgp-vrf)# neighbor 10.10.0.1
ESR1(config-bgp-vrf-neighbor)# remote-as 65501
ESR1(config-bgp-vrf-neighbor)# address-family ipv4 unicast
ESR1(config-bgp-neighbor-af-vrf)# route-map BGP_OUT out
ESR1(config-bgp-neighbor-af-vrf)# enable
ESR1(config-bgp-neighbor-af-vrf)# exit
ESR1(config-bgp-vrf-neighbor)# enable
ESR1(config-bgp-vrf-neighbor)# exit
ESR1(config-bgp-vrf)# address-family ipv4 unicast
ESR1(config-bgp-vrf-af)# redistribute bgp 65500 route-map BGP_OUT
ESR1(config-bgp-vrf-af)# exit
ESR1(config-bgp-vrf)# enable
ESR1(config-bgp-vrf)# exit
ESR1(config-bgp)# exit
ESR1(config)#
ESR1(config)# router ospf 1
ESR1(config-ospf)# router-id 10.12.0.1
ESR1(config-ospf)#   area 0.0.0.0
ESR1(config-ospf-area)#     enable
ESR1(config-ospf-area)#   exit
ESR1(config-ospf)#   enable
ESR1(config-ospf)# exit
ESR1(config)#
ESR1(config)# interface gigabitethernet 1/0/1
ESR1(config-if-gi)# security-zone untrusted
```

```
ESR1(config-if-gi)# ip address 192.0.2.1/30
ESR1(config-if-gi)# exit
ESR1(config)# interface gigabitethernet 1/0/2
ESR1(config-if-gi)# ip vrf forwarding l3vpn_service
ESR1(config-if-gi)# description "from CE1"
ESR1(config-if-gi)# ip firewall disable
ESR1(config-if-gi)# ip address 10.10.0.2/30
ESR1(config-if-gi)# exit
ESR1(config)# interface loopback 1
ESR1(config-loopback)# ip address 10.12.0.1/32
ESR1(config-loopback)# ip ospf instance 1
ESR1(config-loopback)# ip ospf
ESR1(config-loopback)# exit
ESR1(config)# tunnel gre 1
ESR1(config-gre)# key 60
ESR1(config-gre)# ttl 64
ESR1(config-gre)# mtu 1472
ESR1(config-gre)# ip firewall disable
ESR1(config-gre)# local address 192.0.2.1
ESR1(config-gre)# remote address 192.0.2.2
ESR1(config-gre)# ip address 10.11.0.1/30
ESR1(config-gre)# ip ospf instance 1
ESR1(config-gre)# ip ospf
ESR1(config-gre)# enable
ESR1(config-gre)# exit
ESR1(config)#
ESR1(config)# mpls
ESR1(config-mpls)# ldp
ESR1(config-ldp)# router-id 10.12.0.1
ESR1(config-ldp)# address-family ipv4
ESR1(config-ldp-af-ipv4)# interface gre 1
ESR1(config-ldp-af-ipv4-if)# exit
ESR1(config-ldp-af-ipv4)# exit
ESR1(config-ldp)# enable
ESR1(config-ldp)# exit
ESR1(config-mpls)# forwarding interface gre 1
ESR1(config-mpls)# exit
ESR1(config)# security zone-pair untrusted self
ESR1(config-zone-pair)# rule 1
ESR1(config-zone-pair-rule)# action permit
ESR1(config-zone-pair-rule)# match protocol gre
ESR1(config-zone-pair-rule)# enable
ESR1(config-zone-pair-rule)# exit
ESR1(config-zone-pair)# exit
```

```
ESR2(config)# hostname ESR2
ESR2(config)#
ESR2(config)# ip vrf l3vpn_service
ESR2(config-vrf)# ip protocols bgp max-routes 100
ESR2(config-vrf)# rd 65500:1
ESR2(config-vrf)# route-target export 65500:1
ESR2(config-vrf)# route-target import 65500:1
ESR2(config-vrf)# exit
ESR2(config)#
ESR2(config)#
ESR2(config)# system cpu load-balance mpls passenger ip
ESR2(config)# security zone untrusted
ESR2(config-zone)# exit
ESR2(config)# security zone trusted
ESR2(config-zone)# exit
ESR2(config)#
ESR2(config)# route-map BGP_OUT
ESR2(config-route-map)# rule 1
ESR2(config-route-map-rule)# exit
ESR2(config-route-map)# exit
ESR2(config)# router bgp 65500
ESR2(config-bgp)# router-id 10.12.0.2
ESR2(config-bgp)# neighbor 10.12.0.1
ESR2(config-bgp-neighbor)# remote-as 65500
ESR2(config-bgp-neighbor)# update-source 10.12.0.2
ESR2(config-bgp-neighbor)# address-family vpnv4 unicast
ESR2(config-bgp-neighbor-af)# send-community extended
ESR2(config-bgp-neighbor-af)# enable
ESR2(config-bgp-neighbor-af)# exit
ESR2(config-bgp-neighbor)# enable
ESR2(config-bgp-neighbor)# exit
ESR2(config-bgp)# enable
ESR2(config-bgp)# vrf l3vpn_service
ESR2(config-bgp-vrf)# neighbor 10.10.0.6
ESR2(config-bgp-vrf-neighbor)# remote-as 65502
ESR2(config-bgp-vrf-neighbor)# address-family ipv4 unicast
ESR2(config-bgp-neighbor-af-vrf)# route-map BGP_OUT out
ESR2(config-bgp-neighbor-af-vrf)# enable
ESR2(config-bgp-neighbor-af-vrf)# exit
ESR2(config-bgp-vrf-neighbor)# enable
ESR2(config-bgp-vrf-neighbor)# exit
ESR2(config-bgp-vrf)# address-family ipv4 unicast
ESR2(config-bgp-vrf-af)# redistribute bgp 65500 route-map BGP_OUT
ESR2(config-bgp-vrf-af)# exit
ESR2(config-bgp-vrf)# enable
ESR2(config-bgp-vrf)# exit
ESR2(config-bgp)# exit
ESR2(config)#
ESR2(config)# router ospf 1
ESR2(config-ospf)# router-id 10.12.0.2
ESR2(config-ospf)# area 0.0.0.0
ESR2(config-ospf-area)# enable
ESR2(config-ospf-area)# exit
ESR2(config-ospf)# enable
ESR2(config-ospf)# exit
ESR2(config)#
ESR2(config)# interface gigabitethernet 1/0/1
ESR2(config-if-gi)# security-zone untrusted
ESR2(config-if-gi)# ip address 192.0.2.2/30
ESR2(config-if-gi)# exit
```

```
ESR2(config)# interface gigabitethernet 1/0/2
ESR2(config-if-gi)# ip vrf forwarding l3vpn_service
ESR2(config-if-gi)# description "from CE2"
ESR2(config-if-gi)# ip firewall disable
ESR2(config-if-gi)# ip address 10.10.0.5/30
ESR2(config-if-gi)# exit
ESR2(config)# interface loopback 1
ESR2(config-loopback)# ip address 10.12.0.2/32
ESR2(config-loopback)# ip ospf instance 1
ESR2(config-loopback)# ip ospf
ESR2(config-loopback)# exit
ESR2(config)# tunnel gre 1
ESR2(config-gre)# key 60
ESR2(config-gre)# ttl 64
ESR2(config-gre)# mtu 1472
ESR2(config-gre)# ip firewall disable
ESR2(config-gre)# local address 192.0.2.2
ESR2(config-gre)# remote address 192.0.2.1
ESR2(config-gre)# ip address 10.11.0.2/30
ESR2(config-gre)# ip ospf instance 1
ESR2(config-gre)# ip ospf
ESR2(config-gre)# enable
ESR2(config-gre)# exit
ESR2(config)#
ESR2(config)# mpls
ESR2(config-mpls)# ldp
ESR2(config-ldp)# router-id 10.12.0.2
ESR2(config-ldp)# address-family ipv4
ESR2(config-ldp-af-ipv4)# interface gre 1
ESR2(config-ldp-af-ipv4-if)# exit
ESR2(config-ldp-af-ipv4)# exit
ESR2(config-ldp)# enable
ESR2(config-ldp)# exit
ESR2(config-mpls)# forwarding interface gre 1
ESR2(config-mpls)# exit
ESR2(config)# security zone-pair untrusted self
ESR2(config-zone-pair)# rule 1
ESR2(config-zone-pair-rule)# action permit
ESR2(config-zone-pair-rule)# match protocol gre
ESR2(config-zone-pair-rule)# enable
ESR2(config-zone-pair-rule)# exit
ESR2(config-zone-pair)# exit
```

После завершения настройки проверим статус сервиса и доступность узлов в сети:

```
*Конфигурация туннеля GRE*
ESR2# sh tunnels configuration
Tunnel              State      Description
----------------    --------   ------------------------------
gre 1               Enabled    --

ESR2# sh tunnels configuration gre 1
State:                                              Enabled
Description:                                        --
Mode:                                               ip
Bridge group:                                       --
VRF:                                                --
Local address:                                      192.0.2.2
Remote address:                                     192.0.2.1
Calculates checksums for outgoing GRE packets:      No
Requires that all input GRE packets were checksum: No
key:                                                60
TTL:                                                64
DSCP:                                               Inherit
MTU:                                                1472
Path MTU discovery:                                 Enabled
Don't fragment bit suppression:                     Disabled
Security zone:                                      --
Multipoint mode:                                    Disabled
Keepalive:
    State:                                              Disabled
    Timeout:                                            10
    Retries:                                            6
    Destination address:                                --

*Наличие vpnv4-маршрутов*
SR2# sh bgp vpnv4 unicast all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes Route Distinguisher   IP Prefix          Next hop        Metric     Label   LocPrf
Weight Path
----- --------------------- ------------------ --------------- ---------- ------- ----------
------ ----------------
*>    65500:1               10.101.0.0/24      --              --         34      100        --
65502 i
*>i   65500:1               10.100.0.0/24      10.12.0.1       --         16      100        0
65501 i

*Состояние протокола LDP*
ESR2# sh mpls ldp neighbor
Peer LDP ID: 10.12.0.1; Local LDP ID 10.12.0.2
    State:                  Operational
    TCP connection:         10.12.0.1:646 - 10.12.0.2:46444
    Messages sent/received: 60/60
    Uptime:                 00:53:59
    LDP discovery sources:
        gre 1
ESR2# sh mpls forwarding-table
Local    Outgoing Prefix                                    Outgoing         Next Hop
label    label    or tunnel ID                              Interface
-------- -------- ----------------------------------------- ----------------
---------------------------------------
35       imp-null 10.12.0.1/32                              gre 1            10.11.0.1
```

```
*Доступность узлов в сети*
CE2# ping 10.100.0.1 source ip 10.101.0.1 detailed
PING 10.100.0.1 (10.100.0.1) from 10.101.0.1 : 56 bytes of data.
64 bytes from 10.100.0.1: icmp_seq=1 ttl=0 time=1.32 ms
64 bytes from 10.100.0.1: icmp_seq=2 ttl=0 time=1.12 ms
64 bytes from 10.100.0.1: icmp_seq=3 ttl=0 time=1.14 ms
64 bytes from 10.100.0.1: icmp_seq=4 ttl=0 time=1.09 ms
64 bytes from 10.100.0.1: icmp_seq=5 ttl=0 time=1.15 ms
```

15 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
- Настройка логирования и защиты от сетевых атак
  - Алгоритм настройки
  - Описание механизмов защиты от атак
  - Пример настройки логирования и защиты от сетевых атак
- Конфигурирование Firewall
  - Алгоритм настройки
  - Пример настройки Firewall
  - Пример настройки фильтрации приложений (DPI)
- Настройка списков доступа (ACL)
  - Алгоритм настройки
  - Пример настройки списка доступа
- Настройка IPS/IDS
  - Алгоритм базовой настройки
  - Алгоритм настройки автообновления правил IPS/IDS из внешних источников
  - Рекомендуемые открытые источники обновления правил
  - Пример настройки IPS/IDS с автообновлением правил
  - Алгоритм настройки базовых пользовательских правил
  - Пример настройки базовых пользовательских правил
  - Алгоритм настройки расширенных пользовательских правил
  - Пример настройки расширенных пользовательских правил
- Настройка взаимодействия с Eltex Distribution Manager
  - Алгоритм базовой настройки
  - Пример настройки
- Настройка сервиса контентной фильтрации
  - Алгоритм базовой настройки
  - Пример настройки правил контентной фильтрации
- Настройка сервиса «Антиспам»
  - Алгоритм базовой настройки
  - Пример настройки

15.1 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.

15.1.1 Алгоритм настройки локальной аутентификации

Шаг	Описание	Команда	Ключи
1	Указать local в качестве метода аутентификации.	**esr(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.	**esr(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).	**esr(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).	**esr(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).	**esr(config)# security passwords default-expired**	
6	Включить режим запрета на использование ранее установленных паролей локальных пользователей (не обязательно).	**esr(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).	**esr(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).	**esr(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).	**esr(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).	**esr(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).	**esr(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).	**esr(config)# security passwords upper-case <COUNT>**	<COUNT> – минимальное количество прописных (заглавных) букв в пароле. Принимает значение в диапазоне [0..128]. Значение по умолчанию: 0.

Шаг	Описание	Команда	Ключи
13	Установить минимальное количество цифр в пароле локального пользователя и ENABLE-пароле (не обязательно).	**esr(config)# security passwords numeric-count <COUNT>**	<COUNT> – минимальное количество цифр в пароле. Принимает значение в диапазоне [0..128]. Значение по умолчанию: 0.
14	Установить минимальное количество специальных символов в пароле локального пользователя и ENABLE-пароле (не обязательно).	**esr(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.	**esr(config)# username <NAME>**	<NAME> – имя пользователя, задаётся строкой до 31 символа.
16	Установить пароль пользователя.	**esr(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.	**esr(config-user)# privilege <PRIV>**	<PRIV> – необходимый уровень привилегий. Принимает значение [1..15].
18	Перейти в режим конфигурирования соответствующего терминала.	**esr(config)# line console** или **esr(config)# line telnet** или **esr(config)# line ssh**	
19	Активировать список аутентификации входа пользователей в систему.	**esr(config-line-ssh)# login authentication <NAME>**	<NAME> – имя списка, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
20	Активировать список аутентификации повышения привилегий пользователей.	**esr(config-line-ssh)# enable authentication <NAME>**	<NAME> – имя списка, задаётся строкой до 31 символа.
21	Задать интервал, по истечении которого будет разрываться бездействующая сессия.	**esr(config-line-ssh)# exec-timeout <SEC>**	<SEC> – период времени в минутах, принимает значения [1..65535].

15.1.2 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).	**esr(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).	**esr(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).	**esr(config)# radius-server timeout <SEC>**	<SEC> – период времени в секундах, принимает значения [1..30]. Значение по умолчанию: 3 секунды.
4	Добавить RADIUS-сервер в список используемых серверов и перейти в режим его конфигурирования.	**esr(config)# radius-server host { <IP-ADDR> | <IPV6-ADDR> } [vrf <VRF>]** **esr(config-radius-server)#**	<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::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF] <VRF> – имя экземпляра VRF, задается строкой до 31 символа.

Шаг	Описание	Команда	Ключи
5	Указать количество неудачных попыток аутентификации для блокировки логина пользователя и времени блокировки (не обязательно).	**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.
6	Задать пароль для аутентификации на удаленном RADIUS-сервере.	**esr(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.
7	Задать приоритет использования удаленного RADIUS-сервера (не обязательно).	**esr(config-radius-server)# priority <PRIORITY>**	<PRIORITY> – приоритет использования удаленного сервера, принимает значения [1..65535]. Чем ниже значение, тем приоритетнее сервер. Значение по умолчанию: 1.
8	Задать интервал, по истечении которого маршрутизатор считает, что данный RADIUS-сервер недоступен (не обязательно).	**esr(config-radius-server)# timeout <SEC>**	<SEC> – период времени в секундах, принимает значения [1..30]. Значение по умолчанию: используется значение глобального таймера.

Шаг	Описание	Команда	Ключи
9	Задать IPv4/IPv6-адрес, который будет использоваться в качестве IP/IPv6-адреса источника в отправляемых RADIUS-пакетах.	**esr(config-radius-server)# source-address { <ADDR> | <IPV6-ADDR> }**	<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::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
10	Задать интерфейс или туннель маршрутизатора, IPv4/IPv6-адрес которого будет использоваться в качестве IPv4/IPv6-адреса источника в отправляемых RADIUS-пакетах.	**esr(config-radius-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.
11	Указать radius в качестве метода аутентификации.	**esr(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.

Шаг	Описание	Команда	Ключи
12	Указать radius в качестве способа аутентификации повышения привилегий пользователей.	**esr(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.
13	Указать способ перебора методов аутентификации в случае отказа (не обязательно).	**esr(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.
14	Сконфигурировать radius в списке способов учета сессий пользователей (не обязательно).	**esr(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.	**esr(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.	**esr(config-line-console)# login authentication <NAME>**	<NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 8.
17	Активировать список аутентификации повышения привилегий пользователей.	**esr(config-line-console)# enable authentication <NAME>**	<NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 9.

15.1.3 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).	**esr(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).	**esr(config)# tacacs-server timeout <SEC>**	<SEC> – период времени в секундах, принимает значения [1..30]. Значение по умолчанию: 3 секунды.
3	Добавить TACACS-сервер в список используемых серверов и перейти в режим его конфигурирования.	**esr(config)# tacacs -server host { <IP-ADDR> | <IPV6-ADDR> } [vrf <VRF>]** **esr(config-tacacs-server)#**	<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, задается строкой до 31 символа.

Шаг	Описание	Команда	Ключи
4	Указать количество неудачных попыток аутентификации для блокировки логина пользователя и время блокировки (не обязательно)	**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	Задать пароль для аутентификации на удаленном TACACS-сервере	**esr(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.
6	Задать номер порта для обмена данными с удаленным TACACS-сервером (не обязательно).	**esr(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.
7	Задать приоритет использования удаленного TACACS сервера (не обязательно).	**esr(config-tacacs-server)# priority <PRIORITY>**	<PRIORITY> – приоритет использования удаленного сервера, принимает значения [1..65535]. Чем ниже значение, тем приоритетнее сервер. Значение по умолчанию: 1.
8	Задать IPv4/IPv6-адрес, который будет использоваться в качестве IP/IPv6-адреса источника в отправляемых TACACS-пакетах.	**esr(config-tacacs-server)# source-address { <ADDR> | <IPV6-ADDR> }**	<ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Шаг	Описание	Команда	Ключи
9	Задать интерфейс или туннель маршрутизатора, IPv4/IPv6-адрес которого будет использоваться в качестве IPv4/IPv6-адреса источника в отправляемых TACACS-пакетах.	**esr(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.
10	Указать TACACS в качестве способа аутентификации повышения привилегий пользователей.	**esr(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.
11	Указать способ перебора методов аутентификации в случае отказа (не обязательно).	**esr(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
12	Сконфигуровать список способов учета команд, введённых в CLI (не обязательно).	**esr(config)# aaa accounting commands stop-only tacacs**	
13	Сконфигурировать tacacs в списке способов учета сессий пользователей (не обязательно).	**esr(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.
14	Перейти в режим конфигурирования соответствующего терминала.	**esr(config)# line <TYPE>**	<TYPE> – тип консоли: • console – локальная консоль; • ssh – защищенная удаленная консоль.
15	Активировать список аутентификации входа пользователей в систему.	**esr(config-line-console)# login authentication <NAME>**	<NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 7.
16	Активировать список аутентификации повышения привилегий пользователей.	**esr(config-line-console)# enable authentication <NAME>**	<NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 8.

15.1.4 Алгоритм настройки AAA по протоколу LDAP

Шаг	Описание	Команда	Ключи
1	Задать базовый DN (Distinguished name), который будет использоваться при поиске пользователей.	**esr(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).	**esr(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.	**esr(config)# ldap-server bind authenticate root-dn <NAME>**	<NAME> – DN пользователя с правами администратора, задается строкой до 255 символов.

Шаг	Описание	Команда	Ключи
4	Задать пароль пользователя с правами администратора, под которым будет происходить авторизация на LDAP-сервере при поиске пользователей.	**esr(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).	**esr(config)# ldap-server search filter user-object-class <NAME>**	<NAME> – имя класса объектов, задаётся строкой до 127 символов. Значение по умолчанию: posixAccount.
6	Задать область поиска пользователей в дереве LDAP-сервера (не обязательно).	**esr(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).	**esr(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).	**esr(config)# ldap-server naming-attribute <NAME>**	<NAME> – имя атрибута объекта, задаётся строкой до 127 символов. Значение по умолчанию: uid.

Шаг	Описание	Команда	Ключи
9	Задать имя атрибута объекта, значение которого будет определять начальные привилегии пользователя на устройстве (не обязательно).	**esr(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).	**esr(config)# ldap-server dscp <DSCP>**	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 63.
11	Добавить LDAP-сервер в список используемых серверов и перейти в режим его конфигурирования.	**esr(config)# ldap -server host { <IP-ADDR> | <IPV6-ADDR> } [vrf <VRF>]** **esr(config-ldap-server)#**	<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	Указать количество неудачных попыток аутентификации для блокировки логина пользователя и время блокировки (не обязательно).	**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.

Шаг	Описание	Команда	Ключи
13	Задать номер порта для обмена данными с удаленным LDAP-сервером (не обязательно).	**esr(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.
14	Задать приоритет использования удаленного LDAP-сервера (не обязательно).	**esr(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.	**esr(config-ldap-server)# source-address { <ADDR> | <IPV6-ADDR> }**	<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::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
16	Задать интерфейс или туннель маршрутизатора, IPv4/IPv6-адрес которого будет использоваться в качестве IPv4/IPv6-адреса источника в отправляемых LDAP-пакетах.	**esr(config-ldap-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
17	Указать LDAP в качестве метода аутентификации.	**esr(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.
18	Указать LDAP в качестве способа аутентификации повышения привилегий пользователей.	**esr(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.

Шаг	Описание	Команда	Ключи
19	Указать способ перебора методов аутентификации в случае отказа.	**esr(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.	**esr(config)# line <TYPE>**	<TYPE> – тип консоли: • console – локальная консоль; • ssh – защищенная удаленная консоль.
21	Активировать список аутентификации входа пользователей в систему.	**esr(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.	**esr(config-line-console)# enable authentication <NAME>**	<NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 15.

15.1.5 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):

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

Создадим профиль аутентификации:

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

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

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

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

```
esr# show aaa radius-servers
```

Посмотреть профили аутентификации можно командой:

```
esr# show aaa authentication
```

15.2 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.

15.2.1 Алгоритм настройки

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

```
esr(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.

15.2.2 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:

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

15.3 Настройка логирования и защиты от сетевых атак

15.3.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Включить защиту от ICMP flood-атак.	**esr(config)# ip firewall screen dos-defense icmp-threshold { <NUM> }**	<NUM> – количество ICMP-пакетов в секунду, задается в диапазоне [1..10000].
2	Включить защиту от land-атак.	**esr(config)# firewall screen dos-defense land**	
3	Включить ограничение числа пакетов, отправляемых за одну секунду на один адрес назначения	**esr(config)# ip firewall screen dos-defense limit-session-destination { <NUM> }**	<NUM> – ограничение числа IP-пакетов в секунду, задается в диапазоне [1..10000].
4	Включить ограничение числа пакетов, отправляемых за одну секунду с единого адреса источника	**esr(config)# ip firewall screen dos-defense limit-session-source { <NUM> }**	<NUM> – ограничение числа IP-пакетов в секунду, задается в диапазоне [1..10000].
5	Включить защиту от SYN flood-атак.	**esr(config)# ip firewall screen dos-defense syn-flood { <NUM> } [src-dsr]**	<NUM> – максимальное количество TCP пакетов с установленным флагом SYN в секунду, задается в диапазоне [1..10000]. src-dst – ограничение количества TCP пакетов с установленным флагом SYN на основании адреса источника и адреса назначения.
6	Включить защиту от UDP flood-атак.	**esr(config)# ip firewall screen dos-defense udp-threshold { <NUM> }**	<NUM> – максимальное количество UDP пакетов в секунду, задается в диапазоне [1..10000].

Шаг	Описание	Команда	Ключи
7	Включить защиту от winnuke-атак.	**esr(config)# ip firewall screen dos-defense winnuke**	
8	Включить блокировку TCP-пакетов с установленным флагом FIN и не установленным флагом ACK.	**esr(config)# ip firewall screen spy-blocking fin-no-ack**	
9	Включить блокировку ICMP-пакетов различных типов.	**esr(config)# ip firewall screen spy-blocking icmp-type**	<TYPE> – тип ICMP, может принимать значения: • destination-unreachable • echo-request • reserved • source-quench • time-exceeded
10	Включить защиту от IP sweep-атак.	**esr(config)# ip firewall screen spy-blocking ip-sweep { <NUM> }**	<NUM> – интервал выявления ip sweep атаки, задается в миллисекундах [1..1000000].
11	Включить защиту от port scan-атак.	**esr(config)# ip firewall screen spy-blocking port-scan { <threshold> } [<TIME>]**	<threshold> – интервал в секундах, в течение которого будет фиксироваться port scan-атака [1..10000]. <TIME> – время блокировки в миллисекундах [1..1000000].
12	Включить защиту от IP spoofing-атак.	**esr(config)# ip firewall screen spy-blocking spoofing**	
13	Включить блокировку TCP-пакетов, с установленными флагами SYN и FIN.	**esr(config)# ip firewall screen spy-blocking syn-fin**	
14	Включить блокировку TCP-пакетов, со всеми флагами или с набором флагов: FIN, PSH, URG. Данной командой обеспечивается защита от атаки XMAS.	**esr(config)# ip firewall screen spy-blocking tcp-all-flag**	
15	Включить блокировку TCP-пакетов, с нулевым полем flags.	**esr(config)# ip firewall screen spy-blocking tcp-no-flag**	
16	Включить блокировку фрагментированных ICMP-пакетов.	**esr(config)# ip firewall screen suspicious-packets icmp-fragment**	

Шаг	Описание	Команда	Ключи
17	Включить блокировку фрагментированных IP-пакетов.	**esr(config)# ip firewall screen suspicious-packets ip-fragment**	
18	Включить блокировку ICMP-пакетов длиной более 1024 байт.	**esr(config)# ip firewall screen suspicious-packets icmp-fragment**	
19	Включить блокировку фрагментированных TCP-пакетов, с флагом SYN.	**esr(config)# ip firewall screen suspicious-packets syn-fragment**	
20	Включить блокировку фрагментированных UDP-пакетов.	**esr(config)# ip firewall screen suspicious-packets udp-fragment**	
21	Включить блокировку пакетов, с ID протокола в заголовке IP равном 137 и более.	**esr(config)# ip firewall screen suspicious-packets unknown-protocols**	
22	Установить частоту оповещения (по SNMP, syslog и в CLI) об обнаруженных и отраженных сетевых атаках.	**esr(config)# ip firewall logging interval <NUM>**	<NUM> – интервал времени в секундах [30 .. 2147483647].
23	Включить более детальный вывод сообщений по обнаруженным и отраженным сетевым атакам в CLI.	**esr(config)# logging firewall screen detailed**	
24	Включить механизм обнаружения и логирования DoS-атак через CLI, syslog и по SNMP.	**esr(config)# logging firewall screen dos-defense <ATACK_TYPE>**	<ATACK_TYPE> – тип DoS-атаки, принимает значения: icmp-threshold, land, limit-session-destination, limit-session-source, syn-flood, udp-threshold, winnuke.
25	Включить механизм обнаружения и логирования шпионской активности через CLI, syslog и по SNMP.	**esr(config)# logging firewall screen spy-blocking { <ATACK_TYPE> | icmp-type <ICMP_TYPE> }**	<ATACK_TYPE> – тип шпионской активности, принимает значения: fin-no-ack, ip-sweep, port-scan, spoofing, syn-fin, tcp-all-flag, tcp-no-flag. <ICMP_TYPE> – тип ICMP, принимает значения: destination-unreachable, echo-request, reserved, source-quench, time-exceeded.

Шаг	Описание	Команда	Ключи
26	Включить механизм обнаружения нестандартных пакетов и логирования через CLI, syslog и по SNMP.	**esr(config)# logging firewall screen suspicious-packets <PACKET_TYPE>**	<PACKET_TYPE> – тип нестандартных пакетов, принимает значения: icmp-fragment, ip-fragment, large-icmp, syn-fragment, udp-fragment, unknown-protocols.

15.3.2 Описание механизмов защиты от атак

Команда	Описание
ip firewall screen dos-defense icmp-threshold	Данная команда включает защиту от ICMP flood-атак. При включенной защите ограничивается количество ICMP-пакетов всех типов в секунду для одного адреса назначения. Атака приводит к перегрузке хоста и выводу его из строя из-за необходимости обрабатывать каждый запрос и отвечать на него.
firewall screen dos-defense land	Данная команда включает защиту от land-атак. При включенной защите блокируются пакеты с одинаковыми source и destination IP-адресами, и флагом SYN в заголовке TCP. Атака приводит к перегрузке хоста и выводу его из строя из-за необходимости обрабатывать каждый TCP SYN пакет и попыток хоста установить TCP-сессию с самим собой.
ip firewall screen dos-defense limit-session-destination	Когда таблица IP-сессий хоста переполняется, он больше не в состоянии организовывать новые сессии и отбрасывает запросы (такое может происходить при различных DoS-атаках: SYN flood, UDP flood, ICMP flood, и т.д.). Команда включает ограничение числа пакетов, передаваемых за секунду на один адреса назначения, которое смягчает DoS-атаки.
ip firewall screen dos-defense limit-session-source	Когда таблица IP-сессий хоста переполняется, он больше не в состоянии организовывать новые сессии и отбрасывает запросы (такое может происходить при различных DoS-атаках: SYN flood, UDP flood, ICMP flood, и т.д.). Команда включает ограничение числа пакетов, передаваемых за секунду с одного адреса источника, которое смягчает DoS-атаки.
ip firewall screen dos-defense syn-flood	Данная команда включает защиту от SYN flood-атак. При включенной защите ограничивается количество TCP-пакетов с установленным флагом SYN в секунду для одного адреса назначения. Атака приводит к перегрузке хоста и выводу его из строя из-за необходимости обрабатывать каждый TCP SYN пакет и попыток установить TCP-сессии.
ip firewall screen dos-defense udp-threshold	Данная команда включает защиту от UDP flood-атак. При включенной защите ограничивается количество UDP пакетов в секунду для одного адреса назначения. Атака приводит к перегрузке хоста и выводу его из строя из-за массивного UDP-трафика.
ip firewall screen dos-defense winnuke	Данная команда включает защиту от winnuke-атак. При включенной защите блокируются TCP-пакеты с установленным флагом URG и 139 портом назначения. Атака приводит к выходу из строя старых версий Windows (до 95 версии).
ip firewall screen spy-blocking fin-no-ack	Данная команда включает блокировку TCP-пакетов с установленным флагом FIN и не установленным флагом ACK. Такие пакеты являются нестандартными, и по ответу можно определить операционную систему жертвы.

Команда	Описание
ip firewall screen spy-blocking icmp-type destination-unreachable	Данная команда включает блокировку всех ICMP-пакетов 3 типа (destination-unreachable), включая пакеты, сгенерированные самим маршрутизатором. Защита не дает злоумышленнику узнать о топологии сети и доступности хостов.
ip firewall screen spy-blocking icmp-type echo-request	Данная команда включает блокировку всех ICMP-пакетов 8 типа (echo-request), включая пакеты, сгенерированные самим маршрутизатором. Защита не дает злоумышленнику узнать о топологии сети и доступности хостов.
ip firewall screen spy-blocking icmp-type reserved	Данная команда включает блокировку всех ICMP-пакетов 2 и 7 типов (reserved), включая пакеты, сгенерированные самим маршрутизатором. Защита не дает злоумышленнику узнать о топологии сети и доступности хостов.
ip firewall screen spy-blocking icmp-type source-quench	Данная команда включает блокировку всех ICMP-пакетов 4 типа (source quench), включая пакеты, сгенерированные самим маршрутизатором. Защита не дает злоумышленнику узнать о топологии сети и доступности хостов.
ip firewall screen spy-blocking icmp-type time-exceeded	Данная команда включает блокировку всех ICMP-пакетов 11 типа (time exceeded), включая пакеты, сгенерированные самим маршрутизатором. Защита не дает злоумышленнику узнать о топологии сети и доступности хостов.
ip firewall screen spy-blocking ip-sweep	Данная команда включает защиту от IP sweep-атак. При включенной защите, если в течение заданного в параметрах интервала приходит более 10 ICMP-запросов от одного источника, первые 10 запросов пропускаются маршрутизатором, а 11 и последующие отбрасываются на оставшееся время интервала. Защита не дает злоумышленнику узнать о топологии сети и доступности хостов.
ip firewall screen spy-blocking port-scan	Данная команда включает защиту от port scan-атак. Если в течение первого заданного интервала времени (<threshold>) на один источник приходит более 10 TCP-пакетов с флагом SYN на разные TCP-порты, или более 10 UDP-пакетов, на разные UDP-порты, то такое поведение фиксируется как port scan атака и все последующие пакеты такого рода от источника блокируются на второй заданный интервал времени (<TIME>). Злоумышленник не сможет быстро просканировать открытые порты на устройстве.
ip firewall screen spy-blocking spoofing	Данная команда включает защиту от ip spoofing-атак. При включенной защите маршрутизатор проверяет пакеты на соответствие адреса источника и записей в таблице маршрутизации и в случае несоответствия пакет отбрасывается. Например, если пакет с адресом источника 10.0.0.1/24 приходит на интерфейс Gi1/0/1, а в таблице маршрутизации данная подсеть располагается за интерфейсом Gi1/0/2, то считается, что адрес источника был подменен. Защищает от вторжений в сеть с подмененными source IP-адресами.
ip firewall screen spy-blocking syn-fin	Данная команда включает блокировку TCP-пакетов с установленными флагами SYN и FIN. Такие пакеты являются нестандартными и по ответу можно определить операционную систему жертвы.

Команда	Описание
ip firewall screen spy-blocking tcp-all-flag	Данная команда включает блокировку TCP-пакетов со всеми флагами или с набором флагов: FIN, PSH, URG. Обеспечивается защита от атаки XMAS.
ip firewall screen spy-blocking tcp-no-flag	Данная команда включает блокировку TCP-пакетов с нулевым полем flags. Такие пакеты являются нестандартными и по ответу можно определить операционную систему жертвы.
ip firewall screen suspicious-packets icmp-fragment	Данная команда включает блокировку фрагментированных ICMP-пакетов. ICMP-пакеты обычно небольшого размера и необходимости в их фрагментировании нет.
ip firewall screen suspicious-packets ip-fragment	Данная команда включает блокировку фрагментированных пакетов.
ip firewall screen suspicious-packets large-icmp	Данная команда включает блокировку ICMP-пакетов длиной более 1024 байт.
ip firewall screen suspicious-packets syn-fragment	Данная команда включает блокировку фрагментированных TCP-пакетов с флагом SYN. TCP пакеты с SYN флагом обычно небольшого размера и необходимости в их фрагментировании нет. Защита предотвращает накопление фрагментированных пакетов в буфере.
ip firewall screen suspicious-packets udp-fragment	Данная команда включает блокировку фрагментированных UDP-пакетов.
ip firewall screen suspicious-packets unknown-protocols	Данная команда включает блокировку пакетов, с ID протокола в заголовке IP равном 137 и более.

15.3.3 Пример настройки логирования и защиты от сетевых атак

Задача:

Необходимо защитить LAN сеть и маршрутизатор ESR от сетевых атак land, syn-flood, ICMP flood и настроить оповещение об атаках по SNMP на SNMP-сервер 192.168.0.10.

Решение:

Предварительно необходимо настроить интерфейсы и firewall (настройка firewall или ее отсутствие не повлияют на работу защиты от сетевых атак):

```
esr(config)# security zone LAN
esr(config-zone)# exit
esr(config)# security zone WAN
esr(config-zone)# exit
esr(config)# security zone-pair LAN WAN
esr(config-zone-pair)# rule 100
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# ex
esr(config-zone-pair)# exit
esr(config)# security zone-pair WAN LAN
esr(config-zone-pair)# rule 100
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# security-zone LAN
esr(config-if-gi)# ip address 192.168.0.1/24
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# security-zone WAN
esr(config-if-gi)# ip address 10.0.0.1/24
esr(config-if-gi)# exit
```

Настроим защиту от land, syn-flood, ICMP flood-атак:

```
esr(config)# ip firewall screen dos-defense land
esr(config)# ip firewall screen dos-defense syn-flood 100 src-dst
esr(config)# ip firewall screen dos-defense icmp-threshold 100
```

Настроим логирование обнаруженных атак:

```
esr(config)# logging firewall screen dos-defense land
esr(config)# logging firewall screen dos-defense syn-flood
esr(config)# logging firewall screen dos-defense icmp-threshold
```

Настроим SNMP-сервер, на который будут отправляться трапы:

```
esr(config)# snmp-server
esr(config)# snmp-server host 192.168.0.10
esr(config)# snmp-server enable traps screen land
esr(config)# snmp-server enable traps screen syn-flood
esr(config)# snmp-server enable traps screen icmp-threshold
```

Посмотреть статистику по зафиксированным сетевым атакам можно командой:

```
esr# show ip firewall screen counters
```

15.4 Конфигурирование Firewall

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

15.4.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать зоны безопасности.	**esr(config)# security zone <zone-name1>** **esr(config)# security zone <zone-name2>**	<zone-name> – до 12 символов. Имена all, any и self зарезервированы.
2	Задать описание зоны безопасности.	**esr(config-zone)# description <description>**	<description> – до 255 символов.
3	Указать экземпляр VRF, в котором будет работать данная зона безопасности (не обязательно).	**esr(config- zone)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.
4	Включить счетчики сессий для NAT и Firewall (не обязательно, снижает производительность).	**esr(config)# ip firewall sessions counters**	

Шаг	Описание	Команда	Ключи
5	Отключить фильтрацию пакетов, для которых не удалось определить принадлежность к какому-либо известному соединению и которые не являются началом нового соединения (не обязательно, снижает производительность).	**esr(config)# ip firewall sessions allow-unknown**	
6	Выбрать режим работы межсетевого экрана (не обязательно) В режиме stateful проверяется только первый пакет сессии, и если "прямой" трафик разрешён, "ответный" трафик разрешается автоматически. В режиме stateless происходит проверка каждого пакета. "Прямой" и "ответный" трафик требуется разрешать в соответствующих zone-pair (см. шаг 29) Работа межсетевого экрана по списку приложений возможна только в режиме stateless	**esr(config)# ip firewall mode <MODE>**	<MODE> – режим работы межсетевого экрана, может принимать значения: stateful, stateless. Значение по умолчанию: stateful
7	Определить время жизни сессии для неподдерживаемых протоколов (не обязательно).	**esr(config)# ip firewall sessions generic-timeout <TIME>**	<TIME> – время жизни сессии для неподдерживаемых протоколов, принимает значения в секундах [1..8553600]. По умолчанию: 60 секунд.
8	Определить время жизни ICMP-сессии, по истечении которого она считается устаревшей (не обязательно).	**esr(config)# ip firewall sessions icmp-timeout <TIME>**	<TIME> – время жизни ICMP-сессии, принимает значения в секундах [1..8553600]. По умолчанию: 30 секунд.
9	Определить время жизни ICMPv6-сессии, по истечении которого она считается устаревшей (не обязательно).	**esr(config)# ip firewall sessions icmpv6-timeout <TIME>**	<TIME> – время жизни ICMP-сессии, принимает значения в секундах [1..8553600]. По умолчанию: 30 секунд.
10	Определить размер таблицы сессий ожидающих обработки (не обязательно).	**esr(config)# ip firewall sessions max-expect <COUNT>**	<COUNT> – размер таблицы, принимает значения [1..8553600]. По умолчанию: 256.

Шаг	Описание	Команда	Ключи
11	Определить размер таблицы отслеживаемых сессий (не обязательно).	**esr(config)# ip firewall sessions max-tracking <COUNT>**	<COUNT> – размер таблицы, принимает значения [1..8553600]. По умолчанию: 512000.
12	Определить время жизни TCP-сессии в состоянии «соединение устанавливается», по истечении которого она считается устаревшей (не обязательно).	**esr(config)# ip firewall sessions tcp-connect-timeout <TIME>**	<TIME> – время жизни TCP-сессии в состоянии "соединение устанавливается", принимает значения в секундах [1..8553600]. По умолчанию: 60 секунд.
13	Определить время жизни TCP-сессии в состоянии "соединение закрывается", по истечении которого она считается устаревшей (не обязательно).	**esr(config)# ip firewall sessions tcp-disconnect-timeout <TIME>**	<TIME> – время жизни TCP-сессии в состоянии "соединение закрывается", принимает значения в секундах [1..8553600]. По умолчанию: 30 секунд.
14	Определить время жизни TCP-сессии в состоянии "соединение установлено", по истечении которого она считается устаревшей (не обязательно).	**esr(config)# ip firewall sessions tcp-established-timeout <TIME>**	<TIME> – время жизни TCP-сессии в состоянии "соединение установлено", принимает значения в секундах [1..8553600]. По умолчанию: 120 секунд.
15	Определить время ожидания, по истечении которого происходит фактическое удаление закрытой TCP-сессии из таблицы отслеживаемых сессий (не обязательно).	**esr(config)# ip firewall sessions tcp-latecome-timeout <TIME>**	<TIME> – время ожидания, принимает значения в секундах [1..8553600]. По умолчанию: 120 секунд.

Шаг	Описание	Команда	Ключи
16	Включить функцию отслеживания сессий уровня приложений для отдельных протоколов (не обязательно).	**esr(config)# ip firewall sessions tracking**	<PROTOCOL> – протокол уровня приложений [ftp, h323, pptp, netbios-ns, tftp], сессии которого должны отслеживаться. <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. Вместо имени отдельного протокола можно использовать ключ "all", который включает функцию отслеживания сессий уровня приложений для всех доступных протоколов. По умолчанию – отключено для всех протоколов.
17	Определить время жизни UDP-сессии в состоянии "соединение подтверждено", по истечении которого она считается устаревшей (не обязательно).	**esr(config)# ip firewall sessions udp-assured-timeout <TIME>**	<TIME> – время жизни UDP-сессии в состоянии "соединение подтверждено", принимает значения в секундах [1..8553600]. По умолчанию: 180 секунд.
18	Определить время жизни UDP-сессии в состоянии «соединение не подтверждено», по истечении которого она считается устаревшей.	**esr(config)# ip firewall sessions udp-wait-timeout <TIME>**	<TIME> – время жизни UDP-сессии в состоянии «соединение не подтверждено», принимает значения в секундах [1..8553600]. По умолчанию: 30 секунд.
19	Создать списки IP-адресов, которые будут использоваться при фильтрации.	**esr(config)# object-group network <obj-group-name>**	<obj-group-name> – до 31 символа.
20	Задать описание списка IP-адресов (не обязательно).	**esr(config-object-group-network)# description <description>**	<description> – описание профиля, задается строкой до 255 символов.

Шаг	Описание	Команда	Ключи
21	Внести необходимые IPv4/IPv6-адреса в список.	**esr(config-object-group-network)# ip prefix <ADDR/LEN>**	<ADDR/LEN> – подсеть, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].
		esr(config-object-group-network)# ip address-range <FROM-ADDR>-<TO-ADDR>	<FROM-ADDR> – начальный IP-адрес диапазона адресов; <TO-ADDR> – конечный IP-адрес диапазона адресов, опциональный параметр. Если параметр не указан, то командой задаётся одиночный IP-адрес. Адреса задаются в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
		esr(config-object-group-network)# ipv6 prefix <IPV6-ADDR/LEN>	<IPV6-ADDR/LEN> – IP-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].
		esr(config-object-group-network)# ipv6 address-range <FROM-ADDR>-<TO-ADDR>	<FROM-ADDR> – начальный IPv6-адрес диапазона адресов; <TO-ADDR> – конечный IPv6-адрес диапазона адресов, опциональный параметр. Если параметр не указан, то командой задаётся одиночный IPv6-адрес. Адреса задаются в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
22	Создать списки сервисов, которые будут использоваться при фильтрации.	**esr(config)# object-group service <obj-group-name>**	<obj-group-name> – имя профиля сервисов, задается строкой до 31 символа.

Шаг	Описание	Команда	Ключи
23	Задать описание списка сервисов (не обязательно).	**esr(config-object-group-service)# description <description>**	<description> – описание профиля, задается строкой до 255 символов.
24	Внести необходимые сервисы (tcp/udp-порты) в список.	**esr(config-object-group-service)# port-range <port>**	<port> – принимает значение [1..65535]. Можно указать несколько портов перечислением через запятую «,» либо указать диапазон портов через «-».
25	Создать списки приложений, которые будут использоваться в механизме DPI.	**esr(config)# object-group application <NAME>**	<NAME> – имя профиля приложений, задается строкой до 31 символа.
26	Задать описание списка приложений (не обязательно).	**esr(config-object-group-application)# description <description>**	<description> – описание профиля, задается строкой до 255 символов.
27	Внести необходимые приложения в списки.	**esr(config-object-group-application)# application < APPLICATION >**	<APPLICATION> – указывает приложение подпадающее под действие данного профиля
28	Включить интерфейсы (физические, логические, E1/Multilink и подключаемые), сервер удаленного доступа (l2tp, openvpn, pptp) или туннели (gre, ip4ip4, l2tp, lt, pppoe, pptp) в зоны безопасности (если необходимо).	**esr(config-if-gi)# security-zone <zone-name>**	<zone-name> – до 12 символов.
	Отключить функции Firewall на сетевом интерфейсе (физические, логические, E1/Multilink и подключаемые), сервере удаленного доступа (l2tp, openvpn, pptp) или туннели (gre, ip4ip4, l2tp, lt, pppoe, pptp) (если необходимо)	**esr(config-if-gi)# ip firewall disable**	

Шаг	Описание	Команда	Ключи
29	Создать набор правил межзонового взаимодействия. 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». Очерёдность обработки трафика для разных zone-pair описана в примечании.	**esr(config)# security zone-pair <src-zone-name1> <dst-zone-name2>**	<src-zone-name> – до 12 символов. <dst-zone-name> – до 12 символов.
30	Создать правило межзонового взаимодействия.	**esr(config-zone-pair)# rule <rule-number>**	<rule-number> – 1..10000.
31	Задать описание правила (не обязательно).	**esr(config-zone-rule)# description <description>**	<description> – до 255 символов.
32	Указать действие данного правила.	**esr(config-zone-rule)# action <action> [log]**	<action> – permit/deny/reject/ netflow-sample/sflow-sample log – ключ для активации логирования сессий, устанавливающимися согласно данному правилу.
33	Установить имя или номер IP-протокола, для которого должно срабатывать правило (не обязательно).	**esr(config-zone-rule)# match [not] protocol <protocol-type>**	<protocol-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.
		esr(config-zone-rule)# match [not] protocol-id <protocol-id>	<protocol-id> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF].

Шаг	Описание	Команда	Ключи
34	Установить профиль IP-адресов отправителя, для которых должно срабатывать правило (не обязательно).	**esr(config-zone-rule)# match [not] source-address <OBJ-GROUP-NETWORK-NAME>**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа. При указании значения «any» правило будет срабатывать для любого IP-адреса отправителя/получателя.
35	Установить профиль IP-адресов получателя, для которых должно срабатывать правило (не обязательно).	**esr(config-zone-rule)# match [not] destination-address <OBJ-GROUP-NETWORK-NAME>**	
36	Установить MAC-адрес отправителя, для которого должно срабатывать правило (не обязательно).	**esr(config-zone-rule)# match [not] source-mac <mac-addr>**	<mac-addr> – задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF].
37	Установить MAC-адрес получателя, для которого должно срабатывать правило (не обязательно).	**esr(config-zone-rule)# match [not] destination-mac <mac-addr>**	
38	Установить профиль TCP/UDP-портов отправителя, для которых должно срабатывать правило (если указан протокол).	**esr(config-zone-rule)# match [not] source-port <PORT-SET-NAME>**	<PORT-SET-NAME> – задаётся строкой до 31 символа. При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта отправителя/получателя.
39	Установить профиль TCP/UDP-портов получателя, для которых должно срабатывать правило (если указан протокол).	**esr(config-zone-rule)# match [not] destination-port <PORT-SET-NAME>**	
40	Установить тип и код сообщений протокола ICMP, для которых должно срабатывать правило (если в качестве протокола выбран ICMP) (не обязательно).	**esr(config-zone-rule)# match [not] icmp <ICMP_TYPE> <ICMP_CODE>**	<ICMP_TYPE> – тип сообщения протокола ICMP, принимает значения [0..255]; <ICMP_CODE> – код сообщения протокола ICMP, принимает значения [0..255]. При указании значения «any» правило будет срабатывать для любого кода сообщения протокола ICMP.
41	Установить ограничение, при котором правило будет срабатывать только для трафика, измененного сервисом трансляции IP-адресов и портов получателя.	**esr(config-zone-rule)# match [not] destination-nat**	

Шаг	Описание	Команда	Ключи
42	Установить максимальную скорость прохождения пакетов (не обязательно, доступно только для zone-pair any self и zone-pair <zone-name> any).	**esr(config-zone-pair-rule)# rate-limit pps <rate-pps>**	<rate-pps> – максимальное количество пакетов, которое может быть передано. Принимает значения [1..10000].
43	Установить фильтрацию только для фрагментированных IP-пакетов (не обязательно, доступно только для zone-pair any self и zone-pair <zone-name> any).	**esr(config-zone-pair-rule)# match [not] fragment**	
44	Установить фильтрацию для IP-пакетов, содержащих ip-option (не обязательно, доступно только для zone-pair any self и zone-pair <zone-name> any).	**esr(config-zone-pair-rule)# match [not] ip-option**	
45	Включить правило межзонового взаимодействия.	**esr(config-zone-rule)# enable**	
46	Активировать фильтрацию и режим отслеживания сессий при прохождении пакетов между участниками одной Bridge-группы (не обязательно, доступно только на ESR-1000/1200/1500/1511/1700 /3100).	**esr(config-bridge)# ports firewall enable**	

[1] При использовании ключа not правило будет срабатывать для значений, которые не входят в указанный профиль.

Очерёдность обработки трафика правилами firewall

Порядок обработки транзитного трафика правилами firewall

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

15.4.2 Пример настройки Firewall

Задача:

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

Решение:

Для каждой сети ESR создадим свою зону безопасности:

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

Настроим сетевые интерфейсы и определим их принадлежность к зонам безопасности:

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

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

```
esr(config)# security zone-pair LAN WAN
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match destination-address WAN_GATEWAY
esr(config-zone-pair-rule)# match source-address LAN_GATEWAY
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-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:*

```
esr(config)# security zone-pair WAN LAN
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match destination-address LAN_GATEWAY
esr(config-zone-pair-rule)# match source-address WAN_GATEWAY
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-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 ESR, для того чтобы маршрутизатор начал отвечать на ICMP-запросы из зоны «WAN»:

```
esr(config)# security zone-pair WAN self
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match destination-address WAN
esr(config-zone-pair-rule)# match source-address WAN_GATEWAY
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
```

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

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

Посмотреть членство портов в зонах можно с помощью команды:

```
esr# show security zone
```

Посмотреть пары зон и их конфигурацию можно с помощью команд:

```
esr# show security zone-pair
esr# show security zone-pair configuration
```

Посмотреть активные сессии можно с помощью команд:

```
esr# show ip firewall sessions
```

15.4.3 Пример настройки фильтрации приложений (DPI)

Использование механизма фильтрации приложений многократно снижает производительность маршрутизатора из-за необходимости проверки каждого пакета. Производительность снижается с ростом количества выбранных приложений для фильтрации.

Задача:

Блокировать доступ к ресурсам youtube, bittorrent и facebook.

Решение:

Для каждой сети ESR создадим свою зону безопасности:

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

Настроим сетевые интерфейсы и определим их принадлежность к зонам безопасности:

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

Переключаем режим работы межсетевого экрана ESR в stateless:

```
esr(config)# ip firewall mode stateless
```

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

```
esr(config)# object-group application APP
esr(config-object-group-application)# application youtube
esr(config-object-group-application)# application bittorrent
esr(config-object-group-application)# application facebook
esr(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:*

```
esr(config)# security zone-pair WAN LAN
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action deny
esr(config-zone-pair-rule)# match application APP
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# rule 2
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-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:*

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

Посмотреть членство портов в зонах можно с помощью команды:

```
esr# show security zone
```

Посмотреть пары зон и их конфигурацию можно с помощью команд:

```
esr# show security zone-pair
esr# show security zone-pair configuration
```

Посмотреть активные сессии можно с помощью команд:

```
esr# show ip firewall sessions
```

15.5 Настройка списков доступа (ACL)

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

15.5.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать список контроля доступа и перейти в режим его конфигурирования.	**esr(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).	**esr(config-acl)# description <DESCRIPTION>**	<DESCRIPTION> – описание списка контроля доступа, задаётся строкой до 255 символов.
3	Создать правило и перейти в режим его конфигурирования. Правила обрабатываются маршрутизатором в порядке возрастания их номеров.	**esr(config-acl)# rule <ORDER>**	<ORDER> – номер правила, принимает значения [1..4094].
4	Указать действие, которое должно быть применено для трафика, удовлетворяющего заданным критериям.	**esr(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).	**esr(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;
		esr(config-acl-rule)# match protocol-id <ID>	<ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF].

Шаг	Описание	Команда	Ключи
6	Установить IP-адреса отправителя, для которых должно срабатывать правило (не обязательно).	**esr(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]; <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.
7	Установить IP-адреса получателя, для которых должно срабатывать правило (не обязательно).	**esr(config-acl-rule)# match destination-address { <ADDR> <MASK> | any }**	
8	Установить MAC-адреса отправителя, для которых должно срабатывать правило (не обязательно).	**esr(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]; <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.
9	Установить MAC-адреса получателя, для которых должно срабатывать правило (не обязательно).	**esr(config-acl-rule)# match destination-mac <ADDR><WILDCARD>**	
10	Установить номер TCP/UDP-порта отправителя, для которого должно срабатывать правило (если указан протокол).	**esr(config-acl-rule)# match source-port { <PORT> | any }**	<PORT> – номер TCP/UDP-порта отправителя, принимает значения [1..65535]. При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта отправителя.
11	Установить номер TCP/UDP-порта получателя, для которого должно срабатывать правило (если указан протокол).	**esr(config-acl-rule)# match destination-port { <PORT> | any }**	
12	Установить значение 802.1p приоритета, для которого должно срабатывать правило (не обязательно).	**esr(config-acl-rule)# match c os <COS>**	<COS> – значение 802.1p приоритета, принимает значения [0..7].

Шаг	Описание	Команда	Ключи
13	Установить значение кода DSCP, для которого должно срабатывать правило (не обязательно). Невозможно использовать совместно с IP Precedence.	**esr(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.	**esr(config-acl-rule)# match ip-precedence <IPP>**	<IPP> – значение кода IP Precedence, принимает значения [0..7].
15	Установить значение идентификационного номера VLAN, для которого должно срабатывать правило (не обязательно).	**esr(config-acl-rule)# match vlan <VID>**	<VID> – идентификационный номер VLAN, принимает значения [1..4094].
16	Активировать правило.	**esr(config-acl-rule)# enable**	
17	Указать список контроля доступа к конфигурируемому интерфейсу для фильтрации входящего трафика.	**esr(config-if-gi)# service-acl input <NAME>**	<NAME> – имя списка контроля доступа, задаётся строкой до 31 символа.

Также списки доступа могут использоваться для организации политик QoS.

15.5.2 Пример настройки списка доступа

Задача:

Разрешить прохождения трафика только из подсети 192.168.20.0/24.

Решение:

Настроим список доступа для фильтрации по подсетям:

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

Применим список доступа на интерфейс Gi1/0/19 для входящего трафика:

```
esr(config)# interface gigabitethernet 1/0/19
esr(config-if-gi)# service-acl input white
```

Просмотреть детальную информацию о списке доступа возможно через команду:

```
esr# show ip access-list white
```

15.6 Настройка IPS/IDS

Данный функционал активируется только при наличии лицензии.

IPS/IDS (*Intrusion Prevention System/Intrusion Detection System*) – система предотвращения вторжений – программная система сетевой и компьютерной безопасности, обнаруживающая вторжения или нарушения безопасности и автоматически защищающая от них.

Работа системы основана на сигнатурном анализе трафика. Сигнатуры для систем IPS/IDS принято называть правилами. Устройства ESR позволяют скачивать актуальные правила с открытых источников в сети Интернет или с корпоративного сервера. Также с помощью CLI можно создавать свои специфические правила.

По умолчанию на устройствах ESR установлен базовый набор правил от компании EmergingThreats, предназначенный для тестирования и проверки работоспособности системы.

15.6.1 Алгоритм базовой настройки

Шаг	Описание	Команда	Ключи
1	Создать политику безопасности IPS/IDS.	**esr(config)# security ips policy <NAME>**	<NAME> – имя политики безопасности, задаётся строкой до 32 символов.
2	Задать описание политики (не обязательно).	**esr(config-ips-policy)# description <DESCRIPTION>**	<DESCRIPTION> – описание задаётся строкой до 255 символов.
3	Задать профиль IP-адресов, которые будет защищать IPS/IDS.	**esr(config-ips-policy)# protect network-group <OBJ-GROUP-NETWORK_NAME>**	<OBJ-GROUP-NETWORK-NAME> – имя профиля защищаемых IP-адресов, задается строкой до 32 символов.
4	Задать профиль IP-адресов, внешних для IPS/IDS (не обязательно).	**esr(config-ips-policy)# external network-group <OBJ-GROUP-NETWORK_NAME>**	<OBJ-GROUP-NETWORK-NAME> – имя профиля внешних IP-адресов, задается строкой до 32 символов.
5	Перейти в режим конфигурирования IPS/IDS.	**esr(config)# security ips**	

Шаг	Описание	Команда	Ключи
6	Назначить политику безопасности IPS/IDS.	**esr(config-ips)# policy <NAME>**	<NAME> – имя политики безопасности, задаётся строкой до 32 символов
7	Использовать все ресурсы ESR для IPS/IDS (не обязательно).	**esr(config-ips)# perfomance max**	По умолчанию для IPS/IDS отдается половина доступных ядер процессора.

Шаг	Описание	Команда	Ключи
8	Задать параметры удаленного сервера для отправки статистики работы сервиса IPS/IDS в формате EVE (elasticsearch) (не обязательно).	**esr(config-ips)# logging remote-server { <ADDR> | <IPV6-ADDR> } [<TRANSPORT>] [<PORT>] [source-address { <SRC-ADDR> | <IPV6-SRC-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::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <TRANSPORT> – протокол передачи данных, по умолчанию - UDP, принимает значения: • TCP – передача данных осуществляется по протоколу TCP; • UDP – передача данных осуществляется по протоколу UDP; <PORT> – номер TCP/UDP-порта, опциональный параметр, принимает значения [1..65535], по умолчанию 514; <SRC-ADDR> – IPv4-адрес маршрутизатора, который будет использоваться в качестве IP-адреса источника в отправляемых syslog-пакетах, по умолчанию – IPv4-адрес интерфейса, с которого отправляются пакеты; <IPV6-SRC-ADDR> – IPv6-адрес маршрутизатора, который будет использоваться в качестве IP v6-адреса источника в отправляемых syslog-пакетах, по умолчанию – IPv6-адрес интерфейса, с которого отправляются пакеты.
9	Установить интервал отправки статистики работы сервиса IPS/IDS в формате EVE (elasticsearch) (не обязательно).	**esr(config-ips)# logging update-interval <INTERVAL>**	<INTERVAL> – интервал отправки статистики работы сервиса IPS/IDS, задаётся в минутах.

Шаг	Описание	Команда	Ключи
10	Активировать IPS/IDS на интерфейсе.	**esr(config-if-gi)# service-ips { inline | monitor }**	inline – этот режим устанавливается, когда ESR с сервисом IPS/IDS ставится в разрыв сети. monitor – этот режим устанавливается, когда ESR с сервисом IPS/IDS мониторит зеркалируемый трафик.

15.6.2 Алгоритм настройки автообновления правил IPS/IDS из внешних источников

Шаг	Описание	Команда	Ключи
1	Перейти в режим конфигурирования автообновлений.	**esr(config-ips)# auto-upgrade**	
2	Задать имя и перейти в режим конфигурирования пользовательского сервера обновлений.	**esr(config-ips-auto-upgrade)# user-server <WORD>**	<WORD> – имя сервера, задаётся строкой до 32 символов.
3	Задать описание пользовательского сервера обновлений (не обязательно).	**esr(config-ips-upgrade-user-server)# description <DESCRIPTION>**	<DESCRIPTION> – описание задаётся строкой до 255 символов.
4	Задать URL.	**esr(config-ips-upgrade-user-server)# url <URL>**	<URL> – текстовое поле, содержащее URL-ссылку длинной от 8 до 255 символов. В качестве URL-ссылки может быть указан: • файл правил с расширение .rule; • файл классификатора правил с именем classification.config; • каталог на сервере содержащий файлы правил и/или файл классификатора правил.

Шаг	Описание	Команда	Ключи
5	Задать частоту проверки обновлений (не обязательно).	**esr(config-ips-upgrade-user-server)# upgrade interval <HOURS>**	<HOURS> – интервал обновлений в часах, от 1 до 240. Значение по умолчанию: 24 часа.

Для правил IPS/IDS, загружаемых из внешних источников, на маршрутизаторах ESR выделена отдельная область энергозависимой памяти.
Размер этой области зависит от модели ESR:

- **ESR-1X – 25 МБ;**
- **ESR-2X – 50 МБ;**

Для всех остальных моделей – 100 МБ.
Если настроить слишком много источников правил или загружать правила, превышающие указанные лимиты, то маршрутизатор будет выдавать сообщения об ошибке %STORAGE_IPS_MGR-I-ERR: There no free space in rules directory.
В этом случае стоит уменьшить объем запрашиваемых правил.

15.6.3 Рекомендуемые открытые источники обновления правил

https://sslbl.abuse.ch/	SSL Blacklist содержит списки «плохих» SSL-сертификатов, т.е. сертификатов, в отношении которых установлен факт их использования вредоносным ПО и ботнетами. В списках содержатся SHA1 отпечатки публичных ключей из SSL-сертификатов.
https://feodotracker.abuse.ch/	Feodo Tracker – список управляющих серверов для троянской программы Feodo. Feodo (также известный как Cridex или Bugat) используется злоумышленниками для кражи чувствительной информации в сфере электронного банкинга (данные по кредитным картам, логины/пароли) с компьютеров пользователей. В настоящее время существует четыре версии троянской программы (версии A, B, C и D), главным образом отличающиеся инфраструктурой управляющих серверов.
https://rules.emergingthreats.net/open/suricata/rules/botcc.rules	Данные правила описывают известные ботнеты и управляющие сервера. Источники: Shadowserver.org, Zeus Tracker, Palevo Tracker, Feodo Tracker, Ransomware Tracker.
https://rules.emergingthreats.net/open/suricata/rules/ciarmy.rules	Данные правила описывают вредоносные хосты по классификации проекта www.cinsarmy.com.
https://rules.emergingthreats.net/open/suricata/rules/compromised.rules	Данные правила описывают известные скомпрометированные и вредоносные хосты. Источники: Daniel Gerzo's BruteForceBlocker, The OpenBL, Emerging Threats Sandnet, SidReporter Projects.
https://rules.emergingthreats.net/open/suricata/rules/drop.rules	Данные правила описывают спамерские хосты / сети по классификации проекта www.spamhaus.org.
https://rules.emergingthreats.net/open/suricata/rules/dshield.rules	Данные правила описывают вредоносные хосты по классификации проекта www.dshield.org.
https://rules.emergingthreats.net/open/suricata/rules/emerging-activex.rules	Данные правила содержат сигнатуры использования ActiveX-контента.
https://rules.emergingthreats.net/open/suricata/rules/emerging-attack_response.rules	Правила, детектирующие поведение хоста после успешно проведенных атак.
https://rules.emergingthreats.net/open/suricata/rules/emerging-chat.rules	Данные правила описывают признаки обращения к популярным чатам.
https://rules.emergingthreats.net/open/suricata/rules/emerging-current_events.rules	Временные правила, ожидающие возможного включения в постоянные списки правил.
https://rules.emergingthreats.net/open/suricata/rules/emerging-dns.rules	Данные правила содержат сигнатуры уязвимостей в протоколе DNS, признаки использования DNS вредоносным ПО, некорректного использования протокола DNS.
https://rules.emergingthreats.net/open/suricata/rules/emerging-dos.rules	Данные правила содержат сигнатуры DOS-атак.
https://rules.emergingthreats.net/open/suricata/rules/emerging-exploit.rules	Данные правила содержат сигнатуры эксплойтов.

https://rules.emergingthreats.net/open/suricata/rules/emerging-ftp.rules	Данные правила содержат сигнатуры уязвимостей в протоколе FTP, признаки некорректного использования протокола FTP.
https://rules.emergingthreats.net/open/suricata/rules/emerging-games.rules	Данные правила описывают признаки обращения к популярным игровым сайтам: World of Warcraft, Starcraft и т.п.
https://rules.emergingthreats.net/open/suricata/rules/emerging-icmp.rules	Данные правила содержат сигнатуры некорректного использования протокола ICMP.
https://rules.emergingthreats.net/open/suricata/rules/emerging-icmp_info.rules	Данные правила содержат сигнатуры информационных ICMP-сообщений.
https://rules.emergingthreats.net/open/suricata/rules/emerging-imap.rules	Данные правила содержат сигнатуры уязвимостей в протоколе IMAP, признаки некорректного использования протокола IMAP.
https://rules.emergingthreats.net/open/suricata/rules/emerging-inappropriate.rules	Данные правила описывают признаки обращения к нежелательным ресурсам.
https://rules.emergingthreats.net/open/suricata/rules/emerging-info.rules	Данные правила содержат сигнатуры различных уязвимостей.
https://rules.emergingthreats.net/open/suricata/rules/emerging-malware.rules	Данные правила содержат сигнатуры вредоносного ПО, использующего в своей работе протокол HTTP.
https://rules.emergingthreats.net/open/suricata/rules/emerging-misc.rules	Данные правила содержат сигнатуры различных уязвимостей.
https://rules.emergingthreats.net/open/suricata/rules/emerging-mobile_malware.rules	Данные правила содержат сигнатуры вредоносного ПО для мобильных платформ.
https://rules.emergingthreats.net/open/suricata/rules/emerging-netbios.rules	Данные правила содержат сигнатуры уязвимостей в протоколе NetBIOS, признаки некорректного использования протокола NetBIOS.
https://rules.emergingthreats.net/open/suricata/rules/emerging-p2p.rules	Данные правила описывают признаки обращения к P2P-сетям (Bittorrent, Gnutella, Limewire).
https://rules.emergingthreats.net/open/suricata/rules/emerging-policy.rules	Данные правила описывают нежелательную сетевую активность (обращение к MySpace, Ebay).
https://rules.emergingthreats.net/open/suricata/rules/emerging-poprules	Данные правила содержат сигнатуры уязвимостей в протоколе POP3, признаки некорректного использования протокола POP3.
https://rules.emergingthreats.net/open/suricata/rules/emerging-rpc.rules	Данные правила содержат сигнатуры уязвимостей в протоколе RPC, признаки некорректного использования протокола RPC.
https://rules.emergingthreats.net/open/suricata/rules/emerging-scada.rules	Данные правила содержат сигнатуры уязвимостей для SCADA-систем.

https://rules.emergingthreats.net/open/suricata/rules/emerging-scan.rules	Данные правила описывают признаки активности, связанной с сетевым сканированием (Nessus, Nikto, portscanning).
https://rules.emergingthreats.net/open/suricata/rules/emerging-shellcode.rules	Данные правила описывают признаки активности, связанной с попытками получить шелл-доступ в результате выполнения эксплойтов.
https://rules.emergingthreats.net/open/suricata/rules/emerging-smtp.rules	Данные правила содержат сигнатуры уязвимостей в протоколе SMTP, признаки некорректного использования протокола SMTP.
https://rules.emergingthreats.net/open/suricata/rules/emerging-sql.rules	Данные правила содержат сигнатуры уязвимостей для СУБД SQL.
https://rules.emergingthreats.net/open/suricata/rules/emerging-telnet.rules	Данные правила содержат сигнатуры уязвимостей для протокола TELNET, признаки некорректного использования протокола TELNET.
https://rules.emergingthreats.net/open/suricata/rules/emerging-tftp.rules	Данные правила содержат сигнатуры уязвимостей в протоколе TFTP, признаки некорректного использования протокола TFTP.
https://rules.emergingthreats.net/open/suricata/rules/emerging-trojan.rules	Данные правила содержат признаки сетевой активности троянских программ.
https://rules.emergingthreats.net/open/suricata/rules/emerging-user_agents.rules	Данные правила содержат признаки подозрительных и потенциально опасных HTTP-клиентов (идентифицируются по значениям в HTTP-заголовке User-Agent).
https://rules.emergingthreats.net/open/suricata/rules/emerging-l.rules	Данные правила содержат сигнатуры уязвимостей в VoIP-протокола.
https://rules.emergingthreats.net/open/suricata/rules/emerging-web_client.rules	Данные правила содержат сигнатуры уязвимостей для веб-клиентов.
https://rules.emergingthreats.net/open/suricata/rules/emerging-web_server.rules	Данные правила содержат сигнатуры уязвимостей для веб-серверов.
https://rules.emergingthreats.net/open/suricata/rules/emerging-web_specific_apps.rules	Данные правила содержат сигнатуры эксплуатации уязвимостей веб-приложений.
https://rules.emergingthreats.net/open/suricata/rules/emerging-worm.rules	Данные правила описывают признаки активности сетевых червей.

15.6.4 Пример настройки IPS/IDS с автообновлением правил

Задача:

Организовать защиту локальной сети с автообновлением правил из открытых источников.

192.168.1.0/24 – локальная сеть.

Решение:

Создадим профиль адресов защищаемой локальной сети:

```
esr(config)# object-group network LAN
esr(config-object-group-network)# ip prefix 192.168.1.0/24
esr(config-object-group-network)# exit
```

Настроим на ESR DNS-клиента для разрешения имен источников обновления правил IPS/IDS:

```
esr(config)# domain lookup enable
esr(config)# domain name-server 8.8.8.8
```

Создадим политику безопасности IPS/IDS:

```
esr(config)# security ips policy OFFICE
esr(config-ips-policy)# description "My Policy"
esr(config-ips-policy)# protect network-group LAN
```

Разрешим работу IPS/IDS на интерфейсе локальной сети bridge 1:

```
esr(config)# bridge 1
esr(config-bridge)# service-ips inline
```

Настроим параметры IPS/IDS:

```
esr(config)# security ips
esr(config-ips)# logging remote-server 192.168.10.1
esr(config-ips)# logging update-interval 15
esr(config-ips)# policy OFFICE
esr(config-ips)# enable
```

Устройство будет использоваться только как шлюз безопасности, по этому отдадим сервису IPS/IDS все доступные ресурсы:

```
esr(config-ips)# perfomance max
```

Настроим автообновление правил с сайтов EmergingThreats.net, etnetera.cz и Abuse.ch:

```
esr(config-ips)# auto-upgrade
esr(config-auto-upgrade)# user-server ET-Open
esr(config-ips-upgrade-user-server)# description "emerging threats open rules"
esr(config-ips-upgrade-user-server)# url https://rules.emergingthreats.net/open/suricata-4.0/
emerging-all.rules
esr(config-ips-upgrade-user-server)# exit
esr(config-auto-upgrade)# user-server Aggressive
esr(config-ips-upgrade-user-server)# description "Etnetera aggressive IP blacklist"
esr(config-ips-upgrade-user-server)# url https://security.etnetera.cz/feeds/
etn_aggressive.rules
esr(config-ips-upgrade-user-server)# upgrade interval 4
esr(config-ips-upgrade-user-server)# exit
esr(config-auto-upgrade)# user-server SSL-BlackList
esr(config-ips-upgrade-user-server)# description "Abuse.ch SSL Blacklist"
esr(config-ips-upgrade-user-server)# url https://sslbl.abuse.ch/blacklist/sslblacklist.rules
esr(config-ips-upgrade-user-server)# upgrade interval 4
esr(config-ips-upgrade-user-server)# exit
esr(config-auto-upgrade)# user-server C2-Botnet
esr(config-ips-upgrade-user-server)# description "Abuse.ch Botnet C2 IP Blacklist"
esr(config-ips-upgrade-user-server)# url https://sslbl.abuse.ch/blacklist/sslipblacklist.rules
esr(config-ips-upgrade-user-server)# upgrade interval 4
esr(config-ips-upgrade-user-server)# exit
```

15.6.5 Алгоритм настройки базовых пользовательских правил

Шаг	Описание	Команда	Ключи
1	Задать имя и перейти в режим конфигурирования набора пользовательских правил.	**esr(config)# security ips-category user-defined <WORD>**	<WORD> – имя набора пользовательских правил, задаётся строкой до 32 символов.
2	Задать описание набора пользовательских правил (не обязательно).	**esr(config-ips-category)# description <DESCRIPTION>**	<DESCRIPTION> – описание задаётся строкой до 255 символов.
3	Создать правило и перейти в режим конфигурирования правила.	**esr(config-ips-category)# rule <ORDER>**	<ORDER> – номер правила, принимает значения [1..512].
4	Задать описание правила (не обязательно).	**esr(config-ips-category-rule)# description <DESCRIPTION>**	<DESCRIPTION> – описание задаётся строкой до 255 символов.

Шаг	Описание	Команда	Ключи
5	Указать действие данного правила.	**esr(config-ips-category-rule)# action { alert | reject | pass | drop }**	• alert – прохождение трафика разрешается, и сервис IPS/IDS генерирует сообщение; • reject – прохождение трафика запрещается. Если это TCP-трафик, отправителю и получателю посылается пакет TCP-RESET, для остального типа трафика посылается пакет ICMP-ERROR. Сервис IPS/IDS генерирует сообщение; • pass – прохождение трафика разрешается; • drop – прохождение трафика запрещается, и сервис IPS/IDS генерирует сообщение.
6	Установить имя IP-протокола, для которого должно срабатывать правило.	**esr(config-ips-category-rule)# protocol <PROTOCOL>**	<PROTOCOL> – принимает значения any/ip/icmp/http/tcp/udp. При указании значения «any» правило будет срабатывать для любых протоколов.

Шаг	Описание	Команда	Ключи
7	Установить IP-адреса отправителя, для которых должно срабатывать правило.	**esr(config-ips-category-rule)# source-address {ip <ADDR> | ip-prefix <ADDR/LEN> | object-group <OBJ_GR_NAME> | policy-object-group { protect | external } | any }**	<ADDR> – IP-адрес отправителя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <ADDR/LEN> – IP-подсеть отправителя, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и LEN принимает значения [1..32]. < OBJ_GR_NAME> – имя профиля IP-адресов, который содержит IP-адреса отправителя, задаётся строкой до 31 символа. • protect – устанавливает в качестве адресов отправителя и protect-адреса определенные адреса в политике IPS/IDS; • external – устанавливает в качестве адресов отправителя и external-адреса определенные адреса в политике IPS/IDS. При указании значения «any» правило будет срабатывать для любого IP-адреса отправителя.
8	Установить номера TCP/UDP-портов отправителя, для которых должно срабатывать правило. Для значения protocol icmp, значение source-port может быть только any.	**esr(config-ips-category-rule)# source-port {any | <PORT> | object-group <OBJ-GR-NAME> }**	<PORT> – номер TCP/UDP-порта отправителя, принимает значения [1..65535]. <OBJ_GR_NAME> – имя профиля TCP/UDP-портов отправителя, задаётся строкой до 31 символа. При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта отправителя.

Шаг	Описание	Команда	Ключи
9	Установить IP-адреса получателя, для которых должно срабатывать правило.	**esr(config-ips-category-rule)# destination-address {ip <ADDR> | ip-prefix <ADDR/LEN> | object-group <OBJ_GR_NAME> | policy-object-group { protect | external } | any }**	<ADDR> – IP-адрес получателя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <ADDR/LEN> – IP-подсеть получателя, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и LEN принимает значения [1..32]. <OBJ_GR_NAME> – имя профиля IP-адресов, который содержит IP-адреса получателя, задаётся строкой до 31 символа. • protect – устанавливает в качестве адресов получателя protect-адреса, определенные в политике IPS/IDS; • external – устанавливает в качестве адресов получателя external-адреса, определенные в политике IPS/IDS. При указании значения «any» правило будет срабатывать для любого IP-адреса получателя.
10	Установить номера TCP/UDP-портов получателя, для которых должно срабатывать правило. Для значения protocol icmp, значение destination-port может быть только any.	**esr(config-ips-category-rule)# destination-port {any | <PORT> | object-group <OBJ-GR-NAME> }**	<PORT> – номер TCP/UDP-порта получателя, принимает значения [1..65535]. <OBJ_GR_NAME> – имя профиля TCP/UDP портов получателя, задаётся строкой до 31 символа. При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта получателя.

Шаг	Описание	Команда	Ключи
11	Установить направление потока трафика, для которого должно срабатывать правило.	**esr(config-ips-category-rule)# direction { one-way | round-trip }**	• one-way – трафик передаётся в одну сторону. • round-trip – трафик передаётся в обе стороны.
12	Определить сообщение, которое IPS/IDS будет записывать в лог, при срабатывании этого правила.	**esr(config-ips-category-rule)# meta log-message <MESSAGE>**	<MESSAGE> – текстовое сообщение, задаётся строкой до 129 символов.

Шаг	Описание	Команда	Ключи
13	Определить классификацию трафика, которая будет записывать в лог, при срабатывании этого правила (не обязательно).	**esr(config-ips-category-rule)# meta classification-type { not-suspicious | unknown | bad-unknown | attempted-recon | successful-recon-limited | successful-recon-largescale | attempted-dos | successful-dos | attempted-user | unsuccessful-user | successful-user | attempted-admin | successful-admin | rpc-portmap-decode | shellcode-detect | string-detect | suspicious-filename-detect | suspicious-login | system-call-detect | tcp-connection | trojan-activity | unusual-client-port-connection | network-scan | denial-of-service | non-standard-protocol | protocol-command-decode | web-application-activity | web-application-attack | misc-activity | misc-attack | icmp-event | inappropriate-content | policy-violation | default-login-attempt }**	• not-suspicious – не подозрительный трафик. • unknown – неизвестный трафик. • bad-unknown – потенциально плохой трафик. • attempted-recon – попытка утечки информации. • successful-recon-limited – утечка информации. • successful-recon-largescale – масштабная утечка информации. • attempted-dos – попытка отказа в обслуживании. • successful-dos – отказ в обслуживании. • attempted-user – попытка получения привилегий пользователя. • unsuccessful-user – безуспешная попытка получения привилегий пользователя. • successful-user – успешная попытка получения привилегий пользователя. • attempted-admin – попытка получения привилегий администратора. • successful-admin – успешная попытка получения привилегий администратора. • rpc-portmap-decode – декодирование запроса RPC. • shellcode-detect – обна ружен исполняемый код. • string-detect – обнаружена подозрительная строка.

Шаг	Описание	Команда	Ключи
			• suspicious-filename-detect – было обнаружено подозрительное имя-файла. • suspicious-login – была обнаружена попытка входа с использованием подозрительного имени пользователя. • system-call-detect – обнаружен системный вызов. • tcp-connection – обнаружено TCP-соединение. • trojan-activity – был обнаружен сетевой троян. • unusual-client-port-connection – клиент использовал необычный порт. • network-scan – обнаружение сетевого сканирования. • denial-of-service – обнаружение атаки отказа в обслуживании. • non-standard-protocol – обнаружение нестандартного протокола или события. • protocol-command-decode – обнаружена попытка шифрования. • web-application-activity – доступ к потенциально уязвимому веб-приложению. • web-application-attack – атака на веб-приложение. • misc-activity – прочая активность. • misc-attack – прочие атаки. • icmp-event – общее событие ICMP.

Шаг	Описание	Команда	Ключи
			• inappropriate-content – обнаружено неприемлемое содержание. • policy-violation – потенциальное нарушение корпоративной конфиденциальности. • default-login-attempt – попытка входа с помощью стандартного логина/пароля.
14	Установить значение кода DSCP, для которого должно срабатывать правило (не обязательно).	**esr(config-ips-category-rule)# ip dscp <DSCP>**	<DSCP> – значение кода DSCP, принимает значения [0..63].
15	Установить значение времени жизни пакета (TTL), для которого должно срабатывать правило (не обязательно).	**esr(config-ips-category-rule)# ip ttl <TTL>**	<TTL> – значение TTL, принимает значения в диапазоне [1..255].
16	Установить номер IP-протокола, для которого должно срабатывать правило (не обязательно). Применимо только для значения protocol any.	**esr(config-ips-category-rule)# ip protocol-id <ID>**	<ID> – идентификационный номер IP-протокола, принимает значения [1..255].
17	Установить значения ICMP CODE, для которого должно срабатывать правило (не обязательно). Применимо только для значения protocol icmp.	**esr(config-ips-category-rule)# ip icmp code <CODE>**	<CODE> – значение CODE протокола ICMP, принимает значение в диапазоне [0..255].
		esr(config-ips-category-rule)# ip icmp code comparison-operator { greater-than | less-than }	Оператор сравнения для значения ip icmp code: • greater-than – больше чем.. • less-than –меньше чем..
18	Установить значения ICMP ID, для которого должно срабатывать правило (не обязательно). Применимо только для значения protocol icmp.	**esr(config-ips-category-rule)# ip icmp id <ID>**	<ID> – значение ID протокола ICMP, принимает значение в диапазоне [0.. 65535].

Шаг	Описание	Команда	Ключи
19	Установить значения ICMP Sequence-ID, для которого должно срабатывать правило (не обязательно). Применимо только для значения protocol icmp.	**esr(config-ips-category-rule)# ip icmp sequence-id <SEQ-ID>**	<SEQ-ID> – значение Sequence-ID протокола ICMP, принимает значение в диапазоне [0.. 4294967295].
20	Установить значения ICMP TYPE, для которого должно срабатывать правило (не обязательно). Применимо только для значения protocol icmp.	**esr(config-ips-category-rule)# ip icmp type <TYPE>**	<TYPE> – значение TYPE протокола ICMP, принимает значение в диапазоне [0..255].
		esr(config-ips-category-rule)# ip icmp type comparison-operator { greater-than | less-than }	Оператор сравнения для значения ip icmp type: • greater-than – больше чем. • less-than –меньше чем.
21	Установить значения TCP Acknowledgment-Number, для которого должно срабатывать правило (не обязательно). Применимо только для значения protocol tcp.	**esr(config-ips-category-rule)# ip tcp acknowledgment-number <ACK-NUM>**	<ACK-NUM> – значение Acknowledgment-Number протокола TCP, принимает значение в диапазоне [0.. 4294967295].
22	Установить значения TCP Sequence-ID, для которого должно срабатывать правило (не обязательно). Применимо только для значения protocol tcp.	**esr(config-ips-category-rule)# ip tcp sequence-id <SEQ-ID>**	<SEQ-ID> – значение Sequence-ID протокола TCP, принимает значение в диапазоне [0.. 4294967295].
23	Установить значения TCP Window-Size, для которого должно срабатывать правило (не обязательно). Применимо только для значения protocol tcp.	**esr(config-ips-category-rule)# ip tcp window-size <SIZE>**	<SIZE> – значение Window-Size протокола TCP, принимает значение в диапазоне [0.. 65535].
24	Установить ключевые слова протокола HTTP, для которых должно срабатывать правило (не обязательно). Применимо только для значения protocol http.	**esr(config-ips-category-rule)# ip http { accept | accept-enc | accept-lang | client-body | connection | content-type | cookie | file-data | header | header-names | host | method | protocol | referer | request-line | response-line | server-body | start | start-code | start-msg | uri | user-agent }**	Значение ключевых слов см. в документации Suricata 4.X. https://suricata.readthedocs.io/en/suricata-4.1.4/rules/http-keywords.html

Шаг	Описание	Команда	Ключи
25	Установить значение ключевого слова URI LEN протокола HTTP, для которых должно срабатывать правило (не обязательно). Применимо только для значения protocol http.	**esr(config-ips-category-rule)# ip http urilen <LEN>**	<LEN> – принимает значение в диапазоне [0.. 65535].
		esr(config-ips-category-rule)# ip http urilen comparison-operator { greater-than | less-than }	Оператор сравнения для значения ip http urilen: • greater-than – больше чем.. • less-than –меньше чем..
26	Установить значение содержимого пакетов (Payload content), для которых должно срабатывать правило (не обязательно).	**esr(config-ips-category-rule)# payload content <CONTENT>**	<CONTENT> – текстовое сообщение, задаётся строкой до 1024 символов.
27	Не различать прописные и заглавные буквы в описании содержимого пакетов (не обязательно). Применимо только совместно с командой payload content.	**esr(config-ips-category-rule)# payload no-case**	
28	Установить сколько байтов с начала содержимого пакета будет проверено (не обязательно). Применимо только совместно с командой payload content.	**esr(config-ips-category-rule)# payload depth <DEPTH>**	<DEPTH> – число байт с начала содержимого пакета, принимает значение в диапазоне [1.. 65535]. По умолчанию проверяется все содержимое пакета.
29	Установить число байт смещения от начала содержимого пакета для проверки (не обязательно). Применимо только совместно с командой payload content.	**esr(config-ips-category-rule)# payload offset <OFFSET>**	<OFFSET> – число байт смещения от начала содержимого пакета, принимает значение в диапазоне [1.. 65535]. По умолчанию проверяется с начала содержимого.
30	Установить размер содержимого пакетов, для которых должно срабатывать правило (не обязательно).	**esr(config-ips-category-rule)# payload data-size <SIZE>**	<SIZE> – размер содержимого пакетов, принимает значение в диапазоне [0.. 65535].

Шаг	Описание	Команда	Ключи
		esr(config-ips-category-rule)# payload data-size comparison-operator { greater-than | less-than }	Оператор сравнения для значения payload data-size: • greater-than – больше чем.. • less-than –меньше чем.
31	Указать пороговое значение количества пакетов, при котором сработает правило (не обязательно).	**esr(config-ips-category-rule)# threshold count <COUNT>**	<COUNT> – число пакетов, принимает значение в диапазоне [1.. 65535].
32	Указать интервал времени, для которого считается пороговое количество пакетов. (Обязательно, если включен threshold count).	**esr(config-ips-category-rule)# threshold second <SECOND>**	<SECOND> – интервал времени в секундах, принимает значение в диапазоне [1.. 65535].
33	Указать по адресу отправителя или получателя будут считаться пороги. (Обязательно, если включен threshold count).	**esr(config-ips-category-rule)# threshold track { by-src | by-dst }**	• by-src – считать пороговое значение для пакетов с одинаковым IP-отправителя. • by-dst – считать пороговое значение для пакетов с одинаковым IP-получателя.
34	Указать метод обработки пороговых значений.	**esr(config-ips-category-rule)# threshold type {threshold | limit | both }**	• threshold – выдавать сообщение каждый раз по достижении порога. • limit – выдавать сообщение не чаще <COUNT> раз за интервал времени <SECOND>. • both – комбинация threshold и limit. Сообщение будет генерироваться, если в течении интервала времени <SECOND> было <COUNT> или более пакетов подходящих под условия правила, и сообщение будет отправлено только один раз в течении интервала времени <SECOND>.
35	Активировать правило.	**esr(config-ips-category-rule)# enable**	

15.6.6 Пример настройки базовых пользовательских правил

Задача:

Написать правило для защиты сервера с IP 192.168.1.10 от DOS-атаки ICMP-пакетами большого размера.

Решение:

Создадим набор пользовательских правил:

```
esr(config)# security ips-category user-defined USER
```

Создадим правило для защиты от атаки:

```
esr(config-ips-category)# rule 10
esr(config-ips-category-rule)# description "Big ICMP DoS"
```

Мы будем отбрасывать пакеты:

```
esr(config-ips-category-rule)# action drop
```

Настроим сообщение об атаке:

```
esr(config-ips-category-rule)# meta log-message "Big ICMP DoS"
esr(config-ips-category-rule)# meta classification-type successful-dos
```

Укажем тип протокола для правила:

```
esr(config-ips-category-rule)# protocol icmp
```

Так как мы указали протокол icmp, то в качестве порта отправителя и получателя требуется указать any:

```
esr(config-ips-category-rule)# source-port any
esr(config-ips-category-rule)# destination-port any
```

В качестве адреса получателя укажем наш сервер:

```
esr(config-ips-category-rule)# destination-address ip 192.168.1.10
```

Атакующий может отправлять пакеты с любого адреса:

```
esr(config-ips-category-rule)# source-address any
```

Зададим направление трафика:

```
esr(config-ips-category-rule)# direction one-way
```

Правило будет срабатывать на пакеты размером больше 1024 байт:

```
esr(config-ips-category-rule)# payload data-size 1024
esr(config-ips-category-rule)# payload data-size comparison-operator greate r-than
```

Правило будет срабатывать, если нагрузка на сервер будет превышать 3 Мбит/с, при этом сообщение об атаке будет генерироваться не чаше одного раза в минуту:

```
3 Мб/с = 3145728 бит в сек
Пакет размером 1Кбайт = 8192 бита
3145728 / 8192 = 384 пакета в сек
384 * 60 = 23040 пакетов в минуту
```

```
esr(config-ips-category-rule)# threshold count 23040
esr(config-ips-category-rule)# threshold second 60
esr(config-ips-category-rule)# threshold track by-dst
esr(config-ips-category-rule)# threshold type both
```

15.6.7 Алгоритм настройки расширенных пользовательских правил

Шаг	Описание	Команда	Ключи
1	Задать имя и перейти в режим конфигурирования набора пользовательских правил.	**esr(config)# security ips-category user-defined <WORD>**	<WORD> – имя набора пользовательских правил, задаётся строкой до 32 символов.
2	Задать описание набора пользовательских правил (не обязательно).	**esr(config-ips-category)# description <DESCRIPTION>**	<DESCRIPTION> –описание задаётся строкой до 255 символов.
3	Создать расширенное правило и перейти в режим его конфигурирования.	**esr(config-ips-category)# rule-advanced <SID>**	<SID> – номер правила, принимает значения [1.. 4294967295].
4	Задать описание правила (не обязательно).	**esr(config-ips-category-rule-advanced)# description <DESCRIPTION>**	<DESCRIPTION> – описание задаётся строкой до 255 символов.
5	Указать действие данного правила.	**esr(config-ips-category-rule-advanced)# rule-text <LINE>**	<CONTENT> – текстовое сообщение в формате SNORT 2.X / Suricata 4.X, задаётся строкой до 1024 символов. **При написании правил в тексте правила необходимо использовать только двойные кавычки (символ "), а само правило необходимо заключать в одинарные кавычки (символ ').**

Шаг	Описание	Команда	Ключи
6	Активировать правило.	**esr(config-ips-category-rule-advanced)# enable**	

15.6.8 Пример настройки расширенных пользовательских правил

Задача:

Написать правило, детектирующее атаку типа Slowloris.

Решение:

Создадим набор пользовательских правил:

```
esr(config)# security ips-category user-defined ADV
```

Создадим расширенное правило:

```
esr(config-ips-category)# rule-advanced 1
esr(config-ips-category-rule-advanced)# description "Slow Loris rule 1"
esr(config-ips-category-rule-advanced)# rule-text 'alert tcp any any -> any 80 (msg:"Possible
Slowloris Attack Detected"; flow:to_server,established; content:"X-a|3a|"; distance:0; pcre:"/
\d\d\d\d/"; distance:0; content:"|0d 0a|"; sid:10000001;)'
```

Создадим ещё одно расширенное правило, работающее по схожему алгоритму, чтобы определить, какое из правил будет эффективнее:

```
esr(config-ips-category)# rule-advanced 2
esr(config-ips-category-rule-advanced)# description "Slow Loris rule 2"
esr(config-ips-category-rule-advanced)# rule-text 'alert tcp $EXTERNAL_NET any -> $HOME_NET
$HTTP_PORTS (msg:"SlowLoris.py DoS attempt"; flow:established,to_server,no_stream; content:"X-
a:"; dsize:<15; detection_filter:track by_dst, count 3, seconds 30; classtype:denial-of-
service; sid: 10000002; rev:1; )'
```

15.7 Настройка взаимодействия с Eltex Distribution Manager

EDM (Eltex Distribution Manager) — сервис распространения лицензируемого контента на устройства по коммерческой подписке.

Благодаря использованию инфраструктуры безопасности «Лаборатории Касперского» , в том числе облачного «коллективного разума» Kaspersky Security Network с поддержкой Kaspersky SafeStream II, сервисный маршрутизатор ESR способен обнаруживать вредоносное ПО во всех типах трафика (web, email, P2P, сервисы мгновенного обмена сообщениями и т .п.). В результате обеспечивается защита пользователей от самых опасных киберугроз, в том числе угроз нулевого дня, программ-шифровальщиков, заражённых сайтов и иных типов.

Система IPS на устройствах ESR может использовать следующие наборы правил, предоставляемых Kaspersky SafeStream II:

- Данные о репутации IP-адресов — набор IP-адресов с контекстной информацией, сообщающей о подозрительных и вредоносных узлах;
- URL-адреса вредоносных ссылок — набор URL-адресов, соответствующих опасным ссылкам и веб-сайтам;

- URL-адреса фишинговых ссылок — набор URL-адресов, распознаваемых «Лабораторией Касперского» как фишинговые. Доступны записи с масками и без масок;
- URL-адреса командных серверов ботнетов — набор URL-адресов командных серверов ботнетов и связанных с ними вредоносных объектов;
- URL-адреса шифровальщиков — набор URL-адресов шифровальщиков;
- Хэши вредоносных объектов — набор файловых хэшей, охватывающий наиболее опасные и распространенные, а также самые новые вредоносные программы;
- Хэши вредоносных объектов для мобильных устройств — набор файловых хэшей для обнаружения вредоносных объектов, заражающих мобильные устройства;
- URL-адреса командных серверов ботнетов для мобильных устройств — набор URL-адресов с контекстной информацией для выявления командных серверов ботнетов, использующих мобильные устройства;
- URL-адреса веб-сайтов, используемых для размещения вредоносных программ, заражающих устройства Internet of Things (IoT).

Для работы по групповой лицензии предоставляется программное обеспечение EDM Server, позволяющее автоматически включать в работу новый сервисный маршрутизатор ESR в рамках действующей лицензии. Таким образом, пользователь системы может сам управлять распределением лицензий по устройствам ESR в рамках своей организации. Для обеспечения масштабируемости и отказоустойчивости возможна установка ПО EDM Server на нескольких хостах.

15.7.1 Алгоритм базовой настройки

Шаг	Описание	Команда	Ключи
1	Перейти в конфигурирование контент-провайдера.	**esr (config)# content-provider**	
2	Задать IP-адрес edm-сервера.	**esr (config-content-provider)# host address <A.B.C.D | WORD | X:X:X:X::X>**	<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::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. WORD(1-31) – DNS-имя сервера.
3	Задать порт для подключения к edm-серверу.	**esr (config-content-provider)# host port <PORT>**	<PORT> – номер TCP/UDP-порта отправителя, принимает значения [1..65535].
4	Задать тип и раздел внешнего устройства для создания крипто-хранилища.	**esr (config-content-provider)# storage-path <DEVICE>**	<DEVICE> – лейбл и имя раздела на внешнем носителе информации в формате usb://Partion_name:/ mmc://Partion_name:/. На внешнем носителе должна быть создана файловая система в формате exFAT.

Шаг	Описание	Команда	Ключи
5	Установить время перезагрузки устройства после получения сертификата.	**esr (config-content-provider)# reboot immediately | [time <HH:MM:SS>]**	Перезагрузить устройство после получения сертификата. time <HH:MM:SS> – время, в которое ESR перезагрузится <Часы:минуты:секунды>.
6	Включить контент провайдер.	**enable**	
7	Установить интервал обращения к edm-серверу в часах.	**esr (config-content-provider)# upgrade interval <1-240>**	
8	Установить описание (не обязательно).	**esr (config-content-provider)# description < LINE >**	LINE (1-255) String describing server
9	Задать текстовое имя устройства, которое передаётся на сервер EDM-Issue (не обязательно).	**esr (config-content-provider)# system-name < WORD >**	<WORD> – имя, задаётся строкой до 255 символов.
10	Задать текстовое описание, которое передаётся на сервер EDM-Issue (не обязательно).	**esr (config-content-provider)# location < WORD >**	<WORD> – описание, задаётся строкой до 255 символов.
11	Создать списки IP-адресов, которые будут использоваться при фильтрации.	**esr (config)# object-group network <WORD>esr (config-object-group-network)# ip prefix <ADDR/LEN>**	<WORD> – имя сервера, задаётся строкой до 32 символов. <ADDR/LEN> – подсеть, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].
10	На интерфейсе включить service-ips.	**esr (config)# interface gigabitethernet 1/0/Xesr (config-if-gi)# service-ips enable**	
11	Создать политику безопасности IPS/IDS.	**esr (config)# security ips policy WORD(1-31)**	WORD(1-31)

Шаг	Описание	Команда	Ключи
12	Задать профиль IP-адресов, которые будет защищать IPS/IDS.	**esr(config-ips-policy)# protect network-group <OBJ-GROUP-NETWORK_NAME>**	<OBJ-GROUP-NETWORK-NAME> – имя профиля защищаемых IP-адресов, задается строкой до 32 символов.
13	Войти в раздел конфигурирования вендора.	**esr (config-ips-policy)# vendor kaspersky**	
14	Подключить необходимую категорию.	**esr (config-ips-vendor)# category WORD(1-64)**	Phishing URL Data Feed – потоки данных Phishing URL Malicious URL Data Feed – потоки данных Malicious URL Botnet C&C URL Data Feed – потоки данных Botnet C&C URL Malicious Hash Data Feed – потоки данных Malicious Hashes Mobile Malicious Hash Data Feed – потоки данных мобильных Malicious Hashes IP Reputation Data Feed – потоки данных IP-адресов Mobile Botnet Data Feed – потоки данных о мобильных Botnet Ransomware URL Data Feed – поток данных Ransomware URL Botnet C&C URL Exact Data Feed – поток данных Botnet C&C URL Exact Phishing URL Exact Data Feed – поток данных Phishing URL Exact Malicious URL Exact Data Feed – поток данных Malicious URL Exact Iot URL Data Feed – поток данных IoT URL

Шаг	Описание	Команда	Ключи
15	Задать тип правил.	**esr (config-ips-vendor-category)# rules action <ACTION>**	<ACTION> - drop | reject | alert | pass – действия, которые будут применяться к пакетам. • alert – прохождение трафика разрешается, и сервис IPS/IDS генерирует сообщение; • reject – прохождение трафика запрещается. Если это TCP трафик отправителю и получателю посылается пакет TCP-RESET, для остального типа трафика посылается пакет ICMP-ERROR. Сервис IPS/IDS генерирует сообщение; • pass – прохождение трафика разрешается; • drop – прохождение трафика запрещается, и сервис IPS/IDS генерирует сообщение.
16	Задать количество скачиваемых правил.	**esr (config-ips-vendor-category)# rules count <number>**	<number>
17	Включить категорию.	**enable**	
18	Перейти в режим конфигурирования IPS/IDS.	**esr (config)# security ips**	
19	Назначить политику безопасности IPS/IDS.	**esr(config-ips)# policy <NAME>**	<NAME> – имя политики безопасности, задаётся строкой до 32 символов.
20	Использовать все ресурсы ESR для IPS/IDS (не обязательно).	**esr(config-ips)# perfomance max**	

Шаг	Описание	Команда	Ключи
21	Задать параметры удаленного сервера для отправки статистики работы сервиса IPS/IDS в формате EVE (elasticsearch) (не обязательно).	**esr(config-ips)# logging remote-server { <ADDR> | <IPV6-ADDR> } [<TRANSPORT>] [<PORT>] [source-address { <SRC-ADDR> | <IPV6-SRC-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::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <TRANSPORT> – протокол передачи данных, по умолчанию – UDP, принимает значения: • TCP – передача данных осуществляется по протоколу TCP; • UDP – передача данных осуществляется по протоколу UDP; <PORT> – номер TCP/UDP-порта, опциональный параметр, принимает значения [1..65535], по умолчанию 514; <SRC-ADDR> – IPv4-адрес маршрутизатора, который будет использоваться в качестве IP-адреса источника в отправляемых syslog-пакетах, по умолчанию – IPv4-адрес интерфейса, с которого отправляются пакеты; <IPV6-SRC-ADDR> – IPv6-адрес маршрутизатора, который будет использоваться в качестве IPv6-адреса источника в отправляемых syslog-пакетах, по умолчанию – IPv6-адрес интерфейса, с которого отправляются пакеты.
22	Установить интервал отправки статистики работы сервиса IPS/IDS в формате EVE (elasticsearch) (не обязательно).	**esr(config-ips)# logging update-interval <INTERVAL>**	<INTERVAL> – интервал отправки статистики работы сервиса IPS/IDS, задаётся в минутах.
23	Активировать IPS/IDS.	**esr(config- ips)# enable**	

15.7.2 Пример настройки

Задать параметры content-provider — это адрес сервера ELTEX. Между сервером content-provider и маршрутизатором должна быть сетевая доступность.

```
content-provider
  host address edm.eltex-co.ru
  host port 8098
  upgrade interval 1
  storage-path mmc://TEST:/
  reboot immediately
  enable
exit
```

После перезагрузки устройства, можно начинать настраивать сервис IPS.

Задать профиль IP-адресов, которые будет защищать IPS/IDS:

```
object-group network objectgroup0
  ip prefix 192.168.30.0/24
exit
```

На интерфейсе включить IPS:

```
interface gigabitethernet 1/0/1
  service-ips enable
exit
```

Настроить политику безопасности:

```
security ips policy policy0
  protect network-group objectgroup0
  vendor kaspersky
    category MaliciousURLsDF
      rules action alert
      rules count 100
      enable
    exit
    category MobileBotnetCAndCDF
      rules action alert
      rules count 1000
      enable
    exit
    category APTIPDF
      rules action alert
      rules count 1000
      enable
    exit
```

```
    category APTURLsDF
      rules action alert
      rules count 1000
      enable
    exit
    category BotnetCAndCURLsDF
      rules action alert
      rules count 1000
      enable
    exit
    category IPReputationDF
      rules action alert
      rules count 1000
      enable
    exit
    category IoTURLsDF
      rules action alert
      rules count 1000
      enable
    exit
    category MaliciousHashDF
      rules action alert
      rules count 1
      enable
    exit
    category MobileMaliciousHashDF
      rules action alert
      rules count 1
      enable
    exit
    category PSMSTrojanDF
      rules action alert
      rules count 1
      enable
    exit
    category PhishingURLsDF
      rules action alert
      rules count 1000
      enable
    exit
    category RansomwareURLsDF
      rules action alert
      rules count 1000
      enable
    exit
  exit
exit
```

Назначить сервису IPS-политику для работы и включить его:

```
security ips
  performance max
  policy policy0
  enable
exit
```

Для просмотра информации о загруженном контенте для IPS/IDS можно использовать две следующие команды:

show security ips content-provider:

```
esr-20# show security ips content-provider
 Server: content-provider
                Last MD5 of received files:        c60bd0f10716d3f48e18f24828337135
                Next update: 30 October 2020 00:37:06
```

С помощью этой команды можно узнать, скачивал ли контент-провайдер правила с сервера EDM (по признаку присутствия контрольной суммы md5) и когда по времени устройства планируется следующее обновление.

show security ips counters:

```
esr-20# show security ips counters
TCP flows processed :     191
Alerts generated :        0
Blocked by ips engine :   7
Accepted by ips engine :  51483
```

Показывает прошедший трафик через IPS/IDS и действия, которые применялись к трафику, а также число срабатываний правил IPS/IDS.

15.8 Настройка сервиса контентной фильтрации

> ⚠ **Данный функционал активируется только при наличии лицензии.**

Сервис контентной фильтрации предназначен для ограничения доступа к HTTP-сайтам на основании их содержимого. Для каждого сайта определяется принадлежность его к той или иной категории. В качестве базы категорий сайтов используется база Лаборатории Касперского. Для определения категории сайтов ESR отправляет HTTPS-запросы на сервер Лаборатории Касперского по адресу https://ksn-vt.kaspersky-labs.com.

Работа сервиса контентной фильтрации основана на системе предотвращения вторжений (IPS) и настраивается как пользовательские правила IPS.

15.8.1 Алгоритм базовой настройки

Шаг	Описание	Команда	Ключи
1	Определить IP-адрес DNS-сервера, используемого для разрешения DNS-имен.	**esr(config)# domain name-server <IP>**	<IP> – IP-адрес используемого DNS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
2	Включить разрешение DNS-имен на устройстве	**esr(config)# domain lookup enable**	
3	Создать политику безопасности IPS/IDS.	**esr(config)# security ips policy <NAME>**	<NAME> – имя политики безопасности, задаётся строкой до 32 символов.

Шаг	Описание	Команда	Ключи
4	Задать описание политики (не обязательно).	**esr(config-ips-policy)# description <DESCRIPTION>**	<DESCRIPTION> – описание задаётся строкой до 255 символов.
5	Создать списки IP-адресов, которые будут использоваться при фильтрации.	**esr (config)# object-group network <WORD>** **esr (config-object-group-network)# ip prefix <ADDR/LEN>**	<WORD> – имя сервера, задаётся строкой до 32 символов. <ADDR/LEN> – подсеть, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].
6	Задать профиль IP-адресов, которые будет защищать IPS/IDS.	**esr(config-ips-policy)# protect network-group <OBJ-GROUP-NETWORK_NAME>**	<OBJ-GROUP-NETWORK-NAME> – имя профиля защищаемых IP-адресов, задается строкой до 32 символов.
7	Задать профиль IP-адресов, внешних для IPS/IDS (не обязательно).	**esr(config-ips-policy)# external network-group <OBJ-GROUP-NETWORK_NAME>**	<OBJ-GROUP-NETWORK-NAME> – имя профиля внешних IP-адресов, задается строкой до 32 символов.
8	Создать профиль категорий контентной фильтрации	**esr(config)# object-group content-filter <NAME>**	<NAME> – имя профиля контентной фильтрации, задается строкой до 31 символа.
9	Задать описание профиля категорий контентной фильтрации (не обязательно).	**esr(config-object-group-content-filter)# description <DESCRIPTION>**	<DESCRIPTION> – описание задаётся строкой до 255 символов.
10	Задать поставщика категорий контентной фильтрации.	**esr(config-object-group-content-filter)# vendor <CONTENT-FILTER-VENDOR>**	<CONTENT-FILTER-VENDOR> – название поставщика категорий контентной фильтрации. В текущей версии ПО в качестве поставщика категорий контентной фильтрации может выступать только Лаборатория Касперского.
11	Задать необходимые категории контентной фильтрации.	**esr(config-object-group-cf-kaspersky)# category <CATEGORY>**	<CATEGORY> – имя категории. Описание доступных категорий приведено в справочнике команд.

Шаг	Описание	Команда	Ключи
12	Перейти в режим конфигурирования IPS/IDS.	**esr(config)# security ips**	
13	Назначить политику безопасности IPS/IDS.	**esr(config-ips)# policy <NAME>**	<NAME> – имя политики безопасности, задаётся строкой до 32 символов.
14	Использовать все ресурсы ESR для IPS/IDS (не обязательно).	**esr(config-ips)# perfomance max**	По умолчанию для IPS/IDS отдается половина доступных ядер процессора.

Шаг	Описание	Команда	Ключи
15	Задать параметры удаленного сервера для отправки статистики работы сервиса IPS/IDS в формате EVE (elasticsearch) (не обязательно).	**esr(config-ips)# logging remote-server { <ADDR> | <IPV6-ADDR> } [<TRANSPORT>] [<PORT>] [source-address { <SRC-ADDR> | <IPV6-SRC-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::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <TRANSPORT> – протокол передачи данных, по умолчанию - UDP, принимает значения: • TCP – передача данных осуществляется по протоколу TCP; • UDP – передача данных осуществляется по протоколу UDP; <PORT> – номер TCP/UDP-порта, опциональный параметр, принимает значения [1..65535], по умолчанию 514; <SRC-ADDR> – IPv4-адрес маршрутизатора, который будет использоваться в качестве IP-адреса источника в отправляемых syslog-пакетах, по умолчанию – IPv4-адрес интерфейса, с которого отправляются пакеты; <IPV6-SRC-ADDR> – IPv6-адрес маршрутизатора, который будет использоваться в качестве IP v6-адреса источника в отправляемых syslog-пакетах, по умолчанию – IPv6-адрес интерфейса, с которого отправляются пакеты;
16	Установить интервал отправки статистики работы сервиса IPS/IDS в формате EVE (elasticsearch) (не обязательно).	**esr(config-ips)# logging update-interval <INTERVAL>**	<INTERVAL> – интервал отправки статистики работы сервиса IPS/IDS, задаётся в минутах.

Шаг	Описание	Команда	Ключи
17	Активировать IPS/IDS.	**esr(config-ips)# enable**	
18	Активировать IPS/IDS на интерфейсе.	**esr(config-if-gi)# service-ips enable**	
19	Задать имя и перейти в режим конфигурирования набора пользовательских правил.	**esr(config)# security ips-category user-defined <WORD>**	<WORD> – имя набора пользовательских правил, задаётся строкой до 32 символов.
20	Задать описание набора пользовательских правил (не обязательно).	**esr(config-ips-category)# description <DESCRIPTION>**	<DESCRIPTION> – описание задаётся строкой до 255 символов.
21	Создать правило и перейти в режим конфигурирования правила.	**esr(config-ips-category)# rule <ORDER>**	<ORDER> – номер правила, принимает значения [1..512].
22	Задать описание правила (не обязательно).	**esr(config-ips-category-rule)# description <DESCRIPTION>**	<DESCRIPTION> – описание задаётся строкой до 255 символов.
23	Указать действие данного правила.	**esr(config-ips-category-rule)# action { alert | reject | pass | drop }**	• alert – прохождение трафика разрешается, и сервис IPS/IDS генерирует сообщение; • reject – прохождение трафика запрещается. Если это TCP-трафик, отправителю и получателю посылается пакет TCP-RESET, для остального типа трафика посылается пакет ICMP-ERROR. Сервис IPS/IDS генерирует сообщение; • pass – прохождение трафика разрешается; • drop – прохождение трафика запрещается, и сервис IPS/IDS генерирует сообщение.
24	Установить в качестве IP-протокола протокол HTTP.	**esr(config-ips-category-rule)# protocol http**	

Шаг	Описание	Команда	Ключи
25	Установить IP-адреса отправителя, для которых должно срабатывать правило.	**esr(config-ips-category-rule)# source-address {ip <ADDR> | ip-prefix <ADDR/LEN> | object-group <OBJ_GR_NAME> | policy-object-group { protect | external } | any }**	<ADDR> – IP-адрес отправителя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <ADDR/LEN> – IP-подсеть отправителя, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и LEN принимает значения [1..32]. <OBJ_GR_NAME> – имя профиля IP-адресов, который содержит IP-адреса отправителя, задаётся строкой до 31 символа. • protect – устанавливает в качестве адресов отправителя protect-адреса, определенные в политике IPS/IDS; • external – устанавливает в качестве адресов отправителя external-адреса. определенные в политике IPS/IDS. При указании значения «any» правило будет срабатывать для любого IP-адреса отправителя.
26	Установить номера TCP-портов отправителя, для которых должно срабатывать правило.	**esr(config-ips-category-rule)# source-port {any | <PORT> | object-group <OBJ-GR-NAME> }**	<PORT> – номер TCP/UDP-порта отправителя, принимает значения [1..65535]. <OBJ_GR_NAME> – имя профиля TCP/UDP портов отправителя, задаётся строкой до 31 символа. При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта отправителя.

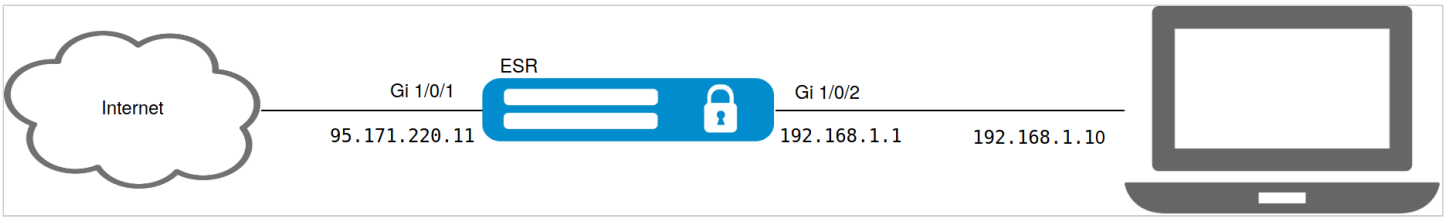
Шаг	Описание	Команда	Ключи
27	Установить IP-адреса получателя, для которых должно срабатывать правило.	**esr(config-ips-category-rule)# destination-address {ip <ADDR> | ip-prefix <ADDR/LEN> | object-group <OBJ_GR_NAME> | policy-object-group { protect | external } | any }**	<<ADDR> – IP-адрес получателя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <ADDR/LEN> – IP-подсеть получателя, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и LEN принимает значения [1..32]. < OBJ_GR_NAME> – имя профиля IP-адресов, который содержит IP-адреса получателя, задаётся строкой до 31 символа. • protect – устанавливает в качестве адресов получателя protect-адреса, определенные в политике IPS/IDS; • external – устанавливает в качестве адресов получателя external-адреса, определенные в политике IPS/IDS. При указании значения «any» правило будет срабатывать для любого IP-адреса получателя.
28	Установить номера TCP-портов получателя, для которых должно срабатывать правило. Обычно для протокола http используется значение TCP-порт 80. В случаях когда когда используются web-сервера на нестандартных портах надо пописывать эти порты тоже.	**esr(config-ips-category-rule)# destination-port {any | <PORT> | object-group <OBJ-GR-NAME> }**	<PORT> – номер TCP/UDP-порта получателя, принимает значения [1..65535]. <OBJ_GR_NAME> – имя профиля TCP/UDP портов получателя, задаётся строкой до 31 символа. При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта получателя.

Шаг	Описание	Команда	Ключи
29	Установить направление потока трафика, для которого должно срабатывать правило.	**esr(config-ips-category-rule)# direction { one-way | round-trip }**	• one-way – трафик передаётся в одну сторону. • round-trip – трафик передаётся в обе стороны.
30	Определить сообщение которое IPS/IDS будет записывать в лог, при срабатывании этого правила.	**esr(config-ips-category-rule)# meta log-message <MESSAGE>**	<MESSAGE> – текстовое сообщение, задаётся строкой до 129 символов.
31	Назначить профиль категорий контентной фильтрации.	**esr(config-ips-category-rule)# ip http content-filter <NAME>**	<NAME> – имя профиля контентной фильтрации задаётся строкой до 31 символа. any – правило будет срабатывать для http-сайтов любой категории.
32	Активировать правило.	**esr(config-ips-category-rule)# enable**	

15.8.2 Пример настройки правил контентной фильтрации

Задача:

Запретить доступ к http-сайтам, относящимся к категориям adult-content, casino, online-betting, online-lotteries из локальной сети 192.168.1.0/24



Решение:

На устройстве предварительно должны быть настроены интерфейсы и правила firewall.

Создадим профиль адресов защищаемой локальной сети:

```
esr(config)# object-group network LAN
esr(config-object-group-network)# ip prefix 192.168.1.0/24
esr(config-object-group-network)# exit
```

Настроим на ESR DNS-клиента для разрешения имен источников обновления правил IPS/IDS:

```
esr(config)# domain lookup enable
esr(config)# domain name-server 8.8.8.8
```

Создадим политику безопасности IPS/IDS:

```
esr(config)# security ips policy OFFICE
esr(config-ips-policy)# description "My Policy"
esr(config-ips-policy)# protect network-group LAN
```

Разрешим работу IPS/IDS на интерфейсе локальной сети gigabitethernet 1/0/2:

```
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# service-ips inline
```

Настроим параметры IPS/IDS:

```
esr(config)# security ips
esr(config-ips)# policy OFFICE
esr(config-ips)# enable
```

Устройство будет использоваться только как шлюз безопасности, поэтому отдадим сервису IPS/IDS все доступные ресурсы:

```
esr(config-ips)# perfomance max
```

Создадим профиль контентной фильтрации для выбранных категорий:

```
esr(config)# object-group content-filter Black
esr(config-object-group-content-filter)# vendor kaspersky-lab
esr(config-object-group-cf-kaspersky)# category adult-content
esr(config-object-group-cf-kaspersky)# category casino
esr(config-object-group-cf-kaspersky)# category online-betting
esr(config-object-group-cf-kaspersky)# category online-lotteries
```

Создадим набор пользовательских правил:

```
esr(config)# security ips-category user-defined USER
```

Создадим правило:

```
esr(config-ips-category)# rule 10
esr(config-ips-category-rule)# description "Content-Filter Block"
```

Будем отбрасывать пакеты:

```
esr(config-ips-category-rule)# action drop
```

Настроим сообщение об атаке:

```
esr(config-ips-category-rule)# meta log-message "Corporate policy violation"
```

Укажем тип протокола для правила:

```
esr(config-ips-category-rule)# protocol http
```

При http-запросах в качестве TCP-порта отправителя операционная система использует случайное значение, поэтому требуется указать any:

```
esr(config-ips-category-rule)# source-port any
```

В качестве TCP-порта назначения для протокола http обычно используется 80 порт, но интернет сайты могут работать и на нестандартных портах, поэтому укажем any:

```
esr(config-ips-category-rule)# destination-port any
```

В качестве адреса получателя может быть любой сайт в интернете:

```
esr(config-ips-category-rule)# destination-address any
```

Запросы к сайтам отправляются из нашей локальной сети:

```
esr(config-ips-category-rule)# source-address policy-object-group protect
```

Зададим направление трафика:

```
esr(config-ips-category-rule)# direction one-way
```

Правило будет срабатывать на категории сайтов, перечисленные в профиле Black:

```
esr(config-ips-category-rule)# ip http content-filter Black
```

Активируем правило:

```
esr(config-ips-category-rule)# enable
esr(config-ips-category-rule)# exit
esr(config-ips-category-rule)# threshold type both
```

15.9 Настройка сервиса «Антиспам»

Данный функционал активируется только при наличии лицензии.

Почтовый антиспам, или спам-фильтр — это программа для определения и фильтрации нежелательных электронных сообщений, которые могут поступать через корпоративные почтовые серверы и публичные сервисы электронной почты (спам, почтовый фишинг и т.п.).

Основная задача сервиса «Антиспам» — распознать такие нежелательные письма еще в процессе доставки этих писем в почтовый ящик получателя. Для этого сервисный маршрутизатор ESR с настроенным сервисом «Антиспам» устанавливается в сети перед защищаемым почтовым сервером и перенаправляет через себя электронную почту между этим сервером и другими почтовыми серверами в сети Интернет, фактически выполняя функцию Mail Proxy.

Письма, пришедшие от внешних почтовых доменов, в сервисе «Антиспам» будут проанализированы следующими способами:

- проверка подлинности домена-отправителя через SPF;
- проверка подписи электронного письма, подписанного ключом домена по технологии DKIM;
- идентификация электронного письма согласно технологии DMARC;

- проверка наличия корректной MX-записи для домена, из которого отправлено электронное письмо;
- поиск отправителя письма в списке известных сервисов широковещательной рассылки;
- поиск отправителя письма в RBL;
- анализ корректности SMTP-команд во время поднятия SMTP-сессии;
- анализ кодировок Unicode, присутствующих в тексте письма;
- анализ ссылок в тексте письма на принадлежность к фишингу.

Письма, не прошедшие большинство проверок, будут отброшены и не попадут на защищаемый почтовый сервер.

При использовании сервиса «Антиспам» для защиты почтового сервера произвести ряд дополнительных настроек, не связанных непосредственно с конфигурацией маршрутизатора ESR.
1) Изменить MX-запись для используемого домена таким образом, чтобы она ссылалась не на защищаемый почтовый сервер, а на IP-адрес ESR с настроенным сервисом «Антиспам».
2) Настроить на почтовом сервере использование SMTP Proxy, где в качестве Proxy выступит ESR с настроенным сервисом «Антиспам».

15.9.1 Алгоритм базовой настройки

Шаг	Описание	Команда	Ключи
1	Настроить сетевое имя маршрутизатора.	**esr(config)# hostname <NAME>**	<NAME> – до 64 символов.
2	Назначить имя домена для маршрутизатора.	**esr(config)# domain name <NAME>**	<NAME> – до 255 символов.
3	Назначить IP-адрес DNS-сервера, используемого для разрешения DNS-имен.	**esr(config)# domain name-server <IP>**	<IP> – в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения от 0 до 255.
4	Включить разрешение имен DNS.	**esr(config)# domain lookup enable**	
5	Создать профиль сервиса «Антиспам»	**esr(config)# security antispam profile <NAME>**	<NAME> – до 31 символа.
6	Задать описание профиля сервиса «Антиспам» (необязательно).	**esr(config-antispam-profile)# description <DESCRIPTION>**	<DESCRIPTION> – до 255 символов.
7	Задать тип маркировки электронных писем, которые сервис «Антиспам» отнес к категории «Спам».	**esr(config-antispam-profile)# mark-type <MARK-TYPE>**	<MARK-TYPE> – тип маркировки писем, отнесенных к категории «Спам». Возможные значения: - header – добавить X-Spam заголовок к заголовкам электронного письма; - subject – добавить тег [SPAM] перед темой электронного письма.
8	Создать профиль почтовых доменов и адресов почтовых ящиков (необязательно).	**esr(config)# object-group email <NAME>**	<NAME> – до 31 символа.
9	Задать описание профиля почтовых доменов и адресов почтовых ящиков (необязательно).	**esr(config-object-group-email)# description <DESCRIPTION>**	<DESCRIPTION> – до 255 символов.
10	Внести в профиль почтовый домен или адрес почтового ящика (необязательно).	**esr(config-object-group-email)# email <NAME>**	<NAME> – до 63 символов.
11	Создать правило в профиле сервиса «Антиспам» (необязательно).	**esr(config-antispam-profile)# rule <ORDER>**	<ORDER> – номер правила, принимает значения от 1 до 100.
12	Задать описание правила профиля сервиса «Антиспам» (необязательно).	**esr(config-antispam-profile)# description <DESCRIPTION>**	<DESCRIPTION> – до 255 символов.

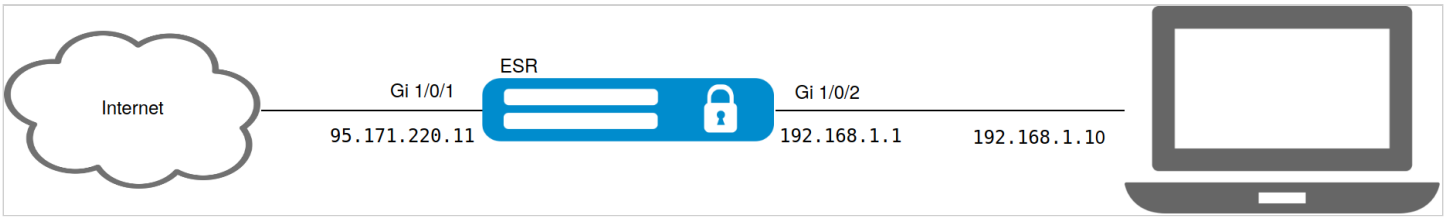
Шаг	Описание	Команда	Ключи
13	Установить профиль IP-адресов отправителя, для которых должно срабатывать правило (не обязательно).	**esr(config-antispam-profile-rule)# sender ip <NAME>**	<NAME> – до 31 символа.
14	Установить профиль почтовых доменов и адресов почтовых ящиков, для которых должно срабатывать правило (не обязательно).	**esr(config-antispam-profile-rule)# sender email <NAME>**	<NAME> – до 31 символа.
15	Указать действие для правила.	**esr(config-antispam-profile-rule)# action <ACTION>**	<ACTION> – назначаемое действие. Возможные значения: - reject – дальнейшая доставка письма запрещена, отправителю письма высылается ответ об ошибке.
16	Включить правило в профиле сервиса «Антиспам» (необязательно).	**esr(config-antispam-profile-rule)# enable**	
17	Создать почтовый домен.	**esr(config)# mailserver domain <DOMAIN-NAME>**	<DOMAIN-NAME> – до 31 символа.
18	Задать описание почтового домена (необязательно).	**esr(config-mailserver-domain)# description <DESCRIPTION>**	<DESCRIPTION> – до 255 символов.
19	Задать имя обслуживаемого домена электронной почты.	**esr(config-mailserver-domain)# mail domain <NAME>**	<NAME> – до 63 символов.
20	Задать IP-адрес почтового сервера, для которого сервис «Антиспам» на ESR выступает в качестве SMTP Proxy.	**esr(config-mailserver-domain)# mail server ip <ADDR>**	<ADDR> – в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения от 0 до 255.
21	Задать профиль сервиса «Антиспам», настройки которого будут применены к текущему почтовому домену.	**esr(config-mailserver-domain)# profile antispam <NAME>**	<NAME> – до 63 символов.
22	Включить почтовый домен.	**esr(config-mailserver-domain)# enable**	
23	Перейти в конфигурирование почтового сервера.	**esr(config)# mailserver**	
24	Задать имя почтового домена.	**esr(config-mailserver)# domain <NAME>**	<NAME> – до 63 символов.

Шаг	Описание	Команда	Ключи
25	Указать сертификаты и ключи для работы протокола TLS (необязательно).	**esr(config-mailserver)# tls keyfile <TYPE> <NAME>**	<TYPE> – Тип файла сертификата или ключа. Возможные значения: • ca – сертификат удостоверяющего центра; • server-key – приватный ключ сервера; • server-crt – публичный сертификат сервера; • dh – ключ Диффи-Хеллмана. <NAME> – имя файла сертификата, задаётся строкой до 31 символа.
26	Включить поддержку TLS на почтовом сервере (необязательно). При включении TLS обязательно наличие в конфигурации прописанного сертификата удостоверяющего центра, приватного ключа сервера и публичного сертификата сервера.	**esr(config-mailserver)# tls enable**	
27	Задать максимальный размер заголовков письма в КБ (необязательно).	**esr(config-mailserver)# headers max-size <SIZE>**	<SIZE> – максимальный размер заголовков письма в КБ, принимает значения от 50 до 200.
28	Задать максимальный размер письма в КБ (необязательно).	**esr(config-mailserver)# mail max-size <SIZE>**	<SIZE> – максимальный размер письма в КБ, принимает значения от 5120 до 51200.
29	Включить обязательное требование SMTP-команды HELO или EHLO при установлении SMTP-сессии (необязательно).	**esr(config-mailserver)# smtp helo-required**	
30	Разрешить SMTP команду VRFY на почтовом сервере во время SMTP-сессии (необязательно).	**esr(config-mailserver)# smtp vrfy-enable**	
31	Включить почтовый сервер.	**esr(config-mailserver)# enable**	

15.9.2 Пример настройки

Задача:

Настроить на ESR сервис «Антиспам» для работы в качестве SMTP Proxy для анализа электронной почты, адресованной почтовому серверу, расположенному в сети предприятия и обслуживающему домен eltex-co.ru.



Решение:

Убедимся, что MX-запись для домена eltex-co.ru указывает на IP-адрес ESR:

```
esr@eltex:~$ dig +noall +answer eltex-co.ru MX
eltex-co.ru.    3548    IN  MX  10 mail-gate.eltex-co.ru.
esr@eltex:~$ dig +noall +answer mail-gate.eltex-co.ru A
mail-gate.eltex-co.ru. 3453 IN  A   95.171.220.11
```

Настроим сетевые интерфейсы:

```
esr# config
esr(config)# interface gi1/0/1
esr(config-if-gi)# ip address 95.171.220.11/18
esr(config-if-gi)# ip firewall disable
esr(config-if-gi)# exit
esr(config)# interface gi1/0/2
esr(config-if-te)# ip address 192.168.1.1/24
esr(config-if-te)# ip firewall disable
esr(config-if-te)# exit
```

Настроим сетевое имя, имя домена и настройки DNS. Сетевое имя и имя домена должны образовать FQDN (англ. Fully Qualified Domain Name — полностью определённое имя домена), прописанное в MX записи для домена eltex-co.ru:

```
esr(config)# hostname mail-gate
esr(config)# domain name eltex-co.ru
esr(config)# domain name-server 1.1.1.1
esr(config)# domain lookup enable
```

Создадим профиль для сервиса «Антиспам», который будет добавлять X-Spam заголовок к письмам, идентифицированным как спам:

```
esr(config)# security antispam profile SimpleProfile
esr(config-antispam-profile)# description "Basic Antispam profile without rules"
esr(config-antispam-profile)# mark-type header
esr(config-antispam-profile)# exit
```

Создадим почтовый домен, который будет настроен для обработки писем для домена eltex-co.ru и ретрансляции таких писем на локальный почтовый сервер. В конфигурацию почтового домена добавим созданный выше профиль сервиса «Антиспам», чтобы транзитная почта анализировалась на принадлежность к спаму:

```
esr(config)# mailserver domain MainDomain
esr(config-mailserver-domain)# mail domain eltex-co.ru
esr(config-mailserver-domain)# description "Mail domain eltex-co.ru"
esr(config-mailserver-domain)# mail server ip 192.168.1.10
esr(config-mailserver-domain)# profile antispam SimpleProfile
esr(config-mailserver-domain)# enable
esr(config-mailserver-domain)# exit
```

Добавим в конфигурацию почтового сервера созданный домен и пропишем настройки для работы TLS:

```
esr(config)# mailserver
esr(config-mailserver)# domain MainDomain
esr(config-mailserver)# tls keyfile ca ca.crt
esr(config-mailserver)# tls keyfile server-crt server.crt
esr(config-mailserver)# tls keyfile server-key server.key
esr(config-mailserver)# tls enable
esr(config-mailserver)# enable
esr(config-mailserver)# exit
```

Применение текущей конфигурации запустит сервис в работу.

В firewall необходимо разрешить протокол SMTP (TCP порт 25).

16 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

16.1 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.

16.1.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим конфигурирования интерфейса/сетевого моста, для которого необходимо настроить протокол VRRP.	**esr(config)# interface <IF-TYPE><IF-NUM>**	<IF-TYPE> – тип интерфейса; <IF-NUM> – F/S/P – F-фрейм (1), S – слот (0), P – порт.
		esr(config)# tunnel <TUN-TYPE><TUN-NUM>	<TUN-TYPE> – тип туннеля; <TUN-NUM> – номер туннеля.
		esr(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.	**esr(config-if-gi)# vrrp**	
		esr(config-if-gi)# ipv6 vrrp	

Шаг	Описание	Команда	Ключи
4	Установить виртуальный IP-адрес VRRP-маршрутизатора.	**esr(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.
		esr(config-if-gi)# ipv6 vrrp ip <IPV6-ADDR>	<IPV6-ADDR> – виртуальный IPv6-адрес, задаётся в виде X: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.	**esr(config-if-gi)# vrrp id <VRID>**	<VRID> – идентификатора VRRP-маршрутизатора, принимает значения [1..255].
		esr(config-if-gi)# ipv6 vrrp id <VRID>	
6	Установить приоритет VRRP-маршрутизатора (не обязательно).	**esr(config-if-gi)# vrrp priority <PR>**	<PR> – приоритет VRRP-маршрутизатора, принимает значения [1..254]. Значение по умолчанию: 100.
		esr(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).	**esr(config-if-gi)# vrrp group <GRID>**	<GRID> – идентификатор группы VRRP-маршрутизатора, принимает значения [1..32].
		esr(config-if-gi)# ipv6 vrrp group <GRID>	

Шаг	Описание	Команда	Ключи
8	Установить IP-адрес, который будет использоваться в качестве IP-адреса отправителя для VRRP-сообщений (не обязательно).	**esr(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].
		esr(config-if-gi)# ipv6 vrrp source-ip <IPV6>	<IPV6> – IPv6-адрес отправителя, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
9	Установить интервал между отправкой VRRP-сообщений (не обязательно).	**esr(config-if-gi)# vrrp timers advertise <TIME>**	<TIME> – время в секундах, принимает значения [1..40]. Значение по умолчанию: 1 секунда.
		esr(config-if-gi)# ipv6 vrrp timers advertise <TIME>	
10	Установить интервал, по истечении которого происходит отправка GratuituousARP-сообщения(ий) при переходе маршрутизатора в состояние Master (не обязательно).	**esr(config-if-gi)# vrrp timers garp delay <TIME>**	<TIME> – время в секундах, принимает значения [1..60]. Значение по умолчанию: 5 секунд.
11	Установить количество GratuituousARP-сообщений, которые будут отправлены при переходе маршрутизатора в состояние Master (не обязательно).	**esr(config-if-gi)# vrrp timers garp repeat <COUNT>**	<COUNT> – количество сообщений, принимает значения [1..60]. Значение по умолчанию: 5.
12	Установить интервал, по истечении которого будет происходить периодическая отправка GratuituousARP-сообщения(ий), пока маршрутизатор находится в состоянии Master (не обязательно).	**esr(config-if-gi)# vrrp timers garp refresh <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: Периодическая отправка отключена.
13	Установить количество GratuituousARP-сообщений, которые будут отправляться с периодом garprefresh пока маршрутизатор находится в состоянии Master (не обязательно).	**esr(config-if-gi)# vrrp timers garp refresh-repeat <COUNT>**	<COUNT> – количество сообщений, принимает значения [1..60]. Значение по умолчанию: 1.

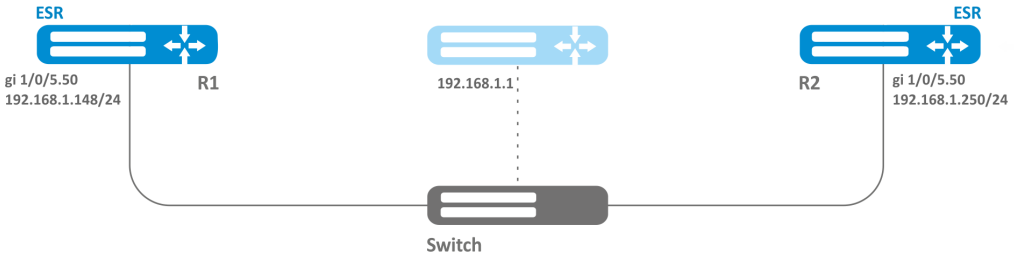
Шаг	Описание	Команда	Ключи
14	Определить, будет ли Backup-маршрутизатор с более высоким приоритетом пытаться перехватить на себя роль Master у текущего Master-маршрутизатора с более низким приоритетом (не обязательно).	**esr(config-if-gi)# vrrp preempt disable** **esr(config-if-gi)# ipv6 vrrp preempt disable**	
15	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).	**esr(config-if-gi)# vrrp preempt delay <TIME>** **esr(config-if-gi)# ipv6 vrrp preempt delay <TIME>**	<TIME> – время ожидания, определяется в секундах [1..1000]. Значение по умолчанию: 0.
16	Установить пароль для аутентификации с соседом (не обязательно).	**esr(config-if-gi)# vrrp 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...).
17	Определить алгоритм аутентификации (не обязательно).	**esr(config-if-gi)# vrrp authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм аутентификации: • **cleartext** – пароль, передается открытым текстом; • **md 5** – пароль хешируется по алгоритму md5.
18	Задать версию VRRP-протокола (не обязательно).	**esr(config-if-gi)# vrrp version <VERSION>**	<VERSION> – версия VRRP-протокола: 2, 3.
19	Установить режим, когда vrrp IP-адрес остается в состоянии UP вне зависимости от состояния самого интерфейса (не обязательно).	**esr(config-if-gi)# vrrp force-up**	
20	Определить задержку между установлением ipv6 vrrp состояния MASTER и началом рассылки ND сообщений (не обязательно).	**esr(config-if-gi)# ipv6 vrrp timers nd delay <TIME>**	<TIME> – время в секундах, принимает значения [1..60]. Значение по умолчанию: 5.

Шаг	Описание	Команда	Ключи
21	Определить период обновления информации протокола ND для ipv6 vrrp в состоянии MASTER (не обязательно).	**esr(config-if-gi)# ipv6 vrrp timers nd refresh <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 5.
22	Определить количество ND сообщений отправляемых за период обновления для ipv6 vrrp в состоянии MASTER (не обязательно).	**esr(config-if-gi)# ipv6 vrrp timers nd refresh-repeat <NUM>**	<NUM> – количество, принимает значения [1..60]. Значение по умолчанию: 0.
23	Определить количество отправок ND-пакетов после установки ipv6 vrrp в состоянии MASTER (не обязательно).	**esr(config-if-gi)# ipv6 vrrp timers nd repeat <NUM>**	<NUM> – количество, принимает значения [1..60]. Значение по умолчанию: 1.

16.1.2 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 1/0/5.50
R1(config-subif)# vrrp id 10
```

Укажем IP-адрес виртуального шлюза 192.168.1.1/24:

```
R1(config-subif)# vrrp ip 192.168.1.1
```

Включим VRRP:

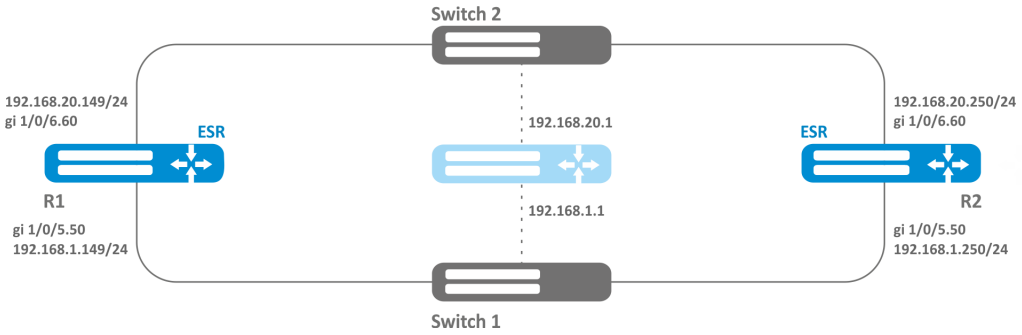
```
R1(config-subif)# vrrp
R1(config-subif)# exit
```

После чего необходимо произвести аналогичные настройки на R2.

16.1.3 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 1/0/5.50
R1(config-subif)# vrrp id 10
```

Укажем IP-адрес виртуального шлюза 192.168.1.1:

```
R1(config-subif)# vrrp ip 192.168.1.1
```

Укажем идентификатор VRRP-группы:

```
R1(config-subif)# vrrp group 5
```

Включим VRRP:

```
R1(config-subif)# vrrp
R1(config-subif)# exit
```

Настроим VRRP для подсети 192.168.20.0/24 в созданном саб-интерфейсе.

Укажем уникальный идентификатор VRRP:

```
R1(config-sub)#interface gi 1/0/6.60
R1(config-subif)# vrrp id 20
```

Укажем IP-адрес виртуального шлюза 192.168.20.1:

```
R1(config-subif)# vrrp ip 192.168.20.1
```

Укажем идентификатор VRRP-группы:

```
R1(config-subif)# vrrp group 5
```

Включим VRRP:

```
R1(config-subif)# vrrp
R1(config-subif)# 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.

16.2 Настройка tracking

Tracking — механизм позволяющий активировать сущности в зависимости от состояния VRRP/SLA.

16.2.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Настроить VRRP согласно разделу "Алгоритм настройки VRRP" или настроить SLA.		
2	Добавить в систему Tracking-объект и перейти в режим настройки параметров Tracking-объекта.	**esr(config)#track <ID>**	<ID> – номер Tracking-объекта, принимает значения [1..100].
3	Задать правило слежения за VRRP/SLA-процессами, на основании которых Tracking-объект будет переходить в активное состояние.	**esr(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.
		esr(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 – отслеживается состояние sla-теста; • reachability – отслеживается состояние канала связи, которое предоставляет sla-тест.
4	Включить Tracking-объект.	**esr(config-track)#enable**	
5	Установить задержку смены состояния отслеживаемого объекта (не обязательно).	**esr(config-track)# delay { down | up } <TIME>**	<TIME> – время задержки в секундах, задается в диапазоне [1..300].

Шаг	Описание	Команда	Ключи
6	Задать режим работы tracking (не обязательно).	**esr(config-track)# mode <MODE>**	<MODE> – условие нахождения Tracking-объекта в активном состоянии, принимает значения: • and – Tracking-объект будет находиться в активном состоянии, если все отслеживаемые условия будут в активном состоянии; • or – Tracking-объект будет находиться в активном состоянии, если хотя бы одно отслеживаемое условие будет в активном состоянии.
7	Создать сущность на ESR, 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).	**esr(config)# ip route [vrf <VRF>] <SUBNET> { <NEXTHOP> [resolve] | interface <IF> | tunnel <TUN> | wan load-balance rule <RULE> | blackhole | unreachable | prohibit } [<METRIC>] [track <TRACK-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 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).	**esr(config-if-gi)# shutdown track <ID>**	<ID> – номер Tracking-объекта, принимает значения [1..100].

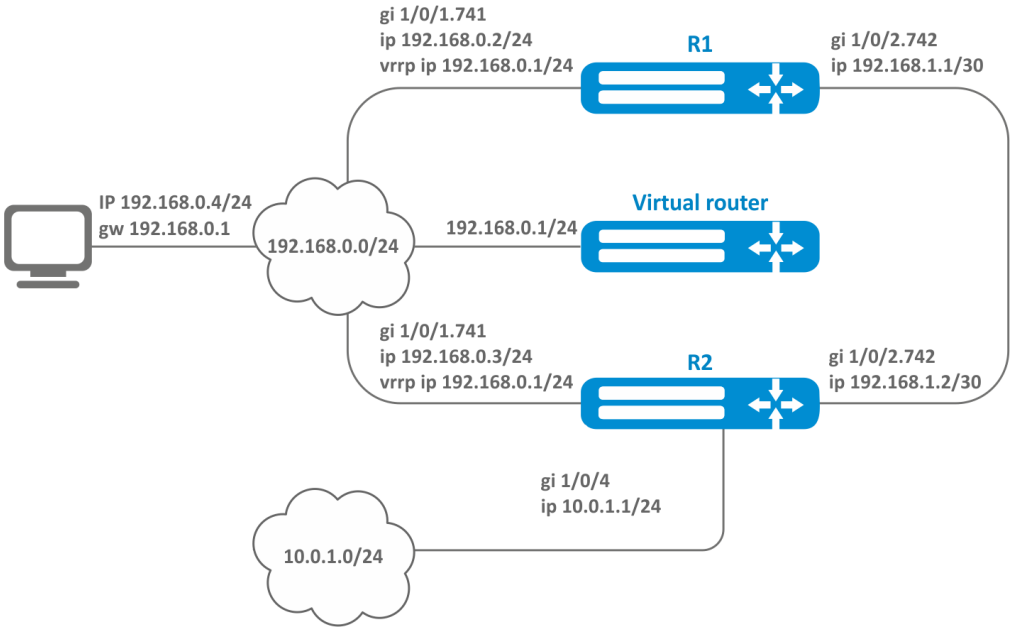
Шаг	Описание	Команда	Ключи
7.3	Добавить возможность управления приоритетом VRRP-процесса (не обязательно).	**esr(config-if-gi)# vrrp priority track <ID> { <PRIO> | increment <INC> | decrement <DEC> }**	<ID> – номер Tracking-объекта, принимает значения в диапазоне [1..100]; <PRIO> – приоритет VRRP-процесса, 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].
7.4	Добавить возможность управления Next-Hop для пакетов, которые попадают под критерии в указанном списке доступа (ACL) (не обязательно).	**esr(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 (не обязательно).	**esr(config-route-map-rule)# action set as-path prepend <AS-PATH> 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]; <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).	**esr(config-route-map-rule)# action set metric bgp <METRIC> track <ID>**	<METRIC> – значение атрибута BGPMED, принимает значения [0..4294967295]; <ID> – номер Tracking-объекта, принимает значения [1..100].

16.2.2 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 терминируется 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
```

16.3 Настройка Firewall/NAT failover

Firewall failover необходим для резервирования сессий firewall.

16.3.1 Алгоритм настройки

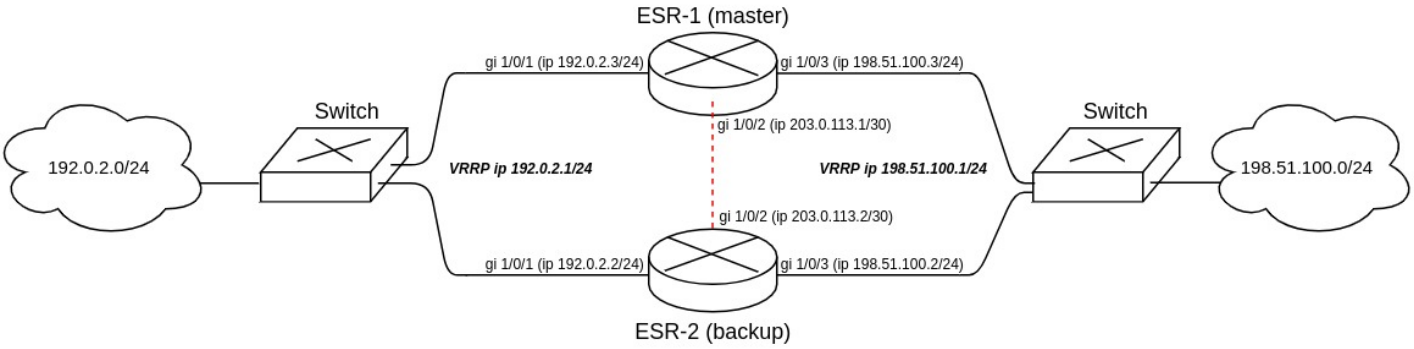
Шаг	Описание	Команда	Ключи
1	Выбор режима обмена информацией между маршрутизаторами.	**ip firewall failover sync-type <MODE>**	<MODE> – режим обмена информацией: • unicast – режим unicast; • multicast – режим multicast.
2	Выбор IP-адреса сетевого интерфейса, с которого будут отправляться сообщения при работе Firewall в режиме резервирования сессий.	**ip firewall failover source-address <ADDR>**	<ADDR> – IP-адрес сетевого интерфейса, с которого будут отправляться сообщения, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
3	Настройка IP-адреса соседа при работе резервирования сессий Firewall в unicast-режиме.	**ip firewall failover destination-address <ADDR>**	<ADDR> – IP-адрес соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
	Настройка многоадресного IP-адреса, который будет использоваться для обмена информации при работе резервирования сессий Firewall в multicast-режиме.	**ip firewall failover multicast-address <ADDR>**	<ADDR> – многоадресный IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
4	Если резервирование сессий Firewall работает в multicast-режиме, то необходимо настроить идентификатор multicast-группы.	**ip firewall failover multicast-group <GROUP>**	<GROUP> – multicast-группа, указывается в диапазоне [1000..9999].
5	Настройка номера UDP-порта службы резервирования сессий Firewall, через который происходит обмен информацией при работе в unicast-режиме. (не обязательно)	**ip firewall failover port <PORT>**	<PORT> – номер порта службы резервирования сессий Firewall, указывается в диапазоне [1..65535].
6	Привязка VRRP-группы, на основе которой определяется состояние (основной/резервный) маршрутизатора при резервировании сессий Firewall. (не обязательно)	**ip firewall failover vrrp-group <GRID>**	<GRID> – идентификатор группы VRRP-маршрутизатора, принимает значения [1..32].
7	Включение резервирования сессий Firewall.	**ip firewall failover**	

При настройке firewall failover также будут синхронизироваться NAT сессии между устройствами.

16.3.2 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 ESR-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 состоянии 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 firewall failover.

Выберем режим резервирование сессий unicast:

```
master(config)# ip firewall failover sync-type unicast
```

Выберем IP-адреса сетевого интерфейса, с которого будут отправляться сообщения при работе Firewall в режиме резервирования сессий:

```
master(config)# ip firewall failover source-address 203.0.113.1
```

Настроим IP-адреса соседа при работе резервирования сессий Firewall в unicast-режиме:

```
master(config)# ip firewall failover destination-address 203.0.113.2
```

Настроим номер UDP-порта службы резервирования сессий Firewall:

```
master(config)# ip firewall failover port 3333
```

Включим резервирования сессий Firewall:

```
master(config)# ip firewall failover
```

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
--------------   ---------------------------------   --------   ----------   ------
1                192.0.2.1/24                        20         Enabled      Master
3                198.51.100.1/24                     20         Enabled      Master
```

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 ESR-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)# exi
```

```
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 firewall failover sync-type unicast
backup(config)# ip firewall failover source-address 203.0.113.2
backup(config)# ip firewall failover destination-address 203.0.113.1
backup(config)# ip firewall failover port 3333
backup(config)# ip firewall failover vrrp-group 1
backup(config)# ip firewall failover
```

Настройка зоны безопасности аналогична настройки на маршрутизаторе ESR-1 (master).

16.4 Настройка DHCP failover

DHCP failover используется для резервирования базы IP-адресов, которые были динамически выданы в процессе работы DHCP-server.

16.4.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Переход в конфигурационное меню DHCP failover для его настройки.	**ip dhcp-server failover [vrf <VRF>]**	<VRF> – имя VRF, задается строкой до 31 символа;

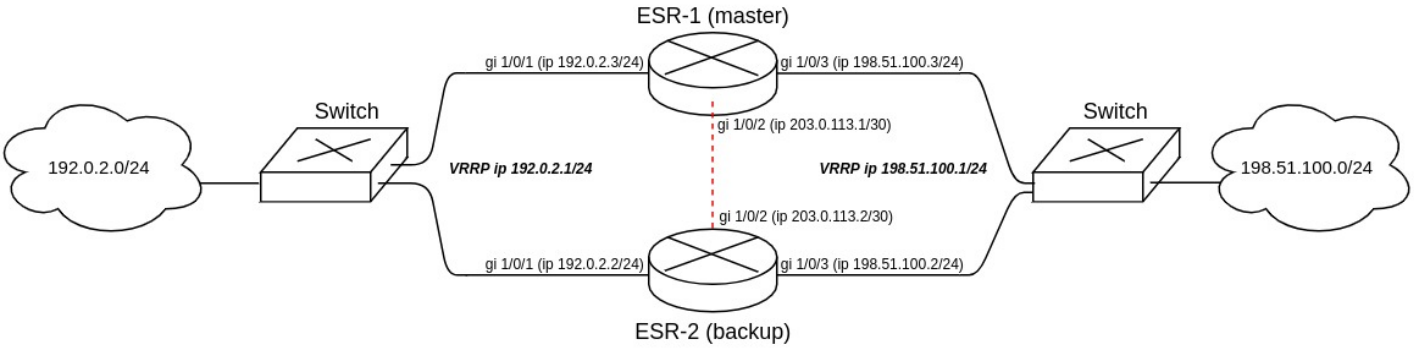
Шаг	Описание	Команда	Ключи
2	Выбор режима работы DHCP failover.	**mode { active-active | active-standby }**	active-active – режим работы с двумя активными маршрутизаторами; active-standby – режим работы с одним активным маршрутизатором и одним резервным.
3	Настройка IP-адреса, с которого будет работать DHCP failover.	**local-address <ADDR>**	<ADDR> – IP-адрес соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
4	Настройка удаленного IP-адреса соседа, с которым будет работать DHCP failover.	**remote-address <ADDR>**	<ADDR> – IP-адрес соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
5	Настройка роли DHCP failover, при работе резервирования в режиме Active-Active.	**role <ROLE>**	<ROLE> – роль DHCP-сервера при работе в режиме резервирования: • primary – режим активного DHCP-сервера; • secondary – режим резервного DHCP-сервера.
6	Привязка VRRP-группы, на основе которой определяется состояние (основной/резервный) маршрутизатора при резервировании сессий в режиме Active-Standby.	**vrrp-group <GRID>**	<GRID> – идентификатор группы VRRP-маршрутизатора, принимает значения [1..32].
7	Включение резервирования DHCP failover.	**enable**	

Режим active-standby не поддержан в VRF.

16.4.2 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 ESR-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 состоянии 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 dhcp-server failover
master(config-dhcp-server-failover)# mode active-standby
master(config-dhcp-server-failover)# local-address 203.0.113.1
master(config-dhcp-server-failover)# remote-address 203.0.113.2
master(config-dhcp-server-failover)# vrrp-group 1
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
--------------   ---------------------------------   --------   ----------   ------
1                192.0.2.1/24                        20         Enabled      Master
3                198.51.100.1/24                     20         Enabled      Master
```

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 ESR-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 dhcp-server failover
backup(config-dhcp-server-failover)# mode active-standby
backup(config-dhcp-server-failover)# local-address 203.0.113.2
backup(config-dhcp-server-failover)# remote-address 203.0.113.1
backup(config-dhcp-server-failover)# vrrp-group 1
backup(config-dhcp-server-failover)# enable
backup(config-dhcp-server-failover)# exit
```

Настройка зоны безопасности аналогична настройке на маршрутизаторе ESR-1 (master).

17 Управление удаленным доступом

- Настройка сервера удаленного доступа к корпоративной сети по PPTP-протоколу
  - Алгоритм настройки
  - Пример настройки
- Настройка сервера удаленного доступа к корпоративной сети по L2TP over IPsec протоколу
  - Алгоритм настройки
  - Пример настройки
- Настройка сервера удаленного доступа к корпоративной сети по OpenVPN-протоколу
  - Алгоритм настройки
  - Пример настройки
- Настройка клиента удаленного доступа по протоколу PPPoE
  - Алгоритм настройки
  - Пример настройки
- Настройка клиента удаленного доступа по протоколу PPTP
  - Алгоритм настройки
  - Пример настройки
- Настройка клиента удаленного доступа по протоколу L2TP
  - Алгоритм настройки
  - Пример настройки

17.1 Настройка сервера удаленного доступа к корпоративной сети по PPTP-протоколу

PPTP (англ. Point-to-Point Tunneling Protocol) – туннельный протокол типа точка-точка, позволяющий компьютеру устанавливать защищённое соединение с сервером за счёт создания специального туннеля в обычной незащищенной сети. PPTP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например, Интернет. PPTP может также использоваться для организации туннеля между двумя локальными сетями. PPTP использует дополнительное TCP-соединение для обслуживания туннеля.

17.1.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать профиль PPTP-сервера.	**esr(config)# remote-access pptp <NAME>**	<NAME> – имя профиля PPTP-сервера, задаётся строкой до 31 символа.
2	Указать описание конфигурируемого сервера (не обязательно).	**esr(config-pptp-server)# description <DESCRIPTION>**	<DESCRIPTION> – описание PPTP-сервера, задаётся строкой до 255 символов.

Шаг	Описание	Команда	Ключи
3	Указать IP-адрес, который должен обрабатывать PPTP-сервер.	**esr(config-pptp-server)# outside-address { object-group <OBJ-GROUP-NETWORK-NAME> | ip-address <ADDR> | interface { <IF> | <TUN> } }**	<OBJ-GROUP-NETWORK-NAME> – имя профиля содержащего IP-адрес, который должен слушать PPTP-сервер, задаётся строкой до 31 символа; <ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IF> – тип и идентификатор интерфейса маршрутизатора; <TUN> – тип и номер туннеля маршрутизатора.
4	Указать IP-адрес локального шлюза.	**esr(config-pptp-server)# local-address { object-group <OBJ-GROUP-NETWORK-NAME > | ip-address <ADDR> }**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит IP-адрес локального шлюза, задаётся строкой до 31 символа; <ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
5	Указать список IP-адресов, из которого PPTP выдаются динамические IP-адреса удаленным пользователям.	**esr(config-pptp-server)# remote-address { object-group <OBJ-GROUP-NETWORK-NAME > | address-range <FROM-ADDR>-<TO-ADDR> }**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит список IP-адресов удаленных пользователей, задаётся строкой до 31 символа; <FROM-ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <TO-ADDR> – конечный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Шаг	Описание	Команда	Ключи
6	Выбрать режим аутентификации PPTP-клиентов.	**esr(config-pptp-server)# authentication mode { local | radius }**	• local – аутентификация пользователя по локальной базе. • radius – аутентификация пользователя по базе RADIUS-сервера. На маршрутизаторе должен быть сконфигурирован механизм взаимодействия с RADIUS-сервером см. раздел Алгоритм настройки AAA по протоколу RADIUS.
7	Разрешить необходимые методы аутентификации удаленных пользователей.	**esr(config-pptp-server)# authentication method <METHOD>**	<METHOD> - метод аутентификации, принимает значения [chap, mschap, mschap-v2, eap, pap]. По умолчанию разрешен только chap
8	Указать имя пользователя (при использовании локальной аутентификации пользователей).	**esr(config-pptp-server) username < NAME >**	<NAME> – имя пользователя, задаётся строкой до 12 символов.
9	Указать пароль пользователя(при использовании локальной аутентификации пользователей).	**esr(config-pptp-user) password ascii-text { <PASSWORD> | encrypted <PASSWORD> }**	<PASSWORD> – пароль пользователя, задается строкой до 32 символов.
10	Активировать пользователя(при использовании локальной аутентификации пользователей).	**esr(config-pptp-user) enable**	
11	Включить PPTP-сервер в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall (см. раздел Конфигурирование Firewall).	**esr(config-pptp-server)# security-zone <NAME>**	<NAME> – имя зоны безопасности, задаётся строкой до 31 символа.
12	Включить сервер.	**esr(config-pptp-server)# enable**	
13	Указать DSCP-приоритет исходящих пакетов (не обязательно).	**esr(config-pptp-server)# dscp <DSCP>**	<DSCP>– dscp приоритет исходящих пакетов [0..63].

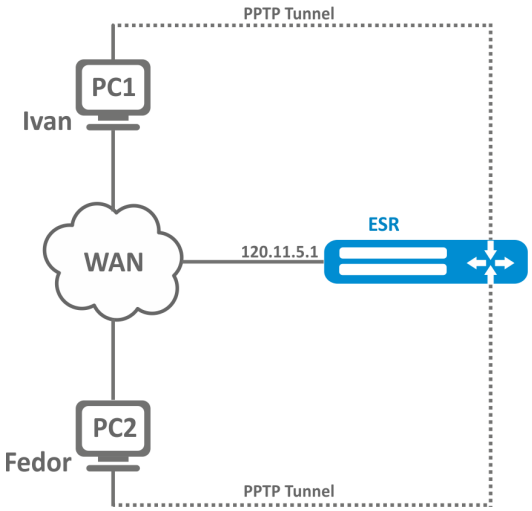
Шаг	Описание	Команда	Ключи
14	Включить шифрование MPPE для PPTP-соединений (не обязательно).	**esr(config-pptp-server)# encryption mppe**	
15	Указать размер MTU (MaximumTransmitionUnit) для сервера (не обязательно). MTU более 1500 будет активно только в случае применения команды "system jumbo-frames".	**esr(config-pptp-server) mtu <MTU>**	<MTU> – значение MTU, принимает значения в диапазоне [1280..1500]. Значение по умолчанию: 1500.
16	Указать список DNS-серверов, которые будут использовать удаленные пользователи (не обязательно).	**esr(config-pptp-server)# dns-servers object-group <OBJ-GROUP-NETWORK -NAME >**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, содержащего, который содержит адреса необходимых DNS-серверов, задаётся строкой до 31 символа.
17	Указать список WINS-серверов, которые будут использовать удаленные пользователи (не обязательно).	**esr(config-pptp-server)# wins-servers object-group <OBJ-GROUP-NETWORK-NAME >**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит адреса необходимых WINS-серверов, задаётся строкой до 31 символа.

17.1.2 Пример настройки

Задача:

Настроить PPTP-сервер на маршрутизаторе.

- адрес PPTP-сервера – 120.11.5.1;
- шлюз внутри туннеля для подключающихся клиентов – 10.10.10.1;
- пул IP-адресов для выдачи 10.10.10.5-10.10.10.25;
- DNS-серверы: 8.8.8.8, 8.8.8.4;
- учетные записи для подключения – fedor, ivan.



Решение:

Создадим профиль адресов, содержащий адрес, который должен слушать сервер:

```
esr# configure
esr(config)# object-group network pptp_outside
esr(config-object-group-network)# ip address-range 120.11.5.1
esr(config-object-group-network)# exit
```

Создадим профиль адресов, содержащий адрес локального шлюза:

```
esr(config)# object-group network pptp_local
esr(config-object-group-network)# ip address-range 10.10.10.1
esr(config-object-group-network)# exit
```

Создадим профиль адресов, содержащий адреса клиентов:

```
esr(config)# object-group network pptp_remote
esr(config-object-group-network)# ip address-range 10.10.10.5-10.10.10.25
esr(config-object-group-network)# exit
```

Создадим PPTP-сервер и привяжем вышеуказанные профили:

```
esr(config)# remote-access pptp remote-workers
esr(config-pptp)# local-address object-group pptp_local
esr(config-pptp)# remote-address object-group pptp_remote
esr(config-pptp)# outside-address object-group pptp_outside
esr(config-pptp)# dns-servers object-group pptp_dns
```

Выберем метод аутентификации пользователей PPTP-сервера:

```
esr(config-pptp)# authentication mode local
```

Укажем зону безопасности, к которой будут относиться сессии пользователей:

```
esr(config-pptp)# security-zone VPN
```

Создадим PPTP-пользователей *Ivan* и *Fedor* для PPTP-сервера:

```
esr(config-pptp)# username ivan
esr(config-pptp-user)# password ascii-text password1
esr(config-pptp-user)# enable
esr(config-pptp-user)# exit
esr(config-pptp)# username fedor
esr(config-pptp-user)# password ascii-text password2
esr(config-pptp-user)# enable
esr(config-pptp-user)# exit
esr(config-pptp)# exit
```

Включим PPTP-сервер:

```
esr(config-pptp)# enable
```

После применения конфигурации маршрутизатор будет прослушивать 120.11.5.1:1723. Состояние сессий PPTP-сервера можно посмотреть командой:

```
esr# show remote-access status pptp server remote-workers
```

Счетчики сессий PPTP-сервера можно посмотреть командой:

```
esr# show remote-access counters pptp server remote-workers
```

Очистить счетчики сессий PPTP-сервера можно командой:

```
esr# clear remote-access counters pptp server remote-workers
```

Завершить сессию пользователя fedor PPTP-сервера можно одной из следующих команд:

```
esr# clear remote-access session pptp username fedor
esr# clear remote-access session pptp server remote-workers username fedor
```

Конфигурацию PPTP-сервера можно посмотреть командой:

```
esr# show remote-access configuration pptp remote-workers
```

Помимо создания PPTP-сервера необходимо в firewall открыть TCP-порт 1723 для обслуживания соединений и разрешить протокол GRE(47) для туннельного трафика.

17.2 Настройка сервера удаленного доступа к корпоративной сети по L2TP over IPsec протоколу

L2TP (англ. Layer 2 Tunneling Protocol – протокол туннелирования второго уровня) – туннельный протокол, использующийся для поддержки виртуальных частных сетей. L2TP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например, Интернет. L2TP может также использоваться для организации туннеля между двумя локальными сетями. L2TP использует дополнительное UDP-соединение для обслуживания туннеля. L2TP-протокол не предоставляет средств шифрования данных и поэтому он обычно используется в связке с группой протоколов IPsec, которая предоставляет безопасность на пакетном уровне.

17.2.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать профиль L2TP-сервера.	**esr(config)# remote-access l2tp <NAME>**	<NAME> – имя профиля L2TP-сервера, задаётся строкой до 31 символа.
2	Указать описание конфигурируемого сервера (не обязательно).	**esr(config-l2tp-server)# description <DESCRIPTION>**	<DESCRIPTION> – описание L2TP-сервера, задаётся строкой до 255 символов.
3	Указать IP-адрес, который должен слушать L2TP-сервер.	**esr(config-l2tp-server)# outside-address { object-group <NAME> | ip-address <ADDR> | interface { <IF> | <TUN> } }**	<OBJ-GROUP-NETWORK-NAME> – имя профиля содержащего IP-адрес, который должен слушать L2TP-сервер, задаётся строкой до 31 символа; <ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IF> – тип и идентификатор интерфейса маршрутизатора; <TUN> – тип и номер туннеля маршрутизатора.

Шаг	Описание	Команда	Ключи
4	Указать IP-адрес локального шлюза либо отключить firewall для PPTP-сервера.	**esr(config-l2tp-server)# local-address { object-group <OBJ-GROUP-NETWORK -NAME> | ip-address <ADDR> }**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит IP-адрес локального шлюза, задаётся строкой до 31 символа; <ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
5	Указать список IP-адресов из которого L2TP выдаются динамические IP-адреса удаленным пользователям.	**esr(config-l2tp-server)# remote-address { object-group <OBJ-GROUP-NETWORK -NAME > | address-range <FROM-ADDR>-<TO-ADDR> }**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит список IP-адресов удаленных пользователей, задаётся строкой до 31 символа; <FROM-ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <TO-ADDR> – конечный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
6	Выбрать режим аутентификации L2TP-клиентов.	**esr(config-l2tp-server)# authentication mode { local | radius }**	• local – аутентификация пользователя по локальной базе. • radius – аутентификация пользователя по базе RADIUS-сервера. На маршрутизаторе должен быть сконфигурирован механизм взаимодействия с RADIUS-сервером см. раздел Алгоритм настройки AAA по протоколу RADIUS.

Шаг	Описание	Команда	Ключи
7	Разрешить необходимые методы аутентификации удаленных пользователей.	**esr(config-l2tp-server)# authentication method <METHOD>**	<METHOD> - метод аутентификации, принимает значения [chap, mschap, mschap-v2, eap, pap]. По умолчанию разрешен только chap.
8	Включить L2TP-сервер в зону безопасности и настроить правила взаимодействия между зонами (см. раздел Конфигурирование Firewall).	**esr(config-l2tp-server)# security-zone <NAME>**	<NAME> – имя зоны безопасности, задаётся строкой до 31 символа.
9	Указать имя пользователя (при использовании локальной базы аутентификации).	**esr(config-l2tp-server) username < NAME >**	<NAME> – имя пользователя, задаётся строкой до 12 символов.
10	Указать пароль пользователя (при использовании локальной базы аутентификации).	**esr(config-l2tp-user) password ascii-text { <PASSWORD> | encrypted <PASSWORD> }**	<PASSWORD> – пароль пользователя, задается строкой до 32 символов.
11	Включить пользователя (при использовании локальной базы аутентификации).	**esr(config-l2tp-user) enable**	
12	Выбрать метод аутентификации по ключу для IKE-соединения (по умолчанию).	**esr(config-l2tp-server)# ipsec authentication method pre-shared-key**	

Шаг	Описание	Команда	Ключи
13	Указать общий секретный ключ для аутентификации, который должен совпадать у обоих сторон, устанавливающих туннель.	**esr(config-l2tp-server)# ipsec authentication pre-shared-key { ascii-text { <TEXT> | encrypted <ENCRYPTED-TEXT> } | hexadecimal {<HEX> | encrypted <ENCRYPTED-HEX> } }**	<TEXT> – строка [1..64] ASCII символов; <HEX> – число размером [1..32] байт задаётся строкой [2..128] символов в шестнадцатеричном формате (0xYYYY...) или (YYYY...). <ENCRYPTED-TEXT> – зашифрованный пароль размером [1..32] байт, задаётся строкой [2..128] символов; <ENCRYPTED-HEX> – зашифрованное число размером [2..64] байт, задаётся строкой [2..256] символов.
14	Ограничить используемые методы аутентификации и шифрования протокола ike (не обязательно).	**esr(config-l2tp-server)# ipsec ike proposal <NAME>**	<NAME> – имя ранее созданного профиля протокола IKE, задаётся строкой до 31 символа.
15	Ограничить используемые методы аутентификации и шифрования протокола ipsec (не обязательно).	**esr(config-l2tp-server)# ipsec proposal <NAME>**	<NAME> – имя ранее созданного профиля IPsec, задаётся строкой до 31 символа.
16	Включить сервер.	**esr(config-l2tp-server)# enable**	
17	Указать DSCP приоритет исходящих пакетов.	**esr(config-l2tp-server)# dscp <DSCP>**	<DSCP> – dscp приоритет исходящих пакетов [0..63].
18	Указать размер MTU (MaximumTransmitionUnit) для сервера (не обязательно). MTU более 1500 будет активно только в случае применения команды "system jumbo-frames".	**esr(config-l2tp-server) mtu <MTU>**	<MTU> – значение MTU, принимает значения в диапазоне [1280..1500]. Значение по умолчанию: 1500.
19	Указать список DNS-серверов, которые будут использовать удаленные пользователи (не обязательно).	**esr(config-l2tp-server)# dns-servers object-group <OBJ-GROUP-NETWORK -NAME >**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, содержащего, который содержит адреса необходимых DNS-серверов, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
20	Указать список WINS-серверов, которые будут использовать удаленные пользователи (не обязательно).	**esr(config-l2tp-server)# wins-servers object-group <OBJ-GROUP-NETWORK -NAME >**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит адреса необходимых WINS-серверов, задаётся строкой до 31 символа.

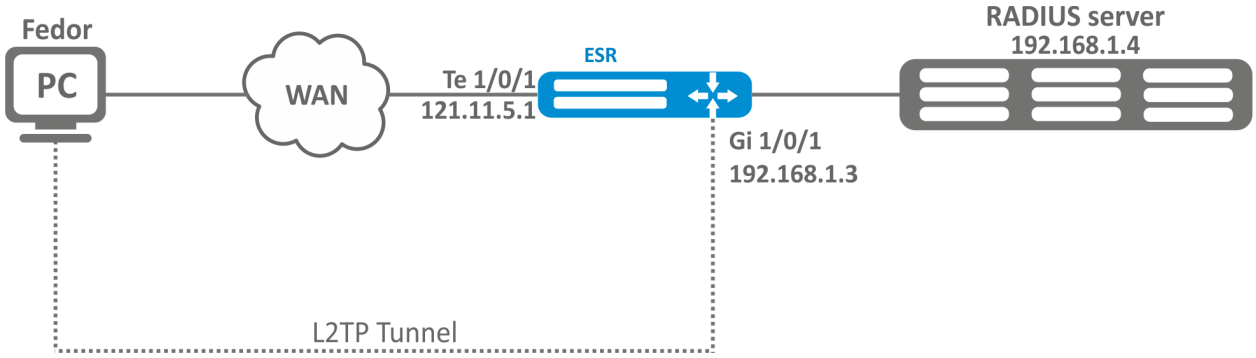
17.2.2 Пример настройки

Задача:

Настроить L2TP-сервер на маршрутизаторе для подключения удаленных пользователей к ЛВС. Аутентификация пользователей проходит на RADIUS-сервере.

- адрес L2TP-сервера – 120.11.5.1;
- шлюз внутри туннеля – 10.10.10.1;
- адрес Radius-сервера – 192.168.1.4;

Для IPsec используется метод аутентификации по ключу: ключ — «password».



Решение:

Предварительно нужно выполнить следующие действия:

- Настроить подключение к RADIUS-серверу;
- Настроить зоны для интерфейсов te1/0/1 и gi1/0/1;
- Указать IP-адреса для интерфейсов te1/0/1 и te1/0/1.

Создадим профиль адресов, содержащий адрес локального шлюза:

```
esr(config)# object-group network l2tp_local
esr(config-object-group-network)# ip address-range 10.10.10.1
esr(config-object-group-network)# exit
```

Создадим профиль адресов, содержащий DNS-серверы:

```
esr(config)# object-group network pptp_dns
esr(config-object-group-network)# ip address-range 8.8.8.8
esr(config-object-group-network)# ip address-range 8.8.4.4
esr(config-object-group-network)# exit
```

Создадим L2TP-сервер и привяжем к нему вышеуказанные профили:

```
esr(config)# remote-access l2tp remote-workers
esr(config-l2tp)# local-address ip-address 10.10.10.1
esr(config-l2tp)# remote-address address-range 10.10.10.5-10.10.10.15
esr(config-l2tp)# outside-address ip-address 120.11.5.1
esr(config-l2tp)# dns-server object-group l2tp_dns
```

Выберем метод аутентификации пользователей L2TP-сервера:

```
esr(config-l2tp)# authentication mode radius
```

Укажем зону безопасности, к которой будут относиться сессии пользователей:

```
esr(config-l2tp)# security-zone VPN
```

Выберем метод аутентификации первой фазы IKE и зададим ключ аутентификации:

```
esr(config-l2tp)# ipsec authentication method psk
esr(config-l2tp)# ipsec authentication pre-shared-key ascii-text password
```

Включим L2TP-сервер:

```
esr(config-l2tp)# enable
```

После применения конфигурации маршрутизатор будет прослушивать IP-адрес 120.11.5.1 и порт 1701.
Состояние сессий L2TP-сервера можно посмотреть командой:

```
esr# show remote-access status l2tp server remote-workers
```

Счетчики сессий L2TP-сервера можно посмотреть командой:

```
esr# show remote-access counters l2tp server remote-workers
```

Очистить счетчики сессий L2TP-сервера можно командой:

```
esr# clear remote-access counters l2tp server remote-workers
```

Завершить сессию пользователя fedor L2TP-сервера можно одной из следующих команд:

```
esr# clear remote-access session l2tp username fedor
esr# clear remote-access session l2tp server remote-workers username fedor
```

Конфигурацию L2TP-сервера можно посмотреть командой:

```
esr# show remote-access configuration l2tp remote-workers
```

Помимо создания L2TP-сервера необходимо в firewall открыть UDP-порты 500, 1701, 4500 для обслуживания соединений и разрешить протоколы ESP (50) и GRE (47) для туннельного трафика.

17.3 Настройка сервера удаленного доступа к корпоративной сети по OpenVPN-протоколу

OpenVPN — полнофункциональное средство для построения виртуальных частных сетей (Virtual Private Networks, VPN), организации удалённого доступа, и решения ряда других задач, связанных с безопасностью передачи данных, базирующееся на SSL.

17.3.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать профиль OpenVPN-сервера.	**esr(config)# remote-access openvpn <NAME>**	<NAME> – имя профиля OpenVPN-сервера, задаётся строкой до 31 символа.
2	Указать описание конфигурируемого сервера (не обязательно).	**esr(config-openvpn-server)# description <DESCRIPTION>**	<DESCRIPTION> – описание OpenVPN-сервера, задаётся строкой до 255 символов.
3	Определим подсеть, из которой выдаются IP-адреса пользователям. (только для tunnel ip).	**esr(config-openvpn-server)# network <ADDR/LEN>**	<ADDR/LEN> – адрес подсети, имеет следующий формат: AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [16..29];
4	Указать инкапсулируемый протокол.	**esr(config-openvpn-server)# protocol <PROTOCOL>**	<PROTOCOL> – тип инкапсуляции, возможные значения: • TCP-инкапсуляция в TCP-сегменты; • UDP-инкапсуляция в UDP-дейтаграммы.

Шаг	Описание	Команда	Ключи
5	Определить тип соединения с частной сетью через OpenVPN-сервер.	**esr(config-openvpn-server)# tunnel <TYPE>**	<TYPE> – инкапсулирующий протокол, принимает значения: • ip – соединение точка-точка; • ethernet – подключение к L2-домену.
6	Указать список IP-адресов, из которого OpenVPN сервером выдаются динамические IP-адреса удаленным пользователям в режиме L2. (только для tunnel ethernet).	**esr(config-openvpn-server)# address-range <FROM-ADDR>-<TO-ADDR>**	<FROM-ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <TO-ADDR> – конечный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
7	Включить клиентские соединения по OpenVPN в L2-домен (только для tunnel ethernet).	**esr(config-openvpn-server)# bridge-group <BRIDGE-ID>**	<BRIDGE-ID> – идентификационный номер моста.
8	Указать сертификаты и ключи.	**esr(config-openvpn-server)# certificate <CERTIFICATE-TYPE> <NAME>**	<CERTIFICATE-TYPE> – тип сертификата или ключа, может принимать следующие значения: • ca – сертификат удостоверяющего сервера; • crl – список отозванных сертификатов; • dh – ключ Диффи-Хеллмана; • server - crt – публичный сертификат сервера; • server - key – приватный ключ сервера; • ta – HMAC ключ. <NAME> – имя сертификата или ключа, задаётся строкой до 31 символа.
9	Выбрать алгоритм шифрования, используемый при передачи данных.	**esr(config-openvpn-server)# encryption algorithm <ALGORITHM>**	<ALGORITHM> – идентификатор протокола шифрования, принимает значения: 3des,blowfish128, aes128.

Шаг	Описание	Команда	Ключи
10	Включить OpenVPN-сервер в зону безопасности и настроить правила взаимодействия между зонами (см. раздел Конфигурирование Firewall).	**esr(config-openvpn-server)# security-zone <NAME>**	<NAME> – имя зоны безопасности, задаётся строкой до 31 символа.
11	Определить дополнительные параметры для указанного пользователя OpenVPN-сервера (при использовании локальной базы для аутентификации пользователей).	**esr(config-openvpn-server)# username < NAME >**	<NAME> – имя пользователя, задаётся строкой до 31 символа.
12	Определить подсеть для указанного пользователя OpenVPN-сервера.	**esr(config-openvpn-user)# subnet <ADDR/LEN>**	<ADDR/LEN> – адрес подсети, имеет следующий формат: AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [16..32].
13	Определить статический ip-адрес для указанного пользователя OpenVPN-сервера	**esr(config-openvpn-user)# ip address <ADDR>**	<ADDR> – адрес имеет следующий формат: AAA.BBB.CCC.DDD – IP-адрес подсети, где AAA-DDD принимают значения [0..255].
14	Включить профиль OpenVPN-сервера.	**esr(config-openvpn-server)# enable**	
15	Включить блокировку передачи данных между клиентами (не обязательно).	**esr(config-openvpn-server)# client-isolation**	
16	Устанавливается максимальное количество одновременных пользовательских сессий (не обязательно).	**esr(config-openvpn-server)# client-max <VALUE>**	<VALUE> – максимальное количество пользователей, принимает значения [1..65535].
17	Включается механизм сжатия передаваемых данных между клиентами и сервером OpenVPN (не обязательно).	**esr(config-openvpn-server)# compression**	
18	Указать список DNS-серверов, которые будут использовать удаленные пользователи (не обязательно).	**esr(config-openvpn-server)# dns-server <ADDR>**	<ADDR> – IP-адрес DNS сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

Шаг	Описание	Команда	Ключи
19	Указать TCP-/UDP-порт, который будет прослушиваться OpenVPN-сервером (не обязательно).	**esr(config-openvpn-server)# port <PORT>**	<PORT> – TCP/UDP порт, принимает значения [1..65535]. Значение по умолчанию: 1194
20	Включить анонсирование маршрута по умолчанию для OpenVPN соединений, что приводит к замене маршрута по умолчанию на клиентской стороне (не обязательно).	**esr(config-openvpn-server)# redirect-gateway**	
21	Включить анонсирование указанных подсетей, шлюзом является IP-адрес OpenVPN-сервера (не обязательно).	**esr(config-openvpn-server)# route <ADDR/LEN>**	<ADDR/LEN> – адрес подсети, имеет следующий формат: 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];
22	Указать временной интервал, по истечению которого встречная сторона считается недоступной (не обязательно).	**esr(config-openvpn-server)# timers holdtime <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 120
23	Указать временной интервал, по истечению которого идет проверка соединения со встречной стороной (не обязательно).	**esr(config-openvpn-server)# timers keepalive <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 10
24	Разрешить подключаться к OpenVPN-серверу нескольким пользователям с одним сертификатом.	**esr(config-openvpn-server)# duplicate-cn**	
25	Указать список WINS-серверов, которые будут использовать удаленные пользователи (не обязательно).	**esr(config-openvpn-server)# wins-server <ADDR>**	<ADDR> – IP-адрес WINS сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

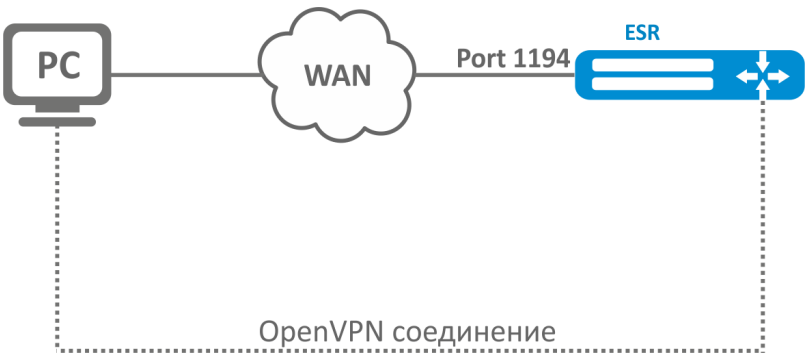
Шаг	Описание	Команда	Ключи
26	Изменить алгоритм аутентификации OpenVPN-клиентов (не обязательно).	**esr(config-openvpn-server)# authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм аутентификации: • 8-128 bits key size: md4, rsa-md4, md5, rsa-md5, mdc2, rsa-mdc2 • 8-160 bits key size: sha, sha1, rsa-sha, rsa-sha1, rsa-sha1-2, dsa, dsa-sha, dsa-sha1, dsa-sha1-old, ripemd160, rsa-ripemd160, ecdsa-with-sha1 • 8-224 bits key size: sha-224, rsa-sha-224 • 8-256 bits key size: sha-256, rsa-sha-256 • 8-384 bits key size: sha-384, rsa-sha-384 • 8-512 bits key size: sha-512, rsa-sha-512, whirlpool Значение по умолчанию: sha

17.3.2 Пример настройки

Задача:

Настроить OpenVPN-сервер в режиме L3 на маршрутизаторе для подключения удаленных пользователей к ЛВС.

- подсеть OpenVPN-сервера – 10.10.100.0/24;
- режим – L3;
- аутентификация на основе сертификатов.



Решение:

Предварительно нужно выполнить следующие действия:

- Подготовить сертификаты и ключи:
  - Сертификат Удостоверяющего Центра (CA)
  - Ключ и сертификат для OpenVPN сервера
  - Ключ Диффи-Хелмена и HMAC для TLS
- Настроить зону для интерфейса te1/0/1
- Указать IP-адреса для интерфейса te1/0/1.

Импортируем по tftp сертификаты и ключи:

```
esr# copy tftp://192.168.16.10:/ca.crt certificate:ca/ca.crt
esr# copy tftp://192.168.16.10:/dh.pem certificate:dh/dh.pem
esr# copy tftp://192.168.16.10:/server.key certificate:server-key/server.key
esr# copy tftp://192.168.16.10:/server.crt certificate:server-crt/server.crt
esr# copy tftp://192.168.16.10:/ta.key certificate:ta/ta.key
```

Создадим OpenVPN-сервер и подсеть, в которой он будет работать:

```
esr(config)# remote-access openvpn AP
esr(config-openvpn)# network 10.10.100.0/24
```

Укажем тип соединения L3 и протокол инкапсуляции:

```
esr(config-openvpn)# tunnel ip
esr(config-openvpn)# protocol tcp
```

Объявим подсети ЛВС которые будут доступны через OpenVPN соединение и укажем DNS-сервер:

```
esr(config-)# route 10.10.0.0/20
esr(config-openvpn)# dns-server 10.10.1.1
```

Укажем ранее импортированные сертификаты и ключи, которые будет использоваться OpenVPN-сервером:

```
esr(config-openvpn)# certificate ca ca.crt
esr(config-openvpn)# certificate dh dh.pem
esr(config-openvpn)# certificate server-key server.key
esr(config-openvpn)# certificate server-crt server.crt
esr(config-openvpn)# certificate ta ta.key
```

Укажем зону безопасности, к которой будут относиться сессии пользователей:

```
esr(config-openvpn)# security-zone VPN
```

Выберем алгоритм шифрования aes128:

```
esr(config-openvpn)# encryption algorithm aes128
```

Включим OpenVPN-сервер:

```
esr(config-openvpn)# enable
```

После применения конфигурации маршрутизатор будет прослушивать порт 1194 (используется по умолчанию).

Состояние сессий OpenVPN-сервера можно посмотреть командой:

```
esr# show remote-access status openvpn server AP
```

Счетчики сессий OpenVPN-сервера можно посмотреть командой:

```
esr# show remote-access counters openvpn server AP
```

Очистить счетчики сессий OpenVPN-сервера можно командой:

```
esr# clear remote-access counters openvpn server AP
```

Завершить сессию пользователя fedor OpenVPN-сервера можно одной из следующих команд:

```
esr# clear remote-access session openvpn username fedor
esr# clear remote-access session openvpn server AP username fedor
```

Конфигурацию OpenVPN-сервера можно посмотреть командой:

```
esr# show remote-access configuration openvpn AP
```

⚠ **Помимо создания OpenVPN-сервера необходимо в firewall открыть TCP-порт 1194.**

17.4 Настройка клиента удаленного доступа по протоколу PPPoE

PPPoE — это туннелирующий протокол (tunneling protocol), который позволяет инкапсулировать IP PPP через соединения Ethernet и обладает программными возможностями PPP-соединений, что позволяет использовать его для виртуальных соединений на соседнюю Ethernet-машину и устанавливать соединение точка-точка, которое используется для транспортировки IP-пакетов, а также работает с возможностями PPP. Это позволяет применять традиционное PPP-ориентированное ПО для настройки соединения, которое использует не последовательный канал, а пакетно-ориентированную сеть (например, Ethernet), чтобы организовать классическое соединение с логином и паролем для Интернет-соединений. Кроме того, IP-адрес по другую сторону соединения назначается только когда PPPoE-соединение открыто, позволяя динамическое переиспользование IP-адресов.

17.4.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать PPPoE-туннель и перейти в режим конфигурирования PPPoE-клиента.	**esr(config)# tunnel pppoe <PPPoE>**	<PPPoE> – порядковый номер туннеля от 1 до 10.

Шаг	Описание	Команда	Ключи
2	Указать описание конфигурируемого клиента (не обязательно).	**esr(config-pppoe)# description <DESCRIPTION>**	<DESCRIPTION> – описание PPPoE-сервера, задаётся строкой до 255 символов.
3	Указать имя экземпляра VRF, в котором будут использоваться PPPoE-клиент (не обязательно).	**esr(config-pppoe)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.
4	Указать интерфейс, через который будет устанавливаться PPPoE соединение.	**esr(config-pppoe)# interface <IF>**	<IF> – интерфейс или группа интерфейсов.
5	Указать имя пользователя и пароль для подключения к PPPoE-серверу.	**esr(config-pppoe)# username <NAME> password ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<NAME> – имя пользователя, задаётся строкой до 31 символа; <CLEAR-TEXT> – пароль, задаётся строкой [8 .. 64] символов; <ENCRYPTED-TEXT> – зашифрованный пароль, задаётся строкой [16..128] символов.
6	Включить PPPoE-туннель в зону безопасности и настроить правила взаимодействия между зонами (см. раздел Конфигурирование Firewall).	**esr(config-pppoe)# security-zone <NAME>**	<NAME> – имя зоны безопасности, задаётся строкой до 31 символа.
7	Активировать конфигурируемый профиль	**esr(config-pppoe)# enable**	
8	Указать метод аутентификации (не обязательно).	**esr(config-pppoe)# authentication method <METHOD>**	<METHOD> – метод аутентификации, возможные значения: chap, mschap, mschap-v2, eap, pap. Значение по умолчанию: chap.
9	Включить отказ от получения маршрута по умолчанию от PPPoE-сервера (не обязательно).	**esr(config-pppoe)# ignore-default-route**	
10	Указать интервал времени, за который усредняется статистика о нагрузке (не обязательно).	**esr(config-pppoe)# load-average <TIME>**	<TIME> – интервал времени в секундах от 5 до 150 (по умолчанию 5 с).

Шаг	Описание	Команда	Ключи
11	Указать размер MTU (MaximumTransmitionUnit) для PPPOE-туннеля. MTU более 1500 будет активно только если применена команда "system jumbo-frames" (не обязательно).	**esr(config-pppoe)# mtu <MTU>**	<MTU> – значение MTU, принимает значения в диапазоне: • для ESR-10/12V(F)/ 14VF – [1280..9600]; • для ESR-20/21 – [1280..9500]; • для ESR-100/200/1000/1200/1500/1511/1700 – [1280..10000] • для ESR-3100 – [1280..9190]. Значение по умолчанию: 1500.
12	Изменить количество неудачных data-link тестов перед разрывом сессии (не обязательно).	**esr(config-pppoe)# ppp failure-count <NUM>**	<NUM> – количество неудачных data-link тестов, задается в диапазоне [1..100]. Значение по умолчанию: 10
13	Изменить интервал времени в секундах, по истечении которого маршрутизатор отправляет keepalive-сообщение (не обязательно).	**esr(config-pppoe)# ppp timeout keepalive <TIME >**	<TIME> – время в секундах, задается в диапазоне [1..32767]. Значение по умолчанию: 10.
14	Переопределить значение поля MSS (Maximum segment size) во входящих TCP-пакетах (не обязательно).	**esr(config-pppoe)# ip tcp adjust-mss <MSS>**	<MSS> – значение MSS, принимает значения в диапазоне [500..1460]. Значение по умолчанию: 1460.
15	Включить запись статистики использования текущего туннеля (не обязательно).	**esr(config-pppoe)# history statistics**	

Также для PPPoE-клиента возможно настроить:

- QoS в базовом или расширенном режимах (см. раздел Управление QoS);
- Proxy (см. раздел Проксирование HTTP/HTTPS-трафика);
- Мониторинг траффика (см. разделы Настройка Netflow и Настройка sFlow).

17.4.2 Пример настройки

Задача:

Настроить PPPoE-клиент на маршрутизаторе.

- Учетные записи для подключения – tester;
- Пароли учетных записей – password;
- Подключение должно осуществляться с интерфейса gigabitethernet 1/0/7.

Решение:

Предварительно настроить PPPoE-сервер с учетными записями.

Зайдем в режим конфигурирования PPPoE-клиента и отключим межсетевой экран:

```
esr# configure
esr(config)# tunnel pppoe 1
esr(config-pppoe)# ip firewall disable
```

Укажем пользователя и пароль для подключения к PPPoE-серверу:

```
esr(config-pppoe)# username tester password ascii-text password
```

Укажем интерфейс через который будет устанавливаться PPPoE-соединение:

```
esr(config-pppoe)# interface gigabitethernet 1/0/7
esr(config- pppoe)# enable
```

Состояние PPPoE-туннеля можно посмотреть командой:

```
esr# show tunnels configuration pppoe 1
```

Счетчики сессий PPPoE-клиента можно посмотреть командой:

```
esr# show tunnels counters pppoe 1
```

17.5 Настройка клиента удаленного доступа по протоколу PPTP

PPTP (англ. Point-to-Point Tunneling Protocol) – туннельный протокол типа точка-точка, позволяющий устанавливать защищённое соединение за счёт создания специального туннеля в обычной незащищенной сети. PPTP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например, Интернет. PPTP может также использоваться для организации туннеля

между двумя локальными сетями. PPTP использует дополнительное TCP-соединение для обслуживания туннеля.

17.5.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать PPTP-туннель и перейти в режим его конфигурирования.	**esr(config)# tunnel pptp <INDEX>**	<INDEX> – идентификатор туннеля в диапазоне: [1..10].
2	Указать описание конфигурируемого туннеля (не обязательно).	**esr(config-pptp)# description <DESCRIPTION>**	<DESCRIPTION> – описание туннеля, задается строкой до 255 символов.
3	Указать экземпляр VRF, в котором будет работать данный PPTP-туннель (не обязательно).	**esr(config-pptp)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.
4	Включить PPTP-туннель в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall (см. раздел Конфигурирование Firewall).	**esr(config-pptp)# security-zone <NAME>**	<NAME> – имя зоны безопасности, задаётся строкой до 31 символа.
		esr(config-pptp)# ip firewall disable	
5	Установить удаленный IP-адрес для установки туннеля.	**esr(config-pptp)# remote address <ADDR>**	<ADDR> – IP-адрес локального шлюза, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
6	Установить размер MTU (MaximumTransmitionUnit) для туннеля (не обязательно)	**esr(config-pptp)# mtu <MTU>**	<MTU> – значение MTU, принимает значения в диапазоне: • для ESR-10/12V(F)/ 14VF – [552..9600]; • для ESR-20/21 – [552..9500]; • для ESR-100/200/1000/1200/1500/1511/1700 – [552..10000] • для ESR-3100 – [552..9190]. Значение по умолчанию: 1500.

Шаг	Описание	Команда	Ключи
7	Указать пользователя и установить пароль в открытой или зашифрованной форме для аутентификации удаленной стороны.	**esr(config-pptp)# username <NAME> password ascii-text { <WORD> | encrypted <HEX> }**	<NAME> – имя пользователя, задается строкой до 31 символа. <WORD> – пароль в открытой форме, задается строкой [8..64] символов, может включать символы [0-9a-fA-F]. <HEX> – пароль в зашифрованной форме, задается строкой [16..128] символов.
8	Активировать туннель.	**esr(config-pptp)# enable**	
9	Переопределить значение поля MSS (Maximum segment size) во входящих TCP-пакетах (не обязательно).	**esr(config-pptp)# ip tcp adjust-mss <MSS>**	<MSS> – значение MSS, принимает значения в диапазоне [500..1460]. Значение по умолчанию: 1460.
10	Игнорировать маршрут по умолчанию через данный PPTP-туннель (не обязательно)	**esr(config-pptp)# ignore-default-route**	
11	Задать интервал времени, за который усредняется статистика о нагрузке на туннель (не обязательно).	**esr(config-pptp)# load-average <TIME>**	<TIME> – интервал в секундах, принимает значения [5..150] Значение по умолчанию: 5.
12	Указать метод аутентификации (не обязательно).	**esr(config-pptp)# authentication method <METHOD>**	<METHOD> – метод аутентификации, возможные значения: chap, mschap, mschap-v2, eap, pap Значение по умолчанию: chap.
13	Включить запись статистики использования текущего туннеля (не обязательно).	**esr(config-pptp)# history statistics**	
14	Изменить интервал времени в секундах, по истечении которого маршрутизатор отправляет keepalive-сообщение (не обязательно).	**esr(config-pptp)# ppp timeout keepalive <TIME >**	<TIME> – время в секундах, задается в диапазоне [1..32767]. Значение по умолчанию: 10.

Шаг	Описание	Команда	Ключи
15	Изменить количество неудачных data-link тестов перед разрывом сессии (не обязательно).	**esr(config-pptp)# ppp failure-count <NUM>**	<NUM> – количество неудачных data-link тестов, задается в диапазоне [1..100]. Значение по умолчанию: 10.

17.5.2 Пример настройки

Задача:

Настроить PPTP-туннель на маршрутизаторе:

- адрес PPTP-сервера 20.20.0.1;
- учетная запись для подключения – логин: ivan, пароль: simplepass.

Решение:

Создадим туннель PPTP:

```
esr(config)# tunnel pptp 1
```

Укажем учетную запись (пользователя Ivan) для подключения к серверу:

```
esr(config-pptp)# username ivan password ascii-text simplepass
```

Укажем удаленный шлюз:

```
esr(config-pptp)# remote address 20.20.0.1
```

Укажем зону безопасности:

```
esr(config-pptp)# security-zone VPN
```

Включим туннель PPTP:

```
esr(config-pptp)# enable
```

Состояние туннеля можно посмотреть командой:

```
esr# show tunnels status pptp
```

Счетчики входящих и отправленных пакетов можно посмотреть командой:

```
esr# show tunnels counters pptp
```

Конфигурацию туннеля можно посмотреть командой:

```
esr# show tunnels configuration pptp
```

17.6 Настройка клиента удаленного доступа по протоколу L2TP

L2TP (англ. Layer 2 Tunneling Protocol – протокол туннелирования второго уровня) – туннельный протокол, использующийся для поддержки виртуальных частных сетей. L2TP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например, Интернет. L2TP может также использоваться для организации туннеля между двумя локальными сетями. L2TP использует дополнительное UDP-соединение для обслуживания туннеля. L2TP-протокол не предоставляет средств шифрования данных и поэтому он обычно используется в связке с группой протоколов IPsec, которая предоставляет безопасность на пакетном уровне.

17.6.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать L2TP-туннель и перейти в режим его конфигурирования.	**esr(config)# tunnel l2tp <INDEX>**	<INDEX> – идентификатор туннеля в диапазоне: [1..10].
2	Указать экземпляр VRF, в котором будет работать данный L2TP-туннель (не обязательно).	**esr(config-l2tp)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задаётся строкой до 31 символа.
3	Указать описание конфигурируемого туннеля (не обязательно).	**esr(config-l2tp)# description <DESCRIPTION>**	<DESCRIPTION> – описание туннеля, задается строкой до 255 символов.
4	Включить L2TP-туннель в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall (см. раздел Конфигурирование Firewall).	**esr(config-l2tp)# security-zone <NAME>**	<NAME> – имя зоны безопасности, задаётся строкой до 31 символа.
		esr(config-l2tp)# ip firewall disable	
5	Установить удаленный IP-адрес для установки туннеля.	**esr(config-l2tp)# remote address <ADDR>**	<ADDR> – IP-адрес локального шлюза, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Шаг	Описание	Команда	Ключи
6	Указать пользователя и установить пароль в открытой или зашифрованной форме для аутентификации удалённой стороны.	**esr(config-l2tp)# username <NAME> password ascii-text { <WORD> | encrypted <HEX> }**	<NAME> – имя пользователя, задается строкой до 31 символа. <WORD> – пароль в открытой форме, задается строкой [8..64] символов, может включать символы [0-9a-fA-F]. <HEX> – пароль в зашифрованной форме, задается строкой [16..128] символов.
7	Выбрать метод аутентификации по ключу для IKE-соединения.	**esr(config-l2tp)# ipsec authentication method pre-shared-key**	
8	Указать общий секретный ключ для аутентификации, который должен совпадать у обоих сторон, устанавливающих туннель.	**esr(config-l2tp)# ipsec authentication pre-shared-key { ascii-text { <TEXT> | encrypted <ENCRYPTED-TEXT> } | hexadecimal {<HEX> | encrypted <ENCRYPTED-HEX> } }**	<TEXT> – строка [1..64] ASCII символов; <HEX> – число размером [1..32] байт задаётся строкой [2..128] символов в шестнадцатеричном формате (0xYYYY...) или (YYYY...); <ENCRYPTED-TEXT> – зашифрованный пароль размером [1..32] байт, задаётся строкой [2..128] символов; <ENCRYPTED-HEX> – зашифрованное число размером [2..64] байт, задаётся строкой [2..256] символов.
9	Ограничить используемые методы аутентификации и шифрования протокола ike (не обязательно).	**esr(config-l2tp)# ipsec ike proposal <NAME>**	<NAME> – имя ранее созданного профиля протокола IKE, задаётся строкой до 31 символа.
10	Ограничить используемые методы аутентификации и шифрования протокола ipsec (не обязательно).	**esr(config-l2tp)# ipsec proposal <NAME>**	<NAME> – имя ранее созданного профиля IPsec, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
11	Определяется номер udp-порта по которому устанавливается соединение с l2tp-сервером (не обязательно).	**esr(config-l2tp)# port <PORT>**	<PORT> – номер udp-порта, задаётся в диапазоне [1024..65535]. Значение по умолчанию: 1701
12	Активировать туннель.	**esr(config-l2tp)# enable**	
13	Установить размер MTU (MaximumTransmitionUnit) для туннеля (не обязательно).	**esr(config-l2tp)# mtu <MTU>**	<MTU> – значение MTU, принимает значения в диапазоне: • для ESR-10/12V(F)/ 14VF – [552..9600]; • для ESR-20/21 – [552..9500]; • для ESR-100/200/1000/1200/1500/1511/1700 – [552..10000] • для ESR-3100 – [552..9190]. Значение по умолчанию: 1500.
14	Игнорировать маршрут по умолчанию через данный L2TP-туннель (не обязательно)	**esr(config-l2tp)# ignore-default-route**	
15	Указать метод аутентификации (не обязательно).	**esr(config-l2tp)# authentication method <METHOD>**	<METHOD> – метод аутентификации, возможные значения: chap, mschap, mschap-v2, eap, pap Значение по умолчанию: chap.
16	Задать интервал времени, за который усредняется статистика о нагрузке на туннель (не обязательно).	**esr(config-l2tp)# load-average <TIME>**	<TIME> – интервал в секундах, принимает значения [5..150] Значение по умолчанию: 5.
17	Изменить интервал времени в секундах, по истечении которого маршрутизатор отправляет keepalive-сообщение (не обязательно).	**esr(config-l2tp)# ppp timeout keepalive <TIME >**	<TIME> – время в секундах, задается в диапазоне [1..32767]. Значение по умолчанию: 10.

Шаг	Описание	Команда	Ключи
18	Изменить количество неудачных data-link тестов перед разрывом сессии (не обязательно).	**esr(config-l2tp)# ppp failure-count <NUM>**	<NUM> – количество неудачных data-link тестов, задается в диапазоне [1..100]. Значение по умолчанию: 10.
Также для L2TP-клиента возможно настроить QoS в базовом или расширенном режимах (см. раздел Управление QoS).			

17.6.2 Пример настройки

Задача:

Настроить PPTP-туннель на маршрутизаторе:

- адрес PPTP сервера 20.20.0.1;
- учетная запись для подключения – логин: ivan, пароль: simplepass

Решение:

Создадим туннель L2TP:

```
esr(config)# tunnel l2tp 1
```

Укажем учетную запись (пользователя Ivan) для подключения к серверу:

```
esr(config-l2tp)# username ivan password ascii-text simplepass
```

Укажем удаленный шлюз:

```
esr(config-l2tp)# remote address 20.20.0.1
```

Укажем зону безопасности:

```
esr(config-l2tp)# security-zone VPN
```

Укажем метод аутентификации IPsec:

```
esr(config-l2tp)# ipsec authentication method pre-shared-key
```

Укажем ключ безопасности для IPsec:

```
esr(config-l2tp)# ipsec authentication pre-shared-key ascii-text password
```

Включим туннель L2TP:

```
esr(config-l2tp)# enable
```

Состояние туннеля можно посмотреть командой:

```
esr# show tunnels status l2tp
```

Счетчики входящих и отправленных пакетов можно посмотреть командой:

```
esr# show tunnels counters l2tp
```

Конфигурацию туннеля можно посмотреть командой:

```
esr# show tunnels configuration l2tp
```

18 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
- Проксирование HTTP/HTTPS-трафика
  - Алгоритм настройки
  - Пример настройки HTTP-прокси
- Настройка NTP
  - Алгоритм настройки
  - Пример настройки

18.1 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.

18.1.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Включить IPv4/IPv6 DHCP-сервер.	**esr(config)# ip dhcp-server [vrf <VRF>]**	<VRF> – имя экземпляра VRF, в рамках которого будет работать DHCP-сервер. Задается строкой до 31 символа.
		esr(config)# ipv6 dhcp-server [vrf <VRF>]	
2	Задать значение кода DSCP для использования в IP-заголовке исходящих пакетов DHCP-сервера (не обязательно).	**esr(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.	**esr(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. Задается строкой до 31 символа
		esr(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.	**esr(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].
		esr(config-ipv6-dhcp-server)# network <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].
5	Добавить диапазон IPv4/IPv6-адресов к пулу адресов, конфигурируемого DHCP-сервера.	**esr(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
		esr(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::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).	**esr(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 DHCPOption61. Может быть задан в одном из следующих видов: • 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.
		esr(config-ipv6-dhcp-server)# address <ADDR> mac-address <MAC>	<IPV6-ADDR> – IPv6-адрес клиента, задаётся в виде X: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.	**esr(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).	**esr(config-dhcp-server)# domain-name <NAME>**	<NAME> – DNS-имя домена клиента, задаётся строкой до 255 символов.
		esr(config-ipv6-dhcp-server)# domain-name <NAME>	
9	Задать список IPv4/IPv6-адресов DNS-серверов. Список передаётся клиентам в составе DHCP-опции 6 (не обязательно).	**esr(config-dhcp-server)# dns-server <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.
		esr(config-ipv6-dhcp-server)# dns-server <IPV6-ADDR>	<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.	**esr(config-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
		esr(config-ipv6-dhcp-server)# max-lease-time <TIME>	

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.	**esr(config-dhcp-server)# default-lease-time <TIME>** **esr(config-ipv6-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.
12	Создать идентификатор класса поставщика (DHCP Опция 60) (не обязательно).	**esr(config)# ip dhcp-server vendor-class-id <NAME>** **esr(config)# ipv6 dhcp-server vendor-class-id <NAME>**	<NAME> – идентификатор класса поставщика, задаётся строкой до 31 символа.
13	Задать специфическую информацию поставщика (DHCP Опция 43).	**esr(config-dhcp-vendor-id)# vendor-specific-options <HEX>** **esr(config-ipv6-dhcp-vendor-id)# vendor-specific-options <HEX>**	<HEX> – специфическая информация поставщика, задаётся в шестнадцатеричном формате до 128 символов.
14	Задать IP-адрес NetBIOS-сервера (DHCP опция 44) (не обязательно).	**esr(config-dhcp-server)# netbios-name-server <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 (DHCPOption 150) (не обязательно).	**esr(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].

18.1.2 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:

```
esr# configure
esr(config)# security zone trusted
esr(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:

```
esr# configure
esr(config)# ip dhcp-server pool Simple
esr(config-dhcp-server)# network 192.168.1.0/24
esr(config-dhcp-server)# address-range 192.168.1.100-192.168.1.125
esr(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.

```
esr(config-dhcp-server)# domain-name "eltex.loc"
esr(config-dhcp-server)# default-router 192.168.1.1
esr(config-dhcp-server)# dns-server 172.16.0.1,8.8.8.8
esr(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.

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# security-zone trusted
esr(config-if-gi)# ip address 192.168.1.1/24
esr(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:

```
esr(config)# object-group service dhcp_server
esr(config-object-group-service)# port-range 67
esr(config-object-group-service)# exit
esr(config)# object-group service dhcp_client
esr(config-object-group-service)# port-range 68
esr(config-object-group-service)# exit
esr(config)# security zone-pair trusted self
esr(config-zone-pair)# rule 30
esr(config-zone-rule)# match protocol udp
esr(config-zone-rule)# match source-port dhcp_client
esr(config-zone-rule)# match destination-port dhcp_server
esr(config-zone-rule)# action permit
esr(config-zone-rule)# enable
esr(config-zone-rule)# exit
esr(config-zone-pair)# exit
```

Разрешим работу сервера:

```
esr(config)# ip dhcp-server
esr(config)# exit
```

Просмотреть список арендованных адресов можно с помощью команды:

```
esr# show ip dhcp binding
```

Просмотреть сконфигурированные пулы адресов можно командами:

```
esr# show ip dhcp server pool
esr# show ip dhcp server pool Simple
```

Конфигурирование настроек для IPv6 производится по аналогии с IPv4.

18.2 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.

18.2.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим настройки сервиса трансляции адресов получателя.	**esr(config)# nat destination**	

Шаг	Описание	Команда	Ключи
2	Создать пул IP-адресов и/или TCP/UDP-портов с определённым именем (не обязательно).	**esr(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.	**esr(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.	**esr(config-dnat-pool)# ip port <PORT>**	<PORT> – TCP/UDP-порт, принимает значения [1..65535].
5	Создать группу правил с определённым именем.	**esr(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).	**esr(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.	**esr(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.	**esr(config-dnat-ruleset)# rule <ORDER>**	<ORDER> – номер правила, принимает значения [1..10000].
9	Задать профиль IP-адресов {отправителя | получателя}, для которых должно срабатывать правило.	**esr(config-dnat-rule)# match [not] {source|destination}-address <OBJ-GROUP-NETWORK-NAME>**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа. Значение «any» указывает на любой IP-адрес отправителя.

Шаг	Описание	Команда	Ключи
10	Задать профиль сервисов (tcp/udp-портов) {отправителя | получателя}, для которых должно срабатывать правило (не обязательно).	**esr(config-dnat-rule)# match [not] {source|destination}-port <PORT-SET-NAME>**	<PORT-SET-NAME> – имя профиля порта, задаётся строкой до 31 символа. Значение «any» указывает на любой TCP/UDP-порт отправителя.
11	Установить имя или номер IP-протокола, для которого должно срабатывать правило (не обязательно).	**esr(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).	**esr(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».	**esr(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.	**esr(config-dnat-rule)# enable**	

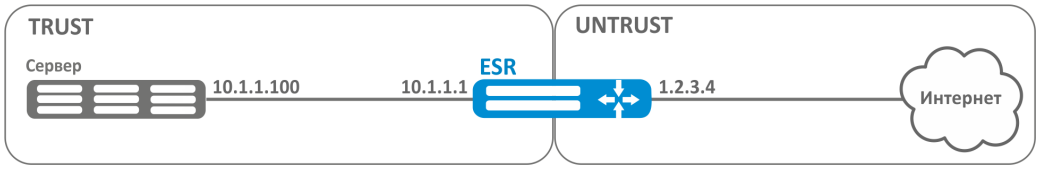
Шаг	Описание	Команда	Ключи
15	Включить функцию отслеживания сессий уровня приложений для протоколов FTP, SIP, H323, netbios-ns, PPTP (не обязательно).	**esr(config)# ip firewall sessions tracking** **{<PROTOCOL> | sip [port <OBJECT-GROUP-SERVICE>] | all}**	all – включает функцию отслеживания сессий уровня 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).	**esr(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].

⚠ [1] 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».

18.2.2 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.

```
esr# configure
esr(config)# security zone UNTRUST
esr(config-zone)# exit
esr(config)# security zone TRUST
esr(config-zone)# exit
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)#   security-zone TRUST
esr(config-if-gi)#   ip address 10.1.1.1/25
esr(config-if-gi)# exit
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip address 1.2.3.4/29
esr(config-if-te)# security-zone UNTRUST
esr(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.

```
esr(config)# object-group network NET_UPLINK
esr(config-object-group-network)# ip address 1.2.3.4
esr(config-object-group-network)# exit
```

```
esr(config)# object-group service SRV_HTTP
esr(config-object-group-service)# port 80
esr(config-object-group-service)# exit
```

```
esr(config)# object-group network SERVER_IP
esr(config-object-group-network)# ip address 10.1.1.100
esr(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.

```
esr(config)# nat destination
esr(config-dnat)# pool SERVER_POOL
esr(config-dnat-pool)# ip address 10.1.1.100
esr(config-dnat-pool)# ip port 80
esr(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».

```
esr(config-dnat)# ruleset DNAT
esr(config-dnat-ruleset)# from zone UNTRUST
esr(config-dnat-ruleset)# rule 1
esr(config-dnat-rule)# match destination-address NET_UPLINK
esr(config-dnat-rule)# match protocol tcp
esr(config-dnat-rule)# match destination-port SRV_HTTP
esr(config-dnat-rule)# action destination-nat pool SERVER_POOL
esr(config-dnat-rule)# enable
esr(config-dnat-rule)# exit
esr(config-dnat-ruleset)# exit
esr(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.

```
esr(config)# security zone-pair UNTRUST TRUST
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# match destination-address SERVER_IP
esr(config-zone-pair-rule)# match destination-nat
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# exit
```

Произведенные настройки можно посмотреть с помощью команд:

```
esr# show ip nat destination pools
esr# show ip nat destination rulesets
esr# show ip nat proxy-arp
esr# show ip nat translations
```

18.3 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.

18.3.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим настройки сервиса трансляции адресов отправителя.	**esr(config)# nat source**	
2	Создать пул IP-адресов и/или TCP/UDP-портов с определённым именем (не обязательно).	**esr(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.	**esr(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.	**esr(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.	**esr(config-snat-pool)# ip port <PORT>**	<PORT> – TCP/UDP-порт, принимает значения [1..65535].
6	Включить функции NAT persistent.	**esr(config-snat-pool)# persistent**	
7	Создать группу правил с определённым именем.	**esr(config-snat)# ruleset <NAME>**	<NAME> – имя группы правил, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
8	Указать экземпляр VRF, в котором будет работать данная группа правил (не обязательно).	**esr(config-snat-ruleset)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.
9	Задать область применения группы правил. Правила будут применяться только для трафика, идущего в определенную зону или интерфейс.	**esr(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.	**esr(config-snat-ruleset)# rule <ORDER>**	<ORDER> – номер правила, принимает значения [1..10000].
11	Задать профиль IP-адресов {отправителя | получателя}, для которых должно срабатывать правило.	**esr(config-snat-rule)# match [not] {source|destination}-address <OBJ-GROUP-NETWORK-NAME>**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа. Значение «any» указывает на любой IP-адрес отправителя.
12	Задать профиль IP-адресов {отправителя | получателя}, для которых должно срабатывать правило (не обязательно).	**esr(config-snat-rule)# match [not] {source | destination}-port <PORT-SET-NAME>**	<PORT-SET-NAME> – имя профиля порта, задаётся строкой до 31 символа. Значение «any» указывает на любой TCP/UDP-порт отправителя.
13	Установить имя или номер IP-протокола, для которого должно срабатывать правило (не обязательно).	**esr(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].

Шаг	Описание	Команда	Ключи
14	Задать тип и код сообщений протокола ICMP, для которых должно срабатывать правило (не обязательно).	**esr(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
15	Задать действие «трансляция адреса и порта отправителя» для трафика, удовлетворяющего критериям, заданным командами «match».	**esr(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.	**esr(config-snat-rule)# enable**	

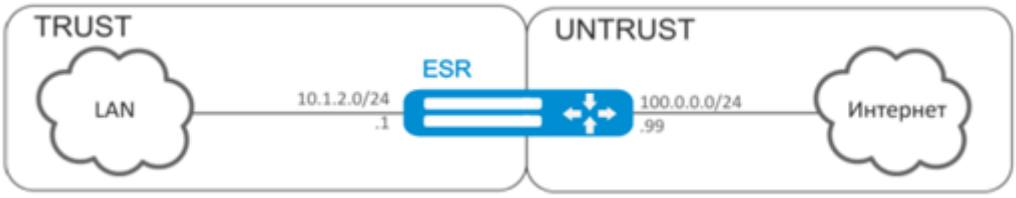
Шаг	Описание	Команда	Ключи
17	Включить функцию отслеживания сессий уровня приложений для протоколов FTP, SIP, H323, netbios-ns, PPTP (не обязательно).	**esr(config)# ip firewall sessions tracking** **{<PROTOCOL> | sip [port <OBJECT-GROUP-SERVICE>] | all}**	all – включает функцию отслеживания сессий уровня 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).	**esr(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].

[1] 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».

18.3.2 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.

```
esr# configure
esr(config)# security zone UNTRUST
esr(config-zone)# exit
esr(config)# security zone TRUST
esr(config-zone)# exit
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 10.1.2.1/24
esr(config-if-gi)# security-zone TRUST
esr(config-if-gi)# exit
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip address 100.0.0.99/24
esr(config-if-te)# security-zone UNTRUST
esr(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».

```
esr(config)# object-group network LOCAL_NET
esr(config-object-group-network)# ip address-range 10.1.2.2-10.1.2.254
esr(config-object-group-network)# exit
esr(config)# object-group network PUBLIC_POOL
esr(config-object-group-network)# ip address-range 100.0.0.100-100.0.0.249
esr(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*.

```
esr(config)# security zone-pair TRUST UNTRUST
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# match source-address LOCAL_NET
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
```

Конфигурируем сервис SNAT. Первым шагом создаётся пул адресов публичной сети, используемых для сервиса SNAT.

```
esr(config)# nat source
esr(config-snat)# pool TRANSLATE_ADDRESS
esr(config-snat-pool)# ip address-range 100.0.0.100-100.0.0.249
esr(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».

```
esr(config-snat)# ruleset SNAT
esr(config-snat-ruleset)# to zone UNTRUST
esr(config-snat-ruleset)# rule 1
esr(config-snat-rule)# match source-address LOCAL_NET
esr(config-snat-rule)# action source-nat pool TRANSLATE_ADDRESS
esr(config-snat-rule)# enable
esr(config-snat-rule)# exit
esr(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».

```
esr(config)# interface tengigabitethernet 1/0/1
esr(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.

```
esr(config)# ip route 0.0.0.0/0 100.0.0.1
esr(config)# exit
```

18.3.3 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:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 21.12.2.1/24
esr(config-if-gi)# ip firewall disable
esr(config-if-gi)# exit
```

```
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip address 200.10.0.1/24
esr(config-if-te)# ip firewall disable
esr(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»:

```
esr(config)# object-group network LOCAL_NET
esr(config-object-group-network)# ip address-range 21.12.2.2-21.12.2.254
esr(config-object-group-network)# exit

esr(config)# object-group network PUBLIC_POOL
esr(config-object-group-network)# ip address-range 200.10.0.100-200.10.0.249
esr(config-object-group-network)# exit
```

Конфигурируем сервис SNAT.

Первым шагом создаётся пул адресов публичной сети, используемых для сервиса SNAT:

```
esr(config)# nat source
esr(config-snat)# pool TRANSLATE_ADDRESS
esr(config-snat-pool)# ip address-range 200.10.0.100-200.10.0.249
esr(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»:

```
esr(config-snat)# ruleset SNAT
esr(config-snat-ruleset)# to interface te1/0/1
esr(config-snat-ruleset)# rule 1
esr(config-snat-rule)# match source-address LOCAL_NET
esr(config-snat-rule)# action source-nat pool TRANSLATE_ADDRESS
esr(config-snat-rule)# enable
esr(config-snat-rule)# exit
esr(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»:

```
esr(config)# interface tengigabitethernet 1/0/1
esr(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:

```
esr(config)# ip route 0.0.0.0/0 200.10.0.254
esr(config)# exit
```

18.4 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.

18.4.1 Алгоритм настройки

Настройка Static NAT осуществляется средствами Source NAT, алгоритм настройки которой описан в разделе Конфигурирование Source NAT, алгоритм настройки настоящего руководства.

18.4.2 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:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 21.12.2.1/24
esr(config-if-gi)# ip firewall disable
esr(config-if-gi)# exit
```

```
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip address 200.10.0.1/24
esr(config-if-te)# ip firewall disable
esr(config-if-te)# exit
```

Для конфигурирования Static NAT потребуется создать профиль адресов локальной сети «LOCAL_NET», включающий локальную подсеть, и профиль адресов публичной сети «PUBLIC_POOL»:

```
esr(config)# object-group network LOCAL_NET
esr(config-object-group-network)# ip prefix 21.12.2.0/24
esr(config-object-group-network)# exit
```

```
esr(config)# object-group network PUBLIC_POOL
esr(config-object-group-network)# ip prefix 200.10.0.0/24
esr(config-object-group-network)# exit
```

Диапазон адресов публичной сети для использования Static NAT задаем в профиле «PROXY»:

```
esr(config)# object-group network PROXY
esr(config-object-group-network)# ip address-range 200.10.0.100-200.10.0.150
esr(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» и проверку адресов назначения на принадлежность к пулу «PUBLIC_POOL».

```
esr(config)# nat source
esr(config-snat)# ruleset SNAT
esr(config-snat-ruleset)# to interface te1/0/1
esr(config-snat-ruleset)# rule 1
esr(config-snat-rule)# match source-address LOCAL_NET
esr(config-snat-rule)# action source-nat netmap 200.10.0.0/24 static
esr(config-snat-rule)# enable
esr(config-snat-rule)# exit
esr(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».

```
esr(config)# interface tengigabitethernet 1/0/1
esr(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.

```
esr# commit
Configuration has been successfully committed
esr# confirm
Configuration has been successfully confirmed
```

Посмотреть активные трансляции можно с помощью команды:

```
esr# show ip nat translations
```

18.5 Проксирование HTTP/HTTPS-трафика

18.5.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать объект с URL.	**esr(config)# object-group url <NAME>**	
2	Указать набор.	**esr(config-object-group-url)# url <URL>**	<URL> – адрес веб страницы, сайта.
3	Создать профиль проксирования.	**esr(config)# ip http profile <NAME>**	<NAME> – название профиля.
4	Выбрать действие по умолчанию.	**esr(config-profile)# default action {deny|permit|redirect} [redirect-url <URL>]**	<URL> – адрес хоста, на который будут передаваться запросы.
5	Указать описание (не обязательно).	**esr(config-profile)# description <description>**	<description> – до 255 символов.
6	Указать удаленный или локальный список URL и тип операции (блокировка/ пропуск трафика/ перенаправление) (не обязательно).	**esr(config-profile)# urls {local|remote} <URL_OBJ_GROUP_NAME> action {deny|permit|redirect} [redirect-url <URL>]**	<URL_OBJ_GROUP_NAME> – указать название объекта, содержащего набор URL.
7	Указать удаленный сервер, где лежат необходимые списки URL (не обязательно).	**esr(config)# ip http proxy server-url <URL>**	<URL> – адрес сервера, откуда будут брать удалённые списки url.
8	Указать прослушиваемый порт для проксирования (не обязательно).	**esr(config)# ip http proxy listen-ports <OBJ_GROUP_NAME>**	<OBJ_GROUP_NAME> – имя профиля порта, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
9	Указать прослушиваемый порт для проксирования (не обязательно).	**esr(config)# ip https proxy listen-ports <OBJ_GROUP_NAME>**	<OBJ_GROUP_NAME> – имя профиля порта, задаётся строкой до 31 символа.
10	Указать базовый порт для проксирования (не обязательно).	**esr(config)# ip https proxy redirect-port <PORT>**	<PORT> – номер порта, указывается в диапазоне [1..65535]. Значение по умолчанию 3128.
11	Включить проксирование на интерфейсе на основе выбранного HTTP-профиля.	**esr(config-if)# ip http proxy <PROFILE_NAME>**	<PROFILE_NAME> – название профиля.
12	Включить проксирование на интерфейсе на основе выбранного HTTPS-профиля.	**esr(config-if)# ip https proxy <PROFILE_NAME>**	<PROFILE_NAME> – название профиля.
13	Создать списки сервисов, которые будут использоваться при фильтрации.	**esr(config)# object-group service <obj-group-name>**	<obj-group-name> – имя профиля сервисов, задается строкой до 31 символа.
14	Задать описание списка сервисов (не обязательно).	**esr(config-object-group-service)# description <description>**	<description> – описание профиля, задается строкой до 255 символов.
15	Внести необходимые сервисы (tcp/udp-порты) в список.	**esr(config-object-group-service)# port-range 3128-3135**	Прокси-сервер ESR использует для своей работы порты начиная с базового порта определённого на 10 шаге. Для http proxy используются порты начиная с базового порта по базовый порт + количество cpu данной модели ESR - 1. Для https proxy используются порты начиная с базового порта + количество cpu данной модели ESR по базовый порт + количество cpu данной модели ESR * 2 - 1.

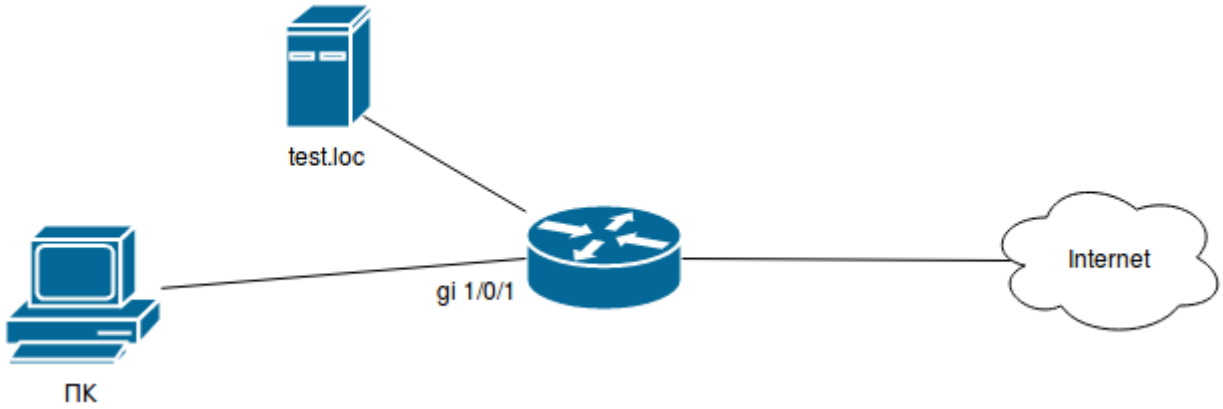
Шаг	Описание	Команда	Ключи
16	Создать набор правил межзонового взаимодействия.	**esr(config)# security zone-pair <src-zone-name1> self**	<src-zone-name> – зона безопасности, в которой находятся интерфейсы с функцией ip http proxy или ip https proxy. self – предопределенная зона безопасности для трафика, поступающего на сам ESR.
17	Создать правило межзонового взаимодействия.	**esr(config-zone-pair)# rule <rule-number>**	<rule-number> – 1..10000.
18	Задать описание правила (не обязательно).	**esr(config-zone-rule)# description <description>**	<description> – до 255 символов.
19	Указать действие данного правила.	**esr(config-zone-rule)# action <action> [log]**	<action> – permit. log – ключ для активации логирования сессий, которые устанавливаются согласно данному правилу.
20	Установить имя IP-протокола, для которого должно срабатывать правило	**esr(config-zone-rule)# match protocol <protocol-type>**	<protocol-type> – tcp. Прокси-сервер ESR работает по протоколу ESR.
21	Установить профиль TCP/UDP-портов получателя, для которых должно срабатывать правило (если указан протокол).	**esr(config-zone-rule)# match [not] destination-port <obj-group-name>**	<obj-group-name> – имя профиля сервисов, созданного на шаге 12.
22	Включить правило межзонового взаимодействия.	**esr(config-zone-rule)# enable**	

Если функция Firewall на ESR принудительно не отключена, необходимо создать разрешающее правило для зоны Self.

18.5.2 Пример настройки HTTP-прокси

Задача:

Организовать фильтрацию по URL для ряда адресов посредством прокси.



Решение:

Создадим набор URL, по которым будет осуществляться фильтрация. Настроим прокси-фильтр и укажем действия для созданного набора URL:

```
esr# configure
esr(config)# object-group url test1
esr(config-object-group-url)# url http://speedtest.net/
esr(config-object-group-url)# url http://www.speedtest.net/
esr(config-object-group-url)# url https://speedtest.net/
esr(config-object-group-url)# url https://www.speedtest.net/
esr(config-object-group-url)# exit
```

Создаем профиль:

```
esr(config)# ip http profile list1
esr(config-profile)# default action permit
esr(config-profile)# urls local test1 action redirect redirect-url http://test.loc
esr(config-profile)# exit
```

Включим проксирование на интерфейсе по профилю ‘list1’:

```
esr(config)# interface gi 1/0/1
esr(config-if)# ip http proxy list1
esr(config-if)# ip https proxy list1
```

Если используется Firewall, создадим для него разрешающие правила:

Допустим мы используем модель ESR-20 у которой 4 CPU.

Для http proxy нам надо открыть порты с 3128 по 3131

Для https proxy нам надо открыть порты с 3132 по 3135

Создаем профиль портов Прокси-сервера:

```
esr(config)# object-group service proxy
esr(config-object-group-service)# port-range 3128-3135
esr(config-object-group-service)# exit
```

Создаем разрешающее правило межзонового взаимодействия:

```
esr(config)# security zone-pair LAN self
esr(config-zone-pair)# rule 50
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol tcp
esr(config-zone-pair-rule)# match destination-port proxy
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
```

18.6 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.

18.6.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Включить NTP.	**esr(config)# ntp enable**	
2	Задать IP-адрес NTP-сервера, либо участника NTP-синхронизации.	**esr(config)# ntp { server | peer } { <IP> }**	<IP> – IP-адрес назначения (шлюз), задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
3	Задать ключ для аутентификации (не обязательно).	**esr(config-ntp)# key <ID>**	<ID> – идентификатор ключа, задается в диапазоне [1..255].
4	Установить максимальное значение интервала времени между отправкой сообщений NTP-серверу (не обязательно).	**esr(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).

Шаг	Описание	Команда	Ключи
5	Установить минимальное значение интервала времени между отправкой сообщений NTP-серверу (не обязательно).	**esr(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).
6	Отметить данный NTP-сервер как предпочтительный (не обязательно).	**esr(config-ntp)# prefer**	
7	Определить список доверенных IP-адресов, с которыми может происходить обмен ntp-пакетами (не обязательно).	**esr(config)# ntp access-addresses <NAME>**	<NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.
8	Указать идентификатор ключа из профиля связки ключей (не обязательно).	**esr(config)# ntp authentication trusted-key <ID>**	<ID> – идентификатор ключа из профиля связки ключей.
9	Указать имя профиля связки ключей (не обязательно).	**esr(config)# ntp authentication key-chain <WORD>**	<WORD> – имя профиля связки ключей.
10	Активировать аутентификацию для NTP по ключу (не обязательно).	**esr(config)# ntp authentication enable**	
11	Включить режим приёма широковещательных сообщений NTP-серверов для глобальной конфигурации и всех существующих VRF (не обязательно).	**esr(config)# ntp broadcast-client enable**	
12	Задать значение кода DSCP для использования в IP-заголовке исходящих пакетов NTP-сервера (не обязательно).	**esr(config)# ntp dscp <DSCP>**	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63] Значение по умолчанию: 46.
13	Включить режим query-only, ограничивающий взаимодействие по NTP для определенного профиля IP-адресов (не обязательно).	**esr(config)# ntp object-group query-only <NAME>**	<NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
14	Включить режим serve-only, ограничивающий взаимодействие по NTP для определенного профиля IP-адресов (не обязательно).	**esr(config)# ntp object-group serve-only <NAME>**	<NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.
15	Указать source-IP-адреса для NTP-пакетов для всех peer (не обязательно).	**esr(config)# ntp source address <ADDR>**	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
16	Задать текущие время и дату в ручном режиме (не обязательно).	**esr# 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].

18.6.2 Пример настройки

Задача:

Настроить синхронизацию времени от NTP-сервера.

IP-адрес маршрутизатора ESR – 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 NTP
    enable
  exit
exit
```

Основной этап конфигурирования:

Включение синхронизации системных часов с удаленными серверами:

```
esr(config)# ntp enable
```

Настройка NTP-сервера:

```
esr-(config)# ntp server 192.168.52.41
```

Указать предпочтительность данного NTP-сервера (необязательно):

```
esr-1000(config-ntp)# prefer
```

Указать интервал времени между отправкой сообщений NTP-серверу:

```
esr(config-ntp)# minpoll 4
esr(config-ntp)# end
esr# commit
esr# confirm
```

Команда для просмотра текущей конфигурации протокола NTP:

```
esr# show ntp configuration
```

Команда для просмотра текущего состояние NTP-серверов (пиров):

```
esr# show ntp peers
```

19 Мониторинг

- Настройка Netflow
  - Алгоритм настройки
  - Пример настройки
- Настройка sFlow
  - Алгоритм настройки
  - Пример настройки
- Настройка SNMP
  - Алгоритм настройки
  - Пример настройки
- Настройка Zabbix-agent/proxy
  - Алгоритм настройки
  - Пример настройки zabbix-agent
  - Пример настройки zabbix-server
- Настройка Syslog
  - Алгоритм настройки
  - Пример настройки
- Проверка целостности
  - Процесс настройки
  - Пример конфигурации
- Настройка архивации конфигурации маршрутизатора
  - Процесс настройки
  - Пример конфигурации

19.1 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.

> ⓘ **В текущей реализации трафик, отброшенный маршрутизатором по каким-либо причинам, не будет учитываться в статистике.**

19.1.1 Алгоритм настройки

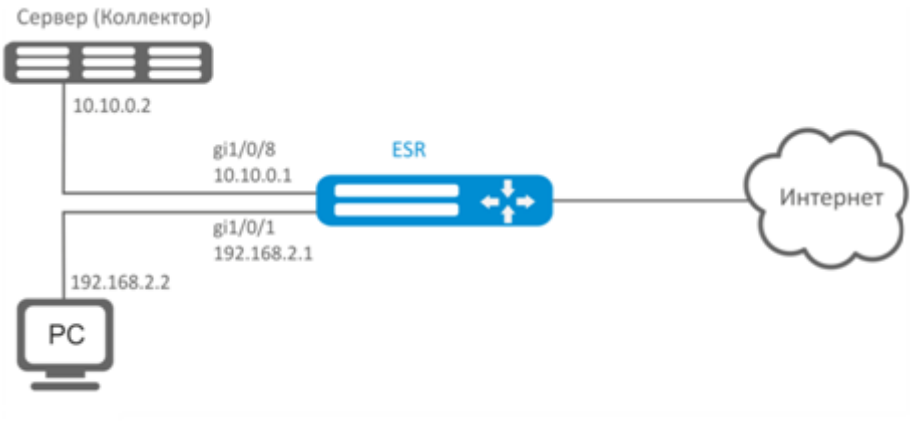
Шаг	Описание	Команда	Ключи
1	Задать версию Netflow-протокола.	**esr(config)# netflow version <VERSION>**	<VERSION> – версия Netflow-протокола: 5, 9 и 10.
2	Установить максимальное количество наблюдаемых сессий.	**esr(config)# netflow max-flows <COUNT>**	<COUNT> – количество наблюдаемых сессий, принимает значение [10000..2000000]. Значение по умолчанию: 512000.

Шаг	Описание	Команда	Ключи
3	Установить интервал, по истечении которого информация об активных сессиях экспортируются на коллектор.	**esr(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.	**esr(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.	**esr(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.	**esr(config)# netflow enable**	
7	Создать коллектор Netflow и перейти в режим его конфигурирования.	**esr(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.	**esr(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.	**esr(config-if-gi)# ip netflow export**	

19.1.2 Пример настройки

Задача:

Организовать учет трафика с интерфейса gi1/0/1 для передачи на сервер через интерфейс gi1/0/8 для обработки.



Решение:

Предварительно необходимо настроить адресацию на интерфейсах.

Основной этап конфигурирования:

Укажем IP-адрес коллектора:

```
esr(config)# netflow collector 10.10.0.2
```

Включим сбор экспорта статистики netflow на сетевом интерфейсе gi1/0/1:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip netflow export
```

Активируем netflow на маршрутизаторе:

```
esr(config)# netflow enable
```

Для просмотра статистики Netflow используется команда:

```
esr# show netflow statistics
```

Настройка Netflow для учета трафика между зонами аналогична настройке sFlow, описание приведено в разделе Настройка sFlow.

19.2 Настройка sFlow

Sflow — стандарт для мониторинга компьютерных сетей, беспроводных сетей и сетевых устройств, предназначенный для учета и анализа трафика.

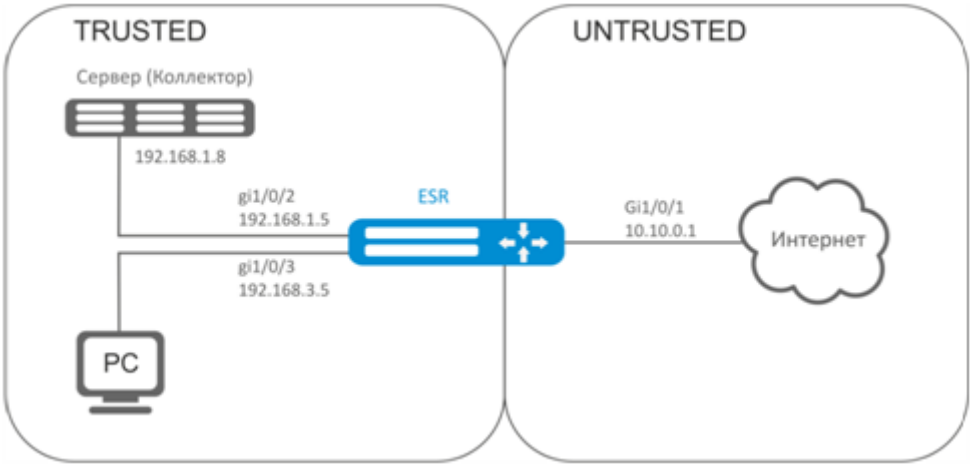
19.2.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Установить частоту отправки пакетов пользовательского трафика в неизменном виде на sFlow-коллектор.	**esr(config)# sflow sampling-rate <RATE>**	<RATE> – частота отправки пакетов пользовательского трафика на коллектор, принимает значение [1..10000000]. При значении частоты 10 на коллектор будет отправлен один пакет из десяти. Значение по умолчанию: 1000.
2	Установить интервал, по истечении которого происходит получение информации о счетчиках сетевого интерфейса.	**esr(config)# sflow poll-interval <TIMEOUT>**	<TIMEOUT> – интервал, по истечении которого происходит получение информации о счетчиках сетевого интерфейса, принимает значение [1..10000]. Значение по умолчанию: 10 секунд.
3	Активировать sFlow на маршрутизаторе.	**esr(config)# sflow enable**	
4	Создать коллектор sFlow и перейти в режим его конфигурирования.	**esr(config)# sflow collector <ADDR>**	<ADDR> – IP-адрес коллектора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
5	Включить отправку статистики на sFlow-сервер в режиме конфигурирования интерфейса/туннеля/сетевого моста.	**esr(config-if-gi)# ip sflow export**	

19.2.2 Пример настройки

Задача:

Организовать учет трафика между зонами trusted и untrusted.



Решение:

Для сетей ESR создадим две зоны безопасности:

```
esr# configure
esr(config)# security zone TRUSTED
esr(config-zone)# exit
esr(config)# security zone UNTRUSTED
esr(config-zone)# exit
```

Настроим сетевые интерфейсы и определим их принадлежность к зонам безопасности:

```
esr(config)# interface gi1/0/1
esr(config-if-gi)# security-zone UNTRUSTED
esr(config-if-gi)# ip address 10.10.0.1/24
esr(config-if-gi)# exit
esr(config)# interface gi1/0/2-3
esr(config-if-gi)# security-zone TRUSTED
esr(config-if-gi)# exit
esr(config)# interface gi1/0/2
esr(config-if-gi)# ip address 192.168.1.5/24
esr(config-if-gi)# exit
esr(config)# interface gi1/0/3
esr(config-if-gi)# ip address 192.168.3.5/24
esr(config-if-gi)# exit
```

Укажем IP-адрес коллектора:

```
esr(config)# sflow collector 192.168.1.8
```

Включим экспорт статистики по протоколу sFlow для любого трафика в правиле «rule1» для направления TRUSTED-UNTRUSTED:

```
esr(config)# security zone-pair TRUSTED UNTRUSTED
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action sflow-sample
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
```

Активируем sFlow на маршрутизаторе:

```
esr(config)# sflow enable
```

Настройка sFlow для учета трафика с интерфейса осуществляется аналогично настройке Netflow.

19.3 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.

19.3.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Включить SNMP-сервер.	**esr(config)# snmp-server**	

Шаг	Описание	Команда	Ключи
2	Определить community для доступа по протоколу SNMPv2c.	**esr(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::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.
3	Устанавливает значение переменной SNMP, содержащей контактную информацию.	**esr(config)# snmp-server contact <CONTACT>**	<CONTACT> – контактная информация, задается строкой до 255 символов.

Шаг	Описание	Команда	Ключи
4	Установить значение кода DSCP для использования в IP-заголовке исходящих пакетов SNMP-сервера (не обязательно).	**esr(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)	**esr(config)# snmp-server system-shutdown**	
6	Создать SNMPv3-пользователь.	**esr(config)# snmp-server user <NAME>**	<NAME> – имя пользователя, задаётся строкой до 31 символа.
7	Устанавливает значение переменной SNMP, содержащей информацию о расположении оборудования	**esr(config)# snmp-server location <LOCATION>**	<LOCATION> – информация о расположении оборудования, задается строкой до 255 символов.
8	Определить уровень доступа пользователя по протоколу SNMPv3.	**esr(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.	**esr(config-snmp-user)# authentication access <TYPE>**	<TYPE> – режим безопасности: • **auth** – используется только аутентификация; • **priv** – используется аутентификация и шифрование данных.
10	Определить алгоритм аутентификации SNMPv3-запросов.	**esr(config-snmp-user)# authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм шифрования: • **md 5** – пароль шифруется по алгоритму md5; • **sha 1** – пароль шифруется по алгоритму sha1.

Шаг	Описание	Команда	Ключи
11	Установить пароль для аутентификации SNMPv3-запросов.	**esr(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.	**esr(config-snmp-user)# client-list <NAME>**	<NAME> – имя ранее сознанной object-group, задается строкой до 31 символа.
13	Указать vrf для SNMPv3-пользователя (не обязательно).	**esr-21(config-snmp-user)# ip vrf forwarding <VRF>**	<VRF> – имя экземпляра VRF, из которого будет разрешен доступ, задается строкой до 31 символа.
14	Активировать фильтрацию и установить IPv4/IPv6-адрес, которому предоставлен доступ к маршрутизатору под данным SNMPv3-пользователем.	**esr(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].
		esr(config-snmp-user)# ipv6 address <ADDR>	<IPV6-ADDR> – IPv6-адрес клиента, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
15	Активировать SNMPv3-пользователя.	**esr(config-snmp-user)# enable**	Значение по умолчанию: процесс выключен.

Шаг	Описание	Команда	Ключи
16	Определить алгоритм шифрования передаваемых данных.	**esr(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.	**esr(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.	**esr(config-snmp-user)# view <VIEW-NAME>**	<VIEW-NAME> – имя SNMP view профиля, на основании которого обеспечивается доступ к OID, задается строкой до 31 символа.
19	Включить передачу SNMP-уведомлений на указанный IP-адрес и перейти в режим настройки SNMP-уведомлений.	**esr(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::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).	**esr(config-snmp-host)# port <PORT>**	<PORT> – номер UDP-порта, указывается в диапазоне [1..65535]. Значение по умолчанию: 162.

Шаг	Описание	Команда	Ключи
21	Разрешить отправку SNMP-уведомлений различных типов.	**esr(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. WLC-30, ESR-15. Справочник команд CLI.
22	Создать профиль snmp view, позволяющий разрешать или запрещать доступ к тем или иным OID для community (SNMPv2) и user (SNMPv3).	**esr(config)# snmp-server enable traps <TYPE>**	<VIEW-NAME> – имя профиля SNMP view, задаётся строкой до 31 символа.

19.3.2 Пример настройки

Задача:

Настроить SNMPv3-сервер с аутентификацией и шифрованием данных для пользователя admin. IP-адрес маршрутизатора ESR – 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:

```
esr(config)# snmp-server
```

Создаем пользователя SNMPv3:

```
esr(config)# snmp-server user admin
```

Определим режим безопасности:

```
esr(snmp-user)# authentication access priv
```

Определим алгоритм аутентификации для SNMPv3-запросов:

```
esr(snmp-user)# authentication algorithm md5
```

Установим пароль для аутентификации SNMPv3-запросов:

```
esr(snmp-user)# authentication key ascii-text 123456789
```

Определим алгоритм шифрования передаваемых данных:

```
esr(snmp-user)# privacy algorithm aes128
```

Установим пароль для шифрования передаваемых данных:

```
esr(snmp-user)# privacy key ascii-text 123456789
```

Активируем SNMPv3-пользователя:

```
esr(snmp-user)# enable
```

Определяем сервер-приемник Trap-PDU-сообщений:

```
esr(config)# snmp-server host 192.168.52.41
```

19.4 Настройка Zabbix-agent/proxy

Zabbix-agent — агент, предназначенный для мониторинга устройства, а также выполнения удаленных команд с Zabbix-сервера. Агент может работать в двух режимах: пассивный и активный. Для работы в пассивном режиме, по умолчанию, необходимо разрешающее правило в firewall — протокол tcp, порт 10050. Для активного режима – протокол tcp, порт 10051.

Zabbix-прокси — это процесс, способный собирать данные мониторинга с одного или нескольких наблюдаемых устройств и отправлять эту информацию Zabbix-серверу.

19.4.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перейти в контекст настройки агента/ proxy.	**esr(config)# zabbix-agent** **esr(config)# zabbix-proxy**	
2	Указать имя узла сети (опционально). Для активного режима имя должно совпадать с именем узла сети на Zabbix-сервере.	**esr(config-zabbix)# hostname <WORD>** **esr(config-zabbix-proxy)# hostname <WORD>**	<WORD> – имя узла сети, задается строкой до 255 символов.
3	Указать адрес Zabbix-сервера.	**esr(config-zabbix)# server <ADDR>** **esr(config-zabbix-proxy)# server <ADDR>**	<ADDR> – IP-адрес сервера, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
4	Указать адрес сервера для активных проверок (при использовании активного режима).	**esr(config-zabbix)# active-server <ADDR> <PORT>** **esr(config-zabbix-proxy)# active-server <ADDR> <PORT>**	<ADDR> – IP-адрес сервера, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. <PORT> – порт сервера, задается в диапазоне [1..65535]. Значение по умолчанию 10051.
5	Указать порт, который будет слушать агент/прокси (не обязательно).	**esr(config-zabbix)# port <PORT>** **esr(config-zabbix-proxy)# port <PORT>**	<PORT> – порт, который слушает zabbix-агент/прокси, задается в диапазоне [1..65535]. Значение по умолчанию: 10050.
6	Разрешить выполнение удаленных команд zabbix-агентом/прокси (при использовании активного режима).	**esr(config-zabbix)# remote-commands** **esr(config-zabbix-proxy)# remote-commands**	

Шаг	Описание	Команда	Ключи
7	Указать адрес, с которого будет осуществляться взаимодействием с сервером (не обязательно).	**esr(config-zabbix)# source-address <ADDR>** **esr(config-zabbix-proxy)# source-address <ADDR>**	<ADDR> – IP-адрес сервера, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Значение по умолчанию: ближайший адрес по маршрутизации.
8	Указать время обработки удаленных команд (не обязательно).	**esr(config-zabbix)# timeout <TIME>** **esr(config-zabbix-proxy)# timeout <TIME>**	<TIME> – время ожидания, определяется в секундах [1..30]. Значение по умолчанию 3. Рекомендуется устанавливать максимальное значение, т.к. некоторые команды могут выполняться дольше значения по умолчанию. Если за указанное время команда не будет выполнена, то обработка команды будет прекращена.
9	Включить функционал агента/прокси.	**esr(config-zabbix)# enable** **esr(config-zabbix-proxy)# enable**	
10	Разрешить из соответствующей зоны безопасности firewall обращение к маршрутизатору (в зону self) по TCP портам 10050, 10051. См. раздел Конфигурирование Firewall.		

19.4.2 Пример настройки zabbix-agent

Задача:

Настроить взаимодействие между агентом и сервером для выполнения удаленных команд с сервера.

Решение:

В контексте настройки агента укажем адрес Zabbix-сервера и адрес, с которого будет осуществляться взаимодействие с сервером:

```
esr(config-zabbix)# server 192.168.32.101
esr(config-zabbix)# source-address 192.168.39.170
```

Для активации активного режима укажем hostname, active-server, а также включим выполнение удаленных команд:

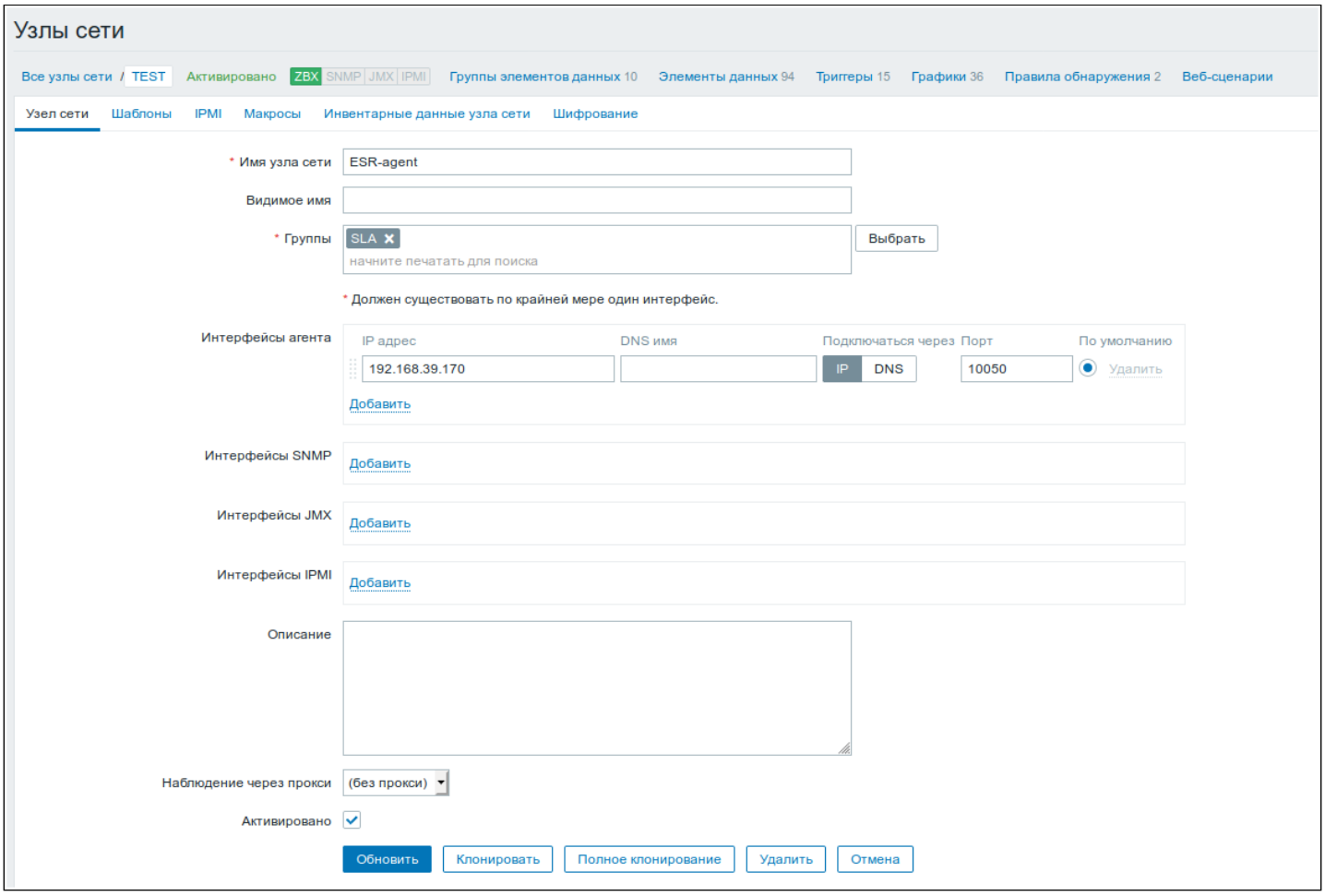
```
esr(config-zabbix)# hostname ESR-agent
esr(config-zabbix)# active-server 192.168.32.101
esr(config-zabbix)# remote-commands
```

Зададим время выполнения удаленных команд и активируем функционал агента:

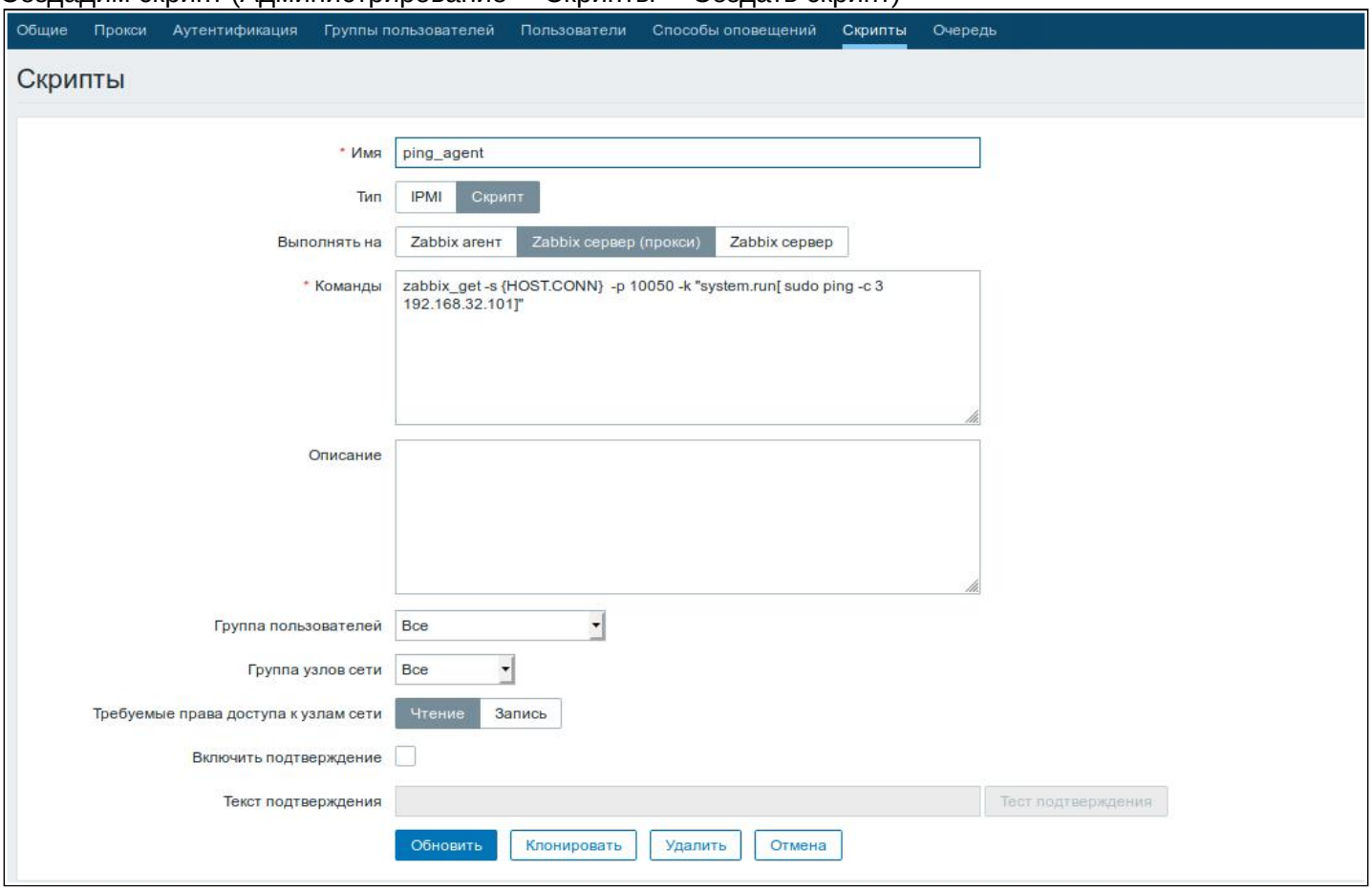
```
esr(config-zabbix)# timeout 30
esr(config-zabbix)# enable
```

19.4.3 Пример настройки zabbix-server

Создадим узел сети:



Создадим скрипт (Администрирование -> Скрипты -> Создать скрипт)



Маршрутизаторы ESR поддерживают выполнение следующих привилегированных команд:

- **Ping:**

```
zabbix_get -s {HOST.CONN}  -p 10050 -k "system.run[ sudo ping -c 3 192.168.32.101]"
```

Клиент (ESR), получивший данную команду от сервера, выполнит ping до заданного узла (в нашем примере до 192.168.32.101), и вернет результат серверу.

⚠ Использование ключа "-c" с указанием количества пакетов в тесте — обязательно. Без данного ключа команда ping не остановится самостоятельно и тест не будет считаться завершенным.

- **Ping в VRF:**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[sudo  netns -exec -n backup sudo ping
192.168.32.101 -c 5 -W 2 ]"
```

Вышеупомянутая команда будет выполнена в заданном VRF с именем backup.

- **Fping**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[ sudo fping 192.168.32.101]"
```

Клиент (ESR), получивший данную команду от сервера, выполнит fping до заданного узла (в нашем примере до 192.168.32.101), и вернет результат серверу.

- **Fping в VRF**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[sudo  netns-exec -n backup sudo fping
192.168.32.101 ]"
```

- **Traceroute**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[ sudo traceroute 192.168.32.101]
```

Клиент (ESR), получивший данную команду от сервера, выполнит traceroute до заданного узла (в нашем примере до 192.168.32.101), и вернет результат серверу.

- **Traceroute в VRF**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[ sudo  netns-exec -n backup sudo
traceroute 192.168.32.179]"
```

- **Iperf**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[ sudo iperf -c 192.168.32.101 -u -b 100K
-i 1 -t 600]"
```

Клиент (ESR), получивший данную команду от сервера, выполнит iperf до заданного сервера (в нашем примере до 192.168.32.101), и вернет результат серверу.

- **Iperf в VRF**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[ sudo  netns-exec -n backup  sudo iperf
-c 192.168.32.101 -u -b 100K -i 1 -t 600]"
```

- **Nslookup**

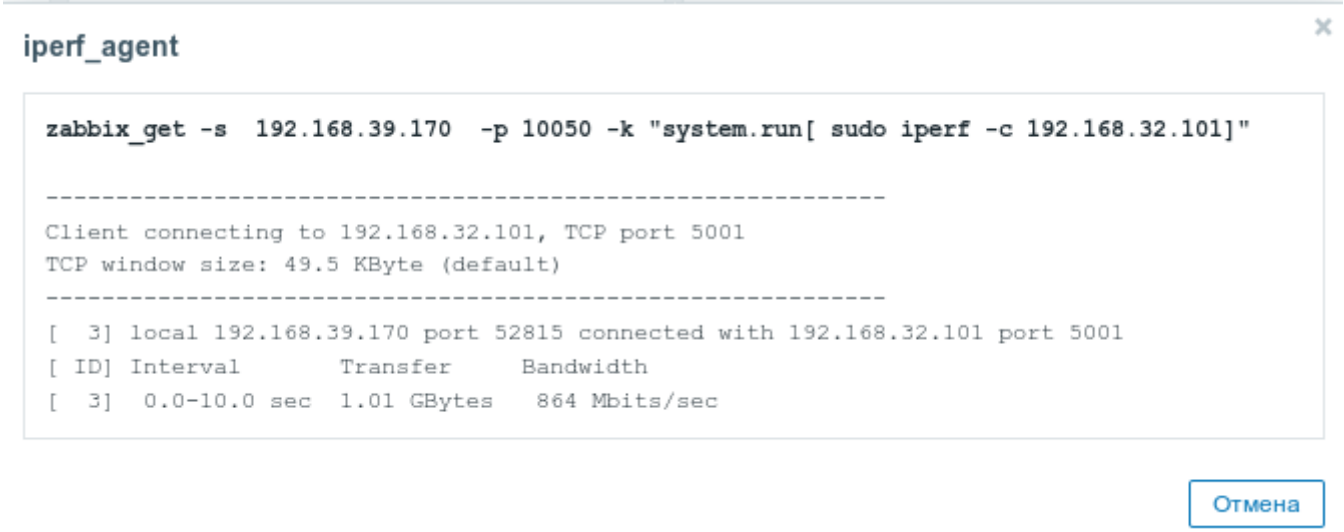
```
zabbix_get -s  {HOST.CONN} -p 10050 -k "system.run[sudo  nslookup ya.ru ]"
```

Клиент (ESR), получивший данную команду от сервера, выполнит nslookup , и вернет результат серверу.

- **Nslookup в VRF**

```
zabbix_get -s  {HOST.CONN} -p 10050 -k "system.run[sudo  netns-exec  sudo   nslookup
ya.ru ]"
```

Пример выполнения команды Iperf:



Кроме того, возможно выполнение команд, не требующих привилегий, таких как: snmpget, cat, pwd, wget и др.

Пример выполнения команды snmpget:

19.5 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.

19.5.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Включить отправку syslog-сообщений на snmp-сервер в виде snmp-trap.	**esr(config)# syslog snmp**	
2	Активировать или деактивировать отправку на snmp-сервер событий работы отдельных процессов маршрутизатора (не обязательно).	**esr(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.

Шаг	Описание	Команда	Ключи
3	Указать уровень важности сообщений, которые будут отправляться на snmp-сервер.	**esr(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.
4	Включить отображение syslog-сообщений при удаленных подключениях (Telnet, SSH) (не обязательно).	**esr(config)# syslog monitor**	
5	Активировать или деактивировать отображение при удаленных подключениях событий работы отдельных процессов маршрутизатора (не обязательно).	**esr(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.	**esr(config-syslog-monitor)# severity <SEVERITY>**	<SEVERITY> – описано в 3 пункте.
7	Включить отображение syslog-сообщений при консольном подключении (не обязательно).	**esr(config)# syslog console**	

Шаг	Описание	Команда	Ключи
8	Активировать или деактивировать отображение при консольном подключении событий работы отдельных процессов маршрутизатора (не обязательно).	**esr(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.	**esr(config-syslog-console)# severity <SEVERITY>**	<SEVERITY> – описано в 3 пункте.
10	Включить сохранение сообщений syslog в указанный файл журнала (при необходимости ведения локального syslog-файла).	**esr(config)# syslog file <NAME>**	<NAME> – имя файла, в который будет производиться запись сообщений заданного уровня, задается строкой до 31 символа;
11	Активировать или деактивировать сохранение в локальный syslog-файл событий работы отдельных процессов маршрутизатора (не обязательно).	**esr(config-syslog-file)# match [not] process-name <PROCESS-NAME>**	<PROCESS-NAME> – описано во 2 пункте.
12	Указать уровень важности сообщений, которые будут сохраняться в локальный syslog-файл.	**esr(config-syslog-file)# severity <SEVERITY>**	<SEVERITY> – описано в 3 пункте.
13	Указать максимальный размер файла журнала (не обязательно).	**esr(config)# syslog file-size <SIZE>**	<SIZE> – размер файла, принимает значение [10..10000000] Кбайт.
14	Задать максимальное количество файлов, сохраняемых при ротации (не обязательно).	**esr(config)# syslog max-files <NUM>**	<NUM> – максимальное количество файлов, принимает значения [1.. 1000].

Шаг	Описание	Команда	Ключи
15	Включить передачу сообщений syslog на удаленный syslog-сервер (при необходимости отправки сообщений на удаленный syslog-сервер).	**esr(config)#syslog host <HOSTNAME> <ADDR> <TRANSPORT>**	<HOSTNAME> – наименование syslog-сервера, задаётся строкой до 31 символа. Используется только для идентификации сервера при конфигурировании. Значение «all» используется в команде no syslog host для удаления всех syslog-серверов; <ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <TRANSPORT> – протокол передачи данных, опциональный параметр, принимает значения: • **TCP** – передача данных осуществляется по протоколу TCP; • **UDP** – передача данных осуществляется по протоколу UDP.
16	Указать IPv4/IPv6-адрес удаленного syslog-сервера.	**esr(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::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
17	Указать IPv4/IPv6-адрес маршрутизатора, от которого будут отправляться пакеты на удаленный syslog-сервер (не обязательно).	**esr(config-syslog-host)# source-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::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; Значение по умолчанию: IPv4/ IPv6-адрес интерфейса, с которого отправляется пакеты на удаленный syslog-сервер.

Шаг	Описание	Команда	Ключи
18	Указать транспортный протокол для передачи пакетов на удаленный syslog-сервер (не обязательно).	**esr(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).
19	Указать имя экземпляра VRF, в рамках которого будут отправляться пакеты на удаленный syslog-сервер (не обязательно).	**esr(config-syslog-host)# vrf <VRF>**	
20	Указать номер TCP/UDP-порта, на который будут отправляться пакеты с syslog-сообщениями (не обязательно).	**esr(config-syslog-host)# port <PORT>**	<PORT> – номер TCP/UDP-порта, на который будут отправляться пакеты с syslog-сообщениями. Значение по умолчанию: 514.
21	Активировать или деактивировать отправку на удаленный syslog-сервер событий работы отдельных процессов маршрутизатора (не обязательно).	**esr(config-syslog-host)# match [not] process-name <PROCESS-NAME>**	<PROCESS-NAME> – описано во 2 пункте.
22	Указать уровень важности сообщений, которые будут сохраняться в локальный syslog-файл.	**esr(config-syslog-host)# severity <SEVERITY>**	<SEVERITY> – описано в 3 пункте.
23	Включить вывод отладочных сообщений во время загрузки устройства (не обязательно).	**esr(config)#syslog reload debugging**	
24	Включить процесс логирования введенных команд пользователя на локальный syslog-сервер (не обязательно).	**esr(config)# syslog cli-commands**	
25	Включить нумерацию сообщений (не обязательно).	**esr(config)#syslog sequence-numbers**	
26	Включить точность даты сообщений до миллисекунд (не обязательно).	**esr(config)#syslog timestamp msec**	
27	Включить регистрацию неудачных аутентификаций (не обязательно).	**esr(config)#logging login on-failure**	

Шаг	Описание	Команда	Ключи
28	Включить регистрацию изменений настроек системы аудита (не обязательно).	**esr(config)#logging syslog configuration**	
29	Включить регистрацию изменений настроек пользователя (не обязательно).	**esr(config)#logging userinfo**	

19.5.2 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 ESR – 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:

```
esr(config)# syslog file ESR info
```

Указываем IP адрес и параметры удаленного syslog-сервера:

```
esr(config)# syslog host SERVER 192.168.17.30 info udp 514
```

Задаем логирование неудачных попыток аутентификации:

```
esr(config)# logging login on-failure
```

Задаем логирование изменений конфигурации syslog:

```
esr(config)# logging syslog configuration
```

Задаем логирование старта/остановки системных процессов:

```
esr(config)# logging service start-stop
```

Задаем логирование внесений изменений в профиль пользователей:

```
esr(config)# logging userinfo
```

Изменения конфигурации вступят в действие после применения:

```
esr# commit
Configuration has been successfully committed
esr# confirm
Configuration has been successfully confirmed
```

Посмотреть текущую конфигурацию системного журнала:

```
esr# show syslog configuration
```

Посмотреть записи системного журнала:

```
esr# show syslog ESR
```

19.6 Проверка целостности

Проверка целостности подразумевает проверку целостности хранимых исполняемых файлов.

19.6.1 Процесс настройки

Шаг	Описание	Команда	Ключи
1	Запустить проверку целостности системы	**esr# verify filesystem <detailed>**	**detailed** – детальный вывод информации в консоль.

19.6.2 Пример конфигурации

Задача:

Проверить целостность файловой системы:

Решение:

Запускаем проверку целостности:

```
esr# verify filesystem
Filesystem Successfully Verified
```

19.7 Настройка архивации конфигурации маршрутизатора

На маршрутизаторах ESR предусмотрена функция локального и/или удаленного копирования конфигурации по таймеру или при применении конфигурации.

19.7.1 Процесс настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим настройки параметров резервирования конфигурации.	**esr(config)# archive**	
2	Установить тип сохранения резервных конфигураций маршрутизатора (не обязательно).	**esr(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).	**esr(config-ahchive)# auto**	
4	Включить режим резервирования конфигурации после каждого успешного применения конфигурации (не обязательно).	**esr(config-ahchive)# by-commit**	
5	Указать путь для удаленного копирования конфигураций маршрутизатора (обязательно для типов remote и both).	**esr(config-ahchive)# path <PATH>**	<PATH> – определяет протокол, адрес сервера, расположение и префикс имени файла на сервере.

Шаг	Описание	Команда	Ключи
6	Задать период времени для автоматического резервирования конфигурации (не обязательно, актуально только для режима auto).	**esr(config-ahchive)# time-period <TIME>**	<TIME> – периодичность автоматического резервирования конфигурации, принимает значение в минутах [1..35791394]. Значение по умолчанию: 720 минут.
7	Задать максимальное количество локально сохраняемых резервных копий конфигураций (не обязательно, актуально при типах local и both).	**esr(config-ahchive)# count-backup <NUM>**	<NUM> – максимальное количество локально сохраняемых резервных копий конфигураций. Принимает значения в диапазоне [1..100]. Значение по умолчанию: 1.

19.7.2 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 esr-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:

```
esr# configure
esr(config)# archive
```

Задать режим локального и удаленного резервного копирования конфигурации:

```
esr(config)# type both
```

Настроить путь для удаленного копирования конфигураций и максимальное количество локальных резервных копий:

```
esr(config-archive)# path tftp://172.16.252.77:/esr-example/esr-example.cfg
esr(config-archive)# count-backup 30
```

Задать интервал резервного копирования конфигурации в случае отсутствия изменений:

```
esr(config-archive)# time-period 1440
```

Включить режимы архивации конфигурации маршрутизатора по таймеру и при успешном изменении конфигурации:

```
esr(config-archive)# auto
esr(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 "esr-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.

20 Управление BRAS (Broadband Remote Access Server)

- Алгоритм настройки
- Пример настройки с SoftWLC
- Пример настройки без SoftWLC

Активируется лицензией BRAS.

20.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Добавить RADIUS-сервер в список используемых серверов и перейти в режим его конфигурирования.	**esr(config)# radius-server host { <IP-ADDR> | <IPV6-ADDR> } [vrf <VRF>]** **esr(config-radius-server)#**	<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::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF] <VRF> – имя экземпляра VRF, задается строкой до 31 символа.
2	Задать пароль для аутентификации на удаленном RADIUS-сервере.	**esr(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.
3	Создать профиль AAA.	**esr(config)# aaa radius-profile <NAME>**	<NAME> – имя профиля сервера, задается строкой до 31 символа.
4	В профиле AAA указать RADIUS-сервер.	**esr(config-aaa-radius-profile)# radius-server host { <IP-ADDR> | <IPV6-ADDR> }**	<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::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Шаг	Описание	Команда	Ключи
5	Создать DAS-сервер.	**esr(config)# das-server <NAME>**	<NAME> – имя DAS-сервера, задается строкой до 31 символа.
6	Задать пароль для аутентификации на удаленном DAS-сервере.	**esr(config-das-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.
7	Создать AAA DAS-профиль.	**esr(config)# aaa das-profile <NAME>**	<NAME> – имя DAS-профиля, задается строкой до 31 символа.
8	Указать DAS-сервер в DAS-профиле.	**esr(config-aaa-das-profile)# das-server <NAME>**	<NAME> – имя DAS-сервера, задается строкой до 31 символа.
9	Сконфигурировать BRAS.	**esr(config)# subscriber-control [vrf <VRF>]**	<VRF> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет работать контроль пользователей.
10	Выбрать профиль серверов динамической авторизации (DAS), на которые будут приходить CoA-запросы от PCRF	**esr(config-subscriber-control)# aaa das-profile <NAME>**	<NAME> – имя профиля серверов динамической авторизации (DAS), задается строкой до 31 символа.
11	Выбрать профиль RADIUS-серверов для получения параметров сервисов пользователя	**esr(config-subscriber-control)# aaa services-radius-profile <NAME>**	<NAME> – имя профиля RADIUS-серверов, задается строкой до 31 символа.
12	Выбрать профиль RADIUS-серверов для получения параметров сессии пользователя.	**esr(config-subscriber-control)# aaa sessions-radius-profile <NAME>**	<NAME> – имя профиля RADIUS-серверов, задается строкой до 31 символа.
13	Определить IP-адрес маршрутизатора, который будет использоваться в качестве IP-адреса источника в отправляемых RADIUS пакетах.	**esr(config-subscriber-control)# nas-ip-address <ADDR>**	<ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
14	Включить аутентификацию сессий по MAC-адресу (не обязательно).	**esr(config-subscriber-control)# session mac-authentication**	

Шаг	Описание	Команда	Ключи
15	Организовать прозрачное пропускание служебного трафика (DHCP, DNS и т.д.) на основе фильтров.	**esr(config-subscriber-control)# bypass-traffic-a c l <NAME>**	<NAME> – имя привязываемого ACL, задается строкой до 31 символа.
16	Перейти в режим конфигурирования сервиса по умолчанию.	**esr(config-subscriber-control)# default-service**	
17	Привязать указанный QoS-класс к сервису по умолчанию.	**esr(config-subscriber-default-service)# class-map <NAME>**	<NAME> – имя привязываемого класса, задается строкой до 31 символа.
18	Указать имя списка URL, который будет использоваться для фильтрации HTTP/HTTPS трафика не аутентифицированных пользователей.	**esr(config-subscriber-default-service)# filter-name { local<LOCAL-NAME> | remote<REMOTE-NAME> }**	<LOCAL-NAME> – имя профиля URL, задаётся строкой до 31 символа; <REMOTE-NAME> – имя списка URL на удаленном сервере, задаётся строкой до 31 символа.
19	Указать действия, которые должны быть применены для HTTP/HTTPS-пакетов, URL которых входит в список URL, назначенных командой «filter-name».	**esr(config-subscriber-default-service)# filter-action<ACT>**	<ACT> – назначаемое действие: • **permit** – прохождение трафика разрешается; • **deny** – прохождение трафика запрещается; redirect <URL> – будет выполнен редирект на указанный URL, задается строкой до 255 символов.
20	Указать действия, которые должны быть применены для HTTP/HTTPS-пакетов, URL которых не входит в список URL, назначенных командой «filter-name».	**esr(config-subscriber-default-service)# default -action<ACT>**	<ACT> – назначаемое действие: • **permit** – прохождение трафика разрешается; • **deny** – прохождение трафика запрещается; redirect <URL> – будет выполнен редирект на указанный URL, задается строкой до 255 символов.
21	Активировать профиль контроля пользователей.	**esr(config-subscriber-control)# enable**	

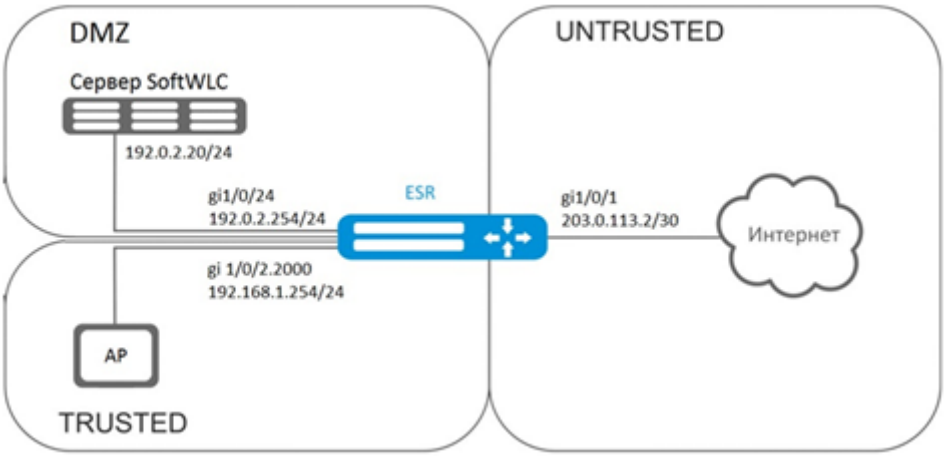
Шаг	Описание	Команда	Ключи
22	Изменить идентификатор сетевого интерфейса (физического, саб-интерфейса или сетевого моста) (не обязательно).	**esr(config-if)# location <ID>**	<ID> – идентификатор сетевого интерфейса, задаётся строкой до 220 символов.
23	Включить контроль пользователей на интерфейсе.	**esr(config-if-gi)# service-subscriber-control {any| object-group <NAME>}**	<NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.
24	Включить перезапрос значения квоты при ее истечении для сервисов пользователя с настроенным ограничением по объему трафика или времени (не обязательно).	**esr(config-subscriber-control)# quota-expired-reauth**	
25	Включить аутентификацию сессий по IP-адресу (не обязательно).	**esr(config-subscriber-control)# session ip-authentication**	
26	Включить прозрачное пропускание трафика в состоянии backup для BRAS (не обязательно).	**esr(config-subscriber-control)# backup traffic-processing transparent**	
27	Задать интервал, по истечении которого с устройства будут удалены неиспользуемые в текущий момент списки URL (не обязательно).	**esr(config)# subscriber-control unused-filters-remove-delay <DELAY>**	<DELAY> – временной интервал в секундах, принимает значения [10800..86400].
28	Задать интервал, по истечении которого, если не было пакетов от пользователя, сессия считается устаревшей и удаляется с устройства (не обязательно).	**esr(config-subscriber-default-service)# session-timeout <SEC>**	<SEC> – период времени в секундах, принимает значения [120..3600].
29	Определить VRRP-группу, на основе которой определяется состояние сервиса контроля абонентов (основной/резервный) (не обязательно).	**esr(config-subscriber-control)# vrrp-group <GRID>**	<GRID> – идентификатор группы VRRP-маршрутизатора, принимает значения [1..32].
30	Определить с каких TCP-портов назначения трафик будет перенаправлен на HTTP Proxy-сервер маршрутизатора (не обязательно).	**esr(config-subscriber-control)# ip proxy http listen-ports <NAME>**	<NAME> – имя профиля TCP/UDP-портов, задаётся строкой до 31 символа.
31	Определить порт HTTP Proxy-сервера на маршрутизаторе (не обязательно).	**esr(config-subscriber-control)# ip proxy http redirect-port <PORT>**	<PORT> – номер порта, указывается в диапазоне [1..65535].

Шаг	Описание	Команда	Ключи
32	Определить с каких TCP-портов назначения трафик будет перенаправлен на HTTPS Proxy-сервер маршрутизатора (не обязательно).	**esr(config-subscriber-control)# ip proxy https listen-ports <NAME>**	<NAME> – имя профиля TCP/UDP-портов, задаётся строкой до 31 символа.
33	Определить порт HTTPS Proxy-сервера на маршрутизаторе (не обязательно).	**esr(config-subscriber-control)# ip proxy https redirect-port <PORT>**	<PORT> – номер порта, указывается в диапазоне [1..65535].
34	Определить IP-адрес маршрутизатора, который будет использоваться в качестве IP-адреса источника в отправляемых Proxy-сервером HTTP/HTTPS пакетах (не обязательно).	**esr(config-subscriber-control)# ip proxy source-address <ADDR>**	<ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
35	Задать URL-адрес сервера, предоставляющего списки приложений для фильтрации трафика (не обязательно).	**esr(config)# subscriber-control apps-server-url <URL>**	<URL> – адрес ссылки, задаётся строкой от 8 до 255 символов.
36	Включить контроль приложений на интерфейсе (не обязательно).	**esr(config-if-gi)# subscriber-control application-filter <NAME>**	<NAME> – имя профиля приложений, задаётся строкой до 31 символа.
37	Установить/сбросить верхнюю границу количества сессий BRAS (не обязательно).	**esr(config-subscriber-control)# thresholds sessions-number high < Threshold>**	<Threshold> – количество сессий BRAS: • [0-50000] – для ESR-1700 • [0-10000] – для ESR-1200/1000/1500/1511/3100/3200 • [0-1000] – для ESR-100/200
38	Установить/сбросить нижнюю границу количества сессий BRAS (не обязательно).	**esr(config-subscriber-control)# thresholds sessions-number low < Threshold>**	<Threshold> – количество сессий BRAS: • [0-50000] – для ESR-1700 • [0-10000] – для ESR-1200/1000/1500/1511/3100/3200 • [0-1000] – для ESR-100/200

20.2 Пример настройки с SoftWLC

Задача:

Предоставлять доступ до ресурсов сети Интернет, только для авторизованных пользователей.



Решение:

За хранение учетных данных пользователей и параметров тарифных планов отвечает сервер SoftWLC. Информацию по установке и настройке сервера SoftWLC можно найти по ссылкам ниже:

Общая статья о SoftWLC;

Установка SoftWLC из репозиториев.

Для маршрутизатора необходимо наличие лицензии BRAS, после ее активации можно переходить к конфигурированию устройства.

Создадим три зоны безопасности на устройстве, согласно схеме сети:

```
esr# configure
esr(config)# security zone trusted
esr(config-zone)# exit
esr(config)# security zone untrusted
esr(config-zone)# exit
esr(config)# security zone dmz
esr(config-zone)# exit
```

Сконфигурируем параметры публичного порта и сразу пропишем шлюз по умолчанию:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# security-zone untrusted
esr(config-if-gi)# ip address 203.0.113.2/30
esr(config-if-gi)# service-policy dynamic upstream
esr(config-if-gi)# exit
esr(config)# ip route 0.0.0.0/0 203.0.113.1
```

Сконфигурируем порт в сторону сервера SoftWLC:

```
esr (config)# interface gigabitethernet 1/0/24
esr (config-if-gi)# security-zone dmz
esr (config-if-gi)# ip address 192.0.2.1/24
esr (config-if-gi)# exit
```

Сконфигурируем порт для подключения Wi-Fi точки доступа.

```
esr(config)# bridge 2
esr(config-bridge)# security-zone trusted
esr(config-bridge)# ip address 192.168.0.254/24
esr(config-bridge)# ip helper-address 192.0.2.20
esr(config-bridge)# service-subscriber-control object-group users
esr(config-bridge)# location ssid1
esr(config-bridge)# enable
esr(config-bridge)# exit
esr(config)# interface gigabitethernet 1/0/2.2000
esr(config-subif)# bridge-group 1
esr(config-subif)# exit
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# service-policy dynamic downstream
esr (config-if-gi)# exit
```

Подключать клиентов необходимо через саб-интерфейсы в бриджи, причем от параметра location (смотри конфигурацию bridge 2) зависит выбор тарифного плана.

Модуль, отвечающий за AAA-операции, основан на eltex-radius и доступен по IP-адресу сервера SoftWLC. Номера портов для аутентификации и аккаунтинга в нашем примере – это значения по умолчанию для SoftWLC.

Зададим параметры для взаимодействия с этим модулем:

```
esr(config)# radius-server host 192.0.2.20
esr(config-radius-server)#   key ascii-text password
esr(config-radius-server)#   auth-port 31812
esr (config-radius-server)#  acct-port 31813
esr (config-radius-server)# exit
```

Создадим профиль AAA:

```
esr(config)# aaa radius-profile RADIUS
esr(config-aaa-radius-profile)# radius-server host 192.0.2.20
esr(config-aaa-radius-profile)# exit
```

Укажем параметры доступа к DAS (Direct-attached storage)-серверу:

```
esr(config)# object-group network server
esr(config-object-group-network)#   ip address-range 192.0.2.20
esr(config-object-group-network)# exit
esr(config)# das-server CoA
esr(config-das-server)#   key ascii-text password
esr(config-das-server)#   port 3799
esr(config-das-server)#   clients object-group server
esr(config-das-server)# exit
esr(config)# aaa das-profile CoA
esr(config-aaa-das-profile)#   das-server CoA
esr(config-aaa-das-profile)# exit
```

До аутентификации весь трафик из зоны trusted блокируется, в том числе DHCP- и DNS-запросы. Необходимо настроить разрешающие правила для пропуска DHCP- и DNS-запросов:

```
esr(config)# ip access-list extended DHCP
esr(config-acl)#  rule 10
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol udp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port 68
esr(config-acl-rule)# match destination-port 67
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# rule 11
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol udp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port any
esr(config-acl-rule)# match destination-port 53
esr(config-acl-rule)# enable
esr(config-acl-rule)#exit
esr(config-acl)# exit
```

Далее создаем правила для редиректа на портал и пропуска трафика в Интернет:

```
esr(config)# ip access-list extended WELCOME
esr(config-acl)# rule 10
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit
esr (config)# ip access-list extended INTERNET
esr(config-acl)#  rule 10
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit
```

Зададим web-ресурсы доступные без авторизации:

```
esr(config)# object-group url defaultservice
esr(config-object-group-url)# url http://eltex.nsk.ru
esr(config-object-group-url)# exit
```

Списки фильтрации по URL находятся на сервере SoftWLC (меняется только IP-адрес сервера SoftWLC, если используется адресация отличная от данного примера, все остальное в URL оставить без изменения):

```
esr(config)# subscriber-control filters-server-url http://192.0.2.20:7070/Filters/file/
```

Сконфигурируем и включим BRAS, в качестве NAS IP указываем адрес интерфейса на стыке с SoftWLC, в данном примере – это IP-адрес интерфейса gigabitethernet 1/0/24:

```
esr(config)# subscriber-control
esr(config-subscriber-control)#  aaa das-profile CoA
esr(config-subscriber-control)#  aaa sessions-radius-profile RADIUS
esr(config-subscriber-control)#  nas-ip-address 192.0.2.1
esr(config-subscriber-control)#  session mac-authentication
esr(config-subscriber-control)#  bypass-traffic-acl DHCP
esr(config-subscriber-control)#  default-service
esr(config-subscriber-default-service)#  class-map INTERNET
esr(config-subscriber-default-service)#  filter-name local defaultservice
esr(config-subscriber-default-service)#  filter-action permit
esr(config-subscriber-default-service)#  default-action redirect http://192.0.2.20:8080/
eltex_portal/
esr(config-subscriber-default-service)#  session-timeout 3600
esr(config-subscriber-default-service)# exit
esr(config-subscriber-control)# enable
esr(config-subscriber-control)# exit
```

Далее необходимо сконфигурировать правила перехода между зонами безопасности:

```
esr(config)# object-group service telnet
esr(config-object-group-service)#   port-range 23
esr(config-object-group-service)# exit
esr(config)# object-group service ssh
esr(config-object-group-service)#   port-range 22
esr(config-object-group-service)# exit
esr(config)# object-group service dhcp_server
esr(config-object-group-service)#   port-range 67
esr(config-object-group-service)# exit
esr(config)# object-group service dhcp_client
esr(config-object-group-service)#   port-range 68
esr(config-object-group-service)# exit
esr(config)# object-group service ntp
esr(config-object-group-service)#   port-range 123
esr(config-object-group-service)# exit
```

Разрешим доступ в Интернет из зон trusted и dmz:

```
esr(config)# security zone-pair trusted untrusted
esr(config-zone-pair)# rule 10
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# security zone-pair dmz untrusted
esr(config-zone-pair)# rule 10
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# security zone-pair dmz trusted
esr(config-zone-pair)# rule 10
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
```

Разрешим прохождение DHCP из trusted в dmz:

```
esr (config)# security zone-pair trusted dmz
esr (config-zone-pair)# rule 10
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol udp
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# match source-port dhcp_client
esr(config-zone-pair-rule)# match destination-port dhcp_server
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
```

Разрешим прохождение ICMP к устройству, для работы BRAS необходимо открыть порты для веб-проксирования – TCP 3129/3128 (NetPort Discovery Port/Active API Server Port):

```
esr(config)# object-group service bras
esr(config-object-group-service)#   port-range 3129
esr(config-object-group-service)#   port-range 3128
esr(config-object-group-service)# exit
esr(config)#  security zone-pair trusted self
esr(config-zone-pair)#  rule 10
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol tcp
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# match source-port any
esr(config-zone-pair-rule)# match destination-port bras
esr(config-zone-pair-rule)# enable
esr (config-zone-pair-rule)# exit
esr(config-zone-pair)# rule 20
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-rule)# exit
esr(config)# security zone-pair dmz self
esr(config-zone-pair)# rule 20
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-rule)# exit
esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule 20
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-rule)# exit
```

Активируем DHCP-Relay:

```
esr(config)# ip dhcp-relay
```

Настроим SNAT в порт gigabitethernet 1/0/1:

```
esr(config)# nat source
esr(config-snat)# ruleset inet
esr(config-snat-ruleset)# to interface gigabitethernet 1/0/1
esr(config-snat-ruleset)# rule 10
esr(config-snat-rule)# match source-address any
esr(config-snat-rule)# action source-nat interface
esr(config-snat-rule)# enable
esr(config-snat-rule)# end
```

20.3 Пример настройки без SoftWLC

Задача:

Настроить BRAS без поддержки SoftWLC.

Дано:

Подсеть с клиентами 10.10.0.0/16, подсеть для работы с FreeRADIUS-сервером 192.168.1.1/24

Решение:

Шаг 1:

Настройка RADIUS-сервера.

Для FreeRADIUS-сервера нужно задать подсеть, из которой могут приходить запросы и добавить список пользователей. Для этого в файл users в директории с файлами конфигурации FreeRADIUS сервера нужно добавить:

Профиль пользователя:

```
<MACADDR> Cleartext-Password := <MACADDR>
```

#Имя пользователя

```
  User-Name = <USER_NAME>,
```

#Максимальное время жизни сессии

```
  Session-Timeout = <SECONDS>,
```

#Максимальное время жизни сессии при бездействии пользователя

```
  Idle-Timeout = <SECONDS>,
```

#Время на обновление статистики по сессии

```
  Acct-Interim-Interval = <SECONDS>,
```

#Имя сервиса для сессии (A – сервис включен, N – сервис выключен)

```
  Cisco-Account-Info = "{A|N}<SERVICE_NAME>"
```

Профиль сервиса:

```
  <SERVICE_NAME> Cleartext-Password := <MACADDR>
```

Соответствует имени class-map в настройках ESR

```
  Cisco-AVPair = "subscriber:traffic-class=<CLASS_MAP>",
```

Действие, которое применяет ESR к трафику (permit, deny, redirect)

```
 Cisco-AVPair = "subscriber:filter-default-action=<ACTION>",
```

Возможность прохождения IP-потоков (enabled-uplink, enabled-downlink, enabled, disabled)

```
 Cisco-AVPair = "subscriber:flow-status=<STATUS>"
```

В файл clients.conf нужно добавить подсеть, в которой находится ESR:

```
client ESR {
ipaddr = <SUBNET>
secret = <RADIUS_KEY>
}
```

В нашем случае настройка RADIUS-сервера будет выглядеть так:

в файл «clients.conf» добавляем строки:

```
client BRAS {
ipaddr = 192.168.1.1
secret = password
}
```

В файл «users» добавляем строки (вместо <MAC> нужно указать MAC-адрес клиента):

```
"54-E1-AD-8F-37-35" Cleartext-Password := "54-E1-AD-8F-37-35"
User-Name = "Bras_user",
Session-Timeout = 259200,
Idle-Timeout = 259200,
Cisco-AVPair += "subscriber:policer-rate-in=1000",
Cisco-AVPair += "subscriber:policer-rate-out=1000",
Cisco-AVPair += "subscriber:policer-burst-in=188",
Cisco-AVPair += "subscriber:policer-burst-out=188",
Cisco-Account-Info = "AINTERNET"
INTERNET Cleartext-Password := "INTERNET"
User-Name = "INTERNET",
Cisco-AVPair = "subscriber:traffic-class=INTERNET",
Cisco-AVPair += "subscriber:filter-default-action=permit"
```

Шаг 2:

Настройка ESR.

Для настройки функционала BRAS необходимо наличие лицензии BRAS.

```
esr(config)# do sh licence
Licence information
-------------------
Name:    Eltex
Version: 1.0
Type:    ESR-X
S/N:     NP00000000
MAC:     XX:XX:XX:XX:XX:XX
Features:
  BRAS - Broadband Remote Access Server
```

Настройка параметров для взаимодействия с RADIUS-сервером:

```
esr(config)# radius-server host 192.168.1.2
esr(config-radius-server)# key ascii-text encrypted 8CB5107EA7005AFF
esr(config-radius-server)# source-address 192.168.1.1
esr(config-radius-server)# exit
```

Создадим профиль AAA:

```
esr(config)#  aaa radius-profile bras_radius
esr(config-aaa-radius-profile)# radius-server host 192.168.1.2
esr(config-aaa-radius-profile)#  exit
esr(config)#  aaa radius-profile bras_radius_servers
esr(config-aaa-radius-profile)#  radius-server host 192.168.1.2
esr(config-aaa-radius-profile)#  exit
```

Укажем параметры к DAS-серверу:

```
esr(config)# das-server das
esr(config-das-server)# key ascii-text encrypted 8CB5107EA7005AFF
esr(config-das-server)#  exit
esr(config)#  aaa das-profile bras_das
esr(config-aaa-das-profile)#  das-server das
esr(config-aaa-das-profile)# exit
esr(config)#  vlan 10
esr(config-vlan)#  exit
```

Далее создаем правила для редиректа на портал и пропуска трафика в Интернет:

```
esr(config)# ip access-list extended BYPASS
esr(config-acl)# rule 1
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol udp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port 68
esr(config-acl-rule)# match destination-port 67
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# rule 2
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol udp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port any
esr(config-acl-rule)# match destination-port 53
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config)# ip access-list extended INTERNET
esr(config-acl)# rule 1
esr(config-acl-rule)#  action permit
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config)# ip access-list extended WELCOME
esr(config-acl)# rule 10
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol tcp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port any
esr(config-acl-rule)# match destination-port 443
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# rule 20
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol tcp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port any
esr(config-acl-rule)# match destination-port 8443
```

```
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# rule 30
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol tcp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port any
esr(config-acl-rule)# match destination-port 80
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# rule 40
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol tcp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port any
esr(config-acl-rule)# match destination-port 8080
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
```

Настройка действие фильтрации по URL обязательно, а именно, необходимо настроить фильтрацию http-proxy на BRAS для неавторизованных пользователей:

```
esr(config)# object-group url defaultserv
esr(config-object-group-url)# url http://eltex.nsk.ru
esr(config-object-group-url)# url http://ya.ru
esr(config-object-group-url)# url https://ya.ru
esr(config-object-group-url)# exit
```

Сконфигурируем и включим BRAS, в качестве NAS IP указываем адрес интерфейса на стыке с RADIUS-сервером в данном примере – это IP-адрес интерфейса gigabitethernet 1/0/2:

```
esr(config)#  subscriber-control
esr(config-subscriber-control)# aaa das-profile bras_das
esr(config-subscriber-control)# aaa sessions-radius-profile bras_radius
esr(config-subscriber-control)# aaa services-radius-profile bras_radius_servers
esr(config-subscriber-control)# nas-ip-address 192.168.1.1
esr(config-subscriber-control)# session mac-authentication
esr(config-subscriber-control)# bypass-traffic-acl BYPASS
esr(config-subscriber-control)# default-service
esr(config-subscriber-default-service)# class-map BYPASS
esr(config-subscriber-default-service)# filter-name local defaultserv
esr(config-subscriber-default-service)# filter-action permit
esr(config-subscriber-default-service)# default-action redirect http://192.
168.1.2:8080/eltex_portal
esr(config-subscriber-default-service)# session-timeout 121
esr(config-subscriber-default-service)# exit
esr(config-subscriber-control)# enable
esr(config-subscriber-control)# exit
```

На интерфейсах, для которых требуется работа BRAS, произвести настройку (для успешного запуска требуется как минимум один интерфейс):

```
esr(config)#  bridge 10
esr(config-bridge)# vlan 10
esr(config-bridge)# ip firewall disable
esr(config-bridge)#  ip address 10.10.0.1/16
esr(config-bridge)#  ip helper-address 192.168.1.2
esr(config-bridge)# service-subscriber-control any
esr(config-bridge)# location USER
esr(config-bridge)#  protected-ports
esr(config-bridge)#  protected-ports exclude vlan
esr(config-bridge)# enable
esr(config-bridge)#  exit
```

Сконфигурируем порт в сторону RADIUS-сервера:

```
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# ip firewall disable
esr(config-if-gi)# ip address 192.168.1.1/24
esr(config-if-gi)#  exit
```

Порт в сторону клиента:

```
esr(config)#  interface gigabitethernet 1/0/3.10
esr(config-subif)#  bridge-group 10
esr(config-subif)# ip firewall disable
esr(config-subif)#  exit
```

Настройка SNAT в порт gigabitethernet 1/0/2:

```
esr(config)# nat source
esr(config-snat)# ruleset factory
esr(config-snat-ruleset)# to interface gigabitethernet 1/0/2
esr(config-snat-ruleset)# rule 10
esr(config-snat-rule)# description "replace 'source ip' by outgoing interface ip address"
esr(config-snat-rule)# match protocol any
esr(config-snat-rule)# match source-address any
esr(config-snat-rule)# match destination-address any
esr(config-snat-rule)# action source-nat interface
esr(config-snat-rule)# enable
esr(config-snat-rule)# exit
esr(config-snat-ruleset)# exit
esr(config-snat)# exit
esr(config)# ip route 0.0.0.0/0 192.168.1.2
```

Изменения конфигурации вступят в действие после применения:

```
esr(config) # do commit
esr(config) # do confirm
```

Для просмотра информации и статистики по сессиям контроля пользователей – можно воспользоваться командой:

```
esr # sh subscriber-control sessions status

Session id      User name    IP address      MAC address       Interface          Domain
--------------------   ---------------  ----------------   ------------------
1729382256910270473    Bras_user   10.10.0.3  54:e1:ad:8f:37:35     gi1/0/3.10     --
```

21 Статьи

21.1 RADIUS-сервер

21.1.1 Настройка локального RADIUS-сервера

```
wlc-30(config)# radius-server local
```

Настраиваем **NAS ap**, который содержит подсети точек доступа, которые будут обслуживаться локальным RADIUS-сервером при Enterprise-авторизации пользователей Wi-Fi:

```
wlc-30(config-radius)# nas ap
wlc-30(config-radius-nas)# key ascii-text password
wlc-30(config-radius-nas)# network 192.168.1.0/24
wlc-30(config-radius-nas)# exit
```

Настраиваем **NAS local**. Используется при обращении WLC к локальному RADIUS-серверу при построении SoftGRE-туннелей:

```
wlc-30(config-radius)# nas local
wlc-30(config-radius-nas)# key ascii-text password
wlc-30(config-radius-nas)# network 127.0.0.1/32
wlc-30(config-radius-nas)# exit
```

Создаем домен для пользователей:

```
wlc-30(config-radius)# domain default
```

В этом домене создаем учетную запись пользователя Wi-Fi для подключения к Enterprise SSID:

```
wlc-30(config-radius-domain)# user name1
wlc-30(config-radius-user)# password ascii-text password1
wlc-30(config-radius-user)# exit
wlc-30(config-radius-domain)# exit
```

Обратите внимание, что в заводской конфигурации учетная запись пользователя не настроена в целях безопасности, поэтому для подключения к Enterprise SSID в заводской конфигурации необходимо создать учетную запись.

Настройки виртуального сервера содержат номера портов для аутентификации и аккаунтинга, настройки проксирования на внешний RADIUS server. Использование стандартных портов (1812 для аутентификации и 1813 для аккаунтинга) не требует настройки. В случае настройки локального Radius-сервера достаточно просто включения виртуального сервера (enable).

```
wlc-30(config-radius)# virtual-server default
wlc-30(config-radius-vserver)# enable

wlc-30(config-radius-vserver)# exit
wlc-30(config-radius)# enable
wlc-30(config)# exit
```

Определим параметры для взаимодействия с RADIUS-сервером: IP-адрес и ключ.
Так как RADIUS-сервер находится локально на контроллере, в качестве адреса хоста задаем 127.0.0.1.
Ключ должен совпадать с ключом, указанным для **nas local**, который мы задали в **radius-server local**.

```
wlc-30(config)# radius-server host 127.0.0.1
wlc-30(config-radius-server)# key ascii-text password
wlc-30(config-radius-server)# exit
```

Добавляем профиль AAA, указываем адрес сервера, который будет использоваться:

```
wlc-30(config)# aaa radius-profile default_radius
wlc-30(config-aaa-radius-profile)# radius-server host 127.0.0.1
wlc-30(config-aaa-radius-profile)# exit
```

Настраиваем и включаем функционал автоматического поднятия SoftGRE-туннелей:

```
wlc-30(config)# softgre-controller
```

RADIUS-сервер находится локально на контроллере, поэтому указываем nas-ip-address 127.0.0.1:

```
wlc-30(config-softgre)# nas-ip-address 127.0.0.1
```

Выбираем режим создания data SoftGRE туннелей – WLC:

```
wlc-30(config-softgre)# data-tunnel configuration wlc
```

Указываем созданный ранее AAA-профиль:

```
wlc-30(config-softgre)# aaa radius-profile default_radius
wlc-30(config-softgre)# keepalive-disable
wlc-30(config-softgre)# enable
wlc-30(config-softgre)# exit
```

Переходим к настройкам модуля управления конфигурацией точек доступа:

```
wlc-30(config)# wlc
```

Настраиваем профиль RADIUS-сервера, который будет использоваться для аутентификации беспроводных клиентов Enterprise SSID точек доступа Wi-Fi.

```
wlc-30(config-wlc)# radius-profile default-radius
```

RADIUS-сервер находится локально на контроллере, указываем адрес контроллера в подсети точек доступа:

```
wlc-30(config-wlc-radius-profile)# auth-address 192.168.1.1
```

Ключ RADIUS-сервера должен совпадать с ключом, указанным для **NAS ap**, который мы указали в **radius-server local**:

```
wlc-30(config-wlc-radius-profile)# auth-password ascii-text password
```

Указываем домен RADIUS. Этот домен должен совпадать с доменом, в котором созданы учетные записи пользователей Enterprise, который располагается в **radius-server local**.

```
wlc-30(config-wlc-radius-profile)# domain default
wlc-30(config-wlc-radius-profile)# exit
```

Профиль SSID содержит настройки SSID точки доступа.

```
wlc-30(config-wlc)# ssid-profile default-ssid
```

Указываем в **ssid-profile** ранее настроенный профиль настроек RADIUS-сервера, который будет использоваться для авторизации пользователей Wi-Fi:

```
wlc-30(config-wlc-ssid-profile)# radius-profile default-radius
```

21.1.2 Настройка проксирования на внешний RADIUS

Настраиваем локальный RADIUS-сервер

```
wlc-30# configure
wlc-30(config)# radius-server local
```

Настраиваем **NAS ap**, который содержит подсети точек доступа, которые будут обслуживаться локальным RADIUS-сервером при Enterprise-авторизации пользователей Wi-Fi:

```
wlc-30(config-radius)# nas ap
wlc-30(config-radius-nas)# key ascii-text password
wlc-30(config-radius-nas)# network 192.168.1.0/24
wlc-30(config-radius-nas)# exit
```

Настройки виртуального сервера содержат номера портов для аутентификации и аккаунтинга, настройки проксирования на внешний RADIUS server. Использование стандартных портов (1812 для аутентификации и 1813 для аккаунтинга) не требует настройки. Для проксирования RADIUS-запросов на внешний сервер необходимо включить proxy-mode.

Типы upstream серверов
Server-type auth — используется для проксирования только запросов аутентификации. Запросы будут проксироваться на порт, указанный в параметре port (по умолчанию – 1812).
Server-type acct — используется для проксирования только аккаунтинга. Проксирование осуществляется на порт, указанный в параметре port (по умолчанию - 1812). При необходимости измените его (стандартный порт для аккаунтинга – 1813).
Server-type all — используется для проксирования запросов аутентификации и аккаунтинга. Запросы аутентификации будут проксироваться на порт, указанный в параметре port (по умолчанию – 1812), а аккаунтинг будет проксироваться на порт = 'port'+1 (то есть по умолчанию – 1813).

Настраиваем внешний сервер (virtual-server), указывая его адрес, тип (server-type) и ключ, также можно указать порт. По умолчанию выставлен сервер для аутентификации (server-type auth) и порт 1812, если нет необходимости менять эти настройки, тогда достаточно настроить адрес и ключ для сервера.

```
wlc-30(config-radius)# virtual-server default
wlc-30(config-radius-vserver)# enable
wlc-30(config-radius-vserver)# proxy-mode
wlc-30(config-radius-vserver)# upstream-server eltex
wlc-30(config-radius-upstream-server)# host 10.10.10.12
wlc-30(config-radius-upstream-server)# server-type all
wlc-30(config-radius-upstream-server)# key ascii-text password
wlc-30(config-radius-vserver)# exit
```

Настраиваем **NAS eltex,** где eltex – имя внешнего сервера. Используется при обращении WLC к внешнему RADIUS-серверу:

```
wlc-30(config-radius)# nas eltex
wlc-30(config-radius-nas)# key ascii-text password
wlc-30(config-radius-nas)# network 10.10.10.0/24
wlc-30(config-radius-nas)# exit
```

```
wlc-30(config-radius)# enable
wlc-30(config)# exit
```

Переходим к настройкам модуля управления конфигурацией точек доступа:

```
wlc-30(config)# wlc
```

Настраиваем профиль RADIUS-сервера, который будет использоваться для аутентификации беспроводных клиентов Enterprise SSID точек доступа Wi-Fi.

```
wlc-30(config-wlc)# radius-profile default-radius
```

Поскольку мы настраиваем проксирование запросов аутентификации и аккаунтинга, то указываем адрес контроллера локального RADIUS-сервера в подсети точек доступа.
Ключ RADIUS-сервера должен совпадать с ключом, указанным для **NAS ap**, который мы указали в **radius-server local.**

```
wlc-30(config-wlc-radius-profile)# auth-address 192.168.1.1
wlc-30(config-wlc-radius-profile)# auth-password ascii-text password
```

Если вы используете проксирование на SoftWLC, укажите домен RADIUS. Этот домен должен совпадать с доменом, в котором созданы учетные записи пользователей Enterprise на SoftWLC.

wlc-30(config-wlc-radius-profile)# domain root

Указываем IP-адрес RADIUS-сервера подсети точек доступа, используемого для аккаунтинга и ключ RADIUS-сервера.

```
wlc-30(config-wlc-radius-profile)# acct-address 192.168.1.1
wlc-30(config-wlc-radius-profile)# acct-password ascii-text password
```

Активируем отправку аккаунтинга на RADIUS-сервер.

```
wlc-30(config-wlc-radius-profile)# acct-enable
```

Настройки SSID точки доступа.

```
wlc-30(config-wlc)# ssid-profile default-ssid
```

Указываем в **ssid-profile** ранее настроенный профиль настроек RADIUS-сервера, который будет использоваться для авторизации пользователей Wi-Fi:

```
wlc-30(config-wlc-ssid-profile)# radius-profile default-radius
```

Для настройки внешнего RADIUS-сервера, необходимо записать в таблицу NAS внешнего RADIUS-сервера адрес и ключ локального RADIUS-сервера WLC-30.

Пример конфигурации:

```
 radius-server local
  nas ap
    key ascii-text encrypted 8CB5107EA7005AFF
    network 192.168.1.0/24
  exit
  nas eltex
    key ascii-text encrypted 8CB5107EA7005AFF
    network 10.10.10.0/24
  exit
  virtual-server default
    proxy-mode
    upstream-server eltex
      host 10.10.10.12
      server-type all
      key ascii-text encrypted 8CB5107EA7005AFF
    exit
    enable
  exit
  enable
exit

radius-profile default-radius
    auth-address 192.168.1.1
    auth-password ascii-text encrypted 8CB5107EA7005AFF
    acct-enable
    acct-address 192.168.1.1
    acct-password ascii-text encrypted 8CB5107EA7005AFF
exit
```

22 Управление VoIP

- Алгоритм настройки SIP-профиля
- Алгоритм настройки FXS/FXO-портов
- Алгоритм настройки плана нумерации
- Алгоритм настройки PBX-сервера
- Алгоритм создания транка регистрации
- Пример настройки VoIP
- Пример настройки плана нумерации
- Настройка FXO-порта
- Пример настройки voip для регистрации FXS-портов на внешнем sip-сервере
- Пример настройки voip на внутреннем pbx-сервере

VoIP (англ. *Voice over IP*) — набор протоколов, которые позволяют передавать речевую информацию посредством IP-сетей. В рамках данного устройства VoIP используется для подключения аналоговых телефонных аппаратов к IP-сети с возможностью совершения телефонных вызовов.

22.1 Алгоритм настройки SIP-профиля

Шаг	Описание	Команда	Ключи
1	Настройка SIP-профиля.	**esr(config)# sip profile <NUM>**	<NUM> – номер SIP-профиля, задается в виде цифры от 1 до 5.
2	Настройка основного SIP proxy-сервера и сервера регистрации.	**esr(config-sip-profile)# proxy primary**	
3	Настройка адреса SIP proxy-сервера.	**esr(config-voip-sip-proxy)# ip address proxy-server <IP>**	<IP> – IP-адрес proxy-сервера.
4	Настройка порта SIP proxy-сервера.	**esr(config-voip-sip-proxy)# ip port proxy-server <PORT>**	<PORT> – номер UDP-порта proxy-сервера, принимает значения [1..65535]. Если используется стандартный порт 5060, то его можно не указывать.
5	Настройка адреса сервера регистрации.	**esr(config-voip-sip-proxy)# ip address registration-server <IP>**	<IP> – IP-адрес сервера регистрации.
6	Настройка порта сервера регистрации.	**esr(config-voip-sip-proxy)# ip portregistration-server <PORT>**	<PORT> – номер UDP-порта сервера регистрации, принимает значения [1..65535]. Если используется стандартный порт 5060, то его можно не указывать.

Шаг	Описание	Команда	Ключи
7	Активация регистрации.	**esr(config-voip-sip-proxy)# registration**	
8	Активация proxy-сервера и сервера регистрации.	**esr(config-voip-sip-proxy)# enable**	
9	Настройка адреса сервера регистрации.	**esr(config-voip-sip-proxy)# ip address registration-server <IP>**	<IP> – IP-адрес сервера регистрации.
10	Настройка порта сервера регистрации.	**esr(config-voip-sip-proxy)# ip portregistration-server <PORT>**	<PORT> – номер UDP-порта сервера регистрации, принимает значения [1..65535]. Если используется стандартный порт 5060, то его можно не указывать.
11	Указание SIP-домена, в котором находится устройство.	**esr(config-sip-profile)# sip-domain address <ADDRESS>**	<ADDRESS> – SIP-домен, в котором находится устройство, задается ipv4-адресом или доменным именем.
12	Активация использования SIP domain при регистрации.	**esr(config-sip-profile)# sip-domain registration enable**	
13	Настройка SIP-профиля.	**esr(config)# sip profile <NUM>**	<NUM> – номер SIP-профиля, задается в виде цифры от 1 до 5.
14	Назначение плана нумерации текущему SIP-профилю.	**esr(config-sip-profile)# dialplan pattern <DNAME>**	<DNAME> – имя план нумерации, задается стройкой до 31 символа.
15	Активация SIP-профиля.	**esr(config-sip-profile)# enable**	

22.2 Алгоритм настройки FXS/FXO-портов

Шаг	Описание	Команда	Ключи
1	Переход в режим конфигурирования FXO-/FXS-портов.	**esr(config)# interface voice-port <NUM>**	<NUM> – номер порта, принимает значение от 1 до 4.
2	Назначение абонентского номера, закрепленного за телефонным портом.	**esr(config-voice-port-fxs)# sip user phone <PHONE>**	<PHONE> – абонентский номер, закрепленный за телефонным портом, задается до 50 символов.
3	Назначение имя пользователя, сопоставленное с портом.	**esr-12v(config-voice-port-fxs)# sip user display-name <LOGIN>**	<LOGIN> – имя пользователя, которое отображается в поле Display-Name, задается стройкой до 31 символа.
4	Выбор SIP-профиля для конкретного порта.	**esr(config-voice-port-fxs)# profile sip <PROFILE>**	<PROFILE> – номер SIP-профиля, задается от 1 до 5.
5	Настройка логина для аутентификации.	**esr(config-voice-port-fxs)# authentication name <LOGIN>**	<LOGIN> – логин для аутентификации, задается строкой до 31 символа
6	Настройка пароля для аутентификации.	**esr(config-voice-port-fxs)# authentication password <PASS>**	<PASS> – пароль для аутентификации, задается строкой до 16 символов.
7	Активация FXO-порта.	**esr(config)# interface voice-port <NUM>**	<NUM> – номер FXO-порта принимает значение от 1 до 4.
8	Назначение абонентского номера, закрепленного за телефонным портом.	**esr(config-voice-port-fxo)# sip user phone <PHONE>**	<PHONE> – абонентский номер, закрепленный за телефонным портом.
9	Указание UDP-порта, с которого и на который FXO-комплект будет отправлять и принимать SIP-сообщения.	**esr(config-voice-port-fxo)# sip port <PORT>**	<PORT> – номер UDP-порта.
10	Назначение имени пользователя, сопоставленное с портом.	**esr(config-voice-port-fxo)# sip user display-name <LOGIN>**	<LOGIN> – имя пользователя, которое отображается в поле Display-Name, задается строкой до 31 символа.

Шаг	Описание	Команда	Ключи
11	Настройка логина для аутентификации.	**esr(config-voice-port-fxo)# authentication name <LOGIN>**	<LOGIN> – логин для аутентификации, задается строкой до 31 символа.
12	Настройка пароля для аутентификации.	**esr(config-voice-port-fxo)# authentication password <PASS>**	<PASS> – пароль для аутентификации, задается строкой до 16 символов.
13	Разрешение передачи номера в ТфОП.	**esr(config-voice-port-fxo)# pstn transmit-number**	
14	Запретить передачу префикса.	**esr(config-voice-port-fxo)# no pstn transmit-prefix**	
15	Активация услуги «Hostline PSTN to IP».	**esr(config-voice-port-fxo)# hotline ipt**	
16	Номер абонента, который будет получать вызовы с ТфОП.	**esr(config-voice-port-fxo)# hotline number ipt <PHONE>**	<PHONE> – номер телефона, на который осуществляется вызов при использовании услуги, принимает значение от 1 до 50. «Горячая/Теплая линия» в направлении из аналоговой телефонной линии в VoIP.

22.3 Алгоритм настройки плана нумерации

Шаг	Описание	Команда	Ключи
1	Создание плана нумерации.	**esr(config)# dialplan pattern <DNAME>**	<DNAME> – имя плана нумерации, задается строкой до 31 символа.
2	Добавление правил нумерации.	**esr(config-dial-ruleset)# pattern <REGEXP>**	<REGEXP> – регулярное выражение, задающее план нумерации. Задаётся строкой до 1024 символов. Правила составления регулярных выражений описаны в разделе Пример настройки плана нумерации.
3	Активация плана нумерации.	**esr(config-dial-ruleset)# enable**	

22.4 Алгоритм настройки PBX-сервера

Шаг	Описание	Команда	Ключи
1	Настройка PBX-сервера.	**esr(config)# pbx**	
2	Включение PBX-сервера.	**esr(config-pbx)# enable**	
3	Создание плана маршрутизации.	**esr(config-pbx)# ruleset <rule_name>**	<rule_name> – имя плана маршрутизации, задается строкой до 31 символа.
4	Создание правила маршрутизации.	**esr(config-pbx-ruleset)# rule <rule_index>**	<rule_index> – номер правила в плане маршрутизации, принимает значение от 1 до 1000.
5	Создание паттерна в правиле маршрутизации.	**esr(config-pbx-rule)# pattern <REGEXP>**	<REGEXP> – регулярное выражение, задающее правило маршрутизации. Задаётся строкой до 256 символов. Правила составления регулярных выражений описаны в разделе Пример настройки плана нумерации.
6	Применение правила маршрутизации.	**esr(config-pbx-rule)# enable**	
7	Создание SIP-профиля на PBX-сервере.	**esr(config-pbx)# profile <PROFILE>**	<PROFILE> – имя SIP профиля, используемого PBX – сервером, задается строкой до 31 символа.
8	Выбор кодека, поддерживаемого SIP-профилем.	**esr(config-pbx-profile)# codec allow { G711A(alaw) | G711U(ulaw) | G722 | G726 }**	
9	Выбор типа SIP-профиля.	**esr(config-pbx-profile)# client { peer | user | friend }**	• **peer** – входящие и исходящие звоки разрешены без авторизации. • **user** – разрешены только входящие звонки. • **friend** – комбинирует типы профилей peer и user.

Шаг	Описание	Команда	Ключи
10	Выбор политики взаимодействия с NAT (не обязательно).	**esr(config-pbx-profile)# nat { comedia | force-port | both }**	• **comedia** – отправить медиа поток на порт PBX, независимо от указаний SDP. • **force-port** – использовать rport, даже если его нет. • **both** – объединяет comedia и force-port.
11	Выбор плана маршрутизации, связанного с SIP-профилем.	**esr(config-pbx-profile)# ruleset <NAME>**	<NAME> – имя плана маршрутизации, задается строкой до 31 символа.
12	Создание абонента.	**esr(config-pbx)# user <user>**	<user> – номер телефона или имя пользователя, задается строкой до 31 символа.
13	Создание пароля для абонента (не обязательно).	**esr(config-pbx-user)# password <password>**	<password> – пароль, который будет использоваться пользователем для аутентификации, задается строкой до 16 символов.
14	Применение SIP-профиля для абонента.	**esr(config-pbx-user)# profile <SIPPROFILE>**	<SIPPROFILE> – SIP - профиль, используемый для данного абонента, задается строкой до 31 символа.

22.5 Алгоритм создания транка регистрации

Шаг	Описание	Команда	Ключи
1	Настройка PBX-сервера.	**esr(config)# pbx**	
2	Создание транка.	**esr(config-pbx)# register-server <name>**	<name> – имя транка, задается строкой до 31 символа.
3	Настройка адреса сервера регистрации.	**esr(config-pbx-reg-server)# ip address <IP>**	<IP> – адрес сервера, на котором происходит регистрация, может принимать значение IP адреса или задаваться строкой до 31 символа.
4	Настройка порта сервера регистрации.	**esr(config-pbx-reg-server)# ip port <PORT>**	<PORT> – номер UDP-порта сервера регистрации, принимает значения [1..65535]. Если используется стандартный порт 5060, то его можно не указывать.
5	Задание аутентификационного имени.	**esr(config-pbx-reg-server)# username <user>**	<user> – имя пользователя для этого транка на вышестоящем домене, задается строкой до 31 символа.
6	Задание аутентификационного пароля.	**esr(config-pbx-reg-server)# authentication password <password>**	<password> – пароль для этого гранка на вышестоящем домене, задается строкой до 16 символов.
7	Применение SIP-профиля для транка.	**esr(config-pbx-reg-server)# profile <PROFILE>**	<PROFILE> – имя SIP профиля, используемое для данного транка, задается строкой до 31 символа.
8	Выбор транспортного протокола (не обязательно).	**esr(config-pbx-reg-server)# protocol {tcp | udp }**	По умолчанию используется udp.
9	Активация транка.	**esr(config-pbx-reg-server)# enable**	

22.6 Пример настройки VoIP

Задача:

Подключить аналоговые телефонные аппараты и факс-модемы к IP-сети посредством маршрутизатора ESR. В качестве proxy-сервера и сервера регистрации выступает SIP-сервер, находящийся на ESR.

Решение:

Настройка SIP-профиля:

```
esr(config)# sip profile 1
```

Настройка основного SIP proxy-сервера и сервера регистрации:

```
esr(config-sip-profile)# proxy primary
```

Настройка адреса SIP proxy-сервера (в качестве SIP proxy-сервера использовать встроенный SIP-сервер):

```
esr(config-voip-sip-proxy)# ip address proxy-server 192.0.2.5
```

Настройка порта SIP proxy-сервера:

```
esr(config-voip-sip-proxy)# ip port proxy-server 5080
```

Если используется стандартный порт 5060, то его можно не указывать.

Если необходимо использовать регистрацию, то необходимо выполнить следующие пункты:

Настройка адреса сервера регистрации (в качестве сервера регистрации использовать встроенный SIP-сервер):

```
esr(config-voip-sip-proxy)# ip address registration-server 192.0.2.5
```

Настройка порта сервера регистрации:

```
esr(config-voip-sip-proxy)# ip port registration-server 5080
```

Если используется стандартный порт 5060, то его можно не указывать.

Активация регистрации:

```
esr(config-voip-sip-proxy)# registration
```

Активация proxy-сервера и сервера регистрации:

```
esr(config-voip-sip-proxy)# enable
```

На этом конфигурация SIP proxy-сервера и сервера регистрации закончена:

```
esr(config-voip-sip-proxy)# exit
```

Далее продолжается настройка SIP-профиля.

Настройка SIP-домена:

```
esr(config-sip-profile)# sip-domain address sipdomain.com
```

Если необходимо использовать SIP Domain для регистрации:

```
esr(config-sip-profile)# sip-domain registration enable
```

В такой конфигурации все вызовы будут направлены SIP proxy-серверу. Если необходимо указать другое направление для исходящих вызовов, то необходимо проделать следующее:

Создать план нумерации, см. раздел Пример настройки плана нумерации.

Далее созданный план маршрутизации, необходимо присвоить SIP-профилю:

```
esr(config)# sip profile 1
esr(config-sip-profile)# dialplan pattern firstDialplan
```

На этом настройка плана нумерации для SIP-профиля закончена.

Активация SIP-профиля:

```
esr-12v(config-sip-profile)# enable
```

На этом минимально необходимая настройка SIP-профиля закончена:

```
esr(config-sip-profile)# exit
```

Следующим этапом является настройка абонентских портов:

```
esr(config)# interface voice-port 1
```

Указать абонентский номер:

```
esr(config-voice-port-fxs)# sip user phone 4101
```

Указать отображаемое имя:

```
esr(config-voice-port-fxs)# sip user display-name user-one
```

Используемый SIP-профиль:

```
esr(config-voice-port-fxs)# profile sip 1
```

Настройка логина и пароля для аутентификации:

```
esr(config-voice-port-fxs)# authentication name login-4101
esr(config-voice-port-fxs)# authentication password superpassword
```

На этом минимальная настройка абонентского порта закончена:

```
esr(config-voice-port-fxs)# exit
```

22.7 Пример настройки плана нумерации

Задача:

Настроить план нумерации так, чтобы вызовы на локальных (подключенных к данному ESR-12V) коммутировались локально, а вызовы на все остальные направления через SIP-proxy.

Решение:

Создать план нумерации:

```
esr(config)# dialplan pattern firstDialplan
```

План нумерации задается при помощи регулярных выражений:

```
esr(config-dial-ruleset)# pattern "<regular expressions>"
```

Для задачи, обозначенной выше "<*regular* expressions>" будет иметь вид:

“S5, L5 (410[1-3]@{local} | [xABCD*#].S)”

где:

- **410[1-3]@{ local}** – вызовы на номера 4101, 4102, 4103 будут коммутироваться локально;
- **[xABCD*#]. S** – вызовы на все остальные номера будут направлены к SIP-прокси.

Активировать план нумерации:

```
esr(config-dial-ruleset)# enable
```

Настройка плана нумерации закончена.

```
esr(config-dial-ruleset)# exit
```

Структура регулярного выражения:
Sxx, Lxx ( ),

где:

- **xx** – произвольные значения таймеров S и L;
- **()** – границы плана нумерации.

Основой являются обозначения для записи последовательности набранных цифр. Последовательность цифр записывается с помощью нескольких обозначений: цифры, набираемые с клавиатуры телефона: 0, 1, 2, 3, ..., 9, # и *.

Использование символа # в плане нумерации может блокировать завершение набора с помощью этой клавиши.

Последовательность цифр, заключённая в квадратные скобки, соответствует любому из заключённых в скобки символу.

- Пример: ([1239]) – соответствует любой из цифр 1, 2, 3 или 9.
  Через тире может быть указан диапазон символов. Чаще всего используется внутри квадратных скобок.
- Пример 1: (1-5) – любая цифра от 1 до 5.
- Пример 2: ([1-39]) – пример из предыдущего пункта с иной формой записи.
  Символ X соответствует любой цифре от 0 до 9.
- Пример: (1XX) – любой трёхзначный номер, начинающийся на 1.
  «.» – повторение предыдущего символа от 0 до бесконечности раз.
  «+» – повторение предыдущего символа от 1 до бесконечности раз.
  {a,b} – повторение предыдущего символа от a до b раз;
  {a,} – повторение предыдущего символа не меньше a раз;
  {,b} – повторение предыдущего символа не больше b раз.
- Пример: (810X.) – международный номер с любым количеством цифр.
  Настройки, влияющие на обработку плана нумерации:
- Interdigit Long Timer (буква «L» в записи плана нумерации) – время ожидания ввода следующей цифры в том случае, если нет шаблонов, подходящих под набранную комбинацию;
- Interdigit Short Timer (буква «S» в записи плана нумерации) – время ожидания ввода следующей цифры, если с набранной комбинацией полностью совпадает хотя бы один шаблон и при этом имеется еще хотя бы один шаблон, до полного совпадения с которым необходимо осуществить донабор номера.

Дополнительные возможности:

1. Замена набранной последовательности
   Синтаксис: *<arg1:arg2>*
   Данная возможность позволяет заменить набранную последовательность на любую последовательность набираемых символов. При этом второй аргумент должен быть указан определённым значением, оба аргумента могут быть пустыми.
   - Пример: (<83812:> XXXXXX) – данная запись будет соответствовать набранным цифрам 83812, но эта последовательность будет опущена и не будет передана на SIP-сервер.
2. Вставка тона в набор
   При выходе на межгород (в офисных станциях – на город) привычно слышать ответ станции, что можно реализовать вставкой запятой в нужную позицию последовательности цифр.
   - Пример: (8, 770) – при наборе номера 8770 после цифры 8 будет выдан непрерывный тон.
3. Запрет набора номера
   Если в конце шаблона номера добавить восклицательный знак '!', то набор номеров, соответствующих шаблону, будет заблокирован.
   - Пример: (8 10X xxxxxxx ! | 8 xxx xxxxxxx) – выражение разрешает набор только междугородних номеров и исключает международные вызовы.
4. Замена значений таймеров набора номера
   Значения таймеров могут быть назначены как для всего плана нумерации, так и для

определённого шаблона. Буква «S» отвечает за установку *«Interdigit Short Timer»* , а «L» – за *«Interdigit Long Timer»* . Значения таймеров может быть указано для всех шаблонов в плане нумерации, если значения перечислены до открывающейся круглой скобки.

- Пример: S4 (8XXX.) или S4,L8 (XXX)
  Если эти значения указаны только в одной из последовательностей, то действуют только для неё. Также в этом случае не надо ставить двоеточие между ключом и значением таймаута, значение может быть расположено в любом месте шаблона.
- Пример: (S4 8XXX. | XXX) или ([1-5] XX S0) – запись вызовет мгновенную передачу вызова при наборе трехзначного номера, начинающегося на 1,2, … , 5.

5. Набор по прямому адресу (IP Dialing)
   Символ «@», поставленный после номера, означает, что далее будет указан адрес сервера, на который будет отправлен вызов на набранный номер. Рекомендуется использовать *«IP Dialing»*, а также приём и передачу вызовов без регистрации *(« Call Without Reg », « Answer Without Reg »*). Это может помочь в случае отказа сервера.
   Кроме того, формат адреса с IP Dialing может быть использован в номерах, предназначенных для переадресации звонков.
   - Пример 1: (8 xxx xxxxxxx) – 11-значный номер, начинающийся на 8.
   - Пример 2: (8 xxx xxxxxxx | <:8495> xxxxxxx) – 11-значный номер, начинающийся на 8, если введён семизначный, то добавить к передаваемому номеру 8495.
   - Пример 3: (0[123] | 8 [2-9]xx [2-9]xxxxxx) – набор номеров экстренных служб, а так же некоторого странного набора междугородних номеров.
   - Пример 4: (S0 <:82125551234>) – быстрый набор указанного номера, аналог режима «Hotline» на других шлюзах.
   - Пример 5: (S5 <:1000> | xxxx) – данный план нумерации позволяет набрать любой номер, состоящий из цифр, а если ничего не введено в течение 5 секунд, вызвать номер 1000 (допустим, это секретарь).
   - Пример 6: (8, 10x.|1xx@10.110.60.51:5060) – данный план нумерации позволяет набирать номера начинающиеся на 810 и содержащие как минимум одну цифру после "810". После ввода 8 будет выдан сигнал "ответ станции". А также набор трехзначных номеров, начинающихся на "1", Invite на которые будет отправлен на IP-адрес 10.110.60.51 и порт 5060.
   - Пример 7: (S3 *xx#|#xx#|#xx#|*xx*x+#) – управление и использование ДВО.
     Иногда может потребоваться совершать звонки локально внутри устройства. При этом, если IP-адрес устройства не известен или периодически изменяется, удобно использовать в качестве адреса сервера зарезервированное слово «{local}», что означает отправку соответствующей последовательности цифр на собственный адрес устройства.
   - Пример: (123@{local}) – вызов на номер 123 будет обработан локально внутри устройства.

22.8 Настройка FXO-порта

Задача:

Добавить возможность совершения вызова абонента ТфОП через FXO-порт ESR-12V.

Решение:

Активировать FXO-порт:

```
esr(config)# interface voice-port 4
```

Указать номер FXO-порта, он же префикс выхода на ТфОП:

```
esr(config-voice-port-fxo)# sip user phone 9
```

Указать UDP-порт, с которого и на который FXO-комплект будет отправлять и принимать SIP-сообщения:

```
esr(config-voice-port-fxo)# sip port 5064
```

Указать отображаемое имя:

```
esr(config-voice-port-fxo)# sip user display-name user-one
```

Настройка логина и пароля для аутентификации:

```
esr(config-voice-port-fxo)# authentication name login-9
esr(config-voice-port-fxo)# authentication password superpassword
```

Назначить SIP-профиль FXO-порту:

```
esr(config-voice-port-fxo)# profile sip 1
```

Разрешить передачу номера в ТфОП:

```
esr(config-voice-port-fxo)# pstn transmit-number
```

Запретить передачу префикса:

```
esr(config-voice-port-fxo)# no pstn transmit-prefix
```

Для работы исходящих вызовов необходимо в настройках плана нумерации указать следующее правило, которое означает, что исходящие вызовы на номера имеющие префикс 9, маршрутизируются локально на FXO-комплект:

9x.@{local}:5064

На этом минимальная настройка исходящих вызовов на ТфОП закончена. Для того чтобы совершить вызов в ТфОП, нужно набрать номер вызываемого абонента с указанным префиксом (телефонный номер FXO-комплекта).

Для того чтобы принимать вызовы с ТфОП, необходимо выбрать абонента, на которого будут поступать все вызовы их ТфОП, допустим, это будет абонент с номером 305.

Активировать услугу «Hostline PSTN to IP»:

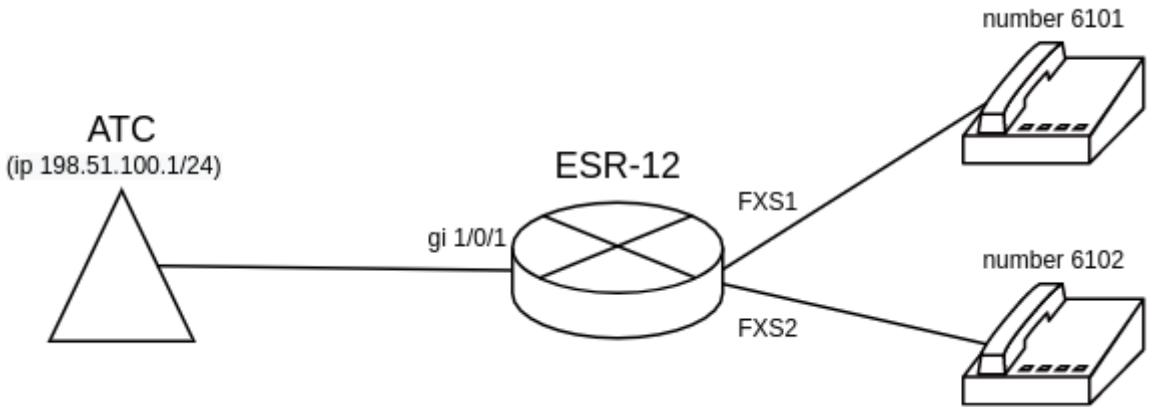
```
esr(config-voice-port-fxo)# hotline ipt
```

Указать номер абонента, который будет получать вызовы с ТфОП:

```
esr(config-voice-port-fxo)# hotline number ipt 305
```

22.9 Пример настройки voip для регистрации FXS-портов на внешнем sip-сервере

Схема:



Задача:

Настроить voip для регистрации FXS-портов на внешнем sip-сервере.

Решение:

Настроим sip-профиль. Необходимо настроить proxy-server для регистрации телефонов, подключенных к FXS-портам:

```
esr(config)# sip profile 1
esr(config-sip-profile)# enable
esr(config-sip-profile)# sip-domain address 198.51.100.1
esr(config-sip-profile)# proxy primary
esr(config-voip-sip-proxy)# enable
esr(config-voip-sip-proxy)# ip address proxy-server 198.51.100.1
esr(config-voip-sip-proxy)# registration
esr(config-voip-sip-proxy)# ip address registration-server 198.51.100.1
esr(config-voip-sip-proxy)# exit
esr(config-sip-profile)# exit
esr(config)#
```

Настроим FXS-порты. Укажем номер, параметры для аутентификации на внешнем сервере и sip-профиль:

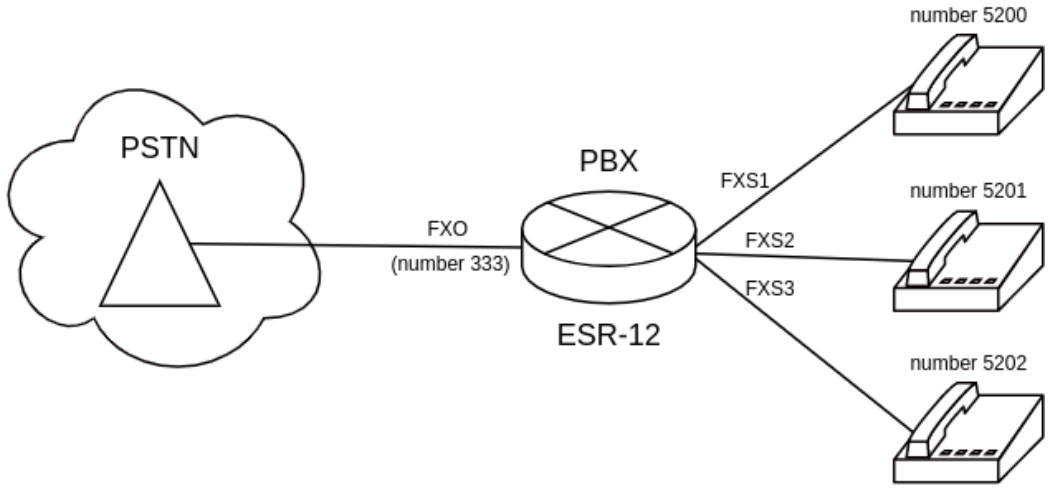
```
esr(config)# interface voice-port 1
esr(config-voice-port-fxs)# sip user phone 6101
esr(config-voice-port-fxs)# authentication name as-phone
esr(config-voice-port-fxs)# authentication password password
esr(config-voice-port-fxs)# profile sip 1
esr(config-voice-port-fxs)# exit
esr(config)# interface voice-port 2
esr(config-voice-port-fxs)# sip user phone 6102
esr(config-voice-port-fxs)# authentication name as-phone
esr(config-voice-port-fxs)# authentication password password
esr(config-voice-port-fxs)# profile sip 1
esr(config-voice-port-fxs)# exit
esr(config)#
```

Для регистрации и прохождения voip-трафика за nat необходимо включить на маршрутизаторе tracking и nat для sip, и включить service-voip routing на интерфейсе, через который доступен sip-сервер:

```
esr(config)# ip firewall sessions tracking sip
esr(config)# nat alg sip
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# service-voip routing
esr(config-if-gi)# exit
esr(config)#
```

22.10 Пример настройки voip на внутреннем pbx-сервере

Схема:



Задача:

Настроить регистрацию телефонов, подключенных к FXS-порту, а также настроить регистрацию номера телефонной линии, подключенной к FXO-порту. Также необходимо настроить перевод звонков с FXO-порта на телефон с номером 5200.

Решение:

Настройка PBX.

Создадим pbx-сервер:

```
esr(config)# pbx
esr(config-pbx)#
```

> ⚠ **Структура регулярного выражения pattern описана в разделе** Пример настройки плана нумерации**.**

Настроим контекст маршрутизации для FXO-порта (пример плана нумерации для перевода вызова на 5200-5202):

```
esr(config-pbx)# ruleset FXO
esr(config-pbx-ruleset)# rule 1
esr(config-pbx-rule)# pattern '_X.,1,Dial(SIP/5200&SIP/5201&SIP/5202)'
esr(config-pbx-rule)# enable
esr(config-pbx-rule)# exit
esr(config-pbx-ruleset)# exit
esr(config-pbx)#
```

Настроим контекст маршрутизации для FXS-портов (пример плана нумерации для набора номера 5200-5202):

```
esr(config-pbx)# ruleset main_rule
esr(config-pbx-ruleset)# rule 1
esr(config-pbx-rule)# pattern '_520[0-3],1,Dial(SIP/${EXTEN},,t)'
esr(config-pbx-rule)# enable
esr(config-pbx-rule)# exit
esr(config-pbx-ruleset)# exit
esr(config-pbx)#
```

Настроим sip-профиль для FXS-портов. Необходимо указать тип клиента, включить необходимые кодеки и подключить контекст маршрутизации:

```
esr(config-pbx)# profile fxs_ports
esr(config-pbx-profile)# client friend
esr(config-pbx-profile)# codec allow g711a
esr(config-pbx-profile)# codec allow g711u
esr(config-pbx-profile)# codec allow g729
esr(config-pbx-profile)# ruleset main_rule
esr(config-pbx-profile)# exit
esr(config-pbx)#
```

Настроим sip-профиль для FXO-портов. Необходимо указать тип клиента, включить необходимые кодеки, настроить invite-port, подключить контекст маршрутизации:

```
esr(config-pbx)# profile fxo_ports
esr(config-pbx-profile)# client friend
esr(config-pbx-profile)# codec allow g711a
esr(config-pbx-profile)# codec allow g711u
esr(config-pbx-profile)# security level invite-port
esr(config-pbx-profile)# ruleset FXO
esr(config-pbx-profile)# exit
esr(config-pbx)#
```

Настроим абонентов на сервере PBX:

```
esr(config-pbx)# user 5200
esr(config-pbx-user)# profile fxs_ports
esr(config-pbx-user)# exit
esr(config-pbx)# user 5201
esr(config-pbx-user)# profile fxs_ports
esr(config-pbx-user)# exit
esr(config-pbx)# user 5202
esr(config-pbx-user)# profile fxs_ports
esr(config-pbx-user)# exit
esr(config-pbx)# user 333
esr(config-pbx-user)# profile fxo_ports
esr(config-pbx-user)# exit
esr(config-pbx)#
```

Включим PBX-сервер:

```
esr(config-pbx)# enable
esr(config-pbx)# exit
esr(config)#
```

Настроим FXS-порты. Укажем номер и sip-профиль:

```
esr(config)# interface voice-port 1
esr(config-voice-port-fxs)# sip user phone 5200
esr(config-voice-port-fxs)# profile pbx fxs_ports
esr(config-voice-port-fxs)# exit
esr(config)# interface voice-port 2
esr(config-voice-port-fxs)# sip user phone 5201
esr(config-voice-port-fxs)# profile pbx fxs_ports
esr(config-voice-port-fxs)# exit
esr(config)# interface voice-port 3
esr(config-voice-port-fxs)# sip user phone 5202
esr(config-voice-port-fxs)# profile pbx fxs_ports
esr(config-voice-port-fxs)# exit
esr(config)#
```

Настроим FXO-порт. Укажем номер и sip-profile, выключим caller-id, активируем услугу «Hostline PSTN to IP»: и укажем номер абонента, который будет получать вызовы с ТфОП:

```
esr(config)# interface voice-port 4
esr(config-voice-port-fxo)# sip user phone 333
esr(config-voice-port-fxo)# profile pbx fxo_ports
esr(config-voice-port-fxo)# caller-id mode off
esr(config-voice-port-fxo)# hotline ipt
esr(config-voice-port-fxo)# hotline number ipt 5200
esr(config-voice-port-fxo)# exit
esr(config)#
```

23 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. Делаем это в режиме конфигурирования VRF:

```
esr(config)# ip vrf <NAME>
esr(config-vrf)# ip protocols ospf max-routes 12000
esr(config-vrf)# ip protocols bgp max-routes 1200000
esr(config-vrf)# end
```

Закрываются сессии SSH/Telnet, проходящие через маршрутизатор ESR

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):

```
esr(config)# ip firewall sessions tcp-estabilished-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:

```
esr# clear ip firewall session
```

Не поднимается LACP на портах XG ESR-1000/1200/1500/1700

По умолчанию на port-channel режим speed 1000M, необходимо выставить speed 10G.

```
esr(config)# interface port-channel 1
esr(config-port-channel)# speed 10G
```

Как полностью очистить конфигурация ESR и как сбросить на заводскую конфигурацию?

Очистка конфигурации происходит путем копирования пустой конфигурации в candidate-config и применения его в running-config.

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

Процесс сброса на заводскую конфигурацию аналогичен.

```
esr# copy system:factory-config system:candidate-config
```

Как привязать subinterface к созданным VLAN?

При создании саб-интерфейса VLAN создается и привязывается автоматически (прямая зависимость индекс sub – VID).

```
esr(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 ESR для анализа трафика?

В маршрутизаторах серии ESR реализована возможность анализировать трафик на интерфейсах из CLI. Сниффер запускается командой monitor.

```
esr# 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.

```
esr(config)# ip prefix-list eltex
esr(config-pl)# permit default-route
```

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:

```
esr(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/".

```
esr# 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:

```
esr# copy flash:data/temp.txt system:candidate-config
esr# copy flash:backup/config_20190918_164455 system:candidate-config
```

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-co.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 или проконсультироваться у инженеров Сервисного центра на техническом форуме:

Официальный сайт компании: https://eltex-co.ru

Технический форум: https://eltex-co.ru/forum

База знаний: https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base

Центр загрузок: https://eltex-co.ru/support/downloads