Межсетевые экраны серии ESR

ESR-20, ESR-21, ESR-1500, ESR-1511

Руководство по эксплуатации, версия ПО 1.5

РПЛТ.465614.151РЭ

Версия документа	Дата выпуска	Содержание изменений
Версия 1.0	03.06.2020	Первая публикация.
Версия программного обеспечения	**1.5**	

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

1.1 Аннотация

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

Сетевые экраны серии ESR могут использоваться на сетях крупных предприятиях и предприятиях малого и среднего бизнеса (SMB), в операторских сетях. Устройства обеспечивают высокую производительность, высокую пропускную способность и поддерживают функции защиты передаваемых данных.

В данном руководстве по эксплуатации изложены назначение, технические характеристики, функции, конструктивное исполнение, порядок установки, рекомендации по начальной настройке и обновлению программного обеспечения межсетевого экрана серии ESR (далее маршрутизатор или устройство).

1.2 Целевая аудитория

Данное руководство пользователя предназначено для технического персонала, выполняющего установку, настройку и мониторинг устройств 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.

1.3 Условные обозначения

Обозначение	Описание
Курсив Calibri	Курсивом Calibri указываются переменные или параметры, которые необходимо заменить соответствующим словом или строкой.
Полужирный курсив	Полужирным шрифтом выделены примечания и предупреждения.
<Полужирный курсив>	В угловых скобках указываются названия клавиш на клавиатуре.
Courier New	Полужирным Шрифтом Courier New записаны примеры ввода команд.
Courier New	Шрифтом Courier New в рамке с тенью указаны результаты выполнения команд.
[ ]	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.
«|»	Данный знак в описании команды обозначает «или».

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.

2 ОПИСАНИЕ ИЗДЕЛИЯ

2.1 Назначение

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 своей сетевой инфраструктуры и 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.

2.2 Функции

2.2.1 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.

2.2.2 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.

2.2.3 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).

2.2.4 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: RIP, OSPFv2, OSPFv3, 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.
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 межсетевым экраном на компьютер пользователя в локальной сети, имеющий внутренний адрес и потому недоступный извне сети непосредственно (без NAT).

2.2.5 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 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 – туннели, использующиеся для организации удаленного доступа клиент-сервер.

2.2.6 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.

2.2.7 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.

2.3 Основные технические характеристики

Основные технические параметры маршрутизатора приведены в таблице 8.

Таблица 8 – Основные технические характеристики

Общие параметры		
Пакетный процессор	ESR-1511	Broadcom XLP532
	ESR-1500	Broadcom XLP516
	ESR-21 ESR-20	Broadcom NorthStar2
Интерфейсы	ESR-1511	4 x Ethernet 10/100/1000BASE-T 4 x Ethernet 10/100/1000BASE-T/1000BASE-X Combo 4 x 10GBASE-R/1000BASE-X (SFP+/SFP) 2 x 40GBASE-SR4/LR4 (QSFP+)
	ESR-1500	4 x Ethernet 10/100/1000BASE-T 4 x Ethernet 10/100/1000BASE-T/1000BASE-X Combo 4 x 10GBASE-R/1000BASE-X (SFP+/SFP)
	ESR-21	8 x Ethernet 10/100/1000BASE-T, 4 x 1000BASE-X (SFP), 3 x RS-232
	ESR-20	2 x Ethernet 10/100/1000BASE-T, 2 x Ethernet 10/100/1000BASE-T/1000BASE-X Combo
Типы оптических трансиверов	ESR-1511	1000BASE-X SFP, 10GBASE-R SFP+, 40GBASE-SR4/LR4 QSFP+
	ESR-1500	1000BASE-X SFP, 10GBASE-R SFP+
	ESR-21 ESR-20	1000BASE-X 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-1511	240 Гбит/с
	ESR-1500	160 Гбит/с
Скорость передачи данных	ESR-1511	- электрические интерфейсы 10/100/1000 Мбит/с - оптические интерфейсы 1/10/40 Гбит/с
	ESR-1500	- электрические интерфейсы 10/100/1000 Мбит/с - оптические интерфейсы 1/10 Гбит/с
	ESR-21 ESR-20	- электрические интерфейсы 10/100/1000 Мбит/с - оптические интерфейсы 1 Гбит/с
Таблица MAC-адресов	ESR-1511 ESR-1500	128k записей
	ESR-21 ESR-20	2k записей на бридж
Поддержка VLAN		до 4k активных VLAN в соответствии с 802.1Q
Количество L3 интерфейсов	ESR-1511 ESR-1500 ESR-21 ESR-20	4000
Количество маршрутов BGP	ESR-1511 ESR-1500	2,8M
	ESR-21 ESR-20	1,5M

Количество маршрутов OSPF	ESR-1511 ESR-1500	500k
	ESR-21 ESR-20	300k
Количество маршрутов RIP		10k
Количество статических маршрутов		11k
Размер базы FIB	ESR-1511 ESR-1500	1,7M
	ESR-21 ESR-20	1,5M
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 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-1511 ESR-1500	Сеть переменного тока: 220В+-20%, 50 Гц Сеть постоянного тока: -36 .. - 72В Варианты питания: - один источник питания постоянного или переменного тока; - два источника питания постоянного или переменного тока, с возможностью горячей замены.
	ESR-21 ESR-20	Сеть переменного тока: 220В+-20%, 50 Гц
Максимально потребляемая мощность	ESR-1511 ESR-1500	160 Вт
	ESR-21 ESR-20	25 Вт
Масса	ESR-1511 ESR-1500	не более 7 кг
	ESR-21	не более 3,15 кг
	ESR-20	не более 2 кг
Габаритные размеры (ШхВхГ)	ESR-1511 ESR-1500	430x425x44 мм
	ESR-21	430x225x44 мм
	ESR-20	267x212x44 мм
Интервал рабочих температур	ESR-1511 ESR-1500 ESR-21 ESR-20	от -10 до +45 °С

Интервал температуры хранения	от -40 до +70 °С
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

2.4 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.

2.4.1 Конструктивное исполнение ESR-1511, ESR-1500

2.4.1.1 Передняя панель устройств ESR-1511, ESR-1500

Внешний вид передней панели показан на рисунке 1.

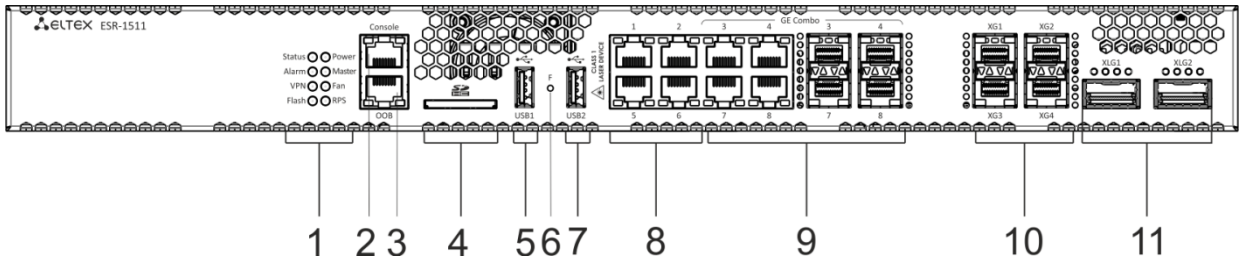

Рисунок 1 – Передняя панель ESR-1511, ESR-1500

В таблице 9 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели устройств ESR-1511, ESR-1500.

Таблица 9 – Описание разъемов, индикаторов и органов управления передней панели ESR-1511, ESR-1500

№	Элемент панели передней	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 для локального управления устройством.
3	OOB	Ethernet порт для управления маршрутизатором.
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/QSFP+ (только на ESR-1511)

2.4.1.2 Задняя панель устройств ESR-1511, ESR-1500

Внешний вид задней панели устройств ESR-1511, ESR-1500 приведен на рисунке 2.

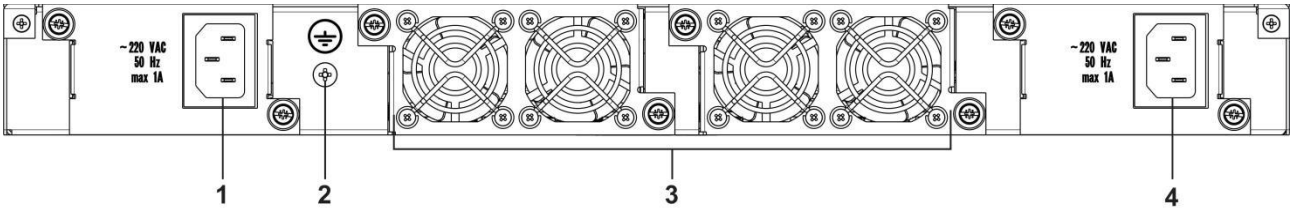

Рисунок 2 – Задняя панель ESR-1511, ESR-1500

В таблице 10 приведен перечень разъемов, расположенных на задней панели маршрутизатора.

Таблица 10 – Описание разъемов задней панели маршрутизатора

№	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.

2.4.1.3 Боковые панели устройств ESR-1511, ESR-1500

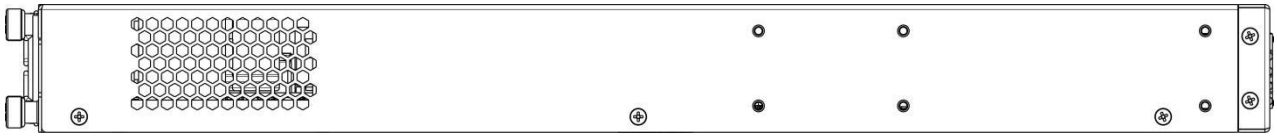

Рисунок 3 – Правая боковая панель маршрутизаторов ESR-1511, ESR-1500

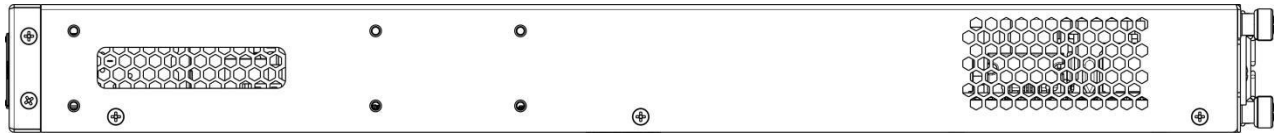

Рисунок 4 – Левая боковая панель маршрутизаторов ESR-1511, ESR-1500

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».

2.4.2 Конструктивное исполнение ESR-21

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

2.4.2.1 Передняя панель устройства ESR-21

Внешний вид передней панели показан на рисунке *5*.

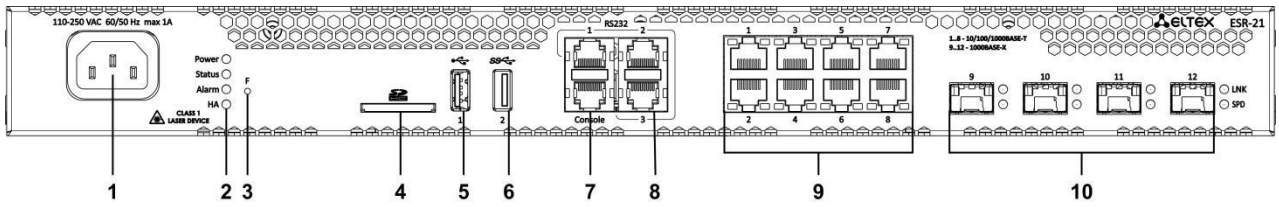

Рисунок 5 – Передняя панель ESR-21

В таблице 11 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели устройства ESR-21.

Таблица 11 – 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)
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 USB2.0 для подключения внешних USB-устройств
6	USB2	Разъем USB3.0 для подключения внешних USB-устройств
7	Console	Консольный порт 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)

2.4.2.2 Задняя панель устройств ESR-21

Внешний вид задней панели устройства ESR-21 показан на рисунке 6.

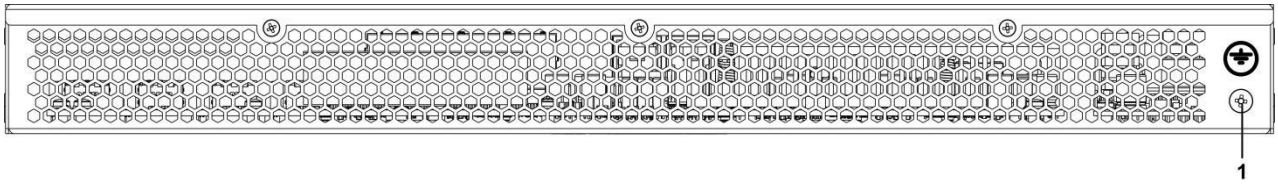

Рисунок 6 – Задняя панель ESR-21

В таблице 12 приведен перечень разъемов, расположенных на задней панели маршрутизатора.

Таблица 12 – Описание разъемов задней панели маршрутизатора

№	Описание
1	Клемма для заземления устройства.

2.4.2.3 Боковые панели устройства ESR-21

Внешний вид боковых панелей устройства ESR-21 приведен на рисунках 7 и 8.

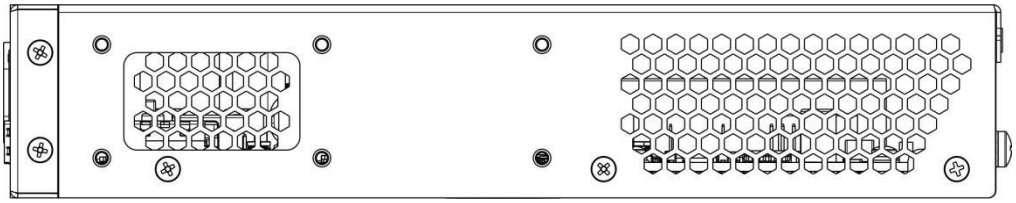

Рисунок 7 – Левая панель ESR-21

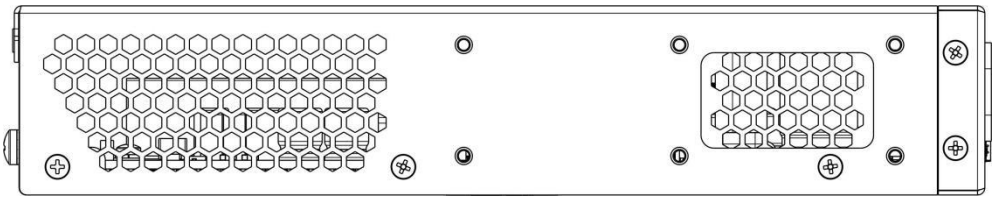

Рисунок 8 – Правая панель ESR-21

2.4.3 Конструктивное исполнение ESR-20

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

2.4.3.1 Передняя панель устройства ESR-20

Внешний вид передней панели показан на рисунке 9.

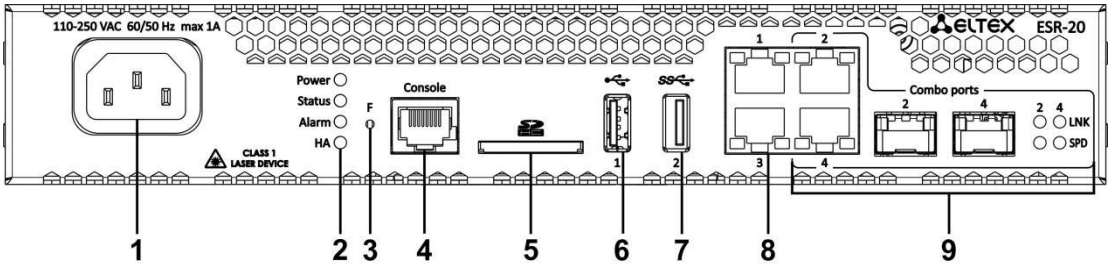

Рисунок 9 – Передняя панель ESR-20

В таблице 13 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели устройства ESR-20.

Таблица 13 – 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 для локального управления устройством.
5	SD	Разъем для установки SD-карт памяти.
6	USB1	Разъем USB2.0 для подключения внешних USB-устройств.
7	USB2	Разъем USB3.0 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.

2.4.3.2 Задняя панель устройств ESR-20

Внешний вид задней панели устройства ESR-20 показан на рисунке 10.

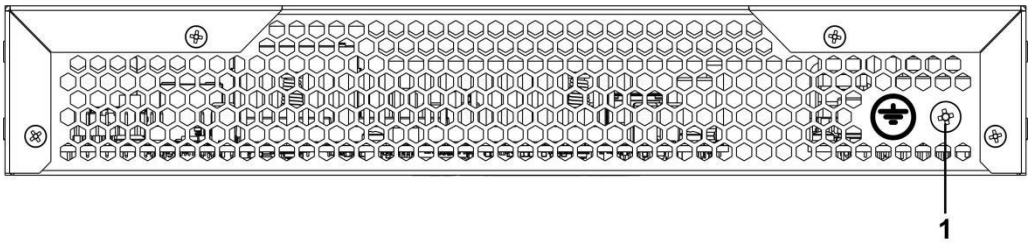

Рисунок 10 – Задняя панель ESR-20

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

Таблица 14 – Описание разъемов задней панели маршрутизатора

№	Описание
1	Клемма для заземления устройства.

2.4.3.3 Боковые панели устройства ESR-20

Внешний вид боковых панелей устройства ESR-20 приведен на рисунках 11 и 12.

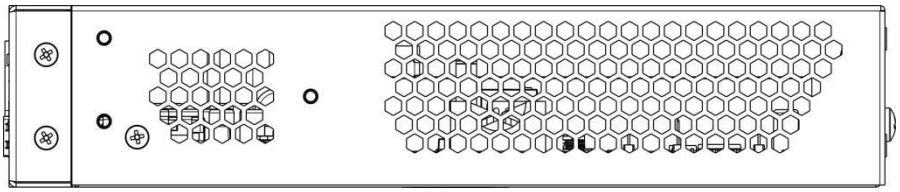

Рисунок 11 – Левая панель ESR-20

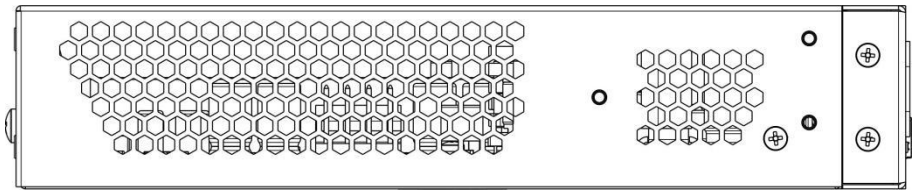

Рисунок 12 – Правая панель ESR-20

2.4.4 Световая индикация

2.4.4.1 Световая индикация 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 13. Состояние SFP-интерфейсов отображается двумя индикаторами RX/ACT и TX/ACT и указано на рисунке *14*. Значения световой индикации описаны в таблицах 15 и *16*, соответственно.

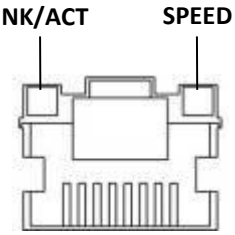

Рисунок 13 – Расположение индикаторов разъема RJ-45

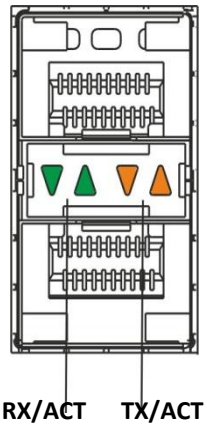

Рисунок 14 – Расположение индикаторов оптических интерфейсов

Таблица 15 – 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 16 – Световая индикация состояния SFP/SFP+ 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 17 – Состояния системных индикаторов

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Status	Индикатор текущего состояния устройства.	Зеленый	Устройство работает нормально.
		Оранжевый	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.	Оранжевый	Выполнение операций чтения/записи по команде «copy».
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.
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.

2.4.4.2 Световая индикация ESR-21/ESR-20

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

Таблица 18 – 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 100Мбит/с.
Горит постоянно	Горит постоянно	Установлено соединение на скорости 1000Мбит/с.
X	Мигание	Идет передача данных.

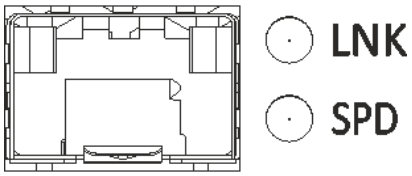

Рисунок 15 – Расположение индикаторов разъема SFP

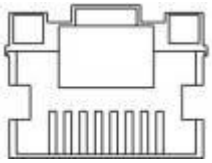

Рисунок 16 – Расположение индикаторов разъема RJ-45

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

Таблица 19 – 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.
		Оранжевый	Устройство находится в состоянии загрузки ПО.
Alarm	Индикатор наличия и уровня аварии устройства.	-	-
HA	Индикатор работы в режиме HA (не используется в текущей версии)	-	-

2.5 Комплект поставки

В базовый комплект поставки ESR-1511 входят:

- маршрутизатор ESR-1511;
- кабель питания;
- кабель для подключения к порту Console (RJ-45 – DB9F);
- комплект для крепления устройства в стойку 19”;
- документация.

В базовый комплект поставки ESR-1500 входят:

- маршрутизатор ESR-1500;
- кабель питания;
- кабель для подключения к порту Console (RJ-45 – DB9F);

- комплект для крепления устройства в стойку 19”;
- документация.

В базовый комплект поставки ESR-21 входят:

- маршрутизатор ESR-21;
- кабель питания;
- кабель для подключения к порту Console (RJ-45 – DB9F);
- комплект для крепления устройства в стойку 19”;
- документация.

В базовый комплект поставки ESR-20 входят:

- маршрутизатор ESR-20;
- кабель питания;
- кабель для подключения к порту Console (RJ-45 – DB9F);
- комплект для крепления устройства в стойку 19”;
- документация.

По заказу покупателя для ESR-1511, ESR-1500 в комплект поставки может быть включен модуль питания (PM160-220/12).

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

3 УСТАНОВКА И ПОДКЛЮЧЕНИЕ

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

3.1 Крепление кронштейнов

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

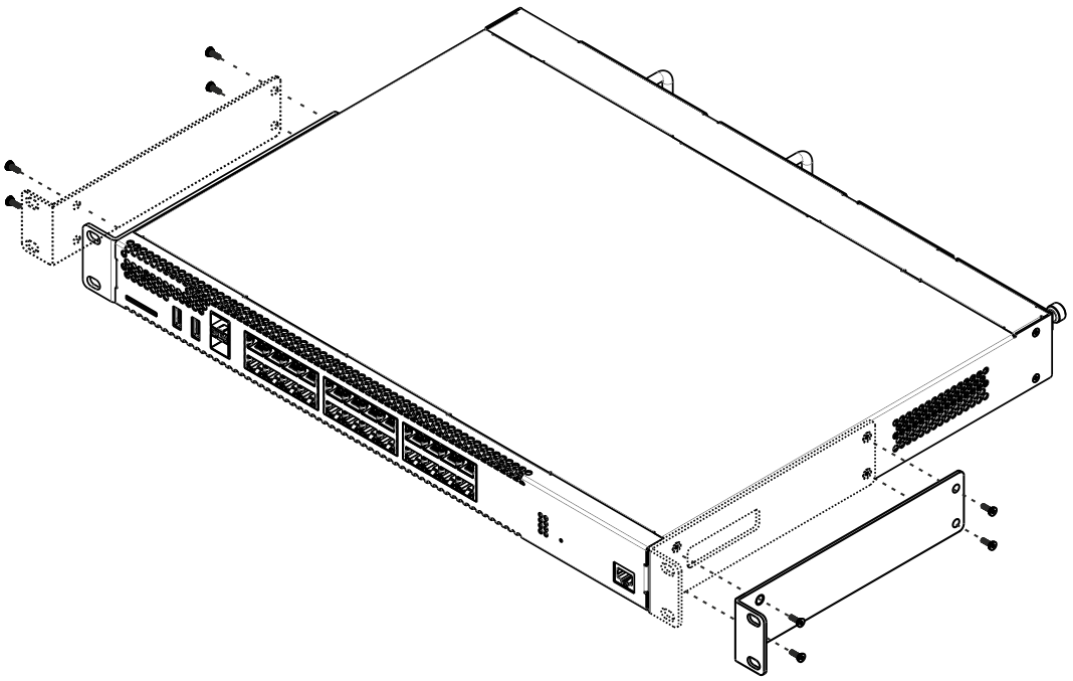

Рисунок 17 – Крепление кронштейнов

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.

3.2 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.

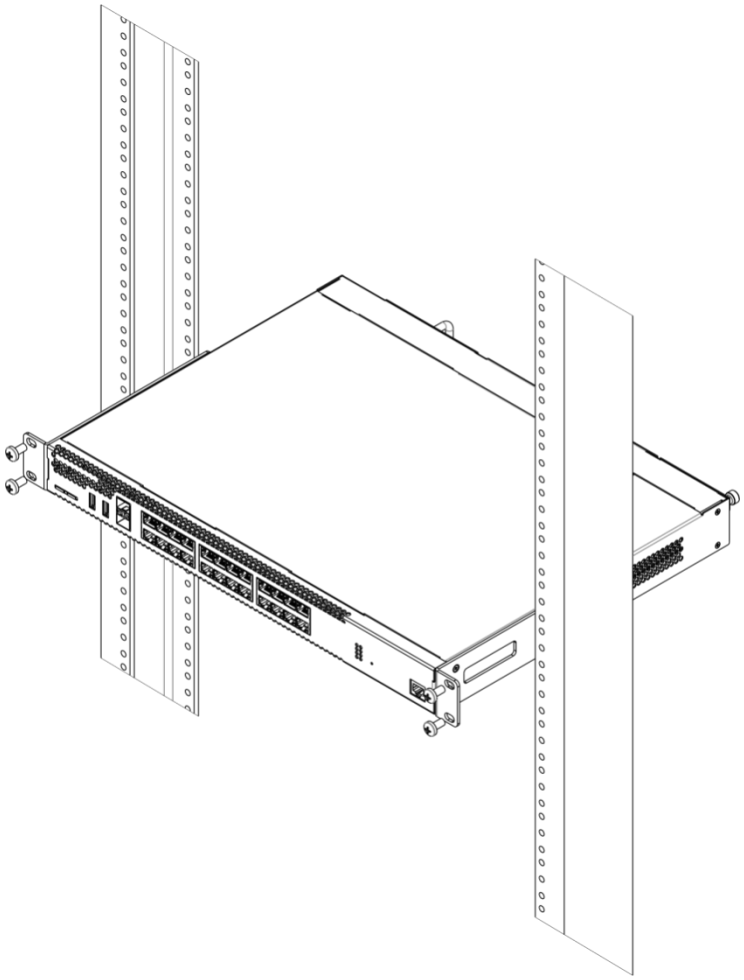

Рисунок 18 – Установка устройства в стойку

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.

3.3 Установка модулей питания ESR-1511, ESR-1500

Маршрутизаторы ESR-1511, ESR-1500 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, находящийся ближе к краю, считается основным, ближе к центру – резервным. Модули питания могут устанавливаться и извлекаться без выключения устройства. При установке или извлечении дополнительного модуля питания маршрутизатор продолжает работу без перезапуска.

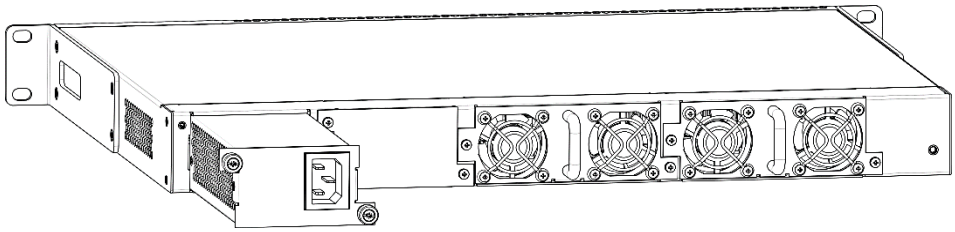

Рисунок 19 – Установка модулей питания

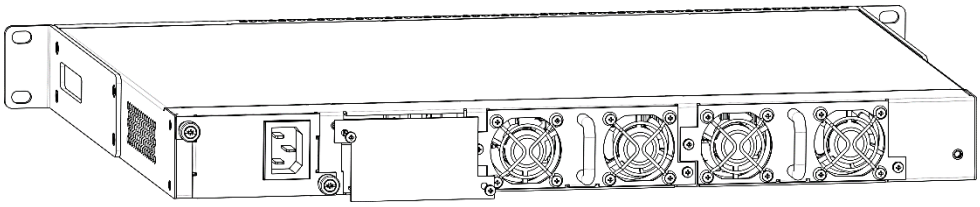

Рисунок 20 – Установка заглушки

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 2.4.4) или по диагностике, доступной через интерфейсы управления маршрутизатором.

3.4 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.

3.5 Установка и удаление SFP-трансиверов

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

3.5.1 Установка трансивера

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

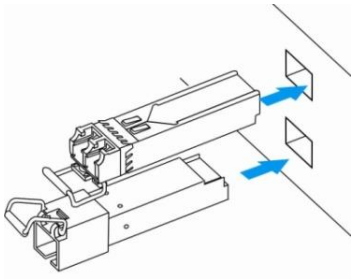

Рисунок 21 – Установка SFP-трансиверов

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

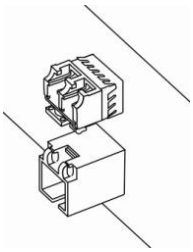

Рисунок 22 – Установленные SFP-трансиверы

3.5.2 Удаление трансивера

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

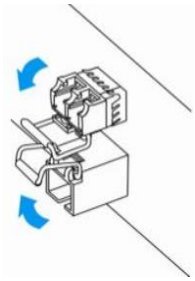

Рисунок 23 – Открытие защелки SFP-трансиверов

2. Извлеките модуль из слота.

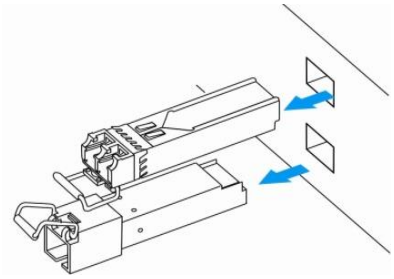

Рисунок 24 – Извлечение SFP-трансиверов

4 ИНТЕРФЕЙСЫ УПРАВЛЕНИЯ

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 ESR-20: GigabitEthernet 1/0/2-4;
для ESR-21: GigabitEthernet 1/0/2-12;
для ESR-1500: GigabitEthernet 1/0/2-8, TengigabitEthernet 1/0/2-4;
для ESR-1511: GigabitEthernet 1/0/2-8, TengigabitEthernet 1/0/2-4, FortygigabitEthernet 1/0/1-2.

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.

4.1 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 протоколу 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.

4.2 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 20 – 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 1Гбит/с	gigabitethernet <UNIT>/<SLOT>/<PORT> Пример обозначения: gigabitethernet 1/0/12 Примечание: Допускается использовать сокращенное наименование, например gi1/0/12.
Порты 10Гбит/с	tengigabitethernet <UNIT>/<SLOT>/<PORT> Пример обозначения: tengigabitethernet 1/0/2 Примечание: Допускается использовать сокращенное наименование, например te1/0/2.
Порты 40Гбит/с	fortygigabitethernet <UNIT>/<SLOT>/<PORT> Пример обозначения: fortygigabitethernet 1/0/2 Примечание: Допускается использовать сокращенное наименование, например fo1/0/2.
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.**
Субинтерфейсы	Обозначение субинтерфейса образуется из обозначения базового интерфейса и идентификатора (VLAN) субинтерфейса, разделенных точкой. Примеры обозначений: gigabitethernet 1/0/12.100 tengigabitethernet 1/0/2.123 port-channel 1.6 Примечание: Идентификатор субинтерфейса 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 port-channel 1.6.34 Примечание: 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
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

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 gi1/0/1-3,gi1/0/7,te1/0/1

4.3 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 21 – 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
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.

5 НАЧАЛЬНАЯ НАСТРОЙКА МАРШРУТИЗАТОРА

5.1 Заводская конфигурация маршрутизатора ESR

При отгрузке устройства потребителю на устройство загружена заводская конфигурация, которая включает минимально необходимые базовые настройки. Заводская конфигурация позволяет использовать маршрутизатор 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.

5.1.1 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 ESR-20: GigabitEthernet 1/0/1

для ESR-21: GigabitEthernet 1/0/1;

для ESR-1500: GigabitEthernet 1/0/1, TengigabitEthernet 1/0/1-2;

для ESR-1511: GigabitEthernet 1/0/1, TengigabitEthernet 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 ESR-20: GigabitEthernet 1/0/2-4;

для ESR-21: GigabitEthernet 1/0/2-12;

для ESR-1500: GigabitEthernet 1/0/2-8, TengigabitEthernet 1/0/3-4;

для ESR-1500: GigabitEthernet 1/0/2-8, TengigabitEthernet 1/0/3-4, FortygigabitEthernet 1/0/1-2.

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 22 – 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/23(Telnet), 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'. 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.

5.2 Подключение и конфигурирование маршрутизатора

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

Базовая настройка маршрутизатора 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.

5.2.1 Подключение к маршрутизатору

Предусмотрены следующие способы подключения к устройству:

5.2.1.1 Подключение по локальной сети Ethernet

При первоначальном старте маршрутизатор загружается с заводской конфигурацией. Описание заводской конфигурации приведено в разделе *5.1 Заводская конфигурация маршрутизатора* 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.

5.2.1.2 Подключение через консольный порт RS-232

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

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

Выполните следующие настройки интерфейса RS-232:

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

5.2.2 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].

5.2.3 Базовая настройка маршрутизатора

Процедура настройки маршрутизатора 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.

5.2.3.1 Изменение пароля пользователя «admin»

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

Учетная запись techsupport необходима для удаленного обслуживания сервисным центром;

Учетная запись remote - аутентификация RADIUS, TACACS+, LDAP;

Удалить пользователей admin, techsupport, remote нельзя. Можно только сменить пароль и уровень привилегий.

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
```

5.2.3.2 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
```

5.2.3.3 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>**.

5.2.3.4 Настройка параметров публичной сети

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

Пример команд настройки статического IP-адреса для субинтерфейса **GigabitEthernet 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 **GigabitEthernet 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
```

5.2.3.5 Настройка удаленного доступа к маршрутизатору

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

При конфигурировании доступа к маршрутизатору правила создаются для пары зон:

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

Для создания разрешающего правила используются следующие команды:

```
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 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
```

6 ОБНОВЛЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

6.1 Обновление программного обеспечения средствами системы

Для обновления программного обеспечения понадобится один из следующих серверов: TFTP, FTP, SCP, SFTP. На сервер должны быть помещены файлы программного обеспечения маршрутизатора, полученные от производителя.

На маршрутизаторе 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 конвертируется в соответствии с новой версией.

При загрузке маршрутизатора 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 6.2.

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 файл дистрибутивный файл программного обеспечения.

2. Маршрутизатор должен быть подготовлен к работе в соответствии с требованиями документации. Конфигурация маршрутизатора должна позволять обмениваться данными по протоколам TFTP/FTP/SCP и ICMP с сервером. При этом должна быть учтена принадлежность сервера к зонам безопасности маршрутизатора.

3. Подключитесь к маршрутизатору локально через консольный порт Console или удаленно, используя проколы Telnet или SSH.

   Проверьте доступность сервера для маршрутизатора, используя команду *ping* на маршрутизаторе. Если сервер не доступен – проверьте правильность настроек маршрутизатора и состояние сетевых интерфейсов сервера.

4. Для обновления программного обеспечения маршрутизатора введите следующую команду. В качестве параметра *<server>* должен быть указан IP-адрес используемого сервера. Для обновления с FTP, SFTP 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 маршрутизатор 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 обновим 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, SFTP 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
```

6.2 Обновление программного обеспечения (firmware) из вторичного загрузчика

Для обновления програмного обеспечения на ESR-20/21 возможно использовать любой ethernet-интерфейс маршрутизатора.

Для обновления програмного обеспечения на ESR-1500/1511 возможно использовать только OOB-интерфейс маршрутизатора.

Программное обеспечение маршрутизатора можно обновить из начального загрузчика следующим образом:

1. Остановите загрузку устройства после окончания инициализации маршрутизатора 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
```

3. Укажите IP-адрес маршрутизатора:

```
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
```

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

6.3 Обновление вторичного загрузчика (U-Boot)

Вторичный загрузчик занимается инициализацией NAND и маршрутизатора. 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 маршрутизатора:

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

Для обновления вторичного загрузчика на ESR-20/21 возможно использовать любой ethernet-интерфейс маршрутизатора.

Для обновления вторичного загрузчика на ESR-1500/1511 возможно использовать только OOB-интерфейс маршрутизатора.

Процедура обновления ПО:

1. Остановите загрузку устройства после окончания инициализации маршрутизатора 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 10.100.100.2
```

3. Укажите IP-адрес маршрутизатора:

```
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
```

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

6. Запустите процедуру обновления программного обеспечения:

```
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 маршрутизатор:

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

6.4 Обновление первичного загрузчика (BL1 для ESR-20/21 и X-Loader для ESR-1500/1511)

Первичный загрузчик занимается первоначальной инициализацией процессора, а также инициализацией и тестированием RAM-памяти. При обновлении, новый файл первичного загрузчика сохраняется на flash на месте старого.

Для обновления первичного загрузчика на ESR-20/21 возможно использовать любой ethernet-интерфейс маршрутизатора.

Для обновления первичного загрузчика на ESR-1500/1511 возможно использовать только OOB-интерфейс маршрутизатора.

Процедура обновления первичного загрузчика:

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

Для ESR-1500/1511:

```
nae-0-2: PHY is Marvell 88E1514 (1410dd1)
SMC Endian Test:5a745a74
nae-0-0, nae-0-1, nae-0-2 [PRIME]
Init I2C: 1
Set default values for mtdids and mtdparts variables
Temp: MAX6657 temperature (int) 40 C
Temp: MAX6657 temperature (ext) 42 C
Temp: LM75/0 temperature          38 C
Temp: LM75/1 temperature          33 C
Temp: LM75/2 temperature          42 C
CPLD(MAIN): FW Revision 3
```

```
CPLD(SEQ) : FW Revision 3

On node 0 Successfully Loaded Power Management UCORE
Hit any key to stop autoboot:  2
```

Для ESR-20/21:

```
 Net:   Registering Northstar2 GMAC ethernet.....
 Broadcom BCM IPROC Ethernet driver 0.1
 |eth_data->mac:0
 Using GMAC0 (0000000061000000)
 NICPM_PADRING_CFG:1627586564, default 0x8000000
 NICPM_PADRING_CFG:1627586564, value 0x74000000
 NICPM_IOMUX_CTRL:1627586568, default 0x196e800
 et0: ethHw_chipAttach: Chip ID: 0x11; phyaddr: 0x1
 ***ICFG_IPROC_IOPAD_CTRL_11 660009dc val:0x1303
 ***Read CMIC_MIIM_SCAN_CTRL 66020008 val:0x30001000
 ***Read CMIC_RATE_ADJUST_EXT_MDIO 66020000 val:0x10008

 MAC: a8:f9:4b:ac:4d:38

 Hit any key to stop autoboot:  2
```

2. Укажите IP-адрес TFTP-сервера:

```
BRCM.XLP532A1.u-boot# serverip 192.168.32.180
```

3. Укажите IP-адрес маршрутизатора:

```
BRCM.XLP532A1.u-boot# ipaddr 192.168.32.2
```

4. Укажите имя файла загрузчика на TFTP-сервере:

Для ESR-1500/1511:

```
BRCM.XLP532A1.u-boot# xload_file xload.bin
```

Для ESR-1500/1511:

```
u-boot> bl1_file bl1.bin
```

5. Для будущих обновлений, можно сохранить окружение командой:

```
BRCM.XLP532A1.u-boot# saveenv
```

6. Запустите процедуру обновления программного обеспечения:

Для ESR-1500/1511:

```
BRCM.XLP532A1.u-boot# run tftp_update_xload

Using nae-0-2 device
TFTP from server 192.168.32.180; our IP address is 192.168.32.2
Filename 'xload.bin'.
Load address: 0xa800000078020000
Loading: TftpStart:TftpTimeoutMsecs = 10000, TftpTimeoutCountMax = 4
#########
done
Bytes transferred = 120144 (1d550 hex)
SF: Detected MX25L128xxF with page size 256, total 16777216 bytes
0x4000 KiB MX25L128xxF at 0:0 is now current device
X-Loader update OK
```

Для ESR-20/21:

```
u-boot> run tftp_update_bl1
```

```
bcmiproc_eth-0 no link
gi1_3 no link
Using gi1_1 device
TFTP from server 192.168.32.180; our IP address is 192.168.32.2
Filename 'bl1.bin'.
Load address: 0x90000000
Loading: bnxt INFO: link_status_change
bnxt INFO: NIC Link is Up, 1000 Mbps full duplex, Flow control: ON - receive &
transmit
#########
         6 MiB/s
done
Bytes transferred = 119040 (1d100 hex)
  Download file 'bl1.bin': OK
  Check BL1 image ... OK
SF: Detected MX25L12805 with page size 256 Bytes, erase size 64 KiB, total 16 MiB
....
SF: 262144 bytes @ 0x0 Erased: OK
device 0 offset 0x0, size 0x1d100
SF: 119040 bytes @ 0x0 Written: OK

Bootloader1 update: OK
```

7. Перезагрузите маршрутизатор:

```
BRCM.XLP532A1.u-boot# reset
```

6.5 Выгрузка программного обеспечения и загрузчиков

Для создания резервной копии программного обеспечения (firmware) введите следующую команду. В качестве параметра *<server>* должен быть указан IP-адрес используемого сервера. Для копирования на FTP, SFTP или SCP-сервера потребуется ввести имя пользователя (параметр *<user>*) и пароль (параметр *<password>*). В качестве параметра *<file_name>* укажите имя, с которым необходимо сохранить файл программного обеспечения на сервере (при использовании SCP нужно указать полный путь – параметр *<folder>*). После ввода команды маршрутизатор скопирует файл программного обеспечения на указанный сервер с указанным именем.

TFTP:

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

FTP:

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

SCP:

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

SFTP:

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

Для создания резервной копии вторичного загрузчика (U-Boot) введите следующую команду. В качестве параметра *<server>* должен быть указан IP-адрес используемого сервера. Для копирования на FTP, SFTP или SCP-сервера потребуется ввести имя пользователя (параметр *<user>*) и пароль (параметр *<password>*). В качестве параметра *<file_name>* укажите имя, с которым

необходимо сохранить файл вторичного загрузчика на сервере (при использовании SCP нужно указать полный путь – параметр *<folder>*). После ввода команды маршрутизатор скопирует файл вторичного загрузчика на указанный сервер с указанным именем.

TFTP:

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

FTP:

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

SCP:

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

SFTP:

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

Для создания резервной копии первичного загрузчика (BL1 для ESR-20/21 и X-Loader для ESR-1500/1511) введите следующую команду. В качестве параметра *<server>* должен быть указан IP-адрес используемого сервера. Для копирования на FTP, SFTP или SCP-сервера потребуется ввести имя пользователя (параметр *<user>*) и пароль (параметр *<password>*). В качестве параметра *<file_name>* укажите имя, с которым необходимо сохранить файл первичного загрузчика на сервере (при использовании SCP нужно указать полный путь – параметр *<folder>*). После ввода команды маршрутизатор скопирует файл первичного загрузчика на указанный сервер с указанным именем.

TFTP:

```
esr# copy system:boot-1 tftp://<server>:/<file_name>
```

FTP:

```
esr# copy system:boot-1 ftp://[<user>[:<password>]@]<server>:/<file_name>
```

SCP:

```
esr# copy system:boot-1
scp://[<user>[:<password>]@]<server>://<folder>/<file_name>
```

SFTP:

```
esr# copy system: boot-1
Sftp://[<user>[:<password>]@]<server>:/<file_name>
```

7 ПРИМЕРЫ НАСТРОЙКИ МАРШРУТИЗАТОРА

7.1 Настройка VLAN

VLAN (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.

7.1.1 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) или диапазона vlan (через дефис).
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)# no switchport forbidden default-vlan**	
5	Установить режим работы физического интерфейса в L2-режим	**esr(config-if-gi)# mode switchport**	
6	Задать режим работы L2 интерфейса.	**esr(config-if-gi)# switchport access**	Только для ESR-20/21. Данный режим является режимом по умолчанию и не отображается в конфигурации.
		esr(config-if-gi)# switchport trunk	Только для ESR-20/21.
		esr(config-gi)# switchport general	Только для ESR-1511/1500. Данный режим является режимом по умолчанию и не отображается в конфигурации.
7	Настроить список VLAN на интерфейсе в тегированном режиме.	**esr(config-if-gi)# switchport trunk allowed vlan add <VID>**	Для ESR-20/21. <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-1511/1500. <VID> – идентификатор VLAN, задаётся в диапазоне [2..4094]. Также есть возможность создания нескольких vlan (через запятую) или диапазона vlan (через дефис).
8	Настроить VLAN на интерфейсе в нетегированном режиме (не обязательно).	**esr(config-if-gi)# switchport trunk native-vlan <VID>**	Для ESR-20/21. <VID> – идентификатор VLAN, задаётся в диапазоне [2..4094].
		esr(config-if-gi)# switchport general allowed vlan add <VID> untagged	Для ESR-1511/1500. <VID> – идентификатор VLAN, задаётся в диапазоне [2..4094].
9	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-20/21.
		esr(config-if-gi)# switchport general allowed vlan auto-all	Только для ESR-1511/1500.

7.1.2 Пример настройки 1. Удаление VLAN с интерфейса

Задача:

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

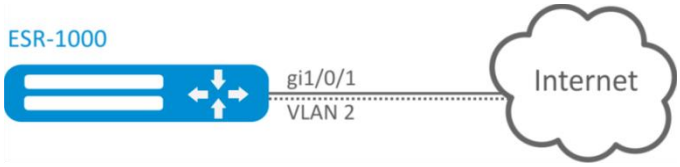

Рисунок 25 – Схема сети

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
```

7.1.3 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.

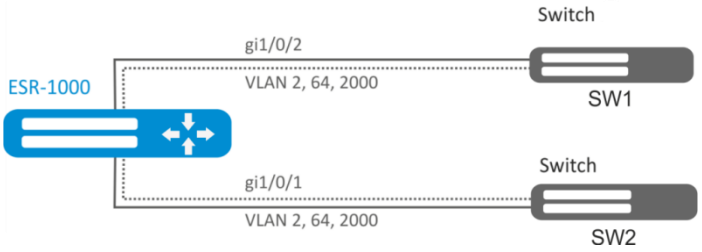

Рисунок 26 – Схема сети

Решение:

Создадим VLAN 2, VLAN 64, VLAN 2000 на ESR-1500:

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

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

```
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 general allowed vlan add 2,64,2000 tagged
```

7.1.4 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-20/ESR-21.

Рисунок 27 – Схема сети

Решение:

Создадим VLAN 2, VLAN 64, VLAN 2000 на ESR-20/ ESR-21:

```
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
```

7.2 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.

7.2.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Активировать LLDP на маршрутизаторе	**esr(config)# lldp enable**	
2	Установить период, в течение которого маршрутизатор хранит информацию, полученную по LLDP (не обязательно).	**esr(config)# lldp hold-multiplier <SEC>**	<SEC> – период времени в секундах, принимает значение [1..10].
3	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
4	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.
5	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
6	Установить период отправки LLDPDU (не обязательно).	**esr(config)# lldp timer <SEC>**	<SEC> – период времени в секундах, принимает значение [1..32768].
7	Включить прием и обработку LLDPDU на физическом интерфейсе.	**esr(config-if-gi)# lldp receive**	
8	Включить отправку LLDPDU на физическом интерфейсе.	**esr(config-if-gi)# lldp transmit**	

7.2.2 Пример настройки

Задача:

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

Рисунок 28 – Схема сети

Решение:

1. Конфигурирование R1

Включим LLDP глобально на маршрутизаторе:

```
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:

```
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
```

7.3 Настройка LLDP MED

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

7.3.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Активировать LLDP на маршрутизаторе	`esr(config)# lldp enable`	
2	Активировать расширение MED LLDP на маршрутизаторе	`esr(config)# lldp med fast-start enable`	
3	Создать сетевую политику	`esr(config)# network-policy <NAME>`	<NAME> – имя network-policy, задается строкой до 31 символа.
4	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.**
5	Установить значение DSCP	`esr(config-net-policy)# dscp <DSCP>`	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].
6	Установить значение COS	`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.
7	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.
8	Установить сетевую политику на интерфейс	`esr(config-if-gi)# lldp network-policy <NAME>`	<NAME> – имя network-policy, задается строкой до 31 символа.
9	Включить отправку LLDPDU на физическом интерфейсе.	`esr(config-if-gi)# lldp transmit`	

7.3.2 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.

Рисунок 29 – Схема сети

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 10,30
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
```

7.4 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.

7.4.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать саб-интерфейс физического интерфейса.	**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	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].
5	Включить саб-интерфейс bridge-group (не обязательно).	**esr(config-subif)#bridge-group <BRIDGE-ID>**	<BRIDGE-ID> – идентификационный номер моста.
6	Установить время жизни IPv4/IPv6 записей в ARP-таблице, изученных на данном интерфейсе (не обязательно).	**esr(config-subif)# ip arp reachable-time <TIME>** или **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>.

7.4.2 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.

7.5 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.

7.5.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать саб-интерфейс физического интерфейса.	**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.
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.
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	Установить интервал времени, в течение которого собирается статистика о нагрузке на Q-in-Q интерфейс (не обязательно).	**esr(config-qinq-if)# load-average <TIME>**	<TIME> – интервал в секундах, принимает значения [5..150].
6	Включить Q-in-Q интерфейс bridge-group (не обязательно).	**esr(config-qinq-if)#bridge-group <BRIDGE-ID>**	<BRIDGE-ID> – идентификационный номер моста.
7	Установить время жизни IPv4/IPv6 записей в ARP-таблице изученных на данном Q-in-Q интерфейсе (не обязательно).	**esr(config-qinq-if)# ip arp reachable-time <TIME>** или **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>.

7.5.2 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 саб-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.

7.6 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-ти USB-модемов.

7.6.1 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 интерфейса, задаётся строкой до 255 символов.
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 данное поле)	**esr(config-cellular-profile)# user <NAME>**	<NAME> – имя пользователя, задаётся строкой до 31 символа.
7	Установить пароля для пользователя мобильной сети (если мобильный оператор требует данное поле)	**esr(config-cellular-profile)# 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.
8	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.
9	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].
10	Ограничить возможность использования семейств IP-адресов в мобильной сети.	**esr(config-cellular-profile)# ip-version { ipv4 | ipv6 }**	ipv4 – семейство IPv4; ipv6 – семейство IPv6;
11	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].
12	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.
13	Задать идентификатор USB-модема, назначенного системой (определен в пункте 2.)	**esr(config-cellular-modem)# device <WORD>**	<WORD> – идентификатор USB-порта подключенного модема [1..12].
14	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].
15	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.

16	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.
17	Задать размер максимального принимаемого пакета (не обязательно)	**esr(config-cellular-modem)# mru { <MRU> }**	<MRU> – значение MRU, принимает значения в диапазоне [128..16383].
18	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]
19	Активировать USB-модем	**esr(config-cellular-modem)# enable**	

7.6.2 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     USB port   Manufacturer     Model      Current     Interface      Link
 device                                             state                    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-cellular-profile)# 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
```

7.7 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.

7.7.1 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.
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
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 неограниченно.
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: 8
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: 128
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	**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

	обязательно)		
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 .. 31] 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.
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].

7.7.2 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.
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.
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	Указать radius в качестве метода аутентификации.	**esr(config)# aaa authentication login { default | <NAME> } <METHOD 1> [<METHOD**	<NAME> – имя списка, задаётся строкой до 31 символа. Способы аутентификации: **local** – аутентификация с помощью

		2>] [<METHOD 3>] [<METHOD 4>]	локальной базы пользователей; **tacacs** – аутентификация по списку TACACS-серверов; **radius** – аутентификация по списку RADIUS-серверов; **ldap** – аутентификация по списку LDAP-серверов.
11	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.
12	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.
13	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.
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 8.
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 9.

7.7.3 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	**esr(config)# tacacs-**	<SEC> – период времени в секундах,

	значение интервала, по истечении которого маршрутизатор считает, что TACACS-сервер недоступен (не обязательно).	**server timeout <SEC>**	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.
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-radius-tacacs)# source-address { <ADDR> | <IPV6-ADDR> }**	<ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

9	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.
10	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.
11	Сконфигурировать список способов учета команд, введённых в CLI (не обязательно).	**esr(config)# aaa accounting commands stop-only tacacs**	
12	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.
13	Перейти в режим конфигурирования соответствующего терминала.	**esr(config)# line <TYPE>**	<TYPE> – тип консоли: **console** – локальная консоль; **ssh** – защищенная удаленная консоль.
14	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.
15	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.

7.7.4 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.
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.
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-tacacs-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 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.
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
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	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.

17	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.
18	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.
19	Перейти в режим конфигурирования соответствующего терминала.	**esr(config)# line <TYPE>**	<TYPE> – тип консоли: **console** – локальная консоль; **ssh** – защищенная удаленная консоль.
20	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.
21	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.

7.7.5 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
```

7.8 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.

7.8.1 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.

7.8.2 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"
```

7.9 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.

7.9.1 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.
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.
		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: - 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]
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>** **esr(config-ipv6-dhcp-server)# max-lease-time <TIME>**	<TIME> – максимальное время аренды IP-адреса, задаётся в формате DD:HH:MM, где: DD – количество дней, принимает значения [0..364]; HH – количество часов, принимает значения [0..23]; MM – количество минут, принимает значения [0..59] Значение по умолчанию: 1 день
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].

7.9.2 Пример настройки DHCP-сервера

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.

7.10 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.

7.10.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим настройки сервиса трансляции адресов получателя.	**esr(config)# nat destination**	
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][1] {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.
10	Задать профиль сервисов (tcp/udp-портов) {отправителя | получателя}, для которых должно срабатывать правило (не обязательно).	**esr(config-dnat-rule)# match [not][1] {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][1] {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][1] 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.

[1] При использовании команды *not* правило будет срабатывать для значений, которые не входят в указанный профиль

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**	

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».

7.10.2 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.

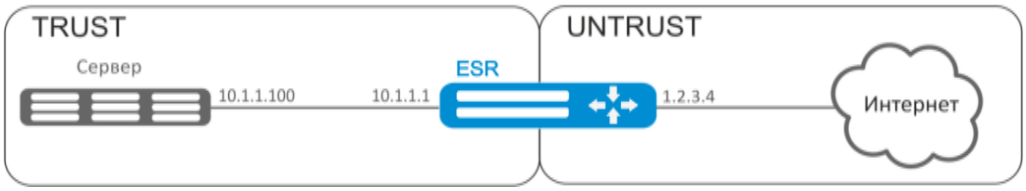

Рисунок 30 – Схема сети

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
```

7.11 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.

7.11.1 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 внутренний 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.
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][1] {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][1] {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][1]{protocol | protocol-id} <TYPE>**	<TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre. Значение «any» указывает на любой тип протокола; <ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF].
14	Задать тип и код сообщений протокола ICMP, для которых должно срабатывать правило (не обязательно).	**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**	

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».

7.11.2 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.

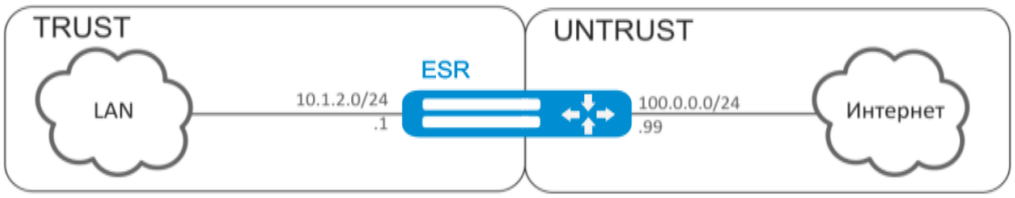

Рисунок 31 – Схема сети

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
```

7.11.3 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.

Рисунок 32 – Схема сети

Решение:

Конфигурирование начнем 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 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
```

7.12 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.

7.12.1 Алгоритм настройки

Настройка Static NAT осуществляется средствами Source NAT, алгоритм настройки которой описан в разделе 7.11.1 настоящего руководства.

7.12.2 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.

Рисунок 33 – Схема сети

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)# match destination-address PUBLIC_POOL
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
```

7.12.3 Пример настройки фильтрации приложений (DPI)

Внимание! 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.

Рисунок 34 – Схема сети

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
```

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, разрешающее прохождение всего 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 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
```

7.13 Проксирование HTTP/HTTPS-трафика

7.13.1 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	Включить логирование событий проксирования трафика (не обязательно)	**esr(config-profile)# log enable**	
8	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.
9	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.
10	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.
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 3128-3136**	Прокси-сервер ESR использует для своей работы следующие порты: 3128 + количество cpu данной модели * 2

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][1] 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.

7.13.2 Пример настройки HTTP-прокси

Задача:

Организовать фильтрацию по URL для ряда адресов посредством прокси.

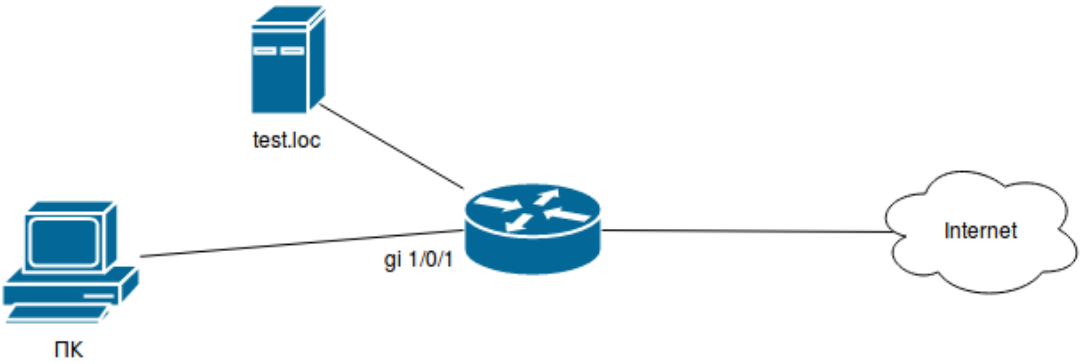

Рисунок 35 – Схема сети

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)# 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 ‘list’

```
esr(config)# interface gi 1/0/1
esr(config-if)# ip http proxy list1
```

Если используется Firewall, создадим для него разрешающие правила:

Создаем профиль портов Прокси-сервера

```
esr(config)# object-group service proxy
esr(config-object-group-service)# port-range 3128-3136
esr(config-object-group-service)# exit
```

Создаем разрешающе 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
```

7.14 Настройка логирования и защиты от сетевых атак

7.14.1 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 количества одновременных сессий на основании адреса назначения.	**esr(config)# ip firewall screen dos-defense limit-session-destination { <NUM> }**	<NUM> – ограничение количества IP-сессий задается в диапазоне [1..10000].
4	Включить ограничение количества одновременных сессий на основании адреса источника, которое смягчает DoS-атаки.	**esr(config)# ip firewall screen dos-defense limit-session-source { <NUM> }**	<NUM> – ограничение количества IP-сессий 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].
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 миллисекундах, в течении которого будет фиксироваться port scan атака [1..1000000]. <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**	
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.
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.

7.14.2 Описание механизмов защиты от атак

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 атаках: SYN flood, UDP flood, ICMP flood, и т.д.). Команда включает ограничение количества одновременных сессий на основании 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 количества одновременных сессий на основании 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.

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, 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.

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.

7.14.3 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.

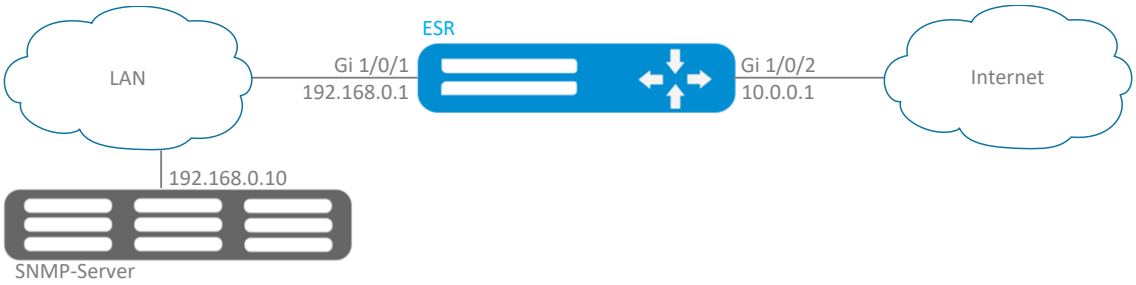

Рисунок 36 – Схема сети

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
```

Посмотреть статистику по зафиксированным сетевым атакам можно командой:

```
esr# show ip firewall screen counters
```

7.15 Конфигурирование Firewall

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

7.15.1 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.
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**	
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 режима работы межсетевого экрана (не обязательно)	**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.
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.

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.
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.
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**	
29	Создать набор правил межзонового взаимодействия.	**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][1] 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][1] protocol-id <protocol-id>	<protocol-id> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF].
34	Установить профиль IP-адресов отправителя, для которых должно срабатывать правило (не обязательно).	**esr(config-zone-rule)# match [not][1] 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][1] destination-address <OBJ-GROUP-NETWORK-NAME>**	
36	Установить MAC-адрес отправителя, для которого должно срабатывать правило (не обязательно).	**esr(config-zone-rule)# match [not][1] 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][1] 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][1] 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][1] 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][1] 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 команду FTP протокола, для которой должно срабатывать правило (не обязательно).	**esr(config-zone-rule)# match [not][1] ftp command <COMMAND>**	any - установить команды FTP-RETR, FTP-RMD, FTP-MKD, FTP-DELE, FTP-STOR, FTP-STOU, FTP-APPE, FTP-ALLO для FTP протокола; delete - установить команду FTP-DELE; get - установить команду FTP-RETR; mkdir - установить команду FTP-MKD; put - установить команды FTP-STOR, FTP-STOU, FTP-APPE, FTP-ALLO; rmdir - установить команду FTP-RMD.
42	Установить команду HTTP протокола, для которой должно срабатывать правило (не обязательно).	**esr(config-zone-rule)# match http command <COMMAND>**	any - установить команды HTTP-GET, HTTP-POST, HTTP-HEAD, HTTP-PUT для HTTP протокола; get - установить команду HTTP-GET; head - уствновить команду HTTP-HEAD; post - установить команду HTTP-POST; put - установить команду HTTP-PUT;
43	Установить ограничение, при котором правило будет срабатывать только для трафика, измененного сервисом трансляции IP-адресов и портов получателя.	**esr(config-zone-rule)# match [not][1] destination-nat**	
44	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].
45	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][1] fragment**	
46	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][1] ip-option**	
47	Включить правило межзонового взаимодействия.	**esr(config-zone-rule)# enable**	
48	Активировать фильтрацию и режим отслеживания сессий при прохождении пакетов между участниками одной Bridge-группы (не обязательно, доступно только на ESR-1511/1500)	**esr(config-bridge)# ports firewall enable**	

[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 межсетевого экрана содержится в «Справочнике команд CLI».

7.15.2 Пример настройки Firewall

Задача:

Разрешить обмен сообщениями по протоколу ICMP между устройствами ПК1, ПК2 и маршрутизатором ESR.

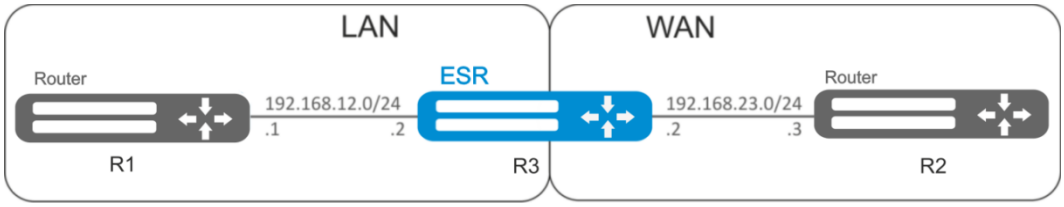

Рисунок 37 – Схема сети

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 ПК1 к ПК2. 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 ПК2 к ПК1. 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 ПК2 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 ПК1 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
```

7.16 Настройка списков доступа (ACL)

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

7.16.1 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].
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

7	Установить IP-адреса получателя, для которых должно срабатывать правило (не обязательно).	**esr(config-acl-rule)# match destination-address { <ADDR> <MASK> | any }**	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.
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 cos <COS>**	<COS> – значение 802.1p приоритета, принимает значения [0..7].
13	Установить значение кода DSCP, для которого должно срабатывать правило (не обязательно). Невозможно использовать совместно с IP Precedence.	**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.

7.16.2 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
```

7.17 Конфигурирование статических маршрутов

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

7.17.1 Процесс 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 4.2;
- <TUN> – имя туннеля, задаётся в виде, описанном в разделе 4.3;
- <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-маршрут 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 3.3;
- 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.

7.17.2 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.

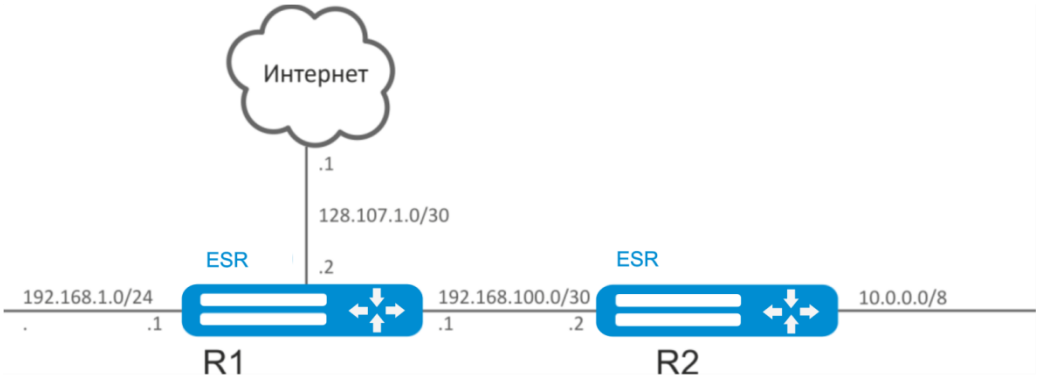

Рисунок 38 – Схема сети

Решение:

Зададим имя устройства для маршрутизатора 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 маршрутизатора 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 маршрутизатора 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
```

7.18 Настройка PPP через E1

PPP (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-SFP в маршрутизаторе ESR.

Процесс настройки

Шаг	Описание	Команда	Ключи
1	Перевести физический интерфейс в режим коммутации	`esr(config-if-gi)# mode switchport`	
2	Задать режим работы интерфейса e1	`esr(config-if-gi)# switchport mode e1`	
3	Задать источник синхронизации	`esr(config-if-gi)# switchport e1 clock source <SOURCE>`	<SOURCE> - источник синхронизации: Internal (по умолчанию) – синхронизироваться с внутренним источником; line – синхронизироваться с линейным сигналом
4	Указать размер MTU (Maximum Transmition Unit) для физических интерфейсов	`esr(config-if-gi)# mtu <MTU>`	<MTU> – значение MTU, для E1 и Multilink интерфейсов принимает значения в диапазоне [128..1500].
5	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.
6	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
7	Задать инвертацию передаваемых бит (не обязательно)	`esr(config-if-gi)# switchport e1 invert data`	
8	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
9	Задать количество тайм слотов	`esr(config-if-gi)# switchport e1 timeslots <RANGE>`	<RANGE> – количество тайм-слотов
10	Использовать E1 как единую сущность, без таймслотов (не обязательно)	`esr(config-if-gi)# switchport e1 unframed`	
11	Конфигурируем E1	`esr(config)# interface e1 1/<SLOT>/1`	<SLOT> – номер слота.
12	Включаем CHAP-аутентификацию для PPP (не обязательно)	`esr(config-e1)# ppp authentication chap`	
13	Задается имя маршрутизатора, которое отправляется удаленной стороне для прохождения CHAP-аутентификации (не обязательно)	`esr(config-e1)# ppp chap hostname <NAME>`	<NAME> – имя маршрутизатора
14	Задать пароль для аутентификации (не обязательно)	`esr(config-e1)# ppp chap password ascii-text <CLEAR-TEXT>`	<CLEAR-TEXT> – пароль в открытой форме

15	Включить игнорирование аутентификации (не обязательно)	**esr(config-e1)# ppp chap refuse**	
16	Задать имя пользователя для аутентификации (не обязательно)	**esr(config-e1)# ppp chap username <NAME>**	<NAME> – имя пользователя
17	Разрешается принимать от соседа любой ненулевой IP-адрес в качестве локального IP-адреса (не обязательно)	**esr(config-e1)# ppp ipcp accept-address**	
18	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
19	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
20	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
21	Задать количество попыток отправки Terminate-Request пакетов, прежде чем сессия будет прервана (не обязательно)	**esr(config-e1)# ppp max-terminate <VALUE>**	<VALUE> – количество попыток
22	Задать размер MRU (Maximum Receive Unit) для интерфейса (не обязательно)	**esr(config-e1)# ppp mru <MRU>**	<MRU> – значение MRU
23	Включение режима MLPPP (не обязательно)	**esr(config-e1)# ppp multilink**	
24	Добавить в MLPPP группу (не обязательно)	**esr(config-e1)# ppp multilink-group <GROUP-ID>**	<GROUP-ID> – номер группы
25	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
26	Задается интервал, по истечении которого маршрутизатор повторяет запрос на установление сессии (не обязательно)	**esr(config-e1)# ppp timeout retry <TIME>**	<TIME> – время в секундах

Пример конфигурации

Задача:

Настроить PPP-соединение со встречной стороной с IP-адресом 10.77.0.1/24 через ToPGATE-SFP, используя 1-8 канальные интервалы для передачи данных; источник синхросигнала – встречная сторона.

Рисунок 39 – Схема сети

Решение:

Переключаем интерфейс, в котором установлен ToPGATE-SFP, gigabitethernet 1/0/3 в режим работы E1:

```
esr# configure
esr(config)# interface gigabitethernet 1/0/3
esr(config-if-gi)# description "*** ToPGATE ***"
esr(config-if-gi)# switchport mode e1
esr(config-if-gi)# switchport e1 timeslots 1-8
esr(config-if-gi)# switchport e1 clock source line
esr(config-if-gi)# switchport e1 slot 3
esr(config-if-gi)# exit
```

Включим interface e1 1/3/1:

```
esr(config)# interface e1 1/3/1
esr(config-e1)# security-zone trusted
esr(config-e1)# ip address 10.77.0.1/24
esr(config-e1)# exit
```

Изменения конфигурации вступят в действие по следующим командам:

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

7.19 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.

Рисунок 40 – Схема сети

7.19.1 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.
6	Включить CHAP-аутентификацию.	**esr(config-multilink)# ppp authentication chap**	
7	Включить игнорирование аутентификации (не обязательно).	**esr(config-multilink)# ppp chap refuse**	
8	Указать имя маршрутизатора, которое отправляется удаленной стороне для прохождения CHAP-аутентификации.	**esr(config-multilink)# ppp chap hostname <NAME>**	<NAME> – имя маршрутизатора, задаётся строкой до 31 символа.
9	Указать пароль, который отправляется удаленной стороне вместе с именем маршрутизатора 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.
10	Разрешить принимать от соседа любой ненулевой IP-адрес в качестве локального IP-адреса (не обязательно).	**esr(config-multilink)# ppp ipcp accept-address**	
11	Установить IP-адрес, который отправляется удаленной стороне для последующего его присвоения.	**esr(config-multilink)# ppp iccp remote-address <ADDR>**	<ADDR> – IP-адрес удаленного шлюза.
12	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.

13	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.
14	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.
15	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].
16	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.
17	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.
18	Указать интервал времени в секундах, по истечении которого маршрутизатор отправляет keepalive-сообщение (не обязательно).	**esr(config-multilink)# ppp timeout keepalive <TIME>**	<TIME> – время в секундах, принимает значения [1..32767]. Значение по умолчанию: 10.
19	Установить интервал времени в секундах, по истечении которого маршрутизатор 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.
20	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].
21	Привязать порт e1 к физическому интерфейсу.	**esr(config-if-gi)# switchport e1 <SLOT>**	<SLOT> – идентификатор слота, принимает значение в диапазоне [0..3].
22	Перевести физический порт в режим работы с SFPe1 модулем.	**esr(config-if-gi)# switchport mode e1**	
23	Включить режим MLPPP на E1-интерфейсе.	**esr(config-e1)# ppp multilink**	
24	Включить E1-интерфейс в группу агрегации.	**esr(config-e1)# ppp multilink-group <GROUP-ID>**	<GROUP-ID> – идентификатор группы, принимает значение [1..4].

7.19.2 Пример настройки

Задача:

Настроить MLPPP-соединение с встречной стороной с IP-адресом 10.77.0.1/24 через устройство MXE.

Рисунок 41 – Схема сети

Решение:

Переключаем интерфейс gigabitethernet 1/0/10 в режим работы E1:

```
esr# configure
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# switchport mode e1
esr(config-if-gi)# switchport e1 slot 0
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# switchport mode e1
esr(config-if-gi)# switchport e1 slot 1
esr(config-if-gi)# exit
```

Настроим MLPPP 3:

```
esr(config)# interface multilink 3
esr(config-multilink)# ip address 10.77.0.2/24
esr(config-multilink)# security-zone trusted
esr(config-multilink)# exit
esr(config)# exit
```

Включим interface e1 1/0/1, interface e1 1/0/2 в группу агрегации MLPPP 3:

```
esr(config)# interface e1 1/0/1
esr(config-e1)# ppp multilink
esr(config-e1)# ppp multilink-group 3
esr(config-e1)# exit
esr(config)# interface e1 1/0/2
esr(config-e1)# ppp multilink
esr(config-e1)# ppp multilink-group 3
esr(config-e1)# exit
```

7.20 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.

7.20.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Добавить сетевой мост (bridge) в систему и	`esr(config)# bridge <BRIDGE-ID>`	<BRIDGE-ID> – идентификационный номер моста, принимает значения в

	перейти в режим настройки его параметров.		диапазоне: для ESR-20/21 – [1..250]; для ESR-1511/1500 – [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	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-20/21 – [552..9500]; для ESR-1511/1500 – [552..10000]. Значение по умолчанию: 1500
6	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
7	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].
8	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].
9	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-20/21 – [1..250]; для ESR-1511/1500 – [1..500].

10	Включить на bridge режим изоляции интерфейсов. В данном режиме обмен трафиком между членами сетевого моста запрещен. (не обязательно; применимо только на ESR-1511/1500)	**esr(config-bridge)# protected-ports [exclude vlan]**	exclude vlan – при указании данного ключа, VLAN (связанный с bridge) исключается из списка изолируемых интерфейсов.
11	Запретить коммутацию unknown-unicast трафика (когда MAC-адрес назначения не содержится в таблице коммутации) в данном bridge. (не обязательно; применимо только на ESR-1511/1500)	**esr(config-bridge)# unknown-unicast-forwarding disable**	
12	Установить время жизни IPv4/IPv6-записей в ARP-таблице, изученных на данном bridge (не обязательно).	**esr(config- bridge)# ip arp reachable-time <TIME>** или **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>.

7.20.2 Пример настройки bridge для VLAN и L2TPv3-туннеля

Задача:

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

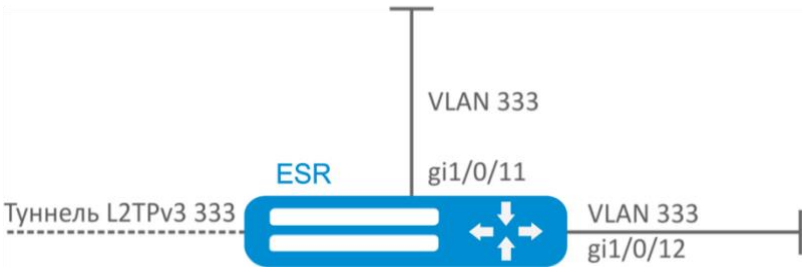

Рисунок 42 – Схема сети

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 7.27 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
```

7.20.3 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.

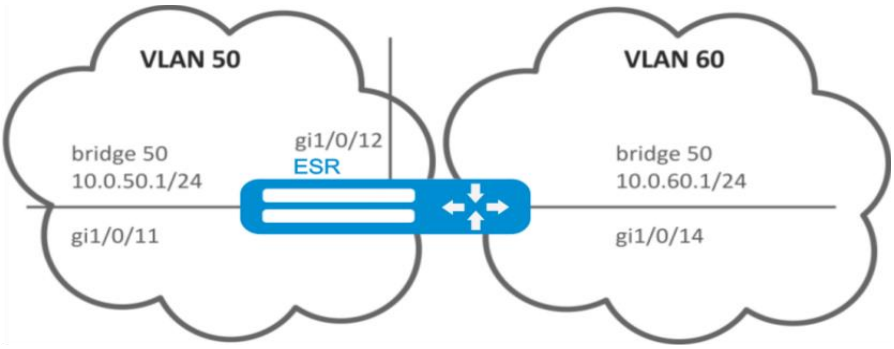

Рисунок 43 – Схема сети

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
```

7.20.4 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.

7.21 Настройка RIP

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

7.21.1 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.

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> [{ eq <LEN> | le <LEN> | ge <LEN> [le <LEN>] }]|default-route}** **esr(config-pl)# deny {object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> | le <LEN> | ge <LEN> [le <LEN>] }] | default-route}**	<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.
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 [1..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 [1..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 [1..65535]. При установке значения нужно учитывать следующее правило: «timersinvalid + 60» Значение по умолчанию: 240 секунд.
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.
		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; **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.
		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.
		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].

7.21.2 Пример настройки RIP

Задача:

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

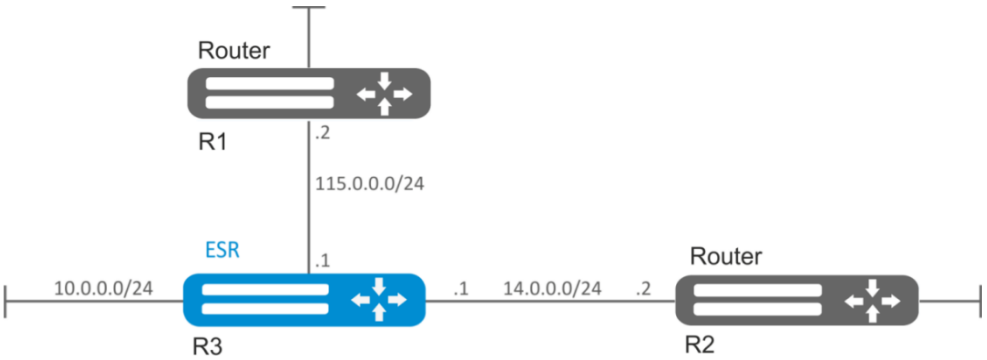

Рисунок 44 – Схема сети

Решение:

Предварительно нужно настроить IP-адреса на интерфейсах согласно схеме сети, приведенной на рисунке 44.

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.

7.22 Настройка OSPF

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

7.22.1 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	`esr(config)# ip protocols ospf max-routes <VALUE>`	<VALUE> – количество маршрутов протокола OSPF в маршрутной таблице,

	протокола OSPF (не обязательно).	**esr(config)# ipv6 protocols ospf max-routes <VALUE>**	принимает значения в диапазоне: для ESR-1511/1500 [1..500000]; для ESR-20/21 [1..300000]. Значение по умолчанию для глобального режима: для ESR-1511/1500 – (500000); для ESR-20/21 – (300000). 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**	
4	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.
5	Разрешить (permit) или запретить (deny) списки префиксов.	**esr(config-pl)# permit {object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> | le <LEN> | ge <LEN> [le <LEN>] }]|default-route}** **esr(config-pl)# deny {object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> | le <LEN> | ge <LEN> [le <LEN>] }] | default-route}** **esr(config-ipv6-pl)# permit {object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> | le <LEN> | ge <LEN> [le <LEN>] }]|default-route}** **esr(config-ipv6-pl)# deny object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> | le <LEN> | ge <LEN> [le <LEN>] }] | default-route}**	<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.
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.
7	Установить идентификатор маршрутизатора для данного OSPF-процесса.	**esr(config-ospf)# router-id <ID>** **esr(config-ipv6-ospf)# router-id <ID>**	<ID> – идентификатор маршрутизатора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
8	Определить	**esr(config-ospf)#**	<VALUE> – приоритетность маршрутов

	приоритетность маршрутов процесса OSPF.	**preference <VALUE>** **esr(config-ipv6-ospf)# preference <VALUE>**	процесса OSPF, принимает значения в диапазоне [1..255]. Значение по умолчанию: 10.
9	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.
12	Включить анонсирование маршрутов, полученных альтернативным способом (не обязательно).	**esr(config-ospf)# redistribute static [route-map <NAME>]** **esr(config-ipv6-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-ospf)# redistribute connected [route-map <NAME>] **esr(config-ipv6-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-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>] **esr(config-ipv6-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.
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>** **esr(config-ipv6-ospf)# area <AREA_ID>**	<AREA_ID> – идентификатор области, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
15	Включить анонсирование подсетей.	**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	**esr(config-ospf-area)# area-type <TYPE> [no-summary]** **esr(config-ipv6-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).
17	Включить генерацию маршрута по умолчанию для NSSA-области и анонсирование его в качестве NSSA-LSA.	**esr(config-ospf-area)# default-information-originate** **esr(config-ipv6-ospf-area)# default-information-originate**	
18	Включить суммаризацию или скрытие подсетей.	**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**	
20	Установить виртуальное соединение между основной и удаленными областями, имеющими между ними несколько областей.	**esr(config-ospf-area)# virtual-link <ID>** **esr(config-ipv6-ospf-area)# virtual-link <ID>**	<ID> – идентификатор маршрутизатора, 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 повторно отправит пакет, который	**esr(config-ospf-vlink)# restransmit-interval <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 5 секунд.

	не получил подтверждения о получении (например, DatabaseDescription пакет или LinkStateRequest пакеты).	**esr(config-ipv6-ospf-vlink)# restransmit-interval <TIME>**	
22	Установить интервал времени в секундах, по истечении которого маршрутизатор отправляет следующий hello-пакет.	**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. 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 выберет DR в сети	**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	**esr(config-ospf-vlink)# authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм аутентификации: **cleartext** – пароль, передается открытым текстом (доступно только для RIP и OSPF-VLINK); **md5** – пароль хешируется по алгоритму md5.
26	Установить пароль для аутентификации с соседом.	**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.	**esr(config-ospf-vlink)# authentication key chain <KEYCHAIN>**	<KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов.
28	Активировать виртуальное соединение.	**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>** **esr(config-if-gi)# ipv6 ospf instance <ID>**	<ID> – номер процесса, принимает значения [1..65535].

31	Определить принадлежность интерфейса к определенной области OSPF-процесса.	**esr(config-if-gi)# ip ospf area <AREA_ID>** **esr(config-if-gi)# ipv6 ospf area <AREA_ID>**	<AREA_ID> – идентификатор области, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
32	Включить маршрутизацию по протоколу OSPF на интерфейсе.	**esr(config-if-gi)# ip ospf** **esr(config-if-gi)# ipv6 ospf**	
33	Включить режим, в котором OSPF-процесс будет игнорировать значение MTU интерфейса во входящих Database Description-пакетах.	**esr(config-if-gi)# ip ospf mtu-ignore** **esr(config-if-gi)# ipv6 ospf mtu-ignore**	
34	Определить алгоритм аутентификации протокола OSPF.	**esr(config-if-gi)# ip ospf authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм аутентификации: **cleartext** – пароль, передается открытым текстом; **md5** – пароль хешируется по алгоритму md5.
35	Установить пароль для аутентификации с OSPF-соседом при передаче пароля открытым текстом.	**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.	**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 выберет DR в сети.	**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 повторно отправит пакет, на который не получил подтверждения о получении (например, DatabaseDescription пакет или LinkStateRequest пакеты).	**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.
39	Установить интервал времени в секундах, по истечении которого маршрутизатор отправляет следующий hello-пакет.	**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	**esr(config-if-gi)# ip dead-interval <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 40 секунд.

	будет считаться неактивным. Этот интервал должен быть кратным значению hello-interval.	**esr(config-if-gi)# ipv6 dead-interval <TIME>**	
41	Установить интервал времени, в течение которого NBMA-интерфейс ждет, прежде чем отправить HELLO-пакет соседу, даже в случае, если сосед неактивен.	**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.	**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.
43	Определить тип сети для установления OSPF соседства.	**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, который используется для выбора DR и BDR.	**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.	**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: 150.
47	Включить протокол BFD для протокола OSPF	**esr(config-if-gi)# ip ospf bfd-enable** **esr(config-if-gi)# ipv6 ospf bfd-enable**	

7.22.2 Пример настройки OSPF

Задача:

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

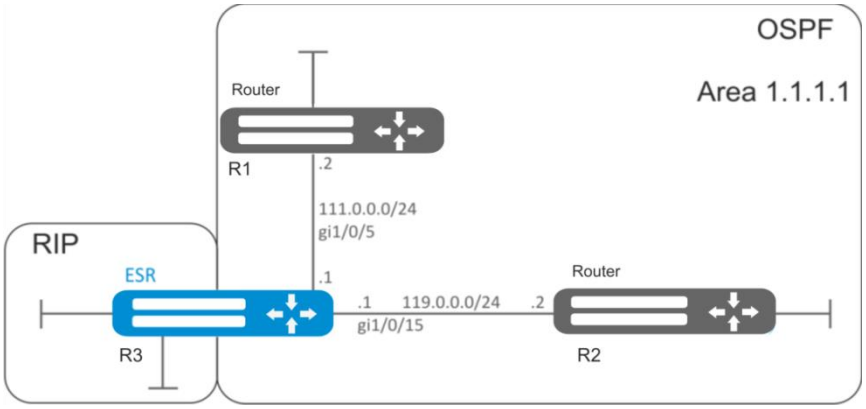

Рисунок 45 – Схема сети

Решение:

Предварительно нужно настроить IP-адреса на интерфейсах согласно схеме, приведенной на рисунке 45.

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 маршрутизаторы подключены к интерфейсам gi1/0/5 и gi1/0/15. Для установления соседства с другими маршрутизаторами 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
```

7.22.3 Пример настройки OSPF stub area

Задача:

Изменить тип области 1.1.1.1, область должна быть тупиковой. Тупиковый маршрутизатор должен анонсировать маршруты, полученные по протоколу RIP.

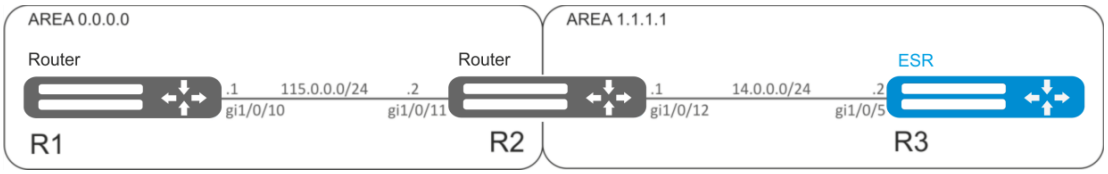

Рисунок 46 – Схема сети

Решение:

Предварительно нужно настроить протокол OSPF и IP-адреса на интерфейсах согласно схеме, приведенной на рисунке 46.

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

```
esr(config-ospf-area)# area-type stub
```

На тупиковом маршрутизаторе R3 включим анонсирование маршрутной информации из протокола RIP:

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

7.22.4 Пример настройки Virtual link

Задача:

Объединить две магистральные области в одну с помощью virtual link.

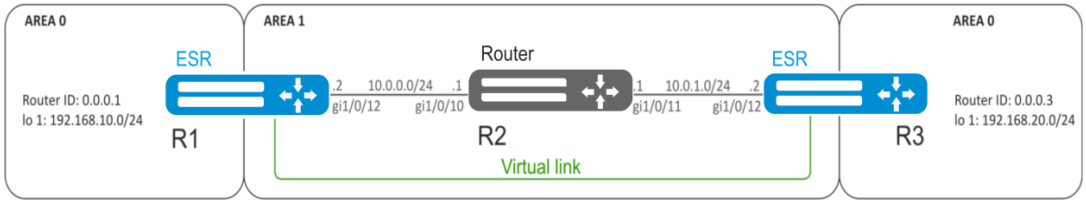

Рисунок 47 – Схема сети

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 маршрутизаторами зоны (Area Border Router, ABR).

Предварительно нужно настроить протокол OSPF и IP-адреса на интерфейсах согласно схеме, приведенной на рисунке 47.

На маршрутизаторе 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 маршрутизаторе 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 маршрутизаторе 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 маршрутизаторе 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).

7.23 Настройка BGP

Протокол BGP предназначен для обмена информацией о достижимости подсетей между автономными системами (далее АС), то есть группами маршрутизаторов под единым техническим управлением, использующими протокол внутридоменной маршрутизации для определения маршрутов внутри себя и протокол междоменной маршрутизации для определения маршрутов доставки пакетов в другие 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.

Расширение протокола BGP Flow Specification позволяет получать и передавать информацию о потоках трафика и применять ее для фильтрации трафика и применения политик безопасности. Основное предназначение функции BGP Flow Specification – защита от атак, направленных на отказ в обслуживании (Distributed Denial of Service, DDoS).

7.23.1 Алгоритм настройки

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).
2	Настроить емкость таблиц маршрутизации протокола BGP (не обязательно).	**esr(config)# ip protocols bgp max-routes <VALUE>**	<VALUE> – количество маршрутов протокола BGP в маршрутной таблице, принимает значения в диапазоне: для ESR-1511/1500 [1..2800000]; для ESR-20/21 [1..1500000]. Значение по умолчанию: для ESR-1511/1500 (2800000); для ESR-20/21 (1500000).
		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	**esr(config)# router bgp maximum-paths <VALUE>**	<VALUE> – количество допустимых равноценных маршрутов до цели,

	максимальное количество равноценных маршрутов до цели.		принимает значения [1..16].
5	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.
6	Разрешить (permit) или запретить (deny) списки префиксов.	**esr(config-pl)# permit {object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> | le <LEN> | ge <LEN> [le <LEN>] }]|default-route}** **esr(config-pl)# deny {object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> | le <LEN> | ge <LEN> [le <LEN>] }] | default-route}**	<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.
7	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].
8	Определить тип конфигурируемой маршрутной информации и перейти в данный режим настройки.	**esr(config-bgp)# address-family { ipv4 | ipv6 } [vrf <VRF>]**	– **ipv4** – семейство IPv4; – **ipv6** – семейство IPv6; <VRF> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет работать протокол маршрутизации.
9	Установить идентификатор маршрутизатора.	**esr(config-bgp-af)# router-id <ID>** **esr(config-ipv6-bgp-af)# router-id <ID>**	<ID> – идентификатор маршрутизатора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
10	Установить временной интервал, по истечении которого идет проверка соединения со встречной стороной.	**esr(config-bgp-af)# timers keeaplive <TIME>** **esr(config-ipv6-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.	**esr(config-bgp-af)# timers holdtime <TIME>** **esr(config-ipv6-bgp-af)# timers holdtime <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 180 секунд.
12	Установить время минимальной и	**esr(config-bgp-af)# timers error-wait <TIME1> <TIME2>**	<TIME1> – время минимальной задержки в секундах, принимает

	максимальной задержки, в течение которого запрещено устанавливать соединение, в целях защиты от частых разрывов соединения	**esr(config-ipv6-bgp-af)# timers error-wait <TIME1> <TIME2>**	значения [1..65535]; <TIME2> – время максимальной задержки в секундах, принимает значения [1..65535].
13	Установить идентификатор Route-Reflector кластера, которому принадлежит BGP-процесс маршрутизатора.	**esr(config-bgp-af)# cluster-id <ID>** **esr(config-ipv6-bgp-af)# cluster-id <ID>**	<ID> – идентификатор Route-Reflector кластера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
14	Определить глобальный алгоритм аутентификации с соседями.	**esr(config-bgp-af)# authentication algorithm <ALGORITHM>** **esr(config-ipv6-bgp-af)# authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм шифрования: md5 – пароль шифруется по алгоритму md5.
15	Установить глобальный пароль для аутентификации с соседями.	**esr(config-bgp-af)# authentication key ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }** **esr(config-ipv6-bgp-af)# 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...).
16	Активировать BGP-процесс.	**esr(config-bgp-af)# enable** **esr(config-ipv6-bgp-af)# enable**	
17	Включить анонсирование статических маршрутов полученных альтернативным образом.	**esr(config-bgp-af)# redistribute static [route-map <NAME>]** **esr(config-ipv6-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>] **esr(config-ipv6-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>] **esr(config-ipv6-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.
		esr(config-bgp-af)# redistribute ospf <ID> <ROUTE-TYPE> [route-map <NAME>]	<ID> – номер процесса, может принимать значение [1..65535]; <ROUTE-TYPE> – тип маршрута:

		esr(config-ipv6-bgp-af)# redistribute ospf <ID> <ROUTE-TYPE> [route-map <NAME>]	- **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.
		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.
		esr(config-ipv6-bgp-af)# redistribute bgp <AS> [route-map <NAME>]	
18	Включить анонсирование подсетей.	**esr(config-bgp-af)# 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-bgp-af)# network <ADDR/LEN>	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	Добавить фильтрацию подсетей во входящих или исходящих обновлениях (не обязательно).	**esr(config-bgp-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.
20	Добавить BGP-соседа и осуществить переход в режим настройки параметров BGP-соседа.	**esr(config-bgp-af)# neighbor <ADDR>**	<ADDR> – IP-адрес соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
		esr(config-ipv6-bgp-af)# neighbor <IPV6-ADDR>	<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	Включить BGP FlowSpec для настраиваемого соседа (не обязательно)	**esr(config-bgp-neighbor)# flow-spec enable**	
23	Установить временной интервал, по истечении	**esr(config-bgp-neighbor)# timers keepalive <TIME>**	<TIME> – время в секундах, принимает значения [1..65535].

	которого идет проверка соединения со встречной стороной. (не обязательно)	**esr(config-ipv6-bgp-neighbor)# timers keepalive <TIME>**	Значение по умолчанию: 60 секунд.
24	Установить временной интервал, по истечении которого встречная сторона считается недоступной (не обязательно).	**esr(config-bgp-neighbor)# timers holdtime <TIME>** **esr(config-ipv6-bgp-neighbor)# timers holdtime <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 180 секунд.
25	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>** **esr(config-ipv6-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
26	Установить номер автономной системы BGP-соседа.	**esr(config-bgp-neighbor)# remote-as <AS>** **esr(config-ipv6-bgp-neighbor)# remote-as <AS>**	<AS> – номер автономной системы, принимает значения [1..4294967295].
27	Разрешить подключение к соседям, которые находятся не в напрямую подключенных подсетях. (не обязательно)	**esr(config-bgp-neighbor)# ebgp-multihop <NUM>** **esr(config-ipv6-bgp-neighbor)# ebgp-multihop <NUM>**	<NUM> - Максимальное количество хопов при установке EBGP (используется для TTL).
28	Задать режим, в котором все обновления отправляются BGP-соседу с указанием в качестве next-hop IP-адреса исходящего интерфейса локального маршрутизатора. (не обязательно)	**esr(config-bgp-neighbor)# next-hop-self** **esr(config-ipv6-bgp-neighbor)# next-hop-self**	
29	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)	**esr(config-bgp-neighbor)# remove-private-as** **esr(config-ipv6-bgp-neighbor)# remove-private-as**	
30	Задать режим, в котором BGP-соседу в обновлении на ряду с другими маршрутами всегда отправляется маршрут по умолчанию. (не обязательно)	**esr(config-bgp-neighbor)# default-originate** **esr(config-ipv6-bgp-neighbor)# default-originate**	
31	Включить генерацию и отправку маршрута по умолчанию, если маршрут	**esr(config-bgp-af)# default-information-originate**	

	по умолчанию есть в таблице маршрутизации FIB. (не обязательно)		
32	Указать, что BGP-сосед является Route-Reflector клиентом. (не обязательно)	**esr(config-bgp-neighbor)# route-reflector-client**	
		esr(config-ipv6-bgp-neighbor)# route-reflector-client	
33	Определить приоритетность маршрутов, получаемых от соседа. (не обязательно)	**esr(config-bgp-neighbor)# preference <VALUE>**	<VALUE> – приоритетность маршрутов соседа, принимает значения в диапазоне [1..255]. Значение по умолчанию: 170.
		esr(config-ipv6-bgp-neighbor)# preference <VALUE>	
34	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> }**	<ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];
		esr(config-ipv6-bgp-neighbor)# update-source <ADDR>	<IPV6-ADDR> – IPv6-адрес источника, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
35	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].
		esr(config-bgp-neighbor)# allow-local-as <NUMBER>	
36	Включить BFD-протокол на конфигурируемом BGP-соседе. (не обязательно)	**esr(config-bgp-neighbor)# bfd-enable**	
		esr(config-ipv6-bgp-neighbor)# bfd-enable	
37	Определить алгоритм аутентификации с соседом. (не обязательно)	**esr(config-bgp-neighbor)# authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм шифрования: md5 – пароль шифруется по алгоритму md5.
		esr(config-ipv6-bgp-neighbor)# authentication algorithm <ALGORITHM>	
38	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...).
		esr(config-ipv6-bgp-neighbor)# authentication key ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }	
39	Включить в межсетевом экране применение правил фильтрации, полученных от BGP FlowSpec (не обязательно)	**esr(config)# ip firewall screen flow-spec**	

40	Включить логирование срабатывания правил фильтрации, полученных от BGP FlowSpec (не обязательно)	`esr(config)# logging firewall screen flow-spec`	

Часто бывает, особенно при конфигурировании iBGP, что в одном bgp address-family 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.

7.23.2 Пример настройки

Задача:

Настроить BGP-протокол на маршрутизаторе со следующими параметрами:

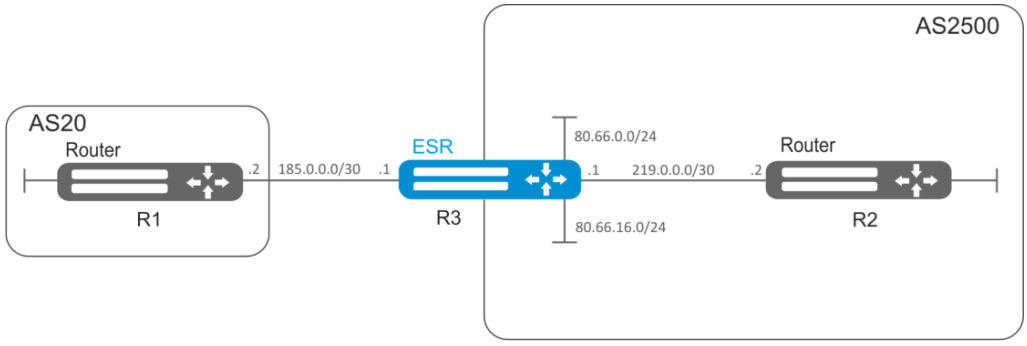

Рисунок 48 – Схема сети

- 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, AS 2500;
- второе соседство - подсеть 185.0.0.0/30, собственный IP-адрес 185.0.0.1, IP-адрес соседа 185.0.0.2, AS 20.

Решение:

Сконфигурируем необходимые сетевые параметры:

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

```
esr(config-if-gi)# exit
```

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

```
esr(config)# router bgp 2500
```

Входим в режим конфигурирования маршрутной информации для IPv4:

```
esr(config-bgp)# address-family ipv4
```

Объявим подсети, подключённые напрямую:

```
esr(config-bgp-af)# redistribute connected
```

Создадим соседства с 185.0.0.2, 219.0.0.2 с указанием автономных систем и включим их:

```
esr(config-bgp-af)# neighbor 185.0.0.2
esr(config-bgp-neighbor)# remote-as 20
esr(config-bgp-neighbor)# enable
esr(config-bgp-neighbor)# exit
esr(config-bgp-af)# neighbor 219.0.0.2
esr(config-bgp-neighbor)# remote-as 2500
esr(config-bgp-neighbor)# enable
esr(config-bgp-neighbor)# exit
```

Включим работу протокола:

```
esr(config-bgp-af)# enable
esr(config-bgp-af)# exit
esr(config)# exit
```

Информацию о BGP-пирах можно посмотреть командой:

```
esr# show ip bgp 2500 neighbors
```

Таблицу маршрутов протокола BGP можно просмотреть с помощью команды:

```
esr# show ip bgp
```

Необходимо в firewall разрешить TCP-порт 179.

7.24 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 (оба маршрутизатора генерируют BFD-пакеты и отвечают друг-другу).

7.24.1 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-1511/1500 и [300..65535] для ESR-20/21 По умолчанию 1 секунда
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-1511/1500 и [300..65535] для ESR-20/21 По умолчанию: 300 миллисекунд на ESR-20/21 200 миллисекунд на ESR-1511/1500
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-1511/1500 и [300..65535] для ESR-20/21 По умолчанию: 300 миллисекунд на ESR-20/21 200 миллисекунд на ESR-1511/1500
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-1511/1500 и [300..65535] для ESR-20/21. По умолчанию: 1 секунда
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-1511/1500 и [300..65535] для ESR-20/21 По умолчанию: 300 миллисекунд на ESR-20/21 200 миллисекунд на ESR-1511/1500
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-1511/1500 и [300..65535] для ESR-20/21 По умолчанию: 300 миллисекунд на ESR-20/21/100/200 200 миллисекунд на ESR-1511/1500
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
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**	

7.24.2 Пример настройки BFD с BGP

Задача:

Необходимо настроить eBGP между ESR R1 и R2 и включить BFD.

Рисунок 49 – Схема сети

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)# address-family ipv4
esr(config-bgp-af)# 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)# ex
esr(config-bgp-af)# enable
esr(config-bgp-af)# 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)# address-family ipv4
esr(config-bgp-af)# 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)# ex
esr(config-bgp-af)# enable
esr(config-bgp-af)# exit
```

7.25 Настройка политики маршрутизации PBR

7.25.1 Настройка 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.

Также Route-map может назначать маршруты на основе списков доступа (ACL).

7.25.1.1 Алгоритм настройки

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.
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>** **esr(config-route-map-rule)# match ipv6 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.
9	Задать профиль, содержащий IP-адреса маршрутизатора, анонсировавшего маршрут, для которого должно срабатывать правило (не обязательно).	**esr(config-route-map-rule)# match ip route-source object-group <OBJ-GROUP-NETWORK -NAME>** **esr(config-route-map-rule)# match ipv6 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.
10	Задать ACL группу, для которой должно срабатывать правило.	**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].

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].
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].
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.

7.25.1.2 Пример настройки 1

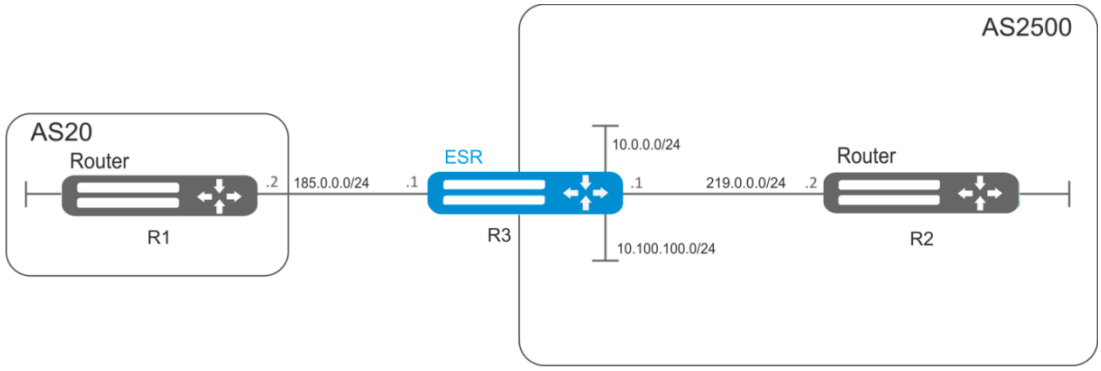

Рисунок 50 – Схема сети

Задача:

Назначить community для маршрутной информации, приходящей из AS 20:

Предварительно нужно выполнить следующие действия:

- Настроить BGP с AS 2500 на маршрутизаторе ESR;
- 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 AS 20, 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 AS 2500 заходим в настройки параметров соседа:

```
esr(config)# router bgp 2500

esr(config-bgp)# address-family ipv4

esr(config-bgp-af)# neighbor 185.0.0.2
```

Привязываем политику к принимаемой маршрутной информации:

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

7.25.1.3 Пример настройки 2

Задача:

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

Предварительно:

Настроить BGP с AS 2500 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 AS 2500 заходим в настройки параметров соседа:

```
esr(config)# router bgp 2500

esr(config-bgp)# address-family ipv4

esr(config-bgp-af)# neighbor 185.0.0.2
```

Привязываем политику к анонсируемой маршрутной информации:

```
esr(config-bgp-neighbor)# route-map to-as20 out
esr(config-bgp-neighbor)# exit
esr(config-bgp)# exit
esr(config)# exit
```

7.25.2 Route-map на основе списков доступа (Policy-based routing)

7.25.2.1 Алгоритм настройки

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(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 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].
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.

7.25.2.2 Пример настройки

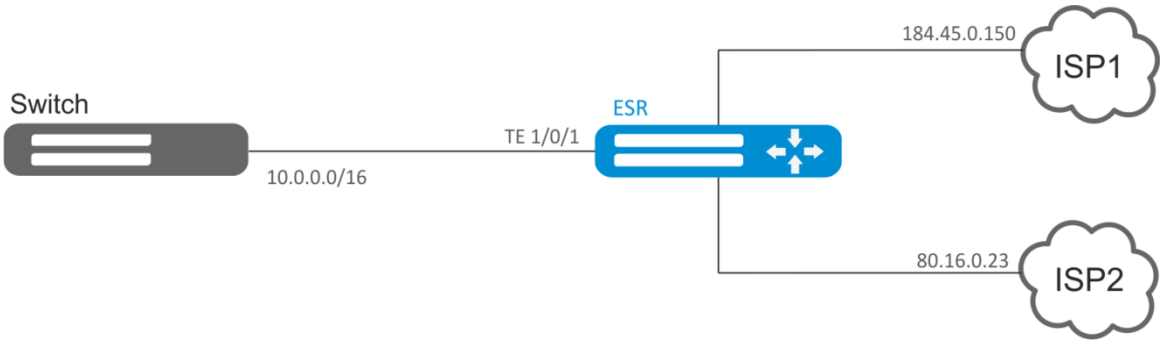

Рисунок 51 – Схема сети

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
```

7.26 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-м уровне модели OSI. В маршрутизаторе ESR 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.

7.26.1 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-20/21 – [1..250]; для ESR-1511/1500 – [1..500].
3	Указать экземпляр VRF, в котором будет работать данный GRE-туннель (не обязательно).	**esr(config-bridge)# 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)#	<IF> – интерфейс, от IP-адреса

		interface <IF>	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.
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-20/21 – [1..250]; для ESR-1511/1500 - [1..500]
10	Указать размер MTU (MaximumTransmitionUnit) 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-20/21 – [1280..9500]; для ESR-1511/1500 [1280..10000]. Значение по умолчанию: 1500.
11	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.
12	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.
13	Разрешить передачу ключа (Key) в туннельном заголовке GRE (в соответствии с RFC 2890) и установить значение ключа. Настраивается 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.
14	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**	

15	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**	
16	Включить проверку доступности удаленного шлюза туннеля (не обязательно)	**esr(config-gre)# keepalive enable**	
17	Задать 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
18	Задать 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
19	Задать 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
20	Включить отправку snmp-trap о включении/отключении туннеля.	**esr(config-gre)# snmp init-trap**	
21	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
22	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
23	Активировать туннель.	**esr(config-gre)# enable**	

7.26.2 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.

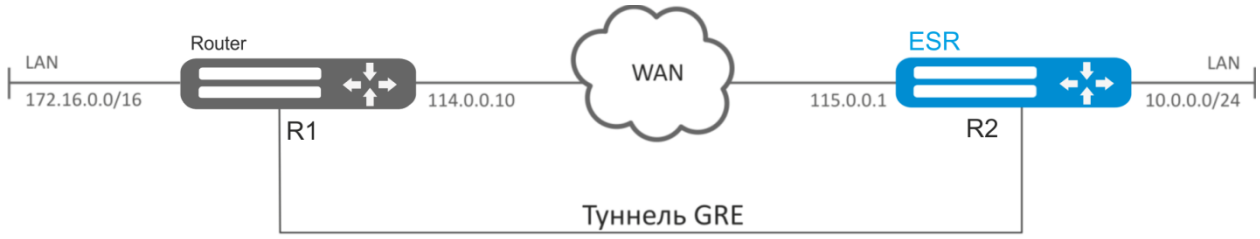

Рисунок 52 – Схема сети

Решение:

Предварительно на маршрутизаторах должны быть настроены интерфейсы для связи с сетью WAN разрешено получение пакетов протокола GRE из зоны безопасности, в которой работают интерфейсы, подключенные к сети WAN.

Создадим туннель GRE 10:

```
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 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).

7.27 Настройка L2TPv3-туннелей

L2TPv3 (Layer 2 Tunneling Protocol Version 3) – протокол для туннелирования пакетов 2-го 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 маршрутизаторе ESR 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.

7.27.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Сконфигурировать L3-интерфейс, от которого будет строиться L2TPv3-туннель.		
2	Создать L2TPv3-туннель и перейти в режим его конфигурирования.	**esr(config)# tunnel l2tpv3 <INDEX>**	<INDEX> – идентификатор туннеля в диапазоне: для ESR-20/21 – [1..250]; для ESR-1511/1500 – [1..500].
3	Указать описание	**esr(config-l2tpv3)#**	<DESCRIPTION> – описание туннеля,

	конфигурируемого туннеля (не обязательно).	**description <DESCRIPTION>**	задаётся строкой до 255 символов.
4	Указать экземпляр VRF, в котором будет работать данный L2TPV3-туннель (не обязательно).	**esr(config-l2tpv3)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.
5	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].
6	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].
7	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.
8	Установить локальный идентификатор сессии.	**esr(config-l2tpv3)# local session-id <SESSION-ID>**	<SESSION-ID> – идентификатор сессии, принимает значения [1..200000].
9	Установить удаленный идентификатор сессии.	**esr(config-l2tpv3)# remote session-id <SESSION-ID>**	<SESSION-ID> – идентификатор сессии, принимает значения [1..200000].
10	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].
11	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].
12	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-20/21 – [1..250]; для ESR-1511/1500 – [1..500]
13	Активировать туннель.	**esr(config-l2tpv3)# enable**	
14	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-20/21 - [1280..9500]; для ESR-1511/1500 [1280..10000]. Значение по умолчанию: 1500.
15	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.
16	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.

17	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.

7.27.2 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.

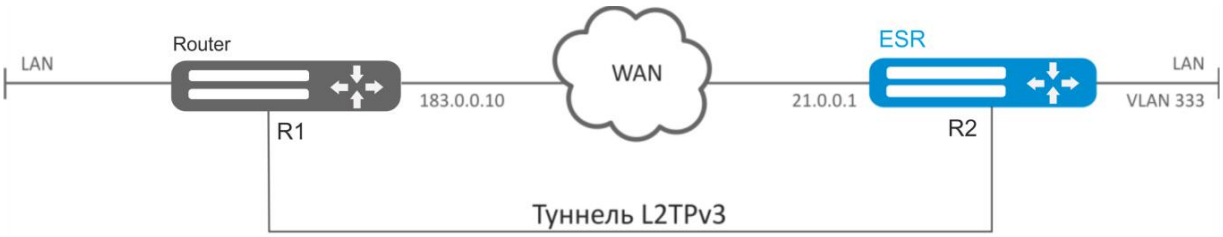

Рисунок 53 – Схема сети

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 7.20.2):

```
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 7.18):

```
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.

7.28 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.

7.28.1 Настройка Route-based IPsec VPN

7.28.1.1 Алгоритм настройки

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>**	<NAME> – имя зоны безопасности, задаётся строкой до 12 символов.
		esr(config-vti)# ip firewall disable	
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
10	Определить номер группы Диффи-Хеллмана. (не обязательно)	**esr(config-ike-proposal)# dh-group <DH-GROUP>**	<DH-GROUP> – номер группы Диффи-Хеллмана, принимает значения [1, 2, 5, 14, 15, 16, 17, 18]. Значение по умолчанию: 1

11	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; **rsa-public-key** – метод аутентификации, использующий RSA-сертификат. Значение по умолчанию: pre-shared-key
12	Создать ike-политику и перейти в режим её конфигурирования.	**esr(config)# security ike policy <NAME>**	<NAME> – имя политики IKE, задаётся строкой до 31 символа.
13	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
14	Привязать IKE-профиль к IKE-политике.	**esr(config-ike-policy)# proposal <NAME>**	<NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа.
15	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.
16	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.
17	Привязать IKE-политику к IKE-шлюзу.	**esr(config-ike-gw)# ike-policy <NAME>**	<NAME> – имя политики протокола IKE, задаётся строкой до 31 символа.
18	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
19	Установить режим перенаправления трафика в туннель - route-based.	**esr(config-ike-gw)# mode – route-based**	
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 секунд

23	Привязать VTI-туннель к IKE-шлюзу.	**esr(config-ike-gw)# bind-interface vti <VTI>**	<VTI> – идентификационный номер интерфейса VTI.
24	Создать в IPsec-профиль.	**esr(config)# security ipsec proposal <NAME>**	<NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа.
25	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
26	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
27	Указать протокол инкапсуляции для IPsec (не обязательно).	**esr(config-ipsec-proposal)# protocol <PROTOCOL>**	<PROTOCOL> – инкапсулирующий протокол, принимает значения: esp, ah Значение по умолчанию: esp
28	Создать IPsec-политику и перейти в режим её конфигурирования.	**esr(config)# security ipsec policy <NAME>**	<NAME> – имя политики IPsec, задаётся строкой до 31 символа.
29	Привязать IPsec-профиль к IPsec-политике	**esr(config-ipsec-policy)# proposal <NAME>**	<NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа.
30	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
31	Создать IPsec VPN и перейти в режим конфигурирования.	**esr(config)# security ipsecvpn <NAME>**	<NAME> – имя VPN, задаётся строкой до 31 символа.
32	Определить режим согласования данных, необходимых для активации VPN.	**esr(config-ipsec-vpn)# mode <MODE>**	<MODE> – режим работы VPN.
33	Привязать IPsec-политику к IPsec-VPN.	**esr(config-ipsec-vpn)# ike ipsec-policy <NAME>**	<NAME> – имя IPsec-политики, задаётся строка до 31 символа.

34	Задать значение DSCP для использования в IP-заголовке исходящих пакетов IKE-протокола (не обязательно).	**esr(config-ipsec-vpn)# ike dscp <DSCP>**	DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 63
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.
36	Осуществить привязку IKE-шлюза к IPsec-VPN.	**esr(config-ipsec-vpn)# ike gateway <NAME>**	<NAME> – имя IKE-шлюза, задаётся строкой до 31 символа.
37	Установить значение временного интервала в секундах, по истечению которого соединение закрывается, если не было принято или передано ни одного пакета через SA (не обязательно).	**esr(config-ipsec-vpn)# ike idle-time <TIME>**	<TIME> – интервал в секундах, принимает значения [4..86400].
38	Отключить пересогласование ключей до разрыва IKE-соединения по истечению времени, количеству переданных пакетов или байт (не обязательно).	**esr(config-ipsec-vpn)# ike rekey disable**	
39	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.
40	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%
41	Указать описание для IPsec-VPN (не обязательно).	**esr(config-ipsec-vpn)# description <DESCRIPTION>**	<DESCRIPTION> – описание профиля, задаётся строкой до 255 символов.
42	Активировать IPsec VPN.	**esr(config-ipsec-vpn)# enable**	

7.28.1.2 Пример настройки

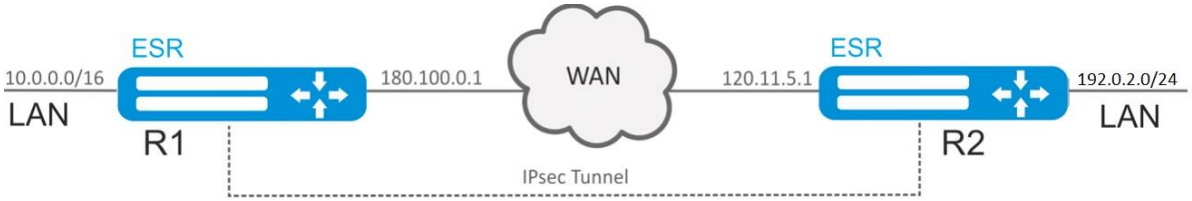

Рисунок 54 – Схема сети

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.

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 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 IPsec-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 IPsec-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).

7.28.2 Настройка Policy-based IPsec VPN

7.28.2.1 Алгоритм настройки

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-Хеллмана.	**esr(config-ike-proposal)# dh-group <DH-GROUP>**	<DH-GROUP> – номер группы Диффи-Хеллмана, 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; **rsa-public-key** – метод аутентификации, использующий RSA-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.
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	**esr(config-ike-gw)#mode<MODE>**	<MODE> – режим перенаправления трафика в

	туннель.		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.
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.

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: esp, ah.
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.
28	Привяжем 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].
34	Устанавливается 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**	
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**	

7.28.2.2 Пример настройки

Задача:

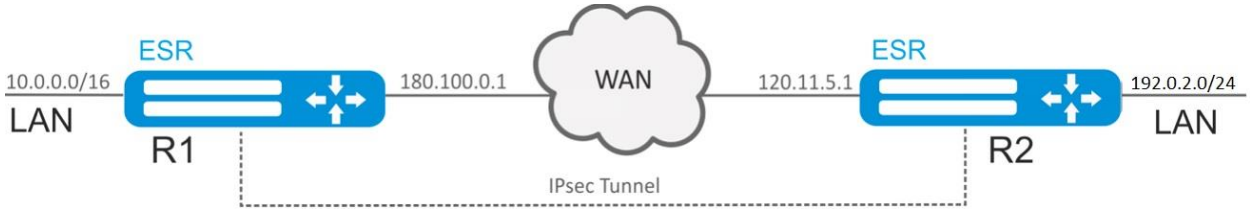

Рисунок 55 – Схема сети

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.

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 120.11.5.1/24
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 180.100.0.1
esr(config-ike-gw)# local network 10.0.0.0/16
esr(config-ike-gw)# remote address 120.11.5.1
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 IPsec-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 immediate
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
```

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 180.100.0.1
esr(config-ike-gw)# remote network 10.0.0.0/16
esr(config-ike-gw)# local address 120.11.5.1
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 IPsec-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 immediate
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).

7.29 Настройка LT-туннелей

LT (англ. Logical Tunnel - логический туннель) - тип туннелей, предназначенный для передачи маршрутной информации и трафика между различными виртуальными маршрутизаторами (VRF Lite), сконфигурированными на одном аппаратном маршрутизаторе. LT-туннель может использоваться для организации взаимодействия между двумя или более VRF с применением ограничений firewall.

7.29.1 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].
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-20/21 - [1280..9500]; для ESR-1511/1500 [1280..10000]. Значение по умолчанию: 1500.

7.29.2 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 работает 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
```

7.30 Настройка 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.

7.30.1 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	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.

3	Указать описание конфигурируемого сервера (не обязательно).	**esr(config-pptp-server)# description <DESCRIPTION>**	<DESCRIPTION> – описание PPTP-сервера, задаётся строкой до 255 символов.
4	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.
5	Указать DSCP-приоритет исходящих пакетов (не обязательно).	**esr(config-pptp-server)# dscp <DSCP>**	<DSCP>– dscp приоритет исходящих пакетов [0..63].
6	Включить шифрование MPPE для PPTP-соединений (не обязательно).	**esr(config-pptp-server)# encryption mppe**	
7	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].
8	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.
9	Указать IP-адрес, который должен обрабатывать PPTP-сервер.	**esr(config-pptp-server)# outside-address { object-group <OBJ-GROUP-NETWORK-NAME> | ip-address <ADDR> }**	<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].
10	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].
11	Включить PPTP-сервер в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall.	**esr(config-pptp-server)# security-zone <NAME>**	<NAME> – имя зоны безопасности, задаётся строкой до 31 символа.
12	Указать имя пользователя (при использовании локальной аутентификации пользователей).	**esr(config-pptp-server) username <NAME>**	<NAME> – имя пользователя, задаётся строкой до 12 символов.

13	Указать пароль пользователя.	**esr(config-pptp-user) password ascii-text { <PASSWORD> | encrypted <PASSWORD> }**	<PASSWORD> - пароль пользователя, задается строкой до 32 символов.
14	Активировать пользователя.	**esr(config-pptp-user) enable**	
15	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.

7.30.2 Пример настройки PPTP-сервера

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.

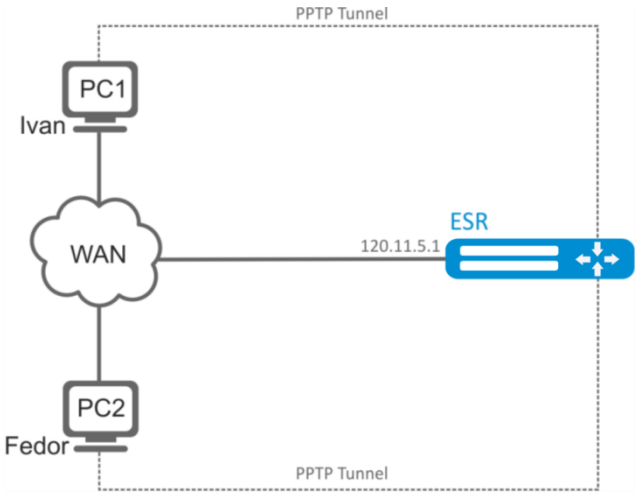

Рисунок 56 – Схема сети

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 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 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.

7.31 Настройка 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.

7.31.1 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	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.
3	Указать описание конфигурируемого сервера (не обязательно).	**esr(config-l2tp-server)# description <DESCRIPTION>**	<DESCRIPTION> – описание L2TP-сервера, задаётся строкой до 255 символов.
4	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.
5	Указать DSCP приоритет исходящих пакетов.	**esr(config-l2tp-server)# dscp <DSCP>**	<DSCP> – dscp приоритет исходящих пакетов [0..63].
6	Включить сервер.	**esr(config-l2tp-server)# enable**	
7	Выбрать метод аутентификации по ключу для IKE-соединения.	**esr(config-l2tp-server)# ipsec authentication method pre-shared-key**	
8	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.
9	Указать IP-адрес локального шлюза	**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].
10	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.
11	Указать IP-адрес, который должен слушать L2TP-сервер.	**esr(config-l2tp-server)# outside-address object-group <OBJ-GROUP-NETWORK-NAME> ip-address <ADDR>**	<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].
12	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].
13	Включить L2TP-сервер в зону безопасности и настроить правила взаимодействия между зонами.	**esr(config-l2tp-server)# security-zone <NAME>**	<NAME> – имя зоны безопасности, задаётся строкой до 31 символа.
14	Указать имя пользователя (при использовании локальной базы аутентификации).	**esr(config-l2tp-server) username <NAME>**	<NAME> – имя пользователя, задаётся строкой до 12 символов.
15	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.
16	Включить пользователя.	**esr(config-l2tp-user) enable**	
17	Указать список WINS-серверов, которые будут использовать удаленные пользователи (не	**esr(config-l2tp-server)# wins-servers object-group <OBJ-**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит адреса необходимых

	обязательно).	GROUP-NETWORK-NAME>	WINS-серверов, задаётся строкой до 31 символа.

7.31.2 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».

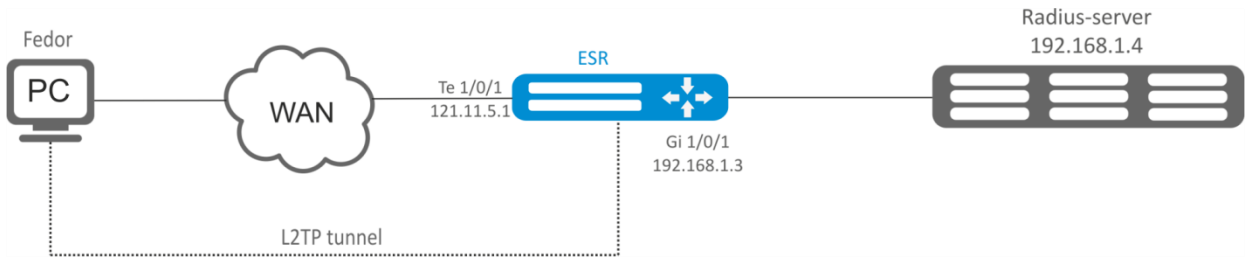

Рисунок 57 – Схема сети

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.

7.32 Настройка 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.

7.32.1 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 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].
3	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.
4	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.
5	Включить блокировку передачи данных между клиентами (не обязательно).	**esr(config-openvpn-server)# client-isolation**	
6	Устанавливается максимальное количество одновременных пользовательских сессий (не обязательно).	**esr(config-openvpn-server)# client-max <VALUE>**	<VALUE> – максимальное количество пользователей, принимает значения [1..65535].
7	Включается механизм сжатия передаваемых данных между клиентами и сервером OpenVPN (не обязательно).	**esr(config-openvpn-server)# compression**	
8	Указать описание конфигурируемого сервера (не обязательно).	**esr(config-openvpn-server)# description <DESCRIPTION>**	<DESCRIPTION> – описание OpenVPN-сервера, задаётся строкой до 255 символов.
9	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];
10	Выбрать алгоритм шифрования, используемый при передачи данных.	**esr(config-openvpn-server)# encryption algorithm <ALGORITHM>**	<ALGORITHM> – идентификатор протокола шифрования, принимает значения: 3des,blowfish128, aes128.
11	Определим подсеть, из которой выдаются IP-адреса пользователям. (только для	**esr(config-openvpn-server)# network <ADDR/LEN>**	<ADDR/LEN> – адрес подсети, имеет следующий формат: AAA.BBB.CCC.DDD/EE – IP-адрес

	tunnel ip)		подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32];
12	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].
13	Указать инкапсулируемый протокол.	**esr(config-openvpn-server)# protocol <PROTOCOL>**	<PROTOCOL> – тип инкапсуляции, возможные значения: **TCP**-инкапсуляция в TCP-сегменты; **UDP**-инкапсуляция в UDP-дейтаграммы.
14	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**	
15	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];
16	Включить OpenVPN-сервер в зону безопасности и настроить правила взаимодействия между зонами.	**esr(config-openvpn-server)# security-zone <NAME>**	<NAME> – имя зоны безопасности, задаётся строкой до 31 символа.
17	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].
18	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].
19	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.
20	Определить подсеть для указанного пользователя OpenVPN-сервера (при использовании локальной базы для аутентификации пользователей).	**esr(config-openvpn-server)# username <NAME>subnet <ADDR/LEN>**	<NAME> – имя пользователя, задаётся строкой до 31 символа. <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].
21	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].
22	Включить профиль OpenVPN-сервера.	**esr(config-openvpn-server)# enable**	

7.32.2 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.

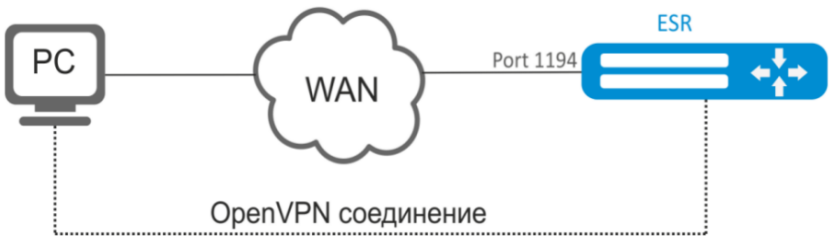

Рисунок 58 – Схема сети

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.

7.33 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.

7.33.1 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.
2	Указать описание конфигурируемого клиента (не обязательно).	**esr(config-pppoe)# description <DESCRIPTION>**	<DESCRIPTION> – описание PPPoE-сервера, задаётся строкой до 255 символов.
3	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
4	Включить отказ от получения маршрута по умолчанию от PPPoE-сервера (не обязательно).	**esr(config-pppoe)# ignore-default-route**	
5	Указать интерфейс через который будет устанавливаться PPPoE соединение.	**esr(config-pppoe)# interface <IF>**	<IF> – интерфейс или группа интерфейсов.
6	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 сек)
7	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-20/21 - [1280..9500]; для ESR-1511/1500 [1280..10000]. Значение по умолчанию: 1500.
8	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.

9	Указать имя экземпляра VRF, в котором будут использоваться указанные сетевой интерфейс, мост, зона безопасности, сервер динамической авторизации (DAS) или группа правил NAT. (не обязательно)	**esr(config-pppoe)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.
10	Отключения функции Firewall на сетевом интерфейсе (не обязательно)	**esr(config-pppoe)# ip firewall disable**	
	Настройка зоны безопасности	**esr(config-pppoe)#security-zone <NAME>**	<NAME>-имя зоны безопасности, задаётся строкой до 31 символа.
11	Активировать конфигурируемый профиль	**esr(config-pppoe)# enable**	

7.33.2 Пример настройки PPPoE-клиента

Задача:

Настроить PPPoE-клиент на маршрутизаторе.

- Учетные записи для подключения – tester;
- Пароли учетных записей – password;
- Подключение должно осуществляться с интерфейса gigabitethernet 1/0/7.

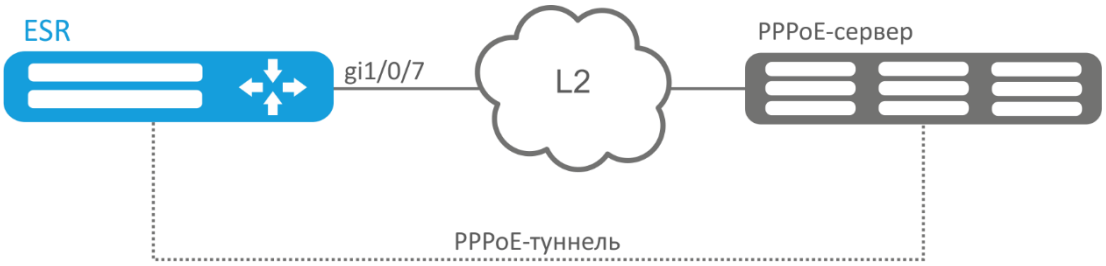

Рисунок 59 – Схема сети

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
```

7.34 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.

7.34.1 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 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
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	Указать описание конфигурируемого туннеля (не обязательно).	**esr(config-pptp)# description <DESCRIPTION>**	<DESCRIPTION> – описание туннеля, задается строкой до 255 символов.
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-20/21 - [552..9500]; для ESR-1511/1500 [552..10000]. Значение по умолчанию: 1500.
7	Игнорировать маршрут по умолчанию через данный PPTP-туннель (не обязательно)	**esr(config-pptp)# ignore-default-route**	
8	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
9	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.

10	Включить PPTP-туннель в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall (не обязательно).	**esr(config-pptp)# security-zone <NAME>**	<NAME> – имя зоны безопасности, задаётся строкой до 31 символа.
11	Задать исключение обработки входящего трафика в Firewall (не обязательно).	**esr(config-pptp)# ip firewall disable**	
12	Активировать туннель	**esr(config-pptp)# enable**	

7.34.2 Пример настройки удаленного подключения по PPTP-протоколу

Задача:

Настроить PPTP-туннель на маршрутизаторе:

- адрес PPTP-сервера 20.20.0.1;
- учетная запись для подключения – логин: ivan, пароль: simplepass.

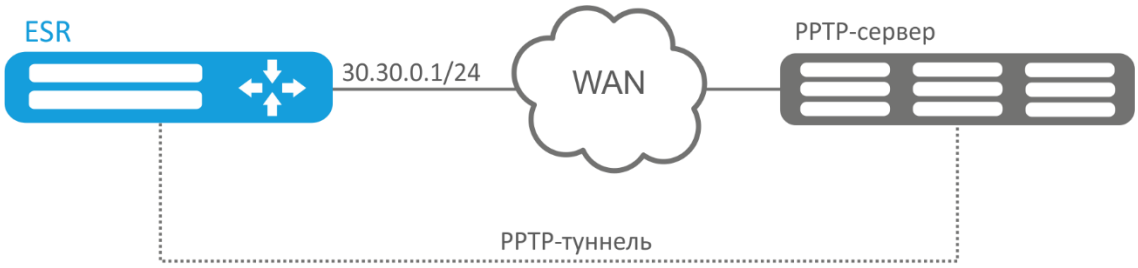

Рисунок 60 – Схема сети

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
```

7.35 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.

7.35.1 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 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
3	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.
4	Указать описание конфигурируемого туннеля (не обязательно).	**esr(config-l2tp)# description <DESCRIPTION>**	<DESCRIPTION> – описание туннеля, задается строкой до 255 символов.
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].
6	Установить размер MTU (MaximumTransmitionUnit) для туннеля (не обязательно)	**esr(config-l2tp)# mtu <MTU>**	<MTU> – значение MTU, принимает значения в диапазоне: для ESR-20/21 - [552..9500]; для ESR-1511/1500 [552..10000]. Значение по умолчанию: 1500.
7	Игнорировать маршрут по умолчанию через данный L2TP-туннель (не обязательно)	**esr(config-l2tp)# ignore-default-route**	
8	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

9	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.
10	Выбрать метод аутентификации по ключу для IKE-соединения.	**esr(config-l2tp-server)# ipsec authentication method pre-shared-key**	
11	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.
12	Включить L2TP-туннель в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall (не обязательно).	**esr(config-l2tp)# security-zone <NAME>**	<NAME> – имя зоны безопасности, задаётся строкой до 31 символа.
13	Задать исключение обработки входящего трафика в Firewall (не обязательно).	**esr(config-l2tp)# ip firewall disable**	
14	Активировать туннель	**esr(config-l2tp)# enable**	

7.35.2 Пример настройки удаленного подключения по L2TP-протоколу

Задача:

Настроить PPTP-туннель на маршрутизаторе:

- адрес PPTP сервера 20.20.0.1;
- учетная запись для подключения – логин: ivan, пароль: simplepass

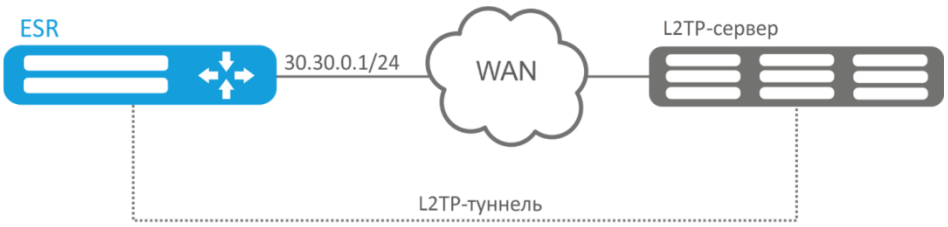

Рисунок 61 – Схема сети

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
```

7.36 Настройка QoS

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.

7.36.1 Базовый QoS

7.36.1.1 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.
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].
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 веса 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.
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.

7.36.1.2 Пример настройки

Задача:

Настроить следующие ограничения на интерфейсе gigabitethernet 1/0/8: передавать трафик с DSCP 22 в первую приоритетную очередь, трафик с DSCP 14 в седьмую взвешенную очередь, установить ограничение по скорости в 60 Мбит/с для седьмой очереди.

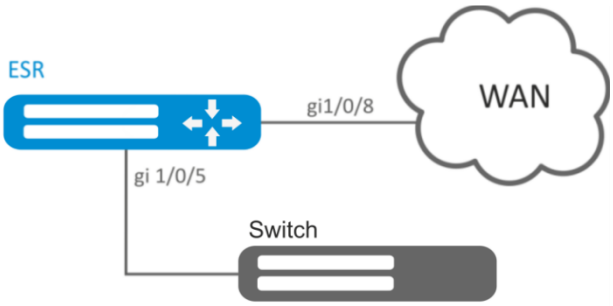

Рисунок 62 – Схема сети

Решение:

Для того чтобы первая очередь осталась приоритетной, а очереди со второй по восьмую 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 1
```

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 60Мбит/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
```

7.36.2 Расширенный QoS

7.36.2.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать списки доступа		См. Раздел Настройка списков доступа

	для определения трафика, к которому должен быть применен расширенный QOS.		(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].
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> [BURST]**	<BANDWIDTH> – гарантированная полоса трафика в Кбит/с, принимает значение [64..10000000]; <BURST> – размер сдерживающего порога в КБайт, принимает значение [4..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**	
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 неклассифицированный 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> [BURST]**	<BANDWIDTH> – гарантированная полоса трафика в Кбит/с, принимает значение [64..10000000]; <BURST> – размер сдерживающего порога в КБайт, принимает значение [4..16000]. По умолчанию 128 КБайт.
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> [BURST]**	
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**.
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.
21	Определить параметры RED (Random Early Detection). (при необходимости)	**esr(config-class-policy-map)# random-detect <LIMIT><MAX><MIN><PROBABILITY>**	<LIMIT> – предельный размер очереди в байтах, принимает значения в диапазоне [1..1000000]; <MAX> – максимальный размер очереди в байтах, принимает значения в диапазоне [1..1000000]; <MIN> – минимальный размер очереди в байтах, принимает значения в диапазоне [1..1000000]; <PROBABILITY> – вероятность отбрасывания пакетов, принимает значения [0..100]. При указании значений должны выполняться следующие правила: <MAX>> 2 * <MIN> <LIMIT>> 3 * <MAX>
22	Определить параметры GRED (Generalized Random Early Detection). (при необходимости)	**esr(config-class-policy-map)# random-detect precedence <PRECEDENCE><LIMIT><MAX><MIN><PROBABILITY>**	<PRECEDENCE> – значение IPPrecendence [0..7]; <LIMIT> – предельный размер очереди в байтах, принимает значения в диапазоне [1..1000000]; <MAX> – максимальный размер очереди в байтах, принимает значения в диапазоне [1..1000000]; <MIN> – минимальный размер очереди в байтах, принимает значения в диапазоне [1..1000000]; <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**	

25	Назначить политику QoS на сконфигурируемом интерфейсе/туннеле/сетевом мосту для классификации входящего (input) или приоритезации исходящего (output) трафика.	**esr(config-if-gi)# service-policy { input | output } <NAME>**	<NAME> – имя QoS-политики, задаётся строкой до 31 символа.

7.36.2.2 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.

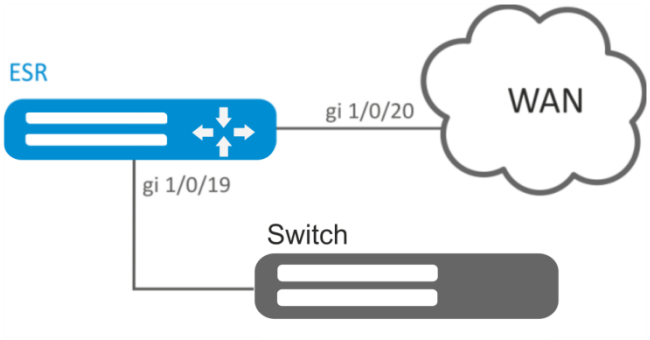

Рисунок 63 – Схема сети

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 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
```

7.37 Настройка зеркалирования

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).

7.37.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Включить режим удаленного	`esr(config)# port monitor remote`	

	зеркалирования (в случае использования удаленного зеркалирования).		
2	Определить режим порта передающего отзеркалированный трафик.	**esr(config)# port monitor mode <MODE>**	<MODE> – режим: **network** – совмещенный режим передачи данных и зеркалирование; **monitor-only** – только зеркалирование.
3	В режиме конфигурации интерфейса включить зеркалирование.	**esr(config-if-gi)# port monitor interface <IF><DIRECTION>**	<IF> – интерфейс в который будет осуществляться зеркалирование; <DIRECTION> – направление трафика: **tx** – зеркалирование только исходящего трафика; **rx** – зеркалирование только входящего трафика.

7.37.2 Пример настройки

Задача:

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

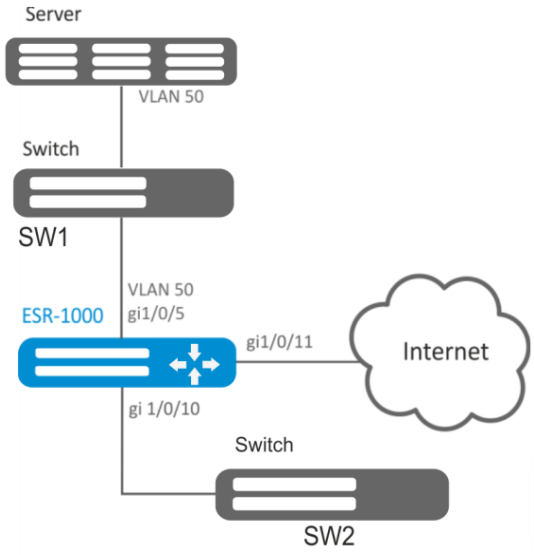

Рисунок 64 – Схема сети

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
```

7.38 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.

7.38.1 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.
3	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.
4	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.
5	Активировать Netflow на маршрутизаторе.	**esr(config)# netflow enable**	
6	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].
7	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.
8	Включить отправку статистики на Netflow-сервер в режим конфигурирования интерфейса/туннеля/ сетевого моста.	**esr(config-if-gi)# ip netflow export**	

7.38.2 Пример настройки

Задача:

Организовать учет трафика с интерфейса gi1/0/1 для передачи на сервер через интерфейс gi1/0/8 для обработки.

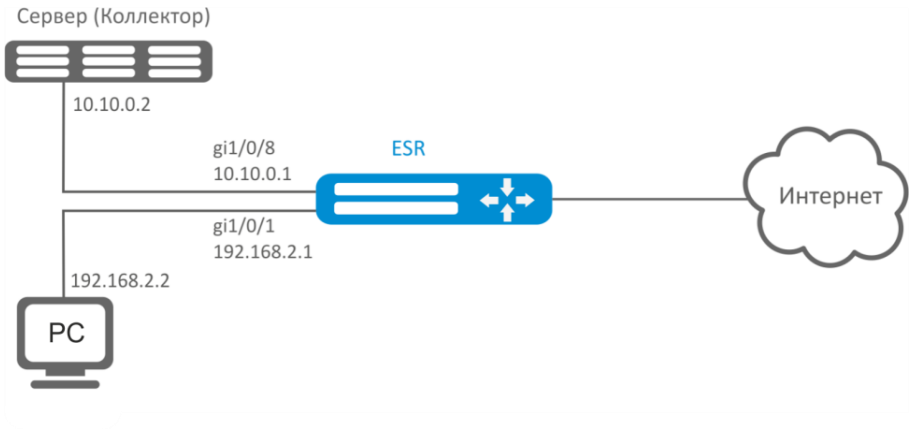

Рисунок 65 – Схема сети

Решение:

Предварительно нужно выполнить следующие действия:

- На интерфейсах gi1/0/1, gi1/0/8 отключить firewall командой «ip firewall disable».
- Назначить IP-адреса на портах.

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 7.39 Настройка sFlow.

7.39 Настройка sFlow

Sflow — стандарт для мониторинга компьютерных сетей, беспроводных сетей и сетевых устройств, предназначенный для учета и анализа трафика.

7.39.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Установить частоту отправки пакетов	`esr(config)# sflow sampling-rate <RATE>`	<RATE> – частота отправки пакетов пользовательского трафика на

	пользовательского трафика в неизменном виде на sFlow-коллектор.		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 режим конфигурирования интерфейса/туннеля/ сетевого моста.	**esr(config-if-gi)# ip sflow export**	

7.39.2 Пример настройки

Задача:

Организовать учет трафика между зонами trusted и untrusted.

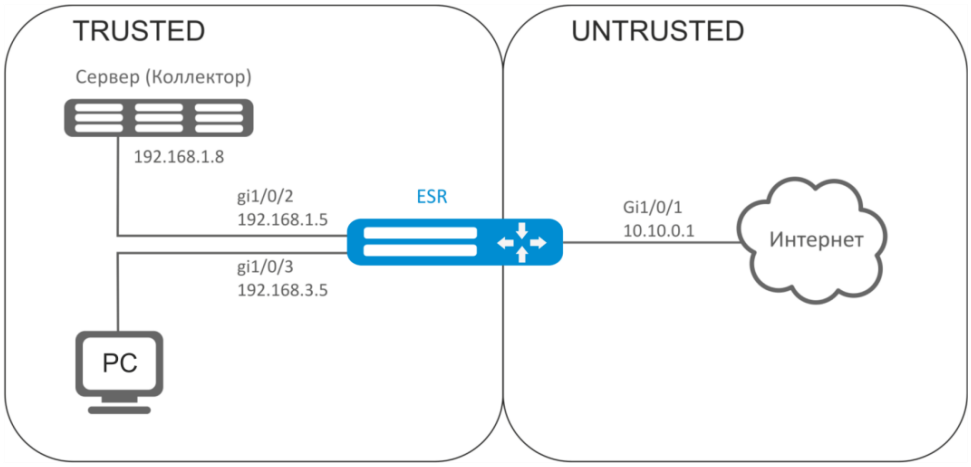

Рисунок 66 – Схема сети

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 7.38 Настройка Netflow .

7.40 Настройка LACP

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

7.40.1 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.
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.

7.40.2 Пример настройки

Задача:

Настроить агрегированный канал между маршрутизатором ESR и коммутатором.

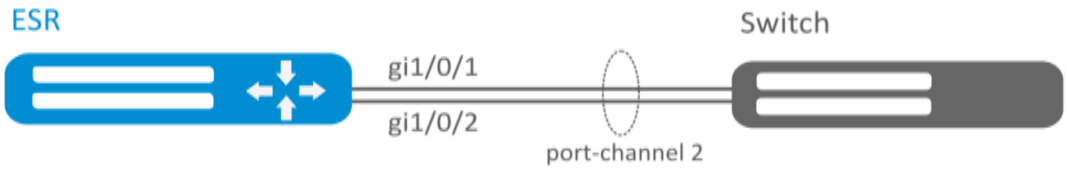

Рисунок 67 – Схема сети

Решение:

Предварительно нужно 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.

7.41 Настройка VRRP

VRRP (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.

7.41.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим конфигурирования интерфейса/туннеля/ 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/туннеле/ сетевом мосту, включая IP-адрес		
3	Включить VRRP-процесс на IP-интерфейсе.	**esr(config-if-gi)# vrrp**	
		esr(config-if-gi)# ipv6 vrrp	
4	Установить виртуальный IP-адрес VRRP-маршрутизатора.	**esr(config-if-gi)# vrrp ip <ADDR/LEN>**	<ADDR/LEN> – виртуальный IP-адрес, 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 4 IP-адресов на интерфейс.

		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 8ми 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.	**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 произведется смена ролей.	**esr(config-if-gi)# vrrp group <GRID>**	<GRID> – идентификатор группы VRRP-маршрутизатора, принимает значения [1..32].
		esr(config-if-gi)# ipv6 vrrp group <GRID>	
8	Установить IP-адрес, который будет использоваться в качестве IP-адреса отправителя для VRRP-сообщений.	**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	**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.	**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.	**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.	**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.	**esr(config-if-gi)# vrrp timers garp refresh-repeat <COUNT>**	<COUNT> –количество сообщений, принимает значения [1..60]. Значение по умолчанию: 1.
14	Определить, будет ли Backup-маршрутизатор с более высоким приоритетом пытаться перехватить на себя роль Master у текущего Master-маршрутизатора с более низким приоритетом.	**esr(config-if-gi)# vrrp preemption disable** **esr(config-if-gi)# ipv6 vrrp preemption 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.	**esr(config-if-gi)# vrrp preemption delay <TIME>** **esr(config-if-gi)# ipv6 vrrp preemption delay <TIME>**	<TIME> – время ожидания, определяется в секундах [1..1000]. Значение по умолчанию: 0
16	Установить пароль для аутентификации с соседом.	**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.	**esr(config-if-gi)# vrrp authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм аутентификации: - **cleartext** – пароль, передается открытым текстом; - **md5** – пароль хешируется по алгоритму md5.
18	Задать версию VRRP-протокола.	**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.	**esr(config-if-gi)# ipv6 vrrp timers nd delay <TIME>**	<TIME> – время в секундах, принимает значения [1..60]. Значение по умолчанию: 5
21	Определить период обновления информации протокола ND для ipv6 vrrp в состоянии MASTER.	**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.	**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.	**esr(config-if-gi)# ipv6 vrrp timers nd repeat <NUM>**	<NUM> – количество, принимает значения [1..60]. Значение по умолчанию: 1

7.41.2 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.

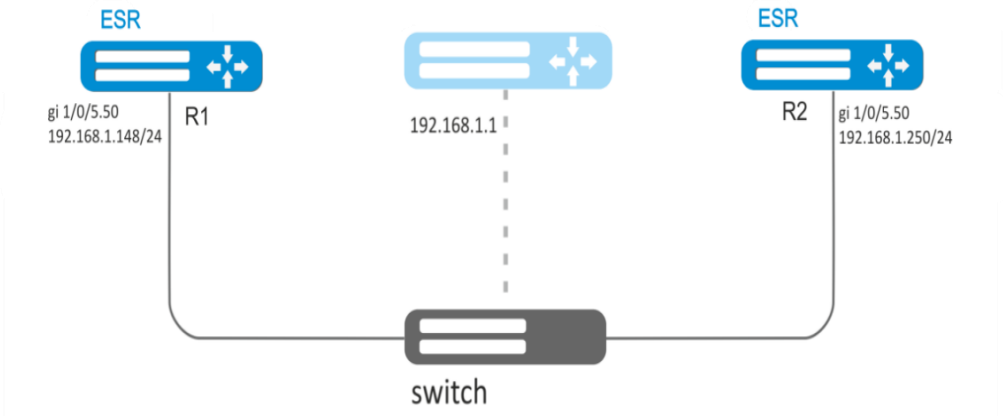

Рисунок 68 – Схема сети

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
```

Произвести аналогичные настройки на R2.

7.41.3 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.

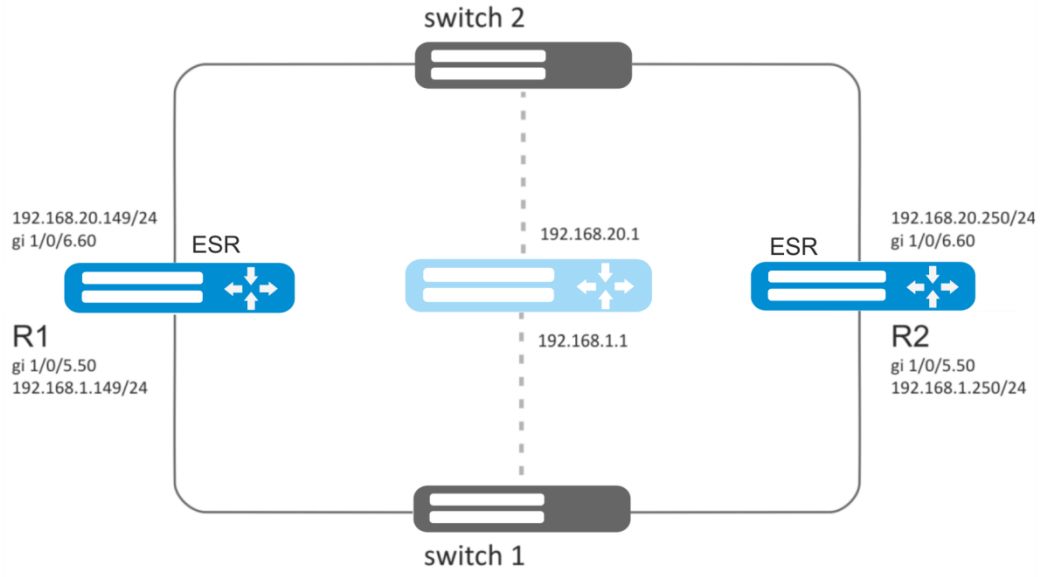

Рисунок 69 – Схема сети

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).

7.42 Настройка VRRP tracking

VRRP tracking — механизм позволяющий активировать статические маршруты в зависимости от состояния VRRP.

7.42.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Настроить VRRP согласно разделу 7.6.1.		
2	Добавить в систему Tracking-объект и перейти в режим настройки параметров Tracking-объекта.	**esr(config)#tracking <ID>**	<ID> – номер Tracking-объекта, принимает значения [1..60].
3	Задать правило слежения за состоянием VRRP-процесса.	**esr(config-tracking)# vrrp <VRID> [not] state { master | backup | fault }**	<VRID> – идентификатор отслеживаемого VRRP-маршрутизатора, принимает значения [1..255].
4	Включить Tracking-объект.	**esr(config-**	

		tracking)#enable	
5	Создать статический IP-маршрут к указанной подсети с указанием Tracking-объекта.	**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 4.2; <TUN> – имя туннеля, задаётся в виде, описанном в разделе 4.3; <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); [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.

7.42.2 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. Так же 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.

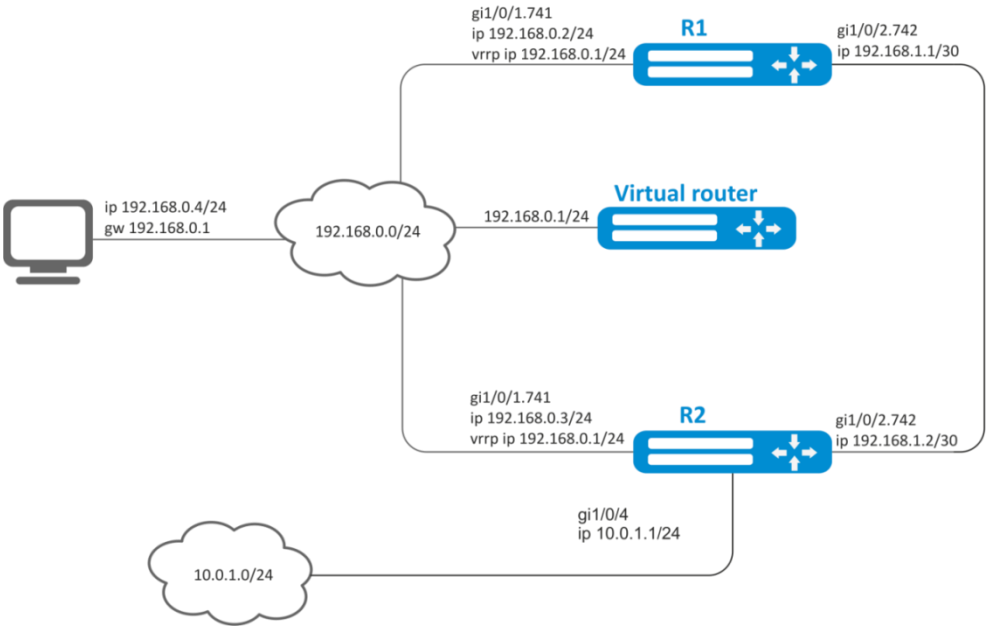

Рисунок 70 – Схема сети

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 tracking-object с соответствующим условием:

```
R1(config)# tracking 1
R1(config-tracking)# vrrp 10 state master
R1(config-tracking)# enable
R1(config-tracking)# exit
```

Создадим статический маршрут в подсеть 10.0.1.0/24 через 192.168.1.2, который будет работать в случае удовлетворения условия из tracking 1:

```
R1(config)# ip route 10.0.1.0/24 192.168.1.2 track 1
```

7.43 Настройка VRF Lite

VRF (Virtual Routing and Forwarding) – технология, которая позволяет изолировать маршрутную информацию, принадлежащую различным классам (например, маршруты одного клиента).

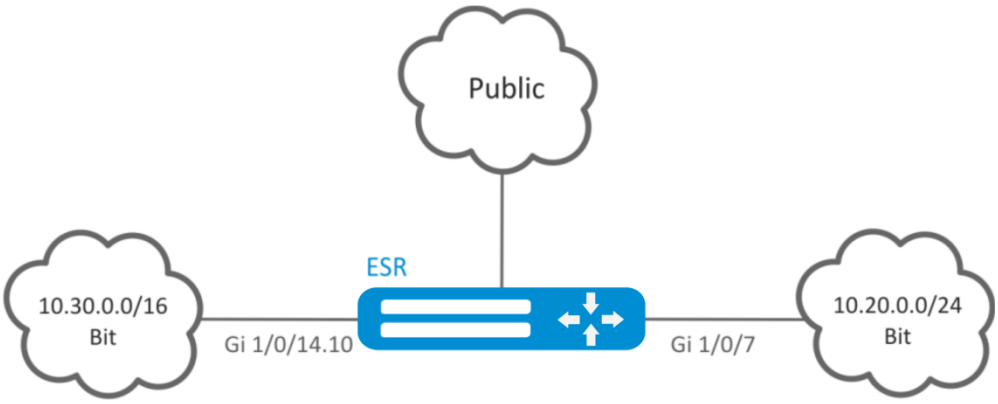

Рисунок 71 – Схема сети

7.43.1 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 конфигурируемомого экземпляра VRF.	`esr(config-vrf)# description <DESCRIPTION>`	<DESCRIPTION> – описание экземпляра VRF, задаётся строкой до 255 символов.
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-1511/1500 [1..500000], ESR-20/21 [1..300000]. BGP ESR-1511/1500 [1..2800000], ESR-20/21 [1..1500000]. Значение по умолчанию: 0
4	Включить и настроить протоколы динамической маршрутизации трафика (Static/OSPF/BGP) в экземпляре VRF (не обязательно). См. соответствующий раздел 7.17, 7.22 и 7.23.		
5	В режиме конфигурирования физического/логического интерфейса, туннеля, правила DNAT/SNAT, DAS-сервера или SNMPv3 пользователя указать имя экземпляра VRF для	`esr(config-snat-ruleset)# ip vrf forwarding <VRF>`	<VRF> – имя экземпляра VRF, задается строкой до 31 символа.

	которого будет использоваться (при необходимости).		
6	Настроить LT-туннель для передачи трафика в глобальный режим или другие VRF (при необходимости).		

7.43.2 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
```

7.44 Настройка MultiWAN

Технология MultiWAN позволяет организовать отказоустойчивое соединение с резервированием линков от нескольких провайдеров, а также решает проблему балансировки трафика между резервными линками.

7.44.1 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].
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 устройства; <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].
		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 13-17 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>** **esr(config-if-gi)# ipv6 wan load-balance failure-count <VALUE>**	<VALUE> – количество попыток, определяется в диапазоне [1..10]. Значение по умолчанию 1.
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>** **esr(config-if-gi)# ipv6 wan load-balance success-count <VALUE>**	<VALUE> – количество попыток, определяется в диапазоне [1..10]. Значение по умолчанию 1.

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.
		`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 одного 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 (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].
		`esr(config)# ipv6 route <SUBNET> wan load-balance rule <ID> [<METRIC>]`	

7.44.2 Пример настройки

Задача:

Настроить маршрут к серверу (108.16.0.1/28) с возможностью балансировки нагрузки.

Рисунок 72 – Схема сети

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
```

7.45 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.

7.45.1 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).
5	Установить минимальное значение	**esr(config-ntp)# minpoll <INTERVAL>**	<INTERVAL> – минимальное значение интервала опроса в секундах,

	интервала времени между отправкой сообщений NTP-серверу (не обязательно).		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 NTPдля определенного профиля IP-адресов (не обязательно)	**esr(config)# ntp object-group query-only <NAME>**	<NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.
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-адресадля NTP-пакетов для всех peer (не	**esr(config)# ntp source address <ADDR>**	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

	обязательно)		
16	Задать текущее 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, принимаетзначения[January/February/March/April/May/June/July/August/September/October/November/December]; <YEAR> – год, принимает значения [2001..2037].

7.45.2 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.

Рисунок 73 – Схема сети

Решение:

Предварительно нужно выполнить следующие действия:

- указать зону безопасности для интерфейса gi1/0/1;
- настроить IP-адрес для интерфейсов gi1/0/1.

```
security zone untrust
exit
object-group service NTP
port-range 123
exit
interface gigabitethernet 1/0/1
security-zone untrust
ip address 192.168.52.10/24
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
```

Настроика 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
```

7.46 Настройка SNMP

SNMP (англ. Simple Network Management Protocol — простой протокол сетевого управления) — протокол, предназначенный для управления устройствами в IP-сетях на основе архитектур TCP/UDP. SNMP предоставляет данные для управления в виде переменных, описывающих конфигурацию управляемой системы.

7.46.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Включить SNMP-сервер	**esr(config)# snmp-server**	
2	Определить community для доступа по протоколу SNMPv2c.	**esr(config)# snmp-server community <COMMUNITY> [<TYPE>] [{ <IP-ADDR> | <IPV6-ADDR>] [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]; <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.
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: **md5** – пароль шифруется по алгоритму md5; **sha1** – пароль шифруется по алгоритму sha1.
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	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].
14	Активировать SNMPv3-пользователя.	**esr(config-snmp-user)# enable**	Значение по умолчанию: процесс выключен.
15	Определить алгоритм шифрования передаваемых данных.	**esr(config-snmp-user)# privacy algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм шифрования: **aes128** – использовать алгоритм шифрования AES-128; **des** – использовать алгоритм шифрования DES.
16	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...).
	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.
17	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.
18	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.
19	Установить фильтрацию на отправляемые SNMP-уведомления.	**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. Справочник команд CLI.
20	Создать профиль snmp view, позволяющий разрешать или запрещать доступ к тем или иным OID для	**esr(config)# snmp-server enable traps <TYPE>**	<VIEW-NAME> – имя профиля SNMP view, задаётся строкой до 31 символа.

	community (SNMPv2) и user (SNMPv3).		

7.46.2 Пример настройки

Задача:

Настроить SNMPv3 сервер с аутентификацией и шифрованием данных для пользователя admin. IP-адрес маршрутизатора esr - 192.168.52.41, IP-адрес сервера – 192.168.52.8.

Рисунок 74 – Схема сети

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
```

7.47 Настройка Syslog

Syslog (англ. system log – системный журнал) – стандарт отправки и регистрации сообщений о происходящих в системе событиях, используется в сетях, работающих по протоколу IP.

7.47.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Задать уровень syslog-сообщений, которые будут передаваться SNMP-Traps сообщениями (не обязательно)	**esr(config)# syslog alarms <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.
2	Задать уровень syslog-сообщений, которые будут отображаться при удаленных подключениях (Telnet, SSH) (не обязательно)	**esr(config)# syslog monitor <SEVERITY>**	
3	Включить процесс логирования введённых команд пользователя на локальный syslog-сервер (не обязательно)	**esr(config)# syslog cli-commands**	
4	Включить сохранение сообщений syslog заданного уровня важности в указанный файл журнала	**esr(config)# syslog file <NAME> <SEVERITY>**	<NAME> – имя файла, в который будет производиться запись сообщений заданного уровня, задается строкой до 31 символа; <SEVERITY> описано в команде syslog alarms.
5	Указать максимальный размер файла журнала (не обязательно)	**esr(config)# syslog file-size <SIZE>**	<SIZE> – размер файла, принимает значение [10..10000000] кбайт

6	Задать максимальное количество файлов, сохраняемых при ротации (не обязательно)	**esr(config)# syslog max-files <NUM>**	<NUM> – максимальное количество файлов, принимает значения [1.. 1000]
7	Включить передачу сообщений syslog заданного уровня важности на удаленный syslog-сервер	**esr(config)#syslog host <HOSTNAME> <ADDR> <SEVERITY> <TRANSPORT> <PORT>**	<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]; <SEVERITY> – уровень важности сообщения, опциональный параметр, возможные значения приведены в разделе 0; <TRANSPORT> – протокол передачи данных, опциональный параметр, 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
8	Включить вывод отладочных сообщений во время загрузки устройства (не обязательно)	**esr(config)#syslog reload debugging**	
9	Включить нумерацию сообщений (не обязательно)	**esr(config)#syslog sequence-numbers**	
10	Включить точность даты сообщений до миллисекунд (не обязательно).	**esr(config)#syslog timestamp msec**	
11	Включить регистрацию неудачных аутентификаций (не обязательно).	**esr(config)#logging login on-failure**	
12	Включить регистрацию изменений настроек системы аудита (не обязательно).	**esr(config)#logging syslog configuration**	
13	Включить регистрацию изменений настроек пользователя (не обязательно).	**esr(config)#logging userinfo**	

7.47.2 Пример настройки Syslog

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.

Рисунок 75 – Схема сети

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
```

7.48 Проверка целостности

Проверка целостности подразумевает проверку целостности хранимых исполняемых файлов.

Процесс настройки

Шаг	Описание	Команда	Ключи
1	Запустить проверку целостности системы	`esr# verify filesystem`	detailed – детальный вывод информации в консоль

Пример конфигурации

Задача:

Проверить целостность файловой системы:

Решение:

Основной этап конфигурирования:

Запускаем проверку целостности:

```
esr# verify filesystem
Filesystem Successfully Verified
```

8 БЕЗОПАСНАЯ НАСТРОЙКА

Правила безопасной настройки подходят для большинства инсталляций. Настоящие ограничения 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 правил может привести к неработоспособности сети. При настройке устройства следует в первую очередь следовать техническим требованиям и регламентам сетей, в которых будет эксплуатироваться данное устройство.

8.1 Общие ограничения

- ✓ Всегда отключайте не используемые физические интерфейсы с помощью команды **shutdown**. Команда подробно описана в разделе 10.1.13 справочника команд CLI.
- ✓ Всегда настраивайте синхронизацию системных часов с доверенными источниками сетевого времени (NTP). Алгоритм настройки NTP приведен в разделе 7.45 «Настройка NTP» настоящего руководства. Подробная информация о командах для настройки NTP приведена в разделе 8 «Управление системными часами» справочника команд CLI.
- ✓ Отключайте NTP broadcast client, включенный по умолчанию в заводской конфигурации.
- ✓ Не используйте 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 7.15 «Конфигурирование Firewall» настоящего руководства. Подробная информация о командах для настройки межсетевого экрана приведена в разделе 19 «Управление Firewall» справочника команд CLI.

8.2 Настройка системы логирования событий

Алгоритмы настройки системы логирования событий приведены в разделе 7.47 «Настройка Syslog» настоящего руководства.

Подробная информация о командах для настройки системы логирования событий приведена в разделе 30.2 «Управление SYSLOG» справочника команд CLI.

8.2.1 Правила настройки

- ✓ Настройте хранение сообщений о событиях в файл syslog на устройстве и передачу этих событий на внешний syslog-сервер.
- ✓ Ограничьте размер syslog-файла на устройстве.
- ✓ Настройте ротацию syslog-файлов на устройстве.
- ✓ Включите нумерацию сообщений syslog.
- ✓ Включите 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 ESR.

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 512кб. Включить ротацию 3-х 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 7.7 «Настройка AAA» настоящего руководства.

Подробная информация о командах для настройки политики использования паролей приведена в разделе 9 «Настройка AAA» справочника команд CLI.

8.3.1 Правила настройки

- ✓ Всегда включайте требования на смену пароля по умолчанию пользователя admin.
- ✓ Ограничьте время жизни паролей и запретите повторно использовать, как минимум, предыдущий пароль.

- ✓ Установите требование минимальной длины пароля больше 8 символов
- ✓ Установите требование 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 7.7 «Настройка AAA» настоящего руководства.

Подробная информация о командах для настройки политики AAA приведена в разделе 9 «Настройка AAA» справочника команд CLI.

8.4.1 Правила настройки

- ✓ Используйте ролевую модель доступа на устройство.
- ✓ Используйте персональные учетные записи для аутентификации на устройстве.

- ✓ Включите логирование вводимых пользователем команд.
- ✓ Используйте несколько методов аутентификации для входа на устройства через консоль, удаленного входа на устройства и повышения привилегий. Оптимальной считается комбинация из аутентификации по одному из протоколов RADIUS/TACACS/LDAP и локальной аутентификации.
- ✓ Понизьте уровень привилегий встроенной учетной записи **admin** до 1.
- ✓ Настройте логирование изменений локальных учетных записей.
- ✓ Настройте логирование изменений политики AAA.

8.4.2 Предупреждения

- ✓ Встроенную учетную запись admin удалить нельзя.
- ✓ Команда **`no username admin`** не удаляет пользователя **admin**, сбрасывает его конфигурацию в значения по умолчанию. После применения этой команды, пользователь **admin** не будет отображаться в конфигурации.
- ✓ Команда **`no password`** для пользователя **admin**, также не удаляет пароль пользователя **admin**, а сбрасывает его в значение по умолчанию. После применения этой команды, пароль пользователя **admin** перестает отображаться в конфигурации и становится ‘password'.
- ✓ **Важно!** 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 удаленного 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 учетных 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
```

Задаем 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 удаленного управления

Подробная информация о командах настройки удаленного доступа приведена в разделе 30.3 «Настройка доступа SSH, Telnet» справочника команд CLI.

8.5.1 Правила настройки

- ✓ Отключите удаленное управление по протоколу telnet.
- ✓ Не включайте удаленное управление по протоколам SNMP v1, SNMP v2 (по умолчанию на устройстве выключено).
- ✓ Сгенерируйте новые криптографические ключи.
- ✓ Используйте криптостойкие алгоритмы аутентификации sha2-256, sha2-512 и отключите все остальные.
- ✓ Используйте криптостойкие алгоритмы шифрования aes256, aes256ctr и отключите все остальные

- ✓ Используйте криптостойкий алгоритм обмена ключами шифрования dh-group-exchange-sha256 и отключите все остальные.
- ✓ Разрешите доступ к удаленному управлению устройством только с определенных ip-адресов.

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
```

Генерируем новые ключи шифрования:

```
esr-20(config)# crypto key generate dsa
esr-20(config)# crypto key generate ecdsa
esr-20(config)# crypto key generate ed25519
esr-20(config)# crypto key generate rsa
esr-20(config)# crypto key generate rsa1
```

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 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 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
```

8.6 Настройка механизмов защиты от сетевых атак

Алгоритмы настройки механизмов защиты от сетевых атак приведены в разделе 7.14 «Настройка логирования и защиты от сетевых атак» настоящего руководства.

Подробная информация о командах для настройки политики использования паролей приведена в разделе 21 «Управление логированием и защитой от сетевых атак» справочника команд CLI.

8.6.1 Правила настройки

- ✓ Всегда включайте защиту от ip spoofing.
- ✓ Всегда включайте защиту от TCP-пакетов с неправильно выставленными флагами.
- ✓ Всегда включайте защиту от фрагментированных TCP-пакетов с выставленным флагом SYN.
- ✓ Всегда включайте защиту от фрагментированных ICMP-пакетов.
- ✓ Всегда включайте защиту ICMP-пакетов большого размера.
- ✓ Всегда включайте защиту от незарегистрированных ip-протоколов.
- ✓ Всегда включайте 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 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**

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 создаётся 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 трафика при ассиметричной маршрутизации.**

В случае организации сети с ассиметричной 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
```

Либо разрешить окрытие сессий для ассиметричного трафика:

```
esr(config-if-gi)# ip firewall sessions allow-unknown
```

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/**
Sevicedesk: **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/**