Комплексные решения для построения сетей

Маршрутизаторы серии ESR

ESR-100, ESR-200, ESR-1000

Версии ПО esr-100-1.0.7-ST, esr-200-1.0.7-ST esr-1000-1.0.7-ST

Руководство по эксплуатации

РПЛТ.465600.131.РЭ

Листов 164

Оглавление

1. Общие сведения о маршрутизаторе

1.1. Аннотация

Данное руководство пользователя разработано компанией ЭЛТЕКС для администраторов, осуществляющих управление маршрутизаторами ESR-100/200/1000 с версией программного обеспечения (далее ПО) 1.0.7-ST. В нем содержится информация по корректной настройке маршрутизатора.

1.2. Условные обозначения

Обозначение	Описание
Курсив Times New Roman	Курсивом Times New Roman указываются переменные или параметры, которые необходимо заменить соответствующим словом или строкой.
Полужирный курсив	Полужирным шрифтом выделены примечания и предупреждения.
< >	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».

1.3. Требования к персоналу

Квалификация технического персонала предполагает знание основ работы вычислительный сетей, семиуровневой модели OSI, стека протоколов TCP/IP и принципов построения Ethernet сетей

1.4. Назначение маршрутизатора

Устройства серии ESR являются высокопроизводительными многоцелевыми сетевыми маршрутизаторами, но в первую очередь представляют собой криптошлюзы с поддержкой ГОСТ шифрования. 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. Функции маршрутизатора

2.1. Функции интерфейсов

В таблице 2.1 приведен список функций интерфейсов устройства.

Таблица 2.1 – Функции интерфейсов устройства

Определение полярности подключения кабеля (Auto MDI/MDIX)	Автоматическое определение типа кабеля - перекрестный кабель или кабель прямого подключения. MDI (Media-Dependent Interface – прямой) – стандарт кабелей для подключения оконечных устройств; MDIX (Media-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. Функции при работе с MAC–адресами

В таблице 2.2 приведены функции устройства при работе с MAC–адресами.

Таблица 2.2 – 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 16К 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.

2.3. Функции второго уровня сетевой модели OSI

В таблице 2.3 приведены функции и особенности второго уровня (уровень 2 OSI)

Таблица 2.3 – 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 IEEE802.1Q; VLAN на базе портов устройства (port-based); VLAN на базе использования правил классификации данных (policy-based).
Протокол связующего дерева (Spanning Tree Protocol) [1]	Задачей протокола Spanning Tree является исключение избыточных сетевых соединений и приведение топологии сети к древовидной. Основные применения протокола связаны с предотвращением зацикливания сетевого трафика и с организацией резервных каналов связи.

2.4. Функции третьего уровня сетевой модели OSI

В таблице 2.4 приведены функции третьего уровня (уровень 3 OSI)

Таблица 2.4 – 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.

[1] В текущей версии ПО данный функционал поддерживается только на маршрутизаторе ESR-1000

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).

2.5. Функции туннелирования трафика

В таблице 2.5 приведены функции туннелирования трафика

Таблица 2.5 – 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 ГОСТ шифрованием передаваемых данных.

2.6. Функции управления и конфигурирования

В таблице 2.6 приведены функции управления и конфигурирования

Таблица 2.6 – 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 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	Функции сервера SSH 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.

2.7. Функции сетевой защиты

В таблице 2.7 приведены функции сетевой защиты, выполняемые устройством.

Таблица 2.7 – Функции сетевой защиты

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

3. Основные технические характеристики

Основные технические параметры маршрутизатора приведены в таблице 3.1.

Таблица 3.1 – Основные технические характеристики

Общие параметры		
Пакетный процессор	ESR-1000	Broadcom XLP316L
	ESR-200	Broadcom XLP204
	ESR-100	Broadcom XLP104
Интерфейсы	ESR-1000	24 x Ethernet 10/100/1000 Base-T 2 x 10G Base Base-R/1000 Base-X (SFP+/SFP)
	ESR-200	4 x Ethernet 10/100/1000 Base-T / 1000 Base-X Combo 4 x Ethernet 10/100/1000 Base-T
	ESR-100	4 x Ethernet 10/100/1000 Base-T / 1000 Base-X Combo
Типы оптических трансиверов	ESR-1000	1000 BASE-X SFP, 10G BASE-R SFP+
	ESR-100 ESR-200	1000 BASE-X SFP
Дуплексный и полудуплексный режимы интерфейсов		- дуплексный и полудуплексный режим для электрических портов - дуплексный режим для оптических портов
Максимальная пропускная способность маршрутизатора ESR-1000 (при аппаратной коммутации)		88 Гбит/с
Объем буферной памяти встроенного коммутатора (для ESR-1000)		12 Mb
Скорость передачи данных	ESR-1000	- электрические интерфейсы 10/100/1000 Мбит/с - оптические интерфейсы 1/10 Гбит/с
	ESR-100 ESR-200	- электрические интерфейсы 10/100/1000 Мбит/с - оптические интерфейсы 1 Гбит/с
Таблица MAC-адресов (для ESR-1000)		16K записей
Поддержка VLAN		до 4K активных VLAN в соответствии с 802.1Q
Количество L3 интерфейсов		до 2K
Количество маршрутов BGP	ESR-1000	2,6M
	ESR-100 ESR-200	1,2M
Количество маршрутов OSPF	ESR-1000	500K
	ESR-100 ESR-200	300K
Количество маршрутов RIP		10K
Количество статических маршрутов		11K
Размер FIB	ESR-1000	1,7M
	ESR-100 ESR-200	550K

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		SSH
Физические характеристики и условия окружающей среды		
Источники питания	ESR-1000	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-100 ESR-200	сеть переменного тока: 220В+-20%, 50 Гц
Максимально потребляемая мощность	ESR-1000	75 Вт
	ESR-100	20 Вт
	ESR-200	25 Вт
Масса	ESR-1000	не более 3,6 кг
	ESR-100 ESR-200	не более 2,5 кг
Габаритные размеры	ESR-1000	430x352x44 мм
	ESR-100 ESR-200	310x240x44 мм
Интервал рабочих температур		от -10 до +45 оС
Интервал температуры хранения		от -40 до +70 оС
Относительная влажность при эксплуатации (без образования конденсата)		не более 80%
Относительная влажность при хранении (без образования конденсата)		от 10% до 95%
Средний срок службы		20 лет

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.

4.1. Конструктивное исполнение ESR-1000

4.1.1. Передняя панель устройства ESR-1000

Внешний вид передней панели показан на рисунке 4.1.

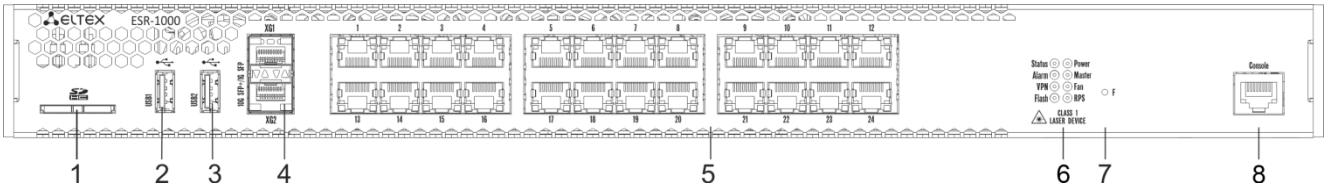


Рисунок 4.1 – Передняя панель ESR-1000

В таблице 4.1 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели устройства.

Таблица 4.1 – Описание разъемов, индикаторов и органов управления передней панели

№	Элемент панели	Описание
1	SD	Разъем для установки SD-карт памяти.
2	USB1	Порт для подключения USB-устройств.
3	USB2	Порт для подключения USB-устройств.
4	XG1, XG2	Слоты для установки трансиверов 10G SFP+/ 1G SFP.
5	[1 .. 24]	24 порта Gigabit Ethernet 10/100/1000 Base-T (RJ-45).
6	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	VPN	Индикатор наличия активных VPN-сессий (на текущий момент не активен).
	Flash	Индикатор активности обмена с накопителем данных - SD-картой или USB Flash.
	Power	Индикатор питания устройства.
	Master	Индикатор работы устройства в failover-режимах.
	Fan	Индикатор аварии вентиляторов.
	RPS	Индикатор резервного источника электропитания.
7	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: при длительности нажатия на кнопку менее 10 секунд происходит перезагрузка устройства;

		при длительности нажатия на кнопку более 10 секунд происходит сброс устройства к заводской конфигурации.
8	Console	Консольный порт RS-232 для локального управления устройством.

4.1.2. Задняя панель устройства ESR-1000

Внешний вид задней панели устройства ESR-1000 приведен на рисунке 4.2[2].

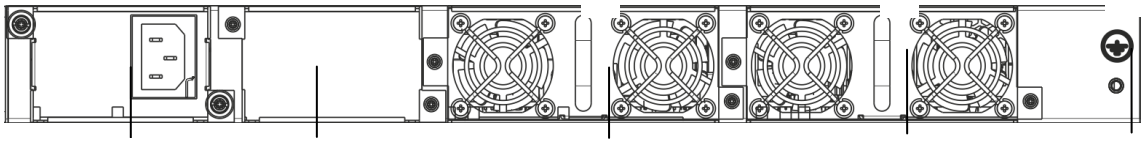


Рисунок 4.2 – Задняя панель ESR-1000

В таблице 4.2 приведен перечень разъемов, расположенных на задней панели маршрутизатора.

Таблица 4.2 – Описание разъемов задней панели маршрутизатора

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

4.1.3. Боковые панели устройства

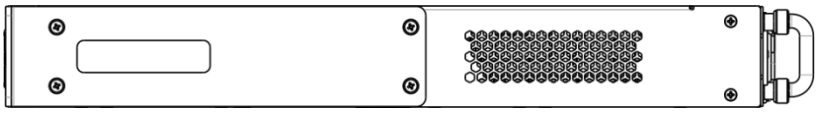


Рисунок 4.3 – Правая боковая панель маршрутизатора ESR-1000

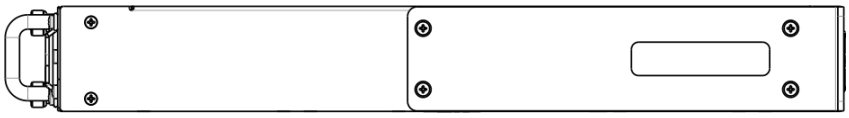


Рисунок 4.4– Левая боковая панель маршрутизатора ESR-1000

На боковых панелях устройства расположены вентиляционные решетки, которые служат для отвода тепла. Не закрывайте вентиляционные отверстия посторонними предметами. Это может привести к перегреву компонентов устройства и вызвать нарушения в его работе. Рекомендации по установке устройства расположены в разделе «Установка и подключение».

[2] На рисунке показана комплектация маршрутизатора с одним источником питания переменного тока.

4.2. Конструктивное исполнение ESR-100, ESR-200

4.2.1. Передняя панель устройств ESR-100, ESR-200

Внешний вид передней панели ESR-100 показан на рисунке 4.5.

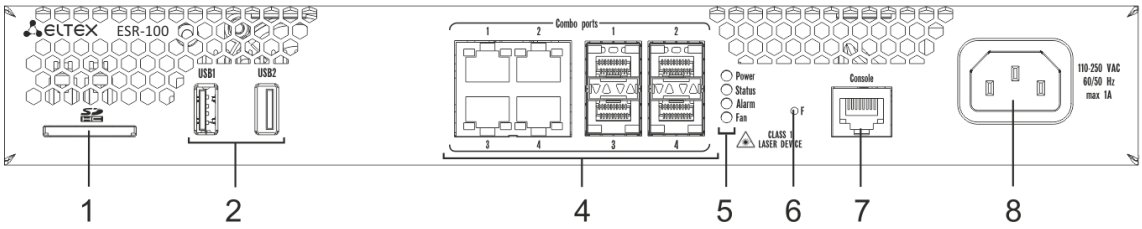


Рисунок 4.5 – Передняя панель ESR-100

Внешний вид передней панели ESR-200 показан на рисунке 4.6.

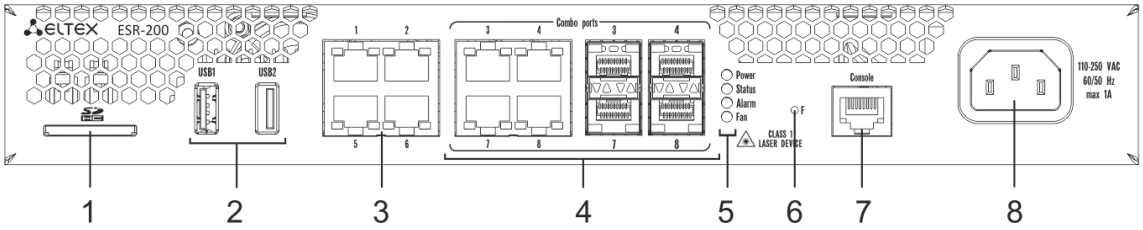


Рисунок 4.6 – Передняя панель ESR-200

В таблице 4.3 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели устройств ESR-100, ESR-200.

Таблица 4.3 – Описание разъемов, индикаторов и органов управления передней панели

№	Элемент панели передней	Описание
1	SD	Разъем для установки SD-карт памяти.
2	USB1, USB2	2 порта для подключения USB-устройств.
3	[1 .. 4]	4 порта Gigabit Ethernet 10/100/1000 Base-T (RJ-45).
4	Combo Ports	4 порта Gigabit Ethernet 10/100/1000 Base-X (SFP).
5	Power	Индикатор питания устройства.
	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	Fan	Индикатор аварии вентиляторов.
6	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: при длительности нажатия на кнопку менее 10 секунд происходит перезагрузка устройства; при длительности нажатия на кнопку более 10 секунд происходит сброс устройства к заводской конфигурации.
7	Console	Консольный порт RS-232 для локального управления устройством.
8	110-250 VAC	Источник питания.

	60/50 Hz max 1A	

4.2.2. Задняя панель устройств ESR-100, ESR-200

Внешний вид задней панели устройств ESR-100, ESR-200 приведен на рисунке 4.7[3].

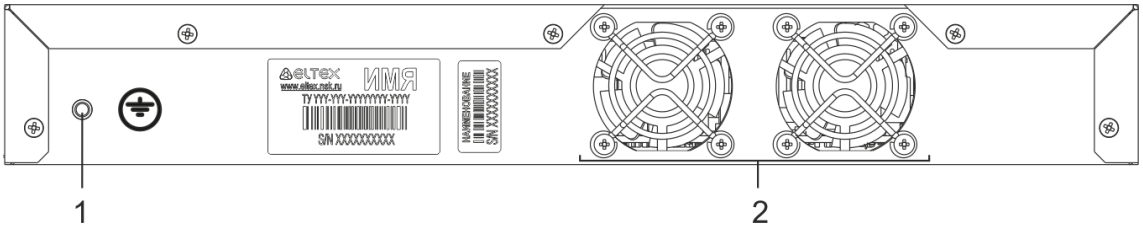


Рисунок 4.7 – ESR-1000, задняя панель

В таблице 4.4 приведен перечень разъемов, расположенных на задней панели маршрутизатора.

Таблица 4.4 – Описание разъемов задней панели маршрутизатора

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

4.2.3. Боковые панели устройства ESR-100, ESR-200

Рисунок 4.8 – Правая боковая панель маршрутизатора ESR-100, ESR-200

Рисунок 4.9– Левая боковая панель маршрутизатора ESR-100, ESR-200

[3] На рисунке показана комплектация маршрутизатора с одним источником питания переменного тока.

5. Световая индикация

5.1. Световая индикация ESR-1000

Состояние медных интерфейсов GigabitEthernet отображается двумя светодиодными индикаторами - LINK/ACT зеленого цвета и SPEED янтарного цвета. Расположение индикаторов медных интерфейсов показано на рисунке 5.1. Состояние SFP-интерфейсов отображается двумя индикаторами RX/ACT и TX/ACT и указано на рисунке 5.2. Значения световой индикации описаны в таблицах 5.1 и 2.14.

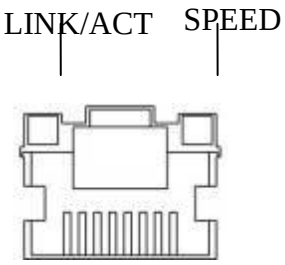


Рисунок 5.1 – Расположение индикаторов разъема RJ-45

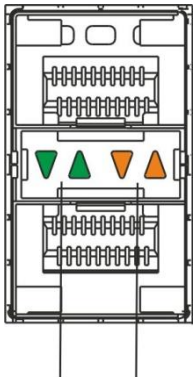


Рисунок 5.2 – Расположение индикаторов оптических интерфейсов

Таблица 5.1 – 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 100Мбит/с
Горит постоянно	Горит постоянно	Установлено соединение на скорости 1000Мбит/с
X	Мигание	Идет передача данных

Таблица 5.2 – 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 5.3 – 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

5.2. Световая индикация ESR-100/ESR-200

Состояние медных интерфейсов GigabitEthernet и SFP-интерфейсов отображается двумя светодиодными индикаторами - LINK/ACT зеленого цвета и SPEED янтарного цвета. Расположение индикаторов медных интерфейсов показано на рисунке 5.1. Состояние SFP-интерфейсов указано на рисунке 5.3. Значения световой индикации описаны в таблице 5.4.

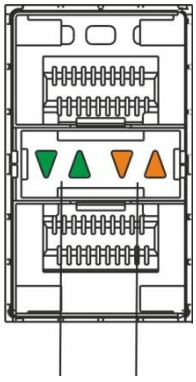


Рисунок 5.3 – Расположение индикаторов оптических интерфейсов

Таблица 5.4 – 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

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

Таблица 5.5 – 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. [4]	-	-
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
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

[4] Не поддерживается в текущей версии ПО

6. Установка и подключение

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

6.1. Крепление кронштейнов

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

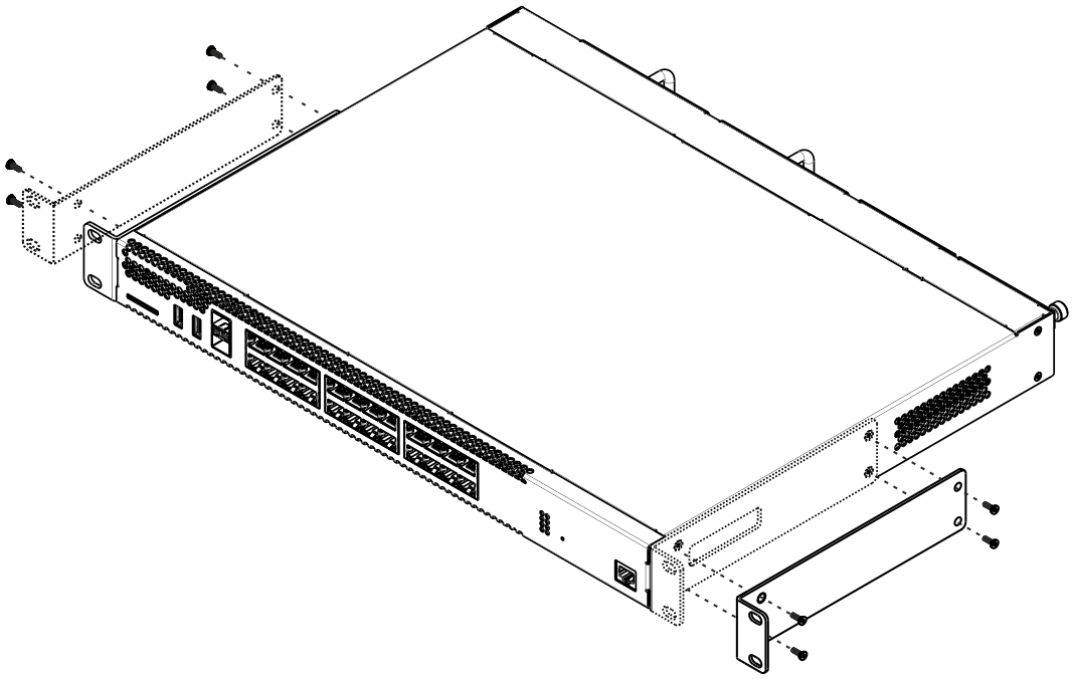


Рисунок 6.1 – Крепление кронштейнов

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.

6.2. 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.

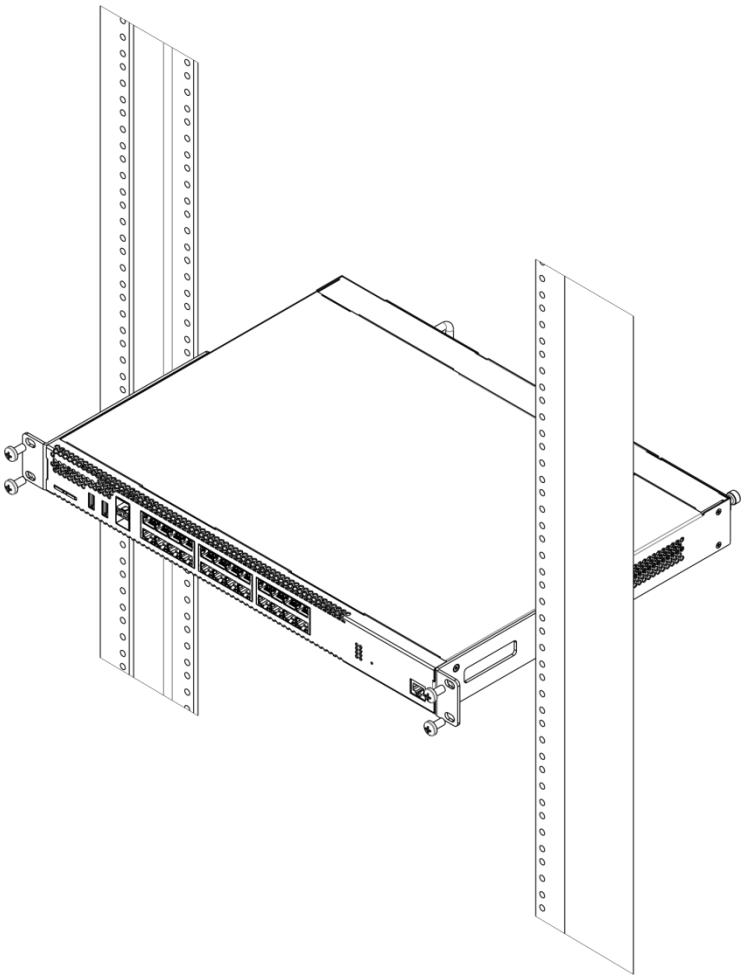


Рисунок 6.2 – Установка устройства в стойку

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.

6.3. Установка модулей питания ESR-1000

Маршрутизатор ESR-1000 может 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.

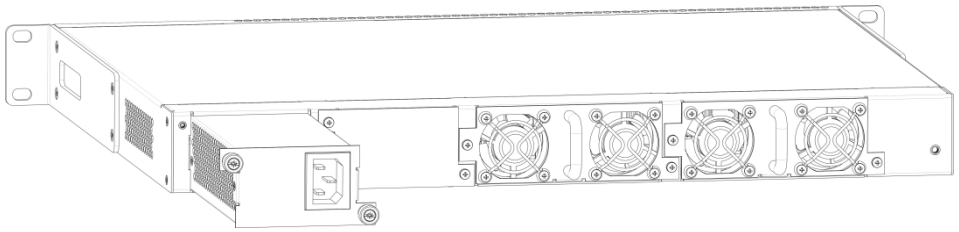


Рисунок 6.3 – Установка модулей питания

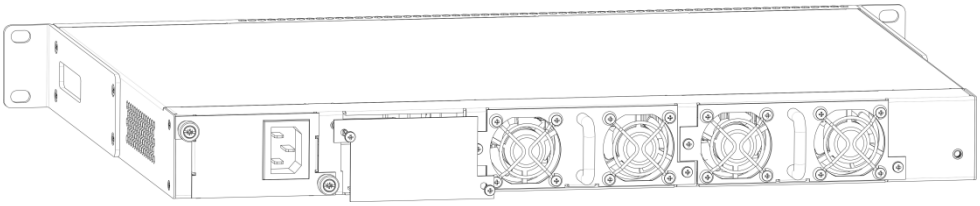


Рисунок 6.4 – Установка заглушки

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

6.4. 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.

6.5. Установка и удаление SFP-трансиверов

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

Установка трансивера

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

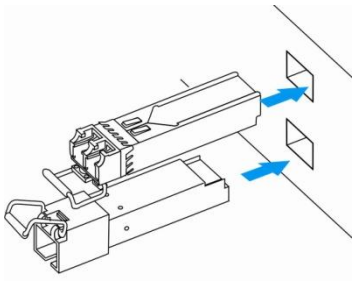


Рисунок 6.5 – Установка SFP-трансиверов

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

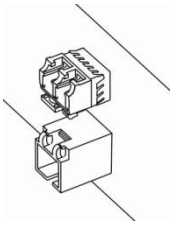


Рисунок 6.6 – Установленные SFP-трансиверы

Удаление трансивера

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

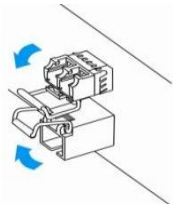


Рисунок 6.7 – Открытие защелки SFP-трансиверов

2. Извлеките модуль из слота.

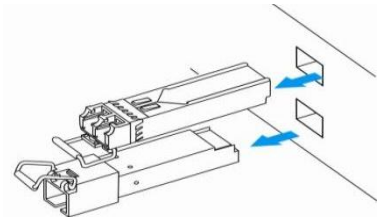


Рисунок 6.8 – Извлечение SFP-трансиверов

7. Заводская конфигурация и подключение

7.1. Заводская конфигурация маршрутизатора ESR

При отгрузке устройства потребителю на оборудование загружается заводская конфигурация, которая в целях безопасности не имеет никаких настроек и в которой выключены все физические интерфейсы.

7.2. Подключение маршрутизатора

Первоначальная настройка маршрутизаторов серии ESR осуществляется через консольный порт RS-232

Для этого необходимо:

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

2. запустить 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 бод;
- Биты данных: 8 бит;
- Четность: нет;
- Стоповые биты: 1;
- Управление потоком: нет.

7.3. Инициализация

Инициализация проводится в режиме Initial CLI и является обязательной процедурой:

[administrator@esr] **initialize**

При запуске данной команды инициализируется ДСЧ (Датчик Случайных Чисел), посредством интерактивного ввода в терминал запрашиваемых значений.

```
Progress: [*** ]

Press key: R
```

После успешного прохождения инициализации вся передача трафика будет запрещена, чтобы разрешить прохождение трафика, необходимо ввести команду run csconf_mgr activate.

```
[administrator@esr] run csconf_mgr activate
```

8. Обновление программного обеспечения

8.1. Обновление программного обеспечения средствами системы

Обновление программного обеспечения на устройстве, может осуществляться посредством обращения на сервер (TFTP, FTP, SCP), либо посредством USB FLASH.

Для обновления программного обеспечения понадобится USB накопитель с программным обеспечением или один из следующих серверов: TFTP, FTP, SCP. 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.

Обновление программного обеспечения на устройстве посредством USB накопителя выполняется в следующем порядке.

1. Подготовьте для работы USB накопитель, отформатированный в FAT/NTFS/EXT2/EXT3/EXT4

2. ,Поместите в данный отформатированный раздел программное обеспечение

3. Вставьте накопитель в USB порт маршрутизатора.

4. Определите имя раздела в USB накопителе через команду show storage-devices.

esr:esr# show storage-devices

```
Name Total, MB Used, MB Free, MB
------------------------------ ---------- ---------- ----------
EDCE-911D 88.84 84.70 4.14
BDE7S 1884.44 0.00 1884.44
```

1. Проверьте содержимое и путь к программному обеспечению, через команду dir, где <USB-device-name> название раздела USB накопителя, а [PATH] – указание месторасположение, если файл расположен в директории.

   dir usb://<USB-device-name>/[PATH]

   Пример:

esr:esr# dir usb://EDCE-911D/

```
Name Type Size
---------------------------------------- ---------- -------- --
gnome Directory 24.73 MB
firmware File 64.82 MB
install.txt File 1.00 KB
```

2. Для обновления программного обеспечения маршрутизатора введите следующую команду. Укажите название раздела и полный путь к файлу.

esr:esr# copy usb://usb_name:/PATH fs://firmware

Пример:

esr:esr# copy usb://EDCE-911D:/firmware fs://firmware

```
Download firmware from usb://EDCE-911D:/firmware...
Basic verify image ...
```

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

esr:esr# show bootvar

```
Image Version Date Status After reboot
----- ------------------------ -------------------- ------------ ------------
1 1.0.7-ST build date 29/07/2016 time Not Active
 75[0b77453] 17:09:24


2 1.0.7-ST build date 28/07/2016 time Active *
 75[0b77453] 14:54:43 16:12:54
```

Для выбора образа используйте команду

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

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

Подготовьте для работы выбранный сервер. Должен быть известен адрес сервера, на сервере должен быть размещен файл дистрибутивный файл программного обеспечения.

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.

Подключитесь к маршрутизатору локально через консольный порт Console или удаленно, используя прокол SSH.

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

1. Для обновления программного обеспечения маршрутизатора введите следующую команду. В качестве параметра <*server*> должен быть указан IP-адрес используемого

сервера. Для обновления с FTP или SCP-сервера потребуется ввести имя пользователя (параметр <*user*>) и пароль (параметр <*password*>). В качестве параметра <*file_name*> укажите имя файла программного обеспечения, помещенного на сервер (при использовании SCP нужно указать полный путь – параметр <*folder*>). После ввода команды маршрутизатор скопирует файл во внутреннюю память, проверит целостность данных и сохранит его в энергонезависимую память устройства.

– TFTP:

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

– FTP:

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

– SCP:

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

Для примера обновим основное ПО через SCP:

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

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

```
esr:esr# show bootvar
```

```
Image Version Date Status After reboot
----- ------------------------ ------------------- ------------ ------------
1 1.0.7-ST build date 29/07/2016 time Not Active
 75[0b77453] 17:09:24


2 1.0.7-ST build date 28/07/2016 time Active *
 75[0b77453] 14:54:43 16:12:54
```

Для выбора образа используйте команду

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

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

– TFTP:

```
esr:esr# copy tftp://<server>:/<file_name> fs://boot
```

– FTP:

esr:esr# copy ftp://<server>:/<file_name> fs://boot

– SCP:

esr:esr# copy scp://[<user>[:<password>]@]<server>://<folder>/<file_name> fs://boot

8.2. Обновление программного обеспечения из начального загрузчика

Программное обеспечение маршрутизатора можно обновить из начального загрузчика следующим образом:

1. Подготовить SD карту:
    a. Разбить SD карту на 2 раздела;
    b. Отформатировать второй раздел под FAT;
    c. Поместить файл обновления на второй раздел.
2. Установить в устройство SD-карту и подать питание.
3. 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
```

4. Записать ПО, выполнив команды, где в качестве параметра <file_name> укажите имя файла программного обеспечения, помещенного на SD карте (если файл расположен в папке, нужно указать полный путь – параметр <folder>):

- **sdcard_update_firmware <folder>/<file_name> image [1|2]**

5. Выбрать образ загрузки

- **boot system image-[1|2]**

6. Перезагрузить устройство

- **reset**

Пример

```
BRCM.XLP316Lite Rev B2.u-boot#sdcard_update_firmware esr200/firmware image2
BRCM.XLP316Lite Rev B2.u-boot#boot system image2
BRCM.XLP316Lite Rev B2.u-boot#reset
```

– Перезагрузить устройство и дождаться запуска ОС. Должна появиться возможность авторизации в консоли управления(Initial CLI), как в примере ниже:

```
S-Terra Gate administrative console
login as:
```

9. Конфигурирование маршрутизатора

9.1. Конфигурирование базовых параметров

9.1.1. Изменение пароля пользователей.

Для защищенного входа в систему необходимо сменить пароль привилегированного пользователей «administrator», «admin», «cscons».

Учетная запись techsupport необходима для удаленного обслуживания сервисным центром

Учетная запись remote - аутентификация RADIUS, TACACS+, LDAP

Удалить пользователей admin, cscons 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 «administrator» в Initial CLI используются следующая команда:

```
administrator@esr] change user password administrator
```

Для изменения пароля пользователя «admin» используются следующие команды:

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

Аналогично, необходимо сменить пароль для пользователя «cscons».

```
esr:esr(config)# username cscons
esr:esr(config-user)# password <new-password>
esr:esr(config-user)# exit
```

9.1.2. Создание новых пользователей

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

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

Уровни привилегий пользователей ESR CLI

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

9.2. Назначение имени устройства

Для назначения имени устройства используется следующая команда в режиме глобального конфигурирования:

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

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

9.3. 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.(Трафик будет передаваться только после настройки Firewall см. главу 10.7)

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:esr# configure
esr:esr(config)# interface gigabitethernet 1/0/2
esr:esr(config-if)# no shutdown
esr:esr(config-if)# exit
esr:esr(config)# interface gigabitethernet 1/0/2.150
esr:esr(config-subif)# ip address 192.168.16.144/24
esr:esr(config-subif)# exit
esr: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: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:esr# configure
esr:esr(config)# interface gigabitethernet 1/0/10
esr:esr(config-if)# no shutdown
esr:esr(config-if)# ip address dhcp enable
esr:esr(config-if)# exit
```

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

```
esr:esr# show ip interfaces
```

```
IP address Interface Type
------------------- -------------------------------- -------
192.168.11.5/25 gigabitethernet 1/0/10 DHCP
```

9.4. Применение базовых настроек

Для применения выполненных изменений конфигурации маршрутизатора требуется ввести следующие команды из корневого раздела командного интерфейса.

```
esr:esr# commit
esr:esr# confirm
```

Если при конфигурировании использовался удаленный доступ к устройству и сетевые параметры интерфейса управления изменились, то после ввода команды **commit** соединение с устройством может быть потеряно. Используйте новые сетевые параметры, заданные в конфигурации, для подключения к устройству и ввода команды **confirm**.

Если ввести команду **confirm** не удастся, то по истечении таймера подтверждения конфигурация устройства вернётся в прежнее состояние, существовавшее до ввода команды **commit**.

10. Примеры настройки маршрутизатора

10.1.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.

Процесс настройки

Шаг	Описание	Команда	Ключи
1	Создать VLAN	**esr:esr(config)# vlan <VID>**	<VID> – идентификатор VLAN, задаётся в диапазоне [2..4094] Так-же есть возможность создания нескольких vlan (через запятую) или диапазона vlan (через дефис)
2	Задать имя vlan (не обязательно)	**esr:esr(config-vlan)# name <vlan-name>**	<vlan-name> - до 255 символов
3	Переключить режим работы физического интерфейса в L2-режим	**esr:esr(config-gi)# switchport**	
4	Задать режим работы L2 интерфейса	**esr:esr(config-gi)# switchport access**	Только для ESR-100/200
		esr:esr(config-gi)# switchport trunk	Только для ESR-100/200
		esr:esr(config-gi)# switchport general	Только для ESR-1000
5	Настроить список vlan на интерфейсе в тегированном режиме	**esr:esr(config-if-gi)# switchport trunk allowed vlan add <VID>**	<VID> – идентификатор VLAN, задаётся в диапазоне [2..4094] Также есть возможность создания нескольких vlan (через запятую) или диапазона vlan (через дефис) Для ESR-100/200
		esr:esr(config-if-gi)# switchport general allowed vlan add <VID> tagged	<VID> – идентификатор VLAN, задаётся в диапазоне [2..4094] Также есть возможность создания нескольких vlan (через запятую) или диапазона vlan (через дефис) Для ESR-1000

5	Настроить список vlan на интерфейсе в нетегированном режиме (не обязательно)	`esr:esr(config-if-gi)# switchport trunk native-vlan <VID>`	<VID> – идентификатор VLAN, задаётся в диапазоне [2..4094] Для ESR-100/200
		`esr:esr(config-if-gi)# switchport general allowed vlan add <VID> untagged`	<VID> – идентификатор VLAN, задаётся в диапазоне [2..4094] Для ESR-1000

Пример конфигурации 1

Задача:

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

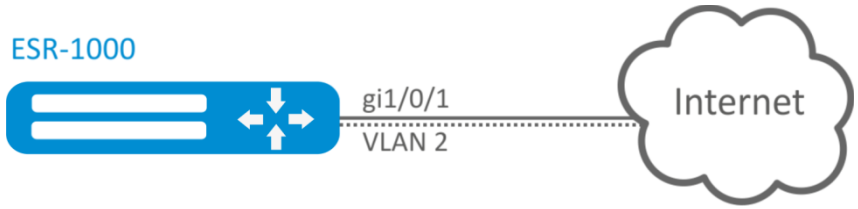


Рисунок 10.1 – Схема сети

Решение:

Удалим VLAN 2 с порта gi1/0/1:

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

Изменения конфигурации вступят в действие после применения:

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

Пример конфигурации 2

Задача:

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

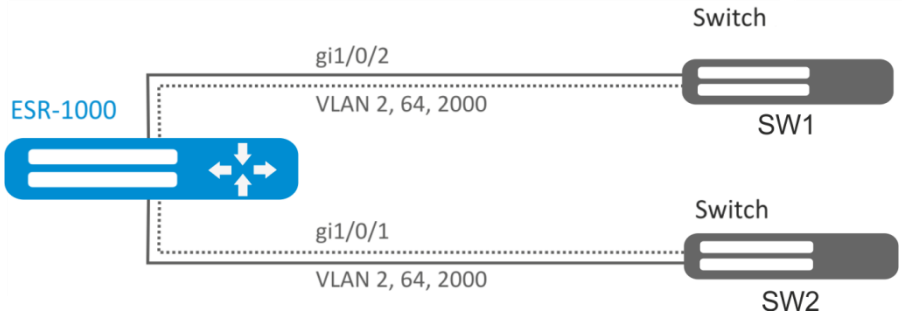


Рисунок 10.2 – Схема сети

Решение:

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

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

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

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

Изменения конфигурации вступят в действие после применения:

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

Пример конфигурации 3

Задача:

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

Рисунок 10.3 – Схема сети

Решение:

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

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

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

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

Пропишем VLAN 2 на порт gi1/0/2:

```
esr:esr(config)# interface gi1/0/1
esr:esr(config-if-gi)# switchport
esr:esr(config-if-gi)# switchport access vlan 2
```

Изменения конфигурации вступят в действие после применения:

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

10.2.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.

Процесс 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:esr(config)# radius-server dscp <DSCP>**	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63] Значение по умолчаню: 63
2	Задать глобальное значение количества перезапросов к последнему активному RADIUS-серверу (не обязательно)	**esr:esr(config)# radius-server retransmit <COUNT>**	<COUNT> – количество перезапросов к RADIUS-серверу, принимает значения [1..10] Значение по умолчаню: 1

3	Задать глобальное значение интервала, по истечении которого маршрутизатор считает, что RADIUS-сервер недоступен (не обязательно)	**esr: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:esr(config)# radius-server host <IP-ADDR> esr(config-radius-server)#**	<ADDR> – IP-адрес RADIUS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]
5	Задать пароль для аутентификации на удаленном RADIUS сервере	**esr: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.
6	Задать приоритет использования удаленного RADIUS сервера (не обязательно)	**esr: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
7	Задать интервал, по истечении которого маршрутизатор считает, что данный RADIUS-сервер недоступен (не обязательно)	**esr:esr(config-radius-server)# timeout <SEC>**	<SEC> – период времени в секундах, принимает значения [1..30] Значение по умолчанию: используется значение глобального таймера
8	Указать radius в качестве метода аутентификации	**esr: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.

9	Указать radius в качестве способа аутентификации повышения привилегий пользователей	**esr:esr(config)# aaa authentication enable <NAME> <METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]**	<NAME> – имя списка строка до 31 символа; default – имя списка «default». <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: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 аутентифицироваться. Если сервер недоступен, продолжить попытки аутентифицироваться следующими в цепочке методами Значение по умолчанию: chain
11	Сконфигурировать radius в списоке способов учета сессий пользователей (не обязательно)	**esr: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.
12	Перейти в режим конфигурирования соответствующего терминала	**esr:esr(config)# line <TYPE>**	<TYPE> – тип консоли: **console** – локальная консоль; **ssh** – защищенная удаленная консоль.
13	Активировать список аутентификации входа пользователей в систему	**esr:esr(config-line-console)# login authentication <NAME>**	<NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 8.
18	Активировать список аутентификации повышения привилегий пользователей	**esr:esr(config-line-console)# enable authentication <NAME>**	<NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 9.

Процесс 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:esr(config)# tacacs-server dscp <DSCP>**	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63] Значение по умолчаню: 63
2	Задать глобальное значение интервала, по истечении которого маршрутизатор считает, что TACACS-сервер недоступен (не обязательно)	**esr:esr(config)# tacacs-server timeout <SEC>**	<SEC> – период времени в секундах, принимает значения [1..30] Значение по умолчанию: 3 секунды
3	Добавить TACACS-сервер в список используемых серверов и перейти в режим его конфигурирования	**esr:esr(config)# tacacs-server host <IP-ADDR>** **esr:esr(config-tacacs-server)#**	<ADDR> – IP-адрес TACACS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]
4	Задать пароль для аутентификации на удаленном TACACS-сервере	**esr: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.
5	Задать номер порта для обмена данными с удаленным TACACS-сервером (не обязательно)	**esr: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
6	Задать приоритет использования удаленного TACACS сервера (не обязательно)	**esr: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

7	Указать TACACS в качестве метода аутентификации	**esr: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.
8	Указать TACACS в качестве способа аутентификации повышения привилегий пользователей	**esr:esr(config)# aaa authentication enable <NAME> <METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]**	<NAME> – имя списка строка до 31 символа; default – имя списка «default». <METHOD> – способы аутентификации: **enable** – аутентификация с помощью enable-паролей; **tacacs** – аутентификация по протоколу TACACS; **radius** – аутентификация по протоколу RADIUS; **ldap** – аутентификация по протоколу LDAP.
9	Указать способ перебора методов аутентификации в случае отказа (не обязательно)	**esr: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 аутентифицироваться. Если сервер недоступен, продолжить попытки аутентифицироваться следующими в цепочке методами Значение по умолчанию: chain
10	Сконфигурировать список способов учета команд, введённых в CLI (не обязательно)	**esr:esr(config)# aaa accounting commands stop-only tacacs**	
11	Сконфигурировать tacacs в списоке способов учета сессий пользователей (не обязательно)	**esr: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.

12	Перейти в режим конфигурирования соответствующего терминала	**esr:esr(config)# line <TYPE>**	<TYPE> – тип консоли: **console** – локальная консоль; **ssh** – защищенная удаленная консоль.
13	Активировать список аутентификации входа пользователей в систему	**esr:esr(config-line-console)# login authentication <NAME>**	<NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 7.
14	Активировать список аутентификации повышения привилегий пользователей	**esr:esr(config-line-console)# enable authentication <NAME>**	<NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 8.

Процесс настройки AAA по протоколу LDAP

Шаг	Описание	Команда	Ключи
1	Задать базовый DN (Distinguished name), который будет использоваться при поиске пользователей	**esr: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: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: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: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	Задаёть имя класса объектов, среди которых необходимо выполнять поиск пользователей на LDAP-сервере (не обязательно)	**esr: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: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: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: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: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) (не обязательно)	**esr:esr(config)# ldap-server dscp <DSCP>**	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63] Значение по умолчаню: 63
11	Добавить LDAP-сервер в список используемых серверов и перейти в режим его конфигурирования	**esr:esr(config)# ldap-server host <IP-ADDR>** **esr:esr(config-tacacs-server)#**	<ADDR> – IP-адрес LDAP-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]
12	Задать номер порта для обмена данными с удаленным LDAP-сервером (не обязательно)	**esr: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
13	Задать приоритет использования удаленного LDAP сервера (не обязательно)	**esr: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
14	Указать LDAP в качестве метода аутентификации	**esr: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.

15	Указать LDAP в качестве способа аутентификации повышения привилегий пользователей	**esr:esr(config)# aaa authentication enable <NAME> <METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]**	<NAME> – имя списка строка до 31 символа; default – имя списка «default». <METHOD> – способы аутентификации: **enable** – аутентификация с помощью enable-паролей; **tacacs** – аутентификация по протоколу TACACS; **radius** – аутентификация по протоколу RADIUS; **ldap** – аутентификация по протоколу LDAP.
16	Указать способ перебора методов аутентификации в случае отказа	**esr: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 аутентифицироваться. Если сервер недоступен, продолжить попытки аутентифицироваться следующими в цепочке методами Значение по умолчанию: chain
17	Перейти в режим конфигурирования соответствующего терминала	**esr:esr(config)# line <TYPE>**	<TYPE> – тип консоли: console – локальная консоль; ssh – защищенная удаленная консоль.
18	Активировать список аутентификации входа пользователей в систему	**esr:esr(config-line-console)# login authentication <NAME>**	<NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 14.
19	Активировать список аутентификации повышения привилегий пользователей	**esr:esr(config-line-console)# enable authentication <NAME>**	<NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 15.

Пример конфигурации

Задача:

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

Решение:

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

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

```
esr:esr(config-radius-server)# exit
```

Создадим профиль аутентификации:

```
esr:esr(config)# aaa authentication login log radius
```

Укажем режим аутентификации, используемый при подключении по протоколу SSH:

```
esr:esr(config)# line ssh
esr:esr(config-line-ssh)# login authentication log
esr:esr(config-line-ssh)# exit
esr:esr(config)# exit
```

Изменения конфигурации вступят в действие после применения:

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

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

```
esr:esr# show aaa radius-servers
```

Посмотреть профили аутентификации можно командой:

```
esr:esr# show aaa authentication
```

10.3.Настройка привилегий команд

Настройка привилегий команд для ESR CLI 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.

Процесс настройки

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

```
esr: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.

Пример настройки

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

Изменения конфигурации вступят в действие после применения и только для новых сессий пользователей:

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

10.4.Настройка DHCP-сервера

Встроенный DHCP-сервер маршрутизатора может быть использован для настройки сетевых параметров устройств в локальной сети. DHCP-сервер маршрутизатора 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.

Процесс настройки

Шаг	Описание	Команда	Ключи
1	Включить DHCP-сервер	**esr:esr(config)# ip dhcp-server**	
2	Задать значение кода DSCP для использования в IP-заголовке исходящих пакетов DHCP-сервера (не обязательно)	**esr:esr(config)# ip dhcp-server dscp <DSCP>**	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 63
3	Создать пул IP-адресов DHCP-сервера и перейти в режим его конфигурирования	esr:esr(config)# ip dhcp-server pool **<NAME>**	<NAME> – имя пула IP-адресов DHCP-сервера, задаётся строка до 31 символа

4	Задать IP-адрес и маску для подсети, из которой будет выделен пул IP-адресов	**esr: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]
5	Добавить диапазон IP-адресов к пулу адресов, конфигурируемого DHCP-сервера	**esr:esr(config-dhcp-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]. Можно указать до 32 диапазонов IP-адресов, список задаётся через запятую
6	Добавить IP-адрес для определенного физического адреса к пулу адресов конфигурируемого DHCP-сервера (не обязательно)	**esr: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]. Если использовать команду для удаления, то при указании значения «all» будут удалены все IP-адреса; <MAC> – MAC-адрес клиента, которому будет выдан IP-адрес, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]. <CI> - идентификатор клиента согласно DHCP Optionion61. Может быть задан в одном из следующих видов: HH:HH:HH:HH:HH:HH:HH: - идентификатор клиента в шеснатцатеричной форме и mac-адрес клиента STRING - текстовая строка длинной от 1 до 64 символов.

7	Задать список IP-адресов шлюзов по умолчанию, которые DHCP-сервер будет сообщать клиентам, используя DHCP опцию 3	**esr: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:esr(config-dhcp-server)# domain-name <NAME>**	<NAME> – DNS-имя домена клиента, задаётся строкой до 255 символов
9	Задать список IP-адресов DNS-серверов. Список передаётся клиентам в составе DHCP-опции 6 (не обязательно)	**esr: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.
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:esr(config-dhcp-server)# max-lease-time <TIME>**	<TIME> – максимальное время аренды IP-адреса, задаётся в формате DD:HH:MM, где: DD – количество дней, принимает значения [0..364]; HH – количество часов, принимает значения [0..23]; MM – количество минут, принимает значения [0..59] Значение по умолчанию: 1 день
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:esr(config-dhcp-server)# default-lease-time <TIME>**	<TIME> – максимальное время аренды IP-адреса, задаётся в формате DD:HH:MM, где: DD – количество дней, принимает значения [0..364]; HH – количество часов, принимает значения [0..23]; MM – количество минут, принимает значения [0..59] Значение по умолчанию: 12 часов

12	Создать идентификатор класса поставщика (DHCP Опция 60) (не обязательно)	**esr:esr(config)# ip dhcp-server vendor-class-id <NAME>**	<NAME> – идентификатор класса поставщика, задаётся строкой до 31 символа
13	Задать специфическую информацию поставщика (DHCP Опция 43)	**esr:esr(config-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: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

Пример настройки

Задача:

Настроить работу DHCP-сервера в локальной сети, относящейся к зоне безопасности «trusted». Задать пул IP-адресов из подсети 192.168.1.0/24 для раздачи клиентам. Задать время аренды адресов 1 день. Настроить передачу клиентам маршрута по умолчанию, доменного имени и адресов DNS-серверов с помощью DHCP-опций.

Решение:

Создадим зону безопасности «**trusted**» и установим принадлежность используемых сетевых интерфейсов к зонам:

```
esr:esr# configure
esr:esr(config)# security zone trusted
esr:esr(config-zone)# exit
esr:esr(config)# interface gi1/0/2-24
esr:esr(config-if-gi)# security-zone TRUSTED
esr:esr(config-if-gi)# 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:esr# configure
esr:esr(config)# ip dhcp-server pool Simple
esr:esr(config-dhcp-server)# network 192.168.1.0/24
esr:esr(config-dhcp-server)# address-range 192.168.1.100-192.168.1.125
esr: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:esr(config-dhcp-server)# domain-name "eltex.loc"
esr:esr(config-dhcp-server)# default-router 192.168.1.1
```

```
esr:esr(config-dhcp-server)# dns-server 172.16.0.1 8.8.8.8
esr: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:esr(config)# interface gigabitethernet 1/0/1
esr:esr(config-if-gi)# security-zone trusted
esr:esr(config-if-gi)# ip address 192.168.1.1/24
esr: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:esr(config)# object-group service dhcp_server
esr:esr(config-object-group-service)# port-range 67
esr:esr(config-object-group-service)# exit
esr:esr(config)# object-group service dhcp_client
esr:esr(config-object-group-service)# port-range 68
esr:esr(config-object-group-service)# exit
esr:esr(config)# security zone-pair trusted self
esr:esr(config-zone-pair)# rule 30
esr:esr(config-zone-rule)# match protocol udp
esr:esr(config-zone-rule)# match source-address any
esr:esr(config-zone-rule)# match destination-address any
esr:esr(config-zone-rule)# match source-port dhcp_client
esr:esr(config-zone-rule)# match destination-port dhcp_server
esr:esr(config-zone-rule)# action permit
esr:esr(config-zone-rule)# enable
esr:esr(config-zone-rule)# exit
esr:esr(config-zone-pair)# exit
```

Разрешим работу сервера:

```
esr:esr(config)# ip dhcp-server
esr:esr(config)# exit
```

Изменения конфигурации вступят в действие после применения:

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

Просмотреть список арендованных адресов можно с помощью команды:

```
esr:esr# show ip dhcp binding
```

Просмотреть сконфигурированные пулы адресов можно командами:

```
esr:esr# show ip dhcp server pool
esr:esr# show ip dhcp server pool Simple
```

10.5.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.

Процесс настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим настройки сервиса трансляции адресов получателя	`esr:esr(config)# nat destination`	
2	Создать пул IP-адресов и/или TCP/UDP-портов с определённым именем (не обязательно)	`esr:esr(config-dnat)# pool <NAME>`	<NAME> – имя пула NAT-адресов, задаётся строкой до 31 символа
3	Устанавить внутренний IP-адрес, на который будет заменяться IP-адрес получателя	`esr: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:esr(config-dnat-pool)# ip port <PORT>`	<PORT> – TCP/UDP порт, принимает значения [1..65535]
5	Создать группу правил с определённым именем	`esr:esr(config-dnat)# ruleset <NAME>`	<NAME> – имя группы правил, задаётся строкой до 31 символа
6	Задать область применения группы правил. Правила будут применяться только для трафика, идущего из определенной зоны или интерфейса	`esr:esr(config-dnat-ruleset)# from { zone <NAME> | interface <IF> | default }`	<NAME> – имя зоны изоляции; <IF> – имя интерфейса устройства; default – обозначает группу правил для всего трафика, источник которого не попал под критерии других групп правил

7	Задать правило с определённым номером. Правила обрабатываются в порядке возрастания	**esr:esr(config-dnat-rule set)# rule <ORDER>**	<ORDER> – номер правила, принимает значения [1..10000]
8	Задать профиль IP-адресов {отправителя | получателя}, для которых должно срабатывать правило	**esr:esr(config-dnat-rule)# match [not][5] {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
9	Задать профиль IP-адресов {отправителя | получателя}, для которых должно срабатывать правило (не обязательно)	**esr:esr(config-dnat-rule)# match [not][6] {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
10	Устанавить имя или номер IP-протокола, для которого должно срабатывать правило (не обязательно)	**esr:esr(config-dnat-rule)# match [not][6] {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]
11	Задать тип и код сообщений протокола ICMP, для которых должно срабатывать правило (не обязательно)	**esr:esr(config-dnat-rule)# match [not][6] 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

[5] При использовании команды «not» правило будет срабатывать для значений, которые не входят в указанный профиль

[6] При использовании команды «not» правило будет срабатывать для значений, которые не входят в указанный профиль

12	Задать действие «трансляция адреса и порта получателя» для трафика, удовлетворяющего критериям, заданным командами «match»	`esr: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]
13	Активируем конфигурируемое правило	`esr:esr(config-dnat-rule)# enable`	

Пример конфигурации

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 172.16.0.1, доступный порт 80.

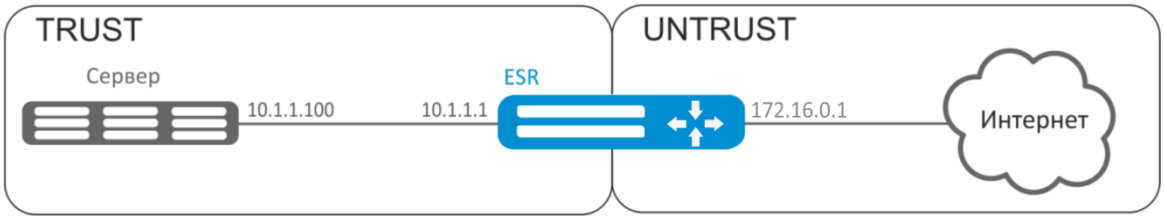


Рисунок 10.4 – Схема сети

Решение:

Создадим зоны безопасности «UNTRUST» и «TRUST». Установим принадлежность используемых сетевых интерфейсов к зонам. Одновременно назначим IP-адреса интерфейсам.

```
esr:esr# configure
esr:esr(config)# security zone UNTRUST
esr:esr(config-zone)# exit
esr:esr(config)# security zone TRUST
esr:esr(config-zone)# exit


esr:esr(config)# interface gigabitethernet 1/0/1
esr:esr(config-if-gi)# security-zone TRUST
esr:esr(config-if-gi)# ip address 10.1.1.1/25
esr:esr(config-if-gi)# exit
```

```
esr:esr(config)# interface tengigabitethernet 1/0/1
esr:esr(config-if-te)# ip address 172.16.0.1/29
esr:esr(config-if-te)# security-zone UNTRUST
esr: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:esr(config)# object-group network NET_UPLINK
esr:esr(config-object-group-network)# ip address 172.16.0.1
esr:esr(config-object-group-network)# exit


esr:esr(config)# object-group service SRV_HTTP
esr:esr(config-object-group-network)# port 80
esr:esr(config-object-group-network)# exit


esr:esr(config)# object-group network SERVER_IP
esr:esr(config-object-group-network)# ip address 10.1.1.100
esr: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:esr(config)# nat destination
esr:esr(config-dnat)# pool SERVER_POOL
esr:esr(config-dnat-pool)# ip address 10.1.1.100
esr:esr(config-dnat-pool)# ip port 80
esr: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:esr(config-dnat)# ruleset DNAT
esr:esr(config-dnat-ruleset)# from zone UNTRUST
esr:esr(config-dnat-ruleset)# rule 1
esr:esr(config-dnat-rule)# match destination-address NET_UPLINK
esr:esr(config-dnat-rule)# match protocol tcp
esr:esr(config-dnat-rule)# match destination-port SERV_HTTP
```

```
esr:esr(config-dnat-rule)# action destination-nat pool SERVER_POOL
esr:esr(config-dnat-rule)# enable
esr:esr(config-dnat-rule)# exit
esr:esr(config-dnat-ruleset)# exit
esr: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:esr(config)# security zone-pair UNTRUST TRUST
esr:esr(config-zone-pair)# rule 1
esr:esr(config-zone-rule)# match source-address any
esr:esr(config-zone-rule)# match destination-address SERVER_IP
esr:esr(config-zone-rule)# match protocol any
esr:esr(config-zone-rule)# match destination-nat
esr:esr(config-zone-rule)# action permit
esr:esr(config-zone-rule)# enable
esr:esr(config-zone-rule)# exit
esr:esr(config-zone-pair)# exit
esr:esr(config)# exit
```

Изменения конфигурации вступят в действие после применения:

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

Произведенные настройки можно посмотреть с помощью команд:

```
esr:esr# show ip nat destination pools
esr:esr# show ip nat destination rulesets
esr:esr# show ip nat proxy-arp
esr:esr# show ip nat translations
```

10.6.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.

Процесс настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим настройки сервиса трансляции адресов отправителя	**esr:esr(config)# nat source**	
2	Создать пул IP-адресов и/или TCP/UDP-портов с определённым именем (не обязательно)	**esr:esr(config-dnat)# pool <NAME>**	<NAME> – имя пула NAT-адресов, задаётся строкой до 31 символа
3	Устанавить внутренний IP-адрес, на который будет заменяться IP-адрес отправителя	**esr: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 отправителя	**esr:esr(config-dnat-pool)# ip port <PORT>**	<PORT> – TCP/UDP порт, принимает значения [1..65535]
5	Создать группу правил с определённым именем	**esr:esr(config-dnat)# ruleset <NAME>**	<NAME> – имя группы правил, задаётся строкой до 31 символа
6	Задать область применения группы правил. Правила будут применяться только для трафика, идущего в определенную зону или интерфейс	**esr:esr(config-dnat-ruleset)# to { zone <NAME> | interface <IF> | default }**	<NAME> – имя зоны изоляции; <IF> – имя интерфейса устройства; default – обозначает группу правил для всего трафика, источник которого не попал под критерии других групп правил
7	Задать правило с определённым номером. Правила обрабатываются в порядке возрастания	**esr:esr(config-dnat-ruleset)# rule <ORDER>**	<ORDER> – номер правила, принимает значения [1..10000]
8	Задать профиль IP-адресов {отправителя | получателя}, для которых должно срабатывать правило	**esr: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

9	Задать профиль IP-адресов {отправителя | получателя}, для которых должно срабатывать правило (не обязательно)	**esr: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
10	Устанавить имя или номер IP-протокола, для которого должно срабатывать правило (не обязательно)	**esr:esr(config-dnat-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]
11	Задать тип и код сообщений протокола ICMP, для которых должно срабатывать правило (не обязательно)	**esr:esr(config-dnat-rule)# match [not] icmp {<ICMP_TYPE> <ICMP_CODE> | <TYPE-NAME>}**	<ICMP_TYPE> – тип сообщения протокола ICMP, принимает значения [0..255]; <ICMP_CODE> – код сообщения протокола ICMP, принимает значения [0..255]. Значение «any» указывает на любой код сообщения; <TYPE-NAME> - имя типа ICMP сообщения
12	Задать действие «трансляция адреса и порта отправителя» для трафика, удовлетворяющего критериям, заданным командами «match»	**esr:esr(config-dnat-rule)# action source-nat { off | pool <NAME> | netmap <ADDR/LEN> | 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. 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

13	Активируем конфигурируемое правило	`esr:esr(config-dnat-rule)# enable`	

Пример конфигурации 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 172.16.0.100-172.16.0.249.

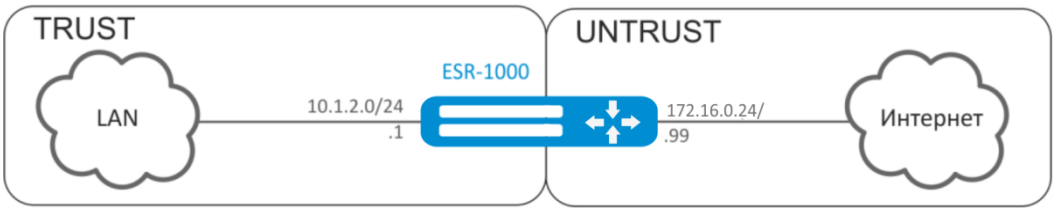


Рисунок 10.5 – Схема сети

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:esr# configure
esr:esr(config)# security zone UNTRUST
esr:esr(config-zone)# exit
esr:esr(config)# security zone TRUST
esr:esr(config-zone)# exit
```

```
esr:esr(config)# interface gigabitethernet 1/0/1
esr:esr(config-if-gi)# ip address 10.1.2.1/24
esr:esr(config-if-gi)# security-zone TRUST
esr:esr(config-if-gi)# exit
```

```
esr:esr(config)# interface tengigabitethernet 1/0/1
esr:esr(config-if-te)# ip address 172.16.0.99/24
esr:esr(config-if-te)# security-zone UNTRUST
esr: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:esr(config)# object-group network LOCAL_NET
```

```
esr:esr(config-object-group-network)# ip address-range 10.1.2.2-10.1.2.254
esr:esr(config-object-group-network)# exit
```

```
esr:esr(config)# object-group network PUBLIC_POOL
esr:esr(config-object-group-network)# ip address-range 172.16.0.100-172.16.0.249
esr: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:esr(config)# security zone-pair TRUST UNTRUST
esr:esr(config-zone-pair)# rule 1
esr:esr(config-zone-rule)# match source-address LOCAL_NET
esr:esr(config-zone-rule)# match destination-address any
esr:esr(config-zone-rule)# match protocol any
esr:esr(config-zone-rule)# action permit
esr:esr(config-zone-rule)# enable
esr:esr(config-zone-rule)# exit
esr:esr(config-zone-pair)# exit
```

Конфигурируем сервис SNAT. Первым шагом создаётся пул адресов публичной сети, используемых для сервиса SNAT.

```
esr:esr(config)# nat sourse
esr:esr(config-snat)# pool TRANSLATE_ADDRESS
esr:esr(config-snat-pool)# ip address-range 172.16.0.100-172.16.0.249
esr: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:esr(config-snat)# ruleset SNAT
esr:esr(config-snat-ruleset)# to zone UNTRUST
esr:esr(config-snat-ruleset)# rule 1
esr:esr(config-snat-rule)# match source-address LOCAL_NET
esr:esr(config-snat-rule)# match destination-address any
esr:esr(config-snat-rule)# match destination-port any
esr:esr(config-snat-rule)# action source-nat pool TRANSLATE_ADDRESS
esr:esr(config-snat-rule)# enable
esr:esr(config-snat-rule)# exit
esr: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:esr(config)# interface tengigabitethernet 1/0/1
esr: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:esr(config)# ip route 0.0.0.0/0 172.16.0.98
esr:esr(config)# exit
```

Изменения конфигурации вступают в действие по команде применения.

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

Пример конфигурации 2

Задача:

Настроить доступ пользователей локальной сети 10.12.2.0/24 к публичной сети с использованием функции Source NAT без использования межсетевого экрана (firewall). Диапазон адресов публичной сети для использования SNAT 198.51.100.100-198.51.100.249.

Рисунок 10.6 – Схема сети

Решение:

Конфигурирование начнем с настройки сетевых интерфейсов и отключения межсетевого экрана:

```
esr:esr(config)# interface gigabitethernet 1/0/1
esr:esr(config-if-gi)# ip address 10.12.2.1/24
esr:esr(config-if-gi)# ip firewall disable
esr:esr(config-if-gi)# exit
```

```
esr:esr(config)# interface tengigabitethernet 1/0/1
esr:esr(config-if-te)# ip address 198.51.100.99/24
esr:esr(config-if-te)# ip firewall disable
esr: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:esr(config)# object-group network LOCAL_NET
esr:esr(config-object-group-network)# ip address-range 10.12.2.2-10.12.2.254
esr:esr(config-object-group-network)# exit



esr:esr(config)# object-group network PUBLIC_POOL
esr:esr(config-object-group-network)# ip address-range 198.51.100.100-198.51.100.249
esr:esr(config-object-group-network)# exit
```

Конфигурируем сервис SNAT.

Первым шагом создаётся пул адресов публичной сети, используемых для сервиса SNAT:

```
esr:esr(config)# nat source
esr:esr(config-snat)# pool TRANSLATE_ADDRESS
esr:esr(config-snat-pool)# ip address-range 198.51.100.100-198.51.100.249
esr: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:esr(config-snat)# ruleset SNAT
esr:esr(config-snat-ruleset)# to interface te1/0/1
esr:esr(config-snat-ruleset)# rule 1
esr:esr(config-snat-rule)# match source-address LOCAL_NET
esr:esr(config-snat-rule)# match destination-address any
esr:esr(config-snat-rule)# match protocol any
esr:esr(config-snat-rule)# action source-nat pool TRANSLATE_ADDRESS
esr:esr(config-snat-rule)# enable
esr:esr(config-snat-rule)# exit
esr: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:esr(config)# interface tengigabitethernet 1/0/1
esr: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 10.12.2.1 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:esr(config)# ip route 0.0.0.0/0 198.51.100.98
esr:esr(config)# exit
```

Изменения конфигурации вступают в действие по команде применения:

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

10.7.Конфигурирование Firewall

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

Межсетевой экран работает на основе правил, настраиваемых между зонами безопасности. Фильтрация настраивается на основании различных полей/атрибутов, таких как:

- destination-address
- destination-mac
- destination-nat
- destination-port
- icmp
- protocol
- protocol-id
- source-address
- source-mac
- source-port

Процесс настройки

Шаг	Описание	Команда	Ключи

1	Создать зоны безопасности	`esr:esr(config)# security zone <zone-name1>`
		
		`esr:esr(config)# security zone <zone-name2>`
			<zone-name> - до 12 символов

2	Задать описание зоны безопасности	`esr:esr(config-zone)# description <description>`	<description> - до 255 символов
3	Создать списки IP адресов, которые будут использоваться при фильтрации	`esr:esr(config)# object-group network <obj-group-name>`	<obj-group-name> - до 31 символа

4	Задать описание списка IP адресов (не обязательно)	**esr:esr(config-object-group-network)# description <description>**	<description> - до 255 символов
5	Внести необходимые IP адреса в список	**esr:esr(config-object-group-network)# ip prefix <ip-prefix>**	<ip-prefix> - задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]
		esr: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]
6	Создать списки сервисов, которые будут использоваться при фильтрации	**esr:esr(config)# object-group service <obj-group-name>**	<obj-group-name> - до 31 символа
7	Задать описание списка сервисов (не обязательно)	**esr:esr(config-object-group-service)# description <description>**	<description> - до 255 символов
8	Внести необходимые сервисы (tcp/udp порты) в список	**esr: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 «-».
9	Включить интерфейсы, саб-интерфейсы, мосты (bridge) или туннели (gre, ip4ip4, l2tp) в зоны безопасности	**esr:esr(config-if-gi)# security-zone <zone-name>**	<zone-name> - до 12 символов
10	Создать набор правил межзонового взаимодействия	**esr:esr(config)# security zone-pair <src-zone-name1> <dst-zone-name2>**	<src-zone-name> - до 12 символов <dst-zone-name> - до 12 символов

11	Создать правило межзонового взаимодействия	**esr:esr(config-zone-pair)# rule <rule-number>**	<rule-number> - 1..10000
12	Задать описание правила (не обязательно)	**esr:esr(config-zone-rule)# description <description>**	<description> - до 255 символов
13	Указать действие данного правила	**esr:esr(config-zone-rule)# action <action> [log]**	<action> - permit/deny/reject/netflow-sample/sflow-sample [log] - не обязательный ключ, включающий запись сообщений о действиях межсетевого экрана. Возможен только для действий permit/deny/reject
14	Установить имя или номер IP-протокола, для которого должно срабатывать правило	**esr:esr(config-zone-rule)# match 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:esr(config-zone-rule)# match protocol-id <protocol-id>	<protocol-id> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF]
15	Устанавливить профиль IP-адресов отправителя, для которых должно срабатывать правило	**esr:esr(config-zone-rule)# match 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
16	Устанавливить профиль IP-адресов получателя, для которых должно срабатывать правило	**esr:esr(config-zone-rule)# match destination-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
17	Устанавливить MAC-адрес отправителя, для которого должно срабатывать правило (не обязательно)	**esr:esr(config-zone-rule)# match source-mac <mac-addr>**	<mac-addr> – задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]

18	Устанавливить MAC-адрес получателя, для которого должно срабатывать правило (не обязательно)	**esr:esr(config-zone-rule)# match destination-mac <mac-addr>**	<mac-addr> – задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]
19	Устанавливить профиль TCP/UDP-портов отправителя, для которых должно срабатывать правило (если указан протокол)	**esr:esr(config-zone-rule)# match 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.
20	Устанавливить профиль TCP/UDP-портов получателя, для которых должно срабатывать правило(если указан протокол)	**esr:esr(config-zone-rule)# match destination-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.
21	Устанавливить тип и код сообщений протокола ICMP, для которых должно срабатывать правило (если в качестве протокола выбран ICMP)	**esr:esr(config-zone-rule)# match 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.
22	Устанавливить ограничение, при котором правило будет срабатывать только для трафика, измененного сервисом трансляции IP-адресов и портов получателя	**esr:esr(config-zone-rule)# match destination-nat**	
23	Установить максимальную скорость прохождения пакетов (не обязательно, доступно только для zone-pair any self и zone-pair <zone-name> any)	**esr:esr(config-zone-pair-rule)# rate-limit pps <rate-pps>**	<rate-pps> - максимальное количество пакетов которое может быть передано на обработку центральным процессором

24	Установить фильтрацию только для фрагментированных IP пакетов (не обязательно, доступно только для zone-pair any self и zone-pair <zone-name> any)	`esr:esr(config-zone-pair-rule)# match fragment`	
25	Установить фильтрацию для IP пакетов, содержащих ip-option (не обязательно, доступно только для zone-pair any self и zone-pair <zone-name> any)	`esr:esr(config-zone-pair-rule)# match ip-option`	
26	Установить фильтрацию для пакетов полученых от модуля ГОСТ-шифрования	`esr:esr(config-zone-pair-rule)# match ipsec-decrypted`	
27	Включить правило межзонового взаимодействия	`esr:esr(config-zone-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”

Пример конфигурации

Задача:

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

Разрешить прохождение SSH трафика от R2 к R1, а все попытки установления сессий на 22-й TCP порт с IP-адресов, отличных от IP устройства R2, необходимо логировать и блокировать.

Настроить фильтрацию фрагментов из зоны безопасности WAN.

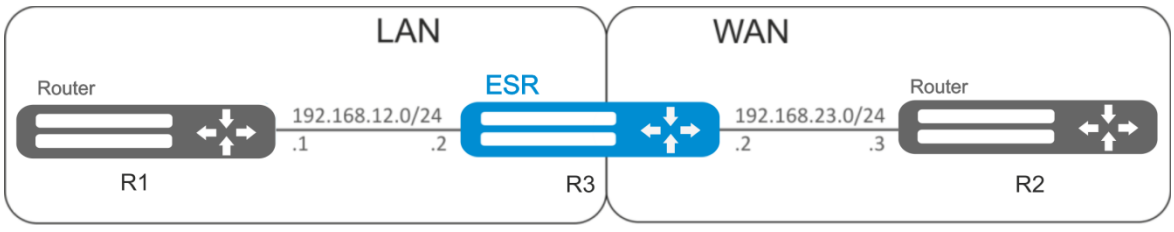


Рисунок 10.7 – Схема сети

Решение:

Для каждой сети ESR создадим свою зону безопасности:

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

Настроим сетевые интерфейсы и определим их принадлежность к зонам безопасности:

```
esr:esr(config)# interface gi1/0/2
esr:esr(config-if-gi)# ip address 192.168.12.2/24
esr:esr(config-if-gi)# security-zone LAN
esr:esr(config-if-gi)# exit
esr:esr(config)# interface gi1/0/3
esr:esr(config-if-gi)# ip address 192.168.23.2/24
esr:esr(config-if-gi)# security-zone WAN
esr: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», а также профиль портов для SSH сессий.

```
esr:esr(config)# object-group network R3
esr:esr(config-object-group-network)# ip address-range 192.168.23.2,192.168.12.2
esr:esr(config-object-group-network)# exit
esr:esr(config)# object-group network R1
esr:esr(config-object-group-network)# ip address-range 192.168.12.1
esr:esr(config-object-group-network)# exit
esr:esr(config)# object-group network R2
esr:esr(config-object-group-network)# ip address-range 192.168.23.3
esr:esr(config-object-group-network)# exit

esr:esr(config)# object-group service ssh

esr:esr(config-object-group-service)# port-range 22

esr:esr(config-object-group-service)# exit
```

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

```
esr:esr(config)# security zone-pair LAN WAN
esr:esr(config-zone-pair)# rule 1

esr:esr(config-zone-pair-rule)# description ICMP
esr:esr(config-zone-pair-rule)# action permit
esr:esr(config-zone-pair-rule)# match protocol icmp
esr:esr(config-zone-pair-rule)# match destination-address R2
```

```
esr:esr(config-zone-pair-rule)# match source-address R1
esr:esr(config-zone-pair-rule)# enable
esr:esr(config-zone-pair-rule)# exit
esr:esr(config-zone-pair)# exit
```

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

```
esr:esr(config)# security zone-pair WAN LAN
esr:esr(config-zone-pair)# rule 1

esr:esr(config-zone-pair-rule)# description ICMP
esr:esr(config-zone-pair-rule)# action permit
esr:esr(config-zone-pair-rule)# match protocol icmp
esr:esr(config-zone-pair-rule)# match destination-address R1
esr:esr(config-zone-pair-rule)# match source-address R2
esr:esr(config-zone-pair-rule)# enable
esr:esr(config-zone-pair-rule)# exit
esr:esr(config-zone-pair)# exit
```

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

```
esr:esr(config)# security zone-pair WAN self
esr:esr(config-zone-pair)# rule 1

esr:esr(config-zone-pair-rule)# description ICMP
esr:esr(config-zone-pair-rule)# action permit
esr:esr(config-zone-pair-rule)# match protocol icmp
esr:esr(config-zone-pair-rule)# match destination-address R3
esr:esr(config-zone-pair-rule)# match source-address R2
esr:esr(config-zone-pair-rule)# enable
esr:esr(config-zone-pair-rule)# exit
esr:esr(config-zone-pair)# exit
```

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

```
esr:esr(config)# security zone-pair LAN self
esr:esr(config-zone-pair)# rule 1

esr:esr(config-zone-pair-rule)# description ICMP
esr:esr(config-zone-pair-rule)# action permit
esr:esr(config-zone-pair-rule)# match protocol icmp
esr:esr(config-zone-pair-rule)# match destination-address R3
esr:esr(config-zone-pair-rule)# match source-address R1
```

```
esr:esr(config-zone-pair-rule)# enable
esr:esr(config-zone-pair-rule)# exit
esr:esr(config-zone-pair)# exit
esr:esr(config)# exit
```

В пару зон из «WAN» в зону «LAN» добавим правило с порядковым номером 2, разрешающее SSH трафик от R2 к R1 и правило, со следующим порядковым номером, для логирования блокировок SSH сессии до R1 со всех IP:

```
esr:esr(config)# security zone-pair WAN LAN
esr:esr(config-zone-pair)# rule 2

esr:esr(config-zone-pair-rule)# description SSH
esr:esr(config-zone-pair-rule)# action permit
esr:esr(config-zone-pair-rule)# match protocol tcp
esr:esr(config-zone-pair-rule)# match destination-address R1
esr:esr(config-zone-pair-rule)# match destination-port ssh
esr:esr(config-zone-pair-rule)# match source-address R2

esr:esr(config-zone-pair-rule)# match source-port any
esr:esr(config-zone-pair-rule)# enable
esr:esr(config-zone-pair-rule)# exit

esr:esr(config-zone-pair)# rule 3

esr:esr(config-zone-pair-rule)# description SSH
esr:esr(config-zone-pair-rule)# action deny log
esr:esr(config-zone-pair-rule)# match protocol tcp
esr:esr(config-zone-pair-rule)# match destination-address R1
esr:esr(config-zone-pair-rule)# match destination-port ssh
esr:esr(config-zone-pair-rule)# match source-address any

esr:esr(config-zone-pair-rule)# match source-port any
esr:esr(config-zone-pair-rule)# enable
esr:esr(config-zone-pair-rule)# exit
esr:esr(config-zone-pair)# exit
esr:esr(config)# exit
```

Второй зоной безопасности по умолчанию является зона с именем «any». В эту зону включаются все зоны безопасности маршрутизатора за исключением зоны «self», т.е. все зоны безопасности, созданные администратором.

Создадим пару зон для фильтрации фрагментов из зоны WAN. Добавим правило для фильтрации фрагментов:

```
esr:esr(config)# security zone-pair WAN any
esr:esr(config-zone-pair)# rule 1

esr:esr(config-zone-pair-rule)# description FRAGMENT
esr:esr(config-zone-pair-rule)# action deny

esr:esr(config-zone-pair-rule)# match fragment
```

```
esr:esr(config-zone-pair-rule)# match protocol any
esr:esr(config-zone-pair-rule)# match destination-address any
esr:esr(config-zone-pair-rule)# match source-address any

esr:esr(config-zone-pair-rule)# enable
esr:esr(config-zone-pair-rule)# exit

esr:esr(config-zone-pair)# exit
```

Изменения конфигурации вступят в действие по следующим командам:

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

Посмотреть членство портов в зонах можно с помощью команды:

```
esr:esr# show security zone
```

Посмотреть пары зон и их конфигурацию можно с помощью команд:

```
esr:esr# show security zone-pair
esr:esr# show security zone-pair configuration
```

Посмотреть активные сессии можно с помощью команды:

```
esr:esr# show ip firewall sessions
```

Посмотреть счетчики сессии можно с помощью команды:

```
esr:esr# show ip firewall counters
```

10.8.Настройка списков доступа (ACL)

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

Процесс настройки

Шаг	Описание	Команда	Ключи
1	Создать список контроля доступа и перейти в режим его конфигурирования	`esr: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	`esr: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:esr(config-acl)# rule <ORDER>**	<ORDER> – номер правила, принимает значения [1..2000000].
4	Указать действие, которое должно быть применено для трафика, удовлетворяющего заданным критериям	**esr:esr(config-acl-rule)# action <ACT>**	<ACT> – назначаемое действие: – permit – прохождение трафика разрешается; – deny – прохождение трафика запрещается.
5	Установить имя IP-протокола, для которого должно срабатывать правило	**esr: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.
6	Установить IP-адреса отправителя, для которых должно срабатывать правило	**esr:esr(config-acl-rule)# match source-address { <ADDR> <WILDCARD> | any }**	<ADDR> – IP-адрес отправителя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <WILDCARD> – маска IP-адреса, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Биты маски, установленные в 0, задают биты IP-адреса, исключаемые из сравнения при поиске. При указании значения «any» правило будет срабатывать для любого IP-адреса отправителя
7	Установить IP-адреса получателя, для которых должно срабатывать правило	**esr:esr(config-acl-rule)# match destination-address { <ADDR> <WILDCARD> | any }**	
8	Установить MAC-адреса отправителя, для которых должно срабатывать правило	**esr: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	**esr:esr(config-acl-rule)# match destination-mac <ADDR> <WILDCARD>**	

10	Установить номер TCP/UDP-порта отправителя, для которого должно срабатывать правило (если протокол указан)	**esr: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 протокол указан)	**esr:esr(config-acl-rule)# match destination-port { <PORT> | any }**	
12	Установить значение 802.1p приоритета, для которого должно срабатывать правило	**esr: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 возможно использовать совместно с IP Precedence)	**esr: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 возможно использовать совместно с DSCP)	**esr: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	**esr:esr(config-acl-rule)# match vlan <VID>**	<VID> – идентификационный номер VLAN, принимает значения [1..4094]
16	Активировать правило	**esr:esr(config-acl-rule)# enable**	
17	Указать список контроля доступа к конфигурируемому интерфейсу для фильтрации входящего трафика	**esr: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.

Пример конфигурации

Задача:

Разрешить прохождения трафика только из подсети 192.168.20.0/24.

Решение:

Настроим список доступа для фильтрации по подсетям:

```
esr:esr# configure
esr:esr(config)# ip access-list extended white
esr:esr(config-acl)# rule 1
esr:esr(config-acl-rule)# action permit
esr:esr(config-acl-rule)# match protocol any
esr:esr(config-acl-rule)# match source-address 192.168.20.0 255.255.255.0
esr:esr(config-acl-rule)# match destination-address any
esr:esr(config-acl-rule)# enable
esr:esr(config-acl-rule)# exit
esr:esr(config-acl)# exit
```

Применим список доступа на интерфейс Gi1/0/19 для входящего трафика:

```
esr:esr(config)# interface gigabitethernet 1/0/19
esr:esr(config-if-gi)# service-acl input white
```

Изменения конфигурации вступят в действие по следующим командам:

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

Просмотреть детальную информацию о списке доступа возможно через команду:

```
esr:esr# show ip access-list white
```

10.9.Конфигурирование статических маршрутов

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

Процесс настройки

Добавление статический маршрут возможно командой в режиме глобальной конфигурации:

```
esr:esr(config)# ip route <SUBNET> { <NEXTHOP> | interface <IF> | tunnel <TUN> | wan
load-balance rule <RULE> [<METRIC>] | blackhole | unreachable | prohibit } [ <METRIC> ]
[ track <TRACK-ID> ]
```

<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 3.3;

<TUN> – имя туннеля, задаётся в виде, описанном в разделе 0;

<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);

Пример конфигурации

Задача:

Настроить доступ к сети Internet для пользователей локальной сети 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.

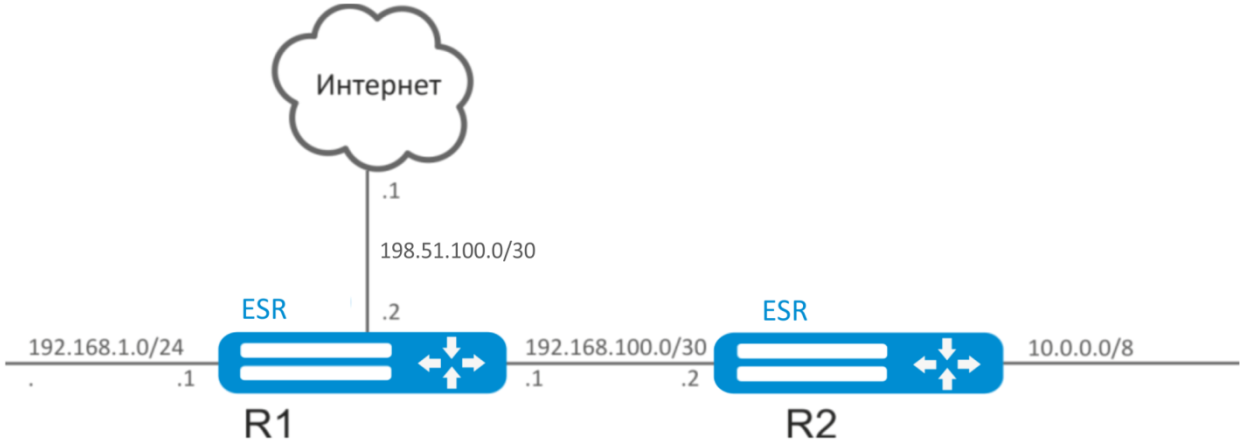


Рисунок 10.8 – Схема сети

Решение:

Зададим имя устройства для маршрутизатора R1:

```
esr:esr# hostname R1
esr:esr(config)# do commit
R1#(config)# do confirm
```

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:

```
R1(config)# interface gi1/0/1
R1(config-if-gi)# security-zone LAN
R1(config-if-gi)# ip address 192.168.1.1/24
R1(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:

```
R1(config)# interface gi1/0/2
R1(config-if-gi)# security-zone LAN
R1(config-if-gi)# ip address 192.168.100.1/30
R1(config-if-gi)# exit
```

Для интерфейса gi1/0/3 укажем адрес 198.51.100.2/30 и зону «WAN». Через данный интерфейс R1 будет подключен к сети Internet:

```
R1(config)# interface gi1/0/3
R1(config-if-gi)# security-zone WAN
R1(config-if-gi)# ip address 198.51.100.2/30
R1(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):

```
R1(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 (198.51.100.1):

```
R1(config)# ip route 0.0.0.0/0 198.51.100.1
```

Изменения конфигурации на маршрутизаторе R1 вступят в действие по следующим командам:

```
R1# commit
Configuration has been successfully committed
R1# confirm
Configuration has been successfully confirmed
```

Зададим имя устройства для маршрутизатора R2:

```
esr:esr# hostname R2
esr:esr#(config)# do commit
R2#(config)# do confirm
```

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:

```
R2(config)# interface gi1/0/1
R2(config-if-gi)# security-zone LAN
R2(config-if-gi)# ip address 10.0.0.1/8
R2(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:

```
R2(config)# interface gi1/0/2
R2(config-if-gi)# security-zone LAN
R2(config-if-gi)# ip address 192.168.100.2/30
```

```
R2(config-if-gi)# exit
```

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

```
R2(config)# ip route 0.0.0.0/0 192.168.100.1
```

Изменения конфигурации на маршрутизаторе R2 вступят в действие по следующим командам:

```
R2# commit
Configuration has been successfully committed
R2# confirm
Configuration has been successfully confirmed
```

Проверить таблицу маршрутов можно командой:

```
R2(config)# show ip route
```

10.10. 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	Первести физичекский интерфейс в режим коммутации	`esr:esr(config-if-gi)# switchport`	
2	Задать режим работы интерфейса e1	`esr:esr(config-if-gi)# switchport mode e1`	
3	Задать источник синхронизации	`esr: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	Задать хэш алгоритм проверки кадра (не обязательно)	`esr:esr(config-if-gi)# switchport e1 crc <FCS>`	<FCS> - последовательность проверки кадра: 16 (по умолчанию) – FCS16; 32 – FCS32.

5	Задать проверку на наличие ошибок при передаче (не обязательно)	**esr: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
6	Задать инвертацию передаваемых бит (не обязательно)	**esr:esr(config-if-gi) # switchport e1 invert data**	
7	Задать тип линейного кодирования (не обязательно)	**esr: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
8	Задать количесто тайм слотов	**esr:esr(config-if-gi) # switchport e1 timeslots <RANGE>**	<RANGE> – количество тайм-слотов
9	Использовать E1 как единую сущность, без таймслотов (не обязательно)	**esr:esr(config-if-gi) # switchport e1 unframed**	
10	Конфигурируем E1	**esr:esr(config)# interface e1 1/<SLOT>/1**	<SLOT> – номер слота.
11	Включаем CHAP-аутентификацию для PPP (не обязательно)	**esr:esr(config-e1)# ppp authentication chap**	
12	Задается имя маршрутизатора, которое отправляется удаленной стороне для прохождения CHAP-аутентификации (не обязательно)	**esr:esr(config-e1)# ppp chap hostname <NAME>**	<NAME> – имя маршрутизатора
13	Задать пароль для аутентификации (не обязательно)	**esr:esr(config-e1)# ppp chap password ascii-text <CLEAR-TEXT>**	<CLEAR-TEXT> – пароль в открытой форме

14	Включить игнорирование аутентификации (не обязательно)	**esr:esr(config-e1)# ppp chap refuse**	
15	Задать имя пользователя для аутентификации (не обязательно)	**esr:esr(config-e1)# ppp chap username <NAME>**	<NAME> – имя пользователя
16	Разрешается принимать от соседа любой ненулевой IP-адрес в качестве локального IP-адреса (не обязательно)	**esr:esr(config-e1)# ppp ipcp accept-address**	
17	Задать IP-адрес, который отправляется удаленной стороне для последующего его присвоения (не обязательно)	**esr:esr(config-e1)# ppp ipcp remote-address <ADDR>**	<ADDR> – IP-адрес удаленного шлюза
18	Задать количество попыток отправки Configure-Request пакетов, прежде чем удаленный пир будет признан неспособным ответить (не обязательно).	**esr:esr(config-e1)# ppp max-configure <VALUE>**	<VALUE> – количество попыток.
19	Задать количество попыток выслать Configure-NAK пакеты, прежде чем будут подтверждены все опции (не обязательно)	**esr:esr(config-e1)# ppp max-failure <VALUE>**	<VALUE> – количество попыток.
20	Задать количество попыток выслать Terminate-Request пакеты, прежде чем сессия будет прервана (не обязательно)	**esr:esr(config-e1)# ppp max-terminate <VALUE>**	<VALUE> – количество попыток.
21	Задать размер MRU (Maximum Receive Unit) для интерфейса (не обязательно)	**esr:esr(config-e1)# ppp mru <MRU>**	<MRU> – значение MRU
22	Включение режима MLPPP (не обязательно)	**esr:esr(config-e1)# ppp multilink**	

23	Добавить в MLPPP группу (не обязательно)	`esr:esr(config-e1)# ppp multilink-group <GROUP-ID>`	<GROUP-ID> – номер группы
24	Задается интервал времени в секундах, по истечении которого маршрутизатор отправляет keepalive-сообщение (не обязательно)	`esr:esr(config-e1)# ppp timeout keepalive <TIME>`	<TIME> – время в секундах
25	Задается интервал, по истечении которого маршрутизатор повторяет запрос на установление сессии (не обязательно)	`esr:esr(config-e1)# ppp timeout retry <TIME>`	<TIME> – время в секундах

Пример конфигурации

Задача:

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

Рисунок 10.9 – Схема сети

Решение:

Переключаем интерфейс, в котором установлен ToPGATE-SFP, gigabitethernet 1/0/10 в режим работы E1:

```
esr:esr# configure

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

Включим interface e1 1/3/1:

```
esr:esr(config)# interface e1 1/3/1
```

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

Изменения конфигурации вступят в действие по следующим командам:

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

10.11. 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.

Процесс настройки

Шаг	Описание	Команда	Ключи
1	Добавить сетевой мост в систему и перейти в режим настройки его параметров	`esr:esr(config)# bridge <BRIDGE-ID>`	<BRIDGE-ID> – идентификационный номер моста, принимает значения в диапазоне: для esr100/200 – [1..250], для esr1000 - [1..500]
2	Активировать сетевой мост	`esr:esr(config-bridge)# enable`	
3	Назначить описание конфигурируемому сетевому мосту	`esr:esr(config-bridge)# description <DESCRIPTION>`	<DESCRIPTION> – описание сетевого моста, задаётся строкой до 255 символов
4	Связать текущий сетевого моста с VLAN. Все порты, являющиеся членами назначаемого VLAN, автоматически включаются в сетевой мост и становятся участниками общего L2 домена	`esr:esr(config-bridge)# vlan <VID>`	<VID> – идентификатор VLAN, задаётся в диапазоне [1..4094].
5	Задать MAC-адрес сетевого моста, отличный от системного (не обязательно)	`esr: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].

6	Связать саб-интерфейс или L2TPv3 туннель с сетевым мостом. Связанные саб-интерфейсы, туннели и сетевые мосты автоматически становятся участниками общего L2 домена	**esr:esr(config-if-gi)# bridge-group <BRIDGE-ID>** **esr:esr(config-if-l2tpv3)# bridge-group <BRIDGE-ID>**	<BRIDGE-ID> – идентификационный номер моста, принимает значения в диапазоне: для esr100/200 – [1..250], для esr1000 - [1..500]

Пример конфигурации 1

Задача:

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

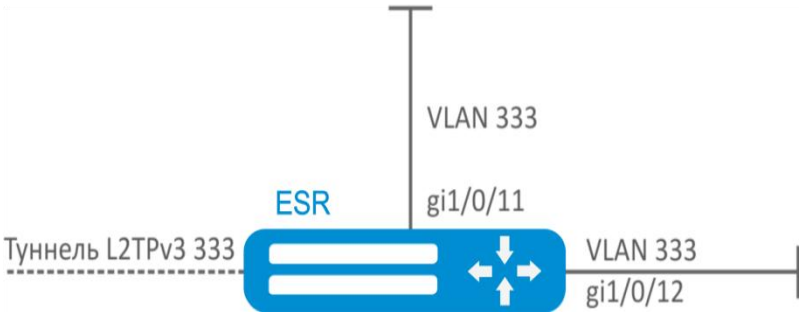


Рисунок 10.10 – Схема сети

Решение:

Создадим VLAN 333:

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

Создадим зону безопасности «trusted»:

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

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

```
esr:esr(config)# interface gigabitethernet 1/0/11-12
esr: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:esr(config)# bridge 333
esr:esr(config-bridge)# vlan 333
esr:esr(config-bridge)# security-zone trusted
esr:esr(config-bridge)# enable
```

Установим принадлежность L2TPv3-туннеля к мосту, который связан с локальной сетью (настройка L2TPv3-туннеля рассматривается в разделе 10.17). В общем случае идентификаторы моста и туннеля не должны совпадать с VID как в данном примере.

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

Пример конфигурации 2

Задача:

Настроить маршрутизацию между VLAN 50 (10.0.50.0/24) и VLAN 60 (10.0.60.1/24). VLAN 50 должен относиться к зоне «LAN1», VLAN 60 – к зоне «LAN2», разрешить свободную передачу трафика между зонами.

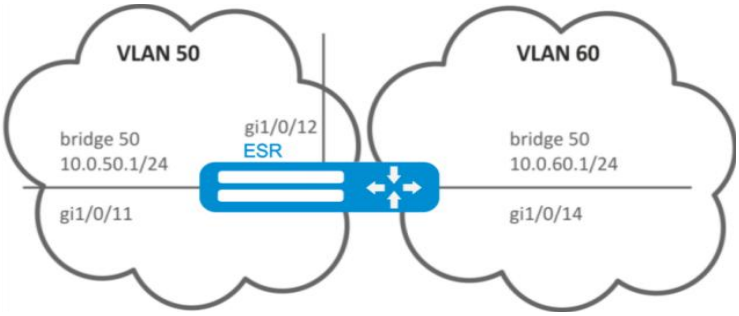


Рисунок 10.11 – Схема сети

Решение:

Создадим VLAN 50, 60:

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

Создадим зоны безопасности «LAN1» и «LAN2»:

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

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

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

Назначим интерфейсу gi1/0/14 VLAN 60:

```
esr:esr(config)# interface gigabitethernet 1/0/14
esr: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:esr(config)# bridge 50
esr:esr(config-bridge)# vlan 50
```

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

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

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

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

```
esr:esr(config)# security zone-pair LAN1 LAN2
esr:esr(config-zone-pair)# rule 1
esr:esr(config-zone-rule)# action permit
esr:esr(config-zone-rule)# match protocol any
esr:esr(config-zone-rule)# match source-address any
esr:esr(config-zone-rule)# match destination-address any
esr:esr(config-zone-rule)# enable
esr:esr(config-zone-rule)# exit
esr:esr(config-zone-pair)# exit
esr:esr(config)# security zone-pair LAN2 LAN1
esr:esr(config-zone-pair)# rule 1
esr:esr(config-zone-rule)# action permit
esr:esr(config-zone-rule)# match protocol any
esr:esr(config-zone-rule)# match source-address any
esr:esr(config-zone-rule)# match destination-address any
esr:esr(config-zone-rule)# enable
esr:esr(config-zone-rule)# exit
esr:esr(config-zone-pair)# exit
esr:esr(config)# exit
```

Изменения конфигурации вступят в действие по следующим командам:

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

Посмотреть членство интерфейсов в мосте можно командой:

```
esr:esr# show interfaces bridge
```

10.12. 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.

Процесс настройки

Шаг	Описание	Команда	Ключи
1	Настроить приоритетность протокола RIP маршрутизации для основной таблицы маршрутизации (не обязательно)	**esr: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: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: RIP (10000)
3	Создать списки IP-подсетей, которые в дальнейшем будут использоваться для фильтрации анонсируемых и получаемых IP-маршрутов	**esr: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:esr(config-pl)# permit {object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> | le <LEN> | ge <LEN> [le <LEN>] }]|default-route}** **esr: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:esr(config)# router rip** **esr:esr(config-rip)#**	
6	Включить RIP-протокол	**esr:esr(config-rip)# enable**	
7	Определить алгоритм аутентификации протокола RIP (не обязательно)	**esr:esr(config-rip)# authentication algorithm { cleartext | md5 }**	cleartext – пароль, передается открытым текстом; md5 – пароль хешируется по алгоритму md5
8	Устанавить пароль для аутентификации с соседом (не обязательно)	**esr: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:esr(config-rip)# authentication key-chain <KEYCHAIN>**	<KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов
10	Выключить анонсирование маршрутов на интерфейсах, где это не нужно (не обязательно)	**esr: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: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: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 данного маршрута (не обязательно)	**esr:esr(config-rip)# timers flush <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. При установке значения нужно учитывать следующее правило: «timers invalid + 60» Значение по умолчанию: 240 секунд

14	Включить анонсирование подсетей	**esr: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: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: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: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: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: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: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:esr(config)# tunnel <TUN-TYPE> <TUN-NUM>	<TUN-TYPE> тип туннеля <TUN-NUM> номер туннеля
		esr:esr(config)# bridge <BR-NUM>	<BR-NUM> - номер bridge
18	Установить величину метрики RIP-маршрутов на интерфейсе (не обязательно)	**esr: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: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: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: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]

Пример конфигурации

Задача:

Настроить на маршрутизаторе протокол RIP для обмена маршрутной информацией с соседними маршрутизаторами. Маршрутизатор должен анонсировать статические маршруты и подсети 10.0.115.0/24, 10.0.14.0/24, 10.0.0.0/24. Анонсирование маршрутов должно происходить каждые 25 секунд.

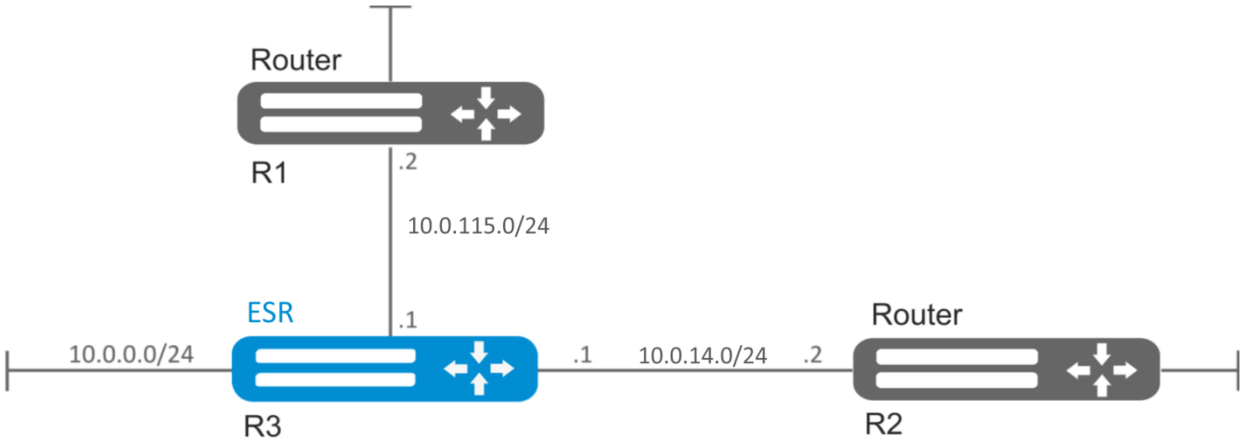


Рисунок 10.12 – Схема сети

Решение:

Предварительно нужно настроить IP-адреса на интерфейсах согласно схеме сети, приведенной на рисунке 10.13

Перейдём в режим конфигурирования протокола RIP:

```
esr:esr(config)# router rip
```

Укажем подсети, которые будут анонсироваться протоколом: 10.0.115.0/24, 10.0.14.0/24 и 10.0.0.0/24:

```
esr:esr(config-rip)# network 10.0.115.0/24
esr:esr(config-rip)# network 10.0.14.0/24
esr:esr(config-rip)# network 10.0.0.0/24
```

Для анонсирования протоколом статических маршрутов выполним команду:

```
esr:esr(config-rip)# redistribute static
```

Настроим таймер, отвечающий за отправку маршрутной информации:

```
esr:esr(config-rip)# timers update 25
```

После установки всех требуемых настроек включаем протокол:

```
esr:esr(config-rip)# enable
```

Изменения конфигурации вступят в действие после применения:

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

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

Для того чтобы просмотреть таблицу маршрутов RIP воспользуемся командой:

```
esr:esr# show ip rip
```

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

10.13. Настройка OSPF

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

Процесс настройки

Шаг	Описание	Команда	Ключи
1	Настроить приоритетность протокола OSPF маршрутизации для основной таблицы маршрутизации (не обязательно)	`esr:esr(config)# ip protocols ospf preference <VALUE>`	<VALUE> – приоритетность протокола, принимает значения в диапазоне [1..255] Значение по умолчанию: OSPF (150)
2	Настроить емкость таблиц маршрутизации протокола OSPF (не обязательно)	`esr:esr(config)# ip protocols ospf max-routes <VALUE>`	<VALUE> – количество маршрутов протокола OSPF в маршрутной таблице, принимает значения в диапазоне [1..500000] Значение по умолчанию: OSPF (500000)
3	Включить вывод информации о состоянии отношений с соседями для протокола маршрутизации OSPF (не обязательно)	`esr:esr(config)# router ospf log-adjacency-changes`	
4	Создать списки IP-подсетей, которые в дальнейшем будет использоваться для фильтрации анонсируемых и получаемых IP-маршрутов	`esr:esr(config)# ip prefix-list <NAME>`	<NAME> – имя конфигурируемого списка подсетей, задаётся строкой до 31 символа.

5	Разрешить (permit) или запретить (deny) списки префиксов	**esr:esr(config-pl)# permit {object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> | le <LEN> | ge <LEN> [le <LEN>] }]|default-route}** **esr: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
6	Добавить OSPF-процесс в систему и осуществить переход в режим настройки параметров OSPF-процесса	**esr:esr(config)# router ospf <ID>**	<ID> – номер автономной системы процесса, принимает значения [1..65535]
7	Установить идентификатор маршрутизатора для данного OSPF процесса	**esr:esr(config-ospf)# router-id <ID>**	<ID> – идентификатор маршрутизатора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]
8	Определить приоритетность маршрутов процесса OSPF	**esr:esr(config-ospf)# preference <VALUE>**	<VALUE> – приоритетность маршрутов процесса OSPF, принимает значения в диапазоне [1..255] Значение по умолчанию: 10
9	Включить совместимость с RFC 1583 (не обязательно)	**esr:esr(config-ospf)# compatible rfc1583**	
10	Включить анонсирование подсетей	**esr:esr(config- ospf)# 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]

11	Добавить фильтрацию подсетей во входящих или исходящих обновлениях (не обязательно)	**esr:esr(config- ospf)# prefix-list <PREFIX-LIST-NAME> { in | out }**	<PREFIX-LIST-NAME> – имя сконфигурированного списка подсетей, задаётся строкой до 31 символа in – фильтрация входящих маршрутов; out – фильтрация анонсируемых маршрутов.
12	Включить анонсирование маршрутов полученных альтернативным способом (не обязательно)	**esr:esr(config- ospf)# redistribute static [route-map <NAME>]**	<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых статических маршрутов, задаётся строкой до 31 символа
		esr:esr(config- ospf)# redistribute connected [route-map <NAME>]	<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых напрямую подключенных подсетей, задаётся строкой до 31 символа
		esr: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:esr(config- ospf)# redistribute bgp <AS> [route-map <NAME>]	<AS> – номер автономной системы, может принимать значения [1..4294967295]; <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых BGP-маршрутов, задаётся строкой до 31 символа
13	Активировать OSPF-процесс	**esr:esr(config-ospf)# enable**	
14	Создать OSPF-область и перейти в режим конфигурирования области	**esr:esr(config-ospf)# area <AREA_ID>**	<AREA_ID> – идентификатор области, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]

15	Определить тип области	**esr:esr(config-ospf-area)# area-type <TYPE> [no-summary]**	<TYPE> – тип области: - **stub** – устанавливает значение stub (тупиковая область); no-summary – команда в связке с параметром «stub» образует область «totally stubby» (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 totally nssa (автоматически генерирует маршрут по умолчанию как межобластной)
16	Включить генерацию маршрута по умолчанию для NSSA-области и анонсирование его в качестве NSSA-LSA	**esr:esr(config-ospf-area)# default-information-originate**	
17	Включтть суммаризацию или скрытие подсетей	**esr: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.
18	Активироваль OSPF-область	**esr:esr(config-ospf-area)# enable**	
19	Установить виртуальное соединение между основной и удаленными областями, имеющими между ними несколько областей	**esr:esr(config-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].

20	Установить виртуальное соединение между основной и удаленными областями, имеющими между ними несколько областей	**esr:esr(config-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 не получил подтверждения о получении (например, Database Description пакет или Link State Request пакеты)	**esr:esr(config-ospf-vlink)# restransmit-interval <TIME>**	<TIME> – время в секундах, принимает значения [1..65535] Значение по умолчанию: 5 секунд
22	Установить интервал времени в секундах, по истечении которого маршрутизатор отправляет следующий hello-пакет	**esr:esr(config-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:esr(config-ospf-vlink)# dead-interval <TIME>**	<TIME> – время в секундах, принимает значения [1..65535] Значение по умолчанию: 40 секунд
24	Активироваль виртуальное соединение	**esr:esr(config-ospf-vlink)# enable**	
25	Перейти в режим конфигурирования интерфейса/туннеля/ сетевого моста	**esr: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:esr(config)# tunnel <TUN-TYPE> <TUN-NUM>	<TUN-TYPE> тип туннеля <TUN-NUM> номер туннеля
		esr:esr(config)# bridge <BR-NUM>	<BR-NUM> - номер bridge

26	Определить принадлежность интерфейса/туннеля/сетевого моста к определенному OSPF-процессу	**esr:esr(config-if-gi)# ip ospf instance <ID>**	<ID> – номер процесса, принимает значения [1..65535].
27	Определить принадлежность интерфейса к определенной области OSPF-процесса	**esr:esr(config-if-gi)# ip ospf area <AREA_ID>**	<AREA_ID> – идентификатор области, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]
28	Включить маршрутизацию по протоколу OSPF на интерфейсе	**esr:esr(config-if-gi)# ip ospf**	
29	Включить режим, в котором OSPF-процесс будет игнорировать значение MTU интерфейса во входящих Database Description-пакетах	**esr:esr(config-if-gi)# ip ospf mtu-ignore**	
30	Определить алгоритм аутентификации протокола OSPF	**esr:esr(config-if-gi)# ip ospf authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм аутентификации: **cleartext** – пароль, передается открытым текстом; **md5** – пароль хешируется по алгоритму md5
31	Установить пароль для аутентификации с OSPF-соседом при передаче пароля открытым текстом	**esr: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...).
32	Определить список паролей для аутентификации по алгоритму хеширования md5 с соседом	**esr:esr(config-if-gi)# ip ospf authentication key-chain <KEYCHAIN>**	<KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов
33	Определить интервал времени в секундах, по истечении которого маршрутизатор выберет DR в сети	**esr:esr(config-if-gi)# ip ospf wait-interval <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 40 секунд.

34	Установить интервал времени в секундах, по истечении которого маршрутизатор повторно отправит пакет, на который не получил подтверждения о получении (например, Database Description пакет или Link State Request пакеты)	**esr:esr(config-if-gi)# ip ospf restransmit-interval <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 5 секунд
35	Установить интервал времени в секундах, по истечении которого маршрутизатор отправляет следующий hello-пакет	**esr:esr(config-if-gi)# ip ospf hello-interval <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 10 секунд
36	Установить интервал времени в секундах, по истечении которого сосед будет считаться неактивным. Этот интервал должен быть кратным значению hello-interval	**esr:esr(config-if-gi)# ip dead-interval <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 40 секунд
37	Установить интервал времени, в течение которого NBMA-интерфейс ждет, прежде чем отправить HELLO-пакет соседу, даже в случае, если сосед неактивен	**esr:esr(config-if-gi)# ip poll-interval <TIME>**	<TIME> – время в секундах, принимает значения [1 .. 65535]. Значение по умолчанию: 120 секунд
38	Задать статический IP-адрес соседа для установления отношения в NMBA и P2MP (Point-to-MultiPoint) сетях	**esr: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

39	Определить тип сети для установления OSPF соседства	`esr:esr(config-if-gi)# ip ospf network <TYPE>`	<TYPE> – тип сети: **broadcast** – тип соединения широковещательный; non-broadcast – тип соединения NBMA; **point-to-multipoint** – тип соединения точка-многоточие; **point-to-multipoint non-broadcast** – тип соединения NBMA точка-многоточие; **point-to-point** – тип соединения точка-точка Значение по умолчанию: broadcast
40	Установить приоритет маршрутизатора, который используется для выбора DR и BDR	`esr:esr(config-if-gi)# ip ospf priority <VALUE>`	<VALUE> – приоритет интерфейса, принимает значения [1..65535]. Значение по умолчанию: 120
41	Установить величину метрики на интерфейсе или туннеле	`esr:esr(config-if-gi)# ip ospf cost <VALUE>`	<VALUE> – величина метрики, задаётся в размере [0..32767]. Значение по умолчанию: 150
42	Включить логирование изменений состояния OSPF-соседей	`esr:esr(config-if-gi)# router ospf log-neighbor-changes`	Значение по умолчанию: Логирование выключено

Пример конфигурации 1

Задача:

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

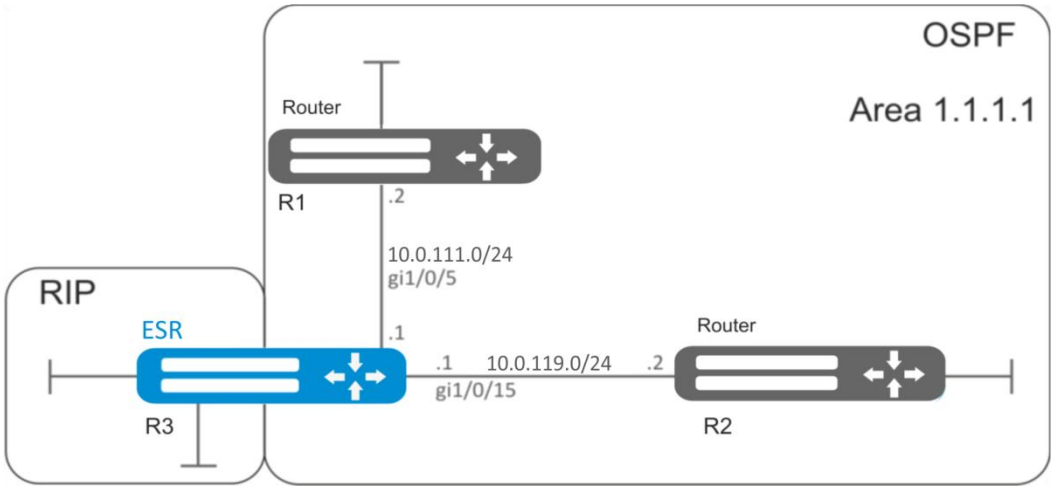


Рисунок 10.14 – Схема сети

Решение:

Предварительно нужно настроить IP-адреса на интерфейсах согласно схеме, приведенной на рисунке 10.15

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

```
esr:esr(config)# router ospf 10
```

Создадим и включим требуемую область.

```
esr:esr(config-ospf)# area 1.1.1.1
esr:esr(config-ospf-area)# enable
esr:esr(config-ospf-area)# exit
```

Включим анонсирование маршрутной информации из протокола RIP:

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

Включим OSPF-процесс:

```
esr:esr(config-ospf)# enable
esr: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:esr(config)# interface gigabitethernet 1/0/5
esr:esr(config-if-gi)# ip ospf instance 10
esr:esr(config-if-gi)# ip ospf area 1.1.1.1
esr:esr(config-if)# ip ospf
esr:esr(config-if)# exit
```

```
esr:esr(config)# interface gigabitethernet 1/0/15
esr:esr(config-if-gi)# ip ospf instance 10
esr:esr(config-if-gi)# ip ospf area 1.1.1.1
esr:esr(config-if-gi)# ip ospf
esr:esr(config-if-gi)# exit
esr:esr(config)# exit
```

Изменения конфигурации вступят в действие после применения:

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

Пример конфигурации 2

Задача:

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

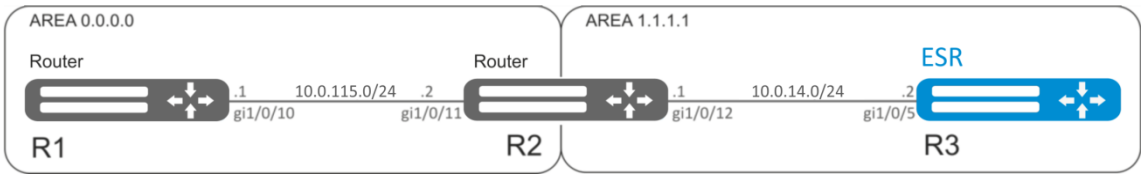


Рисунок 10.16 – Схема сети

Решение:

Предварительно нужно настроить протокол OSPF и IP-адреса на интерфейсах согласно схеме, приведенной на рисунке 10.17

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

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

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

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

Изменения конфигурации вступают в действие по команде применения:

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

Пример конфигурации 3

Задача:

Объединить две магистральные области в одну с помощью virtual link.

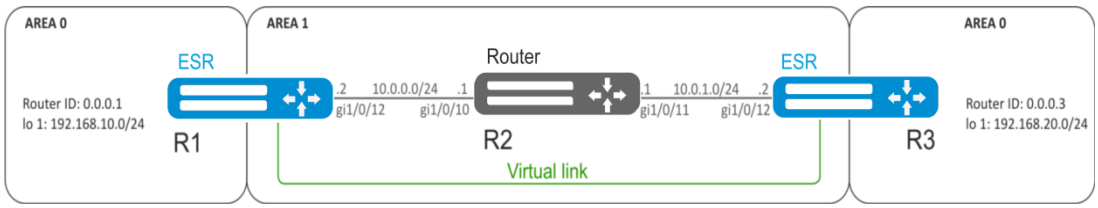


Рисунок 10.18 – Схема сети

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 Рисунок 10.18.

На маршрутизаторе R1 перейдем в режим конфигурирования области 1.1.1.1:

```
esr:esr(config-ospf)# area 1.1.1.1
```

Создадим virtual link с идентификатором 0.0.0.3 и включим его:

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

На маршрутизаторе R3 перейдем в режим конфигурирования области 1.1.1.1:

```
esr:esr(config-ospf)# area 1.1.1.1
```

Создадим virtual link с идентификатором 0.0.0.1 и включим его:

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

Изменения конфигурации вступят в действие после применения:

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

Рассмотрим таблицу маршрутизации на маршрутизаторе R1:

```
esr: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: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:esr# show ip ospf neighbors 10
```

Таблицу маршрутов протокола OSPF можно просмотреть командой:

```
esr:esr# show ip ospf 10
```

В firewall необходимо разрешить протокол OSPF (89).

10.14. 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.

Процесс настройки

Шаг	Описание	Команда	Ключи
1	Настроить приоритетность протокола BGP маршрутизации для основной таблицы маршрутизации (не обязательно)	**esr: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:esr(config)# ip protocols bgp max-routes <VALUE>**	<VALUE> – количество маршрутов протокола OSPF в маршрутной таблице, принимает значения в диапазоне [1..2600000] Значение по умолчанию: OSPF (2600000)
3	Включить вывод информации о состоянии отношений с соседями для протокола маршрутизации BGP (не обязательно)	**esr:esr(config)# router bgp log-adjacency-changes**	
4	Создать списки IP-подсетей, которые в дальнейшем будут использоваться для фильтрации анонсируемых и получаемых IP-маршрутов	**esr:esr(config)# ip prefix-list <NAME>**	<NAME> – имя конфигурируемого списка подсетей, задаётся строкой до 31 символа.
5	Разрешить (permit) или запретить (deny) списки префиксов	**esr:esr(config-pl)# permit {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

		esr:esr(config-pl)# deny object-group <OBJ-GROUP-NETWORK-NAME> [{ eq <LEN> | le <LEN> | ge <LEN> [le <LEN>] }] | default-route}	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 BGP-процесс в систему и осуществить переход в режим настройки параметров BGP-процесса	**esr:esr(config)# router bgp <AS>**	<AS> – номер автономной системы процесса, принимает значения [1..4294967295].
7	Определить тип конфигурируемой маршрутной информации и перейти в данный режим настройки	**esr:esr(config-bgp)# address-family { ipv4 }**	ipv4 – семейство IPv4;
8	Установить идентификатор маршрутизатора	**esr:esr(config-bgp-af)# router-id <ID>**	<ID> – идентификатор маршрутизатора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]
9	Установить временной интервал, по истечении которого идет проверка соединения со встречной стороной	**esr:esr(config-bgp-af)# timers keeaplive <TIME>**	<TIME> – время в секундах, принимает значения [1..65535] Значение по умолчанию: 60 секунд
10	Установить временной интервал, по истечении которого встречная сторона считается недоступной	**esr:esr(config-bgp-af)# timers holdtime <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 180 секунд
11	Установить идентификатор Route-Reflector кластера, которому принадлежит BGP-процесс маршрутизатора	**esr:esr(config-bgp-af)# cluster-id <ID>**	<ID> – идентификатор Route-Reflector кластера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]
12	Определить глобальный алгоритм аутентификации с соседями	**esr:esr(config-bgp-af)# authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм шифрования: md5 – пароль шифруется по алгоритму md5.

13	Установить глобальный пароль для аутентификации с соседями	**esr:esr(config-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...).
14	Активировать BGP-процесс	**esr:esr(config-bgp-af)# enable**	
15	Включить анонсирование статических маршрутов полученых альтернативным образом	**esr:esr(config-bgp-af)# redistribute static [route-map <NAME>]**	<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых статических маршрутов, задаётся строкой до 31 символа.
		esr:esr(config-bgp-af)# redistribute connected [route-map <NAME>]	<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых напрямую подключенных подсетей, задаётся строкой до 31 символа.
		esr:esr(config-bgp-af)# redistribute rip [route-map <NAME>]	<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых RIP-маршрутов, задаётся строкой до 31 символа.
		esr:esr(config-bgp-af)# 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: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.
16	Включить анонсирование подсетей	**esr: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]
17	Добавить фильтрацию подсетей во входящих или исходящих обновлениях (не обязательно)	**esr: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.
18	Добавить BGP-соседа и осуществить переход в режим настройки параметров BGP-соседа	**esr:esr(config-bgp-af)# neighbor <ADDR>**	<ADDR> – IP адрес соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
19	Установить временной интервал, по истечении которого идет проверка соединения со встречной стороной	**esr:esr(config-bgp-neighbor)# timers keeaplive <TIME>**	<TIME> – время в секундах, принимает значения [1..65535] Значение по умолчанию: 60 секунд
20	Установить временной интервал, по истечении которого встречная сторона считается недоступной	**esr:esr(config-bgp-neighbor)# timers holdtime <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 180 секунд
21	Установить номер автономной системы BGP-соседа	**esr:esr(config-bgp-neighbor)# remote-as <AS>**	<AS> – номер автономной системы, принимает значения [1..4294967295].

22	Разрешить подключение к соседям, которые находятся не в напрямую подключенных подсетях	**esr:esr(config-bgp-neighbor)# ebgp-multihop**	
23	Задать режим, в котором все обновления отправляются BGP-соседу с указанием в качестве next-hop IP-адреса исходящего интерфейса локального маршрутизатора	**esr:esr(config-bgp-neighbor)# next-hop-self**	
24	Задать режим, в котором перед отправлением обновления из BGP атрибута AS Path маршрутов удаляются приватные номера автономных систем (в соответствии с RFC 6996)	**esr:esr(config-bgp-neighbor)# remove-private-as**	
25	Задать режим, в котором BGP-соседу в обновлении на ряду с другими маршрутами отправляется маршрут по умолчанию	**esr:esr(config-bgp-neighbor)# default-originate**	
26	Указать, что BGP-сосед является Route-Reflector клиентом	**esr:esr(config-bgp-neighbor)# route-reflector-client**	
27	Определить приоритетность маршрутов, получаемых от соседа	**esr:esr(config-bgp-neighbor)# preference <VALUE>**	<VALUE> – приоритетность маршрутов соседа, принимает значения в диапазоне [1..255] Значение по умолчанию: 170
28	Определить алгоритм аутентификации с соседом	**esr:esr(config-bgp-neighbor)# authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм шифрования: md5 – пароль шифруется по алгоритму md5.

29	Установить пароль для аутентификации с соседом	**esr: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...).

Пример конфигурации

Задача:

Настроить BGP-протокол на маршрутизаторе со следующими параметрами:

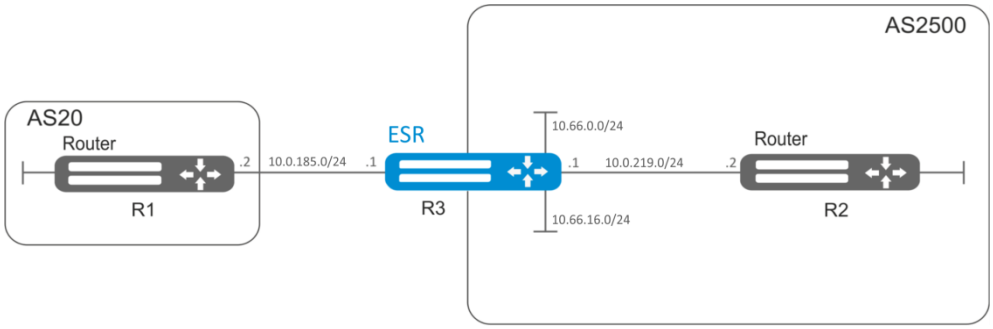


Рисунок 10.19 – Схема сети

– собственные подсети: 10.66.0.0/24, 10.66.16.0/24;
– анонсирование подсетей, подключенных напрямую;
– собственная AS 2500;
– первое соседство - подсеть 10.0.219.0/30, собственный IP-адрес 10.0.219.1, IP-адрес соседа 10.0.219.2, AS 2500;
– второе соседство - подсеть 10.0.185.0/30, собственный IP-адрес 10.0.185.1, IP-адрес соседа 10.0.185.2, AS 20.

Решение:

Сконфигурируем необходимые сетевые параметры:

```
esr:esr# configure
esr:esr(config)# interface gigabitethernet 1/0/1
esr:esr(config-if-gi)# ip address 10.0.185.1/30
esr:esr(config-if-gi)# exit
esr:esr(config)# interface gigabitethernet 1/0/2
esr:esr(config-if-gi)# ip address 10.0.219.1/30
esr:esr(config-if-gi)# exit
esr:esr(config)# interface gigabitethernet 1/0/3
esr:esr(config-if-gi)# ip address 10.66.0.1/24
esr:esr(config-if-gi)# exit
esr:esr(config)# interface gigabitethernet 1/0/4
esr:esr(config-if-gi)# ip address 10.66.16.1/24
esr:esr(config-if-gi)# exit
```

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

процесса:

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

Входим в режим конфигурирования маршрутной информации для IPv4

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

Объявим подсети, подключённые напрямую:

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

Создадим соседства с 10.0.185.2, 10.0.219.2 с указанием автономных систем:

```
esr:esr(config-bgp-af)# neighbor 10.0.185.2
esr:esr(config-bgp-neighbor)# remote-as 20
esr:esr(config-bgp-neighbor)# exit
esr:esr(config-bgp-af)# neighbor 10.0.219.2
esr:esr(config-bgp-neighbor)# remote-as 2500
esr:esr(config-bgp-neighbor)# exit
```

Включим работу протокола:

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

Изменения конфигурации вступят в действие после применения:

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

Информацию о BGP-пирах можно посмотреть командой:

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

Таблицу маршрутов протокола BGP можно просмотреть с помощью команды:

```
esr:esr# show ip bgp
```

Необходимо в firewall разрешить TCP-порт 179.

10.15. Настройка политики маршрутизации PBR

10.15.1. Настройка Route-map для BGP

Route-map могут служить фильтрами, позволяющими обрабатывать маршрутную информацию при её приёме от соседа либо при её 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).

Процесс настройки

Шаг	Описание	Команда	Ключи
1	Создать маршрутную карту, для фильтрации и модификации IP-маршрутов	**esr:esr(config)# route-map <NAME>**	<NAME> – имя маршрутной карты, задаётся строкой до 31 символа
2	Создать правило маршрутной карты	**esr:esr(config-route-map)# rule <ORDER>**	<ORDER> – номер правила, принимает значения [1 .. 10000]
3	Указать действие, которое должно быть применено для маршрутной информации	**esr:esr(config-route-map-rule)# action <ACT>**	<ACT> – назначаемое действие: permit – прием или анонсирование маршрутной информации разрешено; deny – запрещено
4	Задать значение атрибута BGP AS-Path в маршруте, для которого должно срабатывать правило (не обязательно)	**esr:esr(config-route-map-rule)# match as-path [begin | end | contain] <AS-PATH>**	<AS-PATH> – список номеров автономных систем, задаётся в виде AS,AS,AS, принимает значения [1..4294967295]. Опциональные параметры: begin – значение атрибута начинается с указанных номеров AS; end – значение атрибута оканчивается указанными номерами AS; contain – значение атрибута содержит указанный список номеров AS
5	Задать значение атрибута BGP Community, для которого должно срабатывать правило (не обязательно)	**esr:esr(config-route-map-rule)# match community <COMMUNITY-LIST>**	<COMMUNITY-LIST> – список community, задаётся в виде AS:N,AS:N, принимает значения [1..4294967295]. Можно указать до 64 community
6	Задать значение атрибута BGP Extended Community, для которого должно срабатывать правило (не обязательно)	**esr:esr(config-route-map-rule)# match extcommunity <EXTCOMMUNITY-LIST>**	<EXTCOMMUNITY-LIST> – список extcommunity, задаётся 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:esr(config-route-map-rule)# match ip address object-group <OBJ-GROUP- NETWORK -NAME>**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, содержащий префиксы подсетей назначения, задаётся строкой до 31 символа

8	Задать профиль IP-адресов, содержащий значения атрибута BGP Next-Hop в маршруте (не обязательно)	**esr:esr(config-route-map-rule)# match ip next-hop object-group <OBJ-GROUP- NETWORK -NAME>**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, содержащий префиксы подсетей назначения, задаётся строкой до 31 символа
9	Задать профиль, содержащий IP-адреса маршрутизатора, анонсировавшего маршрут (не обязательно)	**esr:esr(config-route-map-rule)# match ip route-source object-group <OBJ-GROUP- NETWORK -NAME>**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, содержащий префиксы подсетей назначения, задаётся строкой до 31 символа
10	Задать значение атрибута BGP MED в маршруте (не обязательно)	**esr:esr(config-route-map-rule)# match metric bgp <METRIC>**	<METRIC> – значение атрибута BGP MED, принимает значения [0..4294967295]
11	Задать значение атрибута BGP AS-Path, которое будет добавляться в начало списка AS-Path (не обязательно)	**esr:esr(config-route-map-rule)# action set as-path prepend <AS-PATH>**	<AS-PATH> – список номеров автономных систем, который будет добавлен к текущему значению в маршруте. Задаётся в виде AS,AS,AS, принимает значения [1..4294967295]
12	Задать значение атрибута BGP Community, которое будет установлено в маршруте (не обязательно)	**esr:esr(config-route-map-rule)# action set community {COMMUNITY-LIST> | no-advertise | no-export }**	<COMMUNITY-LIST> – список community, задаётся в виде AS:N,AS:N, где каждая часть принимает значения [1..65535]; no-advertise – маршруты, передаемые 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
13	Задать атрибута BGP ExtCommunity, которое будет установлено в маршруте (не обязательно)	**esr:esr(config-route-map-rule)# action set extcommunity <EXTCOMMUNITY-LIST>**	<EXTCOMMUNITY-LIST> – список extcommunity, задаётся 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]

14	Задать атрибут BGP Next-Hop, который будет установлен в маршруте при анонсировании (не обязательно)	**esr:esr(config-route-map-rule)# action set ip bgp-next-hop <ADDR>**	<ADDR> – IP-адрес шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]
15	Задаеть значение Next-Hop, которое будет установлено в маршруте, полученном по BGP (не обязательно)	**esr: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 ICMP Destination unreachable (Communication administratively prohibited, code 13)
16	Задать значение атрибута BGP Local Preference, которое будет установлено в маршруте (не обязательно)	**esr:esr(config-route-map-rule)# action set local-preference <PREFERENCE>**	<PREFERENCE> – значение атрибута BGP Local Preference, принимает значения [0..255]
17	Задать значение атрибута BGP Origin, которое будет установлено в маршруте (не обязательно)	**esr: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
18	Задать BGP MED, которое будет установлено в маршруте (не обязательно)	**esr:esr(config-route-map-rule)# action set metric bgp <METRIC>**	<METRIC> – значение атрибута BGP MED, принимает значения [0..4294967295]

19	Добавить фильтрацию и модификацию маршрутов во входящих или исходящих направлениях	**esr:esr(config-bgp-neighbor)# route-map <NAME> <DIRECTION>**	<NAME> – имя сконфигурированной маршрутной карты; <DIRECTION> –направление: in – фильтрация и модификация получаемых маршрутов; out – фильтрация и модификация анонсируемых маршрутов

Пример конфигурации 1

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.

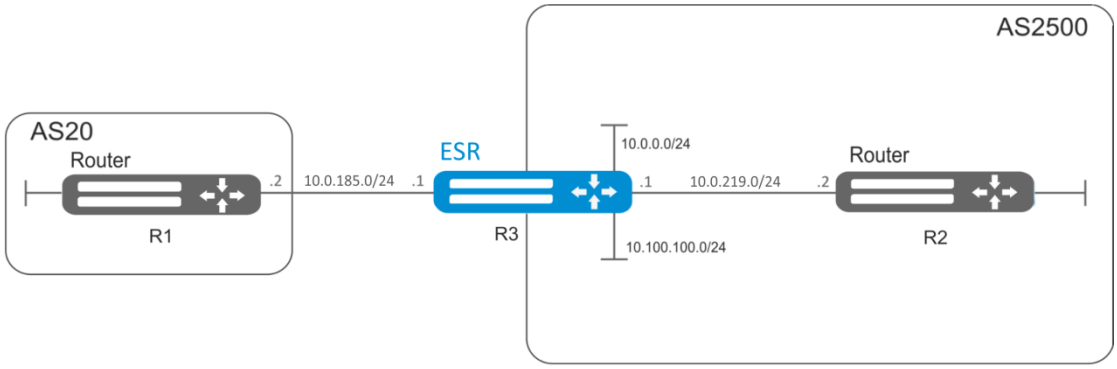


Рисунок 10.20 – Схема сети

Решение:

Создаем политику:

```
esr:esr# configure

esr:esr(config)# route-map from-as20
```

Создаем правило 1:

```
esr:esr(config-route-map)# rule 1
```

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

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

В BGP процессе AS 2500 заходим в настройки параметров соседа:

```
esr:esr(config)# router bgp 2500
esr:esr(config-bgp)# neighbor 10.0.185.2
```

Привязываем политику к принимаемой маршрутной информации:

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

Пример конфигурации 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:esr(config)# route-map to-as20
```

Создаем правило:

```
esr:esr(config-route-map)# rule 1
```

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

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

В BGP процессе AS 2500 заходим в настройки параметров соседа:

```
esr:esr(config)# router bgp 2500
esr:esr(config-bgp)# neighbor 10.0.185.2
```

Привязываем политику к анонсируемой маршрутной информации:

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

Изменения конфигурации вступят в действие после применения:

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

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

Процесс настройки

Шаг	Описание	Команда	Ключи
1	Создать маршрутную карту, для фильтрации и модификации IP-маршрутов	`esr:esr(config)# route-map <NAME>`	<NAME> – имя маршрутной карты, задаётся строкой до 31 символа
2	Создать правило маршрутной карты	`esr:esr(config-route-map)# rule <ORDER>`	<ORDER> – номер правила, принимает значения [1 .. 10000]

3	Указать действие, которое должно быть применено для маршрутной информации	`esr: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: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: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:esr(config-if-gi)# ip policy route-map <NAME>`	<NAME> – имя сконфигурированной политики маршрутизации, строка до 31 символа

Пример конфигурации

Задача:

Распределить трафик между Интернет провайдерами на основе подсетей пользователей.

– Предварительно нужно выполнить следующие действия:

– Назначить IP адреса на интерфейсы.

– Требуется направлять трафик с адресов 10.0.20.0/24 через ISP1 (192.0.2.150), а трафик с адресов 10.0.30.0/24 – через ISP2 (198.51.100.23). Требуется контролировать доступность адресов провайдеров (работоспособность подключений к ISP), и при неработоспособности одного из подключений переводить с него на рабочее подключение весь трафик.

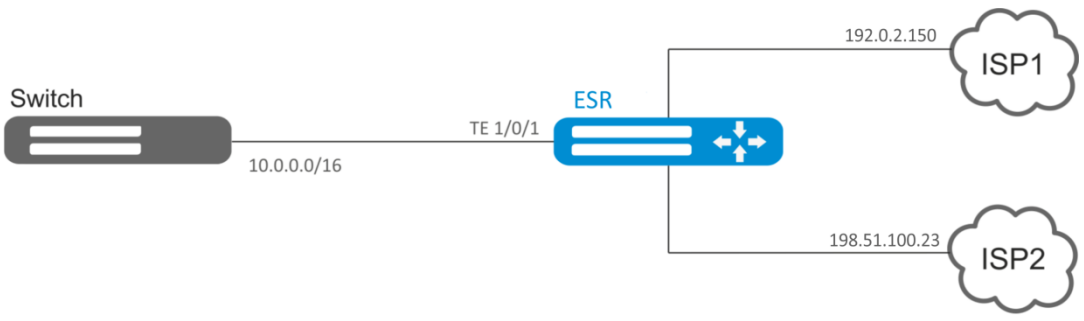


Рисунок 10.21 – Схема сети

Решение:

Создаем ACL:

```
esr:esr# configure
esr:esr(config)# ip access-list extended sub20
```

```
esr:esr(config-acl)# rule 1
esr:esr(config-acl-rule)# match source-address 10.0.20.0 255.255.255.0
esr:esr(config-acl-rule)# match destination-address any
esr:esr(config-acl-rule)# match protocol any
esr:esr(config-acl-rule)# action permit
esr:esr(config-acl-rule)# enable
esr:esr(config-acl-rule)# exit
esr:esr(config-acl)# exit
esr:esr(config)# ip access-list extended sub30
esr:esr(config-acl)# rule 1
esr:esr(config-acl-rule)# match source-address 10.0.30.0 255.255.255.0
esr:esr(config-acl-rule)# match destination-address any
esr:esr(config-acl-rule)# match protocol any
esr:esr(config-acl-rule)# action permit
esr:esr(config-acl-rule)# enable
esr:esr(config-acl-rule)# exit
esr:esr(config-acl)# exit
```

Создаем политику:

```
esr:esr(config)# route-map PBR
```

Создаем правило 1:

```
esr:esr(config-route-map)# rule 1
```

Указываем список доступа (ACL) в качестве фильтра:

```
esr:esr(config-route-map-rule)# match ip access-group sub20
```

Указываем nexthop для sub20:

```
esr:esr(config-route-map-rule)# action set ip next-hop verify-availability 192.0.2.150
10
esr:esr(config-route-map-rule)# action set ip next-hop verify-availability 198.51.100.23
30
esr:esr(config-route-map-rule)# exit
esr:esr(config-route-map)# exit
```

Правилом 1 будет обеспечена маршрутизация трафика с сети 10.0.20.0/24 на адрес 192.0.2.150, а при его недоступности – на адрес 198.51.100.23. Приоритетность шлюзов задается значениями метрик – 10 и 30.

Создаем правило 2:

```
esr:esr(config-route-map)# rule 2
```

Указываем список доступа(ACL) в качестве фильтра:

```
esr:esr(config-route-map-rule)# match ip access-group sub30
```

Указываем nexthop для sub30 и выходим:

```
esr:esr(config-route-map-rule)# action set ip next-hop verify-availability 198.51.100.23
10
esr:esr(config-route-map-rule)# action set ip next-hop verify-availability 192.0.2.150
```

```
30
esr:esr(config-route-map-rule)# exit
esr:esr(config-route-map)# exit
```

Правилом 2 будет обеспечена маршрутизация трафика с сети 10.0.30.0/24 на адрес 198.51.100.23, а при его недоступности – на адрес 192.0.2.150. Приоритетность задается значениями метрик.

Заходим на интерфейс TE 1/0/1:

```
esr:esr(config)# interface tengigabitethernet 1/0/1
```

Привязываем политику на соответствующий интерфейс:

```
esr:esr(config-if-te)# ip policy route-map PBR
```

Изменения конфигурации вступят в действие после применения:

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

10.16. 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.

Процесс 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:esr(config)# tunnel gre <INDEX>`	<INDEX> – идентификатор туннеля в диапазоне: для esr100/200 – [1..250], для esr1000 - [1..500]
3	Указать описание конфигурируемого туннеля (не обязательно)	`esr:esr(config-gre)# description <DESCRIPTION>`	<DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов
4	Установить локальный IP-адрес для установки туннеля	`esr: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]

5	Установить удаленный IP-адрес для установки туннеля	**esr: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]
6	Установить IP-адрес локальной стороны туннеля	**esr: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-ми IP-адресов перечислением через запятую.
7	Указать размер MTU (Maximum Transmition Unit) для туннелей (не обязательно)	**esr:esr(config-gre)# mtu <MTU>**	<MTU> – значение MTU, принимает значения в диапазоне [1280..1500]. Значение по умолчанию: 1500
8	Указать значение времени жизни TTL для туннельных пакетов (не обязательно)	**esr:esr(config-gre)# ttl <TTL>**	<TTL> – значение TTL, принимает значения в диапазоне [1..255]. Значение по умолчанию: Наследуется от инкапсулируемого пакета.
9	Указать DSCP для использования в IP заголовке инкапсулирующего пакета (не обязательно)	**esr:esr(config-gre)# dscp <DSCP>**	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: Наследуется от инкапсулируемого пакета
10	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:esr(config-gre)# key <KEY>**	<KEY> – значение KEY, принимает значения в диапазоне [1..2000000] Значение по умолчанию: Ключ не передаётся
11	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:esr(config-gre)# local checksum**	

12	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:esr(config-gre)# remote checksum`	
13	Активировать туннель	`esr:esr(config-gre)# enable`	

Пример конфигурации

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 198.51.100.1;
– в качестве удаленного шлюза для туннеля используется IP-адрес 192.0.2.10;
– IP-адрес туннеля на локальной стороне 10.0.25.1/24.

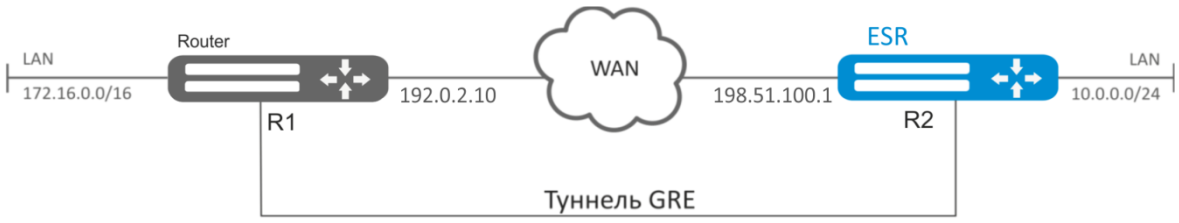


Рисунок 10.22 – Схема сети

Решение:

Создадим туннель GRE 10:

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

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

```
esr:esr(config-gre)# local address 198.51.100.1
esr:esr(config-gre)# remote address 192.0.2.10
```

Укажем IP-адрес туннеля 10.0.25.1/24:

```
esr:esr(config-gre)# ip address 10.0.25.1/24
```

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

Включим туннель**:**

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

На маршрутизаторе должен быть создан маршрут до локальной сети партнера. В качестве интерфейса назначения указываем ранее созданный туннель GRE:

```
esr:esr(config)# ip route 172.16.0.0/16 tunnel gre 10
```

Для применения изменений конфигурации выполним следующие команды:

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

После применения настроек трафик будет инкапсулироваться в туннель и отправляться партеру, 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:esr(config-gre)# local checksum
```

Включить проверку наличия и корректности контрольной суммы GRE для входящего трафика:

```
esr:esr(config-gre)# remote checksum
```

Указать уникальный идентификатор:

```
esr:esr(config-gre)# key 15808
```

Указать значение DSCP, MTU, TTL:

```
esr:esr(config-gre)# dscp 44
esr:esr(config-gre)# mtu 1426
esr:esr(config-gre)# ttl 18
```

Состояние туннеля можно посмотреть командой:

```
esr:esr# show tunnels status gre 10
```

Счетчики входящих и отправленных пакетов можно посмотреть командой:

```
esr:esr# show tunnels counters gre 10
```

Конфигурацию туннеля можно посмотреть командой:

```
esr:esr# show tunnels configuration gre 10
```

Настройка туннеля IPv4-over-IPv4 производится аналогичным образом.

При создании туннеля необходимо в firewall разрешить протокол GRE(47).

10.17. 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.

Процесс 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:esr(config)# tunnel l2tpv3 <INDEX>**	<INDEX> – идентификатор туннеля в диапазоне: для esr100/200 – [1..250], для esr1000 - [1..500]
3	Указать описание конфигурируемого туннеля (не обязательно)	**esr:esr(config-l2tpv3)# description <DESCRIPTION>**	<DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов
4	Установить локальный IP-адрес для установки туннеля	**esr:esr(config-l2tpv3)# local address <ADDR>**	<ADDR> – IP-адрес локального шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]
5	Установить удаленный IP-адрес для установки туннеля	**esr:esr(config-l2tpv3)# remote address <ADDR>**	<ADDR> – IP-адрес локального шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]
6	Выбрать метод инкапсуляции для туннеля L2TPv3	**esr:esr(config-l2tpv3)# protocol <TYPE>**	<TYPE> – тип инкапсуляции, возможные значения: **ip**-инкапсуляция в IP-пакет; **udp**-инкапсуляция в UDP-дейтаграммы
7	Установить локальный идентификатор туннеля	**esr:esr(config-l2tpv3)# local tunnel-id <TUNNEL-ID>**	<TUNNEL-ID> – идентификатор сессии, принимает значения [1..200000].

8	Установить удаленный идентификатор туннеля	**esr:esr(config-l2tpv3)# remote tunnel-id <TUNNEL-ID>**	<TUNNEL-ID> – идентификатор сессии, принимает значения [1..200000].
9	Установить локальный идентификатор сессии	**esr:esr(config-l2tpv3)# local session-id <SESSION-ID>**	<SESSION-ID> – идентификатор сессии, принимает значения [1..200000].
10	Установить удаленный идентификатор сессии	**esr:esr(config-l2tpv3)# remote session-id <SESSION-ID>**	<SESSION-ID> – идентификатор сессии, принимает значения [1..200000].
11	Определить локальный UDP-порт (если в качестве метода инкапсуляции был выбран UDP протокол)	**esr:esr(config-l2tpv3)# local port <UDP>**	<UDP> – номер UDP-порта в диапазоне [1..65535]
12	Определить удаленный UDP-порт (если в качестве метода инкапсуляции был выбран UDP протокол)	**esr:esr(config-l2tpv3)# remote port <UDP>**	<UDP> – номер UDP-порта в диапазоне [1..65535]
13	Активировать туннель	**esr:esr(config-l2tpv3)# enable**	
14	Указать размер MTU (Maximum Transmition Unit) для туннелей (не обязательно)	**esr:esr(config-l2tpv3)# mtu <MTU>**	<MTU> – значение MTU, принимает значения в диапазоне [1280..1500]. Значение по умолчанию: 1500
15	Определить локальное значение cookie для дополнительной проверки соответствия между передаваемыми данными и сессией (не обязательно)	**esr: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:esr(config-l2tpv3)# remote cookie <COOKIE>**	<COOKIE> – значение COOKIE, параметр принимает значения длиной восемь или шестнадцать символов в шестнадцатеричном виде

Пример конфигурации

Задача:

Организовать L2 VPN между офисами компании через IP-сеть, используя для туннелирования трафика протокол L2TPv3.

– в качестве локального шлюза для туннеля используется IP-адрес 198.51.100.1;
– в качестве удаленного шлюза для туннеля используется IP-адрес 192.0.2.10;
– идентификатор туннеля на локальной стороне равен 3, на стороне партнера 3;
– идентификатор сессии внутри туннеля равен 100, на стороне партнера 100;

– в туннель направим трафик из bridge с идентификатором 200.

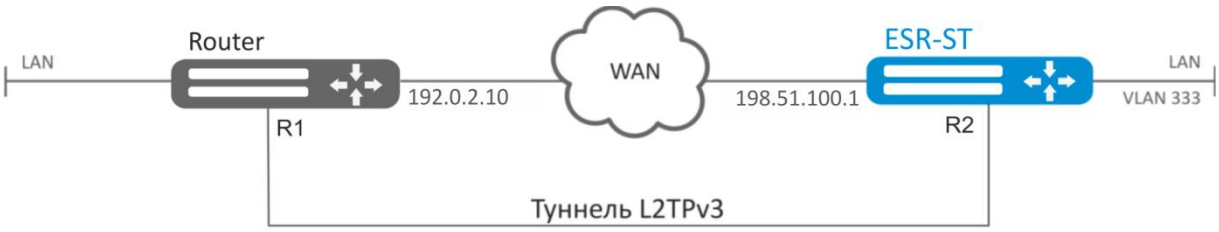


Рисунок 10.23 – Схема сети

Решение:

Создадим туннель L2TPv3 200:

```
esr:esr# configure
esr:esr(config)# tunnel l2tpv3 200
```

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

```
esr:esr(config-l2tpv3)# local address 198.51.100.1
esr:esr(config-l2tpv3)# remote address 192.0.2.10
```

Укажем тип инкапсулирующего протокола:

```
esr:esr(config-l2tpv3)# protocol ip
```

Укажем идентификаторы туннеля для локальной и удаленной сторон:

```
esr:esr(config-l2tpv3)# local tunnel-id 3
esr:esr(config-l2tpv3)# remote tunnel-id 3
```

Укажем идентификаторы сессии внутри туннеля для локальной и удаленной сторон:

```
esr:esr(config-l2tpv3)# local session-id 100
esr:esr(config-l2tpv3)# remote session-id 100
```

Установим принадлежность L2TPv3-туннеля к мосту, который должен быть связан с сетью удаленного офиса (настройка моста рассматривается в пункте 10.10):

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

Включим ранее созданный туннель и выйдем:

```
esr:esr(config-l2tpv3)# enable
esr:esr(config-l2tpv3)# exit
```

Создадим саб-интерфейс для коммутации трафика, поступающего из туннеля, в локальную сеть с тегом VLAN id 333:

```
esr: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 10.10):

```
esr:esr(config-subif)# bridge-group 200
esr:esr(config-subif)# exit
```

Для применения изменений конфигурации выполним следующие команды:

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

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 192.0.2.10. В качестве удаленного шлюза должен использоваться IP-адрес 198.51.100.1. Идентификатор туннеля на локальной стороне должен быть равным 3, на стороне партнера 3. Идентификатор сессии внутри туннеля должен быть равным 200, на стороне партнера 200. Также туннель должен принадлежать мосту, который необходимо соединить с сетью партнера.

Состояние туннеля можно посмотреть командой:

```
esr:esr# show tunnels status l2tpv3 200
```

Счетчики входящих и отправленных пакетов можно посмотреть командой:

```
esr:esr# show tunnels counters l2tpv3 200
```

Конфигурацию туннеля можно посмотреть командой:

```
esr:esr# show tunnels configuration l2tpv3 200
```

Помимо создания туннеля необходимо в firewall разрешить входящий трафик по протоколу L2TP.

10.18. Настройка Dual-Homing [7]

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

Процесс настройки

Шаг	Описание	Команда	Ключи
1	Задать переключение на основной интерфейс при восстановлении связи (не обязательно)	`esr:esr(config)# backup-interface preemption`	
2	Задать количество копий пакетов с одним и тем же MAC-адресом, которые будут отправлены в активный интерфейс при переключении (не обязательно)	`esr:esr(config)# backup-interface mac-duplicate <COUNT>`	<COUNT> – количество копий пакетов, принимает значение [1..4] (по умолчанию 1)

[7] В текущей версии ПО данный функционал поддерживается только на маршрутизаторе ESR-1000

3	Задать количество пакетов в секунду, которое будет отправлено в активный интерфейс при переключении (не обязательно)	`esr:esr(config)# backup-interface mac-per-second <COUNT>`	<COUNT> – количество MAC-адресов в секунду, принимает значение [50..400] (по умолчанию 400)
4	Указать резервный интерфейс, на котором отключен протокол Spanning Tree и включен VLAN Ingress Filtering.	`esr:esr(config)# backup interface <IF> vlan <VID>`	<IF> – интерфейс, { gigabitethernet | port-channel | tengigabitethernet U/S/P} <VID > – указывается в виде {VID | VID,VID-VID}, идентификационный номер VLAN, задаётся в диапазоне [2…4094]

Пример конфигурации

Задача:

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

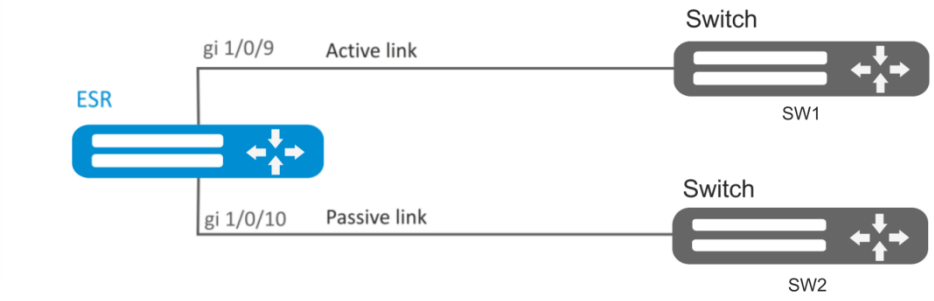


Рисунок 10.24 – Схема сети

Решение:

Предварительно нужно выполнить следующие действия:

Создадим VLAN 50-55:

```
esr-1000(config)# vlan 50-55
```

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

```
esr-1000(config)# interface gigabitethernet 1/0/9-10
esr-1000(config-if-gi)# spanning-tree disable
```

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

```
esr-1000(config-if-gi)# switchport general allowed vlan add 50-55
esr-1000(config-if-gi)# exit
```

Основной этап конфигурирования:

Сделаем интерфейс gigabitethernet 1/0/10 резервным для gigabitethernet 1/0/9:

```
esr-1000(config)# interface gigabitethernet 1/0/9
esr-1000(config-if-gi)# backup interface gigabitethernet 1/0/10 vlan 50-55
```

Изменения конфигурации вступят в действие после применения:

```
esr-1000# commit
Configuration has been successfully committed
esr-1000# confirm
Configuration has been successfully confirmed
```

Просмотреть информацию о резервных интерфейсах можно командой:

```
esr-1000# show interfaces backup
```

10.19. 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.

10.19.1. Базовый QoS

Процесс настройки

Шаг	Описание	Команда	Ключи
1	Включить сервис QoS на интерфейсе/туннеле/сетевом мосту. Если к интерфейсу не привязана политика QoS, то интерфейс работает в режиме Basic QoS.	`esr:esr(config-if-gi)# qos enable`	

2	Установить режим доверия к значениям кодов 802.1p и DSCP во входящих пакетах	**esr: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	**esr: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	**esr: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 Данное соответствие работает на входящие пакеты интерфейса/туннеля/моста, на котором включен QOS	**esr:esr(config)# qos map dscp-queue <DSCP> to <DSCP>**	<DSCP> – классификатор обслуживания в IP-заголовке пакета, принимает значения [0..63].
6	Включить применение изменений кодов DSCP в соответствии с таблицей DSCP-Mutation	**esr:esr(config)# qos dscp mutation**	
7	Установить номер очереди по умолчанию, в которую попадает весь трафик кроме IP в режиме доверия DSCP-приоритетам	**esr:esr(config)# qos queue default <QUEUE>**	<QUEUE> – идентификатор очереди, принимает значения [1..8].
	Задать количество приоритетных очередей. Оставшиеся очереди являются взвешенными	**esr: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 «strict priority» (strict priority – приоритетная очередь обслуживается сразу, как только появляются пакеты).
8	Определить веса для соответствующих взвешенных очередей	**esr:esr(config)# qos wrr-queue <QUEUE> bandwidth <WEIGHT>**	<QUEUE> – идентификатор очереди, принимает значение [1..8]; <WEIGHT> – значение веса, принимает значение [1..255].

9	Установить ограничение скорости исходящего трафика для определенной очереди или интерфейса в целом. Команда актуальна только для Basic QoS режима интерфейса. Ели трафик на входе был класифицирован при помощи расширенного QOS, ограничение не сратотает.	**esr: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
10	Установить ограничение скорости входящего трафика	**esr: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

Пример конфигурации

Задача:

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

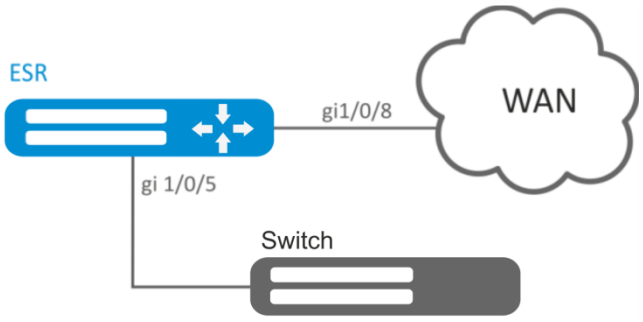


Рисунок 10.25 – Схема сети

Решение:

Для того чтобы восьмая очередь стала приоритетной, а с первой по седьмую взвешенной, ограничим количество приоритетных очередей до 1:

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

Перенаправим трафик с DSCP 22 в восьмую приоритетную очередь:

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

Перенаправим трафик с DSCP 14 в седьмую взвешенную очередь:

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

Включим QoS на входящем интерфейсе со стороны LAN:

```
esr:esr(config)# interface gigabitethernet 1/0/5
esr:esr(config-if-gi)# qos enable
esr:esr(config-if-gi)# exit
```

Включим QoS на интерфейсе со стороны WAN**:**

```
esr:esr(config)# interface gigabitethernet 1/0/8

esr:esr(config-if-gi)# qos enable
```

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

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

Изменения конфигурации вступят в действие после применения:

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

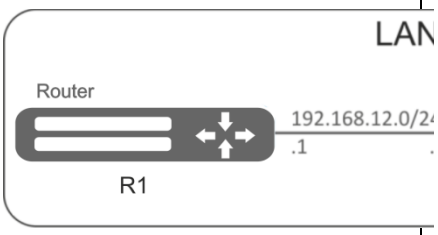
Просмотреть статистику по QoS можно командой:

```
esr:esr# show qos statistics gigabitethernet 1/0/8
```

10.19.2. Расширенный QoS

Процесс настройки

Шаг	Описание	Команда	Ключи

1	Создать списки доступа для определения трафика, к которому должен быть применен расширенный QOS		**См. раздел 0 Пример конфигурации** **Задача:** Разрешить обмен сообщениями по протоколу ICMP между устройствами R1, R2 и маршрутизатором ESR. Разрешить прохождение SSH трафика от R2 к R1, а все попытки установления сессий на 22-й TCP порт с IP-адресов, отличных от IP устройства R2, необходимо логировать и блокировать. Настроить фильтрацию фрагментов из зоны безопасности WAN.  *Рисунок 10.7 – Схема сети* **Решение:** Для каждой сети ESR создадим свою зону безопасности: **esr:esr# configure** **esr:esr(config)# security zone LAN** **esr:esr(config-zone)# exit** **esr:esr(config)# security zone WAN** **esr:esr(config-zone)# exit** Настроим сетевые интерфейсы и определим их принадлежность к зонам безопасности: **esr:esr(config)# interface gi1/0/2** **esr:esr(config-if-gi)# ip address 192.168.12.2/24** **esr:esr(config-if-gi)# security-zone LAN**

2	Создать класс QoS и перехйти в режим настройки параметров класса	**esr:esr(config)# class-map <NAME>**	<NAME> – имя создаваемого класса, задается строкой до 31 символа
3	Задать описание класс QoS	**esr:esr(config-class-map)# description <description>**	<description> - до 255 символов
4	Определить трафик относящегося к конфигурируемому классу по конкретному значению поля DSCP и/или списоку контроля доступа (ACL)	**esr:esr(config-class-map)# match dscp <DSCP>**	<DSCP> – значения поля DSCP пакета, относящегося к конфигурируемому классу
		esr: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)	**esr: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)	**esr: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)	**esr: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:esr(config)# policy-map <NAM** **esr:esr(config-policy-map)#**	<NAME> – имя создаваемой политики, задается строкой до 31 символа.
9	Задать описание политики QoS	**esr:esr(config-policy-map)# description <description>**	<description> - до 255 символов
10	Установить гарантированную полосу пропускания исходящего трафика для политики в целом	**esr: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	**esr:esr(config-policy-map)# shape auto-distribution**	
12	Привязать указанный QoS-класса к политике и осуществить переход в режим настройки параметров класса в рамках политики	**esr:esr(config-policy-map)# class <NAME>** **esr: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	Привязать политика QoS к классу для создания иерархического QoS	**esr: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	**esr: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

15	Установить разделяемую полосу пропускания исходящего трафика для определенного класса. Данную полосу класс может занять, если менее приоритетный класс не занял свою гарантированную полосу.	**esr:esr(config-class-policy-map)# shape peak <BANDWIDTH> [BURST]**	КБайт.
16	Определить режим работы класса	**esr: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	Задаеть приоритет класса в WRR-процессе	**esr: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 Strict Priority и задать приоритет класса.	**esr:esr(config-class-policy-map)# priority level <PRIORITY>**	<PRIORITY> – уровень приоритета в Strict Priority-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	**esr: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	**esr: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)	**esr: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)	**esr:esr(config-class-policy-map)# random-detect precedence <PRECEDENCE> <LIMIT> <MAX> <MIN> <PROBABILITY>**	<PRECEDENCE> – значение IP Precendence [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	**esr:esr(config-class-policy-map)# compression header ip tcp**	
24	Включить сервис QoS на интерфейсе/туннеле/сетевом мосту	**esr: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:esr(config-if-gi)# service-policy { input | output } <NAME>**	<NAME> – имя QoS-политики, задаётся строкой до 31 символа.

Пример конфигурации

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.

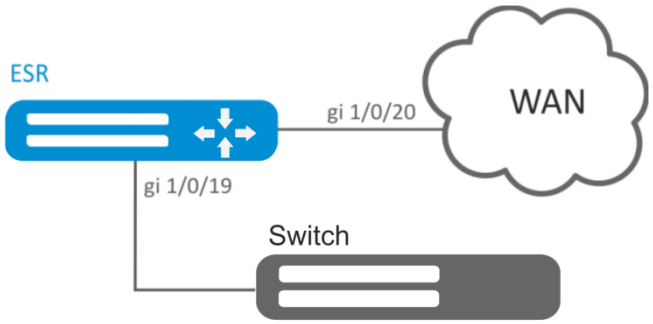


Рисунок 10.26 – Схема сети

Решение:

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

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

```
esr:esr(config-acl-rule)# match destination-address any
esr:esr(config-acl-rule)# enable
esr:esr(config-acl-rule)# exit
esr:esr(config-acl)# exit
```

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

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

Создаём политику и определяем ограничение общей полосы пропускания:

```
esr:esr(config)# policy-map fl
esr:esr(config-policy-map)# shape average 250000
```

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

```
esr:esr(config-policy-map)# class fl1
esr:esr(config-class-policy-map)# shape average 40000
esr:esr(config-class-policy-map)# exit
esr:esr(config-policy-map)# class fl2
esr:esr(config-class-policy-map)# shape average 60000
esr:esr(config-class-policy-map)# exit
```

Для другого трафика настраиваем класс с режимом SFQ:

```
esr:esr(config-policy-map)# class class-default
esr:esr(config-class-policy-map)# mode sfq
esr:esr(config-class-policy-map)# fair-queue 800
esr:esr(config-class-policy-map)# exit
esr: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:esr(config)# interface gigabitethernet 1/0/19
esr:esr(config-if-gi)# qos enable
esr:esr(config-if-gi)# service-policy input fl
esr:esr(config-if-gi)# exit
esr:esr(config)# interface gigabitethernet 1/0/20
esr:esr(config-if-gi)# qos enable
esr:esr(config-if-gi)# service-policy output fl
esr:esr(config-if-gi)# exit
```

Изменения конфигурации вступят в действие после применения:

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

Для просмотра статистики используется команда:

```
esr:esr# do show qos policy statistics gigabitethernet 1/0/20
```

10.20. Настройка зеркалирования [8]

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).

Процесс настройки удаленного зеркалирования

Шаг	Описание	Команда	Ключи
1	Создать VLAN, по которму будет зеркалироваться трафик	`esr:esr(config)# vlan <VID>`	<VID> – идентификатор VLAN, задаётся в диапазоне [1..4095]
2	Указать VLAN, по которому будет передаваться отзеркалированный трафик	`esr(config)# port monitor remote vlan <VID>`	<VID> – идентификатор VLAN, из п.1
3	Задать режим работы L2 интерфейса, на который будет отправляться отзеркалированный трафик	`esr:esr(config-if-gi)# switchport general`	
4	Настроить на итерфейсе VLAN для зеркалирования	`esr:esr(config-if-gi)# switchport general allowed vlan add <VID> tagged`	<VID> – идентификатор VLAN, из п.1
5	Тут же указать интерфейс для зеркалирования	`esr(config-if-gi)# port monitor interface <IF>`	<IF> – имя интерфейса устройства
6	На интерфейсе для зеркалирования включить удаленное зеркалирование	`esr(config-if-gi)# port monitor remote`	

[8] В текущей версии ПО данный функционал поддерживается только на маршрутизаторе ESR-1000

7	Выставить режим порта, передающего отзеркалированный трафик. (не обязательно)	`esr(config)# port monitor mode { network | monitor-only }`	**network** – совмещенный режим передачи данных и зеркалирование (по умолчанию) **monitor-only** – только зеркалирование

Процесс настройки локального зеркалирования

Шаг	Описание	Команда	Ключи
1	На интерфейсе для зеркалирования включить локальное зеркалирование	`esr(config-if-gi)# port monitor interface <IF> [ rx | tx ]`	<IF> – имя интерфейса на который отправлять отзеркалированный трафик. Необязательно: **rx** – зеркалирование только входящего трафика **tx** – зеркалирование только исходящего трафика
2	Выставить режим порта, передающего отзеркалированный трафик. (не обязательно)	`esr(config)# port monitor mode { network | monitor-only }`	**network** – совмещенный режим передачи данных и зеркалирования (по умолчанию) **monitor-only** – только зеркалирование

Пример конфигурации

Задача:

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

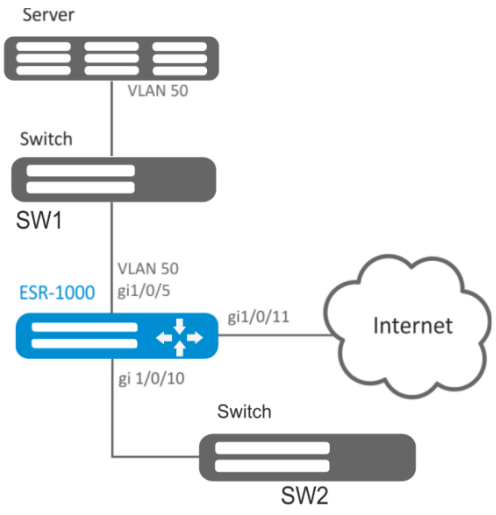


Рисунок 10.27 – Схема сети

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
```

Изменения конфигурации вступят в действие после применения:

```
esr1000# commit
Configuration has been successfully committed
esr1000# confirm
Configuration has been successfully confirmed
```

10.21. 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.

Процесс настройки

Шаг	Описание	Команда	Ключи
1	Задать версию Netflow-протокола	`esr:esr(config)# netflow version <VERSION>`	<VERSION> – версия Netflow-протокола: 5, 9 и 10.
2	Установить максимальное количество наблюдаемых сессий	`esr: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: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: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:esr(config)# netflow enable`	

6	Создать коллектор Netflow и перейти в режим его конфигурирования	`esr: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: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:esr(config-if-gi)# ip netflow export`	

Пример конфигурации

Задача:

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

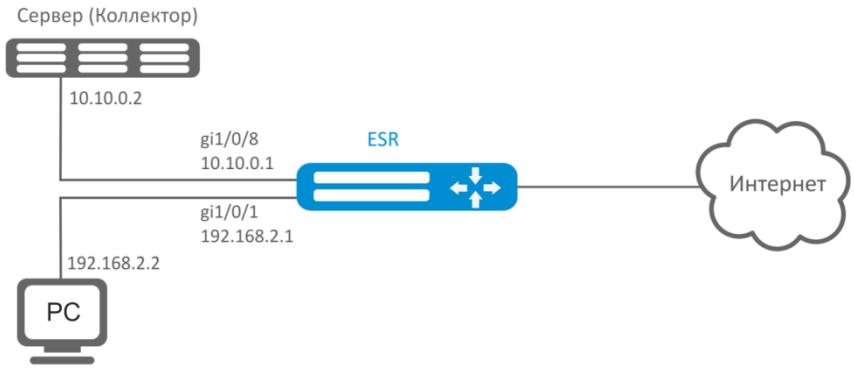


Рисунок 10.28 – Схема сети

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:esr(config)# netflow collector 10.10.0.2
```

Включим сбор экспорта статистики netflow на сетевом интерфейсе gi1/0/1:

```
esr:esr(config)# interface gigabitethernet 1/0/1
esr:esr(config-if-gi)# ip netflow export
```

Активируем netflow на маршрутизаторе:

```
esr:esr(config)# netflow enable
```

Изменения конфигурации вступят в действие после применения:

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

Для просмотра статистики Netflow используется команда:

```
esr:esr# show netflow statistics
```

Настройка Netflow для учета трафика между зонами аналогична настройке sFlow, описание приведено в разделе 10.22 Настройка sFlow.

10.22. Настройка sFlow

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

Процесс настройки

Шаг	Описание	Команда	Ключи
1	Установить частоту отправки пакетов пользовательского трафика в неизменном виде на sFlow-коллектор	`esr:esr(config)# sflow sampling-rate <RATE>`	<RATE> – частота отправки пакетов пользовательского трафика на коллектор, принимает значение [1..10000000]. При значении частоты 10 на коллектор будет отправлен один пакет из десяти. Значение по умолчанию: 1000
2	Установить интервал, по истечении которого происходит получение информации о счетчиках сетевого интерфейса	`esr: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:esr(config)# sflow enable`	
4	Создать коллектор sFlow и перейти в режим его конфигурирования	`esr: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:esr(config-if-gi)# ip sflow export`	

Пример конфигурации

Задача:

Организовать учет трафика между зонами trusted и untrusted.

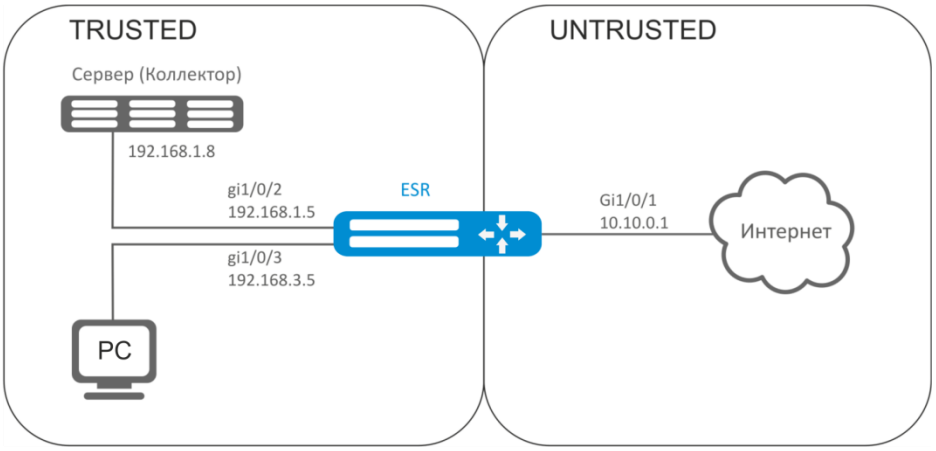


Рисунок 10.29 – Схема сети

Решение:

Для сетей ESR создадим две зоны безопасности:

```
esr:esr# configure

esr:esr(config)# security zone TRUSTED
esr:esr(config-zone)# exit
esr:esr(config)# security zone UNTRUSTED
esr:esr(config-zone)# exit
```

Настроим сетевые интерфейсы и определим их принадлежность к зонам безопасности:

```
esr:esr(config)# interface gi1/0/1
esr:esr(config-if-gi)# security-zone UNTRUSTED
esr:esr(config-if-gi)# ip address 10.10.0.1/24
esr:esr(config-if-gi)# exit
esr:esr(config)# interface gi1/0/2-3
esr:esr(config-if-gi)# security-zone TRUSTED
esr:esr(config-if-gi)# exit
esr:esr(config)# interface gi1/0/2
esr:esr(config-if-gi)# ip address 192.168.1.5/24
esr:esr(config-if-gi)# exit
esr:esr(config)# interface gi1/0/3
esr:esr(config-if-gi)# ip address 192.168.3.5/24
esr:esr(config-if-gi)# exit
```

Укажем IP-адрес коллектора:

```
esr: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:esr(config)# security zone-pair TRUSTED UNTRUSTED
```

```
esr:esr(config-zone-pair)# rule 1
esr:esr(config-zone-pair-rule)# action sflow-sample
esr:esr(config-zone-pair-rule)# match protocol any
esr:esr(config-zone-pair-rule)# match source-address any
esr:esr(config-zone-pair-rule)# match destination-address any
esr:esr(config-zone-pair-rule)# enable
esr:esr(config-zone-pair-rule)# exit
esr:esr(config-zone-pair)# rule 10
esr:esr(config-zone-pair-rule)# action permit
esr:esr(config-zone-pair-rule)# match protocol any
esr:esr(config-zone-pair-rule)# match source-address any
esr:esr(config-zone-pair-rule)# match destination-address any
esr:esr(config-zone-pair-rule)# enable
esr:esr(config-zone-pair-rule)# exit
```

Активируем sFlow на маршрутизаторе:

```
esr:esr(config)# sflow enable
```

Изменения конфигурации вступят в действие после применения:

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

Настройка sFlow для учета трафика с интерфейса осуществляется аналогично *10.21 Настройка Netflow*.

10.23. Настройка LACP

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

Процесс настройки

Шаг	Описание	Команда	Ключи
1	Установить приоритет системы для протокола LACP	`esr: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: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-i**p – 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: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: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: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: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:esr(config-if-gi)# lacp port-priority <PRIORITY>**	<PRIORITY> – приоритет, указывается в диапазоне [1..65535]. Значение по умолчанию: 1

Пример конфигурации

Задача:

Настроить агрегированный канал между маршрутизатором ESR и коммутатором.

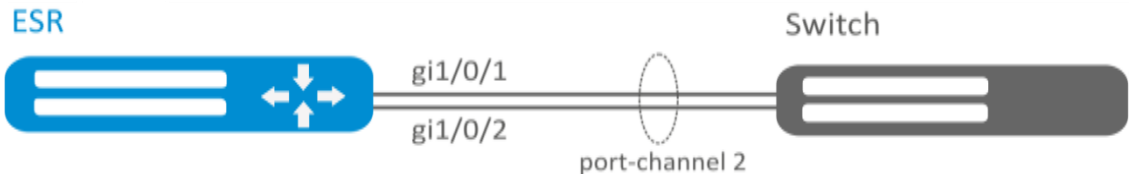


Рисунок 10.30 – Схема сети

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

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

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

Изменения конфигурации вступят в действие после применения:

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

Дальнейшая конфигурация port-channel проводится аналогично с обычным физическим интерфейсом.

10.24. 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.

Процесс настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим конфигурирования интерфейса/туннеля/сетевого моста, для	`esr:esr(config)# interface <IF-TYPE> <IF-NUM>`	<IF-TYPE> – тип интерфейса <IF-NUM> - F/S/P – F-фрейм (1), S – слот (0), P – порт

	которого необходимо настроить протокол VRRP	**esr:esr(config)# tunnel <TUN-TYPE> <TUN-NUM>**	<TUN-TYPE> – тип туннеля <TUN-NUM> – номер туннеля
		esr: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:esr(config-if-gi) # vrrp**	
4	Установить виртуальный IP-адрес VRRP-маршрутизатора	**esr: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.
5	Установить идентификатор VRRP-маршрутизатора	**esr:esr(config-if-gi) # vrrp id <VRID>**	<VRID> – идентификатора VRRP-маршрутизатора, принимает значения [1..255]
6	Установить приоритет VRRP-маршрутизатора	**esr:esr(config-if-gi) # vrrp priority <PR>**	<PR> – приоритет VRRP-маршрутизатора, принимает значения [1..254]. Значение по умолчанию: 100
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:esr(config-if-gi) # vrrp group <GRID>**	<GRID> – идентификатор группы VRRP-маршрутизатора, принимает значения [1..32]

8	Установить IP-адрес, который будет использоваться в качестве IP-адреса отправителя для VRRP-сообщений	**esr: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]
9	Установить интервал между отправкой VRRP-сообщений	**esr:esr(config-if-gi) # vrrp timers advertise <TIME>**	<TIME> – время в секундах, принимает значения [1..40]. Значение по умолчанию: 1 секунда.
10	Установить интервал, по истечении которого происходит отправка Gratuituous ARP сообщения(ий) при переходе маршрутизатора в состояние Master	**esr: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 Gratuituous ARP сообщений, которые будут отправлены при переходе маршрутизатора в состояние Master	**esr: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 Gratuituous ARP сообщения(ий) пока маршрутизатор находится в состоянии Master	**esr: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 Gratuituous ARP сообщений, которые будут отправляться с периодом garp refresh пока маршрутизатор находится в состоянии Master	**esr: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:esr(config-if-gi) # vrrp preemption**	
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:esr(config-if-gi) # vrrp preemption delay <TIME>**	<TIME> – время ожидания, определяется в секундах [1..1000]. Значение по умолчанию: 0
16	Установить пароль для аутентификации с соседом	**esr: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:esr(config-if-gi) # vrrp authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм аутентификации: - cleartext – пароль, передается открытым текстом; - md5 – пароль хешируется по алгоритму md5.

Пример конфигурации 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.

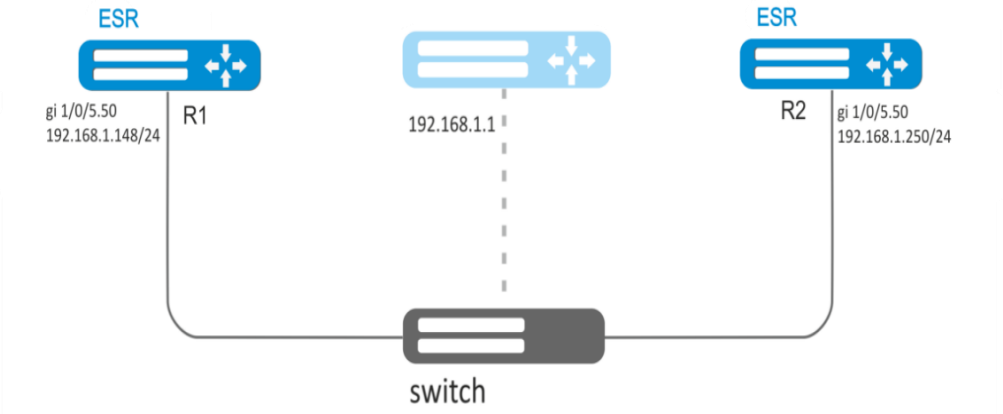


Рисунок 10.31 – Схема сети

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:

```
esr:R1(config)# interface gi 1/0/5.50
esr:R1(config-subif)# vrrp id 10
```

Укажем IP-адрес виртуального шлюза 192.168.1.1/24:

```
esr:R1(config-subif)# vrrp ip 192.168.1.1
```

Включим VRRP**:**

```
esr:R1(config-subif)# vrrp
esr:R1(config-subif)# exit
```

Изменения конфигурации вступят в действие после применения:

```
esr:R1# commit
Configuration has been successfully committed
esr:R1# confirm
Configuration has been successfully confirmed
```

Произвести аналогичные настройки на R2.

Пример конфигурации 2

Задача:

Организовать виртуальные шлюзы для подсети 192.168.20.0/24 в VLAN 50 и подсети 192.168.1.0/24 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.

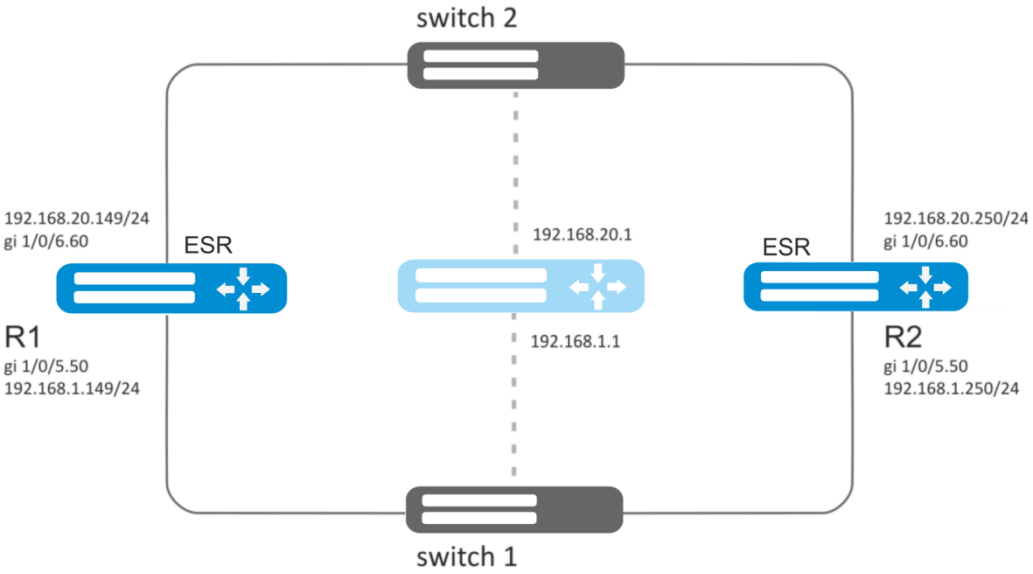


Рисунок 10.32 – Схема сети

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:

```
esr:R1(config-sub)# interface gi 1/0/5.50
esr:R1(config-subif)# vrrp id 10
```

Укажем IP-адрес виртуального шлюза 192.168.1.1:

```
esr:R1(config-subif)# vrrp ip 192.168.1.1
```

Укажем идентификатор VRRP-группы:

```
esr:R1(config-subif)# vrrp group 5
```

Включим VRRP**:**

```
esr:R1(config-subif)# vrrp
esr:R1(config-subif)# exit
```

Настроим VRRP для подсети 192.168.20.0/24 в созданном саб-интерфейсе.

Укажем уникальный идентификатор VRRP:

```
esr:R1(config-sub)# interface gi 1/0/6.60
esr:R1(config-subif)# vrrp id 20
```

Укажем IP-адрес виртуального шлюза 192.168.20.1:

```
esr:R1(config-subif)# vrrp ip 192.168.20.1
```

Укажем идентификатор VRRP-группы:

```
esr:R1(config-subif)# vrrp group 5
```

Включим VRRP**:**

```
esr:R1(config-subif)# vrrp
esr:R1(config-subif)# exit
```

Изменения конфигурации вступят в действие после применения:

```
esr:R1# commit
Configuration has been successfully committed
esr:R1# confirm
Configuration has been successfully confirmed
```

Произвести аналогичные настройки на R2.

Помимо создания туннеля необходимо в firewall разрешить протокол VRRP(112).

10.25. Настройка MultiWAN

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

Процесс настройки

Шаг	Описание	Команда	Ключи
1	Сконфигурировать интерфейсы, по которым будет работать MultiWAN: установить ip адреса и и указать security-zone		
2	Создать правило WAN и перейти в режим настройки параметров правила	`esr:esr(config)# wan load-balance rule <ID>`	<ID> – идентификатор создаваемого правила, принимает значения [1..50].
3	Задать интерфейсы или туннели, которые являются шлюзами в маршруте, создаваемом службой MultiWAN.	`esr: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 с дефолтным значением. В режиме резервирования активным будет маршрут с наибольшим весом. Значение по умолчанию 1

4	Описать правила (необязательно)	**esr:esr(config-wan-rule)# description <DESCRIPTION>**	<DESCRIPTION> – описание правила wan, задаётся строкой до 255 символов
5	Данной командой осуществляется переключение из режима балансировки в режим резервирования (если необходимо)	**esr:esr(config-wan-rule)# failover**	
6	Включить wan правило	**esr:esr(config-wan-rule)# enable**	
7	Создать список IP-адресов для проверки целостности соединения и осуществить переход в режим настройки параметров списка	**esr:esr(config)# wan load-balance target-list <NAME>**	<NAME> – название списка, задается строкой до 31 символа.
8	Задать цель проверки и перейти в режим настройки параметров цели	**esr: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
9	Описать target (необязательно)	**esr:esr(config-wan-target)# description <DESCRIPTION>**	<DESCRIPTION> – описание target, задаётся строкой до 255 символов
10	Указать время ожидания ответа на запрос по протоколу ICMP (необязательно)	**esr:esr(config-wan-target)# resp-time <TIME>**	<TIME> – время ожидания, определяется в секундах [1..30]
11	Указать IP-адрес проверки	**esr: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]
12	Включить проверку цели	**esr:esr(config-wan-target)# enable**	
Комманды для пунктов 13-17 необходимо применить на интерфейсах/туннелях в MultiWAN			
13	Включить WAN режим на интерфейсе для IPv4 стека	**esr1000(config-if-gi)# wan load-balance enable**	

14	Задать количество неудачных попыток проверки соединения, после которых, при отсутствии ответа от встречной стороны, соединение считается неактивным (необязательно)	**esr1000(config-if-gi) # wan load-balance failure-count <VALUE>**	<VALUE> – количество попыток, определяется в диапазоне [1..10] Значение по умолчанию 1
15	Задать количество успешных попыток проверки соединения, после которых, в случае успеха, соединение считается вновь активным (необязательно)	**esr1000(config-if-gi) # wan load-balance success-count <VALUE>**	<VALUE> – количество попыток, определяется в диапазоне [1..10] Значение по умолчанию 1
16	Задать IP-адрес соседа, который будет указан в качестве одного из шлюзов в статическом маршруте, создаваемом службой MultiWAN	**esr1000(config-if-gi) # wan load-balance nexthop { <IP> | dhcp 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
17	Данной командой будут проверяться IP-адреса из списка проверки целостности. В случае недоступности одного из проверяемых узлов, шлюз будет считаться недоступным	**esr: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
18	Прописать статические маршруты через wan (если необходимо)	**esr: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]

Пример конфигурации

Задача:

Настроить маршрут к серверу (203.0.113.1/28) с возможностью балансировки нагрузки.

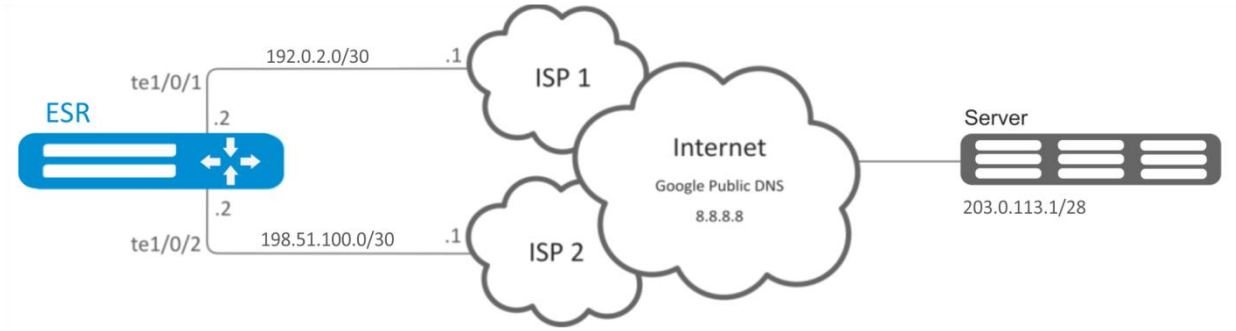


Рисунок 10.33 – Схема сети

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:esr(config)# ip route 203.0.113.0/28 wan load-balance rule 1
```

Создадим правило WAN:

```
esr:esr(config)# wan load-balance rule 1
```

Укажем участвующие интерфейсы:

```
esr:esr(config-wan-rule)# outbound interface tengigabitethernet 1/0/2
esr:esr(config-wan-rule)# outbound interface tengigabitethernet 1/0/1
```

Включим созданное правило балансировки и выйдем из режима конфигурирования правила:

```
esr:esr(config-wan-rule)# enable
esr:esr(config-wan-rule)# exit
```

Создадим список для проверки целостности соединения:

```
esr:esr(config)# wan load-balance target-list google
```

Создадим цель проверки целостности:

```
esr:esr(config-target-list)# target 1
```

Зададим адрес для проверки, включим проверку указанного адреса и выйдем:

```
esr:esr(config-wan-target)# ip address 8.8.8.8
esr:esr(config-wan-target)# enable
esr:esr(config-wan-target)# exit
```

Настроим интерфейсы. В режиме конфигурирования интерфейса te1/0/1 указываем nexthop:

```
esr:esr(config)# interface tengigabitethernet 1/0/1
esr:esr(config-if)# wan load-balance nexthop 192.0.2.1
```

В режиме конфигурирования интерфейса te1/0/1 указываем список целей для

проверки соединения:

```
esr:esr(config-if)# wan load-balance target-list google
```

В режиме конфигурирования интерфейса te1/0/1 включаем WAN-режим и выходим:

```
esr:esr(config-if)# wan load-balance enable
esr:esr(config-if)# exit
```

В режиме конфигурирования интерфейса te1/0/2 указываем nexthop:

```
esr:esr(config)# interface tengigabitethernet 1/0/2
esr:esr(config-if)# wan load-balance nexthop 198.51.100.1
```

В режиме конфигурирования интерфейса te1/0/1 указываем список целей для проверки соединения:

```
esr:esr(config-if)# wan load-balance target-list google
```

В режиме конфигурирования интерфейса te1/0/2 включаем WAN-режим и выходим:

```
esr:esr(config-if)# wan load-balance enable
esr:esr(config-if)# exit
```

Изменения конфигурации вступят в действие после применения:

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

Для переключения в режим резервирования настроим следующее:

Заходим в режим настройки правила WAN:

```
esr: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:esr(config-wan-rule)# failover
```

Изменения конфигурации вступят в действие после применения:

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

10.26. 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.

Процесс настройки

Шаг	Описание	Команда	Ключи
1	включить SNMP-сервер	**esr:esr(config)# snmp-server**	
2	Определить community для доступа по протоколу SNMP v2c	**esr:esr(config)# snmp-server community <COMMUNITY> [<TYPE>] [<ADDR>]**	<COMMUNITY> – сообщество для доступа по протоколу SNMP; <TYPE> – уровень доступа: **ro** – доступ только для чтения; **rw** – доступ для чтения и записи. <ADDR> – IP-адрес клиента, которому предоставлен доступ, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]

3	Включить отправку групп SNMP уведомлений (не обязательно)	**esr:esr(config)# snmp-server enable traps <TRAP-TYPE>**	**<TRAP-TYPE>** - тип трапа, который необходимо включить/отключить. Могут принимать значения: config, config-copy, entity-sensor, entity-sensor threshold, environment, environment cpu-load, environment cpu-temp, environment fan, environment fan-speed, environment low-ram, environment low-space, environment pwrin, environment pwrin-insert, environment pwrin-remove, environment sensor-temp, environment switch-temp – envmon – envmon fan – envmon shutdown – envmon status – envmon supply – envmon temperature – flash – flash insertion – flash removal – license – links – links counters – links status – snmp – snmp authentication – snmp coldstart – snmp linkdown – snmp linkup – syslog –
4	Установить значение кода DSCP для использования в IP-заголовке исходящих пакетов SNMP-сервера (не обязательно)	**esr:esr(config)# snmp-server dscp <DSCP>**	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 63
5	Создать SNMP v3-пользователь	**esr:esr(config)# snmp-server user <NAME>**	<NAME> – имя пользователя, задаётся строкой до 31 символа

6	Определить уровень доступа пользователя по протоколу SNMP v3	**esr:esr(config-user)# access <TYPE>**	<TYPE> – уровень доступа: **ro** – доступ только для чтения; **rw** – доступ для чтения и записи
7	Определить режим безопасности пользователя по протоколу SNMP v3	**esr:esr(config-user)# authentication access <TYPE>**	<TYPE> – режим безопасности: **auth** – используется только аутентификация; **priv** – используется аутентификация и шифрование данных
8	Определить алгоритм аутентификации SNMP v3-запросов	**esr:esr(config-user)# authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм шифрования: **md5** – пароль шифруется по алгоритму md5; **sha1** – пароль шифруется по алгоритму sha1
9	Установить пароль для аутентификации SNMP v3-запросов	**esr:esr(config-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...)
10	Активировать SNMP v3-пользователя	**esr:esr(config-user)# enable**	Значение по умолчанию: Процесс выключен.
11	Определить алгоритм шифрования передаваемых данных	**esr:esr(config-user)# privacy algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм шифрования: **aes128** – использовать алгоритм шифрования AES-128; **des** – использовать алгоритм шифрования DES.
12	Установить пароль для шифрования передаваемых данных	**esr:esr(config-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...).
13	Включить передачу SNMP уведомлений на указанный IP адрес и перейти в режим настройки SNMP уведомлений	**esr:esr(config)# snmp-server host <ADDR>**	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

14	Определить порт коллектора SNMP уведомлений на удаленном сервере (не обязательно)	**esr:esr(config-snmp-host)# port <PORT>**	<PORT> – номер UDP-порта, указывается в диапазоне [1..65535] Значение по умолчанию: 162
15	Определить community которое будет использоваться в отправляемых на snmp хост трапах (не обязательно)	**esr:esr(config-snmp-host)# community <COMMUNITY>**	<COMMUNITY> – текстовый ключ от 1 до 64 символов. Значение по умолчанию: “public”

Пример конфигурации

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 10.34 – 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:esr(config)# snmp-server
```

Создаем пользователя SNMPv3:

```
esr:esr(config)# snmp-server user admin
```

Определим режим безопасности:

```
esr:esr(snmp-user)# authentication access priv
```

Определим алгоритм аутентификации для SNMPv3-запросов:

```
esr:esr(snmp-user)# authentication algorithm md5
```

Установим пароль для аутентификации SNMPv3-запросов:

```
esr:esr(snmp-user)# authentication key ascii-text 123456789
```

Определим алгоритм шифрования передаваемых данных:

```
esr:esr(snmp-user)# privacy algorithm aes128
```

Установим пароль для шифрования передаваемых данных:

```
esr:esr(snmp-user)# privacy key ascii-text 123456789
```

Активируем SNMPv3-пользователя:

```
esr:esr(snmp-user)# enable
```

Определяем сервер-приемник Trap-PDU сообщений:

```
esr:esr(config)# snmp-server host 192.168.52.41
```

Изменения конфигурации вступят в действие после применения:

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

10.27. 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.

Процесс настройки

Шаг	Описание	Команда	Ключи
1	Задать уровень syslog-сообщений, которые будут передаваться SNMP-Traps сообщениями (не обязательно)	`esr: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:esr(config)# syslog monitor <SEVERITY>`	

3	Включить процесс логирования введённых команд пользователя на локальный syslog-сервер (не обязательно)	**esr:esr(config)# syslog cli-commands**	
4	Включить сохранение сообщений syslog заданного уровня важности в указанный файл журнала.	**esr: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: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: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: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 24.2.1; <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:esr(config)#syslog reload debugging**	
9	Включить нумерацию сообщений (не обязательно)	**esr:esr(config)#syslog sequence-numbers**	
10	Включить точность даты сообщений до миллисекунд (не обязательно).	**esr:esr(config)#syslog timestamp msec**	
11	Включить регистрацию неудачных аутентификаций (не обязательно).	**esr:esr(config)#logging login on-failure**	

12	Включить регистрацию изменений настроек системы аудита (не обязательно).	`esr:esr(config)#loggin g syslog configuration`	
13	Включить регистрацию изменений настроек пользователя (не обязательно).	`esr:esr(config)#loggin g userinfo`	

Пример конфигурации

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 10.35 – 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:esr(config)# syslog file ESR info
```

Указываем IP адрес и параметры удаленного Syslog-сервера:

```
esr:esr(config)# syslog host SERVER 192.168.17.30 info udp 514
```

Задаем логирование неудачных попыток аутентификации:

```
esr:esr(config)# logging login on-failure
```

Задаем логирование изменений конфигурации syslog:

```
esr:esr(snmp-user)# logging syslog configuration
```

Задаем логирование старта/остановки системных процессов:

```
esr:esr(snmp-user)# logging service start-stop
```

Задаем логирование внесений изменений в профиль пользователей:

```
esr:esr(snmp-user)# logging userinfo
```

Изменения конфигурации вступят в действие после применения:

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

Посмотреть текущую конфигурацию системного журнала:

```
esr:esr# show syslog configuration
```

Посмотреть записи системного журнала:

```
esr:esr# show syslog ESR
```

10.28. Проверка целостности

Проверка целостности подразумевает проверку целостности хранимых исполняемых файлов.

Процесс настройки

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

Пример конфигурации

Задача:

Проверить целостность файловой системы:

Решение:

Основной этап конфигурирования:

Запускаем проверку целостности:

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