Сервисные маршрутизаторы серии ESR

# ESR-10, ESR-12V, ESR-12VF, ESR-14VF, ESR-20, ESR-21, ESR-100, ESR-200, ESR-1000, ESR-1200, ESR-1500, ESR-1700

Руководство по эксплуатации, Описание функционала (10.2023)

Contents

# 1 Введение

## 1.1 Аннотация

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

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

В данном руководстве изложены описания, алгоритмы и примеры настройки функционала сервисного маршрутизатора серии ESR (далее маршрутизатор или устройство).

## 1.2 Целевая аудитория

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

## 1.3 Примечания и предупреждения

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

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

# 2 Управление интерфейсами



## 2.1 Настройка VLAN

VLAN (Virtual Local Area Network) — логическая («виртуальная») локальная сеть, представляет собой группу устройств, которые взаимодействуют между собой на канальном уровне независимо от их физического местонахождения. Работа VLAN основана на использовании дополнительных полей Ethernet-заголовка согласно стандарту 802.1q. По сути, VLAN изолирует широковещательный домен путем ограничения коммутации Ethernet-фреймов только с одинаковым VLAN-ID в Ethernet-заголовке.

### 2.1.1 Алгоритм настройки

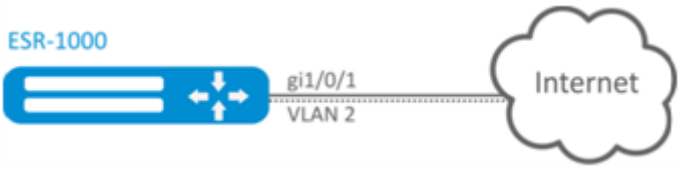
| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Создать VLAN. | `esr(config)# vlan <VID>` | <VID> – идентификатор VLAN, задаётся в диапазоне [2..4094].<br><br>Также есть возможность создания нескольких vlan (через запятую), диапазона vlan (через дефис) или комбинированная запись содержащая запятые и дефисы. |
| 2 | Задать имя vlan (не обязательно). | `esr(config-vlan)# name <vlan-name>` | <vlan-name> – до 255 символов. |
| 3 | Отключить отслеживание состояния интерфейсов, на которых разрешена обработка Ethernet-фреймов данного VLAN (не обязательно). | `esr(config-vlan)# force-up` | |
| 4 | Отключить обработку входящих не тегированных Ethernet-фреймов на основе таблицы коммутации VLAN'a по умолчанию (VLAN-ID – 1) (не обязательно). | `esr(config-if-gi)# no switchport forbidden default-vlan` | |
| 5 | Установить режим работы физического интерфейса в L2-режим. | `esr(config-if-gi)# mode switchport` | |
| 6 | Установить комбинированный режим работы физического интерфейса. | `esr(config-if-gi)# mode hybrid` | Допустимо только для ESR-1000/1200/1500/1700 |
| 7 | Задать режим работы L2 интерфейса. | `esr(config-if-gi)# switchport access` | Только для ESR-10/12V(F)/ 14VF/20/21/100/200. Данный режим является режимом по умолчанию и не отображается в конфигурации. |
| | | `esr(config-if-gi)# switchport trunk` | Только для ESR-10/12V(F)/ 14VF/20/21/100/200. |

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

### 2.1.2 Пример настройки 1. Удаление VLAN с интерфейса

**Задача:**

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




**Решение:**

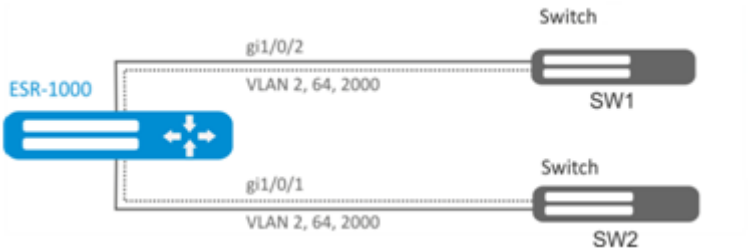
Удалитим VLAN 2 с порта gi1/0/1:

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

### 2.1.3 Пример настройки 2. Разрешение обработки VLAN в тегированном режиме

**Задача:**

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




**Решение:**

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

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

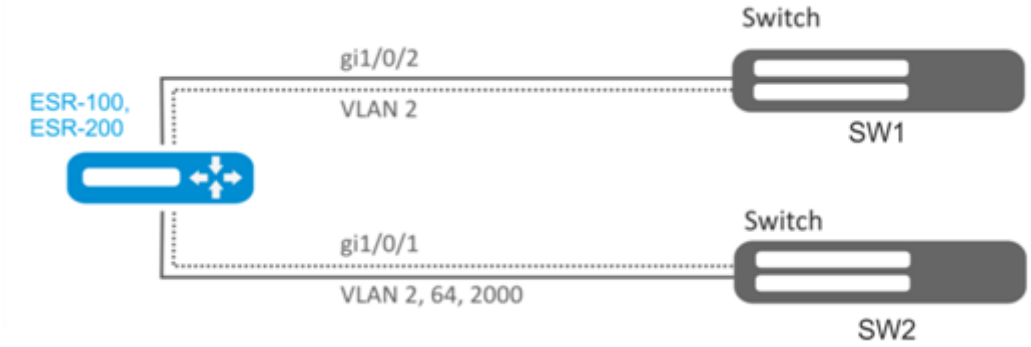
Пропишем VLAN 2, VLAN 64, VLAN 2000 на порт gi1/0/1-2:

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

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

**Задача:**

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




**Решение:**

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

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

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

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

Пропишем VLAN 2 на порт gi1/0/2:

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

## 2.2 Настройка LLDP

Link Layer Discovery Protocol (LLDP) — протокол канального уровня, позволяющий сетевому оборудованию оповещать оборудование, работающее в локальной сети, о своём существовании и передавать ему свои характеристики, а также получать от него аналогичные сведения.

### 2.2.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Активировать LLDP на маршрутизаторе. | `esr(config)# lldp enable` | |
| 2 | Включить прием и обработку LLDPDU на физическом интерфейсе. | `esr(config-if-gi)# lldp receive` | |
| 3 | Включить отправку LLDPDU на физическом интерфейсе. | `esr(config-if-gi)# lldp transmit` | |
| 8 | Установить период отправки LLDPDU (не обязательно). | `esr(config)# lldp timer <SEC>` | <SEC> – период времени в секундах, принимает значение [1..32768].<br>Значение по умолчанию: 30 |
| 4 | Установить период, в течение которого маршрутизатор хранит информацию, полученную по LLDP (не обязательно). | `esr(config)# lldp hold-multiplier <SEC>` | <SEC> – период времени в секундах, принимает значение [1..10].<br>Значение по умолчанию: 4 |
| 5 | Установить IP-адрес, который будет передаваться в LLDP TLV в качестве management-address (не обязательно). | `esr(config)# lldp management-address <ADDR>` | <ADDR> – IP-адрес, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].<br><br>По умолчанию задается один из существующих |
| 6 | Установить поле system-description, которое будет передаваться в LLDP TLV в качестве system-description (не обязательно). | `esr(config)# lldp system-description <DESCRIPTION>` | <DESCRIPION> – описание системы, задаётся строкой до 255 символов.<br><br>По умолчанию содержит информацию о модели и версии ПО маршрутизатора. |
| 7 | Установить поле system-name, которое будет передаваться в LLDP TLV в качестве system-name (не обязательно). | `esr(config)# lldp system-name <NAME>` | <NAME> – имя системы, задается строкой до 255 символов.<br><br>По умолчанию совпадает с заданным hostname |

### 2.2.2 Пример настройки

**Задача:**

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


**Решение:**

1. Конфигурирование R1
   Включим LLDP глобально на маршрутизаторе:

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

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

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

2. Конфигурирование R2
   Включим LLDP глобально на маршрутизаторе:

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

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

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

   Общую информацию по LLDP соседям можно посмотреть командой:

```
esr# show lldp neighbors
```

   Подробную информацию по соседу конкретного интерфейса можно посмотреть командой:

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

   Общую статистику по LLDP можно посмотреть командой:

```
esr# show lldp statistics
```

## 2.3 Настройка LLDP MED

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

### 2.3.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Активировать LLDP на маршрутизаторе | `esr(config)# lldp enable` | |
| 2 | Включить отправку LLDPDU на физическом интерфейсе. | `esr(config-if-gi)# lldp transmit` | |
| 3 | Активировать расширение MED LLDP на маршрутизаторе | `esr(config)# lldp med fast-start enable` | |
| 4 | Создать сетевую политику. | `esr(config)# network-policy <NAME>` | <NAME> – имя network-policy, задается строкой до 31 символа. |
| 5 | Указать тип приложения. | `esr(config-net-policy)# application <APP_TYPE>` | <APP-TYPE> – тип приложения, для которого будет срабатывать network-policy.<br>Принимает значения:<br>• voice;<br>• voice-signaling;<br>• guest-voice;<br>• guest-voice-signaling;<br>• softphone-voice;<br>• video-conferencing;<br>• streaming-video;<br>• video-signaling. |
| 6 | Установить значение DSCP (не обязательно). | `esr(config-net-policy)# dscp <DSCP>` | <DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. |
| 7 | Установить значение COS (не обязательно). | `esr(config-net-policy)# priority  <PRIORITY>` | <COS> – значение приоритета, принимает значения:<br>• best-effort – COS0;<br>• background – COS1;<br>• excellent-effort – COS2;<br>• critical-applications – COS3;<br>• video – COS4;<br>• voice – COS5;<br>• internetwork-control – COS6;<br>• network-control – COS7. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 8 | Установить значение VLAN ID. | `esr(config-net-policy)# vlan <VID> [tagged]` | <VID> – идентификационный номер VLAN, принимает значения [1...4094];<br>• **tagged** – ключ, при установке которого абонентское устройство будет отправлять Ethernet-фреймы указанного приложения в тегированном виде. |
| 9 | Установить сетевую политику на интерфейс. | `esr(config-if-gi)# lldp network-policy <NAME>` | <NAME> – имя network-policy, задается строкой до 31 символа. |

### 2.3.2 Пример настройки Voice VLAN

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

**Задача:**

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


**Решение:**

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

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

Включим LLDP и поддержку MED в LLDP глобально на маршрутизаторе:

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

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

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

Настроим LLDP на интерфейсе и установим на него сетевую политику:

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

## 2.4 Настройка терминации на саб-интерфейсе

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

### 2.4.1 Алгоритм настройки

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

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 2 | Задать описание саб-интерфейса (не обязательно). | `esr(config-subif)# description <DESCRIPTION>` | <DESCRIPTION> – описание интерфейса, задаётся строкой до 255 символов. |
| 3 | Указать экземпляр VRF, в котором будет работать данный саб-интерфейс (не обязательно). | `esr(config-subif)# ip vrf forwarding <VRF>` | <VRF> – имя VRF, задается строкой до 31 символа. |
| 4 | Указать IPv4/IPv6-адрес и маску подсети для конфигурируемого интерфейса или включить получение IP-адреса динамически. | `esr(config-subif)# ip address <ADDR/LEN>` | <ADDR/LEN> – IP-адрес и длина маски подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].<br>Дополнительные функции IPv4-адресации см. в разделе Настройка IP-адресации. |
| | | `esr(config-subif)# ipv6 address <IPV6-ADDR/LEN>` | <IPV6-ADDR/LEN> – IP-адрес и префикс подсети, задаётся в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128].<br>Дополнительные функции IPv6-адресации см. в разделе Настройка IPv6-адресации.<br><br>Можно указать несколько UIPv4/IPv6-адресов перечислением через запятую. Может быть назначено до 8 IPv4/IPv6-адресов на интерфейс. |
| | | `esr(config-subif)# ip address dhcp` | Дополнительные функции при работе DHCP-клиента см. в разделе Управление DHCP-клиентом. |
| 5 | Отключить на интерфейсе функции Firewall или включить интерфейс в зону безопасности (см. раздел Конфигурирование Firewall). | `esr(config-subif)# ip firewall disable` | |
| | | `esr(config-subif)# security-zone <NAME>` | <NAME> – имя зоны безопасности, задаётся строкой до 31 символа. |

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

Также для саб-интерфейса возможно настроить:

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

### 2.4.2 Пример настройки саб-интерфейса

**Задача:**

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

**Решение:**

Создадим саб-интерфейс для VLAN: 828

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

Настроим IP-адрес из необходимой подсети:

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

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

## 2.5 Настройка терминации на Q-in-Q интерфейсе

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

### 2.5.1 Алгоритм настройки

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

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

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| | | `esr(config-qinq-if)# ipv6 address <IPV6-ADDR/LEN>` | <IPV6-ADDR/LEN> – IP-адрес и префикс подсети, задаётся в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128].<br><br>Дополнительные функции IPv6-адресации см. в разделе Настройка IPv6-адресации.<br><br>Можно указать несколько UIPv4/IPv6-адресов перечислением через запятую. Может быть назначено до 8 IPv4/IPv6-адресов на интерфейс. |
| | | `esr(config-qinq-if)# ip address dhcp` | Дополнительные функции при работе DHCP-клиента см. в разделе Управление DHCP-клиентом. |
| 6 | Отключить на интерфейсе функции Firewall или включить интерфейс в зону безопасности (см. раздел Конфигурирование Firewall). | `esr(config-qinq-if)# ip firewall disable` | |
| | | `esr(config-qinq-if)# security-zone <NAME>` | <NAME> – имя зоны безопасности, задаётся строкой до 31 символа. |
| 7 | Установить интервал времени, в течение которого собирается статистика о нагрузке на саб-интерфейс (не обязательно). | `esr(config-subif)# load-average <TIME>` | <TIME> – интервал в секундах, принимает значения [5..150]. |
| 8 | Установить время жизни IPv4/IPv6 записей в ARP-таблице, изученных на данном интерфейсе (не обязательно). | `esr(config-subif)# ip arp reachable-time <TIME>`<br><br>или<br><br>`esr(config-subif)# ipv6 nd reachable-time <TIME>` | <TIME> – время жизни динамических MAC-адресов, в миллисекундах.<br>Допустимые значения от 5000 до 100000000 миллисекунд.<br>Реальное время обновления записи варьируется от [0,5;1,5]*<TIME>. |
| 9 | Изменить размер MTU (MaximumTransmitionUnit).<br>MTU более 1500 будет активно только если применена команда "system jumbo-frames"<br>(не обязательно). | `esr(config-subif)# mtu <MTU>` | <MTU> – значение MTU в байтах.<br>Значение по умолчанию: 1500. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 10 | Включить запись статистики использования текущего интерфейса (не обязательно). | `esr(config-subif)# history statistics` | |
| 11 | Переопределить значение поля MSS (Maximum segment size) во входящих TCP-пакетах (не обязательно). | `esr(config-subif)# ip tcp adjust-mss <MSS>`<br>`esr(config-subif)# ipv6 tcp adjust-mss <MSS>` | <MSS> – значение MSS, принимает значения в диапазоне [500..1460]. Значение по умолчанию: 1460 |
| Также для qinq-интерфейса возможно настроить:<br>• QoS в базовом или расширенном режимах (см. раздел Управление QoS);<br>• proxy (см. раздел Проксирование HTTP/HTTPS-трафика);<br>• мониторинг траффика (см. разделы Настройка Netflow и Настройка sFlow);<br>• функционал протоколов маршрутизации (см. раздел Управление маршрутизацией);<br>• протокол VRRF (см. раздел Управление резервированием);<br>• функционал BRAS (см. раздел Управление BRAS (Broadband Remote Access Server));<br>• функционал IDS/IPS (см. раздел Настройка IPS/IDS). | | | |

### 2.5.2 Пример настройки Q-in-Q интерфейса

**Задача:**

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

**Решение:**

Создадим саб-интерфейс для S-VLAN: 828

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

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

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

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

## 2.6 Настройка USB модемов

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

### 2.6.1 Алгоритм настройки USB-модемов

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | После подключения USB-модема дождаться, когда система обнаружит подключенное устройство. | | |
| 2 | Определить, какой номер устройства назначен на подключенный USB-модем. | `esr# show cellulars status modem` | В поле "USB port" будет указан идентификатор подключенного устройства. |
| 3 | Создать профиль настроек для USB-модема и перейти в режим конфигурирования профиля. | `esr(config)# cellular profile <ID>` | <ID> – идентификатор профиля настроек для USB-модема в системе [1..10]. |
| 4 | Задать описание профиля настроек (не обязательно). | `esr(config-cellular-profile)# description <DESCRIPTION>` | <DESCRIPTION> – описание профиля, задаётся строкой до 255 символов. |
| 5 | Задать точку доступа мобильной сети | `esr(config-cellular-profile)# apn <NAME>` | <NAME> – точка доступа мобильной сети, задаётся строкой до 31 символа. |
| 6 | Задать имя пользователя мобильной сети (если мобильный оператор требует аутентификации по логину/паролю). | `esr(config-cellular-profile)# user <NAME>` | <NAME> – имя пользователя, задаётся строкой до 31 символа. |
| 7 | Установить пароля для пользователя мобильной сети (если мобильный оператор требует аутентификации по логину/паролю). | `esr(config-user)# password ascii-text { <CLEAR-TEXT> \| encrypted <ENCRYPTED-TEXT> }` | <CLEAR-TEXT> – пароль в открытой форме, задаётся строкой [1 .. 64] символов, может включать символы [0-9a-fA-F];<br><br><ENCRYPTED-TEXT> – пароль в зашифрованной форме, задаётся строкой [2..128] символов. |
| 8 | Активировать пользователя (если мобильный оператор требует аутентификации по логину/паролю). | `esr(config-user)# enable` | |
| 9 | Установить номер дозвона для подключения к мобильной сети. | `esr(config-cellular-profile)# number <WORD>` | <WORD> – номер дозвона для подключения к мобильной сети, задаётся строкой до 15 символов. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 10 | Задать метод аутентификации пользователя в мобильной сети (не обязательно). | `esr(config-cellular-profile)# allowed-auth <TYPE>` | <TYPE> – метод аутентификации пользователя в мобильной сети [none, PAP, CHAP, MSCHAP, MSCHAPv2, EAP]. Значение по умолчанию: PAP |
| 11 | Ограничить возможность использования семейств IP-адресов в мобильной сети. | `esr(config-cellular-profile)# ip-version { ipv4 \| ipv6 }` | • **ipv4** – семейство IPv4;<br>• **ipv6** – семейство IPv6; |
| 12 | Создать USB-модем в конфигурации маршрутизатора и перейти в режим конфигурирования модема. | `esr(config)# cellular modem <ID>` | <ID> – идентификатор USB-модема в системе [1..10]. |
| 13 | Задать описание модема (не обязательно). | `esr(config-cellular-modem)# description <DESCRIPTION>` | <DESCRIPTION> – описание модема, задаётся строкой до 255 символов. |
| 14 | Указать экземпляр VRF, в котором будет работать данный модем (не обязательно). | `esr(config-cellular-modem)# ip vrf forwarding <VRF>` | <VRF> – имя VRF, задается строкой до 31 символа. |
| 15 | Задать идентификатор USB-модема, назначенного системой (определен в пункте 2). | `esr(config-cellular-modem)# device <WORD>` | <WORD> – идентификатор USB-порта подключенного модема [1..12]. |
| 16 | Назначить ранее созданный профиль настроек для USB-модема. | `esr(config-cellular-modem)# profile <ID>` | <ID> – идентификатор профиля настроек для USB-модема в системе [1..10]. |
| 17 | Задать код разблокировки SIM-карты (в случае необходимости). | `esr(config-cellular-modem)# pin <WORD>` | <WORD> – код разблокировки SIM-карты [4..8]. Возможно использование только цифр. |
| 18 | Разрешить использование того или иного режима работы USB-модема (не обязательно). | `esr(config-cellular-modem)# allowed-mode <MODE>` | <MODE> – допустимый режим работы USB-модема [2g, 3g, 4g].<br><br>По умолчанию: разрешены все режимы, поддерживаемые модемом. |
| 19 | Задать размер максимального принимаемого пакета (не обязательно). | `esr(config-cellular-modem)# mru { <MRU> }` | <MRU> – значение MRU, принимает значения в диапазоне [128..16383]. Значение по умолчанию: 1500. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 20 | Изменить максимальный размер обрабатываемых пакетов MTU (MaximumTransmitionUnit). MTU более 1500 будет активно только если применена команда "system jumbo-frames" (не обязательно). | `esr(config-cellular-modem)# mtu <MTU>` | <MTU> – значение MTU в байтах. Значение по умолчанию: 1500. |
| 21 | Задать предпочтительный режим работы USB-модема в мобильной сети (не обязательно). | `esr(config-cellular-modem)# preferred-mode { <MODE> }` | <MODE> – предпочтительный режим работы USB-модема [2g, 3g, 4g] |
| 22 | Отключить на интерфейсе функции Firewall или включить интерфейс в зону безопасности (см. раздел Конфигурирование Firewall). | `esr(config-subif)# ip firewall disable` | |
| | | `esr(config-subif)# security-zone <NAME>` | <NAME>-имя зоны безопасности, задаётся строкой до 31 символа. |
| 23 | Активировать USB-модем. | `esr(config-cellular-modem)# enable` | |

Также для модема сотовой сети возможно настроить:

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

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

### 2.6.2 Пример настройки

**Задача:**

Настроить подключение к сети Интернет, используя USB-модем.

**Решение:**

Для примера разберём подключение к сотовому оператору МТС.

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

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

Создадим профиль настроек для USB-модема:

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

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

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

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

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

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

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

Назначим соответствующий профиль настроек и активируем модем:

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

## 2.7 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.

### 2.7.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Перевести физический интерфейс в режим коммутации | `esr(config-if-gi)# mode switchport` | |
| 2 | Задать режим работы интерфейса e1 | `esr(config-if-gi)# switchport mode e1` | |
| 3 | Задать источник синхронизации | `esr(config-if-gi)# switchport e1 clock source <SOURCE>` | <SOURCE> – источник синхронизации:<br>• **Internal** (по умолчанию) – синхронизироваться с внутренним источником;<br>• **line** – синхронизироваться с линейным сигналом. |
| 4 | Указать размер MTU (Maximum Transmition Unit) для физических интерфейсов | `esr(config-if-gi)# mtu <MTU>` | <MTU> – значение MTU, для E1 и Multilink интерфейсов принимает значения в диапазоне [128..1500]. |
| 5 | Задать хэш-алгоритм проверки кадра (не обязательно) | `esr(config-if-gi)# switchport e1 crc <FCS>` | <FCS> – последовательность проверки кадра:<br>• **16** (по умолчанию) – FCS16;<br>• **32** – FCS32. |
| 6 | Задать проверку на наличие ошибок при передаче (не обязательно) | `esr(config-if-gi)# switchport e1 framing <CRC>` | <CRC> – проверка циклической избыточности:<br>• **crc-4** – использовать алгоритм CRC-4;<br>• **no-crc4** (по умолчанию) – не использовать проверку. |
| 7 | Задать инвертацию передаваемых бит (не обязательно) | `esr(config-if-gi)# switchport e1 invert data` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 8 | Задать тип линейного кодирования (не обязательно) | `esr(config-if-gi)# switchport e1 linecode <CODE>` | <CODE> – тип линейного кодирования;<br>• **ami** – чередующейся полярностью импульсов;<br>• **hdb3** (по умолчанию) – двухполярный код высокой плотности порядка 3. |
| 9 | Задать количество тайм слотов | `esr(config-if-gi)# switchport e1 timeslots <RANGE>` | <RANGE> – количество тайм-слотов |
| 10 | Использовать E1 как единую сущность, без таймслотов (не обязательно) | `esr(config-if-gi)# switchport e1 unframed` | |
| 11 | Конфигурируем E1 | `esr(config)# interface e1 1/<SLOT>/1` | <SLOT> – номер слота. |
| 12 | Включаем CHAP-аутентификацию для PPP (не обязательно) | `esr(config-e1)# ppp authentication chap` | |
| 13 | Задается имя маршрутизатора, которое отправляется удаленной стороне для прохождения CHAP-аутентификации (не обязательно) | `esr(config-e1)# ppp chap hostname <NAME>` | <NAME> – имя маршрутизатора |
| 14 | Задать пароль для аутентификации (не обязательно) | `esr(config-e1)# ppp chap password ascii-text <CLEAR-TEXT>` | <CLEAR-TEXT> – пароль в открытой форме, задаётся строкой [1 .. 64] символов, может включать символы [0-9a-fA-F] |
| 15 | Включить игнорирование аутентификации (не обязательно) | `esr(config-e1)# ppp chap refuse` | |
| 16 | Задать имя пользователя для аутентификации (не обязательно) | `esr(config-e1)# ppp chap username <NAME>` | <NAME> – имя пользователя |
| 17 | Разрешается принимать от соседа любой ненулевой IP-адрес в качестве локального IP-адреса (не обязательно) | `esr(config-e1)# ppp ipcp accept-address` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 18 | Задать IP-адрес, который отправляется удаленной стороне для последующего его присвоения (не обязательно) | `esr(config-e1)# ppp ipcp remote-address <ADDR>` | <ADDR> – IP-адрес удаленного шлюза |
| 19 | Задать количество попыток отправки Configure-Request пакетов, прежде чем удаленный пир будет признан неспособным ответить (не обязательно) | `esr(config-e1)# ppp max-configure <VALUE>` | <VALUE> – количество попыток |
| 20 | Задать количество попыток отправки Configure-NAK пакетов, прежде чем будут подтверждены все опции (не обязательно) | `esr(config-e1)# ppp max-failure <VALUE>` | <VALUE> – количество попыток |
| 21 | Задать количество попыток отправки Terminate-Request пакетов, прежде чем сессия будет прервана (не обязательно) | `esr(config-e1)# ppp max-terminate <VALUE>` | <VALUE> – количество попыток |
| 22 | Задать размер MRU (Maximum Receive Unit) для интерфейса (не обязательно) | `esr(config-e1)# ppp mru <MRU>` | <MRU> – значение MRU |
| 23 | Включение режима MLPPP (не обязательно) | `esr(config-e1)# ppp multilink` | |
| 24 | Добавить в MLPPP группу (не обязательно) | `esr(config-e1)# ppp multilink-group  <GROUP-ID>` | <GROUP-ID> – номер группы |
| 25 | Задается интервал времени в секундах, по истечении которого маршрутизатор отправляет keepalive-сообщение (не обязательно) | `esr(config-e1)# ppp timeout keepalive <TIME>` | <TIME> – время в секундах |
| 26 | Задается интервал, по истечении которого маршрутизатор повторяет запрос на установление сессии (не обязательно) | `esr(config-e1)# ppp timeout retry <TIME>` | <TIME> – время в секундах |

### 2.7.2 Пример конфигурации

**Задача:**

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


**Решение:**

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

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

Включим interface e1 1/3/1:

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

Изменения конфигурации вступят в действие по следующим командам:

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

## 2.8 Настройка MLPPP

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

### 2.8.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Настроить группу агрегации. | `esr(config)# interface multilink <IF>` | <IF> – наименование интерфейса. |
| 2 | Указать описание конфигурируемой группы агрегации (не обязательно). | `esr(config- multilink )# description <DESCRIPTION>` | <DESCRIPTION> – описание группы агрегации, задаётся строкой до 255 символов. |
| 3 | Задать интервал времени, за который усредняется статистика о нагрузке на группе агрегации (не обязательно). | `esr(config- multilink )# load-average <TIME>` | <TIME> – интервал в секундах, принимает значения [5..150].<br><br>Значение по умолчанию: 5. |
| 4 | Указать размер MTU (Maximum Transmition Unit) для группы агрегации (не обязательно). MTU более 1500 будет активно только в случае применения команды "system jumbo-frames". | `esr(config- multilink )# mtu <MTU>` | <MTU> – значение MTU, принимает значения в диапазоне [1280..1500].<br><br>Значение по умолчанию: 1500. |
| 5 | Включить CHAP-аутентификацию. | `esr(config-multilink)# ppp authentication chap` | |
| 6 | Включить игнорирование аутентификации (не обязательно). | `esr(config-multilink)# ppp chap refuse` | |
| 7 | Указать имя маршрутизатора, которое отправляется удаленной стороне для прохождения CHAP-аутентификации. | `esr(config-multilink)# ppp chap hostname <NAME>` | <NAME> – имя маршрутизатора, задаётся строкой до 31 символа |
| 8 | Указать пароль, который отправляется удаленной стороне вместе с именем маршрутизатора для прохождения CHAP-аутентификации. | `esr(config-multilink)# ppp chap password ascii-text { <CLEAR-TEXT> \| encrypted <ENCRYPTED-TEXT> }` | <CLEAR-TEXT> – пароль в открытой форме, задаётся строкой [8 .. 64] символов, может включать символы [0-9a-fA-F].<br><br><ENCRYPTED-TEXT> – пароль в зашифрованной форме, задаётся строкой [16..128] символов. |
| 9 | Разрешить принимать от соседа любой ненулевой IP-адрес в качестве локального IP-адреса (не обязательно). | `esr(config-multilink)# ppp ipcp accept-address` | |
| 10 | Установить IP-адрес, который отправляется удаленной стороне для последующего его присвоения. | `esr(config-multilink)# ppp iccp remote-address <ADDR>` | <ADDR> – IP-адрес удаленного шлюза. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 11 | Указать пользователя для аутентификации удаленной стороны и перейти в режим конфигурирования указанного пользователя. | `esr(config-multilink)# chap username <NAME>` | <NAME> – имя пользователя, задаётся строкой до 31 символа. |
| 12 | Установить пароль в открытой или зашифрованной форме определенному пользователю для аутентификации удаленной стороны. | `esr(config-ppp-user)# password ascii-text { <CLEAR-TEXT> \| encrypted <ENCRYPTED-TEXT> }` | <CLEAR-TEXT> – пароль в открытой форме, задаётся строкой [8 .. 64] символов, может включать символы [0-9a-fA-F].<br><br><ENCRYPTED-TEXT> – пароль в зашифрованной форме, задаётся строкой [16..128] символов. |
| 13 | Установить количество попыток отправки Configure-Request пакетов, прежде чем удаленный пир будет признан неспособным ответить (не обязательно). | `esr(config-multilink)# ppp max-configure <VALUE>` | <VALUE> – время в секундах, принимает значения [1..255].<br><br>Значение по умолчанию: 10. |
| 14 | Установить количество попыток выслать Configure-NAK пакеты, прежде чем будут подтверждены все опции (не обязательно). | `esr(config-multilink)# ppp max-failure <VALUE>` | <VALUE> – время в секундах, принимает значения [1..255]. |
| 15 | Установить количество попыток выслать Terminate-Request пакеты, прежде чем сессия будет прервана (не обязательно). | `esr(config-multilink)# ppp max-terminate <VALUE>` | <VALUE> – время в секундах, принимает значения [1..255].<br><br>Значение по умолчанию: 2. |
| 16 | Указать размер MRU (Maximum Receive Unit) для интерфейса. | `esr(config-multilink)# ppp mru <MRU>` | <MRU> – значение MRU, принимает значения в диапазоне [128..1485].<br><br>Значение по умолчанию: 1500. |
| 17 | Указать интервал времени в секундах, по истечении которого маршрутизатор отправляет keepalive-сообщение (не обязательно). | `esr(config-multilink)# ppp timeout keepalive <TIME>` | <TIME> – время в секундах, принимает значения [1..32767].<br><br>Значение по умолчанию: 10. |
| 18 | Установить интервал времени в секундах, по истечении которого маршрутизатор повторяет запрос на установление сессии (не обязательно). | `esr(config-multilink)# ppp timeout retry <TIME>` | <TIME> – время в секундах, принимает значения [1..255].<br><br>Значение по умолчанию: 3. |
| 19 | Определить максимальный размер пакета для MLPP интерфейса. | `esr(config-multilink)# mrru <MRRU>` | <MRRU> – максимальный размер принимаемого пакета для MLPP интерфейса, принимает значение в диапазоне [1500..10000]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 20 | Привязать порт e1 к физическому интерфейсу. | `esr(config-if-gi)# switchport e1 <SLOT>` | <SLOT> – идентификатор слота, принимает значение в диапазоне [0..3]. |
| 21 | Перевести физический порт в режим работы с SFPe1 модулем. | `esr(config-if-gi)# switchport mode e1` | |
| 22 | Включить режим MLPPP на E1-интерфейсе. | `esr(config-e1)# ppp multilink` | |
| 23 | Включить E1-интерфейс в группу агрегации. | `esr(config-e1)# ppp multilink-group <GROUP-ID>` | <GROUP-ID> – идентификатор группы, принимает значение [1..4]. |

### 2.8.2 Пример настройки

**Задача:**

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


**Решение:**

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

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

Настроим MLPPP 3:

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

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

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

## 2.9 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.

### 2.9.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Добавить сетевой мост (bridge) в систему и перейти в режим настройки его параметров. | `esr(config)# bridge <BRIDGE-ID>` | <BRIDGE-ID> – идентификационный номер моста, принимает значения в диапазоне:<br>• для ESR-10/12V(F)/14VF – [1..50];<br>• для ESR-20/21/100/200 – [1..250];<br>• для ESR-1000/1200/1500/1700 – [1..500]. |
| 2 | Активировать сетевой мост. | `esr(config-bridge )# enable` | |
| 3 | Указать экземпляр VRF, в котором будет работать данный интерфейс (не обязательно). | `esr(config-bridge )# ip vrf forwarding <VRF>` | <VRF> – имя VRF, задается строкой до 31 символа. |
| 4 | Назначить описание конфигурируемому сетевому мосту (не обязательно). | `esr(config-bridge)# description <DESCRIPTION>` | <DESCRIPTION> – описание сетевого моста, задаётся строкой до 255 символов. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 5 | Связать саб-интерфейс, qinq-интерфейс, L2GRE туннель или L2TPv3 туннель с сетевым мостом. Связанные интерфейсы/туннели и сетевые мосты автоматически становятся участниками общего L2 домена (не обязательно). | `esr(config-if-gi)# bridge-group <BRIDGE-ID>`<br>`esr(config-if-l2tpv3)# bridge-group <BRIDGE-ID>` | <BRIDGE-ID> – идентификационный номер моста, принимает значения в диапазоне:<br>• для ESR-10/12V(F)/14VF – [1..50];<br>• для ESR-20/21/100/200 – [1..250];<br>• для ESR-1000/1200/1500/1700 – [1..500]. |
| 6 | Связать текущий сетевой мост с VLAN. Все интерфейсы и L2-туннели, являющиеся членами назначаемого VLAN, автоматически включаются в сетевой мост и становятся участниками общего L2 домена (не обязательно) | `esr(config-bridge)# vlan <VID>` | <VID> – идентификатор VLAN, задаётся в диапазоне [1..4094]. |
| 7 | Указать размер MTU (Maximum Transmition Unit) пакетов, которые может пропускать данный bridge (не обязательно; возможно, если в bridge включен только VLAN).<br>MTU более 1500 будет активно только в случае применения команды "system jumbo-frames" | `esr(config-bridge)# mtu <MTU>` | <MTU> – значение MTU, принимает значения в диапазоне:<br>• для ESR-10/12V(F)/14VF – [552..9600];<br>• для ESR-20/21 – [552..9500];<br>• для ESR-100/200/1000/1200/1500/1700 – [552..10000].<br>Значение по умолчанию: 1500 |
| 8 | Указать IPv4/IPv6-адрес и маску подсети для конфигурируемого интерфейса или включить получение IP-адреса динамически. | `esr(config-bridge)# ip address <ADDR/LEN>` | <ADDR/LEN> – IP-адрес и длина маски подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].<br><br>Дополнительные функции IPv4-адресации см. в разделе Настройка IP-адресации. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| | | `esr(config-bridge)# ipv6 address <IPV6-ADDR/LEN>` | <IPV6-ADDR/LEN> – IP-адрес и префикс подсети, задаётся в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128].<br><br>Дополнительные функции IPv6-адресации см. в разделе Настройка IPv6-адресации.<br><br>Можно указать несколько UIPv4/IPv6-адресов перечислением через запятую. Может быть назначено до 8 IPv4/IPv6-адресов на интерфейс. |
| | | `esr(config-bridge)# ip address dhcp` | Дополнительные функции при работе DHCP-клиента см. в разделе Управление DHCP-клиентом. |
| 9 | Отключить на интерфейсе функции Firewall или включить интерфейс в зону безопасности (см. раздел Конфигурирование Firewall). | `esr(config-bridge)# ip firewall disable` | |
| | | `esr(config-bridge)# security-zone <NAME>` | <NAME>-имя зоны безопасности, задаётся строкой до 31 символа. |
| 10 | Включить запись статистики использования текущего интерфейса (не обязательно). | `esr(config-bridge)# history statistics` | |
| 11 | Задать интервал времени, за который усредняется статистика о нагрузке на bridge (не обязательно) | `esr(config-bridge)# load-average <TIME>` | <TIME> – интервал в секундах, принимает значения [5..150].<br><br>Значение по умолчанию: 5 |
| 12 | Задать MAC-адрес сетевого моста, отличный от системного (не обязательно). | `esr(config-bridge)# mac-address <ADDR>` | <ADDR> – MAC-адрес сетевого моста, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 13 | Включить на bridge режим изоляции интерфейсов.<br>В данном режиме обмен трафиком между членами сетевого моста запрещен. (не обязательно; применимо только на ESR-1000/1200/1500/1700) | `esr(config-bridge)# protected-ports [ exclude vlan ]` | exclude vlan – при указании данного ключа, VLAN (связанный с bridge) исключается из списка изолируемых интерфейсов. |
| 14 | Запретить коммутацию unknown-unicast трафика (когда MAC-адрес назначения не содержится в таблице коммутации) в данном bridge. (не обязательно; применимо только на ESR-1000/1200/1500/1700) | `esr(config-bridge)# unknown-unicast-forwarding disable` | |
| 15 | Установить время жизни IPv4/IPv6-записей в ARP-таблице, изученных на данном bridge (не обязательно). | `esr(config-bridge)# ip arp reachable-time <TIME>`<br>или<br>`esr(config-bridge)# ipv6 nd reachable-time <TIME>` | <TIME> – время жизни динамических MAC-адресов, в миллисекундах. Допустимые значения от 5000 до 100000000 миллисекунд. Реальное время обновления записи варьируется от [0,5;1,5]*<TIME>. |

Также для bridge-интерфейса возможно настроить:

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

### 2.9.2 Пример настройки bridge для VLAN и L2TPv3-туннеля

**Задача:**

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

**Решение:**

Создадим VLAN 333:

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

Создадим зону безопасности «trusted»:

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

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

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

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

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

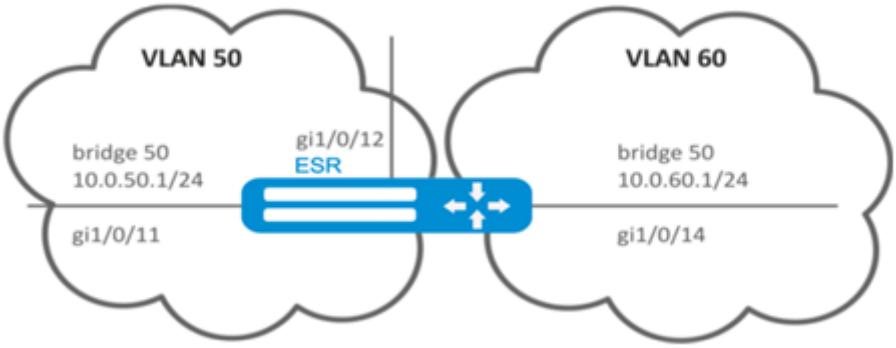
Установим принадлежность L2TPv3-туннеля к мосту, который связан с локальной сетью (настройка L2TPv3-туннеля рассматривается в разделе Настройка L2TPv3-туннелей). В общем случае идентификаторы моста и туннеля не должны совпадать с VID как в данном примере.

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

### 2.9.3 Пример настройки bridge для VLAN

**Задача:**

Настроить маршрутизацию между VLAN 50 (10.0.50.0/24) и VLAN 60 (10.0.60.0/24). VLAN 50 должен относиться к зоне «LAN1», VLAN 60 – к зоне «LAN2», разрешить свободную передачу трафика между зонами.




**Решение:**

Создадим VLAN 50, 60:

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

Создадим зоны безопасности «LAN1» и «LAN2»:

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

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

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

Назначим интерфейсу gi1/0/14 VLAN 60:

```
esr(config)# interface gigabitethernet 1/0/14
esr(config-if-gi)# switchport general allowed vlan add 60 tagged
```

Создадим bridge 50, привяжем VLAN 50, укажем IP-адрес 10.0.50.1/24 и членство в зоне «LAN1»:

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

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

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

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

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

Посмотреть членство интерфейсов в мосте можно командой:

```
esr# show interfaces bridge
```

### 2.9.4 Пример настройки добавления/удаления второго VLAN-тега

**Задача:**

На интерфейс gigabitethernet 1/0/1 поступают Ethernet-кадры с различными VLAN-тегами. Необходимо перенаправить их в интерфейс gigabitethernet 1/0/2, добавив второй VLAN-ID 828. При поступлении на интерфейс gigabitethernet 1/0/2 Ethernet-кадров с VLAN-ID 828, данный тег должен быть удален и отправлен в интерфейс gigabitethernet 1/0/1.

**Решение:**

Создадим на маршрутизаторе bridge без VLAN и без IP-адреса.

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

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

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

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

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

⚠ При добавлении второго VLAN-тега в Ethernet-кадр, его размер увеличивается на 4 байта. На интерфейсе маршрутизатора gigabitethernet 1/0/2 и на всем оборудовании передающем Q-in-Q кадры необходимо увеличить MTU на 4 байта или более.

## 2.10 Настройка Dual-Homing

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

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

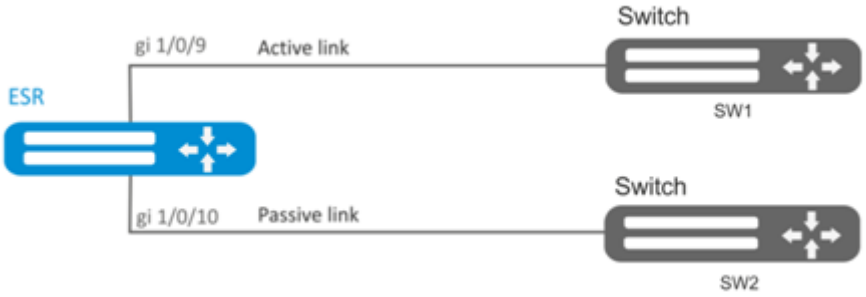
### 2.10.1 Алгоритм настройки

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

### 2.10.2 Пример настройки

**Задача:**

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




**Решение:**

Предварительно нужно выполнить следующие действия:

Создадим VLAN 50-55:

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

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

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

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

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

Основной этап конфигурирования:

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

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

Просмотреть информацию о резервных интерфейсах можно командой:

```
esr# show interfaces backup
```

## 2.11 Настройка зеркалирования (SPAN/RSPAN)

⚠ В текущей версии ПО функционал удаленного зеркалирования (RSPAN) поддерживается только на маршрутизаторах ESR-1000/1200/1500/1700

Зеркалирование трафика — функция маршрутизатора, предназначенная для перенаправления трафика с одного порта маршрутизатора на другой порт этого же маршрутизатора (локальное зеркалирование) или на удаленное устройство (удаленное зеркалирование).

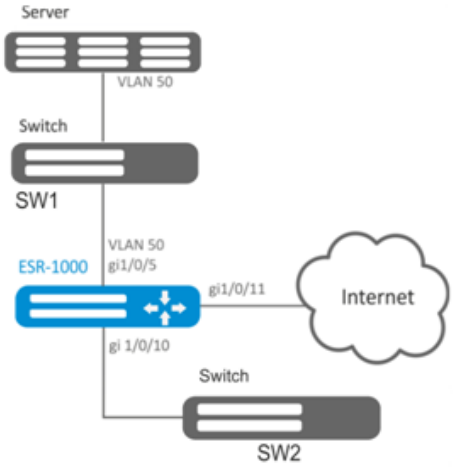
### 2.11.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Определить VLAN, по которому будет передаваться отзеркалированный трафик (в случае использования удаленного зеркалирования). | `esr(config)# port monitor remote vlan <VID> <DIRECTION>` | <VID> – идентификационный номер VLAN, задаётся в диапазоне [2...4094];<br><br><DIRECTION> – направление трафика:<br>• **tx** – зеркалирование в указанный VLAN только исходящего трафика;<br>• **rx** – зеркалирование в указанный VLAN только входящего трафика. |
| 2 | Включить режим удаленного зеркалирования (в случае использования удаленного зеркалирования). | `esr(config)# port monitor remote` | |
| 3 | Определить режим порта передающего отзеркалированный трафик (не обязательно). | `esr(config)# port monitor mode <MODE>` | <MODE> – режим:<br>• **network** – совмещенный режим передачи данных и зеркалирование (по умолчанию);<br>• **monitor-only** – только зеркалирование. |
| 4 | В режиме конфигурации интерфейса включить зеркалирование. | `esr(config-if-gi)# port monitor interface <IF> [ <DIRECTION> ]` | <IF> – интерфейс с которого будут зеркалироваться кадры;<br><br><DIRECTION> – направление трафика:<br>• **tx** – зеркалирование только исходящего трафика;<br>• **rx** – зеркалирование только входящего трафика. |

### 2.11.2 Пример настройки

**Задача:**

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




**Решение:**

Предварительно нужно выполнить следующие действия:

- Создать VLAN 50;
- На интерфейсе gi 1/0/5 добавить VLAN 50 в режиме general.

Основной этап конфигурирования:

Укажем VLAN, по которой будет передаваться зеркалированный трафик:

```
esr1000(config)# port monitor remote vlan 50
```

На интерфейсе gi 1/0/5 укажем порт для зеркалирования:

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

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

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

## 2.12 Настройка LACP

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

### 2.12.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Установить приоритет системы для протокола LACP. | `esr(config)# lacp system-priority <PRIORITY>` | <PRIORITY> – приоритет, указывается в диапазоне [1..65535].<br><br>Значение по умолчанию: 1. |
| 2 | Установить механизм балансировки нагрузки для групп агрегации каналов. | `esr(config)# port-channel load-balance { src-dst-mac-ip \| src-dst-mac \| src-dst-ip \| src-dst-mac-ip-port }` | • **src - dst - mac - ip** – механизм балансировки основывается на MAC-адресе и IP-адресе отправителя и получателя;<br>• **src - dst - mac** – механизм балансировки основывается на MAC-адресе отправителя и получателя;<br>• **src - dst - ip** – механизм балансировки основывается на IP-адресе отправителя и получателя;<br>• **src - dst - mac - ip - port** – механизм балансировки основывается на MAC-адресе, IP-адресе и порте отправителя и получателя. |
| 3 | Установить административный таймаут протокола LACP. | `esr(config)# lacp timeout {short \| long }` | • **long** – длительное время таймаута;<br>• **short** – короткое время таймаута.<br><br>Значение по умолчанию: long. |
| 4 | Создать и перейти в режим конфигурирования агрегированного интерфейса. | `esr(config)# interface port-channel <ID>` | <ID> – порядковый номер группы агрегации каналов, принимает значения [1..12]. |
| 5 | Настроить необходимые параметры агрегированного канала. | | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 6 | Перейти в режим конфигурирования физического интерфейса. | `esr(config)# interface <IF-TYPE><IF-NUM>` | <IF-TYPE> тип интерфейса (gigabitethernet или tengigabitethernet).<br><br><IF-NUM> – F/S/P – F-фрейм (1), S – слот (0), P – порт. |
| 7 | Включить физический интерфейс в группу агрегации каналов с указанием режима формирования группы агрегации каналов. | `esr(config-if-gi)# channel-group <ID> mode <MODE>` | <ID> – порядковый номер группы агрегации каналов, принимает значения [1..12].<br><br><MODE> – режим формирование группы агрегации каналов:<br>• **auto** – добавить интерфейс в динамическую группу агрегации с поддержкой протокола LACP;<br>• **on** – добавить интерфейс в статическую группу агрегации. |
| 8 | Установить LACP-приоритет интерфейса Ethernet. | `esr(config-if-gi)# lacp port-priority <PRIORITY>` | <PRIORITY> – приоритет, указывается в диапазоне [1..65535].<br><br>Значение по умолчанию: 1 |
| 9 | Установить интервал времени, в течение которого собирается статистика о нагрузке на саб-интерфейс (не обязательно). | `esr(config-subif)# load-average <TIME>` | <TIME> – интервал в секундах, принимает значения [5..150]. |
| 10 | Установить время жизни IPv4/IPv6 записей в ARP-таблице, изученных на данном интерфейсе (не обязательно). | `esr(config-subif)# ip arp reachable-time <TIME>`<br><br>или<br><br>`esr(config-subif)# ipv6 nd reachable-time <TIME>` | <TIME> – время жизни динамических MAC-адресов, в миллисекундах.<br>Допустимые значения от 5000 до 100000000 миллисекунд.<br>Реальное время обновления записи варьируется от [0,5;1,5]*<TIME>. |
| 11 | Изменить размер MTU (MaximumTransmitionUnit). MTU более 1500 будет активно только если применена команда "system jumbo-frames" (не обязательно). | `esr(config-subif)# mtu <MTU>` | <MTU> – значение MTU в байтах.<br>Значение по умолчанию: 1500. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 12 | Включить запись статистики использования текущего интерфейса (не обязательно). | `esr(config-subif)# history statistics` | |
| 13 | Переопределить значение поля MSS (Maximum segment size) во входящих TCP-пакетах (не обязательно). | `esr(config-subif)# ip tcp adjust-mss <MSS>`<br>`esr(config-subif)# ipv6 tcp adjust-mss <MSS>` | <MSS> – значение MSS, принимает значения в диапазоне [500..1460]. Значение по умолчанию: 1460 |

Также для агрегированного интерфейса возможно настроить:

- IPv4/IPv6-адресацию (см. в разделах Настройка IP-адресации, Настройка IPv6-адресации и Управление DHCP-клиентом);
- Firewall (см. раздел Конфигурирование Firewall);
- QoS в базовом или расширенном режимах (см. раздел Управление QoS);
- proxy (см. раздел Проксирование HTTP/HTTPS-трафика);
- мониторинг траффика (см. разделы Настройка Netflow и Настройка sFlow);
- функционал протоколов маршрутизации (см. раздел Управление маршрутизацией);
- протокол VRRF (см. раздел Управление резервированием)
- функционал BRAS (см. раздел Управление BRAS (Broadband Remote Access Server));
- функционал IDS/IPS (см. раздел Настройка IPS/IDS).

### 2.12.2 Пример настройки

**Задача:**

Настроить агрегированный канал между маршрутизатором ESR и коммутатором.


**Решение:**

1 Предварительно необходимо выполнить следующие настройки:

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

2 Основной этап конфигурирования:

Создадим интерфейс port-channel 2:

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

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

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

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

# 3 Управление туннелированием



## 3.1 Настройка GRE-туннелей

GRE (англ. Generic Routing Encapsulation — общая инкапсуляция маршрутов) — протокол туннелирования сетевых пакетов. Его основное назначение — инкапсуляция пакетов сетевого уровня сетевой модели OSI в IP-пакеты. GRE может использоваться для организации VPN на 3-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.

### 3.1.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Сконфигурировать L3-интерфейс, от которого будет строиться GRE-туннель. | | |
| 2 | Создать GRE-туннель и перейти в режим его конфигурирования. | `esr(config)# tunnel gre <INDEX>` | <INDEX> – идентификатор туннеля в диапазоне:<br>• для ESR-10/12V(F)/14VF – [1..10];<br>• для ESR-20/21/100/200 – [1..250];<br>• для ESR-1000/1200/1500/1700 – [1..500]. |
| 3 | Указать экземпляр VRF, в котором будет работать данный GRE-туннель (не обязательно). | `esr(config-gre )# ip vrf forwarding <VRF>` | <VRF> – имя VRF, задается строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 4 | Указать описание конфигурируемого туннеля (не обязательно). | `esr(config-gre)# description <DESCRIPTION>` | <DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов. |
| 5 | Установить локальный IP-адрес для установки туннеля. | `esr(config-gre)# local address <ADDR>` | <ADDR> – IP-адрес локального шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| | | `esr(config-gre)# local interface <IF>` | <IF> – интерфейс, от IP-адреса которого устанавливается туннель. |
| 6 | Установить удаленный IP-адрес для установки туннеля. | `esr(config-gre)# remote address <ADDR>` | <ADDR> – IP-адрес локального шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 7 | Указать режим инкапсуляции для GRE туннеля. | `esr(config-gre)# mode <MODE>` | <MODE> – режим инкапсуляции для GRE туннеля:<br>• **ip** – инкапсуляция IP-пакетов в GRE;<br>• **ethernet** – инкапсуляция Ethernet-фреймов в GRE.<br>Значение по умолчанию: ip |
| 8 | Установить IP-адрес локальной стороны туннеля (только в режиме ip). | `esr(config-gre)# ip address <ADDR/LEN>` | <ADDR/LEN> – IP-адрес и префикс подсети задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].<br>Можно указать до 8 IP-адресов перечислением через запятую.<br><br>Дополнительные функции IPv4-адресации см. в разделе Настройка IP-адресации. |

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

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

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

Также для GRE-туннеля возможно настроить:

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

### 3.1.2 Пример настройки IP-GRE-туннеля

**Задача:**

Организовать L3-VPN между офисами компании через IP-сеть, используя для туннелирования трафика протокол GRE.

- в качестве локального шлюза для туннеля используется IP-адрес 115.0.0.1;
- в качестве удаленного шлюза для туннеля используется IP-адрес 114.0.0.10;
- IP-адрес туннеля на локальной стороне 25.0.0.1/24.


**Решение:**

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

Создадим туннель GRE 10:

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

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

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

Укажем IP-адрес туннеля 25.0.0.1/24:

```
esr(config-gre)# ip address 25.0.0.1/24
```

Также туннель должен принадлежать к зоне безопасности, для того чтобы можно было создать правила, разрешающие прохождение трафика в firewall. Принадлежность туннеля к зоне задается следующей командой:

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

Включим туннель:

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

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

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

После применения настроек трафик будет инкапсулироваться в туннель и отправляться партнеру, независимо от наличия GRE-туннеля и правильности настроек с его стороны.

Опционально для GRE-туннеля можно указать следующие параметры:

- Включить вычисление и включение в пакет контрольной суммы заголовка GRE и инкапсулированного пакета для исходящего трафика:

```
esr(config-gre)# local checksum
```

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

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

- Указать уникальный идентификатор:

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

- Указать значение DSCP, MTU, TTL:

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

- Включить и настроить механизм keepalive:

```
esr(config-gre)# keepalive enable
esr(config-gre)# keepalive timeout <TIME>
esr(config-gre)# keepalive retries <VALUE>
```

Состояние туннеля можно посмотреть командой:

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

Счетчики входящих и отправленных пакетов можно посмотреть командой:

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

Конфигурацию туннеля можно посмотреть командой:

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

Настройка туннеля IPv4-over-IPv4 производится аналогичным образом.

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

## 3.2 Настройка DMVPN

DMVPN (*Dynamic Multipoint Virtual Private Network*) – технология для создания виртуальных частных сетей, с возможностью динамического создания туннелей между узлами. Преимуществом данного решения является высокая масштабируемость и легкость настройки при подключении филиалов к головному офису. DMVPN используется в топологии Hub-and-Spoke, и позволяет строить прямые VPN

туннели Spoke-to-Spoke в дополнение к обычным Spoke-to-Hub туннелям. Это означает, что филиалы смогут общаться друг с другом напрямую, без необходимости прохождения трафика через Hub.

Чтобы установить такое соединение, клиенты (NHC) по шифрованному IPsec-туннелю отправляют соответствие своего внутреннего (туннельного) адреса и внешнего (NBMA) адреса на NHRP-сервер (NHS). Когда клиент захочет соединиться с другим NHC, он посылает на сервер запрос, чтобы узнать его внешний адрес. Получив ответ от сервера, клиент теперь самостоятельно может устанавливать соединение с удалённым филиалом.

### 3.2.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Проверить доступность “внешних” IP-адресов, находящихся на физических интерфейсах. | | |
| 2 | Подготовить IPsec-туннели для работы совместно с динамическими GRE-туннелями. | | См. раздел Настройка Policy-based IPsec VPN. |
| 2 | Создать GRE-туннель и перейти в режим его конфигурирования. | `esr(config)# tunnel gre <INDEX>` | <INDEX> – идентификатор туннеля. |
| 3 | Перевести GRE-туннель в режим multipoint. | `esr(config-gre )# multipoint` | |
| 4 | Установить открытый пароль для NHRP пакетов (не обязательно). | `esr(config-gre)# ip nhrp authentication <WORD>` | <WORD> – пароль в открытой форме, задается строкой [1..8] символов, может включать символы [0-9a-fA-F]. |
| 5 | Указать время, в течении которого на NHS будет существовать запись о данном клиенте (не обязательно). | `esr(config-gre)# ip nhrp holding-time <TIME>` | <TIME> – время в секундах, в течении которого на сервере будет существовать запись о данном клиенте, принимает значения [1..65535].<br><br>Значение по умолчанию: 7200 |
| 6 | Задать «логический(туннельный)» адрес NHRP сервера. | `esr(config-gre)# ip nhrp nhs <ADDR> [ no-registration ]` | <ADDR/LEN> – адрес, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32];<br><br>• **no - registration** — не регистрироваться на NHRP сервере. |

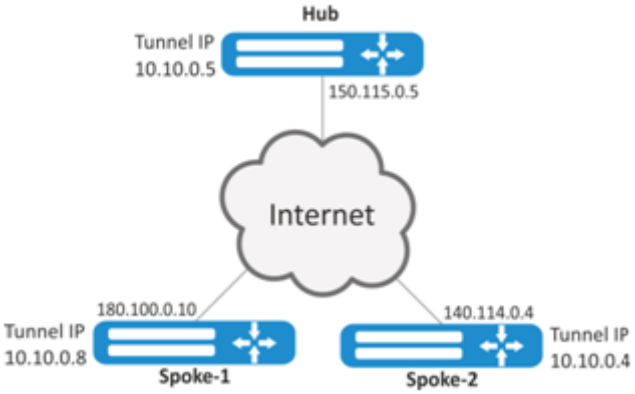
| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 7 | Задать соответствие «внутреннего» туннельного адреса с «внешним» NBMA адресом. | `esr(config-gre)# ip nhrp map <ADDR> <ADDR>` | <ADDR> – IP-адрес задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 8 | Определить адресата мультикастного трафика. | `esr(config-gre)# ip nhrp multicast { dynamic \| nhs \| <ADDR> }` | • **dynamic** — отправлять на все пиры, с которыми есть соединение;<br>• **nhs** — отправлять на все статические сконфигурированные сервера;<br><ADDR> — отправлять на специфически сконфигурированный адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 9 | Включить возможность отправки NHRP Traffic Indication пакетов. Выполняется на NHS (не обязательно). | `esr(config-gre)# ip nhrp redirect` | |
| 10 | Включить возможность создания кратчайших маршрутов. Выполняется на NHC(не обязательно). | `esr(config-gre)# ip nhrp shortcut` | |
| 11 | Привязать IPsec-VPN к mGRE туннелю (не обязательно). | `esr(config-gre)# ip nhrp ipsec <WORD> { static \| dynamic }` | <WORD> – имя VPN, задаётся строкой до 31 символа;<br>• **static** — статическое соединение, применятся для связи с NHS;<br>• **dynamic** — динамически устанавливающееся соединение, конфигурируется для связи между NHC. |
| 12 | Включить работу протокола NHRP. | `esr(config-gre)# ip nhrp enable` | |
| 13 | Организовать IP-связность посредством протокола динамической маршрутизации. | | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| Остальные настройки - аналогичны настройкам статичного GRE-туннеля (см. раздел Настройка GRE-туннелей) | | | |

### 3.2.2 Пример настройки

**Задача:**

Организовать DMVPN между офисами компании, используя mGRE-туннели, NHRP (Next Hop Resolution Protocol), протокол динамической маршрутизации (BGP), Ipsec. В нашем примере у нас будет HUB маршрутизатор и два филиала. HUB – это DMVPN сервер (NHS), а филиалы – DMPVN клиенты (NHC).




Hub внешний IP-адрес — 150.115.0.5;

Spoke-1 внешний IP-адрес — 180.100.0.10;

Spoke-2 внешний IP-адрес — 140.114.0.4.

Параметры IPsec VPN:

IKE:

- группа Диффи-Хэллмана: 2;
- алгоритм шифрования: AES128;
- алгоритм аутентификации: SHA1.

IPsec:

- алгоритм шифрования: AES128;
- алгоритм аутентификации: SHA1.

**Решение:**

1. Конфигурирование Hub
   Создадим туннель GRE:

   ```
   esr# configure
   esr(config)# tunnel gre 5
   ```

   Укажем IP-адрес интерфейса, граничащего с ISP:

   ```
   esr(config-gre)# local address 150.115.0.5
   ```

Зададим значение MTU:

```
esr(config-gre)# mtu 1416
```

Установим значение ttl:

```
esr(config-gre)# ttl 16
```

Зададим IP-адрес GRE туннеля:

```
esr(config-gre)# ip address 10.10.0.5/24
```

Переведём GRE-туннель в mutipoint режим для возможности соединения с несколькими точками:

```
esr(config-gre)# multipoint
```

Перейдём к настройке NHRP. Настроим отправку мультикастовых рассылок в динамически узнаваемые адреса:

```
esr(config-gre)# ip nhrp multicast dynamic
```

Произведём настройку протокола динамической маршрутизации для Hub. В нашем примере это будет BGP:

```
esr(config)# router bgp 65005
esr(config-bgp)# address-family ipv4
esr(config-bgp-af)# neighbor 10.10.0.8
esr(config-bgp-neighbor)# remote-as 65008
esr(config-bgp-neighbor)# enable
esr(config-bgp-neighbor)# exit
esr(config-bgp-af)# neighbor 10.10.0.4
esr(config-bgp-neighbor)# remote-as 65004
esr(config-bgp-neighbor)# enable
esr(config-bgp-neighbor)# exit
esr(config-bgp-af)# enable
```

Произведём настройку IPsec для Hub:

```
esr(config)# security ike proposal IKEPROP
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# exit
```

```
esr(config)# security ike policy IKEPOLICY
esr(config-ike-policy)# pre-shared-key ascii-text encrypted 8CB5107EA7005AFF
esr(config-ike-policy)# proposal IKEPROP
esr(config-ike-policy)# exit
```

```
esr(config)# security ike gateway IKEGW
esr(config-ike-gw)# ike-policy IKEPOLICY
esr(config-ike-gw)# local address 150.115.0.5
esr(config-ike-gw)# local network 150.115.0.5/32 protocol gre
esr(config-ike-gw)# remote address any
esr(config-ike-gw)# remote network any
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

```
esr(config)# security ipsec proposal IPSECPROP
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

```
esr(config)# security ipsec policy IPSECPOLICY
esr(config-ipsec-policy)# proposal IPSECPROP
esr(config-ipsec-policy)# exit
```

```
esr(config)# security ipsec vpn IPSECVPN
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway IKEGW
esr(config-ipsec-vpn)# ike ipsec-policy IPSECPOLICY
esr(config-ipsec-vpn)# enable
```

Привяжем IPsec к GRE туннелю, чтобы клиенты могли устанавливать шифрованное соединение:

```
esr(config-gre)# ip nhrp ipsec IPSECVPN dynamic
```

Включим работу NHRP и сам туннель:

```
esr(config-gre)# ip nhrp enable
esr(config-gre)# enable
```

2. Конфигурирование Spoke
   Проведём стандартную настройку DMVPN на туннеле:

```
esr# configure
esr(config-gre)# tunnel gre 8
esr(config-gre)# mtu 1416
esr(config-gre)# ttl 16
esr(config-gre)# multipoint
esr(config-gre)# local address 180.100.0.10
esr(config-gre)# ip address 10.10.0.8/24
```

Указываем сколько времени будет храниться запись о клиенте на сервере:

```
esr(config-gre)# ip nhrp holding-time 300
```

Указываем туннельный адрес NHS:

```
esr(config-gre)# ip nhrp nhs 10.10.0.5/24
```

Зададим соответствие туннельному адресу – реальный:

```
esr(config-gre)# ip nhrp map 10.10.0.5 150.115.0.5
```

Настроим мультикастовую рассылку на NHRP сервер:

```
esr(config)# ip nhrp multicast nhs
```

Произведём настройку BGP для spoke:

```
esr(config)# router bgp 65008
esr(config-bgp)# address-family ipv4
esr(config-bgp-af)# neighbor 10.10.0.5
esr(config-bgp-neighbor)# remote-as 65005
esr(config-bgp-neighbor)# enable
esr(config-bgp-neighbor)# exit
esr(config-bgp-af)# enable
```

Произведём настройку IPsec. При создании шлюза протокола IKE для NHS, укажем конкретные адреса назначения. А при создании шлюза IKE для NHC – адрес назначения будет any:

```
esr(config)# security ike proposal IKEPROP
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# exit
```

```
esr(config)# security ike policy IKEPOLICY
esr(config-ike-policy)# pre-shared-key ascii-text encrypted 8CB5107EA7005AFF
esr(config-ike-policy)# proposal IKEPROP
esr(config-ike-policy)# exit
```

```
esr(config)# security ike gateway IKEGW_HUB
esr(config-ike-gw)# ike-policy IKEPOLICY
esr(config-ike-gw)# local address 180.100.0.10
esr(config-ike-gw)# local network 180.100.0.10/32 protocol gre
esr(config-ike-gw)# remote address 150.115.0.5
esr(config-ike-gw)# remote network 150.115.0.5/32 protocol gre
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

```
esr(config)# security ike gateway IKEGW_SPOKE
esr(config-ike-gw)# ike-policy IKEPOLICY
esr(config-ike-gw)# local address 180.100.0.10
esr(config-ike-gw)# local network 180.100.0.10/32 protocol gre
esr(config-ike-gw)# remote address any
esr(config-ike-gw)# remote network any
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

```
esr(config)# security ipsec proposal IPSECPROP
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

```
esr(config)# security ipsec policy IPSECPOLICY
esr(config-ipsec-policy)# proposal IPSECPROP
esr(config-ipsec-policy)# exit
```

```
esr(config)# security ipsec vpn IPSECVPN_HUB
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway IKEGW_HUB
esr(config-ipsec-vpn)# ike ipsec-policy IPSECPOLICY
esr(config-ipsec-vpn)# enable
```

```
esr(config)# security ipsec vpn IPSECVPN_SPOKE
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway IKEGW_SPOKE
esr(config-ipsec-vpn)# ike ipsec-policy IPSECPOLICY
esr(config-ipsec-vpn)# enable
```

Привяжем IPsec к GRE туннелю, для возможности установления шифрованного соединения с сервером и с другими клиентами сети:

```
esr(config-gre)# ip nhrp ipsec IPSECVPN_HUB static
esr(config-gre)# ip nhrp ipsec IPSECVPN_SPOKE dynamic
```

Включим работу NHRP и сам туннель:

```
esr(config-gre)# ip nhrp enable
esr(config-gre)# enable
```

Состояние NHRP записей можно посмотреть командой:

```
esr# show ip nhrp
```

Очистить NHRP записи можно командой:

```
esr# clear ip nhrp
```

## 3.3 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.

### 3.3.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Сконфигурировать L3-интерфейс, от которого будет строиться L2TPv3-туннель. | | |
| 2 | Создать L2TPv3-туннель и перейти в режим его конфигурирования. | `esr(config)# tunnel l2tpv3 <INDEX>` | <INDEX> – идентификатор туннеля в диапазоне:<br>• для ESR-10/12V(F)/14VF – [1..10];<br>• для ESR-20/21/100/200 – [1..250];<br>• для ESR-1000/1200/1500/1700 – [1..500]. |
| 3 | Указать описание конфигурируемого туннеля (не обязательно). | `esr(config-l2tpv3)# description <DESCRIPTION>` | <DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов. |
| 4 | Установить локальный IP-адрес для установки туннеля. | `esr(config-l2tpv3)# local address <ADDR>` | <ADDR> – IP-адрес локального шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 5 | Установить удаленный IP-адрес для установки туннеля. | `esr(config-l2tpv3)# remote address <ADDR>` | <ADDR> – IP-адрес локального шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 6 | Выбрать метод инкапсуляции для туннеля L2TPv3. | `esr(config-l2tpv3)# protocol <TYPE>` | <TYPE> – тип инкапсуляции, возможные значения:<br>• **ip** - инкапсуляция в IP-пакет;<br>• **udp** инкапсуляция в UDP-дейтаграммы. |
| 7 | Установить локальный идентификатор сессии. | `esr(config-l2tpv3)# local session-id <SESSION-ID>` | <SESSION-ID> – идентификатор сессии, принимает значения [1..200000]. |
| 8 | Установить удаленный идентификатор сессии. | `esr(config-l2tpv3)# remote session-id <SESSION-ID>` | <SESSION-ID> – идентификатор сессии, принимает значения [1..200000]. |
| 9 | Определить локальный UDP-порт (если в качестве метода инкапсуляции был выбран UDP протокол). | `esr(config-l2tpv3)# local port <UDP>` | <UDP> – номер UDP-порта в диапазоне [1..65535]. |
| 10 | Определить удаленный UDP-порт (если в качестве метода инкапсуляции был выбран UDP протокол). | `esr(config-l2tpv3)# remote port <UDP>` | <UDP> – номер UDP-порта в диапазоне [1..65535]. |
| 11 | Назначить широковещательный домен для инкапсуляции в L2TPV3-пакеты данного туннеля. | `esr(config-l2tpv3)# bridge-group <BRIDGE-ID>` | <BRIDGE-ID> – идентификационный номер моста, принимает значения в диапазоне:<br>• для ESR-10/12V(F)/14VF – [1..50];<br>• для ESR-20/21/100/200 – [1..250];<br>• для ESR-1000/1200/1500/1700 – [1..500] |
| 12 | Активировать туннель. | `esr(config-l2tpv3)# enable` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 13 | Указать размер MTU (MaximumTransmitionUnit) для туннелей (не обязательно).<br>MTU более 1500 будет активно только в случае применения команды "system jumbo-frames" | `esr(config-l2tpv3)# mtu <MTU>` | <MTU> – значение MTU, принимает значения в диапазоне:<br>• для ESR-10/12V(F)/14VF – [1280..9600];<br>• для ESR-20/21 – [1280..9500];<br>• для ESR-100/200/1000/1200/1500/1700 [1280..10000].<br>Значение по умолчанию: 1500. |
| 14 | Определить локальное значение cookie для дополнительной проверки соответствия между передаваемыми данными и сессией (не обязательно). | `esr(config-l2tpv3)# local cookie <COOKIE>` | <COOKIE> – значение COOKIE, параметр принимает значения длиной восемь или шестнадцать символов в шестнадцатеричном виде. |
| 15 | Определить удаленное значение cookie для дополнительной проверки соответствия между передаваемыми данными и сессией (не обязательно). | `esr(config-l2tpv3)# remote cookie <COOKIE>` | <COOKIE> – значение COOKIE, параметр принимает значения длиной восемь или шестнадцать символов в шестнадцатеричном виде. |
| 16 | Задать интервал времени, за который усредняется статистика о нагрузке на туннеле (не обязательно). | `esr(config-l2tpv3)# load-average <TIME>` | <TIME> – интервал в секундах, принимает значения [5..150].<br>Значение по умолчанию: 5. |
| 17 | Включить запись статистики использования текущего туннеля (не обязательно). | `esr(config-subif)# history statistics` | |
| Также для L2TPv3-туннеля возможно настроить:<br>• QoS в базовом или расширенном режимах (см. раздел Управление QoS);<br>• функционал BRAS (см. раздел Управление BRAS (Broadband Remote Access Server)). | | | |

### 3.3.2 Пример настройки L2TPv3-туннеля

**Задача:**

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

- в качестве инкапсулирующего протокола используется UDP, номер порта на локальной стороне и номер порта на стороне партнера 519;
- в качестве локального шлюза для туннеля используется IP-адрес 21.0.0.1;
- в качестве удаленного шлюза для туннеля используется IP-адрес 183.0.0.10;

- идентификатор туннеля на локальной стороне равен 2, на стороне партнера 3;
- идентификатор сессии внутри туннеля равен 100, на стороне партнера 200;
- в туннель направим трафик из bridge с идентификатором 333.


**Решение:**

Создадим туннель L2TPv3 333:

```
esr# configure
esr(config)# tunnel l2tpv3 333
```

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

```
esr(config-l2tpv3)# local address 21.0.0.1
esr(config-l2tpv3)# remote address 183.0.0.10
```

Укажем тип инкапсулирующего протокола и номера UDP-портов:

```
esr(config-l2tpv3)# protocol udp
esr(config-l2tpv3)# local port 519
esr(config-l2tpv3)# remote port 519
```

Укажем идентификаторы сессии внутри туннеля для локальной и удаленной сторон:

```
esr(config-l2tpv3)# local session-id 100
esr(config-l2tpv3)# remote session-id 200
```

Установим принадлежность L2TPv3-туннеля к мосту, который должен быть связан с сетью удаленного офиса (настройка моста рассматривается в пункте Пример настройки bridge для VLAN и L2TPv3-туннеля):

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

Включим ранее созданный туннель и выйдем:

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

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

```
esr(config)# interface gi 1/0/2.333
```

Установим принадлежность саб-интерфейса к мосту, который должен быть связан с локальной сетью (настройка моста рассматривается в пункте Настройка PPP через E1):

```
esr(config-subif)# bridge-group 333
esr(config-subif)# exit
```

После применения настроек трафик будет инкапсулироваться в туннель и отправляться партнеру, независимо от наличия L2TPv3 туннеля и правильности настроек с его стороны.

Настройки туннеля в удаленном офисе должны быть зеркальными локальным. В качестве локального шлюза должен использоваться IP-адрес 183.0.0.10. В качестве удаленного шлюза должен использоваться IP-адрес 21.0.0.1. Номер порта инкапсулирующего протокола на локальной стороне и стороне партнера 519. Идентификатор сессии внутри туннеля должен быть равным 200, на стороне партнера 100. Также туннель должен принадлежать мосту, который необходимо соединить с сетью партнера.

Состояние туннеля можно посмотреть командой:

```
esr# show tunnels status l2tpv3 333
```

Счетчики входящих и отправленных пакетов можно посмотреть командой:

```
esr# show tunnels counters l2tpv3 333
```

Конфигурацию туннеля можно посмотреть командой:

```
esr# show tunnels configuration l2tpv3 333
```

⚠ Помимо создания туннеля необходимо в firewall разрешить входящий трафик по протоколу UDP с портом отправителя 519 и портом назначения 519.

## 3.4 Настройка IPsec VPN

IPsec – это набор протоколов, которые обеспечивают защиту передаваемых с помощью IP-протокола данных. Данный набор протоколов позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и шифрование IP-пакетов, а также включает в себя протоколы для защищённого обмена ключами в сети Интернет.

### 3.4.1 Алгоритм настройки Route-based IPsec VPN

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Создать VTI-туннель и перейти в режим его конфигурирования. | `esr(config)# tunnel vti <TUN>` | <TUN> – имя туннеля устройства. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 2 | Указать локальный IP-адрес VTI-туннеля. | `esr(config-vti)#local address <ADDR>` | <ADDR> – IP-адрес локального шлюза. |
| 3 | Указать удаленный IP-адрес VTI-туннеля. | `esr(config-vti)#remote address <ADDR>` | <ADDR> – IP-адрес удаленного шлюза. |
| 4 | Установить IP-адрес локальной стороны VTI-туннеля | `esr(config-vti)# ip address <ADDR/LEN>` | <ADDR/LEN> – IP-адрес и префикс подсети задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. |
| 5 | Включить VTI-туннель в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall для VTI-туннеля. | `esr(config-vti)# security-zone<NAME>` | <NAME> – имя зоны безопасности, задаётся строкой до 12 символов. |
| | | `esr(config-vti)# ip firewall disable` | |
| 6 | Включить туннель. | `esr(config-vti)#enable` | |
| 7 | Создать IKE-профиль и перейти в режим его конфигурирования. | `esr(config)# security ike proposal <NAME>` | <NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа. |
| 8 | Указать описание конфигурируемого IKE-профиля (не обязательно). | `esr(config-ike- proposal)# description<DESCRIPTION>` | <DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов. |
| 9 | Определить алгоритм аутентификации для IKE. (не обязательно) | `esr(config-ike- proposal)# authentication algorithm <ALGORITHM>` | <ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2_384, sha2-512.<br><br>Значение по умолчанию: sha1 |
| 10 | Определить алгоритм шифрования для IKE. (не обязательно) | `esr(config-ike- proposal)# encryption algorithm <ALGORITHM>` | <ALGORITHM> – протокол шифрования, принимает значения: des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256.<br><br>Значение по умолчанию: 3des |
| 11 | Определить номер группы Диффи-Хеллмана. (не обязательно) | `esr(config-ike- proposal)# dh-group <DH-GROUP>` | <DH-GROUP> – номер группы Диффи-Хеллмана, принимает значения [1, 2, 5, 14, 15, 16, 17, 18].<br><br>Значение по умолчанию: 1 |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 12 | Определить режим аутентификации IKE. (не обязательно) | `esr(config-ike- proposal)# authentication method <METHOD>` | <METHOD> – метод аутентификации ключа. Может принимать значения:<br>• **pre - shared - key** – метод аутентификации, использующий предварительно полученные ключи шифрования;<br>• **rsa - public - key** – метод аутентификации, использующий RSA-сертификат.<br>Значение по умолчанию: pre-shared-key |
| 13 | Создать ike-политику и перейти в режим её конфигурирования. | `esr(config)# security ike policy <NAME>` | <NAME> – имя политики IKE, задаётся строкой до 31 символа. |
| 14 | Задать время жизни соединения протокола IKE (не обязательно). | `esr(config-ike- proposal)# lifetime seconds <SEC>` | <SEC> – период времени, принимает значения [4 .. 86400] секунд.<br>Значение по умолчанию: 3600 |
| 15 | Привязать IKE-профиль к IKE-политике. | `esr(config-ike-policy)# proposal <NAME>` | <NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа. |
| 16 | Указать ключ аутентификации. (обязательно, если в качестве режима аутентификации выбран pre-shared-key) | `esr(config-ike-policy)# pre-shared-key ascii-text<TEXT>` | <TEXT> – строка [1..64] ASCII символов. |
| 17 | Создать IKE-шлюз и перейти в режим его конфигурирования. | `esr(config)# security ike gateway <NAME>` | <NAME> – имя шлюза протокола IKE, задаётся строкой до 31 символа. |
| 18 | Привязать IKE-политику к IKE-шлюзу. | `esr(config-ike-gw)# ike-policy <NAME>` | <NAME> – имя политики протокола IKE, задаётся строкой до 31 символа. |
| 19 | Указать версию IKE (не обязательно). | `esr(config-ike-gw)# version <VERSION>` | <version> – версия IKE-протокола: v1-only или v2-only.<br>Значение по умолчанию: v1-only |

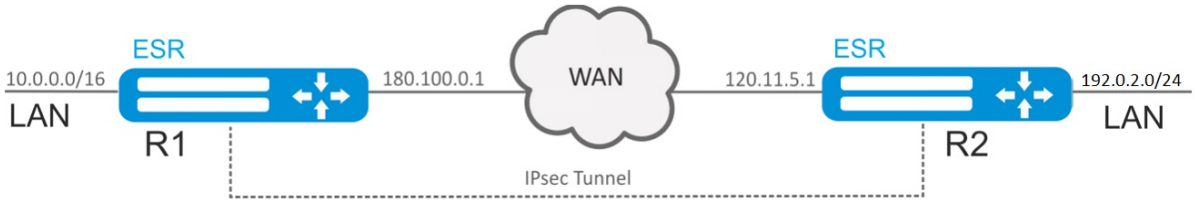
| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 20 | Установить режим перенаправления трафика в туннель – route-based. | `esr(config-ike-gw)# mode route-based` | |
| 21 | Указать действие для<br><br>DPD (не обязательно). | `esr(config-ike-gw)# dead-peer-detection action <MODE>` | <MODE> – режим работы DPD:<br>• **restart** – соединение переустанавливается;<br>• **clear** – соединение останавливается;<br>• **hold** – соединение поддерживается;<br>• **none** – механизм выключен, никаких действий не предпринимается.<br>Значение по умолчанию: none |
| 22 | Указать интервал между отправкой сообщений механизмом DPD (не обязательно). | `esr(config-ike-gw)# dead-peer-detection interval <SEC>` | <SEC> – интервал между отправкой сообщений механизмом DPD, принимает значения [1..180] секунд.<br><br>Значение по умолчанию: 2 |
| 23 | Указать период времени для ответа на сообщения механизма DPD (не обязательно). | `esr(config-ike-gw)# dead-peer-detection timeout <SEC>` | <SEC> – период времени для ответа на сообщения механизма DPD, принимает значения [1..180] секунд.<br><br>Значение по умолчанию: 30 секунд |
| 24 | Привязать VTI-туннель к IKE-шлюзу. | `esr(config-ike-gw)# bind-interface vti <VTI>` | <VTI> – идентификационный номер интерфейса VTI. |
| 25 | Создать в IPsec-профиль. | `esr(config)# security ipsec proposal <NAME>` | <NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа. |
| 26 | Определить алгоритм аутентификации для IPsec. (не обязательно) | `esr(config-ipsec-proposal)# authentication algorithm <ALGORITHM>` | <ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2_384, sha2-512.<br><br>Значение по умолчанию: sha1 |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 27 | Определить алгоритм шифрования для IPsec. (не обязательно) | `esr(config-ipsec-proposal)# encryption algorithm <ALGORITHM>` | <ALGORITHM> – протокол шифрования, принимает значения: des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256.<br><br>Значение по умолчанию: 3des |
| 28 | Указать протокол инкапсуляции для IPsec (не обязательно). | `esr(config-ipsec-proposal)# protocol <PROTOCOL>` | <PROTOCOL> – инкапсулирующий протокол, принимает значения<br><br>Значение по умолчанию: esp |
| 29 | Создать IPsec-политику и перейти в режим её конфигурирования. | `esr(config)# security ipsec policy <NAME>` | <NAME> – имя политики IPsec, задаётся строкой до 31 символа. |
| 30 | Привязать IPsec-профиль к IPsec-политике | `esr(config-ipsec-policy)# proposal <NAME>` | <NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа. |
| 31 | Задать время жизни IPsec-туннеля (не обязательно). | `esr(config-ipsec- policy)# lifetime { seconds <SEC> \| packets <PACKETS> \| kilobytes <KB> }` | <SEC> – период времени жизни IPsec-туннеля, по истечении происходит пересогласование. Принимает значения [1140..86400] секунд.<br><br><PACKETS> – количество пакетов, после передачи которого происходит пересогласование IPsec-туннеля. Принимает значения [4..86400].<br><br><KB> – объем трафика, после передачи которого происходит пересогласование IPsec-туннеля. Принимает значения [4..86400] секунд.<br><br>Значение по умолчанию: 28800 секунд |
| 32 | Создать IPsec VPN и перейти в режим конфигурирования. | `esr(config)# security ipsec vpn <NAME>` | <NAME> – имя VPN, задаётся строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 33 | Определить режим согласования данных, необходимых для активации VPN. | `esr(config-ipsec-vpn)# mode <MODE>` | <MODE> – режим работы VPN. |
| 34 | Привязать IPsec-политику к IPsec-VPN. | `esr(config-ipsec-vpn)# ike ipsec-policy <NAME>` | <NAME> – имя IPsec-политики, задаётся строка до 31 символа. |
| 35 | Задать значение DSCP для использования в IP-заголовке исходящих пакетов IKE-протокола (не обязательно). | `esr(config-ipsec-vpn)# ike dscp <DSCP>` | DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].<br><br>Значение по умолчанию: 63 |
| 36 | Установить режим активации VPN. | `esr(config-ipsec-vpn)# ike establish-tunnel <MODE>` | <MODE> – режим активации VPN:<br><br>• **by - request** – соединение активируется встречной стороной;<br>• **route** – соединение активируется при появлении трафика, маршрутизируемого в туннель;<br>• **immediate** – туннель активируется автоматически после применения конфигурации. |
| 37 | Осуществить привязку IKE-шлюза к IPsec-VPN. | `esr(config-ipsec-vpn)# ike gateway <NAME>` | <NAME> – имя IKE-шлюза, задаётся строкой до 31 символа. |
| 38 | Установить значение временного интервала в секундах, по истечению которого соединение закрывается, если не было принято или передано ни одного пакета через SA (не обязательно). | `esr(config-ipsec-vpn)# ike idle-time <TIME>` | <TIME> – интервал в секундах, принимает значения [4..86400]. |
| 39 | Отключить пересогласование ключей до разрыва IKE-соединения по истечению времени, количеству переданных пакетов или байт (не обязательно). | `esr(config-ipsec-vpn)# ike rekey disable` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 40 | Настроить начало пересогласования ключей IKE-соединения до истечения времени жизни (не обязательно). | `esr(config-ipsec-vpn)# ike rekey margin { seconds <SEC> \| packets <PACKETS> \| kilobytes <KB> }` | <SEC> – интервал времени в секундах, оставшийся до закрытия соединения (задается командой lifetimeseconds, см. 22.2.13). Принимает значения [4..86400].<br><br><PACKETS> – количество пакетов, оставшихся до закрытия соединения (задается командой lifetimepackets). Принимает значения [4..86400]<br><br><KB> – объем трафика в килобайтах, оставшийся до закрытия соединения (задается командой lifetimekilobytes). Принимает значения [4..86400]<br><br>Значение по умолчанию:<br>• Пересогласование ключей до истечения времени – за 540 секунд.<br>• Пересогласование ключей до истечения объема трафика и количества пакетов – отключено. |
| 41 | Установить уровень случайного разброса значений параметров margin seconds, margin packets, margin kilobytes (не обязательно). | `esr(config-ipsec-vpn)# ike rekey randomization <VALUE>` | <VALUE> – максимальный процент разброса значений, принимает значения [1..100].<br><br>Значение по умолчанию: 100% |
| 42 | Указать описание для IPsec-VPN (не обязательно). | `esr(config-ipsec-vpn)# description <DESCRIPTION>` | <DESCRIPTION> – описание профиля, задаётся строкой до 255 символов. |
| 43 | Активировать IPsec VPN. | `esr(config-ipsec-vpn)# enable` | |

### 3.4.2 Пример настройки Route-based IPsec VPN




**Задача:**

Настроить IPsec-туннель между R1 и R2.

- R1 IP-адрес – 120.11.5.1;
- R2 IP-адрес – 180.100.0.1;

IKE:

- группа Диффи-Хэллмана: 2;
- алгоритм шифрования: AES 128 bit;
- алгоритм аутентификации: MD5.

IP sec:

- алгоритм шифрования: AES 128 bit;
- алгоритм аутентификации: MD5.

**Решение:**

1. Конфигурирование R1
   Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```
esr# configure
esr(config)# interface gi 1/0/1
esr(config-if-gi)# ip address 180.100.0.1/24
esr(config-if-gi)# security-zone untrusted
esr(config-if-gi)# exit
```

   Создадим туннель VTI. Трафик будет перенаправляться через VTI в IPsec-туннель. В качестве локального и удаленного шлюза указываются IP-адреса интерфейсов, граничащих с WAN:

```
esr(config)# tunnel vti 1
esr(config-vti)# local address 180.100.0.1
esr(config-vti)# remote address 120.11.5.1
esr(config-vti)# enable
esr(config-vti)# exit
```

   Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```
esr(config)# object-group service ISAKMP
esr(config-object-group-service)# port-range 500
esr(config-object-group-service)# exit
```

Создадим статический маршрут до удаленной LAN-сети. Для каждой подсети, которая находится за IPsec-туннелем, нужно указать маршрут через VTI-туннель:

```
esr(config)# ip route 192.0.2.0/24 tunnel vti 1
```

Создадим профиль протокола IKE. В профиле укажем группу Диффи-Хэллмана 2, алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IKE-соединения:

```
esr(config)# security ike proposal ike_prop1
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm md5
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# exit
```

Создадим политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы и ключ аутентификации:

```
esr(config)# security ike policy ike_pol1
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit
```

Создадим шлюз протокола IKE. В данном профиле указывается VTI-туннель, политика, версия протокола и режим перенаправления трафика в туннель:

```
esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_pol1
esr(config-ike-gw)# mode route-based
esr(config-ike-gw)# bind-interface vti 1
esr(config-ike-gw)# version v2-only
esr(config-ike-gw)# exit
```

Создадим профиль параметров безопасности для IPsec-туннеля. В профиле укажем алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IPsec-туннеля:

```
esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы.

```
esr(config)# security ipsec policy ipsec_pol1
esr(config-ipsec-policy)# proposal ipsec_prop1
esr(config-ipsec-policy)# exit
```

Создадим IPsec VPN. В VPN указывается шлюз IKE-протокола, политика IP sec-туннеля, режим обмена ключами и способ установления соединения. После ввода всех параметров включим туннель командой *enable*.

```
esr(config)# security ipsec vpn ipsec1
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway ike_gw1
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
esr(config)# exit
```

2. Конфигурирование R2
Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```
esr# configure
esr(config)# interface gi 1/0/1
esr(config-if)# ip address 120.11.5.1/24
esr(config-if)# security-zone untrusted
esr(config-if)# exit
```

Создадим туннель VTI. Трафик будет перенаправляться через VTI в IPsec-туннель. В качестве локального и удаленного шлюза указываются IP-адреса интерфейсов, граничащих с WAN:

```
esr(config)# tunnel vti 1
esr(config-vti)# remote address 180.100.0.1
esr(config-vti)# local address 120.11.5.1
esr(config-vti)# enable
esr(config-vti)# exit
```

Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```
esr(config)# object-group service ISAKMP
esr(config-object-group-service)# port-range 500
esr(config-object-group-service)# exit
```

Создадим статический маршрут до удаленной LAN-сети. Для каждой подсети, которая находится за IPsec-туннелем, нужно указать маршрут через VTI-туннель:

```
esr(config)# ip route 10.0.0.0/16 tunnel vti 1
```

Создадим профиль протокола IKE. В профиле укажем группу Диффи-Хэллмана 2, алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IKE-соединения:

```
esr(config)# security ike proposal ike_prop1
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm md5
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# exit
esr(config)#
```

Создадим политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы и ключ аутентификации:

```
esr(config)# security ike policy ike_pol1
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit
```

Создадим шлюз протокола IKE. В данном профиле указывается VTI-туннель, политика, версия протокола и режим перенаправления трафика в туннель:

```
esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_pol1
esr(config-ike-gw)# mode route-based
esr(config-ike-gw)# bind-interface vti 1
esr(config-ike-gw)# version v2-only
esr(config-ike-gw)# exit
```

Создадим профиль параметров безопасности для IPsec-туннеля. В профиле укажем алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IPsec-туннеля:

```
esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы.

```
esr(config)# security ipsec policy ipsec_pol1
esr(config-ipsec-policy)# proposal ipsec_prop1
esr(config-ipsec-policy)# exit
```

Создадим IPsec VPN. В VPN указывается шлюз IKE-протокола, политика IP sec-туннеля, режим обмена ключами и способ установления соединения. После ввода всех параметров включим туннель командой *enable*.

```
esr(config)# security ipsec vpn ipsec1
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway ike_gw1
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
esr(config)# exit
```

Состояние туннеля можно посмотреть командой:

```
esr# show security ipsec vpn status ipsec1
```

Конфигурацию туннеля можно посмотреть командой:

```
esr# show security ipsec vpn configuration ipsec1
```

⚠ В firewall необходимо разрешить протокол ESP и ISAKMP (UDP-порт 500).

### 3.4.3 Алгоритм настройки Policy-based IPsec VPN

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Создать IKE-экземпляр и перейти в режим его конфигурирования. | `esr(config)# security ike proposal <NAME>` | <NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа. |
| 2 | Указать описание конфигурируемого туннеля (не обязательно). | `esr(config-ike- proposal)# description<DESCRIPTION>` | <DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов. |
| 3 | Определить алгоритм аутентификации для IKE. | `esr(config-ike- proposal)# authentication algorithm <ALGORITHM>` | <ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2_384, sha2-512. |
| 4 | Определить алгоритм шифрования для IKE. | `esr(config-ike- proposal)# encryption algorithm <ALGORITHM>` | <ALGORITHM> – протокол шифрования, принимает значения: des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256. |
| 5 | Определить номер группы Диффи-Хеллмана. | `esr(config-ike- proposal)# dh-group <DH-GROUP>` | <DH-GROUP> – номер группы Диффи-Хеллмана, принимает значения [1, 2, 5, 14, 15, 16, 17, 18]. |
| 6 | Определить режим аутентификации. | `esr(config-ike- proposal)# authentication method <METHOD>` | <METHOD> – метод аутентификации ключа. Может принимать значения:<br>• **pre - shared - key** – метод аутентификации, использующий предварительно полученные ключи шифрования;<br>• **rsa - public - key** – метод аутентификации, использующий RSA-сертификат. |
| 7 | Создать политику для профиля IKE и перейти в режим её конфигурирования. | `esr(config)# security ike policy <NAME>` | <NAME> – имя политики IKE, задаётся строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 8 | Задать время жизни соединения протокола IKE (не обязательно). | `esr(config-ike- proposal)# lifetime seconds <SEC>` | <SEC> – период времени, принимает значения [4 .. 86400] секунд. |
| 9 | Привязать политику к профилю. | `esr(config-ike-policy)# proposal <NAME>` | <NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа. |
| 10 | Указать ключ аутентификации. | `esr(config-ike-policy)#pre-shared-key ascii-text<TEXT>` | <TEXT> – строка [1..64] ASCII символов. |
| 11 | Создать шлюз для IKE и перейти в режим его конфигурирования. | `esr(config)# security ike gateway <NAME>` | <NAME> – имя шлюза протокола IKE, задаётся строкой до 31 символа. |
| 12 | Привязать политику IKE. | `esr(config-ike-gw)# ike-policy <NAME>` | <NAME> – имя политики протокола IKE, задаётся строкой до 31 символа. |
| 13 | Указать версию IKE (не обязательно). | `esr(config-ike-gw)# version <VERSION>` | <version> – версия IKE-протокола: **v1-only** или **v2-only**. |
| 14 | Установить режим перенаправления трафика в туннель. | `esr(config-ike-gw)#mode<MODE>` | <MODE> – режим перенаправления трафика в туннель, принимает значения:<br>• **policy - based** – трафик перенаправляется на основе принадлежности к указанным в политиках подсетям;<br>• **route - based** – трафик перенаправляется на основе маршрутов, шлюзом у которых является туннельный интерфейс. |
| 15 | Указать действие для DPD (не обязательно). | `esr(config-ike-gw)# dead-peer-detection action <MODE>` | <MODE> – режим работы DPD:<br>• **restart** – соединение переустанавливается;<br>• **clear** – соединение останавливается;<br>• **hold** – соединение поддерживается;<br>• **none** – механизм выключен, никаких действий не предпринимается. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 16 | Указать интервал между отправкой сообщений механизмом DPD (не обязательно). | `esr(config-ike-gw)#dead-peer-detection interval <SEC>` | <SEC> – интервал между отправкой сообщений механизмом DPD, принимает значения [1..180] секунд. |
| 17 | Указать период времени для ответа на сообщения механизма DPD (не обязательно). | `esr(config-ike-gw)# dead-peer-detection timeout <SEC>` | <SEC> – период времени для ответа на сообщения механизма DPD, принимает значения [1..180] секунд. |
| 18 | Указать версию IKE (не обязательно). | `esr(config-ike-gw)# version <VERSION>` | <version> – версия IKE-протокола: **v1-only** или **v2-only**. |
| 19 | Установить IP подсети отправителя. | `esr(config-ike-gw)# local network <ADDR/LEN> [ protocol { <TYPE> \| <ID> } [ port <PORT> ] ]` | <ADDR/LEN> – IP-адрес и маска подсети отправителя. Параметр задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32];<br><br><TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre;<br><br><ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF];<br><br><PORT> – TCP/UDP порт, принимает значения [1..65535]. |
| 20 | Установить IP-адрес локального шлюза IPsec-туннеля. | `esr(config-ike-gw)#local address <ADDR>` | <ADDR> – IP-адрес локального шлюза. |
| 21 | Установить IP-адрес удаленного шлюза IPsec-туннеля. | `esr(config-ike-gw)#remote address <ADDR>` | <ADDR> – IP-адрес удаленного шлюза. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 22 | Установить IP-адрес подсети получателя, а также IP-протокол и порт. | `esr(config-ike-gw)# remote network <ADDR/LEN> [ protocol { <TYPE> \| <ID> } [ port <PORT> ] ]` | <ADDR/LEN> – IP-адрес и маска подсети отправителя. Параметр задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32];<br><br><TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre;<br><br><ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF];<br><br><PORT> – TCP/UDP порт, принимает значения [1..65535]. |
| 23 | Создать в профиль IPsec. | `esr(config)# security ipsec proposal <NAME>` | <NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа. |
| 24 | Определить алгоритм аутентификации для IPsec. | `esr(config-ipsec-proposal)# authentication algorithm <ALGORITHM>` | <ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2_384, sha2-512. |
| 26 | Определить алгоритм шифрования для IPsec. | `esr(config-ipsec-proposal)# encryption algorithm <ALGORITHM>` | <ALGORITHM> – протокол шифрования, принимает значения: des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256. |
| 26 | Указать протокол (не обязательно). | `esr(config-ipsec-proposal)#protocol <PROTOCOL>` | <PROTOCOL> – инкапсулирующий протокол, принимает значения |
| 27 | Создать политику для профиля IPsec и перейти в режим её конфигурирования | `esr(config)# security ipsec policy <NAME>` | <NAME> – имя политики IPsec, задаётся строкой до 31 символа. |
| 28 | Привяжем политику к профилю | `esr(config-ipsec-policy)# proposal <NAME>` | <NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа. |

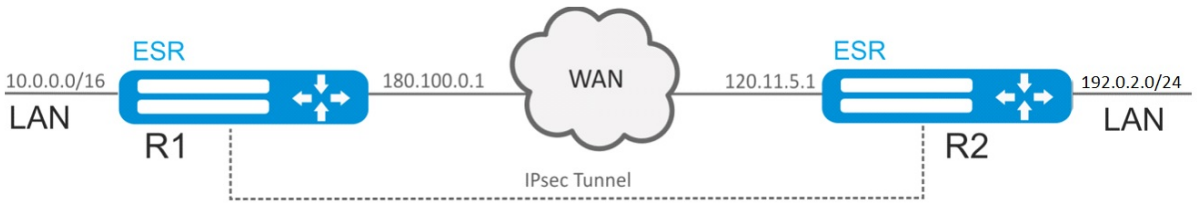
| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 29 | Задать время жизни IPsec туннеля (не обязательно). | `esr(config-ipsec- policy)# lifetime { seconds <SEC> \| packets <PACKETS> \| kilobytes <KB> }` | <SEC> – период времени жизни IPsec-туннеля, по истечении которого происходит пересогласование. Принимает значения [1140..86400] секунд.<br><br><PACKETS> – количество пакетов, после передачи которых происходит пересогласование IPsec-туннеля. Принимает значения [4..86400].<br><br><KB> – объем трафика, после передачи которого происходит пересогласование IPsec-туннеля. Принимает значения [4..86400] секунд. |
| 30 | Создать IPsec VPN и перейти в режим конфигурирования. | `esr(config)# security ipsecvpn <NAME>` | <NAME> – имя VPN, задаётся строкой до 31 символа. |
| 31 | Определить режим согласования данных, необходимых для активации VPN. | `esr(config-ipsec-vpn)# mode <MODE>` | <MODE> – режим работы VPN. |
| 32 | Привязать IPsec политику к VPN. | `esr(config-ipsec-vpn)#ike ipsec-policy <NAME>` | <NAME> – имя IPsec-политики, задаётся строка до 31 символа. |
| 33 | Задать значение DSCP для использования в IP-заголовке исходящих пакетов IKE-протокола (не обязательно). | `esr(config-ipsec-vpn)#ike dscp <DSCP>` | DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 34 | Устанавливается режим активации VPN. | `esr(config-ipsec-vpn)#ike establish-tunnel <MODE>` | <MODE> – режим активации VPN:<br>• **by - request** – соединение активируется встречной стороной;<br>• **route** – соединение активируется при появлении трафика, маршрутизируемого в туннель;<br>• **immediate** – туннель активируется автоматически после применения конфигурации. |
| 35 | Осуществить привязка IKE-шлюза к VPN. | `esr(config-ipsec-vpn)# ike gateway <NAME>` | <NAME> – имя IKE-шлюза, задаётся строкой до 31 символа. |
| 36 | Установить значение временного интервала в секундах, по истечению которого соединение закрывается, если не было принято или передано ни одного пакета через SA (не обязательно). | `esr(config-ipsec-vpn)# ike idle-time <TIME>` | <TIME> – интервал в секундах, принимает значения [4..86400]. |
| 37 | Отключить пересогласование ключей до разрыва IKE соединения по истечению времени, количеству переданных пакетов или байт (не обязательно). | `esr(config-ipsec-vpn)#ike rekey disable` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 38 | Настроить начало пересогласования ключей IKE соединения до истечения времени жизни (не обязательно). | `esr(config-ipsec-vpn)# Ike rekey margin { seconds <SEC> \| packets <PACKETS> \| kilobytes <KB> }` | <SEC> – интервал времени в секундах, оставшийся до закрытия соединения (задается командой lifetimeseconds) . Принимает значения [4..86400].<br><br><PACKETS> – количество пакетов, оставшихся до закрытия соединения (задается командой lifetimepackets). Принимает значения [4..86400].<br><br><KB> – объем трафика в килобайтах, оставшийся до закрытия соединения (задается командой lifetimekilobytes). Принимает значения [4..86400] |
| 39 | Установить уровень случайного разброса значений параметров marginseconds, marginpackets, marginkilobytes (не обязательно). | `esr(config-ipsec-vpn)# ike rekey randomization <VALUE>` | <VALUE> – максимальный процент разброса значений, принимает значения [1..100]. |
| 40 | Описать VPN (не обязательно). | `esr(config-ipsec-vpn)# description <DESCRIPTION>` | <DESCRIPTION> – описание профиля, задаётся строкой до 255 символов. |
| 41 | Активировать IPsec VPN. | `esr(config-ipsec-vpn)# enable` | |

### 3.4.4 Пример настройки Policy-based IPsec VPN

**Задача:**




Настроить IPsec-туннель между R1 и R2.

R1 IP-адрес – 120.11.5.1;

R2 IP-адрес – 180.100.0.1;

IKE:

- группа Диффи-Хэллмана: 2;
- алгоритм шифрования: AES 128 bit;
- алгоритм аутентификации: MD5.

IPsec:

- алгоритм шифрования: AES 128 bit;
- алгоритм аутентификации: MD5.

**Решение:**

1. Конфигурирование R1
   Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```
esr# configure
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 120.11.5.1/24
esr(config-if-gi)# security-zone untrusted
esr(config-if-gi)# exit
```

   Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```
esr(config)# object-group service ISAKMP
esr(config-object-group-service)# port-range 500
esr(config-object-group-service)# exit
```

   Создадим профиль протокола IKE. В профиле укажем группу Диффи-Хэллмана 2, алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IKE-соединения:

```
esr(config)# security ike proposal ike_prop1
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm md5
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# exit
```

   Создадим политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы и ключ аутентификации:

```
esr(config)# security ike policy ike_pol1
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit
```

   Создадим шлюз протокола IKE. В данном профиле указывается VTI-туннель, политика, версия протокола и режим перенаправления трафика в туннель:

```
esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_pol1
esr(config-ike-gw)# local address 180.100.0.1
esr(config-ike-gw)# local network 10.0.0.0/16
esr(config-ike-gw)# remote address 120.11.5.1
esr(config-ike-gw)# remote network 192.0.2.0/24
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

Создадим профиль параметров безопасности для IPsec-туннеля. В профиле укажем алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IPsec-туннеля:

```
esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы.

```
esr(config)# security ipsec policy ipsec_pol1
esr(config-ipsec-policy)# proposal ipsec_prop1
esr(config-ipsec-policy)# exit
```

Создадим IPsec VPN. В VPN указывается шлюз IKE-протокола, политика IP sec-туннеля, режим обмена ключами и способ установления соединения. После ввода всех параметров включим туннель командой *enable*.

```
esr(config)# security ipsec vpn ipsec1
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel immediate
esr(config-ipsec-vpn)# ike gateway ike_gw1
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
esr(config)# exit
```

2. Конфигурирование R2
   Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```
esr# configure
esr(config)# interface gi 1/0/1
esr(config-if)# ip address 120.11.5.1/24
esr(config-if)# security-zone untrusted
esr(config-if)# exit
```

Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```
esr(config)# object-group service ISAKMP
esr(config-addr-set)# port-range 500
esr(config-addr-set)# exit
```

Создадим профиль протокола IKE. В профиле укажем группу Диффи-Хэллмана 2, алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IKE-соединения:

```
esr(config)# security ike proposal ike_prop1
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm md5
esr(config-ike-proposal)# encryption algorithm aes128
esr(config-ike-proposal)# exit
esr(config)#
```

Создадим политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы и ключ аутентификации:

```
esr(config)# security ike policy ike_pol1
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit
```

Создадим шлюз протокола IKE. В данном профиле указывается VTI-туннель, политика, версия протокола и режим перенаправления трафика в туннель:

```
esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_pol1
esr(config-ike-gw)# remote address 180.100.0.1
esr(config-ike-gw)# remote network 10.0.0.0/16
esr(config-ike-gw)# local address 120.11.5.1
esr(config-ike-gw)# local network 192.0.2.0/24
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

Создадим профиль параметров безопасности для IPsec-туннеля. В профиле укажем алгоритм шифрования AES 128 bit, алгоритм аутентификации MD5. Данные параметры безопасности используются для защиты IPsec-туннеля:

```
esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# exit
```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы.

```
esr(config)# security ipsec policy ipsec_pol1
esr(config-ipsec-policy)# proposal ipsec_prop1
esr(config-ipsec-policy)# exit
```

Создадим IPsec VPN. В VPN указывается шлюз IKE-протокола, политика IP sec-туннеля, режим обмена ключами и способ установления соединения. После ввода всех параметров включим туннель командой *enable*.

```
esr(config)# security ipsec vpn ipsec1
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel immediate
esr(config-ipsec-vpn)# ike gateway ike_gw1
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
esr(config)# exit
```

Состояние туннеля можно посмотреть командой:

```
esr# show security ipsec vpn status ipsec1
```

Конфигурацию туннеля можно посмотреть командой:

```
esr# show security ipsec vpn configuration ipsec1
```

⚠ В firewall необходимо разрешить протокол ESP и ISAKMP (UDP-порт 500).

### 3.4.5 Алгоритм настройки Remote Access IPsec VPN

Remote Access IPsec VPN – сценарий организации временных VPN-подключений, в котором сервер IPsec VPN находится в режиме ожидания входящих подключений, а клиенты осуществляют временные подключения к серверу для получения доступа к сетевым ресурсам.

Дополнительной особенностью RA IPsec VPN является возможность использования второго фактора аутентификации IPsec – Extended Authentication (XAUTH), вторым фактором аутентификации является пара логин-пароль для клиента IPsec VPN.

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Создать IKE-экземпляр и перейти в режим его конфигурирования. | `esr(config)# security ike proposal <NAME>` | <NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа. |
| 2 | Указать описание конфигурируемого туннеля (не обязательно). | `esr(config-ike- proposal)# description <DESCRIPTION>` | <DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов. |
| 3 | Определить алгоритм аутентификации для IKE (не обязательно). | `esr(config-ike- proposal)# authentication algorithm <ALGORITHM>` | <ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2_384, sha2-512. Значение по умолчанию: sha1 |
| 4 | Установить IP-адрес локальной стороны VTI-туннеля (не обязательно). | `esr(config-vti)# ip address <ADDR/LEN>` | <ADDR/LEN> – IP-адрес и префикс подсети задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..31]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 5 | Определить номер группы Диффи-Хеллмана (не обязательно). | `esr(config-ike- proposal)# dh-group <DH-GROUP>` | <DH-GROUP> – номер группы Диффи-Хеллмана, принимает значения [1, 2, 5, 14, 15, 16, 17, 18].<br><br>Значение по умолчанию: 1 |
| 6 | Создать политику для профиля IKE и перейти в режим её конфигурирования. | `esr(config)# security ike policy <NAME>` | <NAME> – имя политики IKE, задаётся строкой до 31 символа. |
| 7 | Определить режим аутентификации. | `esr(config-ike- policy)# authentication method <METHOD>` | <METHOD> – метод аутентификации ключа. Может принимать значения:<br><br>• **xauth - psk - key** – метод двухфакторной аутентификации, использующий пару логин-пароль и предварительно полученные ключи шифрования. |
| 8 | Задать режим клиента (только для клиента). | `esr(config-ike- policy)# authentication mode client` | |
| 9 | Задать время жизни соединения протокола IKE (не обязательно). | `esr(config-ike- policy)# lifetime seconds <SEC>` | <SEC> – период времени, принимает значения [4 .. 86400] секунд.<br><br>Значение по умолчанию: 3600 |
| 10 | Привязать политику к профилю. | `esr(config-ike-policy)# proposal <NAME>` | <NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа. |
| 11 | Указать ключ аутентификации. | `esr(config-ike-policy)#pre-shared-key ascii-text <TEXT>` | <TEXT> – строка [1..64] ASCII символов. |
| 12 | Создать профиль доступа. | `esr(config)# access profile <NAME>` | <NAME> – имя профиля доступа, задаётся строкой до 31 символа. |
| 13 | Создать имя пользователя. | `esr(config-access-profile)# user <LOGIN>` | <LOGIN> – логин клиента, задаётся строкой до 31 символа. |
| 14 | Задать пароль пользователя. | `esr(config-profile)# password ascii-text <TEXT>` | <TEXT> – строка [8..32] ASCII символов. |
| 15 | Создать пул адресов назначения (только для сервера). | `esr(config)# address-assignment pool <NAME>` | <NAME> – имя пула адресов назначения, задаётся строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 16 | Задать подсеть, из которой будут выдаваться IP клиентам (только для сервера). | `esr(config-pool)# ip prefix <ADDR/LEN>` | <ADDR/LEN> – адрес подсети и префикс. |
| 17 | Создать шлюз для IKE и перейти в режим его конфигурирования. | `esr(config)# security ike gateway <NAME>` | <NAME> – имя шлюза протокола IKE, задаётся строкой до 31 символа. |
| 18 | Привязать политику IKE. | `esr(config-ike-gw)# ike-policy <NAME>` | <NAME> – имя политики протокола IKE, задаётся строкой до 31 символа. |
| 19 | Установить режим перенаправления трафика в туннель. | `esr(config-ike-gw)# mode <MODE>` | <MODE> – режим перенаправления трафика в туннель, принимает значения:<br>• **policy - based** – трафик перенаправляется на основе принадлежности к указанным в политиках подсетям. |
| 20 | Указать действие для DPD (не обязательно). | `esr(config-ike-gw)# dead-peer-detection action <MODE>` | <MODE> – режим работы DPD:<br>• **restart** – соединение переустанавливается;<br>• **clear** – соединение останавливается;<br>• **hold** – соединение поддерживается;<br>• **none** – механизм выключен, никаких действий не предпринимается.<br>Значение по умолчанию: none |
| 21 | Указать интервал между отправкой сообщений механизмом DPD (не обязательно). | `esr(config-ike-gw)#dead-peer-detection interval <SEC>` | <SEC> – интервал между отправкой сообщений механизмом DPD, принимает значения [1..180] секунд.<br>Значение по умолчанию: 2 |
| 22 | Указать период времени для ответа на сообщения механизма DPD (не обязательно). | `esr(config-ike-gw)# dead-peer-detection timeout <SEC>` | <SEC> – период времени для ответа на сообщения механизма DPD, принимает значения [1..180] секунд.<br>Значение по умолчанию: 30 |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 23 | Указать версию IKE (не обязательно). | `esr(config-ike-gw)# version <VERSION>` | <VERSION> – версия IKE-протокола: **v1-only** или **v2-only**.<br><br>Значение по умолчанию: v1-only |
| 24 | Установить IP подсети отправителя (только для сервера). | `esr(config-ike-gw)# local network <ADDR/LEN> [ protocol { <TYPE> \| <ID> } [ port <PORT> ] ]` | <ADDR/LEN> – IP-адрес и маска подсети отправителя. Параметр задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32];<br><br><TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre;<br><br><ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF];<br><br><PORT> – TCP/UDP порт, принимает значения [1..65535]. |
| 25 | Установить IP-адрес локального шлюза IPsec-туннеля. | `esr(config-ike-gw)#local address <ADDR>` | <ADDR> – IP-адрес локального шлюза. |
| 26 | Установить IP-адрес удаленного шлюза IPsec-туннеля. | `esr(config-ike-gw)#remote address [any \| <ADDR/LEN> [ protocol { <TYPE> \| <ID> } [ port <PORT> ] ]` | Any – установить в качестве удаленного адреса – любой адрес клиента, в конфигурации сервера;<br><br><ADDR/LEN> – IP-адрес и маска подсети сервера, в кофигурации клиента. |
| 27 | Задать пул динамического выделения IP-адресов клиентам (только для сервера). | `esr(config-ike-gw)# remote network dynamic pool <NAME>` | <NAME> – имя пула адресов назначения, задаётся строкой до 31 символа. |
| 28 | Задать режим динамического установления удаленной подсети (только для клиента). | `esr(config-ike-gw)# remote network dynamic client` | |
| 29 | Задать профиль доступа для XAUTH параметров (только для сервера). | `esr(config-ike-gw)# xauth access-profile <NAME>` | <NAME> – имя профиля доступа, задаётся строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 30 | Задать профиль доступа и логин для XAUTH параметров (только для клиента). | `esr(config-ike-gw)# xauth access-profile <NAME> client <LOGIN>` | <NAME> – имя профиля доступа, задаётся строкой до 31имвола;<br><br><LOGIN> – логин клиента, задаётся строкой до 31 символа. |
| 31 | Задать интерфейс терминации выделенного IP для построения IPsec VPN (только для клиента). | `esr(config-ike-gw)# assign-interface loopback <INDEX>` | <INDEX> – индекс интерфейса, принимает значения [1..65535]. |
| 32 | Создать профиль IPsec. | `esr(config)# security ipsec proposal <NAME>` | <NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа. |
| 33 | Определить алгоритм аутентификации для IPsec (не обязательно). | `esr(config-ipsec-proposal)# authentication algorithm <ALGORITHM>` | <ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2_384, sha2-512.<br><br>Значение по умолчанию: sha1 |
| 34 | Определить алгоритм шифрования для IPsec (не обязательно). | `esr(config-ipsec-proposal)# encryption algorithm <ALGORITHM>` | <ALGORITHM> – протокол шифрования, принимает значения: des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256.<br><br>Значение по умолчанию: 3des |
| 35 | Указать протокол (не обязательно). | `esr(config-ipsec-proposal)#protocol <PROTOCOL>` | <PROTOCOL> – инкапсулирующий протокол, принимает значения. |
| 36 | Создать политику для профиля IPsec и перейти в режим её конфигурирования | `esr(config)# security ipsec policy <NAME>` | <NAME> – имя политики IPsec, задаётся строкой до 31 символа. |
| 37 | Привяжем политику к профилю | `esr(config-ipsec-policy)# proposal <NAME>` | <NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 38 | Задать время жизни IPsec туннеля (не обязательно). | `esr(config-ipsec-policy)# lifetime { seconds <SEC> \| packets <PACKETS> \| kilobytes <KB> }` | <SEC> – период времени жизни IPsec-туннеля, по истечении которого происходит пересогласование.<br><br>Принимает значения [1140..86400] секунд.<br><br>Значение по умолчанию: 540<br><br><PACKETS> – количество пакетов, после передачи которых происходит пересогласование IPsec-туннеля.<br><br>Принимает значения [4..86400].<br><br>Значение по умолчанию: отключено.<br><br><KB> – объем трафика, после передачи которого происходит пересогласование IPsec-туннеля. Принимает значения [4..86400] секунд.<br><br>Значение по умолчанию: отключено. |
| 39 | Создать IPsec VPN и перейти в режим конфигурирования. | `esr(config)# security ipsec vpn <NAME>` | <NAME> – имя VPN, задаётся строкой до 31 символа. |
| 40 | Определить режим согласования данных, необходимых для активации VPN. | `esr(config-ipsec-vpn)# mode <MODE>` | <MODE> – режим работы VPN, принимает значения: ike, manual. |
| 41 | Привязать IPsec политику к VPN. | `esr(config-ipsec-vpn)#ike ipsec-policy <NAME>` | <NAME> – имя IPsec-политики, задаётся строка до 31 символа. |
| 42 | Задать значение DSCP для использования в IP-заголовке исходящих пакетов IKE-протокола (не обязательно). | `esr(config-ipsec-vpn)#ike dscp <DSCP>` | DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].<br><br>Значение по умолчанию: 63 |

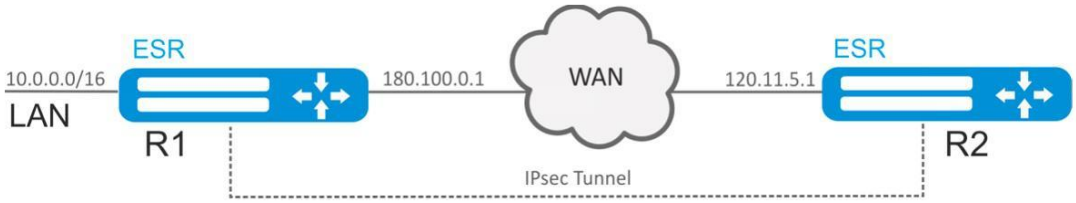
| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 43 | Устанавливается режим активации VPN. | `esr(config-ipsec-vpn)#ike establish-tunnel <MODE>` | <MODE> – режим активации VPN:<br>• **by - request** – соединение активируется встречной стороной, доступно для сервера;<br>• **route** – соединение активируется при появлении трафика, маршрутизируемого в туннель, доступно для сервера;<br>• **immediate** – туннель активируется автоматически после применения конфигурации, доступно для клиента. |
| 44 | Осуществить привязка IKE-шлюза к VPN. | `esr(config-ipsec-vpn)# ike gateway <NAME>` | <NAME> – имя IKE-шлюза, задаётся строкой до 31 символа. |
| 45 | Установить значение временного интервала в секундах, по истечению которого соединение закрывается, если не было принято или передано ни одного пакета через SA (не обязательно). | `esr(config-ipsec-vpn)# ike idle-time <TIME>` | <TIME> – интервал в секундах, принимает значения [4..86400].<br><br>Значение по умолчанию: 0 |
| 46 | Отключить пересогласование ключей до разрыва IKE соединения по истечению времени, количеству переданных пакетов или байт (не обязательно). | `esr(config-ipsec-vpn)#ike rekey disable` | Значение по умолчанию: включено. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 47 | Настроить начало пересогласования ключей IKE соединения до истечения времени жизни (не обязательно). | `esr(config-ipsec-vpn)# Ike rekey margin { seconds <SEC> \| packets <PACKETS> \| kilobytes <KB> }` | <SEC> – интервал времени в секундах, оставшийся до закрытия соединения (задается командой lifetimeseconds) . Принимает значения [4..86400]. Значение по умолчанию: 540<br><br><PACKETS> – количество пакетов, оставшихся до закрытия соединения (задается командой lifetimepackets). Принимает значения [4..86400]. Значение по умолчанию: отключено.<br><br><KB> – объем трафика в килобайтах, оставшийся до закрытия соединения (задается командой lifetimekilobytes). Принимает значения [4..86400] Значение по умолчанию: отключено. |
| 48 | Установить уровень случайного разброса значений параметров marginseconds, marginpackets, marginkilobytes (не обязательно). | `esr(config-ipsec-vpn)# ike rekey randomization <VALUE>` | <VALUE> – максимальный процент разброса значений, принимает значения [1..100].<br><br>Значение по умолчанию: 100 |
| 49 | Описать VPN (не обязательно). | `esr(config-ipsec-vpn)# description <DESCRIPTION>` | <DESCRIPTION> – описание профиля, задаётся строкой до 255 символов. |
| 50 | Активировать IPsec VPN. | `esr(config-ipsec-vpn)# enable` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 51 | Включить режим пере-подключения клиентов XAUTH с одним логином/паролем (только для сервера) (не обязательно). | `esr(config-ipsec-vpn)# security ike session uniqueids <MODE>` | <MODE> – режим пере-подключения, принимает следующие значения:<br>• no - Установленное подключение XAUTH будет удалено, если для нового подключения XAUTH инициатором соединения будет отправлено уведомление "INITIAL_CONTACT", будет назначен ранее использованный IP-адрес. В противном случае, установленное соединение XAUTH будет удержано. Для нового подключения XAUTH будет назначен новый IP-адрес.<br>• never - Установленное подключение XAUTH будет удержано. Для нового подключения XAUTH будет назначен новый IP-адрес. Уведомление " INITIAL_CONTACT" будет в любом случае проигнорировано.<br>• replace - Установленное подключение XAUTH будет удалено. Для нового подключения XAUTH будет использован ранее использованный IP-адрес.<br>• keep - Установленное подключение XAUTH будет удержано. Новое подключение XAUTH будет отклонено. |

### 3.4.6 Пример настройки Remote Access IPsec VPN

**Задача:**




Настроить Remote Access IPsec VPN между R1 и R2 с использованием второго фактора аутентификации IPsec - XAUTH. В качестве сервера IPsec VPN настроить маршрутизатор R1, а маршрутизатор R2 в качестве клиента IPsec VPN.

R2 IP-адрес – 120.11.5.1;

R1 IP-адрес – 180.100.0.1;

Клиентам IPsec VPN:

- выдавать адреса из пула подсети 192.0.2.0/24
- предоставлять доступ до LAN подсети 10.0.0.0/16

IKE:

- группа Диффи-Хэллмана: 2;
- алгоритм шифрования: 3DES;
- алгоритм аутентификации: SHA1.

IPsec:

- алгоритм шифрования: 3DES;
- алгоритм аутентификации: SHA1.

XAUTH:

- логин: client1;
- пароль: password123.

**Решение:**

1. Конфигурирование R1
   Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```
esr# configure
esr(config)# security zone untrusted
esr(config-zone)# exit
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# security-zone untrusted
esr(config-if-gi)# ip address 180.100.0.1/24
esr(config-if-gi)# exit
```

   Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```
esr(config)# object-group service ISAKMP
esr(config-object-group-service)# port-range 500,4500
esr(config-object-group-service)# exit
```

Создадим профиль протокола IKE. В профиле укажем группу Диффи-Хэллмана 2, алгоритм шифрования 3 DES, алгоритм аутентификации SHA1. Данные параметры безопасности используются для защиты IKE-соединения:

```
esr(config)# security ike proposal IKEPROP
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm sha1
esr(config-ike-proposal)# encryption algorithm 3des
esr(config-ike-proposal)# exit
```

Создадим политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы, ключ аутентификации и метод аутентификации XAUTH по ключу:

```
esr(config)# security ike policy IKEPOLICY
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# authentication method xauth-psk-key
esr(config-ike-policy)# proposal IKEPROP
esr(config-ike-policy)# exit
```

Создадим профиль доступа и заведем в нем пару логин и пароль для клиента IPsec VPN:

```
esr(config)# access profile XAUTH
esr(config-access-profile)# user client1
esr(config-profile)# password ascii-text password123
esr(config-profile)# exit
esr(config-access-profile)# exit
```

Создадим пул адресов назначения, из которого будут выдаваться IP клиентам IPsec VPN:

```
esr-1000(config)# address-assignment pool CLIENT_POOL
esr-1000(config-pool)# ip prefix 192.0.2.0/24
esr-1000(config-pool)# exit
```

Создадим шлюз протокола IKE. В данном профиле необходимо указать политику протокола IKE, указать локальную подсеть, в качестве удаленной подсети указать пул адресов назначения, задать режим перенаправления трафика в туннель по политике и использование второго фактора аутентификации XAUTH:

```
esr(config)# security ike gateway IKEGW
esr(config-ike-gw)# ike-policy IKEPOLICY
esr(config-ike-gw)# local address 180.100.0.1
esr(config-ike-gw)# local network 10.0.0.0/16
esr(config-ike-gw)# remote address any
esr(config-ike-gw)# remote network dynamic pool CLIENT_POOL
esr(config-ike-gw)# dead-peer-detection action clear
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# xauth access-profile XAUTH
esr(config-ike-gw)# exit
```

Создадим профиль параметров безопасности для IPsec-туннеля. В профиле укажем алгоритм шифрования 3DES, алгоритм аутентификации SHA1. Данные параметры безопасности используются для защиты IPsec-туннеля:

```
esr(config)# security ipsec proposal IPSECPROP
esr(config-ipsec-proposal)# authentication algorithm sha1
esr(config-ipsec-proposal)# encryption algorithm 3des
esr(config-ipsec-proposal)# exit
```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы.

```
esr(config)# security ipsec policy IPSECPOLICY
esr(config-ipsec-policy)# proposal IPSECPROP
esr(config-ipsec-policy)# exit
```

Создадим IPsec VPN. В VPN указывается шлюз IKE-протокола, политика IP sec-туннеля, режим обмена ключами и режим ожидания входящего соединения IPsec – *by-request*. После ввода всех параметров включим туннель командой *enable*.

```
esr(config)# security ipsec IPSECVPN
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel by-request
esr(config-ipsec-vpn)# ike gateway IKEGW
esr(config-ipsec-vpn)# ike ipsec-policy IPSECPOLICY
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
```

Разрешим протокол esp и udp порты 500, 4500 в конфигурации firewall для установления IPsec VPN:

```
esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol udp
esr(config-zone-pair-rule)# match destination-port ISAKMP
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)#   rule 2
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol esp
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# end
```

2. Конфигурирование R2
   Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

```
esr# configure
esr(config)# interface gi 1/0/1
esr(config-if)# ip address 120.11.5.1/24
esr(config-if)# security-zone untrusted
esr(config-if)# exit
```

Для настройки правил зон безопасности потребуется создать профиль порта протокола ISAKMP:

```
esr(config)# object-group service ISAKMP
esr(config-addr-set)# port-range 500,4500
esr(config-addr-set)# exit
```

Создадим профиль протокола IKE. В профиле укажем группу Диффи-Хэллмана 2, алгоритм шифрования 3 DES, алгоритм аутентификации SHA1. Данные параметры безопасности используются для защиты IKE-соединения:

```
esr(config)# security ike proposal IKEPROP
esr(config-ike-proposal)# dh-group 2
esr(config-ike-proposal)# authentication algorithm sha1
esr(config-ike-proposal)# encryption algorithm 3des
esr(config-ike-proposal)# exit
```

Создадим политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы, ключ аутентификации, метод аутентификации XAUTH по ключу и режим аутентификации – клиент:

```
esr(config)# security ike policy IKEPOLICY
esr(config-ike-policy)# pre-shared-key hexadecimal 123FFF
esr(config-ike-policy)# authentication method xauth-psk-key
esr(config-ike-policy)# authentication mode client
esr(config-ike-policy)# proposal IKEPROP
esr(config-ike-policy)# exit
```

Создадим профиль доступа и заведем в нем пару логин и пароль:

```
esr(config)# access profile XAUTH
esr(config-access-profile)# user client1
esr(config-profile)# password ascii-text password123
esr(config-profile)# exit
esr(config-access-profile)# exit
```

Создадим интерфейс loopback для терминации IP адреса, полученного от IPsec VPN сервера:

```
esr(config)# interface loopback 8
esr(config-loopback)# exit
```

Создадим шлюз протокола IKE. В данном профиле указывается политика, интерфейс терминации, режим динамического установления удаленной подсети, выбор профиля доступа для XAUTH и режим перенаправления трафика в туннель по политике:

```
esr(config)# security ike gateway IKEGW
esr(config-ike-gw)# ike-policy IKEPOLICY
esr(config-ike-gw)# assign-interface loopback 8
esr(config-ike-gw)# local address 120.11.5.1
esr(config-ike-gw)# remote address 180.100.0.1
esr(config-ike-gw)# remote network dynamic client
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# xauth access-profile XAUTH client client1
esr(config-ike-gw)# exit
```

Создадим профиль параметров безопасности для IPsec-туннеля. В профиле укажем алгоритм шифрования 3DES, алгоритм аутентификации SHA1. Данные параметры безопасности используются для защиты IPsec-туннеля:

```
esr(config)# security ipsec proposal IPSECPROP
esr(config-ipsec-proposal)# authentication algorithm sha1
esr(config-ipsec-proposal)# encryption algorithm 3des
esr(config-ipsec-proposal)# exit
```

Создадим политику для IPsec-туннеля. В политике указывается список профилей IPsec-туннеля, по которым могут согласовываться узлы.

```
esr(config)# security ipsec policy IPSECPOLICY
esr(config-ipsec-policy)# proposal IPSECPROP
esr(config-ipsec-policy)# exit
```

Создадим IPsec VPN. В VPN указывается шлюз IKE-протокола, политика IP sec-туннеля, режим обмена ключами и способ установления соединения. После ввода всех параметров включим туннель командой *enable*.

```
esr(config)# security ipsec vpn IPSECVPN
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# ike establish-tunnel immediate
esr(config-ipsec-vpn)# ike gateway IKEGW
esr(config-ipsec-vpn)# ike ipsec-policy IPSECPOLICY
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
```

Разрешим протокол esp и udp порты 500,4500 в конфигурации firewall для установления IPsec VPN:

```
esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol udp
esr(config-zone-pair-rule)# match destination-port ISAKMP
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)#   rule 2
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol esp
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# end
```

Состояние туннеля можно посмотреть командой:

```
esr# show security ipsec vpn status IPSECVPN
```

Конфигурацию туннеля можно посмотреть командой:

```
esr# show security ipsec vpn configuration IPSECVPN
```

⚠ В firewall необходимо разрешить протокол ESP и ISAKMP (UDP-порт 500,4500).

## 3.5 Настройка LT-туннелей

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

### 3.5.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Создать LT-туннели для каждого из существующих VRF. | `esr(config)# tunnel lt <ID>` | <ID> – идентификатор туннеля в диапазоне [1..128]. |
| 2 | Указать описание конфигурируемых туннелей (не обязательно). | `esr(config-lt)# description <DESCRIPTION>` | <DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов. |
| 3 | Включить каждый LT-туннель в соответствующий VFR. | `esr(config-lt)# ip vrf forwarding <VRF>` | <VRF> – имя VRF, задается строкой до 31 символа. |
| 4 | Включить каждый LT-туннель в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall для LT-туннеля. | `esr(config-lt)# security-zone<NAME>` | <NAME> – имя зоны безопасности, задаётся строкой до 12 символов. |
| | | `esr(config-lt)# ip firewall disable` | |
| 5 | Для каждого LT-туннеля задать номер противоположный LT туннель (в другом VRF). | `esr(config-lt)# peer lt <ID>` | <ID> – идентификатор туннеля в диапазоне [1..128]. |
| 6 | Для каждого LT-туннеля указать IP-адрес для маршрутизации пакетов. Для взаимодействующих LT-туннелей, IP-адреса должны быть из одной IP-подсети. | `esr(config-lt)# ip address <ADDR/LEN>` | <ADDR/LEN> – IP-адрес и префикс подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. |
| 7 | Включить туннели. | `esr(config-lt)# enable` | |
| 8 | Для каждого VRF настроить необходимые протоколы маршрутизации через LT-туннель. | | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 9 | Задать интервал времени, за который усредняется статистика о нагрузке на туннеле (не обязательно) | `esr(config-lt)# load-average <TIME>` | <TIME> – интервал в секундах, принимает значения [5..150].<br><br>Значение по умолчанию: 5 |
| 10 | Указать размер MTU (Maximum Transmition Unit) пакетов, которые может пропускать данный bridge (не обязательно; возможно, если в bridge включен только VLAN).<br>MTU более 1500 будет активно только в случае применения команды "system jumbo-frames" | `esr(config-lt)# mtu <MTU>` | <MTU> – значение MTU, принимает значения в диапазоне:<br>• для ESR-10/12V(F)/14VF – [1280..9600];<br>• для ESR-20/21 – [1280..9500];<br>• для ESR-100/200/1000/1200/1500/1700 [1280..10000].<br>Значение по умолчанию: 1500. |

### 3.5.2 Пример настройки

**Задача:**

Организовать взаимодействие между хостами, терминированными в двух VRF vrf_1 и vrf_2.

Исходная конфигурация:

```
hostname esr
ip vrf vrf_1
exit
ip vrf vrf_2
exit
interface gigabitethernet 1/0/1
  ip vrf forwarding vrf_1
  ip firewall disable
  ip address 10.0.0.1/24
exit
interface gigabitethernet 1/0/2
  ip vrf forwarding vrf_2
  ip firewall disable
  ip address 10.0.1.1/24
exit
```

**Решение:**

Создадим LT-туннели для каждого VRF с указанием IP-адресов из одной подсети:

```
esr(config)# tunnel lt 1
esr(config-lt)# ip vrf forwarding vrf_1
esr(config-lt)# ip firewall disable
esr(config-lt)# ip address 192.168.0.1/30
esr(config-lt)# exit
esr(config)# tunnel lt 2
esr(config-lt)# ip vrf forwarding vrf_2
esr(config-lt)# ip firewall disable
esr(config-lt)# ip address 192.168.0.2/30
esr(config-lt)# exit
```

Укажем для каждого LT-туннеля LT-туннель из VRF, с которым необходимо установить связь, и активируем их:

```
esr(config)# tunnel lt 1
esr(config-lt)# peer lt 2
esr(config-lt)# enable
esr(config-lt)# exit
esr(config)# tunnel lt 2
esr(config-lt)# peer lt 1
esr(config-lt)# enable
esr(config-lt)# exit
```

⚠ Если в VRF не сконфигурирован ни один из протоколов динамической маршрутизации, то необходимо указать статические маршруты для каждого VRF:

```
esr(config)# ip route vrf vrf_1 0.0.0.0/0 192.168.0.2
esr(config)# ip route vrf vrf_2 0.0.0.0/0 192.168.0.1
```

# 4 Управление 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.

## 4.1 Базовый QoS

В базовом режиме на маршрутизаторах ESR классификация (направление трафика в очередь) и перемаркировка работает только на входе (на интерфейсе через который поступает трафик должен быть включен QoS)

### 4.1.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Включить сервис QoS на интерфейсе /туннеле/сетевом мосту.<br><br>Если на интерфейсе не назначена политика QoS, то интерфейс работает в режиме BasicQoS. | `esr(config-if-gi)# qos enable` | |
| 2 | Установить режим доверия к значениям кодов 802.1p и DSCP во входящих пакетах. (не обязательно) | `esr(config)# qos trust <MODE>` | <MODE> – режим доверия к значениям кодов 802.1p и DSCP, принимает одно из следующих значений:<br><br>• **dscp** – режим доверия значениям кодов DSCP в IP-заголовке. Не IP-пакеты будут направлены в очередь по умолчанию.<br>• **cos** – режим доверия значениям кодов 802.1p в теге 802.1q. Нетегированные пакеты будут направлены в очередь по умолчанию.<br>• **cos - dscp** – режим доверия значениям кодов DSCP для IP-пакетов и значениям кодов 802.1p для остальных пакетов. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 3 | Установить соответствие между значениями кодов DSCP входящих пакетов и исходящими очередями<br><br>Данное соответствие работает на входящие пакеты интерфейса/ туннеля/моста, на котором включен QOS (не обязательно). | `esr(config)# qos map dscp-queue <DSCP> to <QUEUE>` | <DSCP> – классификатор обслуживания в IP-заголовке пакета, принимает значения [0..63];<br><br><QUEUE> – идентификатор очереди, принимает значения [1..8].<br><br>Значения по умолчанию:<br><br>• DSCP: (0-7), очередь 1<br>• DSCP: (8-15), очередь 2<br>• DSCP: (16-23), очередь 3<br>• DSCP: (24-31), очередь 4<br>• DSCP: (32-39), очередь 5<br>• DSCP: (40-47), очередь 6<br>• DSCP: (48-55), очередь 7<br>• DSCP: (56-63), очередь 8 |
| 4 | Установить соответствие между значениями кодов 802.1p входящих пакетов и исходящими очередями.<br><br>Данное соответствие работает на входящие пакеты интерфейса/ туннеля/моста, на котором включен QOS. (не обязательно) | `esr(config)# qos map cos-queue <COS> to <QUEUE>` | <COS> – классификатор обслуживания в теге 802.1q пакета, принимает значения [0..7];<br><br><QUEUE> – идентификатор очереди, принимает значения [1..8].<br><br>Значения по умолчанию:<br><br>• CoS: (0), очередь 1<br>• CoS: (1), очередь 2<br>• CoS: (2), очередь 3<br>• CoS: (3), очередь 4<br>• CoS: (4), очередь 5<br>• CoS: (5), очередь 6<br>• CoS: (6), очередь 7<br>• CoS: (7), очередь 8 |
| 5 | Установить соответствие между значениями кодов DSCP входящих пакетов и кодов DSCP на выходе из устройства. (в случае необходимости перемаркировки)<br><br>Данное соответствие работает на входящие пакеты интерфейса/ туннеля/моста, на котором включен QOS. | `esr(config)# qos map dscp-queue <DSCP> to <DSCP>` | <DSCP> – классификатор обслуживания в IP-заголовке пакета, принимает значения [0..63]. |

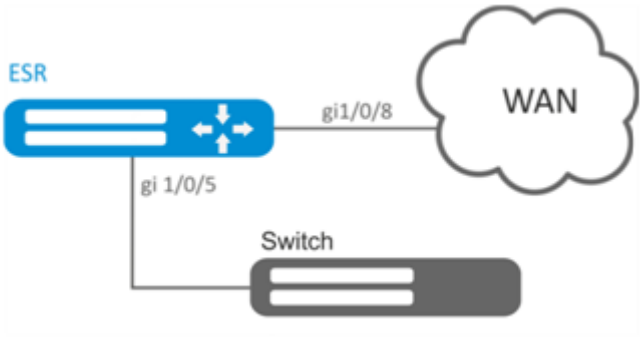
| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 6 | Включить изменения кодов DSCP в соответствии с таблицей DSCP-Mutation. (в случае необходимости перемаркировки) | `esr(config)# qos dscp mutation` | |
| 7 | Установить номер очереди по умолчанию, в которую попадает весь трафик кроме IP в режиме доверия DSCP-приоритетам. | `esr(config)# qos queue default <QUEUE>` | <QUEUE> – идентификатор очереди, принимает значения [1..8]. |
| 8 | Задать количество приоритетных очередей. Оставшиеся очереди являются взвешенными. (не обязательно) | `esr(config)# priority-queue out num-of-queues <VALUE>` | <VALUE> – количество очередей, принимает значение [0..8], где:<br>• **0** – все очереди участвуют в WRR (WRR – механизм обработки очередей на основе веса);<br>• **8** – все очереди обслуживаются как «strictpriority» (strictpriority – приоритетная очередь обслуживается сразу, как только появляются пакеты).<br>Приоритетные очереди выделяются, начиная с 8-й, в сторону уменьшения номера очереди.<br>Значение по умолчанию: 8 |
| 9 | Определить веса для соответствующих взвешенных очередей. | `esr(config)# qos wrr-queue <QUEUE> bandwidth <WEIGHT>` | <QUEUE> – идентификатор очереди, принимает значение [1..8];<br><WEIGHT> – значение веса, принимает значение [1..255].<br>Значение по умолчанию: вес 1 для всех очередей. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 10 | Установить ограничение скорости исходящего трафика для определенной очереди или интерфейса в целом.<br><br>Команда актуальна только для BasicQoS режима интерфейса.<br><br>Ели трафик на входе был классифицирован при помощи расширенного QoS, ограничение не сработает. (в случае необходимости ограничения скорости входящего потока) | `esr(config-if-gi)# traffic-shape { <BANDWIDTH> [BURST] \| queue <QUEUE><BANDWIDTH> [BURST] }` | <QUEUE> – идентификатор очереди, принимает значение [1..8];<br><br><BANDWIDTH> – средняя скорость трафика в Кбит/с, принимает значение [3000..10000000] для TengigabitEthernet интерфейсов и [64..1000000] для прочих интерфейсов и туннелей;<br><br><BURST> – размер сдерживающего порога в КБайт, принимает значение [4..16000]. По умолчанию 128 КБайт.<br><br>Значение по умолчанию: Отключено. |
| 11 | Установить ограничение скорости входящего трафика. (в случае необходимости ограничения скорости исходящего потока) | `esr(config-if-gi)# rate-limit <BANDWIDTH> [BURST]` | <BANDWIDTH> – средняя скорость трафика в Кбит/с, принимает значение [3000..10000000] для TengigabitEthernet интерфейсов и [64..1000000] для прочих интерфейсов и туннелей;<br><br><BURST> – размер сдерживающего порога в КБайт, принимает значение [4..16000]. По умолчанию 128 КБайт.<br><br>Значение по умолчанию: Отключено. |

### 4.1.2 Пример настройки

**Задача:**

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




**Решение:**

Для того чтобы первая очередь осталась приоритетной, а очереди со второй по восьмую стали взвешенными, ограничим количество приоритетных очередей до 1:

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

Перенаправим трафик с DSCP 22 в первую приоритетную очередь:

```
esr(config)# qos map dscp-queue 22 to 1
```

Перенаправим трафик с DSCP 14 в седьмую взвешенную очередь:

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

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

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

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

```
esr(config)# interface gigabitethernet 1/0/8
esr(config-if-gi)# qos enable
```

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

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

Просмотреть статистику по QoS можно командой:

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

## 4.2 Расширенный QoS

### 4.2.1 Алгоритм настройки

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

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Создать списки доступа для определения трафика, к которому должен быть применен расширенный QOS. | | См. Раздел Настройка списков доступа (ACL). |
| 2 | Создать класс QoS и перейти в режим настройки параметров класса. | `esr(config)# class-map <NAME>` | <NAME> – имя создаваемого класса, задается строкой до 31 символа. |
| 3 | Задать описание класса QoS. (не обязательно) | `esr(config-class-map)# description <description>` | <description> – до 255 символов. |
| 4 | Определить трафик относящийся к конфигурируемому классу по списку контроля доступа (ACL). | `esr(config-class-map)# match access-group <NAME>` | <NAME> – имя списка контроля доступа, задаётся строкой до 31 символа. |
| 5 | Задать значение кода DSCP, которое будет установлено в IP-пакетах, соответствующих конфигурируемому классу<br><br>(невозможно назначать одновременно с полями IP Precedence и CoS). (при необходимости перемаркировки) | `esr(config-class-map)# set dscp <DSCP>` | <DSCP> – значение кода DSCP, принимает значения [0..63]. |
| 6 | Задать значение кода IP Precedence, которое будет установлено в IP-пакетах, соответствующих конфигурируемому классу (невозможно назначать одновременно с полями DSCP и CoS). (при необходимости перемаркировки) | `esr(config-class-map)# set ip-precedence <IPP>` | <IPP> – значение кода IP Precedence, принимает значения [0..7]. |
| 7 | Задать значение 802.1p приоритета, которое будет установлено в пакетах, соответствующих конфигурируемому классу (невозможно назначать одновременно с полями DSCP и IP Precedence). (при необходимости перемаркировки) | `esr(config-class-map)# set c os <COS>` | <COS> – значение 802.1p приоритета, принимает значения [0..7]. |
| 8 | Создать политику QoS и осуществить переход в режим настройки параметров политики. | `esr(config)# policy-map <NAME>`<br>`esr(config-policy-map)#` | <NAME> – имя создаваемой политики, задается строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 9 | Задать описание политики QoS. (не обязательно) | `esr(config-policy-map)# description <description>` | <description> – до 255 символов. |
| 10 | Установить гарантированную полосу пропускания исходящего трафика для политики в целом. | `esr(config-policy-map)# shape average <BANDWIDTH> [BURST]` | <BANDWIDTH> – гарантированная полоса трафика в Кбит/с, принимает значение [64..10000000];<br><br><BURST> – размер сдерживающего порога в КБайт, принимает значение [4..16000]. По умолчанию 128 КБайт. |
| 11 | Включить автоматическое распределение полосы пропускания между классами, в которых нет настройки полосы пропускания, включая класс по умолчанию. (в случае необходимости) | `esr(config-policy-map)# shape auto-distribution` | |
| 12 | Включить указанный QoS-класс в политику и осуществить переход в режим настройки параметров класса в рамках политики. | `esr(config-policy-map)# class <NAME>`<br><br>`esr(config-class-policy-map)#` | <NAME> – имя привязываемого класса, задается строкой до 31 символа. При указании значения «class-default» в данный класс попадает трафик неклассифицированный на входе. |
| 13 | Включить политику QoS в класс QoS для создания иерархического QoS. | `esr(config-class-policy-map)# service-policy <NAME>` | <NAME> – имя политики, задается строкой до 31 символа. Вкладываемая политика должна быть уже создана. |
| 14 | Установить гарантированную полосу пропускания исходящего трафика для класса в рамках политики. (при необходимости) | `esr(config-class-policy-map)# shape average <BANDWIDTH> [BURST]` | <BANDWIDTH> – гарантированная полоса трафика в Кбит/с, принимает значение [64..10000000];<br><br><BURST> – размер сдерживающего порога в КБайт, принимает значение [4..16000]. По умолчанию 128 КБайт. |
| 15 | Установить разделяемую полосу пропускания исходящего трафика для определенного класса. Данную полосу класс может занять, если менее приоритетный класс не занял свою гарантированную полосу. (при необходимости) | `esr(config-class-policy-map)# shape peak <BANDWIDTH> [BURST]` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 16 | Определить режим работы класса. (не обязательно) | `esr(config-class-policy-map)# mode <MODE>` | <MODE> – режим класса:<br>• **fifo** – режим FIFO (First In, First Out);<br>• **gred** – режим GRED (Generalized RED);<br>• **red** – режим RED (Random Early Detection);<br>• **sfq** – режим SFQ (очередь SFQ распределяет передачу пакетов на базе потоков).<br>Значение по умолчанию: **FIFO**. |
| 17 | Задать приоритет класса в WRR-процессе. (при необходимости) | `esr(config-class-policy-map)# priority class <PRIORITY>` | <PRIORITY> – приоритет класса в WRR-процессе, принимает значения [1..8].<br>Классы с наибольшим приоритетом обрабатываются в первую очередь. |
| 18 | Перевести класс в режим StrictPriority и задать приоритет класса. (при необходимости) | `esr(config-class-policy-map)# priority level <PRIORITY>` | <PRIORITY> – уровень приоритета в StrictPriority-процессе, принимает значения [1..8].<br>Классы с наибольшим приоритетом обрабатываются в первую очередь. Значение по умолчанию: класс работает в режиме WRR, приоритет не задан. |
| 19 | Определить предельное количество виртуальных очередей. (не обязательно) | `esr(config-class-policy-map)# fair-queue <QUEUE-LIMIT>` | <QUEUE-LIMIT> – предельное количество виртуальных очередей, принимает значения в диапазоне [16..4096].<br>Значение по умолчанию: 16. |
| 20 | Определить предельное количество пакетов для виртуальной очереди. (не обязательно) | `esr(config-class-policy-map)# queue-limit <QUEUE-LIMIT>` | <QUEUE-LIMIT> – предельное количество пакетов в виртуальной очереди, принимает значения в диапазоне [2..4096].<br>Значение по умолчанию: 127. |

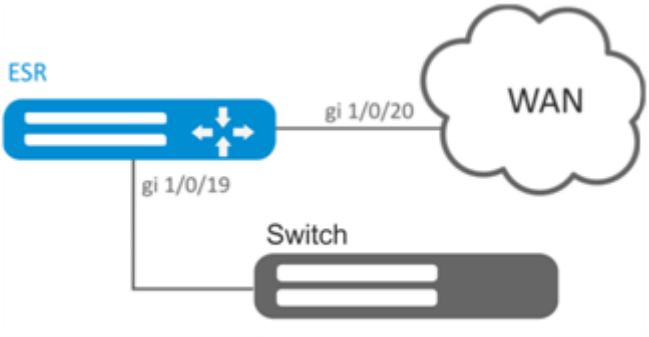
| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 21 | Определить параметры RED (Random Early Detection). (при необходимости) | `esr(config-class-policy-map)# random-detect <LIMIT> <MAX> <MIN> <PROBABILITY>` | <LIMIT> – предельный размер очереди в байтах, принимает значения в диапазоне [1..1000000];<br><br><MAX> – максимальный размер очереди в байтах, принимает значения в диапазоне [1..1000000];<br><br><MIN> – минимальный размер очереди в байтах, принимает значения в диапазоне [1..1000000];<br><br><PROBABILITY> – вероятность отбрасывания пакетов, принимает значения [0..100].<br><br>При указании значений должны выполняться следующие правила:<br><br>• <MAX>> 2 * <MIN><br>• <LIMIT>> 3 * <MAX> |
| 22 | Определить параметры GRED (Generalized Random Early Detection). (при необходимости) | `esr(config-class-policy-map)# random-detect precedence`<br><br>`<PRECEDENCE><LIMIT><MAX><MIN><PROBABILITY>` | <PRECEDENCE> – значение IPPrecendence [0..7];<br><br><LIMIT> – предельный размер очереди в байтах, принимает значения в диапазоне [1..1000000];<br><br><MAX> – максимальный размер очереди в байтах, принимает значения в диапазоне [1..1000000];<br><br><MIN> – минимальный размер очереди в байтах, принимает значения в диапазоне [1..1000000];<br><br><PROBABILITY> – вероятность отбрасывания пакетов, принимает значения [0..100].<br><br>При указании значений должны выполняться следующие правила:<br><br>• <MAX>> 2 * <MIN><br>• <LIMIT>> 3 * <MAX> |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 23 | Включить протокол компрессии tcp заголовков для трафика отдельного класса. (при необходимости) | `esr(config-class-policy-map)# compression header ip tcp` | |
| 24 | Включить сервис QoS на интерфейсе /туннеле/ сетевом мосту. | `esr(config-if-gi)# qos enable` | |
| 25 | Назначить политику QoS на сконфигурируемом интерфейсе/ туннеле/сетевом мосту для классификации входящего (input) или приоритезации исходящего (output) трафика. | `esr(config-if-gi)# service-policy { input \| output } <NAME>` | <NAME> – имя QoS-политики, задаётся строкой до 31 символа. |

### 4.2.2 Пример настройки

**Задача:**

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



**Решение:**

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

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

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

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

Создаём политику и определяем ограничение общей полосы пропускания:

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

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

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

Для другого трафика настраиваем класс с режимом SFQ:

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

Включаем QoS на интерфейсах, политику на входе интерфейса gi 1/0/19 для классификации и на выходе gi1/0/20 для применения ограничений и режима SFQ для класса по умолчанию:

```
esr(config)# interface gigabitethernet 1/0/19
esr(config-if-gi)# qos enable
esr(config-if-gi)# service-policy input fl
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/20
esr(config-if-gi)# qos enable
esr(config-if-gi)# service-policy output fl
esr(config-if-gi)# exit
```

Для просмотра статистики используется команда:

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

# 5 Управление маршрутизацией



## 5.1 Конфигурирование статических маршрутов

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

### 5.1.1 Алгоритм настройки

Добавить статический маршрут возможно командой в режиме глобальной конфигурации:

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

- <VRF> – имя экземпляра VRF, задается строкой до 31 символа;
- <SUBNET> – адрес назначения, может быть задан в следующем формате:
- AAA.BBB.CCC.DDD – IP-адрес хоста, где каждая часть принимает значения [0..255];
- AAA.BBB.CCC.DDD/NN – IP-адрес подсети с маской в виде префикса, где AAA-DDD принимают значения [0..255] и NN принимает значения [1..32].
- <NEXTHOP> – IP-адрес шлюза задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];

- <IF> – имя IP-интерфейса, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора;
- <TUN> – имя туннеля, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора;
- <RULE> – номер правила wan, задаётся в диапазоне [1..50];
- blackhole – при указании команды пакеты до данной подсети будут удаляться устройством без отправки уведомлений отправителю;
- unreachable – при указании команды пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Host unreachable, code 1);
- prohibit – при указании команды пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Communication administratively prohibited, code 13);
- bfd – при указании данного ключа активируется удаление статического маршрута в случае недоступности next-hop.

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

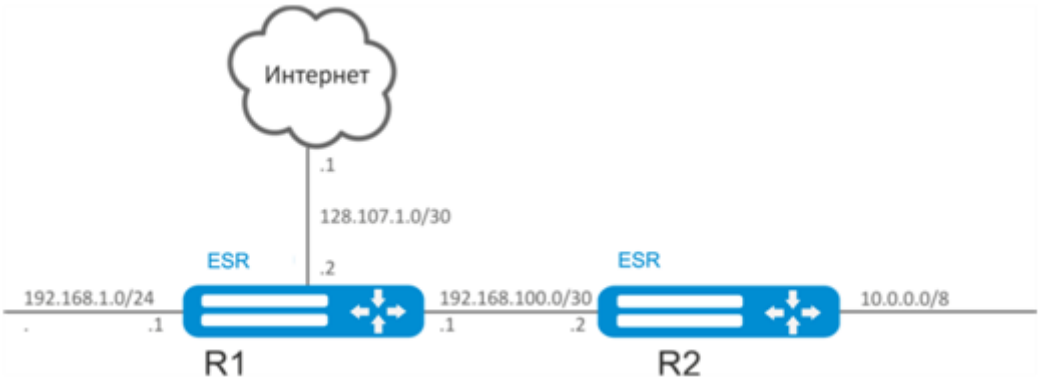
```
ipv6 route [ vrf <VRF> ] <SUBNET> { <NEXTHOP> [ resolve ] | interface <IF> | wan load-
balance rule <RULE> | blackhole | unreachable | prohibit } [ <METRIC> ] [ bfd ]
```

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

### 5.1.2 Пример настройки статических маршрутов

**Задача:**

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




**Решение:**

Зададим имя устройства для маршрутизатора R1:

```
esr# hostname R1
```

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

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

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

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

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

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

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

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

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

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

Зададим имя устройства для маршрутизатора R2:

```
esr# hostname R2
```

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

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

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

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

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

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

Проверить таблицу маршрутов можно командой:

```
esr# show ip route
```

## 5.2 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.

### 5.2.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Настроить приоритетность протокола RIP маршрутизации для основной таблицы маршрутизации (не обязательно). | `esr(config)# ip protocols rip preference <VALUE>` | <VALUE> – приоритетность протокола, принимает значения в диапазоне [1..255].<br><br>Значение по умолчанию: RIP (100). |
| 2 | Настроить емкость таблиц маршрутизации протокола RIP (не обязательно). | `esr(config)# ip protocols rip max-routes <VALUE>` | <VALUE> – количество маршрутов протокола RIP в маршрутной таблице, принимает значения в диапазоне [1..10000];<br>Значение по умолчанию:<br><br>10000. |
| 3 | Создать списки IP-подсетей, которые в дальнейшем будут использоваться для фильтрации анонсируемых и получаемых IP-маршрутов. | `esr(config)# ip prefix-list <NAME>` | <NAME> – имя конфигурируемого списка подсетей, задаётся строкой до 31 символа. |
| 4 | Разрешить (permit) или запретить (deny) списки префиксов. | `esr(config-pl)# permit {object-group <OBJ-GROUP-NETWORK-NAME> [ { eq <LEN> \| le <LEN> \| ge <LEN> [ le <LEN> ] } ]\| default-route}`<br><br>`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;<br><br><LEN> – длина префикса, принимает значения [1..32] в IP-списках префиксов;<br><br>• **eq** – при указании команды длина префикса должна соответствовать указанной;<br>• **le** – при указании команды длина префикса должна быть меньше либо соответствовать указанной;<br>• **ge** – при указании команды длина префикса должна быть больше либо соответствовать указанной;<br>• **default - route** – фильтрация маршрута по умолчанию. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 5 | Перейти в режим настройки параметров RIP-процесса. | `esr(config)# router rip`<br>`esr(config-rip)#` | |
| 6 | Включить RIP-протокол. | `esr(config-rip)# enable` | |
| 7 | Определить алгоритм аутентификации протокола RIP (не обязательно). | `esr(config-rip)# authentication algorithm { cleartext \| md5 }` | • **cleartext** – пароль, передается открытым текстом;<br>• **md5** – пароль хешируется по алгоритму md5. |
| 8 | Установить пароль для аутентификации с соседом (не обязательно). | `esr(config-rip)# authentication key ascii-text { <CLEAR-TEXT> \| encrypted <ENCRYPTED-TEXT> }` | <CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов;<br><br><ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...). |
| 9 | Определить список паролей для аутентификации через алгоритм хеширования md5 (не обязательно). | `esr(config-rip)# authentication key-chain <KEYCHAIN>` | <KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов. |
| 10 | Выключить анонсирование маршрутов на интерфейсах/туннелях/bridge, где это не нужно (не обязательно). | `esr(config-rip)# passive-interface {<IF> \| <TUN> }` | <IF> – интерфейс и идентификатор;<br><br><TUN> – имя и номер туннеля. |
| 11 | Установить временной интервал, по истечении которого производится анонсирование (не обязательно). | `esr(config-rip)# timers update <TIME>` | <TIME> – время в секундах, принимает значения [1..65535].<br><br>Значение по умолчанию: 180 секунд. |
| 12 | Установить временной интервал корректности маршрутной записи без обновления (не обязательно). | `esr(config-rip)# timers invalid <TIME>` | <TIME> – время в секундах, принимает значения [1..65535].<br><br>Значение по умолчанию: 180 секунд. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 13 | Установить временной интервал, по истечении которого производиться удаление маршрута (не обязательно). | `esr(config-rip)# timers flush <TIME>` | <TIME> – время в секундах, принимает значения [1..65535].<br><br>При установке значения нужно учитывать следующее правило: «timersinvalid + 60»<br><br>Значение по умолчанию: 240 секунд. |
| 14 | Включить анонсирование подсетей. | `esr(config-rip)# network <ADDR/LEN>` | <ADDR/LEN> – адрес подсети, указывается в следующем формате:<br><br>AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32]. |
| 15 | Добавить фильтрацию подсетей во входящих или исходящих обновлениях (не обязательно). | `esr(config-rip)# prefix-list <PREFIX-LIST-NAME> { in \| out }` | <PREFIX-LIST-NAME> – имя сконфигурированного списка подсетей, задаётся строкой до 31 символа.<br><br>• **in** – фильтрация входящих маршрутов;<br>• **out** – фильтрация анонсируемых маршрутов. |
| 16 | Включить анонсирование маршрутов, полученных альтернативным способом (не обязательно). | `esr(config-rip)# redistribute static [ route-map <NAME> ]` | <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых статических маршрутов, задаётся строкой до 31 символа. |
| | | `esr(config-rip)# redistribute connected [ route-map <NAME> ]` | <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых напрямую подключенных подсетей, задаётся строкой до 31 символа. |

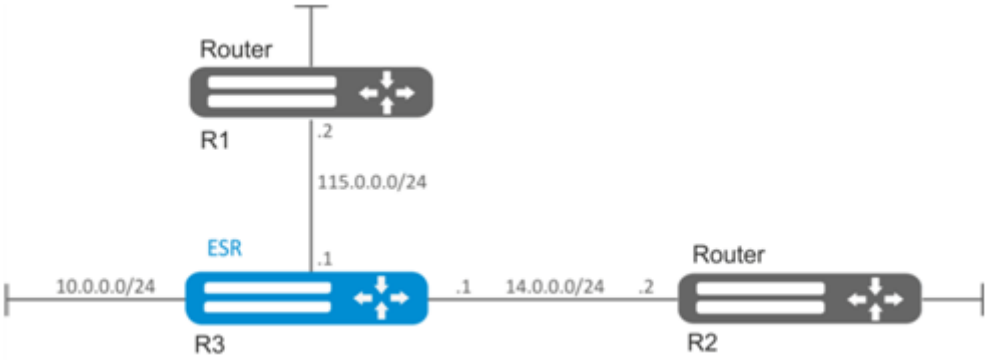
| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| | | `esr(config-rip)# redistribute ospf <ID><ROUTE-TYPE> [ route-map <NAME> ]` | <ID> – номер процесса, может принимать значение [1..65535];<br><br><ROUTE-TYPE> – тип маршрута:<br>• **intra - area** – анонсирование маршрутов OSPF-процесса в пределах зоны;<br>• **inter - area** – анонсирование маршрутов OSPF-процесса между зонами;<br>• **external 1** – анонсирование внешних маршрутов OSPF-формата 1;<br>• **external 2** – анонсирование внешних маршрутов OSPF-формата 2;<br><br><NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых OSPF-маршрутов, задаётся строкой до 31 символа. |
| | | `esr(config-rip)# redistribute bgp <AS> [ route-map <NAME> ]` | <AS> – номер автономной системы, может принимать значения [1..4294967295];<br><br><NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых BGP-маршрутов, задаётся строкой до 31 символа. |
| 17 | Перейти в режим конфигурирования интерфейса/туннеля/ сетевого моста. | `esr(config)# interface <IF-TYPE><IF-NUM>` | <IF-TYPE> тип интерфейса;<br><br><IF-NUM> – F/S/P – F-фрейм (1), S – слот (0), P – порт. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| | | `esr(config)# tunnel <TUN-TYPE><TUN-NUM>` | <TUN-TYPE> тип туннеля;<br><br><TUN-NUM> номер туннеля. |
| | | `esr(config)# bridge <BR-NUM>` | <BR-NUM> – номер bridge. |
| 18 | Установить величину метрики RIP-маршрутов на интерфейсе (не обязательно). | `esr(config-if-gi)# ip rip metric <VALUE>` | <VALUE> – величина метрики, задаётся в размере [0..32767].<br><br>Значение по умолчанию: 5. |
| 19 | Установить режим анонсирования маршрутов по протоколу RIP (не обязательно). | `esr(config-if-gi)# ip rip mode <MODE>` | <MODE> – режим анонсирования маршрутов:<br><br>• **multicast** – маршруты анонсируются в многоадресном режиме;<br>• **broadcast** – маршруты анонсируются в широковещательном режиме;<br>• **unicast** – маршруты анонсируются в unicast-режиме соседям.<br><br>Значение по умолчанию: multicast. |
| 20 | Задать IP-адрес соседа для установления отношения в unicast-режиме анонсирования маршрутов (не обязательно). | `esr(config-if-gi)# ip rip neighbor <ADDR>` | <ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 21 | Включить суммаризацию подсетей (не обязательно). | `esr(config-if-gi)# ip rip summary-address <ADDR/LEN>` | <ADDR/LEN> – IP-адрес и маска подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. |

### 5.2.2 Пример настройки RIP

**Задача:**

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




**Решение:**

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

Перейдём в режим конфигурирования протокола RIP:

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

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

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

Для анонсирования протоколом статических маршрутов выполним команду:

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

Настроим таймер, отвечающий за отправку маршрутной информации:

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

После установки всех требуемых настроек включаем протокол:

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

Для того чтобы просмотреть таблицу маршрутов RIP воспользуемся командой:

```
esr# show ip rip
```

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

## 5.3 Настройка OSPF

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

### 5.3.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Настроить приоритетность протокола OSPF маршрутизации для основной таблицы маршрутизации (не обязательно). | `esr(config)# ip protocols ospf preference <VALUE>` | <VALUE> – приоритетность протокола, принимает значения в диапазоне [1..255].<br><br>Значение по умолчанию: 150. |
| | | `esr(config-vrf)# ip protocols ospf preference <VALUE>` | |
| 2 | Настроить емкость таблиц маршрутизации протокола OSPF (не обязательно). | `esr(config)# ip protocols ospf max-routes <VALUE>` | <VALUE> – количество маршрутов протокола OSPF в маршрутной таблице, принимает значения в диапазоне:<br>• для ESR-1000/1200/1500/1700 [1..500000];<br>• для ESR-20/21/100/200 [1..300000];<br>• для ESR-10/12V(F)/14VF [1..30000]<br>Значение по умолчанию для глобального режима:<br>• для ESR-1000/1200/1500/1700 – (500000);<br>• для ESR-20/21/100/200 – (300000);<br>• для ESR-10/12V(F)/14VF – (30000).<br>Значение по умолчанию для VRF: 0 |
| | | `esr(config)# ipv6 protocols ospf max-routes <VALUE>` | |
| 3 | Включить вывод информации о состоянии отношений с соседями для протокола маршрутизации OSPF (не обязательно). | `esr(config)# router ospf log-adjacency-changes` | |
| | | `esr(config)# ipv6 router ospf log-adjacency-changes` | |
| 4 | Создать списки IP-подсетей, которые в дальнейшем будут использоваться для фильтрации анонсируемых и получаемых IP-маршрутов. | `esr(config)# ip prefix-list <NAME>` | <NAME> – имя конфигурируемого списка подсетей, задаётся строкой до 31 символа. |
| | | `esr(config)# ipv6 prefix-list <NAME>` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 5 | Разрешить (permit) или запретить (deny) списки префиксов. | `esr(config-pl)# permit {object-group <OBJ-GROUP-NETWORK-NAME> [ { eq <LEN> \| le <LEN> \| ge <LEN> [ le <LEN> ] } ]\| default-route}`<br>`esr(config-pl)# deny {object-group <OBJ-GROUP-NETWORK-NAME> [ { eq <LEN> \| le <LEN> \| ge <LEN> [ le <LEN> ] } ] \| default-route}`<br>`esr(config-ipv6-pl)# permit {object-group <OBJ-GROUP-NETWORK-NAME> [ { eq <LEN> \| le <LEN> \| ge <LEN> [ le <LEN> ] } ]\| default-route}`<br>`esr(config-ipv6-pl)# deny object-group <OBJ-GROUP-NETWORK-NAME> [ { eq <LEN> \| le <LEN> \| ge <LEN> [ le <LEN> ] } ] \| default-route}` | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP -адресов, задаётся строкой до 31 символа;<br><br><LEN> – длина префикса, принимает значения [1..32] в IP-списках префиксов;<br>• **eq** – при указании команды длина префикса должна соответствовать указанной;<br>• **le** – при указании команды длина префикса должна быть меньше либо соответствовать указанной;<br>• **ge** – при указании команды длина префикса должна быть больше либо соответствовать указанной;<br>• **default - route** – фильтрация маршрута по умолчанию. |
| 6 | Добавить OSPF-процесс в систему и осуществить переход в режим настройки параметров OSPF-процесса. | `esr(config)# router ospf <ID> [vrf <VRF>]`<br>`esr(config)# ipv6 router ospf <ID> [vrf <VRF>]` | <ID> – номер автономной системы процесса, принимает значения [1..65535]<br><br><VRF> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет работать протокол маршрутизации. |
| 7 | Установить идентификатор маршрутизатора для данного OSPF-процесса. | `esr(config-ospf)# router-id <ID>`<br>`esr(config-ipv6-ospf)# router-id <ID>` | <ID> – идентификатор маршрутизатора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 8 | Определить приоритетность маршрутов процесса OSPF. | `esr(config-ospf)# preference <VALUE>`<br>`esr(config-ipv6-ospf)# preference <VALUE>` | <VALUE> – приоритетность маршрутов процесса OSPF, принимает значения в диапазоне [1..255].<br><br>Значение по умолчанию: 10. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 9 | Включить совместимость с RFC 1583 (не обязательно). | `esr(config-ospf)# compatible rfc1583` | |
| | | `esr(config-ipv6-ospf)# compatible rfc1583` | |
| 11 | Добавить фильтрацию подсетей во входящих или исходящих обновлениях (не обязательно). | `esr(config-ospf)# prefix-list <PREFIX-LIST-NAME> { in \| out }` | <PREFIX-LIST-NAME> – имя сконфигурированного списка подсетей, задаётся строкой до 31 символа.<br>• **in** – фильтрация входящих маршрутов;<br>• **out** – фильтрация анонсируемых маршрутов. |
| | | `esr(config-ipv6-ospf)# prefix-list <PREFIX-LIST-NAME> { in \| out }` | |
| 12 | Включить анонсирование маршрутов, полученных альтернативным способом (не обязательно). | `esr(config-ospf)# redistribute static [ route-map <NAME> ]` | <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых статических маршрутов, задаётся строкой до 31 символа. |
| | | `esr(config-ipv6-ospf)# redistribute static [ route-map <NAME> ]` | |
| | | `esr(config-ospf)# redistribute connected [ route-map <NAME> ]` | <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых напрямую подключенных подсетей, задаётся строкой до 31 символа. |
| | | `esr(config-ipv6-ospf)# redistribute connected [ route-map <NAME> ]` | |
| | | `esr(config-ospf)# redistribute rip [ route-map <NAME> ]` | <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых RIP-маршрутов, задаётся строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| | | esr(config-ospf)# redistribute bgp <AS> [ route-map <NAME> ] | <AS> – номер автономной системы, может принимать значения [1..4294967295];<br><br><NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых BGP-маршрутов, задаётся строкой до 31 символа. |
| | | esr(config-ipv6-ospf)# redistribute bgp <AS> [ route-map <NAME> ] | |
| 13 | Активировать OSPF-процесс. | esr(config-ospf)# enable | |
| | | esr(config-ipv6-ospf)# enable | |
| 14 | Создать OSPF-область и перейти в режим конфигурирования области. | esr(config-ospf)# area <AREA_ID> | <AREA_ID> – идентификатор области, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| | | esr(config-ipv6-ospf)# area <AREA_ID> | |
| 15 | Включить анонсирование подсетей. | esr(config-ospf-area)# network <ADDR/LEN> | <ADDR/LEN> – адрес подсети, указывается в следующем формате:<br><br>AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32]. |
| | | esr(config-ipv6-ospf-area)# network <IPV6-ADDR/LEN> | <IPV6-ADDR/LEN> – IPv6-адрес и маска подсети, задаётся в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 16 | Определить тип области | `esr(config-ospf-area)# area-type <TYPE> [ no-summary ]`<br>`esr(config-ipv6-ospf-area)# area-type <TYPE> [ no-summary ]` | <TYPE> – тип области:<br>• **stub** – устанавливает значение stub (тупиковая область); no-summary – команда в связке с параметром «stub» образует область «totallystubby» (для передачи информации за пределы области используется только маршрут по умолчанию).<br>• **nssa** – устанавливает значение nssa (область NSSA); no-summary – в связке с параметром nssa образует область totallynssa (автоматически генерирует маршрут по умолчанию как межобластной). |
| 17 | Включить генерацию маршрута по умолчанию для NSSA-области и анонсирование его в качестве NSSA-LSA. | `esr(config-ospf-area)# default-information-originate`<br>`esr(config-ipv6-ospf-area)# default-information-originate` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 18 | Включить суммаризацию или скрытие подсетей. | `esr(config-ospf-area)# summary-address <ADDR/LEN> { advertise \| not-advertise }` | <ADDR/LEN> – IP-адрес и маска подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32];<br>• **advertise** – при указании команды вместо указанных подсетей будет анонсироваться суммарная подсеть;<br>• **not - advertise** – при указании команды подсети, входящие в указанную подсеть, анонсироваться не будут. |
| | | `esr(config-ipv6-ospf-area)# summary-address <IPV6-ADDR/LEN> { advertise \| not-advertise }` | <IPV6-ADDR/LEN> – IPv6-адрес и маска подсети, задаётся в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128];<br>• **advertise** – при указании команды вместо подсетей, входящих в указанную подсеть, будет анонсироваться суммарная подсеть;<br>• **not-advertise** – подсети входящие в указанную подсеть анонсироваться не будут. |
| 19 | Активировать OSPF-область. | `esr(config-ospf-area)# enable` | |
| | | `esr(config-ipv6-ospf-area)# enable` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 20 | Установить виртуальное соединение между основной и удаленными областями, имеющими между ними несколько областей. | `esr(config-ospf-area)# virtual-link <ID>`<br>`esr(config-ipv6-ospf-area)# virtual-link <ID>` | <ID> – идентификатор маршрутизатора, с которым устанавливается виртуальное соединение, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 21 | Установить интервал времени в секундах, по истечении которого маршрутизатор повторно отправит пакет, который не получил подтверждения о получении (например, DatabaseDescription пакет или LinkStateRequest пакеты). | `esr(config-ospf- vlink)# restransmit-interval <TIME>`<br>`esr(config-ipv6-ospf-vlink)# restransmit-interval <TIME>` | <TIME> – время в секундах, принимает значения [1..65535].<br><br>Значение по умолчанию: 5 секунд. |
| 22 | Установить интервал времени в секундах, по истечении которого маршрутизатор отправляет следующий hello-пакет. | `esr(config-ospf- vlink)# hello-interval <TIME>`<br>`esr(config-ipv6-ospf-vlink)# hello-interval <TIME>` | <TIME> – время в секундах, принимает значения [1..65535].<br><br>Значение по умолчанию: 10 секунд. |
| 23 | Установить интервал времени в секундах, по истечении которого сосед будет считаться неактивным. Этот интервал должен быть кратным значению «hello-interval». | `esr(config-ospf- vlink)# dead-interval <TIME>`<br>`esr(config-ipv6-ospf-vlink)# dead-interval <TIME>` | <TIME> – время в секундах, принимает значения [1..65535].<br><br>Значение по умолчанию: 40 секунд. |
| 24 | Определяется интервал времени в секундах, по истечении которого маршрутизатор выберет DR в сети | `esr(config-ospf- vlink)# wait-interval <TIME>`<br>`esr(config-ipv6-ospf-vlink)# wait-interval <TIME>` | <TIME> – время в секундах, принимает значения [1..65535].<br>Значение по умолчанию: 40 секунд |
| 25 | Определить алгоритм аутентификации | `esr(config-ospf- vlink)# authentication algorithm <ALGORITHM>` | <ALGORITHM> – алгоритм аутентификации:<br>• **cleartext** – пароль, передается открытым текстом (доступно только для RIP и OSPF-VLINK);<br>• **md 5** – пароль хешируется по алгоритму md5. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 26 | Установить пароль для аутентификации с соседом. | `esr(config-ospf- vlink)# authentication key ascii-text { <CLEAR-TEXT> \| encrypted <ENCRYPTED-TEXT> }` | <CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов.<br><br><ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...). |
| 27 | Определить список паролей для аутентификации через алгоритм хеширования md5. | `esr(config-ospf- vlink)# authentication key chain <KEYCHAIN>` | <KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов. |
| 28 | Активировать виртуальное соединение. | `esr(config-ospf- vlink)# enable` | |
| 29 | Перейти в режим конфигурирования интерфейса/туннеля/ сетевого моста. | `esr(config)# interface <IF-TYPE><IF-NUM>` | <IF-TYPE> тип интерфейса;<br><br><IF-NUM> – F/S/P – F-фрейм (1), S – слот (0), P – порт. |
| | | `esr(config)# tunnel <TUN-TYPE><TUN-NUM>` | <TUN-TYPE> тип туннеля;<br><br><TUN-NUM> номер туннеля. |
| | | `esr(config)# bridge <BR-NUM>` | <BR-NUM> – номер bridge. |
| 30 | Определить принадлежность интерфейса/туннеля/ сетевого моста к определенному OSPF-процессу. | `esr(config-if-gi)# ip ospf instance <ID>` | <ID> – номер процесса, принимает значения [1..65535]. |
| | | `esr(config-if-gi)# ipv6 ospf instance <ID>` | |
| 31 | Определить принадлежность интерфейса к определенной области OSPF-процесса. | `esr(config-if-gi)# ip ospf area <AREA_ID>` | <AREA_ID> – идентификатор области, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| | | `esr(config-if-gi)# ipv6 ospf area <AREA_ID>` | |
| 32 | Включить маршрутизацию по протоколу OSPF на интерфейсе. | `esr(config-if-gi)# ip ospf` | |
| | | `esr(config-if-gi)# ipv6 ospf` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 33 | Включить режим, в котором OSPF-процесс будет игнорировать значение MTU интерфейса во входящих Database Description-пакетах. | `esr(config-if-gi)# ip ospf mtu-ignore`<br>`esr(config-if-gi)# ipv6 ospf mtu-ignore` | |
| 34 | Определить алгоритм аутентификации протокола OSPF. | `esr(config-if-gi)# ip ospf authentication algorithm <ALGORITHM>` | <ALGORITHM> – алгоритм аутентификации:<br>• **cleartext** – пароль, передается открытым текстом;<br>• **md 5** – пароль хешируется по алгоритму md5. |
| 35 | Установить пароль для аутентификации с OSPF-соседом при передаче пароля открытым текстом. | `esr(config-if-gi)# ip ospf authentication key ascii-text { <CLEAR-TEXT> \| encrypted <ENCRYPTED-TEXT> }` | <CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов;<br><br><ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...). |
| 36 | Определить список паролей для аутентификации по алгоритму хеширования md5 с соседом. | `esr(config-if-gi)# ip ospf authentication key-chain <KEYCHAIN>` | <KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов. |
| 37 | Определить интервал времени в секундах, по истечении которого маршрутизатор выберет DR в сети. | `esr(config-if-gi)# ip ospf wait-interval <TIME>`<br>`esr(config-if-gi)# ipv6 ospf wait-interval <TIME>` | <TIME> – время в секундах, принимает значения [1..65535].<br><br>Значение по умолчанию: 40 секунд. |
| 38 | Установить интервал времени в секундах, по истечении которого маршрутизатор повторно отправит пакет, на который не получил подтверждения о получении (например, DatabaseDescription пакет или LinkStateRequest пакеты). | `esr(config-if-gi)# ip ospf retransmit-interval <TIME>`<br>`esr(config-if-gi)# ipv6 ospf retransmit-interval <TIME>` | <TIME> – время в секундах, принимает значения [1..65535].<br><br>Значение по умолчанию: 5 секунд. |

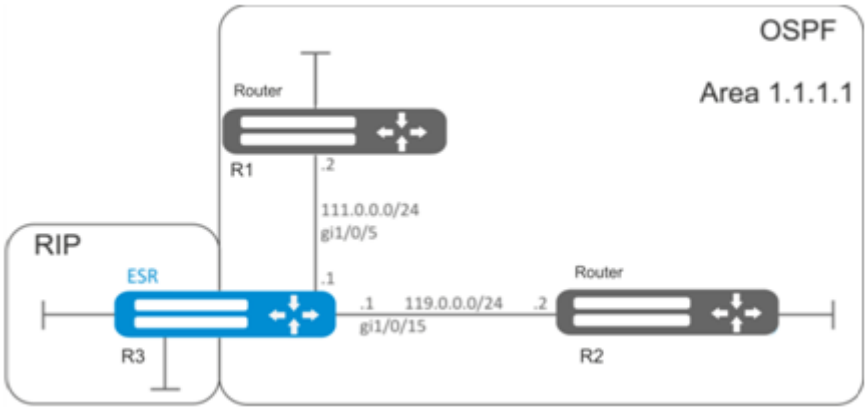
| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 39 | Установить интервал времени в секундах, по истечении которого маршрутизатор отправляет следующий hello-пакет. | `esr(config-if-gi)# ip ospf hello-interval <TIME>` | <TIME> – время в секундах, принимает значения [1..65535].<br><br>Значение по умолчанию: 10 секунд. |
| | | `esr(config-if-gi)# ipv6 ospf hello-interval <TIME>` | |
| 40 | Установить интервал времени в секундах, по истечении которого сосед будет считаться неактивным. Этот интервал должен быть кратным значению hello-interval. | `esr(config-if-gi)# ip dead-interval <TIME>` | <TIME> – время в секундах, принимает значения [1..65535].<br><br>Значение по умолчанию: 40 секунд. |
| | | `esr(config-if-gi)# ipv6 dead-interval <TIME>` | |
| 41 | Установить интервал времени, в течение которого NBMA-интерфейс ждет, прежде чем отправить HELLO-пакет соседу, даже в случае, если сосед неактивен. | `esr(config-if-gi)# ip poll-interval <TIME>` | <TIME> – время в секундах, принимает значения [1 .. 65535].<br><br>Значение по умолчанию: 120 секунд. |
| | | `esr(config-if-gi)# ipv6 poll-interval <TIME>` | |
| 42 | Задать статический IP-адрес соседа для установления отношения в NMBA и P2MP (Point-to-MultiPoint) сетях. | `esr(config-if-gi)# ip ospf neighbor <IP> [ eligible ]` | <IP> – IP-адрес соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].<br><br>**eligible** – опциональный параметр, позволяет устройству участвовать в процессе выбора DR в NBMA-сетях. Приоритет интерфейса должен быть больше нуля. |
| | | `esr(config-if-gi)# ip ospf neighbor <IP> [ eligible ]` | <IPV6-ADDR> – IPv6-адрес соседа, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];<br><br>**eligible** – опциональный параметр, позволяет устройству участвовать в процессе выбора DR в NBMA-сетях. Приоритет интерфейса должен быть больше нуля. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 43 | Определить тип сети для установления OSPF соседства. | `esr(config-if-gi)# ip ospf network <TYPE>`<br>`esr(config-if-gi)# ipv6 ospf network <TYPE>` | <TYPE> – тип сети:<br>• **broadcast** – тип соединения широковещательный;<br>• **non - broadcast** – тип соединения NBMA;<br>• **point - to - multipoint** – тип соединения точка-многоточие;<br>• **point-to-multipoint non-broadcast** – тип соединения NBMA точка-многоточие;<br>• **point - to - point** – тип соединения точка-точка.<br>Значение по умолчанию: broadcast. |
| 44 | Установить приоритет маршрутизатора, который используется для выбора DR и BDR. | `esr(config-if-gi)# ip ospf priority <VALUE>`<br>`esr(config-if-gi)# ipv6 ospf priority <VALUE>` | <VALUE> – приоритет интерфейса, принимает значения [1..65535].<br>Значение по умолчанию: 120. |
| 45 | Установить величину метрики на интерфейсе или туннеле. | `esr(config-if-gi)# ip ospf cost <VALUE>`<br>`esr(config-if-gi)# ipv6 ospf cost <VALUE>` | <VALUE> – величина метрики, задаётся в размере [0..32767].<br>Значение по умолчанию: 150. |
| 47 | Включить протокол BFD для протокола OSPF | `esr(config-if-gi)# ip ospf bfd-enable`<br>`esr(config-if-gi)# ipv6 ospf bfd-enable` | |

### 5.3.2 Пример настройки OSPF

**Задача:**

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




**Решение:**

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

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

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

Создадим и включим требуемую область.

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

Включим анонсирование маршрутной информации из протокола RIP:

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

Включим OSPF-процесс:

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

Соседние маршрутизаторы подключены к интерфейсам gi1/0/5 и gi1/0/15. Для установления соседства с другими маршрутизаторами привяжем их к OSPF-процессу и области. Далее включим на интерфейсе маршрутизацию по протоколу OSPF:

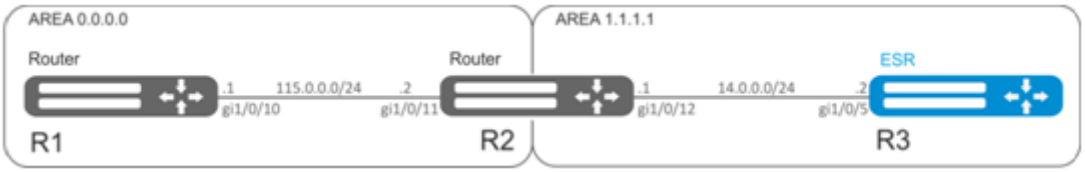
```
esr(config)# interface gigabitethernet 1/0/5
esr(config-if-gi)# ip ospf instance 10
esr(config-if-gi)# ip ospf area 1.1.1.1
esr(config-if-gi)# ip ospf
esr(config-if-gi)# exit
```

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

### 5.3.3 Пример настройки OSPF stub area

**Задача:**

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




**Решение:**

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

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

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

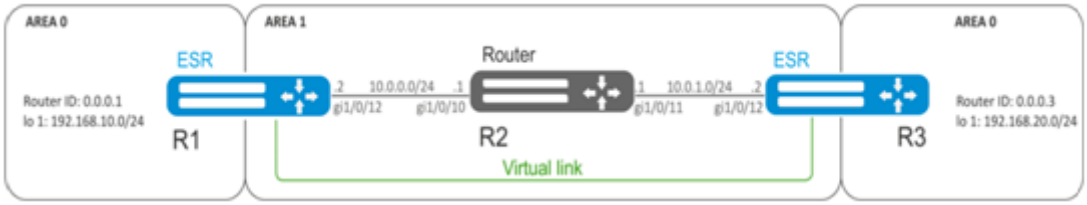
На тупиковом маршрутизаторе R3 включим анонсирование маршрутной информации из протокола RIP:

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

### 5.3.4 Пример настройки Virtual link

**Задача:**

Объединить две магистральные области в одну с помощью virtual link.



**Решение:**

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

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

На маршрутизаторе R1 перейдем в режим конфигурирования области 1.1.1.1:

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

Создадим virtual link с идентификатором 0.0.0.3 и включим его:

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

На маршрутизаторе R3 перейдем в режим конфигурирования области 1.1.1.1:

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

Создадим virtual link с идентификатором 0.0.0.1 и включим его:

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

Рассмотрим таблицу маршрутизации на маршрутизаторе R1:

```
esr# show ip route
C     * 10.0.0.0/24        [0/0]   dev gi1/0/12,                    [direct 00:49:34]
O     * 10.0.1.0/24        [150/20] via 10.0.0.1 on gi1/0/12,       [ospf1 00:49:53]  (0.0.0.3)
O     * 192.168.20.0/24    [150/30] via 10.0.0.1 on gi1/0/12,       [ospf1 00:50:15]  (0.0.0.3)
C     * 192.168.10.0/24    [0/0]   dev lo1,                         [direct 21:32:01]
```

Рассмотрим таблицу маршрутизации на маршрутизаторе R3:

```
esr# show ip route
O     * 10.0.0.0/24        [150/20] via 10.0.1.1 on gi1/0/12,       [ospf1 14:38:35]  (0.0.0.2)
C     * 10.0.1.0/24        [0/0]   dev gi1/0/12,                    [direct 14:35:34]
C     * 192.168.20.0/24    [0/0]   dev lo1,                         [direct 14:32:58]
O     * 192.168.10.0/24    [150/30] via 10.0.1.1 on gi1/0/12,       [ospf1 14:39:54]  (0.0.0.1)
```

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

Для просмотра соседей можно воспользоваться следующей командой:

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

Таблицу маршрутов протокола OSPF можно просмотреть командой:

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

⚠ В firewall необходимо разрешить протокол OSPF (89).

## 5.4 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.

### 5.4.1 Алгоритм настройки

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

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

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 2 | Настроить емкость таблиц маршрутизации протокола BGP (не обязательно при использовании глобальной таблицы маршрутазции). | `esr(config)# ip protocols bgp max-routes <VALUE>`<br>`esr(config)# ipv6 protocols bgp max-routes <VALUE>`<br>`esr(config-vrf)# ip protocols bgp max-routes <VALUE>`<br>`esr(config-vrf)# ipv6 protocols bgp max-routes <VALUE>` | <VALUE> – количество маршрутов протокола BGP в маршрутной таблице, принимает значения в диапазоне:<br>для ESR-1700 [1..5000000];<br>для ESR-1000/1200/1500 [1..3000000];<br>для ESR-20/21/100/200 [1..2000000];<br>для ESR-10/12V(F)/ 14VF [1..800000].<br>Значение по умолчанию для глобальной таблицы маршрутизации:<br>для ESR-1700 (5000000);<br>для ESR-1000/1200/1500 (3000000);<br>для ESR-20/21/100/200 (2000000);<br>для ESR-10/12V/12VF/ 14VF (800000).<br>Значение по умолчанию для VRF:<br>0. |
| 3 | Включить вывод информации о состоянии отношений с соседями для протокола маршрутизации BGP (не обязательно). | `esr(config)# router bgp log-neighbor-changes`<br>`esr(config)# ipv6 router bgp log-neighbor-changes` | |
| 4 | Включить ECMP и определяется максимальное количество равноценных маршрутов до цели. | `esr(config)# router bgp maximum-paths <VALUE>` | <VALUE> – количество допустимых равноценных маршрутов до цели, принимает значения [1..16]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 3 | Выбрать метод фильтрации для передаваемой информации между роутерами. (Обязательно при конфигурировании eBGP для анонсирования подсетей) | | |
| 3.1.1 | При выборе метода фильтрации на основе route-map создать список правил, который в дальнейшем будет использоваться для фильтрации анонсируемых и получаемых IP-маршрутов. | `esr(config)# route-map <NAME>` | <NAME> – имя конфигурируемых правил маршрутизации, задаётся строкой до 31 символа. |
| 3.1.2 | Создать правило | `(config-route-map)# rule <ORDER>` | <ORDER> – номер правила, принимает значения [1 .. 10000]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 3.1.3 | Определить список подсетей, которые затрагиваются правилом. | `esr(config-route-map-rule)#match ip address { <ADDR/LEN> \| object-group <OBJ-GRP-NETNAME> } [ { eq <LEN> \| le <LEN> \| ge <LEN 1> [ le <LEN 2> ] } ]` | <ADDR/LEN> – IP-адрес и маска подсети, задается в виде:<br>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];<br><br><IPV6-ADDR/LEN> – IPv6-адрес и маска подсети, задается в виде:<br>X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128];<br><br><OBJ-GRP-NETNAME> – имя профиля IP -адресов, задаётся строкой до 31 символа*;<br><br><LEN>, <LEN 1>, <LEN 2> – длина префикса, принимает значения [1..32] в IP-списках префиксов для IPv4 и [1..128] для IPv6;<br><br>**eq** – при указании команды длина префикса должна соответствовать указанной;<br><br>**le** – при указании команды длина префикса должна быть меньше либо соответствовать указанной;<br><br>**ge** – при указании команды длина префикса должна быть больше либо соответствовать указанной; |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| | | esr(config-route-map-rule)#match ipv6 address { <IPV6-ADDR/LEN> \| object-group <OBJ-GRP-NETNAME> } [ { eq <LEN> \| le <LEN> \| ge <LEN 1> [ le <LEN 2> ] } ] | **ge** <LEN 1> **le** <LEN 2> – При указании команды длина префикса должна быть больше либо соответствовать <LEN> но меньше или равна <LEN1>.<br><br>* При использовании фильтрации по object-group, их необходимо создать заранее. |
| 3.1.4 | Разрешить (permit) или запретить (deny) действие для указанных подсетей в правеле. | esr(config-route-map-rule)# action {deny \| permit} | |
| 3.2.1 | При выборе метода фильтрации на основе префикс-листов создать списки IP-подсетей, которые в дальнейшем будут использоваться для фильтрации анонсируемых и получаемых IP-маршрутов. | esr(config)# ip prefix-list <NAME><br><br>esr(config)# ipv6 prefix-list <NAME> | <NAME> – имя конфигурируемого списка подсетей, задаётся строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 3.2.2 | Разрешить (permit) или запретить (deny) списки префиксов. | `esr(config-pl)# permit { <ADDR/LEN> \| object-group <OBJ-GRP-NETNAME>} [ { eq <LEN> \| le <LEN> \| ge <LEN 1> [ le <LEN 2> ] } ]` | <ADDR/LEN> – IP-адрес и маска подсети, задается в виде:<br>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];<br><br><IPV6-ADDR/LEN> – IPv6-адрес и маска подсети, задаётся в виде:<br>X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128];<br><br><OBJ-GRP-NETNAME> – имя профиля IP -адресов, задаётся строкой до 31 символа*;<br><br><LEN>, <LEN 1>, <LEN 2> – длина префикса, принимает значения [1..32] в IP-списках префиксов для IPv4 и [1..128] для IPv6;<br><br>**eq** – при указании команды длина префикса должна соответствовать указанной;<br><br>**le** – при указании команды длина префикса должна быть меньше либо соответствовать указанной;<br><br>**ge** – при указании команды длина префикса должна быть больше либо соответствовать указанной; |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| | | esr(config-pl)# deny {<ADDR/LEN> \| object-group <OBJ-GRP-NETNAME>} [ { eq <LEN> \| le <LEN> \| ge <LEN 1> [ le <LEN 2> ] } ] | **ge** <LEN 1> **le** <LEN 2> – При указании команды длина префикса должна быть больше либо соответствовать <LEN> но меньше или равна <LEN1>.<br><br>* При использовании фильтрации по object-group, их необходимо создать заранее. |
| | | esr(config-ipv6-pl)# permit { <IPV6-ADDR/LEN> \| object-group <OBJ-GRP-NETNAME>} [ { eq <LEN> \| le <LEN> \| ge <LEN 1> [ le <LEN 2> ] } ] | |
| | | esr(config-ipv6-pl)# deny {<IPV6-ADDR/LEN> \| object-group <OBJ-GRP-NETNAME> } [ { eq <LEN> \| le <LEN> \| ge <LEN 1> [ le <LEN 2> ] } ] | |
| 4 | Добавить BGP-процесс в систему и осуществить переход в режим настройки параметров BGP-процесса. | esr(config)# router bgp <AS> | <AS> – номер автономной системы процесса, принимает значения [1..4294967295]. |
| 5 | Установить идентификатор маршрутизатора. | esr(config-bgp)# router-id <ID> | <ID> – идентификатор маршрутизатора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 6 | Установить идентификатор Route-Reflector кластера, которому принадлежит BGP-процесс маршрутизатора. (При необходимости) | esr(config-bgp)# cluster-id <ID> | <ID> – идентификатор Route-Reflector кластера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 7 | Включить генерацию и отправку маршрута по умолчанию, если маршрут по умолчанию есть в таблице маршрутизации FIB. (не обязательно) | esr(config-bgp)# default-information-originate | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 8 | Установить временной интервал, по истечении которого идет проверка соединения со встречной стороной. (Не обязательно) | `esr(config-bgp-af)# timers keeaplive <TIME>` | <TIME> – время в секундах, принимает значения [1..65535].<br><br>Значение по умолчанию: 60 секунд. |
| 9 | Установить временной интервал, по истечении которого встречная сторона считается недоступной. (Не обязательно) | `esr(config-bgp-af)# timers holdtime <TIME>` | <TIME> – время в секундах, принимает значения [1..65535].<br><br>Значение по умолчанию: 180 секунд. |
| 10 | Установить время минимальной и максимальной задержки, в течение которого запрещено устанавливать соединение, в целях защиты от частых разрывов соединения (Не обязательно) | `esr(config-bgp-af)# timers error-wait <TIME1> <TIME2>` | <TIME1> – время минимальной задержки в секундах, принимает значения [1..65535];<br><br><TIME2> – время максимальной задержки в секундах, принимает значения [1..65535]. |
| 11 | Определить глобальный алгоритм аутентификации с соседями (При необходимости). | `esr(config-bgp)# authentication algorithm <ALGORITHM>` | <ALGORITHM> – алгоритм шифрования:<br><br>md5 – пароль шифруется по алгоритму md5.<br><br>Значение по умолчанию: Шифрование не используется |
| 12 | Установить глобальный пароль для аутентификации с соседями. (Используется совместно с "authentication algorithm") | `esr(config-bgp)# authentication key ascii-text { <CLEAR-TEXT> \| encrypted <ENCRYPTED-TEXT> }` | <CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов;<br><br><ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...). |
| 13 | Активировать BGP-процесс. | `esr(config-bgp)# enable` | |
| 14 | Определить тип конфигурируемой маршрутной информации и перейти в данный режим настройки. | `esr(config-bgp)# address-family { ipv4 \| ipv6 } unicast` | – **ipv4** – семейство IPv4;<br><br>– **ipv6** – семейство IPv6; |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 15 | Включить анонсирование маршрутов процессом BGP полученных альтернативным образом (При необходимости). | `esr(config-bgp-af)# redistribute static [ route-map <NAME> ]` | <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых статических маршрутов, задаётся строкой до 31 символа. |
| | | `esr(config-bgp-af)# redistribute connected [ route-map <NAME> ]` | <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых напрямую подключенных подсетей, задаётся строкой до 31 символа. |
| | | `esr(config-bgp-af)# redistribute rip [ route-map <NAME> ]` | <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых RIP-маршрутов, задаётся строкой до 31 символа. |

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

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 16 | Включить анонсирование подсетей. | `esr(config-bgp-af)# network <ADDR/LEN>` | <ADDR/LEN> – адрес подсети, указывается в одном из следующих формате:<br><br>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];<br><br>X:X:X:X::X/EE – IPv6-адрес и маска подсети, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128]. |
| 17 | Осуществить выход из режима глобального конфигурирования анонсов маршрутной информации процесса BGP | `esr(config-bgp-af)# exit` | |
| 18 | Добавить BGP-соседа и осуществить переход в режим настройки параметров BGP-соседа. | `esr(config-bgp)# neighbor <ADDR>\|<IPV6-ADDR>` | <ADDR> – IP-адрес соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];<br><br><IPV6-ADDR> – IPv6-адрес клиента, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. |
| 19 | Задать описание соседа (не обязательно). | `esr(config-bgp-neighbor)# description <DESCRIPTION>` | <DESCRIPTION> – описание соседа, задаётся строкой до 255 символов. |
| 20 | Установить временной интервал, по истечении которого идет проверка соединения со встречной стороной. (не обязательно) | `esr(config-bgp-neighbor)# timers keepalive <TIME>` | <TIME> – время в секундах, принимает значения [1..65535].<br><br>Значение по умолчанию: 60 секунд. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 21 | Установить временной интервал, по истечении которого встречная сторона считается недоступной (не обязательно). | `esr(config-bgp- neighbor)# timers holdtime <TIME>` | <TIME> – время в секундах, принимает значения [1..65535].<br><br>Значение по умолчанию: 180 секунд. |
| 22 | Установить время минимальной и максимальной задержки, в течение которого запрещено устанавливать соединение, в целях защиты от частых разрывов соединения (не обязательно). | `esr(config-bgp-af)# timers error-wait <TIME1> <TIME2>` | <TIME1> – время минимальной задержки в секундах, принимает значения [1..65535];<br><br><TIME2> – время максимальной задержки в секундах, принимает значения [1..65535].<br><br>Значение по умолчанию: 60 и 300 секунд |
| 23 | Установить номер автономной системы BGP-соседа. | `esr(config-bgp-neighbor)# remote-as <AS>` | <AS> – номер автономной системы, принимает значения [1..4294967295]. |
| 24 | Разрешить подключение к соседям, которые находятся не в напрямую подключенных подсетях (не обязательно) | `esr(config-bgp-neighbor)# ebgp-multihop <NUM>` | <NUM> – Максимальное количество хопов при установке<br>EBGP (используется для TTL). |
| 25 | Указать, что BGP-сосед является Route-Reflector клиентом. (не обязательно) | `esr(config-bgp-neighbor)# route-reflector-client` | |
| 26 | Задать IP/IPv6-адрес маршрутизатора, который будет использоваться в качестве IP/IPv6-адреса источника в отправляемых обновлениях маршрутной информации BGP. (не обязательно) | `esr(config-bgp-neighbor)# update-source { <ADDR> \| <IPV6-ADDR> }` | <ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];<br><br><IPV6-ADDR> – IPv6-адрес источника, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 27 | Включить режим, в котором разрешен приём маршрутов в BGP-атрибуте, AS Path которых содержит номера автономной системы процесса. (не обязательно) | `esr(config-bgp-neighbor)# allow-local-as <NUMBER>` | <NUMBER> – пороговое число вхождений номера автономной системы процесса в атрибуте AS Path, при которых маршрут будет принят, диапазон допустимых значений [1..10]. |
| 28 | Включить BFD-протокол на конфигурируемом BGP-соседе. (не обязательно, используется совместно с параметром update-source) | `esr(config-bgp-neighbor)# bfd-enable` | |
| 29 | Определить алгоритм аутентификации с соседом. (не обязательно) | `esr(config-bgp-neighbor)# authentication algorithm <ALGORITHM>` | <ALGORITHM> – алгоритм шифрования:<br><br>md5 – пароль шифруется по алгоритму md5. |
| 30 | Установить пароль для аутентификации с соседом. (не обязательно) | `esr(config-bgp-neighbor)# authentication key ascii-text { <CLEAR-TEXT> \| encrypted <ENCRYPTED-TEXT> }` | <CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов;<br><br><ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...). |
| 31 | Сделать соседство активным | `esr(config-bgp-neighbor)# enable` | |
| 32 | Определить тип конфигурируемой маршрутной информации соседа и перейти в данный режим настройки. | `esr(config-bgp-neighbor)# address-family { ipv4 \| ipv6 \| vpnv4 } unicast` | – **ipv4** – семейство IPv4;<br><br>– **ipv6** – семейство IPv6;<br><br>– **vpnv4** – семейство VPNv4; |
| 33 | При выборе режима фильтрации на основе префикс-листов добавить фильтрацию подсетей во входящих или исходящих обновлениях (Обязательно при конфигурировании eBGP для анонсирования подсетей). | `esr(config-bgp-neighbor-af)# prefix-list <PREFIX-LIST-NAME> { in \| out }` | <PREFIX-LIST-NAME> – имя сконфигурированного списка подсетей, задаётся строкой до 31 символа.<br><br>**in** – фильтрация входящих маршрутов;<br><br>**out** – фильтрация анонсируемых маршрутов. |

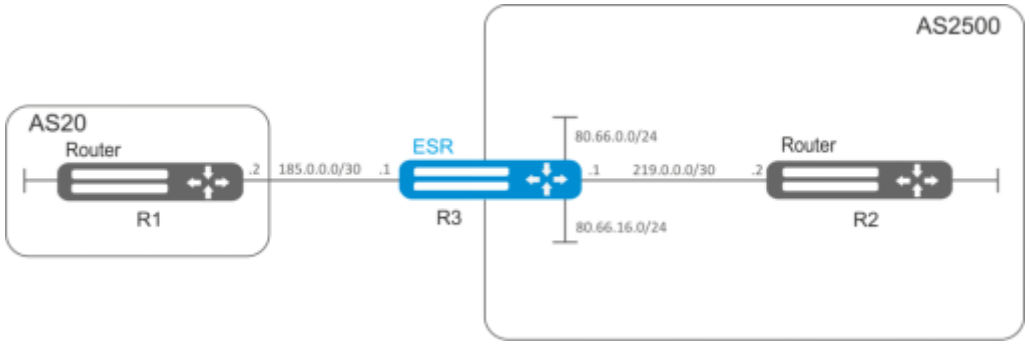
| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 34 | Задать режим, в котором BGP-соседу в обновлении на ряду с другими маршрутами всегда отправляется маршрут по умолчанию. (не обязательно, отсутствует для vpnv4) | `esr(config-bgp-neighbor-af)# default-originate` | |
| 35 | Задать режим, в котором все обновления отправляются BGP-соседу с указанием в качестве next-hop IP-адреса исходящего интерфейса локального маршрутизатора.<br>(не обязательно, отсутствует для vpnv4) | `esr(config-bgp-neighbor-af)# next-hop-self` | |
| 36 | Определить приоритетность маршрутов, получаемых от соседа. (не обязательно) | `esr(config-bgp-neighbor-af)# preference <VALUE>` | <VALUE> – приоритетность маршрутов соседа, принимает значения в диапазоне [1..255].<br><br>Значение по умолчанию: 170. |
| 37 | Задать режим, в котором перед отправлением обновления из BGP-атрибута AS Path маршрутов удаляются приватные номера автономных систем (в соответствии с RFC 6996). (не обязательно, отсутствует для vpnv4) | `esr(config-bgp-neighbor-af)# remove-private-as [ { all \| nearest \| replace } ]` | **all** - удалить все частные номера AS из AS-path;<br><br>**nearest** - Заменить ближайшие частные AS в AS-path на рядомстоящую публичную AS;<br><br>**replace** - Заменить все частные номера AS номером текущего процесса BGP.<br><br>Значение по умолчанию: all. |
| 38 | Включить обмен маршрутной информацией | `esr(config-bgp-neighbor-af)# enable` | |

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

### 5.4.2 Пример настройки

**Задача:**

Настроить BGP-протокол на маршрутизаторе R3 со следующими параметрами:




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

**Решение:**

Сконфигурируем необходимые сетевые интерфейсы:

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

Сконфигурируем firewall для приема маршрутазтором BGP-трафика из зоны безопасности WAN

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

И укажем принадлежность интерфейсов к зоне безопасности

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

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

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

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

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

Сконфигурируем анонсирование подсетей, подключенных напрямую:

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

Создадим соседство с роутером R2 по iBGP

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

И включим обмен ipv4-маршрутами

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

Создадим соседство с роутером R1 по eBGP

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

И включим обмен ipv4-маршрутами, резрешив необходимые маршруты для анонса при помощи заранее подготовленного route-map

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

Включим работу протокола

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

Информацию о BGP-пирах можно посмотреть командой:

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

Таблицу маршрутов протокола BGP можно просмотреть с помощью команды:

```
esr# show ip bgp
```

## 5.5 Настройка BFD

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

### 5.5.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Активировать BFD для протокола OSPF на интерфейсе | `esr(config-if-gi)# ip ospf bfd-enable` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 2 | Активировать BFD для протокола BGP neighbor на интерфейсе | `esr(config-bgp-neighbor)# bfd-enable` | |
| 3 | Задать интервал, по истечении которого происходит отправка BFD-сообщения соседу. Глобально (не обязательно) | `esr(config)# ip bfd idle-tx-interval <TIMEOUT>` | <TIMEOUT> – интервал, по истечении которого происходит отправка BFD-пакета, принимает значение в миллисекундах в диапазоне [200..65535] для ESR-1000/1200/1500/1700 и [300..65535] для ESR-10/12V(F)/14VF/ 20/21/100/200<br><br>По умолчанию 1 секунда |
| 4 | Включить логирование изменений состояния BFD-протокола (не обязательно) | `esr(config)# ip bfd log-adjacency-changes` | |
| 5 | Задать минимальный интервал, по истечении которого сосед должен сгенерировать BFD-сообщение. Глобально (не обязательно) | `esr(config)# ip bfd min-rx-interval <TIMEOUT>` | <TIMEOUT> – интервал, по истечении которого должна происходить отправка BFD-сообщения соседом, принимает значение в миллисекундах в диапазоне [200..65535] для ESR-1000/1200/1500/1700 и [300..65535] для ESR-10/12V(F)/14VF/ 20/21/100/200<br><br>По умолчанию:<br>• 300 миллисекунд на ESR-10/12V(F)/14VF/ 20/21/100/200<br>• 200 миллисекунд на ESR-1000/1200/1500/1700 |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 6 | Задать минимальный интервал, по истечении которого происходит отправка BFD-сообщения соседу. Глобально<br>(не обязательно) | `esr(config)# ip bfd min-tx-interval <TIMEOUT>` | <TIMEOUT> – интервал, по истечении которого должна происходить отправка BFD-сообщения соседом, принимает значение в миллисекундах в диапазоне [200..65535] для ESR-1000/1200/1500/1700 и [300..65535] для ESR-10/12V(F)/14VF/ 20/21/100/200<br><br>По умолчанию:<br>• 300 миллисекунд на ESR-10/12V(F)/14VF/ 20/21/100/200<br>• 200 миллисекунд на ESR-1000/1200/1500/1700 |
| 7 | Задать число пропущенных пакетов, после достижения которого BFD-сосед считается недоступным. Глобально | `esr(config)# ip bfd multiplier <COUNT>` | <COUNT> – число пропущенных пакетов, после достижения которого сосед считается недоступным, принимает значение в диапазоне [1..100].<br><br>По умолчанию: 5 |
| 8 | Запустить работу механизма BFD с определенным IP-адресом. | `esr(config)# ip bfd neighbor <ADDR> [ { interface <IF> \| tunnel <TUN> } ] [local-address <ADDR> [multihop]] [vrf <VRF>]` | <ADDR> – IP-адрес шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];<br><br><IF> – интерфейс или группы интерфейсов;<br><br><TUN> – тип и номер туннеля;<br><br><VRF> – имя экземпляра VRF, задается строкой до 31 символа;<br><br>multihop – ключ для установки TTL=255, для работы механизма BFD через маршрутизируемую сеть. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 9 | Перевести BFD-сессию в пассивный режим, то есть BFD-сообщения не будут отправляться до тех пор, пока не будут получены сообщения от BFD-соседа. Глобально<br><br>(не обязательно) | `esr(config)# ip bfd passive` | |
| 10 | Задать интервал, по истечении которого происходит отправка BFD-сообщения соседу.<br>На интерфейсе<br>(не обязательно) | `esr(config-if-gi)# ip bfd idle-tx-interval <TIMEOUT>` | <TIMEOUT> – интервал, по истечении которого происходит отправка BFD-пакета, принимает значение в миллисекундах в диапазоне [200..65535] для ESR-1000/1200/1500/1700 и [300..65535] для ESR-10/12V(F)/14VF/ 20/21/100/200.<br><br>По умолчанию: 1 секунда |
| 11 | Задать минимальный интервал, по истечении которого сосед должен сгенерировать BFD-сообщение.<br>На интерфейсе<br>(не обязательно) | `esr(config-if-gi)# ip bfd min-rx-interval <TIMEOUT>` | <TIMEOUT> – интервал, по истечении которого должна происходить отправка BFD-сообщения соседом, принимает значение в миллисекундах в диапазоне [200..65535] для ESR-1000/1200/1500/1700 и [300..65535] для ESR-10/12V(F)/14VF/ 20/21/100/200<br><br>По умолчанию:<br>• 300 миллисекунд на ESR-10/12V(F)/14VF/ 20/21/100/200<br>• 200 миллисекунд на ESR-1000/1200/1500/1700 |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 12 | Задать минимальный интервал, по истечении которого происходит отправка BFD-сообщения соседу. На интерфейсе (не обязательно) | `esr(config-if-gi)# ip bfd min-tx-interval <TIMEOUT>` | <TIMEOUT> – интервал, по истечении которого должна происходить отправка BFD-сообщения соседом, принимает значение в миллисекундах в диапазоне [200..65535] для ESR-1000/1200/1500/1700 и [300..65535] для ESR-10/12V(F)/14VF/ 20/21/100/200<br><br>По умолчанию:<br>• 300 миллисекунд на ESR-10/12V(F)/14VF/ 20/21/100/200<br>• 200 миллисекунд на ESR-1000/1200/1500/1700 |
| 13 | Задать число пропущенных пакетов, после достижения которого BFD-сосед считается недоступным. На интерфейсе<br><br>(не обязательно) | `esr(config-if-gi)# ip bfd multiplier <COUNT>` | <COUNT> – число пропущенных пакетов, после достижения которого сосед считается недоступным, принимает значение в диапазоне [1..100].<br><br>По умолчанию: 5 |
| 14 | Перевести BFD-сессию в пассивный режим, то есть BFD-сообщения не будут отправляться до тех пор, пока не будут получены сообщения от BFD-соседа. На интерфейсе (не обязательно) | `esr(config-if-gi)# ip bfd passive` | |

### 5.5.2 Пример настройки BFD с BGP

**Задача:**

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

**Решение:**

1. Конфигурирование R1
   Предварительно необходимо настроить интерфейс Gi1/0/1:

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

   Настроим eBGP с BFD:

```
esr(config)# router bgp 100
esr(config-bgp)# address-family ipv4
esr(config-bgp-af)# neighbor 10.0.0.2
esr(config-bgp-neighbor)# remote-as 200
esr(config-bgp-neighbor)# update-source 10.0.0.1
esr(config-bgp-neighbor)# bfd-enable
esr(config-bgp-neighbor)# enable
esr(config-bgp-neighbor)# ex
esr(config-bgp-af)# enable
esr(config-bgp-af)# exit
```

2. Конфигурирование R2
   Предварительно необходимо настроить интерфейс Gi1/0/1:

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

   Настроим eBGP с BFD:

```
esr(config)# router bgp 200
esr(config-bgp)# address-family ipv4
esr(config-bgp-af)# neighbor 10.0.0.1
esr(config-bgp-neighbor)# remote-as 100
esr(config-bgp-neighbor)# update-source 10.0.0.2
esr(config-bgp-neighbor)# bfd-enable
esr(config-bgp-neighbor)# enable
esr(config-bgp-neighbor)# ex
esr(config-bgp-af)# enable
esr(config-bgp-af)# exit
```

## 5.6 Настройка политики маршрутизации PBR

### 5.6.1 Алгоритм настройки Route-map для BGP

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

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

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Создать маршрутную карту для фильтрации и модификации IP-маршрутов. | `esr(config)# route-map <NAME>` | <NAME> – имя маршрутной карты, задается строкой до 31 символа. |
| 2 | Создать правило маршрутной карты. | `esr(config-route-map)# rule <ORDER>` | <ORDER> – номер правила, принимает значения [1 .. 10000]. |
| 3 | Указать действие, которое должно быть применено для маршрутной информации. | `esr(config-route-map-rule)# action <ACT>` | <ACT> – назначаемое действие:<br>• **permit** – прием или анонсирование маршрутной информации разрешено;<br>• **deny** – запрещено. |
| 4 | Задать значение атрибута BGPAS-Path в маршруте, для которого должно срабатывать правило (не обязательно). | `esr(config-route-map-rule)# match as-path [begin \| end \| contain] <AS-PATH>` | <AS-PATH> – список номеров автономных систем, задается в виде AS,AS,AS, принимает значения [1..4294967295]. Опциональные параметры:<br>• **begin** – значение атрибута начинается с указанных номеров AS;<br>• **end** – значение атрибута заканчивается указанными номерами AS;<br>• **contain** – значение атрибута содержит указанный список номеров AS. |
| 5 | Задать значение атрибута BGPCommunity, для которого должно срабатывать правило (не обязательно). | `esr(config-route-map-rule)# match community <COMMUNITY-LIST>` | <COMMUNITY-LIST> – список community, задается в виде AS:N,AS:N, принимает значения [1..4294967295]. Можно указать до 64 community. |
| 6 | Задать значение атрибута BGPExtendedCommunity, для которого должно срабатывать правило (не обязательно). | `esr(config-route-map-rule)# match extcommunity <EXTCOMMUNITY-LIST>` | <EXTCOMMUNITY-LIST> – список extcommunity, задается в виде KIND:AS:N, KIND:AS:N, где<br>KIND – тип extcommunity:<br>• **rt**(Route Target);<br>• **ro** (Route Origin);<br>N – номер extcommunity, принимает значения [1..65535]. |
| 7 | Задать профиль IP-адресов, содержащий значения подсетей назначения в маршруте (не обязательно). | `esr(config-route-map-rule)# match ip address object-group <OBJ-GROUP- NETWORK -NAME>` | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, содержащего префиксы подсетей назначения, задаётся строкой до 31 символа. |

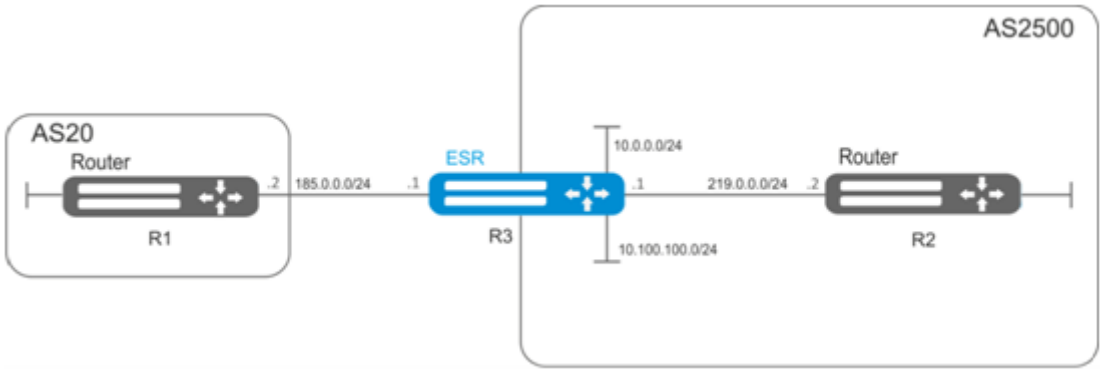
| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| | | esr(config-route-map-rule)# match ipv6 address object-group <OBJ-GROUP- NETWORK -NAME> | |
| 8 | Задать профиль IP-адресов, содержащий значения атрибута BGPNext-Hop в маршруте для которого должно срабатывать правило (не обязательно). | esr(config-route-map-rule)#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

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

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 19 | Задать атрибут BGP Next-Hop, который будет установлен в маршруте при анонсировании (не обязательно). | `esr(config-route-map-rule)# action set ip bgp-next-hop <ADDR>` | <ADDR> – IP-адрес шлюза, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| | | `esr(config-route-map-rule)# action set ipv6 bgp-next-hop <IPV6-ADDR>` | <IPV6-ADDR> – IPv6-адрес шлюза, задается в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. |
| 20 | Задать значение Next-Hop, которое будет установлено в маршруте, полученном по BGP (не обязательно). | `esr(config-route-map-rule)# action set ip next-hop {NEXTHOP> \| blackhole \| unreachable \| prohibit}` | <NEXTHOP> – IP-адрес шлюза задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];<br>• **blackhole** – пакеты до данной подсети будут удаляться без отправки уведомлений отправителю;<br>• **unreachable** – пакеты до данной подсети будут удаляться, отправитель получит в ответ ICMP Destination unreachable (Host unreachable, code 1);<br>• **prohibit** – пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMPDestinationunreachable (Communication administratively prohibited code 13). |
| | | `esr(config-route-map-rule)# action set ipv6 next-hop <IPV6-NEXTHOP>` | <IPV6-NEXTHOP> – IPv6-адрес шлюза, задается в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. |
| 21 | Задать значение атрибута BGP Local Preference, который будет установлен в маршруте (не обязательно). | `esr(config-route-map-rule)# action set local-preference <PREFERENCE>` | <PREFERENCE> – значение атрибута BGP Local Preference, принимает значения [0..255]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 22 | Задать значение атрибута BGP Origin, которое будет установлено в маршруте (не обязательно). | `esr(config-route-map-rule)# action set origin <ORIGIN>` | <ORIGIN> – значение атрибута BGP Origin:<br>• **egp** – маршрут выучен по протоколу EGP;<br>• **igp** – маршрут получен внутри исходной AS;<br>• **incomplete** – маршрут выучен другим образом. |
| 23 | Задать значение BGP MED, которое будет установлено в маршруте (не обязательно). | `esr(config-route-map-rule)# action set metric bgp <METRIC>` | <METRIC> – значение атрибута BGP MED, принимает значения [0..4294967295]. |
| 24 | Добавить фильтрацию и модификацию маршрутов во входящих или исходящих направлениях. | `esr(config-bgp-neighbor)# route-map <NAME><DIRECTION>`<br>`esr(config-ipv6-bgp-neighbor)# route-map <NAME><DIRECTION>` | <NAME> – имя сконфигурированной маршрутной карты;<br><DIRECTION> – направление:<br>• **in** – фильтрация и модификация получаемых маршрутов;<br>• **out** – фильтрация и модификация анонсируемых маршрутов. |

### 5.6.2 Пример настройки 1. Route-map для BGP




**Задача:**

Назначить community для маршрутной информации, приходящей из AS 20:

Предварительно нужно выполнить следующие действия:

- Настроить BGP с AS 2500 на маршрутизаторе ESR;
- Установить соседство с AS20.

**Решение:**

Создаем политику:

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

Создаем правило 1:

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

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

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

В BGP процессе AS 2500 заходим в настройки параметров соседа:

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

Привязываем политику к принимаемой маршрутной информации:

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

### 5.6.3 Пример настройки 2. Route-map для BGP

**Задача:**

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

**Предварительно:**

Настроить BGP с AS 2500 на ESR

**Решение:**

Создаем политику:

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

Создаем правило:

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

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

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

В BGP процессе AS 2500 заходим в настройки параметров соседа:

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

Привязываем политику к анонсируемой маршрутной информации:

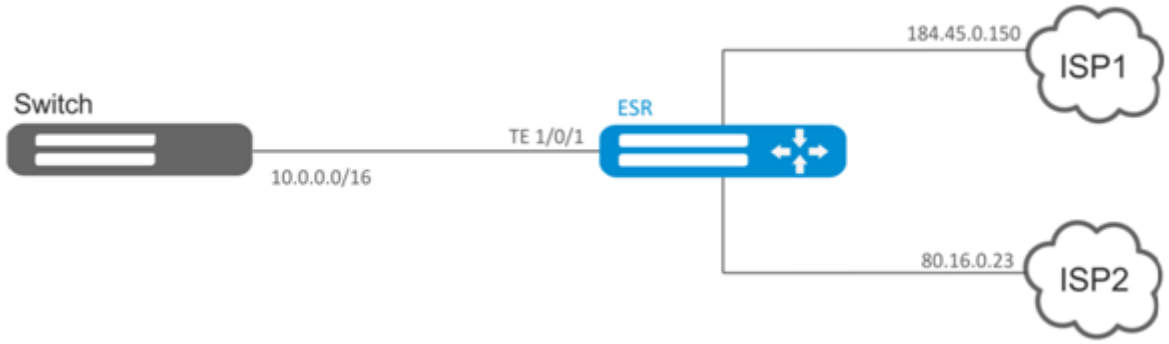
```
esr(config-bgp-neighbor)# route-map to-as20 out
esr(config-bgp-neighbor)# exit
esr(config-bgp)# exit
esr(config)# exit
```

### 5.6.4 Алгоритм настройки Route-map на основе списков доступа (Policy-based routing)

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Создать маршрутную карту для фильтрации и модификации IP-маршрутов. | `esr(config)# route-map <NAME>` | <NAME> – имя маршрутной карты, задаётся строкой до 31 символа. |
| 2 | Создать правило маршрутной карты | `esr(c onfig-route-map)# rule <ORDER>` | <ORDER> – номер правила, принимает значения [1 .. 10000]. |
| 3 | Указать действие, которое должно быть применено для маршрутной информации. | `esr(config-route-map-rule)# action <ACT>` | <ACT> – назначаемое действие:<br>• **permit** – прием или анонсирование маршрутной информации разрешено;<br>• **deny** – запрещено. |
| 4 | Задать ACL, для которого должно срабатывать правило (не обязательно). | `esr(config-route-map-rule)# match ip access-group <NAME>` | <NAME> – имя списка контроля доступа, задаётся строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 5 | Задать Next-Hop для пакетов, которые попадают под критерии в указанном списке доступа (ACL) (не обязательно). | `esr(config-route-map-rule)# action set ip next-hop verify-availability <NEXTHOP><METRIC>` | <NEXTHOP> – IP-адрес шлюза задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];<br><br><METRIC> – метрика маршрута, принимает значения [0..255]. |
| 6 | Назначить политику маршрутизации на основе списков доступа (ACL). | `esr(config-if-gi)# ip policy route-map <NAME>` | <NAME> – имя сконфигурированной политики маршрутизации, строка до 31 символа. |

### 5.6.5 Пример настройки Route-map на основе списков доступа (Policy-based routing)




**Задача:**

Распределить трафик между Интернет провайдерами на основе подсетей пользователей.

Предварительно нужно назначить IP-адреса на интерфейсы.

Требуется направлять трафик с адресов 10.0.20.0/24 через ISP1 (184.45.0.150), а трафик с адресов 10.0.30.0/24 – через ISP2 (80.16.0.23). Требуется контролировать доступность адресов провайдеров (работоспособность подключений к ISP), и при неработоспособности одного из подключений переводить с него на рабочее подключение весь трафик.

**Решение:**

Создаем ACL:

```
esr# configure
esr(config)# ip access-list extended sub20
esr(config-acl)# rule 1
esr(config-acl-rule)# match source-address 10.0.20.0 255.255.255.0
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# action permit
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit
esr(config)# ip access-list extended sub30
esr(config-acl)# rule 1
esr(config-acl-rule)# match source-address 10.0.30.0 255.255.255.0
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# action permit
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit
```

Создаем политику:

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

Создаем правило 1:

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

Указываем список доступа (ACL) в качестве фильтра:

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

Указываем next-hop для sub20:

```
esr(config-route-map-rule)# action set ip next-hop verify-availability 184.45.0.150 10
esr(config-route-map-rule)# action set ip next-hop verify-availability 80.16.0.23 30
esr(config-route-map-rule)# exit
esr(config-route-map)# exit
```

Правилом 1 будет обеспечена маршрутизация трафика из сети 10.0.20.0/24 на адрес 184.45.0.150, а при его недоступности – на адрес 80.16.0.23. Приоритетность шлюзов задается значениями метрик – 10 и 30.

Создаем правило 2:

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

Указываем список доступа (ACL) в качестве фильтра:

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

Указываем nexthop для sub30 и выходим:

```
esr(config-route-map-rule)# action set ip next-hop verify-availability 80.16.0.23 10
esr(config-route-map-rule)# action set ip next-hop verify-availability 184.45.0.150 30
esr(config-route-map-rule)# exit
esr(config-route-map)# exit
```

Правилом 2 будет обеспечена маршрутизация трафика из сети 10.0.30.0/24 на адрес 80.16.0.23, а при его недоступности – на адрес 184.45.0.150. Приоритетность задается значениями метрик.

Заходим на интерфейс TE 1/0/1:

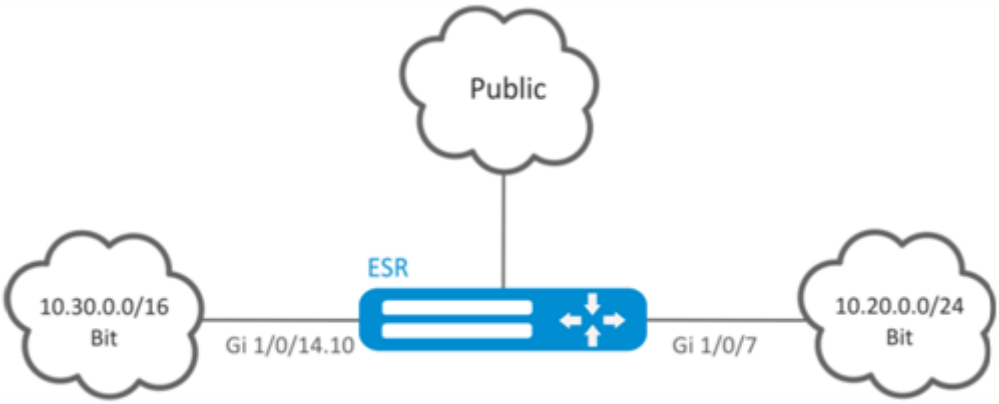
```
esr(config)# interface tengigabitethernet 1/0/1
```

Привязываем политику на соответствующий интерфейс:

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

## 5.7 Настройка VRF Lite

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




### 5.7.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Создать экземпляр VRF и перейти в режим настройки параметров экземпляра VRF. | `esr(config)# ip vrf <VRF>` | <VRF> – имя экземпляра VRF, задается строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 2 | Назначить описание конфигурируемомого экземпляра VRF. | `esr(config-vrf)# description <DESCRIPTION>` | <DESCRIPTION> – описание экземпляра VRF, задаётся строкой до 255 символов. |
| 3 | Настроить емкость таблиц маршрутизации в конфигурируемом VRF для IPv4/IPv6 протоколов маршрутизации (не обязательно). | `esr(config-vrf)# ip protocols <PROTOCOL> max-routes <VALUE>`<br>`esr(config-vrf)#ipv6 protocols <PROTOCOL> max-routes <VALUE>` | <PROTOCOL> – вид протокола, принимает значения: ospf, bgp;<br><br><VALUE> – количество маршрутов в маршрутной таблице, принимает значения в диапазоне:<br><br>OSPF ESR-1000/1200/1500/1700 [1..500000], ESR-20/21/100/200 [1..300000], ESR-10/12V(F)/14VF [1..30000]<br><br>BGP ESR-1000/1200/1500/1700 [1..2800000], ESR-20/21/100/200 [1..1500000], ESR-10/12V(F)/14VF [1..800000].<br><br>Значение по умолчанию: 0 |
| 4 | Включить и настроить протоколы динамической маршрутизации трафика (Static/OSPF/BGP/IS-IS) в экземпляре VRF (не обязательно). См. соответствующий раздел Конфигурирование статических маршрутов, Настройка OSPF и Настройка BGP. | | |
| 5 | В режиме конфигурирования физического/логического интерфейса, туннеля, правила DNAT/SNAT, DAS-сервера или SNMPv3 пользователя указать имя экземпляра VRF для которого будет использоваться (при необходимости). | `esr(config-snat-ruleset)# ip vrf forwarding <VRF>` | <VRF> – имя экземпляра VRF, задается строкой до 31 символа. |
| 6 | Настроить LT-туннель для передачи трафика в глобальный режим или другие VRF (при необходимости). | | см. раздел Настройка LT-туннелей |

### 5.7.2 Пример настройки

**Задача:**

К маршрутизатору серии ESR подключены 2 сети, которые необходимо изолировать от остальных сетей.

**Решение:**

Создадим VRF:

```
esr(config)# ip vrf bit
esr(config-vrf)# exit
```

Создадим зону безопасности:

```
esr(config)# security zone vrf-sec
esr(config-zone)# ip vrf forwarding bit
esr(config-zone)# exit
```

Создадим правило для пары зон и разрешим любой TCP/UDP-трафик:

```
esr(config)# security zone-pair vrf-sec vrf-sec
esr(config-zone-pair)# rule 1
esr(config-zone-rule)# match source-address any
esr(config-zone-rule)# match destination-address any
esr(config-zone-rule)# match protocol udp
esr(config-zone-rule)# match source-port any
esr(config-zone-rule)# match destination-port any
esr(config-zone-rule)# action permit
esr(config-zone-rule)# enable
esr(config-zone-rule)# exit
esr(config-zone-pair)# rule 2
esr(config-zone-rule)# match source-address any
esr(config-zone-rule)# match destination-address any
esr(config-zone-rule)# match protocol tcp
esr(config-zone-rule)# match source-port any
esr(config-zone-rule)# match destination-port any
esr(config-zone-rule)# action permit
esr(config-zone-rule)# enable
esr(config-zone-rule)# exit
```

Создадим привязку интерфейсов, назначим IP-адреса, укажем принадлежность к зоне:

```
esr(config)# interface gigabitethernet 1/0/7
esr(config-if-gi)# ip vrf forwarding bit
esr(config-if-gi)# ip address 10.20.0.1/24
esr(config-if-gi)# security-zone vrf-sec
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/14.10
esr(config-subif)# ip vrf forwarding bit
esr(config-subif)# ip address 10.30.0.1/16
esr(config-subif)# security-zone vrf-sec
esr(config-subif)# exit
esr(config)# exit
```

Информацию об интерфейсах, привязанных к VRF, можно посмотреть командой:

```
esr# show ip vrf
```

Таблицу маршрутов VRF можно просмотреть с помощью команды:

```
esr# show ip route vrf bit
```

## 5.8 Настройка MultiWAN

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

### 5.8.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Сконфигурировать интерфейсы, по которым будет работать MultiWAN: установить ip-адреса и указать security-zone. | | |
| 2 | Прописать статические маршруты через WAN (если необходимо). | `esr(config)# ip route <SUBNET> wan load-balance rule <ID> [<METRIC>]` | <ID> – идентификатор создаваемого правила из п.2.<br><br>[METRIC] – метрика маршрута, принимает значения [0..255]. |
| 3 | Создать правило WAN и перейти в режим настройки параметров правила. | `esr(config)# wan load-balance rule <ID>` | <ID> – идентификатор создаваемого правила, принимает значения [1..50]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 4 | Задать интерфейсы или туннели, которые являются шлюзами в маршруте, создаваемом службой MultiWAN. | `esr(config-wan-rule)# outbound { interface <IF> \| tunnel <TUN> } [WEIGHT]` | <IF>– имя интерфейса;<br><br><TUN> – имя туннеля;<br><br>[WEIGHT] – вес туннеля или интерфейса, определяется в диапазоне [1..255]. Если установить значение 2, то по данному интерфейсу будет передаваться в 2 раза больше трафика, чем по интерфейсу со значением по умолчанию. В режиме резервирования активным будет маршрут с наибольшим весом. Значение по умолчанию 1. |
| 5 | Описать правила (не обязательно). | `esr(config-wan-rule)# description <DESCRIPTION>` | <DESCRIPTION> – описание правила wan, задаётся строкой до 255 символов. |
| 6 | Данной командой осуществляется переключение из режима балансировки в режим резервирования (если необходимо). | `esr(config-wan-rule)# failover` | |
| 7 | Включить wan правило. | `esr(config-wan-rule)# enable` | |
| 8 | Создать список IP-адресов для проверки целостности соединения и осуществить переход в режим настройки параметров списка. | `esr(config)# wan load-balance target-list <NAME>` | <NAME> – название списка, задается строкой до 31 символа. |
| 9 | Задать цель проверки и перейти в режим настройки параметров цели. | `esr(config-target-list)# target <ID>` | <ID> – идентификатор цели, задаётся в пределах [1..50]. Если при удалении используется значение параметра «all», то будут удалены все цели для конфигурируемого списка целей. |
| 10 | Описать target (не обязательно). | `esr(config-wan-target)# description <DESCRIPTION>` | <DESCRIPTION> – описание target, задаётся строкой до 255 символов. |
| 11 | Указать время ожидания ответа на запрос по протоколу ICMP (не обязательно). | `esr(config-wan-target)# resp-time <TIME>` | <TIME> – время ожидания, определяется в секундах [1..30]. |
| 12 | Указать IP-адрес проверки. | `esr(config-wan-target)# ip address <ADDR>` | <ADDR> – IP-адрес назначения, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| | | `esr(config-wan-target)# ipv6 address <IPV6-ADDR>` | <IPV6-ADDR> – IPv6-адрес назначения, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. |
| 13 | Включить проверку цели. | `esr(config-wan-target)# enable` | |
| Команды для пунктов 14-17 необходимо применить на интерфейсах/туннелях в MultiWAN | | | |
| 14 | Включить WAN режим на интерфейсе для IPv4/IPv6 стека. | `esr(config-if-gi)# wan load-balance enable` | |
| | | `esr(config-if-gi)# ipv6 wan load-balance enable` | |
| 15 | Задать количество неудачных попыток проверки соединения, после которых, при отсутствии ответа от встречной стороны, соединение будет считается неактивным (не обязательно). | `esr(config-if-gi)# wan load-balance failure-count <VALUE>` | <VALUE> – количество попыток, определяется в диапазоне [1..10].<br><br>Значение по умолчанию 1. |
| | | `esr(config-if-gi)# ipv6 wan load-balance failure-count <VALUE>` | |
| 16 | Задать количество успешных попыток проверки соединения, после которых, в случае успеха, соединение считается вновь активным (не обязательно). | `esr(config-if-gi)# wan load-balance success-count <VALUE>` | <VALUE> – количество попыток, определяется в диапазоне [1..10].<br><br>Значение по умолчанию 1. |
| | | `esr(config-if-gi)# ipv6 wan load-balance success-count <VALUE>` | |
| 17 | Задать IP-адрес соседа, который будет указан в качестве одного из шлюзов в статическом маршруте, создаваемом службой MultiWAN. | `esr(config-if-gi)# wan load-balance nexthop { <IP> \| dhcp enable \| tunnel enable }` | <IP> – IP-адрес назначения (шлюз), задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].<br><br>dhcp enable – если на интерфейсе IP-адрес получен через DHCP-клиента, используется шлюз с DHCP-сервера.<br><br>tunnel enable – использовать в качестве nexthop – p-t-p адрес назначения. Применимо для подключаемых интерфейсов работающих через ppp. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| | | `esr(config-if-gi)# ipv6 wan load-balance nexthop { <IPV6> }` | <IPV6> – IPv6-адрес назначения (шлюз), задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. |
| 18 | Данной командой будут проверяться IP-адреса из списка проверки целостности. В случае недоступности всех (по умолчанию)/хотябы одной (с использованием ключа chack-all) из проверяемых узлов, шлюз будет считаться недоступным. | `esr(config-if-gi)# wan load-balance target-list { check-all \| <NAME> }` | <NAME> – проверку производить на основании конкретного target листа (заданного в п.7).<br><br>check-all – проверку производить на основании всех target листа. |
| | | `esr(config-if-gi)# ipv6 wan load-balance target-list { check-all \| <NAME> }` | |
| 19 | Прописать статические маршруты через WAN. | `esr(config)# ip route <SUBNET> wan load-balance rule <ID> [<METRIC>]` | <ID> – идентификатор создаваемого правила из п.2.<br><br>[METRIC] – метрика маршрута, принимает значения [0..255]. |
| | | `esr(config)# ipv6 route <SUBNET> wan load-balance rule <ID> [<METRIC>]` | |

### 5.8.2 Пример настройки

**Задача:**

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


**Решение:**

Предварительно нужно выполнить следующие действия:

- настроить зоны для интерфейсов te1/0/1 и te1/0/2;
- указать IP-адреса для интерфейсов te1/0/1 и te1/0/2.

Основной этап конфигурирования:

Настроим маршрутизацию:

```
esr(config)# ip route 108.16.0.0/28 wan load-balance rule 1
```

Создадим правило WAN:

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

Укажем участвующие интерфейсы:

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

Включим созданное правило балансировки и выйдем из режима конфигурирования правила:

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

Создадим список для проверки целостности соединения:

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

Создадим цель проверки целостности:

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

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

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

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

```
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if)# wan load-balance nexthop 203.0.0.1
```

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

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

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

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

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

```
esr(config)# interface tengigabitethernet 1/0/2
esr(config-if)# wan load-balance nexthop 65.6.0.1
```

В режиме конфигурирования интерфейса te1/0/2 указываем список целей для проверки соединения:

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

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

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

Для переключения в режим резервирования настроим следующее:

Заходим в режим настройки правила WAN:

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

Функция MultiWAN также может работать в режиме резервирования, в котором трафик будет направляться в активный интерфейс с наибольшим весом. Включить данный режим можно следующей командой:

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

## 5.9 Настройка IS-IS

IS-IS - протокол динамической маршрутизации, стандартизированный ISO, основанный на состояниях линков (link-state). Он обеспечивает быструю сходимость и отличную масштабируемость, экономно использует пропускную способность сетей, использует Алгоритм Дейкстры для просчёта наилучших маршрутов. Отличительной особенностью протокола IS-IS является работа поверх канального уровня модели OSI, поэтому он не привязан к конкретному протоколу сетевого уровня.

### 5.9.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Создать IS-IS процесс и перейти в режим настройки параметров этого процесса. | `esr(config)# router isis <ID> [vrf <VRF>]` | <ID> – номер процесса, принимает значения [1..65535];<br><br><VRF> – имя экземпляра VRF, задается строкой до 31 символа. |
| 2 | Установить NET адрес. | `esr(config-isis)# net {<NET>}` | <NET> – NET адрес, формат: ff[.ffff.ffff.ffff.ffff.ffff].ffff.ffff.ffff.00. |
| 3 | Включить IS-IS процесс. | `esr(config-isis)# enable` | |

| | | | |
|---|---|---|---|
| 4 | Установить алгоритм аутентификации для L2 уровня (не обязательно). | `esr(config-isis)# authentication domain algorithm <ALGORITHM>` | <ALGORITHM> – алгоритм аутентификации:<br>– cleartext – пароль, передается открытым текстом;<br>– md5 – пароль хешируется по алгоритму md5. |
| 5 | Установить пароль аутентификации для L2 уровня (не обязательно). | `esr(config-isis)# authentication domain key ascii-text { <CLEAR-TEXT> \| encrypted <ENCRYPTED-TEXT> }` | <CLEAR-TEXT> – пароль, задаётся строкой 8 символов;<br><ENCRYPTED-TEXT> – зашифрованный пароль размером 8 байт (16 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...). |
| 6 | Установить список ключей для аутентификации (не обязательно). | `esr(config-isis)# authentication domain key chain <KEYCHAIN>` | <KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов. |
| 7 | Выбрать алгоритм аутентификации для L1 уровня (не обязательно). | `esr(config-isis)# authentication area algorithm <ALGORITHM>` | <ALGORITHM> – алгоритм аутентификации:<br>– cleartext – пароль, передается открытым текстом;<br>– md5 – пароль хешируется по алгоритму md5. |
| 8 | Установить пароль аутентификации для L1 уровня (не обязательно). | `esr(config-isis)# authentication area key ascii-text { <CLEAR-TEXT> \| encrypted <ENCRYPTED-TEXT> }` | <CLEAR-TEXT> – пароль, задаётся строкой 8 символов;<br><ENCRYPTED-TEXT> – зашифрованный пароль размером 8 байт (16 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...). |
| 9 | Установить список ключей для аутентификации (не обязательно). | `esr(config-isis)# authentication area key chain <KEYCHAIN>` | <KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов. |
| 10 | Включить передачу имени маршрутизатора в LSP (не обязательно). | `esr(config-isis)# hostname dynamic` | |

| | | | |
|---|---|---|---|
| 11 | Установить уровень работы IS-IS процесса (не обязательно). | `esr(config-isis)# is-type {<LEVEL>}` | <LEVEL> - уровень работы протокола IS-IS:<br>– level-1 – работа производится только на 1 уровне;<br>– level-1-2 – работа производится и на 1, и на 2 уровне;<br>– level-2 – работа производится только на 2 уровне. |
| 12 | Установить тип метрики, который будет использоваться в работе IS-IS процесса (не обязательно). | `esr(config-isis)# metric-style { narrow \| wide \| transition } [<LEVEL>]` | narrow — принимает и генерирует TLV (о достижимости сетей) старого типа;<br>wide — принимает и генерирует TLV (о достижимости сетей) нового типа;<br>transition — принимает и генерирует TLV (о достижимости сетей) нового и старого типа;<br><LEVEL> — уровень работы протокола IS-IS:<br>– level-1 – работа производится только на 1 уровне;<br>– level-2 – работа производится только на 2 уровне. |
| 13 | Установить приоритетность маршрутов для данного IS-IS процесса (не обязательно). | `esr(config-isis)# preference {<VALUE>}` | <VALUE> – принимает значения [1..255]. |
| 14 | Включить работу IS-IS с IPv4 и/или IPv6 адресами (не обязательно). | `esr(config-isis)# address-family { ipv4 \| ipv6 }` | ipv4 - семейство адресов IPv4;<br>ipv6 - семейство адресов IPv6. |

| | | | |
|---|---|---|---|
| 15 | Установить интервал обновления собственных LSP (не обязательно). | `esr(config-isis)# lsp-refresh-interval { min \| max } <TIME> [ <LEVEL> ]` | min — минимальный интервал обновления/генерации;<br><br>max — максимальный интервал обновления/генерации;<br><br><TIME> — время в секундах, принимает значения [1..65535];<br><br><LEVEL> — уровень работы протокола IS-IS:<br><br>– level-1 – работа производится только на 1 уровне;<br><br>– level-2 – работа производится только на 2 уровне. |
| 16 | Установить время жизни собственных LSP (не обязательно). | `esr(config-isis)# max-lsp-lifetime <TIME> [<LEVEL>]` | <TIME> – время в секундах, принимает значения [1..65535];<br><br><LEVEL> - уровень работы протокола IS-IS:<br><br>– level-1 – работа производится только на 1 уровне;<br><br>– level-2 – работа производится только на 2 уровне. |
| 17 | Установить таймаут перед следующим расчётом SPF (не обязательно). | `esr(config-isis)# spf-timeout <TIME> [<LEVEL>]` | <TIME> — время в милисекундах, принимает значения [1..10000];<br><br><LEVEL> — уровень работы протокола IS-IS:<br><br>– level-1 – работа производится только на 1 уровне;<br><br>– level-2 – работа производится только на 2 уровне. |

| | | | |
|---|---|---|---|
| 18 | Включить анонсирование маршрутов, полученных альтернативным способом (не обязательно). | `esr(config-isis)# redistribute bgp <AS> [ route-map <NAME> ] [is-type <LEVEL>]` | <AS> – номер автономной системы, может принимать значения [1..4294967295];<br><br><NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых маршрутов, задаётся строкой до 31 символа;<br><br><LEVEL> – уровень работы протокола IS-IS:<br><br>– level-1 – работа производится только на 1 уровне;<br><br>– level-2 – работа производится только на 2 уровне. |
| | | `esr(config-isis)# redistribute ipv6 bgp <AS> [ route-map <NAME> ] [is-type <LEVEL>]` | |

| | |
|---|---|
| esr(config-isis)# redistribute ospf <ID> <ROUTE-TYPE> [ route-map <NAME> ] [is-type <LEVEL>] | <ID> – номер процесса, может принимать значение [1..65535];<br><br><ROUTE-TYPE> – тип маршрута:<br><br>- intra-area – анонсирование маршрутов OSPF-процесса в пределах зоны;<br><br>- inter-area – анонсирование маршрутов OSPF-процесса между зонами;<br><br>- external1 – анонсирование внешних маршрутов OSPF-формата 1;<br><br>- external2 – анонсирование внешних маршрутов OSPF-формата 2;<br><br><NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых OSPF-маршрутов,<br><br>задаётся строкой до 31 символа;<br><br><LEVEL> — уровень работы протокола IS-IS:<br><br>– level-1 – работа производится только на 1 уровне;<br><br>– level-2 – работа производится только на 2 уровне. |
| esr(config-isis)# redistribute ipv6 ospf <ID> <ROUTE-TYPE> [ route-map <NAME> ] [is-type <LEVEL>] | |

| | |
|---|---|
| esr(config-isis)# redistribute isis <ID> <ROUTE-TYPE> [ route-map <NAME> ] [is-type <LEVEL>] | <ID> – номер процесса, может принимать значение [1..65535];<br><br><ROUTE-TYPE> – тип маршрута:<br><br>– level-1 – анонсирование маршрутов 1 уровня;<br><br>– level-2 – анонсирование маршрутов 1 уровня;<br><br>– inter-area – анонсирование маршрутов IS-IS-процесса между зонами;<br><br><NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых IS-IS-маршрутов,<br><br>задаётся строкой до 31 символа;<br><br><LEVEL> – уровень работы протокола IS-IS:<br><br>– level-1 – работа производится только на 1 уровне;<br><br>– level-2 – работа производится только на 2 уровне. |
| esr(config-isis)# redistribute rip [ route-map <NAME> ] [is-type <LEVEL>] | <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых RIP-маршрутов,<br><br>задаётся строкой до 31 символа;<br><br><LEVEL> – уровень работы протокола IS-IS:<br><br>– level-1 – работа производится только на 1 уровне;<br><br>– level-2 – работа производится только на 2 уровне. |

| | | | |
|---|---|---|---|
| | | esr(config-isis)# redistribute static [ route-map <NAME> ] [is-type <LEVEL>] | <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых статических маршрутов,<br><br>задаётся строкой до 31 символа;<br><br><LEVEL> – уровень работы протокола IS-IS:<br><br>– level-1 – работа производится только на 1 уровне;<br><br>– level-2 – работа производится только на 2 уровне. |
| | | esr(config-isis)# redistribute connected [ route-map <NAME> ] [is-type <LEVEL>] | <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых подключённых маршрутов,<br><br>задаётся строкой до 31 символа;<br><br><LEVEL> – уровень работы протокола IS-IS:<br><br>– level-1 – работа производится только на 1 уровне;<br><br>– level-2 – работа производится только на 2 уровне. |
| 19 | Добавить фильтрацию подсетей во входящих или исходящих обновлениях<br><br>(не обязательно). | esr(config-isis)# prefix-list { ipv6 <LIST_NAME> \| <LIST_NAME> } {in\|out} | <LIST-NAME> – имя сконфигурированного списка подсетей, задаётся строкой до 31 символа.<br><br>in – фильтрация входящих маршрутов;<br><br>out – фильтрация анонсируемых маршрутов. |
| 20 | Добавить фильтрацию подсетей во входящих или исходящих обновлениях<br><br>(не обязательно). | esr(config-isis)# route-map <NAME> {in\|out} | <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых маршрутов,<br><br>задаётся строкой до 31 символа. |

| | | | |
|---|---|---|---|
| 21 | Установить принадлежность интерфейса к определенному IS-IS процессу. | `esr(config-if-gi)# isis instance <ID>` | <ID> – номер процесса, принимает значения [1..65535]. |
| 22 | Включить работу протокола IS-IS на интерфейсе. | `esr(config-if-gi)# isis enable` | |
| 23 | Включить использование TLV#8 в hello пакетах (не обязательно). | `esr(config-if-gi)# isis hello-padding` | |
| 24 | Установить приоритет при выборе DIS (не обязательно). | `esr(config-if-gi)# isis priority <VALUE> [<LEVEL>]` | <VALUE> – число, принимающее значения [0..127];<br><br><LEVEL> - уровень работы протокола IS-IS:<br><br>– level-1 – работа производится только на 1 уровне;<br><br>– level-2 – работа производится только на 2 уровне. |
| 25 | Установить значение метрики для интерфейса (не обязательно). | `esr(config-if-gi)# isis metric <VALUE> [<LEVEL>]` | <VALUE> – число, принимающее значения [1..16777215];<br><br><LEVEL> - уровень работы протокола IS-IS:<br><br>– level-1 – работа производится только на 1 уровне;<br><br>– level-2 – работа производится только на 2 уровне. |
| 26 | Установить<br>на каком уровне маршрутизации будет работать текущий процесс IS-IS на конкретном интерфейсе (не обязательно). | `esr(config-if-gi)# isis circuit-type {<LEVEL>}` | <LEVEL> - уровень работы протокола IS-IS:<br><br>– level-1 – работа производится только на 1 уровне;<br><br>– level-1-2 – работа производится и на 1, и на 2 уровне;<br><br>– level-2 – работа производится только на 2 уровне. |

| | | | |
|---|---|---|---|
| 27 | Установить интервал отправки hello пакетов (не обязательно). | `esr(config-if-gi)# isis hello-interval <TIME> [<LEVEL>]` | <TIME> – время в секундах, принимает значения [1..65535];<br><br><LEVEL> - уровень работы протокола IS-IS:<br><br>– level-1 – работа производится только на 1 уровне;<br><br>– level-2 – работа производится только на 2 уровне. |
| 28 | Установить множитель для вычисления и отправки Hold Time (не обязательно). | `esr(config-if-gi)# isis hello-multiplier <VALUE> [<LEVEL>]` | <VALUE> – число, принимающее значения [3..1000];<br><br><LEVEL> - уровень работы протокола IS-IS:<br><br>– level-1 – работа производится только на 1 уровне;<br><br>– level-2 – работа производится только на 2 уровне. |
| 29 | Перевести интерфейс в режим работы point-to-point протокола IS-IS (не обязательно). | `esr(config-if-gi)# isis network point-to-point` | |
| 30 | Установить интервал генерации и отправки CSNP (не обязательно). | `esr(config-if-gi)# isis csnp-interval <TIME> [<LEVEL>]` | <TIME> – время в секундах, принимает значения [1..65535];<br><br><LEVEL> - уровень работы протокола IS-IS:<br><br>– level-1 – работа производится только на 1 уровне;<br><br>– level-2 – работа производится только на 2 уровне. |

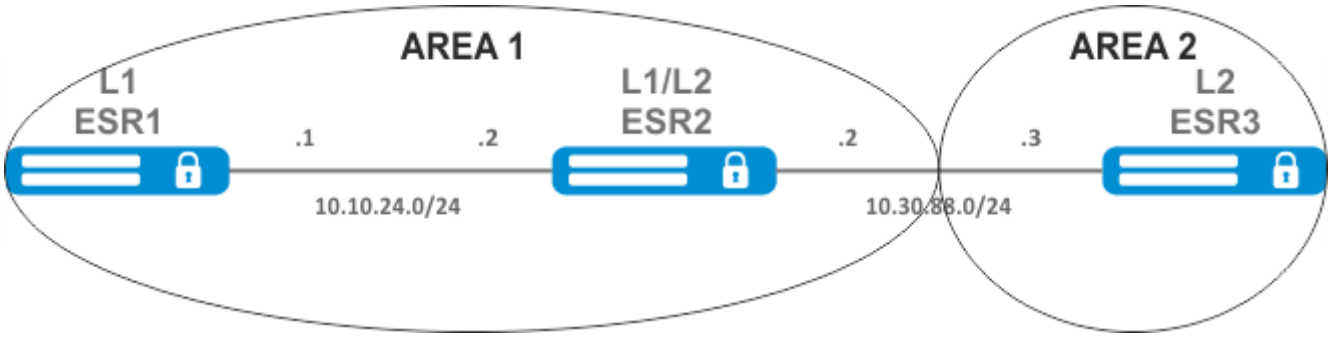
| | | | |
|---|---|---|---|
| 31 | Установить интервал генерации и отправки PSNP (не обязательно). | `esr(config-if-gi)# isis psnp-interval <TIME> [<LEVEL>]` | <TIME> – время в секундах, принимает значения [1..65535];<br><br><LEVEL> - уровень работы протокола IS-IS:<br><br>– level-1 – работа производится только на 1 уровне;<br><br>– level-2 – работа производится только на 2 уровне. |
| 32 | Установить интервал между передачами LSP в Broadcast сети (не обязательно). | `esr(config-if-gi)# isis lsp-interval <TIME> [<LEVEL>]` | <TIME> – время в милисекундах, принимает значения [1-10000];<br><br><LEVEL> - уровень работы протокола IS-IS:<br><br>– level-1 – работа производится только на 1 уровне;<br><br>– level-2 – работа производится только на 2 уровне. |
| 33 | Установить интервал повторного распространения LSP в PtP сети (не обязательно). | `esr(config-if-gi)# isis lsp-retransmit-interval <TIME> [<LEVEL>]` | <TIME> – время в секундах, принимает значения [1..65535];<br><br><LEVEL> - уровень работы протокола IS-IS:<br><br>– level-1 – работа производится только на 1 уровне;<br><br>– level-2 – работа производится только на 2 уровне. |

| | | | |
|---|---|---|---|
| 34 | Установить алгоритм аутентификации для hello пакетов (не обязательно). | `esr(config-if-gi)# isis authentication algorithm <ALGORITHM> [<LEVEL>]` | <ALGORITHM> – алгоритм аутентификации:<br>– cleartext – пароль, передается открытым текстом;<br>– md5 – пароль хешируется по алгоритму md5;<br><LEVEL> – уровень работы протокола IS-IS:<br>– level-1 – работа производится только на 1 уровне;<br>– level-2 – работа производится только на 2 уровне. |
| 35 | Установить пароль для аутентификации hello пакетов (не обязательно). | `esr(config-if-gi)# isis authentication key ascii-text { <CLEAR-TEXT> \| encrypted <ENCRYPTED-TEXT> } [<LEVEL>]` | <CLEAR-TEXT> – пароль, задаётся строкой 8 символов;<br><ENCRYPTED-TEXT> – зашифрованный пароль размером 8 байт (16 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...);<br><LEVEL> – уровень работы протокола IS-IS:<br>– level-1 – работа производится только на 1 уровне;<br>– level-2 – работа производится только на 2 уровне. |
| 36 | Установить список ключей для аутентификации hello пакетов (не обязательно). | `esr(config-if-gi)# isis authentication key chain <KEYCHAIN> [<LEVEL>]` | <KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов;<br><LEVEL> – уровень работы протокола IS-IS:<br>– level-1 – работа производится только на 1 уровне;<br>– level-2 – работа производится только на 2 уровне. |

### 5.9.2 Пример настройки

**Задача:**

Настроить протокол IS-IS на маршрутизаторах для обмена маршрутной информацией с соседями. Маршрутизатор ESR1 будет L1-only, ESR2 - L1/L2, ESR3 - L2-only, который также будет находится в другой area.




**Решение:**

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

Перейдём к настройке маршрутизатора ESR1. Создадим IS-IS процесс с идентификатором 1 и перейдём в режим конфигурирования протокола:

```
ESR1(config)# router isis 1
```

Зададим номер зоны, в которой будет работать маршутизатор и его системный идентификатор:

```
ESR1(config-isis)# net 49.0001.1111.1111.1111.00
```

Настроим работу маршрутизатора только на первом уровне  протокола IS-IS:

```
ESR1(config-isis)# is-type level-1
```

Зададим работу маршрутизатора  с узкой метрикой на первом уровне:

```
ESR1(config-isis)# metric-style narrow level-1
```

Включим работу процесса IS-IS на маршрутизаторе

```
ESR1(config-isis)# enable
```

Перейдём к конфигурированию интерфейсов. Нужно задать номер процесса IS-IS, который будет работать на интерфейсе и включить работу самого протокола на нём:

```
ESR1(config-if-gi)# isis instance 1
ESR1(config-if-gi)# isis enable
```

Перейдём к настройке маршрутизатора ESR2:

```
ESR2(config)# router isis 2
```

Зададим номер зоны, такой же как на ESR1, а также уникальный системный идентификатор:

```
ESR2(config-isis)# net 49.0001.2222.2222.2222.00
```

Зададим работу маршрутизатора  с узкой метрикой на первом уровне и с широкой метрикой на втором, и включим работу данного процесса IS-IS:

```
ESR2(config-isis)# metric-style narrow level-1
ESR2(config-isis)# metric-style wide level-2
ESR2(config-isis)# enable
```

Настроим работу интерфейсов на маршрутизаторе. На обоих интерфейсах настройка будет одинаковая.

```
ESR2(config-if-gi)# isis instance 2
ESR2(config-if-gi)# isis enable
```

Перейдём к настройке маршрутизатора ESR3:

```
ESR3(config)# router isis 3
ESR3(config-isis)# net 49.0002.3333.3333.3333.00
ESR3(config-isis)# is-type level-2
ESR3(config-isis)# metric-style wide level-2
ESR3(config-isis)# enable
ESR3(config-if-gi)# isis instance 3
ESR3(config-if-gi)# isis enable
```

Установление соседства можно посмотреть командой show isis neighbors. Выполним её на ESR2:

```
ESR2# show isis neighbors
IS-IS 2
IS-IS Level 1 Neighbors
System ID               Hostname          Interface         State         Holdtime  SNPA
1111.1111.1111  ESR1                    gi1/0/2            Up              25
a8f9.4baa.1d42
IS-IS Level 2 Neighbors
System ID               Hostname          Interface         State         Holdtime  SNPA
3333.3333.3333  ESR3                    gi1/0/1            Up              8
a8f9.4bab.813a
```

# 6 Управление технологией MPLS



## 6.1 Конфигурирование протокола LDP

LDP - протокол распределения меток. Для нахождения соседей используется рассылка hello-сообщений на мультикастный адрес 224.0.0.2. При обмене hello-сообщениями, маршрутизаторы узнают транспортные адреса друг друга. Маршрутизатор с большим адресом инициализирует TCP-сессию. После проверки параметров, LDP-сессия считается установленной.

В маршрутизаторах ESR поддержаны следующие режимы работы LDP:

- Режим обмена информации о метках - Downstream Unsolicited;
- Механизм контроля за распространением меток - Independent Label Distribution Control;
- Режим сохранения меток - Liberal Label Retention;

На интерфейсах где включены протокол LDP и MPLS-коммутация, firewall должен быть отключен.

### 6.1.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | В контексте настройки параметров MPLS указать интерфейсы, участвующие в процессе MPLS-коммутации | `esr(config-mpls)# forwarding interface { <IF> \| <TUN> }` | <IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора;<br><br><TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора. |
| 2 | Задать router-id для LDP (не обязательно, если указан transport-address). | `esr(config-ldp)# router-id <ID>` | <ID> -идентификатор маршрутизатора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 3 | В контексте настройки address family ipv4 указать transport-address (не обязательно , если указан router-id). | `esr(config-ldp-af-ipv4)# transport-address <ADDR>` | <ADDR> - задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 3 | В контексте настройки address family ipv4 указать интерфейсы для включение на них процесса LDP. | `esr(config-ldp-af-ipv4)# interface { <IF> \| <TUN> }` | <IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора;<br><br><TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора. |
| 4 | Включить процесс LDP. | `esr(config-ldp)# enable` | |
| 5 | Включить функционал explicit-null (не обязательно). | `esr(config-ldp)# egress-label-type explicit-null` | |
| 6 | В режиме конфигурирование соседа LDP задать пароль командой password (не обязательно). | `esr(config-ldp-neig)# password {<TEXT> \| ENCRYPTED-TEXT>}` | <CLEAR-TEXT> – пароль, задаётся строкой, длинной [8..16] символов;<br><br><ENCRYPTED-TEXT> – зашифрованный пароль размером [8..16] байт ([16..32] символа) в шестнадцатеричном формате (0xYYYY...) или (YYYY...). |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| В рамках настройки протокола LDP также доступен следующий функционал:<br>• Настройка фильтрации LDP-меток ( см. Конфигурирование фильтрации LDP-меток)<br>• Настройка параметров LDP-сессии (см. Конфигурирование параметров сессии в протоколе LDP)<br>• Настройка параметров tLDP-сессии (см. Конфигурирование параметров сессии в протоколе targeted-LDP) | | | |

### 6.1.2 Пример настройки

**Задача:**

Настроить взаимодействие по протоколу LDP между пирами.


**Решение:**

1 Предварительная конфигурация ESR:

Предварительно на интерфейсы, должны быть назначены IP-адреса, отключен межсетевой экран и настроен один из протоков внутренней маршрутизации

Предварительная конфигурация ESR:

```
hostname ESR
router ospf 1
  area 0.0.0.0
    enable
  exit
  enable
exit


interface gigabitethernet 1/0/1
  ip firewall disable
  ip address 10.10.10.1/30
  ip ospf instance 1
  ip ospf
exit


interface loopback 1
  ip address 1.1.1.1/32
  ip ospf instance 1
  ip ospf
exit
```

Предварительная конфигурация ESR1:

```
hostname ESR1
router ospf 1
  area 0.0.0.0
    enable
  exit
  enable
exit


interface gigabitethernet 1/0/1
  ip firewall disable
  ip address 10.10.10.2/30
  ip ospf instance 1
  ip ospf
exit


interface loopback 1
  ip address 4.4.4.4/32
  ip ospf instance 1
  ip ospf
exit
```

2 Настройка на ESR:

**ESR**

```
ESR# config
ESR(config)# mpls
ESR(config-mpls)# forwarding interface gigabitethernet 1/0/1
ESR(config-mpls)# ldp
ESR(config-ldp)# router-id 1.1.1.1
ESR(config-ldp)# enable
ESR(config-ldp)# address-family ipv4
ESR(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1
ESR(config-ldp-af-ipv4-if)# end
ESR#
```

3 Настройка на ESR1:

**ESR1**

```
ESR1# configure
ESR1(config)# mpls
ESR1(config-mpls)# forwarding interface gigabitethernet 1/0/1
ESR1(config-mpls)# ldp
ESR1(config-ldp)# router-id 4.4.4.4
ESR1(config-ldp)# enable
ESR1(config-ldp)# address-family ipv4
ESR1(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1
ESR1(config-ldp-af-ipv4-if)# end
ESR1#
```

**Проверка:**

На одном из пиров вести следующие команды:

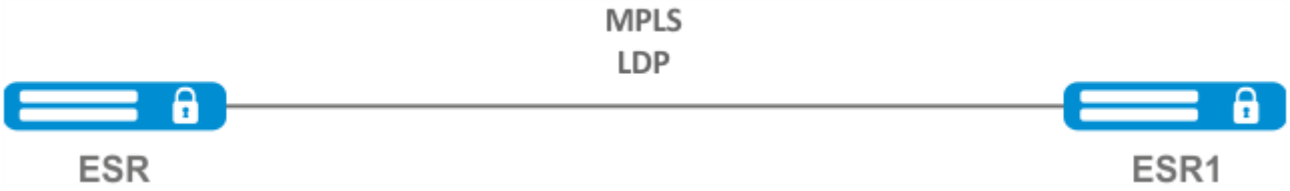
Вывод покажет параметры соседнего пира, полученные из мультикастовых hello-сообщений.

ESR# show mpls ldp discovery detailed
Local LDP ID: 1.1.1.1
Discovery sources:
  Interfaces:
    gigabitethernet 1/0/1:
        **Hello interval: 5 seconds**
    Transport IP address: 1.1.1.1
    LDP ID: 4.4.4.4
      Source IP address: 10.10.10.2
      Transport IP address: 4.4.4.4
            **Hold time: 15 seconds**
            **Proposed hold time: 90/15 (local/peer) seconds**

Сессия LDP должна находиться в статусе "Operational".

ESR1# show mpls ldp neighbor
Peer LDP ID: 4.4.4.4; Local LDP ID 1.1.1.1
  State: **Operational**
  TCP connection: 4.4.4.4:40245 - 1.1.1.1:646
  Messages sent/received: 10/11
  Uptime: 00:00:58
  LDP discovery sources:
    gigabitethernet 1/0/1

## 6.2 Конфигурирование параметров сессии в протоколе LDP




По-умолчанию, в рассылаемых hello сообщениях установлены следующие значения:

| Параметр | LDP |
|---|---|
| Hello interval | 5 секунд |
| Hold timer | 15 секунд |
| Keepalive holdtime | 180 секунд |

Hold timer является согласуемым параметром - выбирается наименьший. В данном примере показано, что ESR после согласования Hold timer равен 10 секундам.

```
ESR# sh mpls ldp discovery detailed
Local LDP ID: 4.4.4.4
Discovery sources:
  Interfaces:
    gigabitethernet 1/0/4:
      Hello interval: 5 seconds
      Transport IP address: 4.4.4.4
      LDP ID: 1.1.1.1
        Source IP address: 10.10.10.1
        Transport IP address: 1.1.1.1
                    Hold time: 10 seconds
                    Proposed hold time: 15/10 (local/peer) seconds
```

Если после согласования, Hello interval стал больше чем Hold timer, то Hello interval будет равным Hold timer / 3.

На маршрутизаторах ESR реализована возможность гибкой настройки параметров Hello holdtime , Hello interval и Keepalive holdtime. Рассмотрим пример настройки Hello holdtime для LDP сессии :

```
ESR# show run mpls
mpls
 ldp
 router-id 4.4.4.4
   discovery hello holdtime 40
  address-family ipv4
   interface gigabitethernet 1/0/4
        discovery hello holdtime 60
  exit
 exit
 enable
exit
```

Если параметры Hello Holdtime и Hello Interval не указаны, то используются значения по-умолчанию. Если параметры указаны, то приоритет значений для address-family будет выше чем для значений, сконфигурированных глобально.

```
ESR# show mpls ldp discovery detailed
Local LDP ID: 4.4.4.4
Discovery sources:
  Interfaces:
    gigabitethernet 1/0/4:
      Hello interval: 5 seconds
      Transport IP address: 4.4.4.4
      LDP ID: 1.1.1.1
        Source IP address: 10.10.10.1
        Transport IP address: 1.1.1.1
        Hold time: 15 seconds
                    Proposed hold time: 60 /15 (local/peer) seconds
```

Параметры, сконфигурированные в address-family, могут быть настроены на каждый отдельный интерфейс, участвующий в процессе LDP.

```
ESR# show running-config mpls
mpls
 ldp
  router-id 4.4.4.4
  discovery hello holdtime 50
  discovery hello interval 10
  address-family ipv4
       interface gigabitethernet 1/0/1
          discovery hello holdtime 60
          discovery hello interval 20
   exit
       interface gigabitethernet 1/0/4
          discovery hello holdtime 30
          discovery hello interval 10
   exit
  exit
 enable
exit
```

Для TCP-сессии, Keepalive holdtime является также согласуемым параметром по аналогии с Hold timer. Keepalive interval рассчитывается автоматически, и равен Keepalive holdtime /3. Keepalive holdtime можно задать как глобально, так и для каждого соседа. Таймер, заданный для определенного соседа, является более приоритетным.

```
ESR# show running-config mpls
mpls
 ldp
 router-id 4.4.4.4
   keepalive 30 // установлен в глобальной конфигурации LDP
 neighbor 1.1.1.1
   keepalive 55// установлен в соседа с адресом 1.1.1.1
 exit
exit
```

ESR# sh mpls ldp neighbor 1.1.1.1
Peer LDP ID: 1.1.1.1; Local LDP ID 4.4.4.4
State: Operational
TCP connection: 1.1.1.1:646 - 4.4.4.4:56668
Messages sent/received: 401/401
Uptime: 02:00:24
Peer holdtime: 55
Keepalive interval: 18
LDP discovery sources:

### 6.2.1 Алгоритм настройки параметров Hello holdtime и Hello interval в глобальной конфигурации LDP

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Настроить протокол LDP (см. раздел Конфигурирование протокола LDP) | | |
| 2 | В режиме конфигурации протокола LDP задать Hello holdtime | `esr(config-ldp)# discovery hello holdtime <TIME>` | <TIME> - Время в секундах в интервале [3..65535]<br>Значение по умолчанию:15 |
| 3 | В режиме конфигурации протокола LDP задать Hello interval | `esr(config-ldp)# discovery hello interval <TIME>` | <TIME> - Время в секундах в интервале [3..65535]<br>Значение по умолчанию: 5 |

### 6.2.2 Алгоритм настройки параметров Hello holdtime и Hello interval для address family

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Настроить протокол LDP (см. раздел Конфигурирование протокола LDP) | | |
| 2 | В режиме конфигурации address familly протокола LDP установить Hello holdtime на нужном интерфейсе | `esr(config-ldp-af-ipv4-if)# discovery hello holdtime <TIME>` | <TIME> - Время в секундах в интервале [3..65535]<br>Значение по умолчанию: 15 |
| 3 | В режиме конфигурации address familly протокола LDP установить Hello interval на нужном интерфейсе | `esr(config-ldp-af-ipv4-if)# discovery hello interval <TIME>` | <TIME> - Время в секундах в интервале [3..65535]<br>Значение по умолчанию: 5 |

### 6.2.3 Алгоритм настройки параметра Keepalive holdtime в глобальной конфигурации LDP

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Настроить протокол LDP (см. раздел Конфигурирование протокола LDP) | | |
| 2 | В режиме конфигурации LDP задать параметр Keepalive | `esr(config-ldp)# keepalive <TIME>` | <TIME> - Время в секундах в интервале [3..65535]<br>Значение по умолчанию: 180 |

### 6.2.4 Алгоритм настройки параметра Keepalive holdtime для определенного соседа

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Настроить протокол LDP (см. раздел Конфигурирование протокола LDP) | | |
| 2 | В режиме конфигурации соседа задать параметр Keepalive holdtime | `esr(config-ldp-neig)# keepalive <TIME>` | <TIME> - Время в секундах в интервале [3..65535]<br>Значение по умолчанию: 180 |

### 6.2.5 Пример настройки

**Задача:**

Переопределить параметры hello holdtime (40 секунд) и hello interval (10 секунд) для всего процесса LDP. Для соседа с адресом 1.1.1.1 установить Keepalive holdtime равным 150 секунд.

**Решение:**

**ESR**

```
ESR(config)# mpls
ESR(config-mpls)# ldp
ESR(config-ldp)# discovery hello holdtime 40
ESR(config-ldp)# discovery hello interval 10
ESR(config-ldp)# neighbor 1.1.1.1
ESR(config-ldp-neig)# keepalive 150
```

**Проверка:**

Для просмотра hello - параметров:

**ESR**

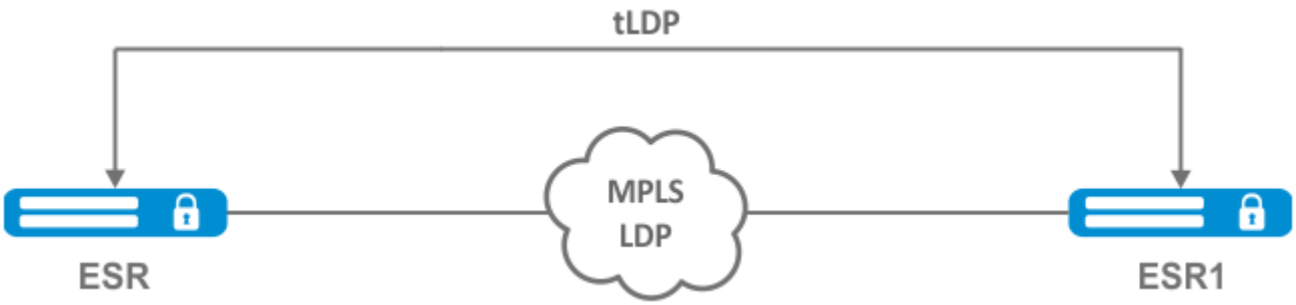
```
ESR# sh mpls ldp discovery detailed
Local LDP ID: 4.4.4.4
Discovery sources:
    Interfaces:
        gigabitethernet 1/0/4:
            Hello interval:       10 seconds
            Transport IP address: 4.4.4.4
            LDP ID:               1.1.1.1
                Source IP address:    10.10.10.1
                Transport IP address: 1.1.1.1
                Hold time:            15 seconds
                Proposed hold time:   40/15 (local/peer) seconds
```

Для просмотра параметров установленной TCP-сессии:

**ESR**

```
ESR# sh mpls ldp neighbor 1.1.1.1
Peer LDP ID: 1.1.1.1; Local LDP ID 4.4.4.4
    State:                  Operational
    TCP connection:         1.1.1.1:646 - 4.4.4.4:45414
    Messages sent/received: 15/15
    Uptime:                 00:06:31
    Peer holdtime:          150
    Keepalive interval:     50
    LDP discovery sources:
```

## 6.3 Конфигурирование параметров сессии в протоколе targeted-LDP




По-умолчанию, для targeted LDP сессии установлены следующие значения:

| Параметр | targeted-LDP |
|---|---|
| hello interval | 5 секунд |
| Hold timer | 45 секунд |
| Keepalive holdtime | 180 секунд |

Hold timer является согласуемым параметром - выбирается наименьший. В данном примере показано, что ESR после согласования установил 30 секунд:

ESR1# sh mpls ldp discovery detailed
...
Targeted hellos:
1.1.1.1 -> 4.4.4.4:
Hello interval: 2 seconds
Transport IP address: 1.1.1.1
LDP ID: 4.4.4.4
Source IP address: 4.4.4.4
Transport IP address: 4.4.4.4
**Hold time: 30 seconds**
**Proposed hold time: 30/45 (local/peer) seconds**

Если после согласования, Hello interval стал больше чем Hold timer, то Hello interval будет равным Hold timer / 3.

На маршрутизаторах ESR реализована возможность гибкой настройки параметров Hello holdtime , Hello interval и Keepalive holdtime: параметры можно задать как для всего процесса LDP, так и на соответствующего соседа.

Пример вывода для процесса LDP:

```
ESR# sh running-config mpls
mpls
 ldp
  router-id 1.1.1.1
     keepalive 160
     discovery targeted-hello holdtime 30
     discovery targeted-hello interval 10
 exit
exit
```

Пример вывода для targeted-LDP-сессии для определенного соседа:

```
ESR# sh running-config mpls
mpls
 ldp
  router-id 1.1.1.1
  neighbor 4.4.4.4
   keepalive 160
   targeted
   discovery targeted-hello holdtime 30
   discovery targeted-hello interval 45
  exit
 exit
exit
```

Если параметры установлены и для процесса LDP, и на определенного соседа, приоритетом будет считаться настройки, установленные для соседа.

```
ESR# sh running-config mpls
mpls
 ldp
  router-id 1.1.1.1
  keepalive  160
  discovery hello holdtime 90
  discovery targeted-hello interval 30
  neighbor 4.4.4.4
   keepalive 140
   targeted
   discovery targeted-hello holdtime 45
   discovery targeted-hello interval 15
  exit
 exit
exit
```

ESR# show mpls ldp discovery detailed
...
Targeted hellos:
1.1.1.1 -> 4.4.4.4:
**Hello interval: 15 seconds**
Transport IP address: 1.1.1.1
LDP ID: 4.4.4.4
Source IP address: 4.4.4.4
Transport IP address: 4.4.4.4
**Hold time: 45 seconds**
Proposed hold time: 45/45 (local/peer) seconds

ESR# show mpls ldp neighbor 4.4.4.4
Peer LDP ID: 4.4.4.4; Local LDP ID 1.1.1.1
State: Operational
TCP connection: 4.4.4.4:51861 - 1.1.1.1:646
Messages sent/received: 10/10
Uptime: 00:00:09
**Peer holdtime: 140**
Keepalive interval: 46
LDP discovery sources:
1.1.1.1 -> 4.4.4.4:

### 6.3.1 Алгоритм настройки параметров Hello holdtime, Hello interval и Keepalive holdtime для процесса LDP

| | | | |
|---|---|---|---|
| 1 | Настроить протокол LDP (см. раздел Конфигурирование протокола LDP) | | |
| 2 | В режиме конфигурации протокола LDP задать Hello holdtime | `esr(config-ldp)# discovery targeted-hello holdtime <TIME>` | <TIME> - Время в секундах в интервале [3..65535]<br>Значение по умолчанию: 45 |
| 3 | В режиме конфигурации протокола LDP задать Hello interval | `esr(config-ldp)# discovery targeted- hello interval <TIME>` | <TIME> - Время в секундах в интервале [1..65535]<br>Значение по умолчанию: 5 |
| 4 | В режиме конфигурации протокола LDP задать Keepalive holdtime | `esr(config-ldp)# keepalive <TIME>` | <TIME> - Время в секундах в интервале [3..65535]<br>Значение по умолчанию: 180 |

### 6.3.2 Алгоритм настройки параметров Hello holdtime, Hello interval и Keepalive holdtime для определенного соседа

| | | | |
|---|---|---|---|
| 1 | Настроить протокол LDP (см. раздел Конфигурирование протокола LDP) | | |
| 2 | В режиме конфигурации LDP-соседа задать Hello holdtime | `esr(config-ldp-neig)# discovery targeted-hello holdtime <TIME>` | <TIME> - Время в секундах в интервале [3..65535]<br>Значение по умолчанию: 45 |

| | | | |
|---|---|---|---|
| 3 | В режиме конфигурации LDP-соседа задать Hello interval | `esr(config-ldp-neig)# discovery targeted- hello interval <TIME>` | <TIME> - Время в секундах в интервале [1..65535]<br>Значение по умолчанию: 5 |
| 4 | В режиме конфигурации LDP-соседа задать Keepalive holdtime | `esr(config-ldp-neig)# keepalive <TIME>` | <TIME> - Время в секундах в интервале [3..65535]<br>Значение по умолчанию: 180 |

### 6.3.3 Пример настройки

**Задача:**

Переопределить параметры hello holdtime (120 секунд) и hello interval (30 секунд ) для всего процесса targeted-LDP. Для соседа с адресом 4.4.4.4 установить Keepalive holdtime равным 150 секунд.

**Решение:**

**ESR**

```
ESR(config)# mpls
ESR(config-mpls)# ldp
ESR(config-ldp)# discovery targeted-hello holdtime 40
ESR(config-ldp)# discovery targeted-hello interval 10
ESR(config-ldp)# neighbor 4.4.4.4
ESR(config-ldp-neig)# keepalive 150
```

**Проверка:**

Для просмотра hello - параметров targeted-LDP сессии:

**ESR**

```
ESR1# sh mpls ldp discovery detailed
...
    Targeted hellos:
         1.1.1.1 -> 4.4.4.4:
            Hello interval:       10 seconds
            Transport IP address: 1.1.1.1
            LDP ID:               4.4.4.4
                Source IP address:    4.4.4.4
                Transport IP address: 4.4.4.4
                Hold time:            40 seconds
                Proposed hold time:   40/45 (local/peer) seconds
```

Для просмотра параметров установленной TCP-сессии:

**ESR**

```
ESR# sh mpls ldp neighbor 4.4.4.4
Peer LDP ID: 4.4.4.4; Local LDP ID 1.1.1.1
    State:                  Operational
    TCP connection:         4.4.4.4:34879 - 1.1.1.1:646
    Messages sent/received: 11/11
    Uptime:                 00:01:05
    Peer holdtime:          150
    Keepalive interval:     50
    LDP discovery sources:
         1.1.1.1 -> 4.4.4.4:
            Hello interval: 10 seconds
            Holdtime:       40 seconds
  ...
```

## 6.4 Конфигурирование фильтрации LDP-меток

По-умолчанию, маршрутизаторы выделяют на каждый FEC отдельную метку. Существуют сценарии, когда необходимо выделять MPLS метки только для определенных FEC.

### 6.4.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Настроить протокол LDP (см. раздел Конфигурирование протокола LDP) | | |
| 2 | Создать object-group типа network | `esr(config)# object-group network <NAME>` | <NAME> – имя конфигурируемого списка подсетей, задаётся строкой до 31 символа. |
| 3 | Описать подсети, для которых будут назначаться метки | `esr(config-object-group-network)# ip prefix <ADDR/LEN>` | <ADDR/LEN> – IP-адрес и маска подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]; |
| 4 | В контексте настройки LDP применить созданную object-group | `esr(config-ldp)# advertise-labels <NAME>` | <NAME> – имя конфигурируемого списка подсетей, задаётся строкой до 31 символа. |

ⓘ Метки будут выделяться ТОЛЬКО на описанные в object-group подсети, независимо от того, как они были изучены ( connected, local, IGP и т.д.).

ⓘ В object-group необходимо описывать префиксы.

ⓘ Данный функционал поддержан для протокола IPv4.

### 6.4.2 Пример настройки


**Задача:**

Назначить mpls метки только FEC 10.10.0.0/24

**Решение:**

На ESR_A и ESR_B создадим object-group ADV_LABELS типа network и добавим в нее подсеть 10.10.0.0/24. На ESR_B также дополнительно добавим 192.168.2.0/24.

**ESR_A**

```
esr(config)# object-group network ADV_LABELS
esr(config-object-group-network)# ip prefix 10.10.0.0/24
```

**ESR_B**

```
esr(config)# object-group network ADV_LABELS
esr(config-object-group-network)# ip prefix 10.10.0.0/24
esr(config-object-group-network)# ip prefix 192.168.2.0/24
```

Применим созданную object-group на обоих маршрутизаторах.

**ESR_A и ESR_B**

```
esr(config)# mpls
esr(config-ldp)# ldp
esr(config-ldp)# advertise-labels ADV_LABELS
```

**Проверка:**

На ESR_B убедимся, что метка назначена для адресов из подсети 10.10.0.0/24

```
esr# sh mpls ldp bindings 10.10.0.1/32
10.10.0.1/32
local label: exp-null
remote label: 75 lsr: 172.16.0.1
```

И не назначена для 192.168.2.0/24

```
esr# sh mpls ldp bindings 192.168.2.0/24
192.168.2.0/24:
local label: --
remote label: imp-null lsr: 172.16.0.1
```

## 6.5 Конфигурирование L2VPN Martini

L2VPN позволяет организовать передачу ethernet-фреймов через MPLS домен. Выделение и распространение туннельных меток, в данном режиме, осуществляется по средствам протокола LDP. В реализации L2VPN можно условно выделить два случая:

1. P2P - туннель создаваемый по схеме "точка-точка"
2. VPLS - туннель создаваемый по схеме "точка-многоточка"

В обоих случаях, для передачи ethernet-фреймов между маршрутизаторами создается виртуальный канал (далее pseudo-wire). Для согласования параметров pseudo-wire, а также для выделения и передачи туннельных меток между маршрутизаторами, устанавливается LDP сессия в targeted режиме.

### 6.5.1 Алгоритм настройки L2VPN VPWS

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Настроить протокол LDP (см. раздел Конфигурирование протокола LDP). | | |
| 2 | Создать pw-class в системе и осуществить переход в режим настройки параметров pw-class. | `esr(config-l2vpn)# pw-class <WORD>` | `<WORD> - Имя pw-class длинной [1..31] символов.` |
| 3 | Добавить описание для pw-class (не обязательно). | `esr(config-l2vpn-pw-class)# description <LINE>` | <LINE> - Описание. Задается в виде строки длинной [1..255] символов |
| 4 | Установить значение MTU для pseudo-wire входящих в pw-class (не обязательно). | `esr(config-l2vpn-pw-class)# encapsulation mpls mtu <MTU>` | <MTU> - значение MTU, принимает значение в диапазоне [552..10000]<br><br>Значение по умолчанию: 1500. |
| 5 | Отключить обмен status-tlv сообщениями (не обязательно). | `esr(config-l2vpn-pw-class)# encapsulation mpls status-tlv disable` | Значение по умолчанию: status-tlv enable |
| 6 | Создать p2p-туннель в системе и осуществить переход в режим настройки параметров p2p-туннеля. | `esr(config-l2vpn)# p2p <NAME>` | <NAME> - Имя p2p сервиса, задается строкой до 31 символа. |

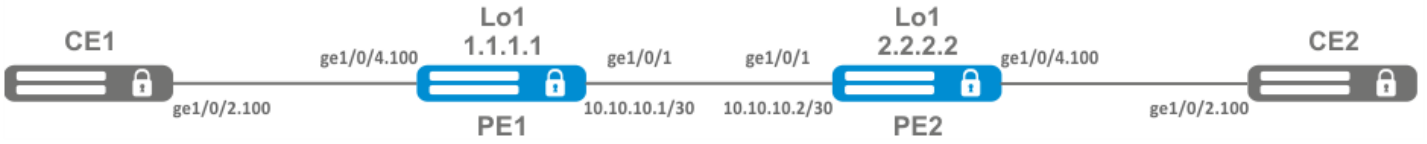
| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 7 | Задать Attached Circuit интерфейс. | `esr(config-l2vpn-p2p)# interface { <IF> \| <TUN> }` | <IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора;<br><br><TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора. |
| 8 | Включить p2p-туннель. | `esr(config-l2vpn-p2p)# enable` | |
| 9 | Задать транспортный режим (не обязательно). | `esr(config-l2vpn-p2p)# transport-mode { ethenet \| vlan }` | <ethernet> - Режим при котором при входе в pseudo-wire из заголовка удаляется 802.1Q тэг ;<br><br><vlan> - Режим при котором 802.1Q тэг может быть сохранен при передаче через pseudo-wire.<br>Значение по умолчанию: ethernet |
| 10 | Создать pseudo-wire и осуществить переход в режим настройки его параметров | `esr(config-l2vpn-p2p)# pw <PW_ID> <LSR_ID>` | <PW_ID> - идентификатор psewdowire, задается в виде числа в диапазоне [1..4294967295 ]<br><br><LSR_ID> - идентификатор LSR до которого строится pseudo-wire, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255] |
| 11 | Добавить описание для pseudo-wire (не обязательно). | `esr(config-l2vpn-pw)# description <LINE>` | <LINE> - Описание. Задается в виде строки длинной [1..255] символов |
| 12 | Задать pw-class для pseudo-wire. | `esr(config-l2vpn-pw)# pw-class <WORD>` | `<WORD> – Имя pw-class длинной [1..31] символов.` |
| 13 | Задать адрес LSR до которого устанавливается pseudo-wire (Не обязательно если neighbor address совпадает с LSR_ID). | `esr(config-l2vpn-pw)# neighbor-address <ADDR>` | <ADDR> – IP-адрес маршрутизатора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 14 | Включить pseudo-wire. | `esr(config-l2vpn-pw)# enable` | |
| | В случае если необходимо изменить параметры по умолчанию для targeted LDP сессии, обратитесь к разделу Конфигурирование параметров сессии в протоколе targeted-LDP. | | |

### 6.5.2 Пример настройки L2VPN VPWS

**Задача:**

Настроить l2vpn таким образом чтобы интерфейс ge1/0/2.100 маршрутизатора CE1 и интерфейс ge1/0/2.100 маршрутизатора CE2 работали в рамках одного широковещательного домена.




**Решение:**

Предварительно нужно:

- Включить поддержку Jumbo-фреймов с помощью команды "system jumbo-frames" (для вступления изменений в силу требуется перезагрузка устройства);
- Настроить IP-адреса на интерфейсах согласно схеме сети, приведенной на рисунке;
- Организовать обмен маршрутами между PE1 и PE2 при помощи IGP протокола (OSPF, IS-IS, RIP).

На маршрутизаторе PE1 создадим саб-интерфейс на который будем принимать трафик от CE1:

```
PE1# configure
PE1(config)# interface gigabitethernet 1/0/4.100
PE1(config-subif)# exit
```

Выставим на интерфейсе в сторону PE2 значение MTU равным 9600 для того чтобы избежать ситуации с превышением MTU после инкапсуляции MPLS заголовка, а также отключим межсетевой экран:

```
PE1#(config)# interface gigabitethernet 1/0/1
PE1(config-if-gi)# mtu 9600
PE1(config-if-gi)# ip firewall disable
PE1(config-if-gi)# exit
```

Разрешим прием пакетов с mpls заголовком на интерфейсе в сторону mpls сети (В данном примере интерфейс в сторону PE2):

```
PE1(config)# mpls
PE1(config-mpls)# forwarding interface gigabitethernet 1/0/1
```

Настроим протокол LDP и включим обнаружение соседей на интерфейсе в сторону PE2:

```
PE1(config-mpls)# ldp
PE1(config-ldp)# router-id 1.1.1.1
PE1(config-ldp)# address-family ipv4
PE1(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1
PE1(config-ldp-af-ipv4-if)# exit
PE1(config-ldp-af-ipv4)# transport-address 1.1.1.1
PE1(config-ldp-af-ipv4)# exit
PE1(config-ldp)# enable
PE1(config-ldp)# exit
```

Создадим pw-class на основе которого в дальнейшем будет создан виртуальный канал (pw). Так как в данном примере на pw будут применяться параметры по умолчанию достаточно будет указать имя класса:

```
PE1(config-mpls)# l2vpn
PE1(config-l2vpn)# pw-class for_p2p_VLAN100
PE1(config-l2vpn-pw-class)# exit
```

Создадим новый l2vpn типа p2p и добавим pw до маршрутизатора PE3, идентификатор pw для удобства возьмем равным VID (в данном случай = 100):

```
PE1(config-l2vpn)# p2p to_PE2_VLAN100
PE1(config-l2vpn-p2p)# interface gigabitethernet 1/0/4.100
PE1(config-l2vpn-p2p)# pw 100 3.3.3.3
PE1(config-l2vpn-pw)# pw-class for_p2p_VLAN100
PE1(config-l2vpn-pw)# enable
PE1(config-l2vpn-pw)# exit
PE1(config-l2vpn-p2p)# enable
PE1(config-l2vpn-p2p)# end
```

Применим конфигурацию:

```
PE1# commit
PE1# confirm
```

Проведем настройку маршрутизатора PE2 по аналогии с PE1:

```
PE2# configure
PE2(config)# interface gigabitethernet 1/0/4.100
PE2(config-subif)# exit
PE2#(config)# interface gigabitethernet 1/0/1
PE2(config-if-gi)# mtu 9600
PE1(config-if-gi)# ip firewall disable
PE1(config-if-gi)# exit
PE2(config)# mpls
PE2(config-mpls)# forwarding interface gigabitethernet 1/0/1
PE2(config-mpls)# ldp
PE2(config-ldp)# router-id 2.2.2.2
PE2(config-ldp)# address-family ipv4
PE2(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1
PE2(config-ldp-af-ipv4-if)# exit
PE2(config-ldp-af-ipv4)# transport-address 2.2.2.2
PE2(config-ldp-af-ipv4)# exit
PE2(config-ldp)# enable
PE2(config-ldp)# exit
PE2(config-mpls)# l2vpn
PE2(config-l2vpn)# pw-class for_p2p_VLAN100
PE2(config-l2vpn-pw-class)# exit
PE2(config-l2vpn)# p2p to_PE1_VLAN100
PE2(config-l2vpn-p2p)# interface gigabitethernet 1/0/4.100
PE2(config-l2vpn-p2p)# pw 100 1.1.1.1
PE2(config-l2vpn-pw)# pw-class for_p2p_VLAN100
PE2(config-l2vpn-pw)# enable
PE2(config-l2vpn-pw)# exit
PE2(config-l2vpn-p2p)# enable
PE2(config-l2vpn-p2p)# end
PE2# commit
PE2# confirm
```

Убедимся в установлении соседства по протоколу LDP и выведем информацию по статусу виртуального канала (pseudowire) между PE1 и PE2

```
PE2# show mpls ldp neighbor
Peer LDP ID: 1.1.1.1; Local LDP ID 2.2.2.2
    State: Operational
    TCP connection: 1.1.1.1:646 - 2.2.2.2:34625
    Messages sent/received: 12/12
    Uptime: 00:03:50
    LDP discovery sources:
        2.2.2.2 -> 1.1.1.1
```

```
PE2# show mpls l2vpn pseudowire
Neighbor                                PW ID           Type          Status
--------------------------------------- ----------      ----------    ------
1.1.1.1                                   100           Ethernet        Up
```

Соседство по протоколу LDP установлено, pseudowire перешел в статус 'UP'. Настройка l2vpn типа p2p завершена.

### 6.5.3 Алгоритм настройки L2VPN VPLS

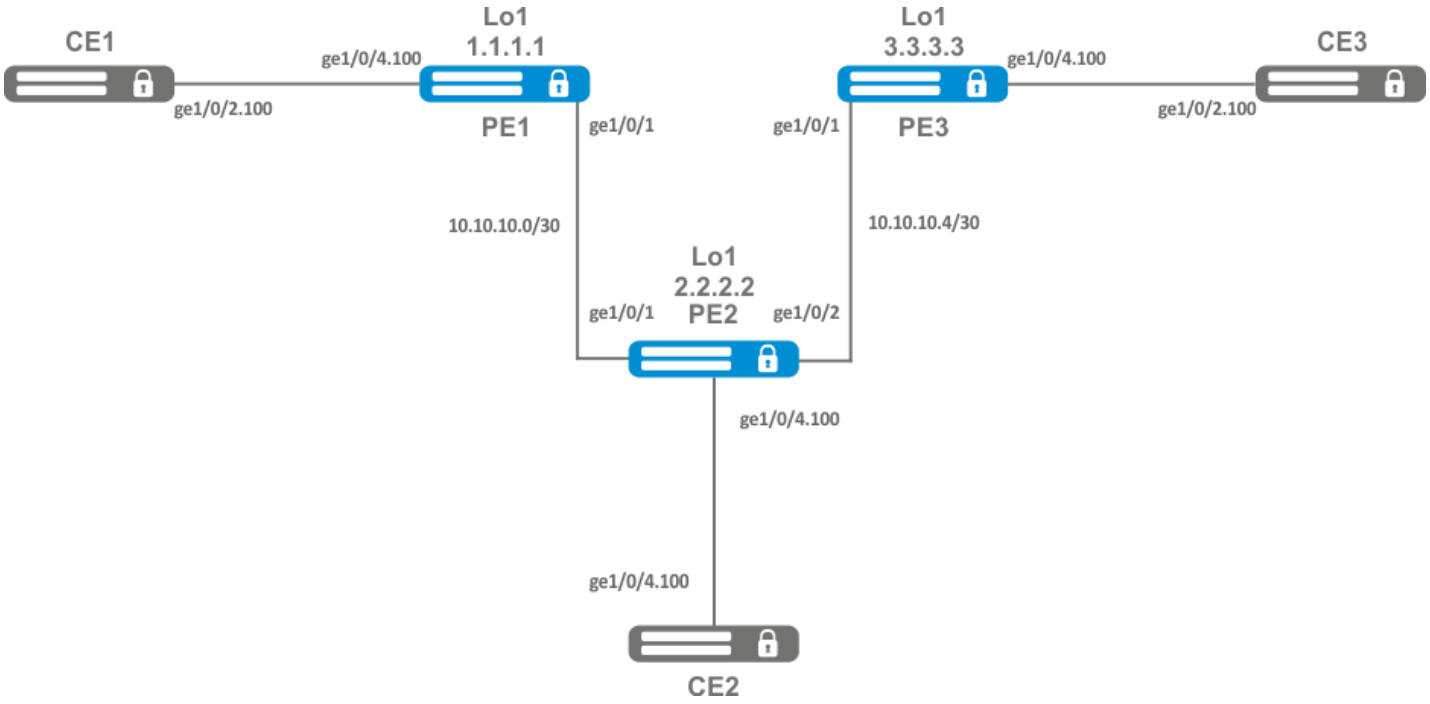
| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Настроить протокол LDP (см. раздел Конфигурирование протокола LDP). | | |
| 2 | Создать сетевой мост в системе без указания ip адреса (см. раздел Настройка Bridge). | | |
| 3 | Создать pw-class в системе и осуществить переход в режим настройки параметров pw-class. | `esr(config-l2vpn)# pw-class <WORD>` | <WORD> - Имя pw-class длинной [1..31] символов. |
| 4 | Добавить описание для pw-class (не обязательно). | `esr(config-l2vpn-pw-class)# description <LINE>` | <LINE> - Описание. Задается в виде строки длинной [1..255] символов |
| 5 | Установить значение MTU для pseudo-wire входящих в pw-class (не обязательно). | `esr(config-l2vpn-pw-class)# encapsulation mpls mtu <MTU>` | <MTU> - значение MTU, принимает значение в диапазоне [552..10000] Значение по умолчанию: 1500. |
| 6 | Отключить обмен status-tlv сообщениями (не обязательно). | `esr(config-l2vpn-pw-class)# encapsulation mpls status-tlv disable` | Значение по умолчанию: status-tlv enable |
| 7 | Создать vpls домен в системе и осуществить переход в режим настройки параметров vpls домена. | `esr(config-l2vpn)# vpls <NAME>` | <NAME> - Имя p2p сервиса, задается строкой до 31 символа. |
| 8 | Включить vpls-туннель. | `esr(config-l2vpn-vpls)# enable` | |
| 9 | Задать транспортный режим (не обязательно). | `esr(config-l2vpn-vpls)# transport-mode { ethenet \| vlan }` | <ethernet> - Режим при котором при входе в pseudo-wire из заголовка удаляется 802.1Q тэг;<br><vlan> - Режим при котором 802.1Q тэг может быть сохранен при передаче через pseudo-wire.<br>Значение по умолчанию: ethernet |
| 10 | Создать pseudo-wire и осуществить переход в режим настройки его параметров | `esr(config-l2vpn-vpls)# pw <PW_ID> <LSR_ID>` | <PW_ID> - идентификатор psewdowire, задается в виде числа в диапазоне [1..4294967295 ]<br><br><LSR_ID> - идентификатор LSR до которого строится pseudo-wire, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255] |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 11 | Добавить описание для pseudo-wire (не обязательно). | `esr(config-l2vpn-pw)# description <LINE>` | <LINE> - Описание. Задается в виде строки длинной [1..255] символов |
| 12 | Задать pw-class для pseudo-wire | `esr(config-l2vpn-pw)# pw-class <WORD>` | `<WORD> - Имя pw-class длинной [1..31] символов.` |
| 13 | Задать адрес LSR до которого устанавливается pseudo-wire(Не обязательно если neighbor address совпадает с LSR_ID). | `esr(config-l2vpn-pw)# neighbor-address <ADDR>` | <ADDR> – IP-адрес маршрутизатора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 14 | Включить pseudo-wire. | `esr(config-l2vpn-pw)# enable` | |
| 15 | В случае если топология создаваемого VPLS домена требует установить более одного pseudo-wire, повторить шаги с 10 по 14. | | |
| 16 | В случае если необходимо изменить параметры по умолчанию для targeted LDP сессии, обратитесь к разделу Конфигурирование параметров сессии в протоколе targeted-LDP. | | |

### 6.5.4 Пример настройки L2VPN VPLS

**Задача:**

Настроить l2vpn таким образом чтобы маршрутизаторы CE1,CE2,CE3 имели L2 связность через интерфейсы gi1/0/2.100



**Решение:**

Предварительно необходимо:

- Включить поддержку Jumbo-фреймов с помощью команды "system jumbo-frames" (для вступления изменений в силу требуется перезагрузка устройства);
- Настроить IP-адреса на интерфейсах согласно схеме сети, приведенной на рисунке;
- Организовать обмен маршрутами между PE1, PE2 и PE3 при помощи IGP протокола (OSPF, IS-IS, RIP);

На маршрутизаторе PE1 создадим бридж-группу и включим ее:

```
PE1# configure
PE1(config)# bridge 10
PE1(config-bridge)# enable
PE1(config-bridge)# exit
```

Интерфейсе в сторону CE1 включим в созданную бридж-группу:

```
PE1(config)# interface gigabitethernet 1/0/4.100
PE1(config-subif)# bridge-group 10
PE1(config-subif)# exit
```

Выставим на интерфейсе в сторону PE2 значение MTU равным 9600 для того чтобы избежать ситуации с превышением MTU после инкапсуляции MPLS заголовка, а также отключим межсетевой экран

```
PE1#(config)# interface gigabitethernet 1/0/1
PE1(config-if-gi)# mtu 9600
PE1(config-if-gi)# ip firewall disable
PE1(config-if-gi)# exit
```

Разрешим прием пакетов с mpls заголовком на интерфейсе в сторону mpls сети (В данном примере интерфейс в сторону PE2):

```
PE1(config)# mpls
PE1(config-mpls)# forwarding interface gigabitethernet 1/0/1
```

Настроим протокол LDP и включим обнаружение соседей на интерфейсе в сторону PE2:

```
PE1(config-mpls)# ldp
PE1(config-ldp)# router-id 1.1.1.1
PE1(config-ldp)# address-family ipv4
PE1(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1
PE1(config-ldp-af-ipv4-if)# exit
PE1(config-ldp-af-ipv4)# transport-address 1.1.1.1
PE1(config-ldp-af-ipv4)# exit
PE1(config-ldp)# enable
PE1(config-ldp)# exit
```

Создадим pw-class на основе которого в дальнейшем будет созданы виртуальные каналы (pw). Так как в данном примере на pw будут применяться параметры по умолчанию достаточно будет указать имя класса:

```
PE1(config-mpls)# l2vpn
PE1(config-l2vpn)# pw-class for_vpls1
PE1(config-l2vpn-pw-class)# exit
```

Создадим новый l2vpn типа vpls и добавим pw до маршрутизаторов PE2 и PE3, идентификатор pw для удобства возьмем равным VID (в данном случай = 100):

```
PE1(config-l2vpn)# vpls vpls1
PE1(config-l2vpn-vpls)# bridge-group 10
PE1(config-l2vpn-vpls)# pw 100 2.2.2.2
PE1(config-l2vpn-pw)# pw-class for_vpls1
PE1(config-l2vpn-pw)# enable
PE1(config-l2vpn-pw)# exit
PE1(config-l2vpn-vpls)# pw 100 3.3.3.3
PE1(config-l2vpn-pw)# pw-class for_vpls1
PE1(config-l2vpn-pw)# enable
PE1(config-l2vpn-pw)# exit
PE1(config-l2vpn-vpls)# enable
PE1(config-l2vpn-vpls)# end
```

Применим созданную конфигурацию:

```
PE1# commit
PE1# confirm
```

Проведем настройку маршрутизатора PE2 и PE3 по аналогии с PE1:

```
PE2# configure
PE2(config)# bridge 10
PE2(config-bridge)# enable
PE2(config-bridge)# exit
PE2(config)# interface gigabitethernet 1/0/4.100
PE2(config-subif)# bridge-group 10
PE2(config-subif)# exit
PE2(config)# interface gigabitethernet 1/0/2
PE2(config-if-gi)# mtu 9600
PE2(config-if-gi)# ip firewall disable
PE2(config-if-gi)# exit
PE2(config)# mpls
PE2(config-mpls)# forwarding interface gigabitethernet 1/0/1
PE2(config-mpls)# forwarding interface gigabitethernet 1/0/2
PE2(config-mpls)# ldp
PE2(config-ldp)# enable
PE2(config-ldp)# router-id 2.2.2.2
PE2(config-ldp)# address-family ipv4
PE2(config-ldp-af-ipv4)# transport-address 2.2.2.2
PE2(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1
PE2(config-ldp-af-ipv4-if)# exit
PE2(config-ldp-af-ipv4)# interface gigabitethernet 1/0/2
PE2(config-ldp-af-ipv4-if)# exit
```

```
PE2(config-ldp-af-ipv4)# exit
PE2(config-ldp)# exit
PE2(config-mpls)# l2vpn
PE2(config-l2vpn)# pw-class for_vpls1
PE2(config-l2vpn-pw-class)# exit
PE2(config-l2vpn)# vpls vpls1
PE2(config-l2vpn-vpls)# enable
PE2(config-l2vpn-vpls)# bridge-group 10
PE2(config-l2vpn-vpls)# pw 100 1.1.1.1
PE2(config-l2vpn-pw)# pw-class for_vpls1
PE2(config-l2vpn-pw)# enable
PE2(config-l2vpn-pw)# exit
PE2(config-l2vpn-vpls)# pw 100 3.3.3.3
PE2(config-l2vpn-pw)# pw-class for_vpls1
PE2(config-l2vpn-pw)# enable
PE2(config-l2vpn-pw)# end
PE2# commit
PE2# confirm
PE3(config)# bridge 10
PE3(config-bridge)# enable
PE3(config-bridge)# exit
PE3(config)# interface gigabitethernet 1/0/4.100
PE3(config-subif)# bridge-group 10
PE3(config-subif)# exit
PE3(config)# interface gigabitethernet 1/0/1
PE3(config-if-gi)# mtu 9600
PE3(config-if-gi)# ip firewall disable
PE3(config-if-gi)# exit
PE3(config)# mpls
PE3(config-mpls)# forwarding interface gigabitethernet 1/0/1
PE3(config-mpls)# exit
PE3(config)# mpls
PE3(config-mpls)# ldp
PE3(config-ldp)# enable
PE3(config-ldp)# router-id 3.3.3.3
PE3(config-ldp)# address-family ipv4
PE3(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1
PE3(config-ldp-af-ipv4-if)# exit
PE3(config-ldp-af-ipv4)# transport-address 3.3.3.3
PE3(config-ldp-af-ipv4)# exit
PE3(config-ldp)# exit
PE3(config-mpls)# l2vpn
PE3(config-l2vpn)# pw-class for_vpls
PE3(config-l2vpn-pw-class)# exit
PE3(config-l2vpn)# vpls vpls1
PE3(config-l2vpn-vpls)# enable
PE3(config-l2vpn-vpls)# bridge-group 10
PE3(config-l2vpn-vpls)# pw 100 2.2.2.2
PE3(config-l2vpn-pw)# pw-class for_vpls
PE3(config-l2vpn-pw)# enable
PE3(config-l2vpn-pw)# exit
PE3(config-l2vpn-vpls)# pw 100 1.1.1.1
PE3(config-l2vpn-pw)# pw-class for_vpls
PE3(config-l2vpn-pw)# enable
PE3(config-l2vpn-pw)# end
PE3# commit
PE3# confirm
```

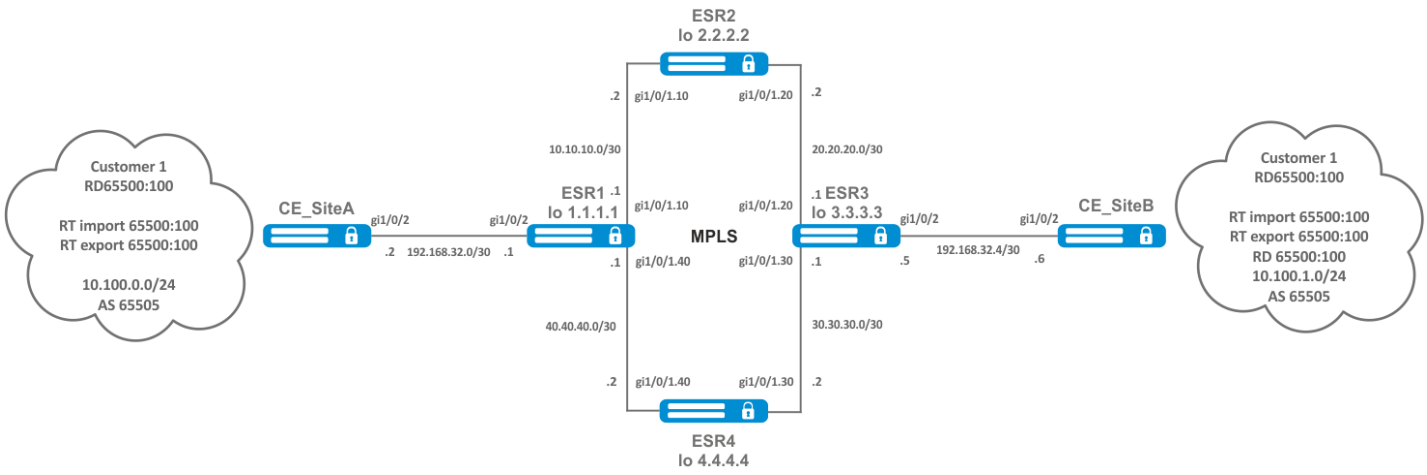
Убедимся в установлении соседства по протоколу LDP и выведем информацию по статусу виртуального канала (pseudowire) между PE1, PE2 и PE3

```
PE3# show mpls ldp neighbor
Peer LDP ID: 1.1.1.1; Local LDP ID 3.3.3.3
    State: Operational
    TCP connection: 1.1.1.1:646 - 3.3.3.3:45979
    Messages sent/received: 22/22
    Uptime: 00:13:16
    LDP discovery sources:
        3.3.3.3 -> 1.1.1.1
Peer LDP ID: 2.2.2.2; Local LDP ID 3.3.3.3
    State: Operational
    TCP connection: 2.2.2.2:646 - 3.3.3.3:59627
    Messages sent/received: 22/22
    Uptime: 00:13:20
    LDP discovery sources:
        3.3.3.3 -> 2.2.2.2
        gigabitethernet 1/0/1
```

```
PE3# show mpls l2vpn pseudowire
Neighbor                                     PW ID     Type           Status
-------------------------------------- ----------      ----------       ------
1.1.1.1                                       100        Ethernet     Up
2.2.2.2                                       100        Ethernet     Up
```

Соседство по протоколу LDP установлено, pseudowire перешел в статус 'UP'. Настройка l2vpn типа vpls завершена.

## 6.6 Конфигурирование L3VPN




### 6.6.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Настроить адресацию и один из протоколов IGP на всех P и PE маршрутизаторах | | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 2 | Настроить распространение транспортных меток по протоколу LDP | | |
| 3 | Создать VRF | `esr(config)# ip vrf <VRF>` | <VRF> – имя экземпляра VRF, задается строкой до 31 символа. |
| 4 | Указать route distinguisher для данного VRF | `esr(config-vrf)# rd <RD>` | <RD> – значение Route distinguisher, задается в одном из следующем виде:<br>• <ASN>:<nn> – где <ASN> - принимает значение [1..65535], nn - принимает значение [1..65535];<br>• <ADDR>:<nn> – где <ADDR> имеет вид - AAA.BBB.CCC.DDD/EE и AAA-DDD принимают значения [0..255], а nn - принимает значение [1..65535];<br>• <4ASN>:<nn> – где <4ASN> - принимает значение [1..4294967295], nn - принимает значение [1..65535]; |
| 5 | Указать route target import для данного VRF | `esr(config-vrf)# route-target import <RT>` | <RT> – значение route-target, задается в одном из следующих видов:<br>• <ASN>:<nn> – где <ASN> - принимает значение [1..65535], nn - принимает значение [1..65535];<br>• <ADDR>:<nn> – где <ADDR> имеет вид - AAA.BBB.CCC.DDD/EE и AAA-DDD принимают значения [0..255], а nn - принимает значение [1..65535];<br>• <4BASN>:<nn> – где <4ASN> - принимает значение [1..4294967295], nn - принимает значение [1..65535]; |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 6 | Указать route target export для данного VRF | `esr(config-vrf)# route-target export <RT>` | <RT> – значение route-target, задается в одном из следующем виде:<br>• <ASN>:<nn> – где <ASN> - принимает значение [1..65535], nn - принимает значение [1..65535];<br>• <ADDR>:<nn> – где <ADDR> имеет вид - AAA.BBB.CCC.DDD/EE и AAA-DDD принимают значения [0..255], а nn - принимает значение [1..65535];<br>• <4BASN>:<nn> – где <4ASN> - принимает значение [1..4294967295], nn - принимает значение [1..65535]; |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 7 | Указать разрешенное количество маршрутов для данного VRF | `esr(config-vrf)# ip protocols <PROTOCOLS> max-routes <VALUE>` | <PROTOCOL> – вид протокола, принимает значения: rip (только в глобальном режиме), ospf, isis, bgp;<br><br><VALUE> – количество маршрутов в маршрутной таблице, принимает значения в диапазоне:<br><br>• BGP<br>  • ESR-1700 [1..5000000];<br>  • ESR-1000/1200/1500 [1..3000000];<br>  • ESR-20/21/100/200 [1..1500000],<br>  • ESR-10/12V/12VF/14VF [1..800000].<br>• OSPF и IS-IS<br>  • ESR-1000/1200/1500/1700 [1..500000];<br>  • ESR-20/21/100/200 [1..300000];<br>  • ESR-10/12V/12VF/14VF [1..30000]. |
| 8 | В рамках настройки address-family VPNv4 протокола BGP включить передачу расширенный атрибутов | `esr(config-bgp-neighbor-af)# send-community extended` | |

### 6.6.2 Пример настройки

**Задача:**

Настроить L3VPN на базе технологии MPLS между ESR1 и ESR3. Конечным результатом настройки является появление связности между узлами, подключенными к VRF на различных маршрутизаторах сети (то есть объединение VRF на разных маршрутизаторах через MPLS-транспорт). При этом должна быть обеспечена передача сервисных MPLS-меток для сервиса L3VPN посредством MP-BGP и передача транспортных меток для достижения nexthop-адресов полученных BGP-маршрутов.

**Решение:**

1 Настройка адресации и включение IGP на маршрутизаторах

**ESR1**

```
router ospf log-adjacency-changes
router ospf 1
  router-id 1.1.1.1
  area 0.0.0.0
    enable
  exit
  enable
exit

interface loopback 1
  ip address 1.1.1.1/32
  ip ospf instance 1
  ip ospf
exit

interface gigabitethernet 1/0/1.10
  ip firewall disable
  ip address 10.10.10.1/30
  ip ospf instance 1
  ip ospf
exit

interface gigabitethernet 1/0/1.40
  ip firewall disable
  ip address 40.40.40.1/30
  ip ospf instance 1
  ip ospf
exit

system jumbo-frames
```

**ESR2**

```
router ospf log-adjacency-changes
router ospf 1
  router-id 2.2.2.2
  area 0.0.0.0
    enable
  exit
  enable
exit

interface loopback 1
  ip address 2.2.2.2/32
  ip ospf instance 1
  ip ospf
exit

interface gigabitethernet 1/0/1.10
  ip firewall disable
  ip address 10.10.10.2/30
  ip ospf instance 1
  ip ospf
exit

interface gigabitethernet 1/0/1.20
  ip firewall disable
  ip address 20.20.20.2/30
  ip ospf instance 1
  ip ospf
exit

system jumbo-frames
```

**ESR3**

```
router ospf log-adjacency-changes
  router ospf 1
  router-id 3.3.3.3
  area 0.0.0.0
    enable
  exit
  enable
exit

interface loopback 1
  ip address 3.3.3.3/32
  ip ospf instance 1
  ip ospf
exit

interface gigabitethernet 1/0/1.20
  ip firewall disable
  ip address 20.20.20.1/30
  ip ospf instance 1
  ip ospf
exit

interface gigabitethernet 1/0/1.30
  ip firewall disable
  ip address 30.30.30.1/30
  ip ospf instance 1
  ip ospf
exit

system jumbo-frames
```

**ESR4**

```
router ospf log-adjacency-changes
router ospf 1
  router-id 4.4.4.4
  area 0.0.0.0
    enable
  exit
  enable
exit

interface loopback 1
  ip address 4.4.4.4/32
  ip ospf instance 1
  ip ospf
exit

interface gigabitethernet 1/0/1.40
  ip firewall disable
  ip address 40.40.40.2/30
  ip ospf instance 1
  ip ospf
exit

interface gigabitethernet 1/0/1.30
  ip firewall disable
  ip address 30.30.30.2/30
  ip ospf instance 1
  ip ospf
exit

system jumbo-frames
```

Необходимо убедиться, что протокол запущен на каждом маршрутизаторе.

```
ESR1# show ip ospf neighbors

  Router ID        Pri  State          DTime  Interface      Router IP
  ---------        ---  -----          -----  -------------  ---------
  2.2.2.2          128  Full/BDR       00:39  gi1/0/1.10     10.10.10.2
  4.4.4.4          128  Full/BDR       00:32  gi1/0/1.40     40.40.40.2
```

```
ESR1# show ip ospf
O       40.40.40.0/30      [150/10]          dev gi1/0/1.40
                    [ospf1 1970-01-08]  (1.1.1.1)
O     * 30.30.30.0/30      [150/20]          via 40.40.40.2 on gi1/0/1.40
      [ospf1 1970-01-08]  (3.3.3.3)
O       1.1.1.1/32              [150/0]             dev lo1      [ospf1 1970-01-08]
 (1.1.1.1)
O     * 4.4.4.4/32             [150/10]          via 40.40.40.2 on gi1/0/1.40
      [ospf1 1970-01-08]  (4.4.4.4)
O     * 20.20.20.0/30      [150/20]          via 10.10.10.2 on gi1/0/1.10
      [ospf1 22:05:45]  (3.3.3.3)
O       10.10.10.0/30      [150/10]          dev gi1/0/1.10
                    [ospf1 22:05:33]  (1.1.1.1)
O     * 3.3.3.3/32             [150/20]          multipath
                         [ospf1 22:05:45]  (3.3.3.3)
                                     via 40.40.40.2 on gi1/0/1.40 weight 1
O     * 2.2.2.2/32             [150/10]          via 10.10.10.2 on gi1/0/1.10
      [ospf1 22:05:45]  (2.2.2.2)
```

2 Настройка LDP:

**ESR1**

```
mpls
  ldp
    address-family ipv4
      transport-address 1.1.1.1
      interface gigabitethernet 1/0/1.10
      exit
      interface gigabitethernet 1/0/1.40
      exit
    exit
    enable
  exit
  forwarding interface gigabitethernet 1/0/1.10
  forwarding interface gigabitethernet 1/0/1.40
exit
```

**ESR2**

```
mpls
  ldp
    address-family ipv4
      transport-address 2.2.2.2
      interface gigabitethernet 1/0/1.10
      exit
      interface gigabitethernet 1/0/1.20
      exit
    exit
    enable
  exit
  forwarding interface gigabitethernet 1/0/1.10
  forwarding interface gigabitethernet 1/0/1.20
exit
```

**ESR3**

```
mpls
  ldp
    address-family ipv4
      transport-address 3.3.3.3
      interface gigabitethernet 1/0/1.20
      exit
      interface gigabitethernet 1/0/1.30
      exit
    exit
    enable
  exit
  forwarding interface gigabitethernet 1/0/1.20
  forwarding interface gigabitethernet 1/0/1.30
exit
```

**ESR4**

```
mpls
  ldp
    address-family ipv4
      transport-address 4.4.4.4
      interface gigabitethernet 1/0/1.30
      exit
      interface gigabitethernet 1/0/1.40
      exit
    exit
    enable
  exit
  forwarding interface gigabitethernet 1/0/1.30
  forwarding interface gigabitethernet 1/0/1.40
exit
```

Для проверки сходимости LDP можно воспользоваться одной из команд:

```
ESR1# show mpls ldp neighbor
Peer LDP ID: 2.2.2.2; Local LDP ID 1.1.1.1
    State: Operational
    TCP connection: 2.2.2.2:33933 - 1.1.1.1:646
    Messages sent/received: 1059/1070
    Uptime: 17:32:07
    LDP discovery sources:
        gigabitethernet 1/0/1.10
Peer LDP ID: 4.4.4.4; Local LDP ID 1.1.1.1
    State: Operational
    TCP connection: 4.4.4.4:40894 - 1.1.1.1:646
    Messages sent/received: 1376/1386
    Uptime: 22:38:38
    LDP discovery sources:
        gigabitethernet 1/0/1.40
```

### 3 Настройка MP-BGP

Создадим VRF на ESR1 и ESR3 соответственно. Укажем RD, rt-export/import в соответствии с нашей схемой.

Без указание атрибутов RD и RT маршрутная информация не попадет в таблицу VPNv4.

**ESR1**

```
ESR1(config)# ip vrf Customer1
ESR1(config-vrf)# ip protocols bgp max-routes 1000
ESR1(config-vrf)# rd 65500:100
ESR1(config-vrf)# route-target import 65500:100
ESR1(config-vrf)# route-target export 65500:100
```

**ESR3**

```
ESR3(config)# ip vrf Customer1
ESR3(config-vrf)# ip protocols bgp max-routes 1000
ESR3(config-vrf)# rd 65500:100
ESR3(config-vrf)# route-target export 65500:100
ESR3(config-vrf)# route-target import 65500:100
ESR3(config-vrf)# exit
```

Настроим iBGP между ESR1 и ESR3. Включим отправку extended community на обоих устройствах.

**ESR1**

```
ESR1(config)# router bgp log-neighbor-changes
ESR1(config)# router bgp 65500
ESR1(config-bgp)# router-id 1.1.1.1
ESR1(config-bgp)# enable
ESR1(config-bgp)# neighbor 3.3.3.3
ESR1(config-bgp-neighbor)# remote-as 65500
ESR1(config-bgp-neighbor)# update-source 1.1.1.1
ESR1(config-bgp-neighbor)# enable
ESR1(config-bgp-neighbor)# address-family ipv4 unicast
ESR1(config-bgp-neighbor-af)# enable
ESR1(config-bgp-neighbor-af)# exit
ESR1(config-bgp-neighbor)# address-family vpnv4 unicast
ESR1(config-bgp-neighbor-af)# send-community extended
ESR1(config-bgp-neighbor-af)# enable
```

**ESR3**

```
ESR3(config)# router bgp log-neighbor-changes
ESR3(config)# router bgp 65500
ESR3(config-bgp)# router-id 3.3.3.3
ESR3(config-bgp)# enable
ESR3(config-bgp)# neighbor 1.1.1.1
ESR3(config-bgp-neighbor)# remote-as 65500
ESR3(config-bgp-neighbor)# update-source 3.3.3.3
ESR3(config-bgp-neighbor)# enable
ESR3(config-bgp-neighbor)# address-family ipv4 unicast
ESR3(config-bgp-neighbor-af)# enable
ESR3(config-bgp-neighbor-af)# exit
ESR3(config-bgp-neighbor)# address-family vpnv4 unicast
ESR3(config-bgp-neighbor-af)# send-community extended
ESR3(config-bgp-neighbor-af)# enable
```

Необходимо убедиться, что BGP-сессия успешно установлена.

```
ESR1# show ip bgp neighbors
BGP neighbor is 3.3.3.3
    BGP state: Established
    Neighbor address: 3.3.3.3
    Neighbor AS: 65500
    Neighbor ID: 3.3.3.3
    Neighbor caps: refresh enhanced-refresh restart-aware AS4
    Session: internal multihop AS4
    Source address: 1.1.1.1
    Weight: 0
    Hold timer: 126/180
    Keepalive timer: 40/60
    Address family ipv4 unicast:
    Default originate: No
    Default information originate: No
    Uptime: 88495 s
```

4 Настройка маршрутизации PE-CE

Customer1 анонсирует по BGP(AS65505) подсеть 10.100.0.0/24. Настроим eBGP-сессию между CE_SiteA и PE.

По-умолчанию: для EBGP анонсирование маршрутов запрещено, необходимо сконфигурировать разрешающее правило; для IBGP-анонсирование маршрутов разрешено.

***CE_SiteA***

Настроим соответствующие интерфейсы. Также создадим route-map, в котором укажем подсети, разрешенные для анонсирования.

**CE _SiteA**

```
interface gigabitethernet 1/0/2
  ip firewall disable
  ip address 192.168.32.2/30
exit

interface loopback 1
  ip address 10.100.0.1/24
exit

route-map OUTPUT
  rule 1
    match ip address 10.100.0.0/24
    action permit
```

Настроим eBGP между ESR1 и CE_SiteA.

**CE_SiteA**

```
router bgp log-neighbor-changes
router bgp 65505
  router-id 192.168.32.1
  neighbor 192.168.32.1
    remote-as 65500
    allow-local-as 1
    update-source 192.168.32.2
    address-family ipv4 unicast
      route-map OUTPUT out
      enable
    exit
    enable
  exit
  address-family ipv4 unicast
    network 10.100.0.0/24
    exit
  enable
```

***ESR1***

Настроим интерфейс в сторону CE. Также создадим route-map, в котором укажем подсети, разрешенные для анонсирования.

**ESR1**

```
interface gigabitethernet 1/0/2
  ip vrf forwarding Customer1
  description "Customer1"
  ip firewall disable
  ip address 192.168.32.1/30

Создаем route-map

route-map OUTPUT
  rule 1
    action permit
```

Настроим eBGP между ESR1 и CE_SiteA.

**ESR1**

```
router bgp 65500
  vrf Customer1
    router-id 192.168.32.1
    neighbor 192.168.32.2
    remote-as 65505
    update-source 192.168.32.1
    address-family ipv4 unicast
```

Разрешим передачу маршрутов BGP пиру.

**ESR1**

```
route-map OUTPUT out
  enable
exit
enable
exit
```

Разрешим пересылку маршрутов из VRF в таблицу VPNv4 unicast

**ESR1**

```
address-family ipv4 unicast
redistribute connected
redistribute bgp 65500
exit
enable
exit
```

Для проверки принятых и анонсированных маршрутов можно воспользоваться следующими командами:

```
ESR1# show ip bgp 65500 vrf Customer1 neighbors 192.168.32.2 advertise-routes
Status codes: u - unicast, b - broadcast, m - multicast, a - anycast
              * - valid, > - best
Origin codes: i - IGP, e - EGP, ? - incomplete


     Network              Next Hop             Metric  LocPrf      Weight Path

*> u 10.100.1.0/24        192.168.32.1                 100                 65500 i
*> u 192.168.32.4/30      192.168.32.1                 100                 65500 i
```

Вывод аноснируемых маршрутов для определенного пира. Маршрутная информация отображается после применения фильтрации.

```
ESR1# show ip bgp 65500 vrf Customer1 neighbors 192.168.32.2 routes
Status codes: u - unicast, b - broadcast, m - multicast, a - anycast
              * - valid, > - best
Origin codes: i - IGP, e - EGP, ? - incomplete


     Network              Next Hop             Metric  LocPrf      Weight Path

*> u 10.100.0.0/24        192.168.32.2                 100         0      65505
```

Вывод принятой маршрутной информации от определенного пира. Маршрутная информация отображается после применения фильтрации.

***CE_SiteB***

Настроим соответствующие интерфейсы.

**CE_SiteB**

```
interface gigabitethernet 1/0/2
ip firewall disable
ip address 192.168.32.6/30
exit

interface loopback 1
ip address 10.100.1.1/24
exit

route-map OUTPUT
rule 1
match ip address 10.100.1.0/24
action permit
```

Настроим eBGP между ESR3 и CE_SiteB.

**CE_SiteB**

```
router bgp 65505
router-id 192.168.32.6
neighbor 192.168.32.5
remote-as 65500
allow-local-as 1
update-source 192.168.32.6
address-family ipv4 unicast
route-map OUTPUT out
enable
exit
enable
exit
address-family ipv4 unicast
network 10.100.1.0/24
exit
enable
```

***ESR3***

Настроим интерфейс в сторону CE.

**ESR3**

```
interface gigabitethernet 1/0/2
ip vrf forwarding Customer1
description "Customer1"
ip firewall disable
ip address 192.168.32.5/30
```

Создадим route-map, в котором укажем подсети, разрешенные для анонсирования.

**ESR3**

```
route-map OUTPUT
rule 1
action permit
```

Настроим eBGP с между ESR3 и CE_SiteB.

**ESR3**

```
router bgp 65500
vrf Customer1
router-id 192.168.32.5
neighbor 192.168.32.6
remote-as 65505
update-source 192.168.32.5
address-family ipv4 unicast
```

Разрешим передачу маршрутов BGP пиру.

**ESR3**

```
route-map OUTPUT out
enable
exit
enable
exit
```

Разрешим пересылку маршрутов из VRF в VPNV4 для address-family IPv4.

**ESR3**

```
address-family ipv4 unicast
redistribute connected
redistribute bgp 65500
exit
enable
exit
```

Для просмотра VPNv4 таблицы можно воспользоваться одной из следущих команд:

```
ESR1# show ip bgp vpnv4 unicast all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete


Codes Route Distinguisher   IP Prefix          Next hop        Metric     Label
  LocPrf     Weight Path
----- --------------------- ------------------ --------------- ---------- -------
---------- ------ -----------------
*>    65500:100             10.100.0.0/24      --              --         23      --
        --     ?
*>i   65500:100             192.168.32.4/30    3.3.3.3         --         84
     100        0      i
*>i   65500:100             10.100.1.0/24      3.3.3.3         --         84
     100        0      i
```

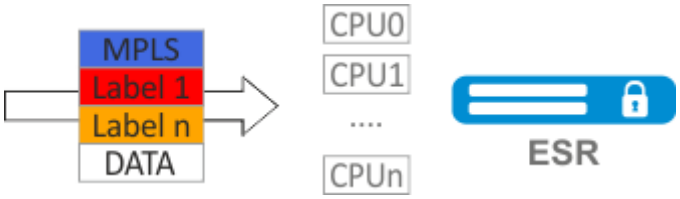
Выводит все принятые VPNv4 маршруты после применения фильтрации

## 6.7 Балансировка трафика MPLS

Маршутизаторы ESR имеют многоядерную архитектуру. Одним из первых звеньев обработки поступающего трафика является load balancer daemon(lbd), который выполняет две основных функции:

1) Равномерно распределяет нагрузку между всеми CPU маршрутизатора.

2) Выявляет аномальные ситуации с высокой нагрузкой на отдельные CPU, и перераспределяет обработку с этих CPU на менее загруженные.




По-умолчанию, lbd использует только MPLS метки для вычисления хэша и дальнейшего распределения нагрузки на различные CPU. Данное поведение не всегда дает преимущество, особенное когда существует "большие" однородные потоки MPLS трафика. Для добавление энтропии в хэш можно включить дополнительный функционал:

**cpu load-balance mpls passenger ip**
Включает возможность "заглядывать" дальше MPLS заголовка для поиска IP-заголовка, и добавления ip-src и ip-dst в расчет хэша.

**cpu load-balance mpls passenger ip-over-ethernet-pseudowire-with-cw**
**cpu load-balance mpls passenger ip-over-ethernet-pseudowire-without-cw**
Позволяет явно указать, используется ли при построении L2VPN функционал Control Word. Позволяет исключить возникновение ошибки, когда пакет с наличием Control word может быть ошибочно распознан как пакет без Control Word.

### 6.7.1 Пример настройки

**Задача:**

Включить балансировку L2VPN трафика без использования функционала Control Word.

**Решение:**

**ESR**

```
ESR(config)# system cpu load-balance mpls passenger ip
ESR(config)# system cpu load-balance mpls passenger ipoe-pw-without-cw
```

# 7 Управление безопасностью



## 7.1 Настройка AAA

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

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

### 7.1.1 Алгоритм настройки локальной аутентификации

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

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

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

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 13 | Установить минимальное количество цифр в пароле локального пользователя и ENABLE-пароле (не обязательно) | `esr(config)# security passwords numeric-count <COUNT>` | <COUNT> – минимальное количество цифр в пароле. Принимает значение в диапазоне [0..128].<br><br>Значение по умолчанию: 0 |
| 14 | Установить минимальное количество специальных символов в пароле локального пользователя и ENABLE-пароле (не обязательно) | `esr(config)# security passwords special-case <COUNT>` | <COUNT> – минимальное количество специальных символов в пароле. Принимает значение в диапазоне [0..128].<br><br>Значение по умолчанию: 0 |
| 15 | Добавить пользователя в локальную базу и перейти в режим настройки параметров пользователя | `esr(config)# username <NAME>` | <NAME> – имя пользователя, задаётся строкой до 31 символа. |
| 16 | Установить пароль пользователя | `esr(config-user)# password { <CLEAR-TEXT> \| encrypted <HASH_SHA512> }` | <CLEAR-TEXT> – пароль, задаётся строкой [8 .. 32] символов, принимает значения [0-9a-fA-F];<br><br><HASH_SHA512> – хеш пароля по алгоритму sha512, задаётся строкой из 110 символов. |
| 17 | Установить уровень привилегий пользователя | `esr(config-user)# privilege <PRIV>` | <PRIV> – необходимый уровень привилегий. Принимает значение [1..15]. |
| 18 | Перейти в режим конфигурирования соответствующего терминала | `esr(config)# line console`<br>или<br>`esr(config)# line telnet`<br>или<br>`esr(config)# line ssh` | |
| 19 | Активировать список аутентификации входа пользователей в систему | `esr(config-line-ssh)# login authentication <NAME>` | <NAME> – имя списка, задаётся строкой до 31 символа. |
| 20 | Активировать список аутентификации повышения привилегий пользователей | `esr(config-line-ssh)# enable authentication <NAME>` | <NAME> – имя списка, задаётся строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 21 | Задать интервал, по истечении которого будет разрываться бездействующая сессия | `esr(config-line-ssh)# exec-timeout <SEC>` | <SEC> – период времени в минутах, принимает значения [1..65535]. |

### 7.1.2 Алгоритм настройки AAA по протоколу RADIUS

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Задать глобальное значение кода DSCP для использования в IP-заголовках исходящих пакетов RADIUS-сервера (не обязательно). | `esr(config)# radius-server dscp <DSCP>` | <DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].<br><br>Значение по умолчанию: 63. |
| 2 | Задать глобальное значение количества перезапросов к последнему активному RADIUS-серверу (не обязательно). | `esr(config)# radius-server retransmit <COUNT>` | <COUNT> – количество перезапросов к RADIUS-серверу, принимает значения [1..10].<br><br>Значение по умолчанию: 1. |
| 3 | Задать глобальное значение интервала, по истечении которого маршрутизатор считает, что RADIUS-сервер недоступен (не обязательно). | `esr(config)# radius-server timeout <SEC>` | <SEC> – период времени в секундах, принимает значения [1..30].<br><br>Значение по умолчанию: 3 секунды. |
| 4 | Добавить RADIUS-сервер в список используемых серверов и перейти в режим его конфигурирования. | `esr(config)# radius-server host { <IP-ADDR> \| <IPV6-ADDR> } [ vrf <VRF> ] esr(config-radius-server)#` | <IP-ADDR> – IP-адрес RADIUS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];<br><br><IPV6-ADDR> – IPv6-адрес RADIUS-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]<br><br><VRF> – имя экземпляра VRF, задается строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 5 | Указать количество неудачных попыток аутентификации для блокировки логина пользователя и времени блокировки (не обязательно). | `aaa authentication attempts max-fail <COUNT> <TIME>` | <COUNT> – количество неудачных попыток аутентификации, после которых произойдет блокировка пользователя, принимает значения [1..65535];<br><br><TIME> – интервал времени в секундах, на который будет заблокирован пользователь, принимает значения [1..65535].<br><br>Значение по умолчанию:<br><br><COUNT> – 5; <TIME> – 300 |
| 6 | Задать пароль для аутентификации на удаленном RADIUS-сервере. | `esr(config-radius-server)# key ascii-text { <TEXT> \| encrypted <ENCRYPTED-TEXT> }` | <TEXT> – строка [8..16] ASCII-символов;<br><br><ENCRYPTED-TEXT> – зашифрованный пароль, размером [8..16] байт, задаётся строкой [16..32] символов. |
| 7 | Задать приоритет использования удаленного RADIUS-сервера (не обязательно). | `esr(config-radius-server)# priority <PRIORITY>` | <PRIORITY> – приоритет использования удаленного сервера, принимает значения [1..65535].<br><br>Чем ниже значение, тем приоритетнее сервер.<br><br>Значение по умолчанию: 1. |
| 8 | Задать интервал, по истечении которого маршрутизатор считает, что данный RADIUS-сервер недоступен (не обязательно). | `esr(config-radius-server)# timeout <SEC>` | <SEC> – период времени в секундах, принимает значения [1..30].<br><br>Значение по умолчанию: используется значение глобального таймера. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 9 | Задать IPv4/IPv6-адрес, который будет использоваться в качестве IP/IPv6-адреса источника в отправляемых RADIUS-пакетах. | `esr(config-radius-server)# source-address { <ADDR> \| <IPV6-ADDR> }` | <ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];<br><br><IPV6-ADDR> – IPv6-адрес источника, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. |
| 10 | Указать radius в качестве метода аутентификации. | `esr(config)# aaa authentication login { default \| <NAME> } <METHOD 1> [ <METHOD 2> ] [ <METHOD 3> ] [ <METHOD 4> ]` | <NAME> – имя списка, задаётся строкой до 31 символа.<br><br>Способы аутентификации:<br>• local – аутентификация с помощью локальной базы пользователей;<br>• tacacs – аутентификация по списку TACACS-серверов;<br>• radius – аутентификация по списку RADIUS-серверов;<br>• ldap – аутентификация по списку LDAP-серверов. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 11 | Указать radius в качестве способа аутентификации повышения привилегий пользователей. | `esr(config)# aaa authentication enable <NAME><METHOD 1> [ <METHOD 2> ] [ <METHOD 3> ] [ <METHOD 4> ]` | <NAME> – имя списка строка до 31 символа;<br>• default – имя списка по умолчанию.<br><METHOD> – способы аутентификации:<br>• enable – аутентификация с помощью enable-паролей;<br>• tacacs – аутентификация по протоколу TACACS;<br>• radius – аутентификация по протоколу RADIUS;<br>• ldap – аутентификация по протоколу LDAP. |
| 12 | Указать способ перебора методов аутентификации в случае отказа (не обязательно). | `esr(config)# aaa authentication mode <MODE>` | <MODE> – способы перебора методов:<br>• chain – если сервер вернул FAIL, переход к следующему в цепочке методу аутентификации;<br>• break – если сервер вернул FAIL, прекратить попытки аутентификации. Если сервер недоступен, продолжить попытки аутентификации следующими в цепочке методами.<br>Значение по умолчанию: chain. |
| 13 | Сконфигурировать radius в списке способов учета сессий пользователей (не обязательно). | `esr(config)# aaa accounting login start-stop <METHOD 1> [ <METHOD 2> ]` | <METHOD> – способы учета:<br>• tacacs – учет сессий по протоколу TACACS;<br>• radius – учет сессий по протоколу RADIUS. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 14 | Перейти в режим конфигурирования соответствующего терминала. | `esr(config)# line <TYPE>` | <TYPE> – тип консоли:<br>• console – локальная консоль;<br>• ssh – защищенная удаленная консоль. |
| 15 | Активировать список аутентификации входа пользователей в систему. | `esr(config-line-console)# login authentication <NAME>` | <NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 8. |
| 16 | Активировать список аутентификации повышения привилегий пользователей. | `esr(config-line-console)# enable authentication <NAME>` | <NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 9. |

### 7.1.3 Алгоритм настройки AAA по протоколу TACACS

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Задать глобальное значение кода DSCP для использования в IP-заголовках исходящих пакетов TACACS-сервера (не обязательно). | `esr(config)# tacacs-server dscp <DSCP>` | <DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].<br><br>Значение по умолчанию: 63. |
| 2 | Задать глобальное значение интервала, по истечении которого маршрутизатор считает, что TACACS-сервер недоступен (не обязательно). | `esr(config)# tacacs-server timeout <SEC>` | <SEC> – период времени в секундах, принимает значения [1..30].<br><br>Значение по умолчанию: 3 секунды. |
| 3 | Добавить TACACS-сервер в список используемых серверов и перейти в режим его конфигурирования. | `esr(config)# tacacs -server host { <IP-ADDR> \| <IPV6-ADDR> } [ vrf <VRF> ]`<br>`esr(config- tacacs -server)#` | <IP-ADDR> – IP-адрес TACACS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]<br><br><IPV6-ADDR> – IPv6-адрес TACACS -сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]<br><br><VRF> – имя экземпляра VRF, задается строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 4 | Указать количество неудачных попыток аутентификации для блокировки логина пользователя и время блокировки (не обязательно) | `aaa authentication attempts max-fail <COUNT> <TIME>` | <COUNT> – количество неудачных попыток аутентификации, после которых произойдет блокировка пользователя, принимает значения [1..65535];<br><br><TIME> – интервал времени в минутах, на который будет заблокирован пользователь, принимает значения [1..65535].<br><br>Значение по умолчанию:<br><br><COUNT> – 5; <TIME> – 300 |
| 5 | Задать пароль для аутентификации на удаленном TACACS-сервере | `esr(config-tacacs-server)# key ascii-text { <TEXT> \| encrypted <ENCRYPTED-TEXT> }` | <TEXT> – строка [8..16] ASCII-символов;<br><br><ENCRYPTED-TEXT> – зашифрованный пароль, размером [8..16] байт, задаётся строкой [16..32] символов. |
| 6 | Задать номер порта для обмена данными с удаленным TACACS-сервером (не обязательно). | `esr(config-tacacs-server)# port <PORT>` | <PORT> – номер TCP-порта для обмена данными с удаленным сервером, принимает значения [1..65535].<br><br>Значение по умолчанию: 49 для TACACS-сервера. |
| 7 | Задать приоритет использования удаленного TACACS сервера (не обязательно). | `esr(config-tacacs-server)# priority <PRIORITY>` | <PRIORITY> – приоритет использования удаленного сервера, принимает значения [1..65535].<br><br>Чем ниже значение, тем приоритетнее сервер.<br><br>Значение по умолчанию: 1. |
| 8 | Задать IPv4/IPv6-адрес, который будет использоваться в качестве IP/IPv6-адреса источника в отправляемых TACACS-пакетах. | `esr(config-radius-tacacs)# source-address { <ADDR> \| <IPV6-ADDR> }` | <ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 9 | Указать TACACS в качестве способа аутентификации повышения привилегий пользователей. | `esr(config)# aaa authentication enable <NAME><METHOD 1> [ <METHOD 2> ] [ <METHOD 3> ] [ <METHOD 4> ]` | <NAME> – имя списка строка до 31 символа;<br>• default – имя списка по умолчанию.<br><METHOD> – способы аутентификации:<br>• enable – аутентификация с помощью enable-паролей;<br>• tacacs – аутентификация по протоколу TACACS;<br>• radius – аутентификация по протоколу RADIUS;<br>• ldap – аутентификация по протоколу LDAP. |
| 10 | Указать способ перебора методов аутентификации в случае отказа (не обязательно). | `esr(config)# aaa authentication mode <MODE>` | <MODE> – способы перебора методов:<br>• chain – если сервер вернул FAIL, переход к следующему в цепочке методу аутентификации;<br>• break – если сервер вернул FAIL, прекратить попытки аутентификации. Если сервер недоступен, продолжить попытки аутентификации следующими в цепочке методами.<br>Значение по умолчанию: chain. |
| 11 | Сконфигурировать список способов учета команд, введённых в CLI (не обязательно). | `esr(config)# aaa accounting commands stop-only tacacs` | |
| 12 | Сконфигурировать tacacs в списке способов учета сессий пользователей (не обязательно). | `esr(config)# aaa accounting login start-stop <METHOD 1> [ <METHOD 2> ]` | <METHOD> – способы учета:<br>• tacacs – учет сессий по протоколу TACACS;<br>• radius – учет сессий по протоколу RADIUS. |
| 13 | Перейти в режим конфигурирования соответствующего терминала. | `esr(config)# line <TYPE>` | <TYPE> – тип консоли:<br>• console – локальная консоль;<br>• ssh – защищенная удаленная консоль. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 14 | Активировать список аутентификации входа пользователей в систему. | `esr(config-line-console)# login authentication <NAME>` | <NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 7. |
| 15 | Активировать список аутентификации повышения привилегий пользователей. | `esr(config-line-console)# enable authentication <NAME>` | <NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 8. |

### 7.1.4 Алгоритм настройки AAA по протоколу LDAP

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

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

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 11 | Добавить LDAP-сервер в список используемых серверов и перейти в режим его конфигурирования. | `esr(config)# ldap -server host { <IP-ADDR> \| <IPV6-ADDR> }`<br>`[ vrf <VRF> ]`<br>`esr(config- ldap -server)#` | <IP-ADDR> – IP-адрес LDAP-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]<br><br><IPV6-ADDR> – IPv6-адрес LDAP-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]<br><br><VRF> – имя экземпляра VRF, задается строкой до 31 символа. |
| 12 | Указать количество неудачных попыток аутентификации для блокировки логина пользователя и время блокировки (не обязательно) | `aaa authentication attempts max-fail <COUNT> <TIME>` | <COUNT> – количество неудачных попыток аутентификации, после которых произойдет блокировка пользователя, принимает значения [1..65535];<br><br><TIME> – интервал времени в минутах, на который будет заблокирован пользователь, принимает значения [1..65535].<br><br>Значение по умолчанию:<br><br><COUNT> – 5; <TIME> – 300 |
| 13 | Задать номер порта для обмена данными с удаленным LDAP-сервером (не обязательно). | `esr(config-ldap-server)# port <PORT>` | <PORT> – номер TCP-порта для обмена данными с удаленным сервером, принимает значения [1..65535].<br><br>Значение по умолчанию: 389 для LDAP-сервера. |
| 14 | Задать приоритет использования удаленного LDAP-сервера (не обязательно). | `esr(config-ldap-server)# priority <PRIORITY>` | <PRIORITY> – приоритет использования удаленного сервера, принимает значения [1..65535].<br><br>Чем ниже значение, тем приоритетнее сервер.<br><br>Значение по умолчанию: 1. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 15 | Задать IPv4/IPv6-адрес, который будет использоваться в качестве IP/IPv6-адреса источника в отправляемых LDAP-пакетах. | `esr(config-ldap-server)# source-address { <ADDR> \| <IPV6-ADDR> }` | <ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];<br><br><IPV6-ADDR> – IPv6-адрес источника, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. |
| 16 | Указать LDAP в качестве метода аутентификации. | `esr(config)# aaa authentication login { default \| <NAME> } <METHOD 1> [ <METHOD 2> ] [ <METHOD 3> ] [ <METHOD 4> ]` | <NAME> – имя списка, задаётся строкой до 31 символа.<br><br>Способы аутентификации:<br>• local – аутентификация с помощью локальной базы пользователей;<br>• tacacs – аутентификация по списку TACACS-серверов;<br>• radius – аутентификация по списку RADIUS-серверов;<br>• ldap – аутентификация по списку LDAP-серверов. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 17 | Указать LDAP в качестве способа аутентификации повышения привилегий пользователей. | `esr(config)# aaa authentication enable <NAME> <METHOD 1> [ <METHOD 2> ] [ <METHOD 3> ] [ <METHOD 4> ]` | <NAME> – имя списка строка до 31 символа;<br>• default – имя списка по умолчанию.<br><METHOD> – способы аутентификации:<br>• enable – аутентификация с помощью enable-паролей;<br>• tacacs – аутентификация по протоколу TACACS;<br>• radius – аутентификация по протоколу RADIUS;<br>• ldap – аутентификация по протоколу LDAP. |
| 18 | Указать способ перебора методов аутентификации в случае отказа. | `esr(config)# aaa authentication mode <MODE>` | <MODE> – способы перебора методов:<br>• chain – если сервер вернул FAIL, переход к следующему в цепочке методу аутентификации;<br>• break – если сервер вернул FAIL, прекратить попытки аутентификации. Если сервер недоступен, продолжить попытки аутентификации следующими в цепочке методами.<br>Значение по умолчанию: chain. |
| 19 | Перейти в режим конфигурирования соответствующего терминала. | `esr(config)# line <TYPE>` | <TYPE> – тип консоли:<br>• console – локальная консоль;<br>• ssh – защищенная удаленная консоль. |
| 20 | Активировать список аутентификации входа пользователей в систему. | `esr(config-line-console)# login authentication <NAME>` | <NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 14. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 21 | Активировать список аутентификации повышения привилегий пользователей. | `esr(config-line-console)# enable authentication <NAME>` | <NAME> – имя списка, задаётся строкой до 31 символа. Создано на шаге 15. |

### 7.1.5 Пример настройки аутентификации по telnet через RADIUS-сервер

**Задача:**

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

**Решение:**

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

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

Создадим профиль аутентификации:

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

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

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

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

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

Посмотреть профили аутентификации можно командой:

```
esr# show aaa authentication
```

## 7.2 Настройка привилегий команд

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

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

- *15 уровень* – позволяет использовать все команды.

### 7.2.1 Алгоритм настройки

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

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

<COMMAND-MODE> – командный режим;

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

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

### 7.2.2 Пример настройки привилегий команд

**Задача:**

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

**Решение:**

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

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

## 7.3 Настройка логирования и защиты от сетевых атак

### 7.3.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Включить защиту от ICMP flood атак. | `esr(config)# ip firewall screen dos-defense icmp-threshold { <NUM> }` | <NUM> – количество ICMP-пакетов в секунду задается в диапазоне [1..10000]. |
| 2 | Включить защиту от land атак. | `esr(config)# firewall screen dos-defense land` | |
| 3 | Включить ограничение количества одновременных сессий на основании адреса назначения. | `esr(config)# ip firewall screen dos-defense limit-session-destination { <NUM> }` | <NUM> – ограничение количества IP-сессий задается в диапазоне [1..10000]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 4 | Включить ограничение количества одновременных сессий на основании адреса источника, которое смягчает DoS-атаки. | `esr(config)# ip firewall screen dos-defense limit-session-source { <NUM> }` | <NUM> – ограничение количества IP-сессий задается в диапазоне [1..10000]. |
| 5 | Включить защиту от SYN flood атак. | `esr(config)# ip firewall screen dos-defense syn-flood { <NUM> } [src-dsr]` | <NUM> – максимальное количество TCP пакетов с установленным флагом SYN в секунду задается в диапазоне [1..10000].<br><br>src-dst – ограничение количества TCP пакетов с установленным флагом SYN на основании адреса источника и адреса назначения. |
| 6 | Включить защиту от UDP flood атак. | `esr(config)# ip firewall screen dos-defense udp-threshold { <NUM> }` | <NUM> – максимальное количество UDP пакетов в секунду задается в диапазоне [1..10000]. |
| 7 | Включить защиту от winnuke-атак. | `esr(config)# ip firewall screen dos-defense winnuke` | |
| 8 | Включить блокировку TCP-пакетов с установленным флагом FIN и не установленным флагом ACK. | `esr(config)# ip firewall screen spy-blocking fin-no-ack` | |
| 9 | Включить блокировку ICMP-пакетов различных типов. | `esr(config)# ip firewall screen spy-blocking icmp-type` | <TYPE> – тип ICMP, может принимать значения:<br><br>• destination-unreachable<br>• echo-request<br>• reserved<br>• source-quench<br>• time-exceeded |
| 10 | Включить защиту от IP-sweep атак. | `esr(config)# ip firewall screen spy-blocking ip-sweep { <NUM> }` | <NUM> – интервал выявления ip sweep атаки, задается в миллисекундах [1..1000000]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 11 | Включить защиту от port scan атак. | `esr(config)# ip firewall screen spy-blocking port-scan { <threshold> } [ <TIME> ]` | <threshold> – интервал в миллисекундах, в течении которого будет фиксироваться port scan атака [1..1000000].<br><br><TIME> – время блокировки в миллисекундах [1..1000000]. |
| 12 | Включить защиту от IP spoofing атак. | `esr(config)# ip firewall screen spy-blocking spoofing` | |
| 13 | Включить блокировку TCP-пакетов, с установленными флагами SYN и FIN. | `esr(config)# ip firewall screen spy-blocking syn-fin` | |
| 14 | Включить блокировку TCP-пакетов, со всеми флагами или с набором флагов: FIN, PSH, URG. Данной командой обеспечивается защита от атаки XMAS. | `esr(config)# ip firewall screen spy-blocking tcp-all-flag` | |
| 15 | Включить блокировку TCP-пакетов, с нулевым полем flags. | `esr(config)# ip firewall screen spy-blocking tcp-no-flag` | |
| 16 | Включить блокировку фрагментированных ICMP-пакетов. | `esr(config)# ip firewall screen suspicious-packets icmp-fragment` | |
| 17 | Включить блокировку фрагментированных IP пакетов. | `esr(config)# ip firewall screen suspicious-packets ip-fragment` | |
| 18 | Включить блокировку ICMP-пакетов длиной более 1024 байт. | `esr(config)# ip firewall screen suspicious-packets icmp-fragment` | |
| 19 | Включить блокировку фрагментированных TCP-пакетов, с флагом SYN. | `esr(config)# ip firewall screen suspicious-packets syn-fragment` | |
| 20 | Включить блокировку фрагментированных UDP-пакетов. | `esr(config)# ip firewall screen suspicious-packets udp-fragment` | |
| 21 | Включить блокировку пакетов, с ID протокола в заголовке IP равном 137 и более. | `esr(config)# ip firewall screen suspicious-packets unknown-protocols` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 22 | Установить частоту оповещения (по SNMP, syslog и в CLI) об обнаруженных и отраженных сетевых атаках. | `esr(config)# ip firewall logging interval <NUM>` | <NUM> – интервал времени в секундах [30 .. 2147483647] |
| 23 | Включить более детальный вывод сообщений по обнаруженным и отраженным сетевым атакам в CLI. | `esr(config)# logging firewall screen detailed` | |
| 24 | Включить механизм обнаружения и логирования DoS атак через CLI, syslog и по SNMP. | `esr(config)# logging firewall screen dos-defense <ATACK_TYPE>` | <ATACK_TYPE> – тип DoS атаки, принимает значения: icmp-threshold, land, limit-session-destination, limit-session-source, syn-flood, udp-threshold, winnuke. |
| 25 | Включить механизм обнаружения и логирования шпионской активности через CLI, syslog и по SNMP | `esr(config)# logging firewall screen spy-blocking { <ATACK_TYPE> \| icmp-type <ICMP_TYPE> }` | <ATACK_TYPE> – тип шпионской активности, принимает значения: fin-no-ack, ip-sweep, port-scan, spoofing, syn-fin, tcp-all-flag, tcp-no-flag.<br><br><ICMP_TYPE> – тип ICMP, принимает значения: destination-unreachable, echo-request, reserved, source-quench, time-exceeded. |
| 26 | Включить механизм обнаружения нестандартных пакетов и логирования через CLI, syslog и по SNMP | `esr(config)# logging firewall screen suspicious-packets <PACKET_TYPE>` | < PACKET_TYPE> – тип нестандартных пакетов, принимает значения: icmp-fragment, ip-fragment, large-icmp, syn-fragment, udp-fragment, unknown-protocols. |

### 7.3.2 Описание механизмов защиты от атак

| Команда | Описание |
|---|---|
| ip firewall screen dos-defense icmp-threshold | Данная команда включает защиту от ICMP flood атак. При включенной защите ограничивается количество ICMP-пакетов всех типов в секунду для одного адреса назначения. Атака приводит к перегрузке хоста и выводу его из строя из-за необходимости обрабатывать каждый запрос и отвечать на него. |
| firewall screen dos-defense land | Данная команда включает защиту от land атак. При включенной защите блокируются пакеты с одинаковыми source и destination IP-адресами, и флагом SYN в заголовке TCP. Атака приводит к перегрузке хоста и выводу его из строя из-за необходимости обрабатывать каждый TCP SYN пакет и попыток хоста установить TCP сессию с самим собой. |

| Команда | Описание |
|---|---|
| ip firewall screen dos-defense limit-session-destination | Когда таблица IP-сессий хоста переполняется, он больше не в состоянии организовывать новые сессии и отбрасывает запросы (такое может происходить при различных атаках: SYN flood, UDP flood, ICMP flood, и т.д.). Команда включает ограничение количества одновременных сессий на основании адреса назначения, которое смягчает DoS-атаки. |
| ip firewall screen dos-defense limit-session-source | Когда таблица IP-сессий хоста переполняется, он больше не в состоянии организовывать новые сессии и отбрасывает запросы (такое может происходить при различных DoS-атаках: SYN flood, UDP flood, ICMP flood, и т.д.). Команда включает ограничение количества одновременных сессий на основании адреса источника, которое смягчает DoS-атаки. |
| ip firewall screen dos-defense syn-flood | Данная команда включает защиту от SYN flood атак. При включенной защите ограничивается количество TCP-пакетов с установленным флагом SYN в секунду для одного адреса назначения. Атака приводит к перегрузке хоста и выводу его из строя из-за необходимости обрабатывать каждый TCP SYN пакет и попыток установить TCP-сессии. |
| ip firewall screen dos-defense udp-threshold | Данная команда включает защиту от UDP flood атак. При включенной защите ограничивается количество UDP пакетов в секунду для одного адреса назначения. Атака приводит к перегрузке хоста и выводу его из строя из-за массивного UDP-трафика. |
| ip firewall screen dos-defense winnuke | Данная команда включает защиту от winnuke атак. При включенной защите блокируются<br>TCP-пакеты с установленным флагом URG и 139 портом назначения. Атака приводит к выходу из строя старых версий Windows (до 95 версии). |
| ip firewall screen spy-blocking fin-no-ack | Данная команда включает блокировку TCP-пакетов с установленным флагом FIN и не установленным флагом ACK. Такие пакеты являются нестандартными и по ответу можно определить операционную систему жертвы. |
| ip firewall screen spy-blocking icmp-type destination-unreachable | Данная команда включает блокировку всех ICMP-пакетов 3 типа (destination-unreachable), включая пакеты, сгенерированные самим маршрутизатором. Защита не дает злоумышленнику узнать о топологии сети и доступности хостов |
| ip firewall screen spy-blocking icmp-type echo-request | Данная команда включает блокировку всех ICMP-пакетов 8 типа (echo-request), включая пакеты, сгенерированные самим маршрутизатором. Защита не дает злоумышленнику узнать о топологии сети и доступности хостов |
| ip firewall screen spy-blocking icmp-type reserved | Данная команда включает блокировку всех ICMP-пакетов 2 и 7 типов (reserved), включая пакеты, сгенерированные самим маршрутизатором. Защита не дает злоумышленнику узнать о топологии сети и доступности хостов |
| ip firewall screen spy-blocking icmp-type source-quench | Данная команда включает блокировку всех ICMP-пакетов 4 типа (source quench), включая пакеты, сгенерированные самим маршрутизатором. Защита не дает злоумышленнику узнать о топологии сети и доступности хостов |
| ip firewall screen spy-blocking icmp-type time-exceeded | Данная команда включает блокировку всех ICMP-пакетов 11 типа (time exceeded), включая пакеты, сгенерированные самим маршрутизатором. Защита не дает злоумышленнику узнать о топологии сети и доступности хостов |

| Команда | Описание |
|---|---|
| ip firewall screen spy-blocking ip-sweep | Данная команда включает защиту от IP-sweep атак. При включенной защите, если в течение заданного в параметрах интервала приходит более 10 ICMP-запросов от одного источника, первые 10 запросов пропускаются маршрутизатором, а 11 и последующие отбрасываются на оставшееся время интервала. Защита не дает злоумышленнику узнать о топологии сети и доступности хостов. |
| ip firewall screen spy-blocking port-scan | Данная команда включает защиту от port scan атак. Если в течение первого заданного интервала времени (<threshold>) на один источник приходит более 10 TCP-пакетов с флагом SYN на разные TCP-порты, то такое поведение фиксируется как port scan атака и все последующие пакеты такого рода от источника блокируются на второй заданный интервал времени (<TIME>). Злоумышленник не сможет быстро просканировать открытые порты на устройстве. |
| ip firewall screen spy-blocking spoofing | Данная команда включает защиту от ip spoofing атак. При включенной защите маршрутизатор проверяет пакеты на соответствие адреса источника и записей в таблице маршрутизации и в случае несоответствия пакет отбрасывается. Например, если пакет с адресом источника 10.0.0.1/24 приходит на интерфейс Gi1/0/1, а в таблице маршрутизации данная подсеть располагается за интерфейсом Gi1/0/2, то считается, что адрес источника был подменен. Защищает от вторжений в сеть с подмененными source IP-адресами. |
| ip firewall screen spy-blocking syn-fin | Данная команда включает блокировку TCP-пакетов с установленными флагами SYN и FIN. Такие пакеты являются нестандартными и по ответу можно определить операционную систему жертвы. |
| ip firewall screen spy-blocking tcp-all-flag | Данная команда включает блокировку TCP-пакетов со всеми флагами или с набором флагов: FIN, PSH, URG. Обеспечивается защита от атаки XMAS. |
| ip firewall screen spy-blocking tcp-no-flag | Данная команда включает блокировку TCP-пакетов с нулевым полем flags. Такие пакеты являются нестандартными и по ответу можно определить операционную систему жертвы. |
| ip firewall screen suspicious-packets icmp-fragment | Данная команда включает блокировку фрагментированных ICMP-пакетов. ICMP-пакеты обычно небольшого размера и необходимости в их фрагментировании нет. |
| ip firewall screen suspicious-packets ip-fragment | Данная команда включает блокировку фрагментированных пакетов. |
| ip firewall screen suspicious-packets large-icmp | Данная команда включает блокировку ICMP-пакетов длиной более 1024 байт. |
| ip firewall screen suspicious-packets syn-fragment | Данная команда включает блокировку фрагментированных TCP-пакетов с флагом SYN. TCP пакеты с SYN флагом обычно небольшого размера и необходимости в их фрагментировании нет. Защита предотвращает накопление фрагментированных пакетов в буфере. |

| Команда | Описание |
|---|---|
| ip firewall screen suspicious-packets udp-fragment | Данная команда включает блокировку фрагментированных UDP-пакетов. |
| ip firewall screen suspicious-packets unknown-protocols | Данная команда включает блокировку пакетов, с ID протокола в заголовке IP равном 137 и более. |

### 7.3.3 Пример настройки логирования и защиты от сетевых атак

**Задача:**

Необходимо защитить LAN сеть и маршрутизатор ESR от сетевых атак land, syn-flood, ICMP flood и настроить оповещение об атаках по SNMP на SNMP-сервер 192.168.0.10.


**Решение:**

Предварительно необходимо настроить интерфейсы и firewall (настройка firewall или ее отсутствие не повлияют на работу защиты от сетевых атак):

```
esr(config)# security zone LAN
esr(config-zone)# exit
esr(config)# security zone WAN
esr(config-zone)# exit
esr(config)# security zone-pair LAN WAN
esr(config-zone-pair)# rule 100
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# ex
esr(config-zone-pair)# exit
esr(config)# security zone-pair WAN LAN
esr(config-zone-pair)# rule 100
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# security-zone LAN
esr(config-if-gi)# ip address 192.168.0.1/24
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# security-zone WAN
esr(config-if-gi)# ip address 10.0.0.1/24
esr(config-if-gi)# exit
```

Настроим защиту от land, syn-flood, ICMP flood атак:

```
esr(config)# ip firewall screen dos-defense land
esr(config)# ip firewall screen dos-defense syn-flood 100 src-dst
esr(config)# ip firewall screen dos-defense icmp-threshold 100
```

Настроим логирование обнаруженных атак:

```
esr(config)# ip firewall logging screen dos-defense land
esr(config)# ip firewall logging screen dos-defense syn-flood
esr(config)# ip firewall logging screen dos-defense icmp-threshold
```

Настроим SNMP-сервер, на который будут отправляться трапы:

```
esr(config)# snmp-server
esr(config)# snmp-server host 192.168.0.10
```

Посмотреть статистику по зафиксированным сетевым атакам можно командой:

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

## 7.4 Конфигурирование Firewall

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

### 7.4.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Создать зоны безопасности. | `esr(config)# security zone <zone-name1>`<br>`esr(config)# security zone <zone-name2>` | <zone-name> – до 12 символов. |
| 2 | Задать описание зоны безопасности. | `esr(config-zone)# description <description>` | <description> – до 255 символов. |
| 3 | Указать экземпляр VRF, в котором будет работать данная зона безопасности (не обязательно). | `esr(config- zone )# ip vrf forwarding <VRF>` | <VRF> – имя VRF, задается строкой до 31 символа. |
| 4 | Включить счетчики сессий для NAT и Firewall (не обязательно, снижает производительность). | `esr(config)# ip firewall sessions counters` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 5 | Отключить фильтрацию пакетов, для которых не удалось определить принадлежность к какому-либо известному соединению и которые не являются началом нового соединения (не обязательно, снижает производительность). | `esr(config)# ip firewall sessions allow-unknown` | |
| 6 | Выбрать режима работы межсетевого экрана (не обязательно) | `esr(config)# ip firewall mode <MODE>` | <MODE> – режим работы межсетевого экрана, может принимать значения: stateful, stateless.<br><br>Значение по умолчанию: stateful |
| 7 | Определить время жизни сессии для неподдерживаемых протоколов (не обязательно). | `esr(config)# ip firewall sessions generic-timeout <TIME>` | <TIME> – время жизни сессии для неподдерживаемых протоколов, принимает значения в секундах [1..8553600].<br><br>По умолчанию: 60 секунд. |
| 8 | Определить время жизни ICMP-сессии, по истечении которого она считается устаревшей (не обязательно). | `esr(config)# ip firewall sessions icmp-timeout <TIME>` | <TIME> – время жизни ICMP-сессии, принимает значения в секундах [1..8553600].<br><br>По умолчанию: 30 секунд. |
| 9 | Определить время жизни ICMPv6-сессии, по истечении которого она считается устаревшей (не обязательно). | `esr(config)# ip firewall sessions icmpv6-timeout <TIME>` | <TIME> – время жизни ICMP-сессии, принимает значения в секундах [1..8553600].<br><br>По умолчанию: 30 секунд. |
| 10 | Определить размер таблицы сессий ожидающих обработки (не обязательно). | `esr(config)# ip firewall sessions max-expect <COUNT>` | <COUNT> – размер таблицы, принимает значения [1..8553600].<br><br>По умолчанию: 256. |
| 11 | Определить размер таблицы отслеживаемых сессий (не обязательно). | `esr(config)# ip firewall sessions max-tracking <COUNT>` | <COUNT> – размер таблицы, принимает значения [1..8553600].<br>По умолчанию: 512000. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 12 | Определить время жизни TCP-сессии в состоянии «соединение устанавливается», по истечении которого она считается устаревшей (не обязательно). | `esr(config)# ip firewall sessions tcp-connect-timeout <TIME>` | <TIME> – время жизни TCP-сессии в состоянии "соединение устанавливается", принимает значения в секундах [1..8553600].<br><br>По умолчанию: 60 секунд. |
| 13 | Определить время жизни TCP-сессии в состоянии "соединение закрывается", по истечении которого она считается устаревшей (не обязательно). | `esr(config)# ip firewall sessions tcp-disconnect-timeout <TIME>` | <TIME> – время жизни TCP-сессии в состоянии "соединение закрывается", принимает значения в секундах [1..8553600].<br>По умолчанию: 30 секунд. |
| 14 | Определить время жизни TCP-сессии в состоянии "соединение установлено", по истечении которого она считается устаревшей (не обязательно). | `esr(config)# ip firewall sessions tcp-established-timeout <TIME>` | <TIME> – время жизни TCP-сессии в состоянии "соединение установлено", принимает значения в секундах [1..8553600].<br><br>По умолчанию: 120 секунд. |
| 15 | Определить время ожидания, по истечении которого происходит фактическое удаление закрытой TCP-сессии из таблицы отслеживаемых сессий (не обязательно). | `esr(config)# ip firewall sessions tcp-latecome-timeout <TIME>` | <TIME> – время ожидания, принимает значения в секундах [1..8553600].<br><br>По умолчанию: 120 секунд. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 16 | Включить функцию отслеживания сессий уровня приложений для отдельных протоколов (не обязательно). | `esr(config)# ip firewall sessions tracking` | <PROTOCOL> – протокол уровня приложений [ftp, h323, pptp, netbios-ns, tftp], сессии которого должны отслеживаться.<br><br><OBJECT-GROUP-SERVICE> – имя профиля TCP/UDP-портов sip сессии, задаётся строкой до 31 символа. Если группа не указана, то отслеживание сессий sip будет осуществляться для порта 5060.<br><br>Вместо имени отдельного протокола можно использовать ключ "all", который включает функцию отслеживания сессий уровня приложений для всех доступных протоколов.<br><br>По умолчанию – отключено для всех протоколов. |
| 17 | Определить время жизни UDP-сессии в состоянии "соединение подтверждено", по истечении которого она считается устаревшей (не обязательно). | `esr(config)# ip firewall sessions udp-assured-timeout <TIME>` | <TIME> – время жизни UDP-сессии в состоянии "соединение подтверждено", принимает значения в секундах [1..8553600].<br><br>По умолчанию: 180 секунд. |
| 18 | Определить время жизни UDP-сессии в состоянии «соединение не подтверждено», по истечении которого она считается устаревшей. | `esr(config)# ip firewall sessions udp-wait-timeout <TIME>` | <TIME> – время жизни UDP-сессии в состоянии «соединение не подтверждено», принимает значения в секундах [1..8553600].<br><br>По умолчанию: 30 секунд. |
| 19 | Создать списки IP-адресов, которые будут использоваться при фильтрации. | `esr(config)# object-group network <obj-group-name>` | <obj-group-name> – до 31 символа. |
| 20 | Задать описание списка IP- адресов (не обязательно). | `esr(config-object-group-network)# description <description>` | <description> – описание профиля, задается строкой до 255 символов. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 21 | Внести необходимые IPv4/IPv6-адреса в список. | `esr(config-object-group-network)# ip prefix <ADDR/LEN>` | <ADDR/LEN> – подсеть, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. |
| | | `esr(config-object-group-network)# ip address-range <FROM-ADDR>-<TO-ADDR>` | <FROM-ADDR> – начальный IP-адрес диапазона адресов;<br><br><TO-ADDR> – конечный IP-адрес диапазона адресов, опциональный параметр. Если параметр не указан, то командой задаётся одиночный IP-адрес.<br><br>Адреса задаются в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| | | `esr(config-object-group-network)# ipv6 prefix <IPV6-ADDR/LEN>` | <IPV6-ADDR/LEN> – IP-адрес и маска подсети, задаётся в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128]. |
| | | `esr(config-object-group-network)# ipv6 address-range <FROM-ADDR>-<TO-ADDR>` | <FROM-ADDR> – начальный IPv6-адрес диапазона адресов;<br><br><TO-ADDR> – конечный IPv6-адрес диапазона адресов, опциональный параметр. Если параметр не указан, то командой задаётся одиночный IPv6-адрес.<br><br>Адреса задаются в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. |
| 22 | Создать списки сервисов, которые будут использоваться при фильтрации. | `esr(config)# object-group service <obj-group-name>` | <obj-group-name> – имя профиля сервисов, задается строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 23 | Задать описание списка сервисов (не обязательно). | `esr(config-object-group-service)# description <description>` | <description> – описание профиля, задается строкой до 255 символов. |
| 24 | Внести необходимые сервисы (tcp/udp порты) в список. | `esr(config-object-group-service)# port-range <port>` | <port> – принимает значение [1..65535].<br><br>Можно указать несколько портов перечислением через запятую «,» либо указать диапазон портов через «-». |
| 25 | Создать списки приложений, которые будут использоваться в механизме DPI. | `esr(config)# object-group application <NAME>` | <NAME> – имя профиля приложений, задается строкой до 31 символа. |
| 26 | Задать описание списка приложений (не обязательно). | `esr(config-object-group-application)# description <description>` | <description> – описание профиля, задается строкой до 255 символов. |
| 27 | Внести необходимые приложения в списки. | `esr(config-object-group-application)# application < APPLICATION >` | < APPLICATION > – указывает приложение подпадающее под действие данного профиля |
| 28 | Включить интерфейсы (физические, логические, E1/Multilink и подключаемые), сервер удаленного доступа (l2tp, openvpn, pptp) или туннели (gre, ip4ip4, l2tp, lt, pppoe, pptp) в зоны безопасности (если необходимо). | `esr(config-if-gi)# security-zone <zone-name>` | <zone-name> – до 12 символов. |
| | Отключить функции Firewall на сетевом интерфейсе (физические, логические, E1/Multilink и подключаемые), сервере удаленного доступа (l2tp, openvpn, pptp) или туннели (gre, ip4ip4, l2tp, lt, pppoe, pptp) (если необходимо) | `esr(config-if-gi)# ip firewall disable` | |
| 29 | Создать набор правил межзонового взаимодействия. | `esr(config)# security zone-pair <src-zone-name1> <dst-zone-name2>` | <src-zone-name> – до 12 символов.<br><br><dst-zone-name> – до 12 символов. |
| 30 | Создать правило межзонового взаимодействия. | `esr(config-zone-pair)# rule <rule-number>` | <rule-number> – 1..10000. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 31 | Задать описание правила (не обязательно). | `esr(config-zone-rule)# description <description>` | <description> – до 255 символов. |
| 32 | Указать действие данного правила. | `esr(config-zone-rule)# action <action> [ log ]` | <action> – permit/deny/reject/ netflow-sample/sflow-sample<br><br>log – ключ для активации логирования сессий, устанавливающимися согласно данному правилу. |
| 33 | Установить имя или номер IP-протокола, для которого должно срабатывать правило (не обязательно). | `esr(config-zone-rule)# match [not] protocol <protocol-type>` | <protocol-type> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre.<br><br>При указании значения «any» правило будет срабатывать для любых протоколов. |
| | | `esr(config-zone-rule)# match [not] protocol-id <protocol-id>` | <protocol-id> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF]. |
| 34 | Установить профиль IP-адресов отправителя, для которых должно срабатывать правило (не обязательно). | `esr(config-zone-rule)# match [not] source-address <OBJ-GROUP-NETWORK-NAME>` | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа. При указании значения «any» правило будет срабатывать для любого IP-адреса отправителя/ получателя. |
| 35 | Установить профиль IP-адресов получателя, для которых должно срабатывать правило (не обязательно). | `esr(config-zone-rule)# match [not] destination-address <OBJ-GROUP-NETWORK-NAME>` | |
| 36 | Установить MAC-адрес отправителя, для которого должно срабатывать правило (не обязательно). | `esr(config-zone-rule)# match [not] source-mac <mac-addr>` | <mac-addr> – задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]. |
| 37 | Установить MAC-адрес получателя, для которого должно срабатывать правило (не обязательно). | `esr(config-zone-rule)# match [not] destination-mac <mac-addr>` | |
| 38 | Установить профиль TCP/UDP-портов отправителя, для которых должно срабатывать правило (если указан протокол). | `esr(config-zone-rule)# match [not] source-port <PORT-SET-NAME>` | <PORT-SET-NAME> – задаётся строкой до 31 символа. При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта отправителя/получателя. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 39 | Установить профиль TCP/UDP-портов получателя, для которых должно срабатывать правило (если указан протокол). | `esr(config-zone-rule)# match [not] destination-port <PORT-SET-NAME>` | |
| 40 | Установить тип и код сообщений протокола ICMP, для которых должно срабатывать правило (если в качестве протокола выбран ICMP) (не обязательно). | `esr(config-zone-rule)# match [not]  icmp <ICMP_TYPE> <ICMP_CODE>` | <ICMP_TYPE> – тип сообщения протокола ICMP, принимает значения [0..255];<br><br><ICMP_CODE> – код сообщения протокола ICMP, принимает значения [0..255]. При указании значения «any» правило будет срабатывать для любого кода сообщения протокола ICMP. |
| 41 | Установить ограничение, при котором правило будет срабатывать только для трафика, измененного сервисом трансляции IP-адресов и портов получателя. | `esr(config-zone-rule)# match [not] destination-nat` | |
| 42 | Установить максимальную скорость прохождения пакетов (не обязательно, доступно только для zone-pair any self и zone-pair <zone-name> any). | `esr(config-zone-pair-rule)# rate-limit pps <rate-pps>` | <rate-pps> – максимальное количество пакетов, которое может быть передано. Принимает значения [1..10000]. |
| 43 | Установить фильтрацию только для фрагментированных IP-пакетов (не обязательно, доступно только для zone-pair any self и zone-pair <zone-name> any). | `esr(config-zone-pair-rule)# match [not] fragment` | |
| 44 | Установить фильтрацию для IP-пакетов, содержащих ip-option (не обязательно, доступно только для zone-pair any self и zone-pair <zone-name> any). | `esr(config-zone-pair-rule)# match [not] ip-option` | |
| 45 | Включить правило межзонового взаимодействия. | `esr(config-zone-rule)# enable` | |
| 46 | Активировать фильтрацию и режим отслеживания сессий при прохождении пакетов между участниками одной Bridge-группы (не обязательно, доступно только на ESR-1000/1200/1500/1700) | `esr(config-bridge)# ports firewall enable` | |

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

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

Более подробная информация о командах для настройки межсетевого экрана содержится в «Справочнике команд CLI».

### 7.4.2 Пример настройки Firewall

**Задача:**

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


**Решение:**

Для каждой сети ESR создадим свою зону безопасности:

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

Настроим сетевые интерфейсы и определим их принадлежность к зонам безопасности:

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

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

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

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

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

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

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

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

```
esr(config)# security zone-pair WAN self
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match destination-address WAN
esr(config-zone-pair-rule)# match source-address WAN_GATEWAY
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
```

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

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

Посмотреть членство портов в зонах можно с помощью команды:

```
esr# show security zone
```

Посмотреть пары зон и их конфигурацию можно с помощью команд:

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

Посмотреть активные сессии можно с помощью команд:

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

### 7.4.3 Пример настройки фильтрации приложений (DPI)

⚠ Использование механизма фильтрации приложений многократно снижает производительность маршрутизатора из-за необходимости проверки каждого пакета. Производительность снижается с ростом количества выбранных приложений для фильтрации.

**Задача:**

Блокировать доступ к ресурсам youtube, bittorrent и facebook.


**Решение:**

Для каждой сети ESR создадим свою зону безопасности:

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

Настроим сетевые интерфейсы и определим их принадлежность к зонам безопасности:

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

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

```
esr(config)# object-group application APP
esr(config-object-group-application)# application youtube
esr(config-object-group-application)# application bittorrent
esr(config-object-group-application)# application facebook
esr(config-object-group-application)# exit
```

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

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

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

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

Посмотреть членство портов в зонах можно с помощью команды:

```
esr# show security zone
```

Посмотреть пары зон и их конфигурацию можно с помощью команд:

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

Посмотреть активные сессии можно с помощью команд:

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

## 7.5 Настройка списков доступа (ACL)

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

### 7.5.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Создать список контроля доступа и перейти в режим его конфигурирования. | `esr(config)# ip access-list extended <NAME>` | <NAME> – имя создаваемого списка контроля доступа, задаётся строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 2 | Указать описание конфигурируемого списка контроля доступа (не обязательно). | `esr(config-acl)# description <DESCRIPTION>` | <DESCRIPTION> – описание списка контроля доступа, задаётся строкой до 255 символов. |
| 3 | Создать правило и перейти в режим его конфигурирования.<br><br>Правила обрабатываются маршрутизатором в порядке возрастания их номеров. | `esr(config-acl)# rule <ORDER>` | <ORDER> – номер правила, принимает значения [1..4094]. |
| 4 | Указать действие, которое должно быть применено для трафика, удовлетворяющего заданным критериям. | `esr(config-acl-rule)# action <ACT>` | <ACT> – назначаемое действие:<br>• permit – прохождение трафика разрешается;<br>• deny – прохождение трафика запрещается. |
| 5 | Установить имя/номер протокола, для которого должно срабатывать правило (не обязательно). | `esr(config-acl-rule)# match protocol <TYPE>` | <TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre. При указании значения «any» правило будет срабатывать для любых протоколов; |
| | | `esr(config-acl-rule)# match protocol-id <ID>` | <ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF]. |
| 6 | Установить IP-адреса отправителя, для которых должно срабатывать правило (не обязательно). | `esr(config-acl-rule)# match source-address { <ADDR> <MASK> \| any }` | <ADDR> – IP-адрес отправителя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];<br><br><MASK> – маска IP-адреса, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Биты маски, установленные в 0, задают биты IP-адреса, исключаемые из сравнения при поиске.<br><br>При указании значения «any» правило будет срабатывать для любого IP-адреса отправителя/получателя. |
| 7 | Установить IP-адреса получателя, для которых должно срабатывать правило (не обязательно). | `esr(config-acl-rule)# match destination-address { <ADDR> <MASK> \| any }` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 8 | Установить MAC-адреса отправителя, для которых должно срабатывать правило (не обязательно). | `esr(config-acl-rule)# match source-mac <ADDR><WILDCARD>` | <ADDR> – MAC-адрес отправителя, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF];<br><br><WILDCARD> – маска MAC-адреса, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]. Биты маски, установленные в 0, задают биты MAC-адреса, исключаемые из сравнения при поиске. |
| 9 | Установить MAC-адреса получателя, для которых должно срабатывать правило (не обязательно). | `esr(config-acl-rule)# match destination-mac <ADDR><WILDCARD>` | |
| 10 | Установить номер TCP/UDP-порта отправителя, для которого должно срабатывать правило (если указан протокол). | `esr(config-acl-rule)# match source-port { <PORT> \| any }` | <PORT> – номер TCP/UDP-порта отправителя, принимает значения [1..65535]. При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта отправителя. |
| 11 | Установить номер TCP/UDP-порта получателя, для которого должно срабатывать правило (если указан протокол). | `esr(config-acl-rule)# match destination-port { <PORT> \| any }` | |
| 12 | Установить значение 802.1p приоритета, для которого должно срабатывать правило (не обязательно). | `esr(config-acl-rule)# match c os <COS>` | <COS> – значение 802.1p приоритета, принимает значения [0..7]. |
| 13 | Установить значение кода DSCP, для которого должно срабатывать правило (не обязательно). Невозможно использовать совместно с IP Precedence. | `esr(config-acl-rule)# match dscp <DSCP>` | <DSCP> – значение кода DSCP, принимает значения [0..63]. |
| 14 | Установить значение кода IP Precedence, для которого должно срабатывать правило (не обязательно). Невозможно использовать совместно с DSCP. | `esr(config-acl-rule)# match ip-precedence <IPP>` | <IPP> – значение кода IP Precedence, принимает значения [0..7]. |
| 15 | Установить значение идентификационного номера VLAN, для которого должно срабатывать правило (не обязательно). | `esr(config-acl-rule)# match vlan <VID>` | <VID> – идентификационный номер VLAN, принимает значения [1..4094]. |
| 16 | Активировать правило. | `esr(config-acl-rule)# enable` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 17 | Указать список контроля доступа к конфигурируемому интерфейсу для фильтрации входящего трафика. | `esr(config-if-gi)# service-acl input <NAME>` | <NAME> – имя списка контроля доступа, задаётся строкой до 31 символа. |

Также списки доступа могут использоваться для организации политик QoS.

### 7.5.2 Пример настройки списка доступа

**Задача:**

Разрешить прохождения трафика только из подсети 192.168.20.0/24.

**Решение:**

Настроим список доступа для фильтрации по подсетям:

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

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

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

Просмотреть детальную информацию о списке доступа возможно через команду:

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

## 7.6 Настройка IPS/IDS

IPS/IDS (*Intrusion Prevention System / Intrusion Detection System*) – система предотвращения вторжений – программная система сетевой и компьютерной безопасности, обнаруживающая вторжения или нарушения безопасности и автоматически защищающая от них.

Работа системы основана на сигнатурном анализе трафика. Сигнатуры для систем IPS/IDS принято называть правилами. Устройства ESR позволяют скачивать актуальные правила с открытых источников в сети Интернет или с корпоративного сервера. Так-же с помощью CLI можно создавать свои, специфические правила.

По умолчанию на устройствах ESR установлен базовый набор правил от компании EmergingThreats предназначенный для тестирования и проверки работоспособности системы.

### 7.6.1 Алгоритм базовой настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Создать политику безопасности IPS/IDS. | `esr(config)# security ips policy <NAME>` | <NAME> – имя политики безопасности, задаётся строкой до 32 символов |
| 2 | Задать описание политики (не обязательно). | `esr(config-ips-policy)# description <DESCRIPTION>` | <DESCRIPTION> – описание задаётся строкой до 255 символов. |
| 3 | Задать профиль IP-адресов, которые будет защищать IPS/IDS. | `esr(config-ips-policy)# protect network-group <OBJ-GROUP-NETWORK_NAME>` | <OBJ-GROUP-NETWORK-NAME> – имя профиля защищаемых IP-адресов, задается строкой до 32 символов. |
| 4 | Задать профиль IP- адресов, внешних для IPS/IDS<br><br>(не обязательно). | `esr(config-ips-policy)# external network-group <OBJ-GROUP-NETWORK_NAME>` | <OBJ-GROUP-NETWORK-NAME> – имя профиля внешних IP-адресов, задается строкой до 32 символов. |
| 5 | Перейти в режим конфигурирования IPS/IDS. | `esr(config)# security ips` | |
| 6 | Назначить политику безопасности IPS/IDS. | `esr(config-ips)# policy <NAME>` | <NAME> – имя политики безопасности, задаётся строкой до 32 символов |
| 7 | Использовать все ресурсы ESR для IPS/IDS.<br><br>(не обязательно). | `esr(config-ips)# perfomance max` | По умолчанию для IPS/IDS отдается половина доступных ядер процессора. |
| 8 | Задать USB диск, для записи логов в формате EVE.<br><br>(не обязательно). | `esr(config-ips)# logging storage-device <DEVICE_NAME>` | <DEVICE_NAME> имя usb накопителя. |
| 9 | Активировать IPS/IDS. | `esr(config- ips )# enable` | |
| 10 | Активировать IPS/IDS на интерфейсе. | `esr(config-if-gi)# service-ips enable` | |

### 7.6.2 Алгоритм настройки автообновления правил IPS/IDS из внешних источников

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Перейти в режим конфигурирования автообновлений. | `esr(config-ips)# auto-upgrade` | |
| 2 | Задать имя и перейти в режим конфигурирования пользовательского сервера обновлений. | `esr(config-ips-auto-upgrade)# user-server <WORD>` | <WORD> – имя сервера, задаётся строкой до 32 символов. |
| 3 | Задать описание пользовательского сервера обновлений.<br><br>(не обязательно). | `esr(config-ips-upgrade-user-server)# description <DESCRIPTION>` | <DESCRIPTION> – описание задаётся строкой до 255 символов. |
| 4 | Задать URL. | `esr(config-ips-upgrade-user-server)# url <URL>` | <URL> – текстовое поле, содержащее URL-ссылку длинной от 8 до 255 символов.<br><br>В качестве URL-ссылки может быть указан:<br><br>• файл правил с расширение .rule;<br>• файл классификатора правил с именем classification.config;<br>• каталог на сервере содержащий файлы правил и/или файл классификатора правил. |
| 5 | Задать частоту проверки обновлений.<br><br>(не обязательно). | `esr(config-ips-upgrade-user-server)# upgrade interval <HOURS>` | <HOURS> – интервал обновлений в часах, от 1 до 240.<br><br>Значение по умолчанию: 24 часа |

### 7.6.3 Рекомендуемые открытые источники обновления правил

| | |
|---|---|
| https://sslbl.abuse.ch/ | SSL Blacklist содержит списки «плохих» SSL сертификатов, т.е. сертификатов, в отношении которых устнановлен факт их использования вредоносным ПО и ботнетами. В списках содержатся SHA1 отпечатки публичных ключей из SSL сертификатов. |

| | |
|---|---|
| https://feodotracker.abuse.ch/ | Feodo Tracker – список управляющих серверов для троянской программы Feodo. Feodo (также известный как Cridex или Bugat) используется злоумышленниками для кражи чувствительной информации в сфере электронного банкинга (данные по кредитным картам, логины/пароли) с компьютеров пользователей. В настоящее время существует четыре версии троянской программы (версии A, B, C и D), главным образом отличающиеся инфраструктурой управляющих серверов. |
| https://rules.emergingthreats.net/open/suricata/rules/botcc.rules | Данные правила описывают известные ботнеты и управляющие сервера. Источники: Shadowserver.org, Zeus Tracker, Palevo Tracker, Feodo Tracker, Ransomware Tracker. |
| https://rules.emergingthreats.net/open/suricata/rules/ciarmy.rules | Данные правила описывают вредоносные хосты по классификации проекта www.cinsarmy.com. |
| https://rules.emergingthreats.net/open/suricata/rules/compromised.rules | Данные правила описывают известные скомпрометированные и вредоносные хосты. Источники: Daniel Gerzo's BruteForceBlocker, The OpenBL, Emerging Threats Sandnet, SidReporter Projects. |
| https://rules.emergingthreats.net/open/suricata/rules/drop.rules | Данные правила описывают спамерские хосты / сети по классификации проекта www.spamhaus.org. |
| https://rules.emergingthreats.net/open/suricata/rules/dshield.rules | Данные правила описывают вредоносные хосты по классификации проекта www.dshield.org. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-activex.rules | Данные правила содержат сигнатуры использования ActiveX-контента. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-attack_response.rules | Правила, детектирующие поведение хоста после успешно проведенных атак. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-chat.rules | Данные правила описывают признаки обращения к популярным чатам. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-current_events.rules | Временные правила, ожидающие возможного включения в постоянные списки правил. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-dns.rules | Данные правила содержат сигнатуры уязвимостей в протоколе DNS, признаки использования DNS вредоносным ПО, некорректного использования протокола DNS. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-dos.rules | Данные правила содержат сигнатуры DOS-атак. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-exploit.rules | Данные правила содержат сигнатуры эксплойтов. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-ftp.rules | Данные правила содержат сигнатуры уязвимостей в протоколе FTP, признаки некорректного использования протокола FTP. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-games.rules | Данные правила описывают признаки обращения к популярным игровым сайтам: World of Warcraft, Starcraft и т.п. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-icmp.rules | Данные правила содержат сигнатуры некорректного использования протокола ICMP. |

| | |
|---|---|
| https://rules.emergingthreats.net/open/suricata/rules/emerging-icmp_info.rules | Данные правила содержат сигнатуры информационных ICMP-сообщений. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-imap.rules | Данные правила содержат сигнатуры уязвимостей в протоколе IMAP, признаки некорректного использования протокола IMAP. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-inappropriate.rules | Данные правила описывают признаки обращения к нежелательным ресурсам. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-info.rules | Данные правила содержат сигнатуры различных уязвимостей. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-malware.rules | Данные правила содержат сигнатуры вредоносного ПО, использующего в своей работе протокол HTTP. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-misc.rules | Данные правила содержат сигнатуры различных уязвимостей. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-mobile_malware.rules | Данные правила содержат сигнатуры вредоносного ПО для мобильных платформ. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-netbios.rules | Данные правила содержат сигнатуры уязвимостей в протоколе NetBIOS, признаки некорректного использования протокола NetBIOS. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-p2p.rules | Данные правила описывают признаки обращения к P2P-сетям (Bittorrent, Gnutella, Limewire). |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-policy.rules | Данные правила описывают нежелательную сетевую активность (обращение к MySpace, Ebay). |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-poprules | Данные правила содержат сигнатуры уязвимостей в протоколе POP3, признаки некорректного использования протокола POP3. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-rpc.rules | Данные правила содержат сигнатуры уязвимостей в протоколе RPC, признаки некорректного использования протокола RPC. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-scada.rules | Данные правила содержат сигнатуры уязвимостей для SCADA-систем. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-scan.rules | Данные правила описывают признаки активности, связанной с сетевым сканированием (Nessus, Nikto, portscanning). |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-shellcode.rules | Данные правила описывают признаки активности, связанной с попытками получить шелл-доступ в результате выполнения эксплойтов. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-smtp.rules | Данные правила содержат сигнатуры уязвимостей в протоколе SMTP, признаки некорректного использования протокола SMTP. |

| | |
|---|---|
| https://rules.emergingthreats.net/open/suricata/rules/emerging-sql.rules | Данные правила содержат сигнатуры уязвимостей для СУБД SQL. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-telnet.rules | Данные правила содержат сигнатуры уязвимостей для протокола telnet, признаки некорректного использования протокола telnet. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-tftp.rules | Данные правила содержат сигнатуры уязвимостей в протоколе TFTP, признаки некорректного использования протокола TFTP. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-trojan.rules | Данные правила содержат признаки сетевой активности троянских программ. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-user_agents.rules | Данные правила содержат признаки подозрительных и потенциально опасных HTTP-клиентов (идентифицируются по значениям в HTTP-заголовке User-Agent). |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-l.rules | Данные правила содержат сигнатуры уязвимостей в VOIP-протокола. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-web_client.rules | Данные правила содержат сигнатуры уязвимостей для веб-клиентов. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-web_server.rules | Данные правила содержат сигнатуры уязвимостей для веб-серверов. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-web_specific_apps.rules | Данные правила содержат сигнатуры эксплуатации уязвимостей веб-приложений. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-worm.rules | Данные правила описывают признаки активности сетевых червей. |

### 7.6.4 Пример настройки IPS/IDS с автообновлением правил

**Задача:**

Организовать защиту локальной сети с автообновлением правил из открытых источников.

192.168.1.0/24 – локальная сеть

**Решение:**

Создадим профиль адресов локальной сети, которую будем защищать:

```
esr(config)# object-group network LAN
esr(config-object-group-network)# ip prefix 192.168.1.0/24
esr(config-object-group-network)# exit
```

Настроим на ESR DNS-клиента для разрешения имен источников обновления правил IPS/IDS:

```
esr(config)# domain lookup enable
esr(config)# domain name-server 8.8.8.8
```

Создадим политику безопасности IPS/IDS:

```
esr(config)# security ips policy OFFICE
esr(config-ips-policy)# description "My Policy"
esr(config-ips-policy)# protect network-group LAN
```

Разрешим работу IPS/IDS на интерфейсе локальной сети bridge 1:

```
esr(config)# bridge 1
esr(config-bridge)# service-ips enable
```

Настроим параметры IPS/IDS:

```
esr(config)# security ips
esr(config-ips)# logging storage-device usb://DATA
esr(config-ips)# policy OFFICE
esr(config-ips)# enable
```

Устройство будет использоваться только как шлюз безопасности, по этому отдадим сервису IPS/IDS все доступные ресурсы:

```
esr(config-ips)# perfomance max
```

Настроим автообновление правил с сайтов EmergingThreats.net, etnetera.cz и Abuse.ch:

```
esr(config-ips)# auto-upgrade
esr(config-auto-upgrade)# user-server ET-Open
esr(config-ips-upgrade-user-server)# description «emerging threats open rules»
esr(config-ips-upgrade-user-server)# url https://rules.emergingthreats.net/open/suricata-4.0/
rules/
esr(config-ips-upgrade-user-server)# exit
esr(config-auto-upgrade)# user-server Aggressive
esr(config-ips-upgrade-user-server)# description «Etnetera aggressive IP blacklist»
esr(config-ips-upgrade-user-server)# url https://security.etnetera.cz/feeds/
etn_aggressive.rules
esr(config-ips-upgrade-user-server)# upgrade interval 4
esr(config-ips-upgrade-user-server)# exit
esr(config-auto-upgrade)# user-server SSL-BlackList
esr(config-ips-upgrade-user-server)# description «Abuse.ch SSL Blacklist»
esr(config-ips-upgrade-user-server)# url https://sslbl.abuse.ch/blacklist/sslblacklist.rules
esr(config-ips-upgrade-user-server)# upgrade interval 4
esr(config-ips-upgrade-user-server)# exit
esr(config-auto-upgrade)# user-server C2-Botnet
esr(config-ips-upgrade-user-server)# description «Abuse.ch Botnet C2 IP Blacklist»
esr(config-ips-upgrade-user-server)# url https://sslbl.abuse.ch/blacklist/sslipblacklist.rules
esr(config-ips-upgrade-user-server)# upgrade interval 4
esr(config-ips-upgrade-user-server)# exit
```

### 7.6.5 Алгоритм настройки базовых пользовательских правил

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Задать имя и перейти в режим конфигурирования набора пользовательских правил | `esr(config)# security ips-category user-defined <WORD>` | <WORD> – имя набора пользовательских правил, задаётся строкой до 32 символов. |
| 2 | Задать описание набора пользовательских правил<br><br>(не обязательно). | `esr(config-ips-category)# description <DESCRIPTION>` | <DESCRIPTION> – описание задаётся строкой до 255 символов. |
| 3 | Создать правило и перейти в режим конфигурирования правила. | `esr(config-ips-category)# rule <ORDER>` | <ORDER> – номер правила, принимает значения [1..512]. |
| 4 | Задать описание правила<br><br>(не обязательно) | `esr(config-ips-category-rule)# description <DESCRIPTION>` | <DESCRIPTION> – описание задаётся строкой до 255 символов. |
| 5 | Указать действие данного правила | `esr(config-ips-category-rule)# action { alert \| reject \| pass \| drop }` | • alert – прохождение трафика разрешается, и сервис IPS/IDS генерирует сообщение;<br>• reject – прохождение трафика запрещается. Если это TCP трафик отправителю и получателю посылается пакет TCP-RESET, для остального типа трафика посылается пакет ICMP-ERROR. Сервис IPS/IDS генерирует сообщение;<br>• pass – прохождение трафика разрешается;<br>• drop – прохождение трафика запрещается, и сервис IPS/IDS генерирует сообщение. |
| 6 | Установить имя IP-протокола, для которого должно срабатывать правило | `esr(config-ips-category-rule)# protocol <PROTOCOL>` | <PROTOCOL> – принимает значения any/ip/icmp/http/tcp/udp<br><br>При указании значения «any» правило будет срабатывать для любых протоколов |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 7 | Установить IP-адреса отправителя для которых должно срабатывать правило | `esr(config-ips-category-rule)# source-address {ip <ADDR> \| ip-prefix <ADDR/LEN> \| object-group <OBJ_GR_NAME> \| policy-object-group { protect \| external } \| any }` | <<ADDR> – IP-адрес отправителя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];<br><br><ADDR/LEN> – IP-подсеть отправителя, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и LEN принимает значения [1..32].<br><br>< OBJ_GR_NAME> – имя профиля IP-адресов, который содержит ip адреса отправителя, задаётся строкой до 31 символа.<br><br>• protect – устанавливает в качестве адресов отправителя, protect адреса определенные в политике IPS/IDS;<br>• external – устанавливает в качестве адресов отправителя, external адреса определенные в политике IPS/IDS.<br><br>При указании значения «any» правило будет срабатывать для любого IP-адреса отправителя. |
| 8 | Установить номера TCP/UDP-портов отправителя, для которых должно срабатывать правило.<br><br>Для значения protocol icmp, значение source-port может быть только any | esr(config-ips-category-rule)# source-port {any \| <PORT> \| object-group <OBJ-GR-NAME> } | <PORT> – номер TCP/UDP-порта отправителя, принимает значения [1..65535].<br><br><OBJ_GR_NAME> – имя профиля TCP/UDP портов отправителя, задаётся строкой до 31 символа.<br><br>При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта отправителя. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 9 | Установить IP-адреса получателя для которых должно срабатывать правило | `esr(config-ips-category-rule)# destination-address {ip <ADDR> \| ip-prefix <ADDR/LEN> \| object-group <OBJ_GR_NAME> \| policy-object-group { protect \| external } \| any }` | <<ADDR> – IP-адрес получателя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];<br><br><ADDR/LEN> – IP-подсеть получателя, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и LEN принимает значения [1..32].<br><br>< OBJ_GR_NAME> – имя профиля IP-адресов, который содержит ip адреса получателя, задаётся строкой до 31 символа.<br><br>• protect – устанавливает в качестве адресов получателя, protect адреса определенные в политике IPS/IDS;<br>• external -устанавливает в качестве адресов получателя, external адреса определенные в политике IPS/IDS.<br><br>При указании значения «any» правило будет срабатывать для любого IP-адреса получателя. |
| 10 | Установить номера TCP/UDP-портов получателя, для которых должно срабатывать правило.<br><br>Для значения protocol icmp, значение destination-port может быть только any | `esr(config-ips-category-rule)# destination-port {any \| <PORT> \| object-group <OBJ-GR-NAME> }` | <PORT> – номер TCP/UDP-порта получателя, принимает значения [1..65535].<br><br><OBJ_GR_NAME> – имя профиля TCP/UDP портов получателя, задаётся строкой до 31 символа.<br><br>При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта получателя. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 11 | Установить направление потока трафика, для которого должно срабатывать правило | `esr(config-ips-category-rule)# direction { one-way \| round-trip }` | • one-way – трафик передаётся в одну сторону.<br>• round-trip – трафик передаётся в обе стороны. |
| 12 | Определить сообщение которое IPS/IDS будет записывать в лог, при срабатывании этого правила | `esr(config-ips-category-rule)# meta log-message <MESSAGE>` | <MESSAGE> – текстовое сообщение, задаётся строкой до 129 символов. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 13 | Определить классификацию трафика, которая будет записывать в лог, при срабатывании этого правила<br><br>(не обязательно) | `esr(config-ips-category-rule)# meta classification-type { not-suspicious \| unknown \| bad-unknown \| attempted-recon \| successful-recon-limited \| successful-recon-largescale \| attempted-dos \| successful-dos \| attempted-user \| unsuccessful-user \| successful-user \| attempted-admin \| successful-admin \| rpc-portmap-decode \| shellcode-detect \| string-detect \| suspicious-filename-detect \| suspicious-login \| system-call-detect \| tcp-connection \| trojan-activity \| unusual-client-port-connection \| network-scan \| denial-of-service \| non-standard-protocol \| protocol-command-decode \| web-application-activity \| web-application-attack \| misc-activity \| misc-attack \| icmp-event \| inappropriate-content \| policy-violation \| default-login-attempt }` | • not-suspicious – не подозрительный трафик.<br>• unknown – неизвестный трафик.<br>• bad-unknown – потенциально плохой трафик.<br>• attempted-recon – попытка утечки информации.<br>• successful-recon-limited – утечка информации.<br>• successful-recon-largescale – масштабная утечка информации.<br>• attempted-dos – попытка отказа в обслуживании.<br>• successful-dos – отказ в обслуживании.<br>• attempted-user – попытка получения привилегий пользователя.<br>• unsuccessful-user – безуспешная попытка получения привилегий пользователя.<br>• successful-user – успешная попытка получения привилегий пользователя.<br>• attempted-admin – попытка получения привилегий администратора.<br>• successful-admin – успешная попытка получения привилегий администратора.<br>• rpc-portmap-decode – декодирование запроса RPC.<br>• shellcode-detect – обнаружен исполняемый код.<br>• string-detect – обнаружена подозрительная строка. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| | | | • suspicious-filename-detect – было обнаружено подозрительное имя-файла.<br>• suspicious-login – была обнаружена попытка входа с использованием подозрительного имени пользователя.<br>• system-call-detect – обнаружен системный вызов.<br>• tcp-connection – обнаружено TCP-соединение.<br>• trojan-activity – был обнаружен сетевой троян.<br>• unusual-client-port-connection – клиент использовал необычный порт.<br>• network-scan – обнаружение сетевого сканирования.<br>• denial-of-service – обнаружение атаки отказа в обслуживании.<br>• non-standard-protocol – обнаружение нестандартного протокола или события.<br>• protocol-command-decode – обнаружена попытка шифрования.<br>• web-application-activity – доступ к потенциально уязвимому веб-приложению.<br>• web-application-attack – атака на веб-приложение.<br>• misc-activity – прочая активность.<br>• misc-attack – прочие атаки.<br>• icmp-event – общее событие ICMP. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| | | | • inappropriate-content – обнаружено неприемлемое содержание.<br>• policy-violation – потенциальное нарушение корпоративной конфиденциальности.<br>• default-login-attempt – попытка входа с помощью стандартного логина/пароля. |
| 14 | Установить значение кода DSCP, для которого должно срабатывать правило (не обязательно). | `esr(config-ips-category-rule)# ip dscp <DSCP>` | <DSCP> – значение кода DSCP, принимает значения [0..63]. |
| 15 | Установить значение времени жизни пакета (TTL), для которого должно срабатывать правило<br><br>(не обязательно). | `esr(config-ips-category-rule)# ip ttl <TTL>` | <TTL> – значение TTL, принимает значения в диапазоне [1..255]. |
| 16 | Установить номер IP-протокола, для которого должно срабатывать правило<br><br>Применимо только для значения protocol any<br><br>(не обязательно). | `esr(config-ips-category-rule)# ip protocol-id <ID>` | <ID> – идентификационный номер IP-протокола, принимает значения [1..255]. |
| 17 | Установить значения ICMP CODE, для которого должно срабатывать правило<br><br>Применимо только для значения protocol icmp<br><br>(не обязательно). | `esr(config-ips-category-rule)# ip icmp code <CODE>` | <CODE> – значение CODE протокола ICMP, принимает значение в диапазоне [0..255]. |
| | | `esr(config-ips-category-rule)# ip icmp code comparison-operator { greater-than \| less-than }` | Оператор сравнения для значения ip icmp code:<br><br>• greater-than – больше чем..<br>• less-than –меньше чем.. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 18 | Установить значения ICMP ID, для которого должно срабатывать правило<br><br>Применимо только для значения protocol icmp<br><br>(не обязательно). | `esr(config-ips-category-rule)# ip icmp id <ID>` | <ID> – значение ID протокола ICMP, принимает значение в диапазоне [0.. 65535]. |
| 19 | Установить значения ICMP Sequence-ID, для которого должно срабатывать правило<br><br>Применимо только для значения protocol icmp<br><br>(не обязательно). | `esr(config-ips-category-rule)# ip icmp sequence-id <SEQ-ID>` | <SEQ-ID> – значение Sequence-ID протокола ICMP, принимает значение в диапазоне [0.. 4294967295]. |
| 20 | Установить значения ICMP TYPE, для которого должно срабатывать правило<br><br>Применимо только для значения protocol icmp<br><br>(не обязательно). | `esr(config-ips-category-rule)# ip icmp type <TYPE>` | <TYPE> – значение TYPE протокола ICMP, принимает значение в диапазоне [0..255]. |
| | | `esr(config-ips-category-rule)# ip icmp type comparison-operator { greater-than \| less-than }` | Оператор сравнения для значения ip icmp type:<br><br>• greater-than – больше чем..<br>• less-than –меньше чем.. |
| 21 | Установить значения TCP Acknowledgment-Number, для которого должно срабатывать правило<br><br>Применимо только для значения protocol tcp<br><br>(не обязательно). | `esr(config-ips-category-rule)# ip tcp acknowledgment-number <ACK-NUM>` | <ACK-NUM> – значение Acknowledgment-Number протокола TCP, принимает значение в диапазоне [0.. 4294967295]. |
| 22 | Установить значения TCP Sequence-ID, для которого должно срабатывать правило<br><br>Применимо только для значения protocol tcp<br><br>(не обязательно). | `esr(config-ips-category-rule)# ip tcp sequence-id <SEQ-ID>` | <SEQ-ID> – значение Sequence-ID протокола TCP, принимает значение в диапазоне [0.. 4294967295]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 23 | Установить значения TCP Window-Size, для которого должно срабатывать правило<br><br>Применимо только для значения protocol tcp<br><br>(не обязательно). | `esr(config-ips-category-rule)# ip tcp window-size <SIZE>` | <SIZE> – значение Window-Size протокола TCP, принимает значение в диапазоне [0.. 65535]. |
| 24 | Установить ключевые слова протокола HTTP, для которых должно срабатывать правило<br><br>Применимо только для значения protocol http<br><br>(не обязательно). | `esr(config-ips-category-rule)# ip http { accept \| accept-enc \| accept-lang \| client-body \| connection \| content-type \| cookie \| file-data \| header \| header-names \| host \| method \| protocol \| referer \| request-line \| response-line \| server-body \| start \| start-code \| start-msg \| uri \| user-agent }` | Значение ключевых слов см в документации Suricata 4.X.<br><br>https://suricata.readthedocs.io/en/suricata-4.1.4/rules/http-keywords.html |
| 25 | Установить значение ключевого слова URI LEN протокола HTTP, для которых должно срабатывать правило<br><br>Применимо только для значения protocol http<br><br>(не обязательно). | `esr(config-ips-category-rule)# ip http urilen <LEN>` | <LEN> – принимает значение в диапазоне [0.. 65535]. |
| | | `esr(config-ips-category-rule)# ip http urilen comparison-operator { greater-than \| less-than }` | Оператор сравнения для значения ip http urilen:<br><br>• greater-than – больше чем..<br>• less-than –меньше чем.. |
| 26 | Установить значение содержимого пакетов (Payload content), для которых должно срабатывать правило<br><br>(не обязательно). | `esr(config-ips-category-rule)# payload content <CONTENT>` | <CONTENT> – текстовое сообщение, задаётся строкой до 1024 символов. |
| 27 | Не различать прописные и заглавные буквы в описании содержимого пакетов.<br><br>Применимо только совместно с командой payload content<br><br>(не обязательно). | `esr(config-ips-category-rule)# payload no-case` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 28 | Установить сколько байтов с начала содержимого пакета будет проверено.<br><br>Применимо только совместно с командой payload content<br><br>(не обязательно). | `esr(config-ips-category-rule)# payload depth <DEPTH>` | <DEPTH> – число байт с начала содержимого пакета, принимает значение в диапазоне [1.. 65535].<br><br>По умолчанию проверяется все содержимое пакета. |
| 29 | Установить число байт смещения от начала содержимого пакета для проверки.<br><br>Применимо только совместно с командой payload content<br><br>(не обязательно). | `esr(config-ips-category-rule)# payload offset <OFFSET>` | <OFFSET> – число байт смещения от начала содержимого пакета, принимает значение в диапазоне [1.. 65535].<br><br>По умолчанию проверяется с начала содержимого. |
| 30 | Установить размер содержимого пакетов, для которых должно срабатывать правило.<br><br>(не обязательно) | `esr(config-ips-category-rule)# payload data-size <SIZE>` | <SIZE> – размер содержимого пакетов, принимает значение в диапазоне [0.. 65535]. |
| | | `esr(config-ips-category-rule)# payload data-size comparison-operator { greater-than \| less-than }` | Оператор сравнения для значения payload data-size:<br><br>• greater-than – больше чем..<br>• less-than –меньше чем. |
| 31 | Указать пороговое значение количества пакетов, при котором сработает правило<br><br>(не обязательно) | `esr(config-ips-category-rule)# threshold count <COUNT>` | <COUNT> – число пакетов, принимает значение в диапазоне [1.. 65535]. |
| 32 | Указать интервал времени, для которого считается пороговое количество пакетов.<br><br>(Обязательно если включен threshold count ) | `esr(config-ips-category-rule)# threshold second <SECOND>` | <SECOND> – интервал времени в секундах, принимает значение в диапазоне [1.. 65535]. |
| 33 | Указать по адресу отправителя или получателя будут считаться пороги.<br><br>(Обязательно если включен threshold count ) | `esr(config-ips-category-rule)# threshold track { by-src \| by-dst }` | • by-src – считать пороговое значение для пакетов с одинаковым IP-отправителя.<br>• by-dst – считать пороговое значение для пакетов с одинаковым IP-получателя. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 34 | Указать метод обработки пороговых значений | `esr(config-ips-category-rule)# threshold type {threshold \| limit \| both }` | • threshold – выдавать сообщение каждый раз по достижении порога.<br>• limit – выдавать сообщение не чаще <COUNT> раз за интервал времени <SECOND>.<br>• both – комбинация threshold и limit.<br>Сообщение будет генерироваться, если в течении интервала времени <SECOND> было <COUNT> или более пакетов подходящих под условия правила, и сообщение будет отправлено только один раз в течении интервала времени <SECOND> |

### 7.6.6 Пример настройки базовых пользовательских правил

**Задача:**

Написать правило для защиты сервера с IP 192.168.1.10 от DOS-атаки ICMP-пакетами большого размера.

**Решение:**

Создадим набор пользовательских правил:

```
esr(config)# security ips-category user-defined USER
```

Создадим правило для защиты от атаки:

```
esr(config-ips-category)# rule 10
esr(config-ips-category-rule)# description «Big ICMP DoS»
```

Мы будем отбрасывать пакеты:

```
esr(config-ips-category-rule)# action drop
```

Настроим сообщение об атаке:

```
esr(config-ips-category-rule)# meta log-message «Big ICMP DoS»
esr(config-ips-category-rule)# meta classification-type successful-dos
```

Укажем тип протокола для правила:

```
esr(config-ips-category-rule)# protocol icmp
```

Так как мы указали протокол icmp, то в качестве порта отправителя и получателя требуется указать any:

```
esr(config-ips-category-rule)# source-port any
esr(config-ips-category-rule)# destination-port any
```

В качестве адреса получателя укажем наш сервер:

```
esr(config-ips-category-rule)# destination-address ip 192.168.1.10
```

Атакующий может отправлять пакеты с любого адреса:

```
esr(config-ips-category-rule)# source-address any
```

Зададим направление трафика:

```
esr(config-ips-category-rule)# direction one-way
```

Правило будет срабатывать на пакеты размером больше 1024байт:

```
esr(config-ips-category-rule)# payload data-size 1024
esr(config-ips-category-rule)# payload data-size comparison-operator greate
r-than
```

Правило будет срабатывать если нагрузка на сервер будет превышать 3Мб/с, при этом сообщение об атаке будет генерироваться не чаше одного раза в минуту:

```
3 Мб/с = 3145728 бит в сек
Пакет размером 1Кбайт = 8192 бита
3145728 / 8192 = 384 пакета в сек
384 * 60 = 23040 пакетов в минуту
```

```
esr(config-ips-category-rule)# threshold count 2340
esr(config-ips-category-rule)# threshold second 60
esr(config-ips-category-rule)# threshold track by-dst
esr(config-ips-category-rule)# threshold type both
```

### 7.6.7 Алгоритм настройки расширенных пользовательских правил

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Задать имя и перейти в режим конфигурирования набора пользовательских правил. | `esr(config)# security ips-category user-defined <WORD>` | <WORD> – имя набора пользовательских правил, задаётся строкой до 32 символов. |
| 2 | Задать описание набора пользовательских правил<br><br>(не обязательно). | `esr(config-ips-category)# description <DESCRIPTION>` | <DESCRIPTION> –описание задаётся строкой до 255 символов. |
| 3 | Создать расширенное правило и перейти в режим его конфигурирования. | `esr(config-ips-category)# rule-advanced <SID>` | <SID> – номер правила, принимает значения [1.. 4294967295] |
| 4 | Задать описание правила<br><br>(не обязательно) | `esr(config-ips-category-rule-advanced)# description <DESCRIPTION>` | <DESCRIPTION> –описание задаётся строкой до 255 символов. |
| 5 | Указать действие данного правила | `esr(config-ips-category-rule-advanced)# rule-text <LINE>` | <CONTENT> -текстовое сообщение в формате SNORT 2.X / Suricata 4.X, задаётся строкой до 1024 символов.<br><br>*При написании правил символ " требуется заменить на символ '* |

### 7.6.8 Пример настройки расширенных пользовательских правил

**Задача:**

Написать правило детектирующее атаку типа Slowloris.

**Решение:**

Создадим набор пользовательских правил:

```
esr(config)# security ips-category user-defined ADV
```

Создадим расширенное правило:

```
esr(config-ips-category)# rule-advanced 1
esr(config-ips-category-rule-advanced)# description «Slow Loris rule 1»
esr(config-ips-category-rule-advanced)# rule-text "alert tcp any any -> any 80 (msg:'Possible
Slowloris Attack Detected';
flow:to_server,established; content:'X-a|3a|'; distance:0; pcre:'/\d\d\d\d/'; distance:0;
content:'|0d 0a|'; sid:10000001;)"
```

Создадим ещё одно расширенное правило, работающее по схожему алгоритму, чтобы определить какое из правил будет эффективнее:

```
esr(config-ips-category)# rule-advanced 2
esr(config-ips-category-rule-advanced)# description «Slow Loris rule 2»
esr(config-ips-category-rule-advanced)# rule-text «alert tcp $EXTERNAL_NET any -> $HOME_NET
$HTTP_PORTS (msg:'SlowLoris.py DoS attempt'; flow:established,to_server,no_stream; content:'X-
a:'; dsize:<15; detection_filter:track by_dst, count 3, seconds 30; classtype:denial-of-
service; sid: 10000002; rev:1; )
```

# 8 Управление резервированием



## 8.1 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.

### 8.1.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Перейти в режим конфигурирования интерфейса/туннеля/сетевого моста, для которого необходимо настроить протокол VRRP | `esr(config)# interface <IF-TYPE><IF-NUM>` | <IF-TYPE> – тип интерфейса;<br><br><IF-NUM> – F/S/P – F-фрейм (1), S – слот (0), P – порт. |
| | | `esr(config)# tunnel <TUN-TYPE><TUN-NUM>` | <TUN-TYPE> – тип туннеля;<br><br><TUN-NUM> – номер туннеля. |
| | | `esr(config)# bridge <BR-NUM>` | <BR-NUM> – номер сетевого моста. |
| 2 | Настроить необходимые параметры на интерфейсе/туннеле/сетевом мосту, включая IP-адрес | | |
| 3 | Включить VRRP-процесс на IP-интерфейсе. | `esr(config-if-gi)# vrrp` | |
| | | `esr(config-if-gi)# ipv6 vrrp` | |
| 4 | Установить виртуальный IP-адрес VRRP-маршрутизатора. | `esr(config-if-gi)# vrrp ip <ADDR/LEN>` | <ADDR/LEN> – виртуальный IP-адрес, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. Можно указать несколько IP-адресов перечислением через запятую. Может быть назначено до 4 IP-адресов на интерфейс. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| | | `esr(config-if-gi)# ipv6 vrrp ip <IPV6-ADDR>` | <IPV6-ADDR> – виртуальный IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. Можно указать до 8ми IPv6-адресов перечислением через запятую. |
| 5 | Установить идентификатор VRRP-маршрутизатора. | `esr(config-if-gi)# vrrp id <VRID>` | <VRID> – идентификатора VRRP-маршрутизатора, принимает значения [1..255]. |
| | | `esr(config-if-gi)# ipv6 vrrp id <VRID>` | |
| 6 | Установить приоритет VRRP-маршрутизатора. | `esr(config-if-gi)# vrrp priority <PR>` | <PR> – приоритет VRRP-маршрутизатора, принимает значения [1..254].<br><br>Значение по умолчанию: 100. |
| | | `esr(config-if-gi)# ipv6 vrrp priority <PR>` | |
| 7 | Установить принадлежность VRRP-маршрутизатора к группе. Группа предоставляет возможность синхронизировать несколько VRRP-процессов, так если в одном из процессов произойдет смена мастера, то в другом процессе также произведется смена ролей. | `esr(config-if-gi)# vrrp group <GRID>` | <GRID> – идентификатор группы VRRP-маршрутизатора, принимает значения [1..32]. |
| | | `esr(config-if-gi)# ipv6 vrrp group <GRID>` | |
| 8 | Установить IP-адрес, который будет использоваться в качестве IP-адреса отправителя для VRRP-сообщений. | `esr(config-if-gi)# vrrp source-ip <IP>` | <IP> – IP-адрес отправителя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| | | `esr(config-if-gi)# ipv6 vrrp source-ip <IPV6>` | <IPV6> – IPv6-адрес отправителя, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. |
| 9 | Установить интервал между отправкой VRRP-сообщений | `esr(config-if-gi)# vrrp timers advertise <TIME>` | <TIME> – время в секундах, принимает значения [1..40].<br><br>Значение по умолчанию: 1 секунда. |
| | | `esr(config-if-gi)# ipv6 vrrp timers advertise <TIME>` | |

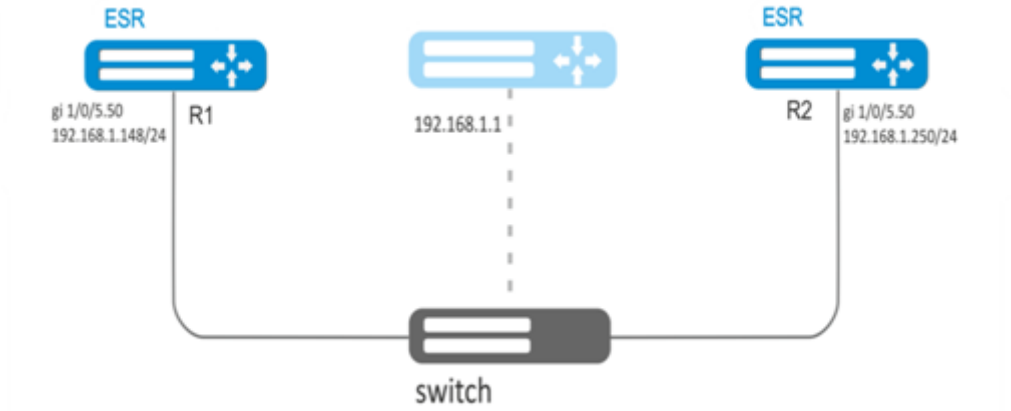
| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 10 | Установить интервал, по истечении которого происходит отправка GratuituousARP сообщения(ий) при переходе маршрутизатора в состояние Master. | `esr(config-if-gi)# vrrp timers garp delay <TIME>` | <TIME> – время в секундах, принимает значения [1..60].<br><br>Значение по умолчанию: 5 секунд. |
| 11 | Установить количество GratuituousARP сообщений, которые будут отправлены при переходе маршрутизатора в состояние Master. | `esr(config-if-gi)# vrrp timers garp repeat <COUNT>` | <COUNT> – количество сообщений, принимает значения [1..60].<br><br>Значение по умолчанию: 5. |
| 12 | Установить интервал, по истечении которого будет происходить периодическая отправка GratuituousARP сообщения(ий), пока маршрутизатор находится в состоянии Master. | `esr(config-if-gi)# vrrp timers garp refresh <TIME>` | <TIME> – время в секундах, принимает значения [1..65535].<br><br>Значение по умолчанию: Периодическая отправка отключена. |
| 13 | Установить количество GratuituousARP сообщений, которые будут отправляться с периодом garprefresh пока маршрутизатор находится в состоянии Master. | `esr(config-if-gi)# vrrp timers garp refresh-repeat <COUNT>` | <COUNT> –количество сообщений, принимает значения [1..60].<br><br>Значение по умолчанию: 1. |
| 14 | Определить, будет ли Backup-маршрутизатор с более высоким приоритетом пытаться перехватить на себя роль Master у текущего Master-маршрутизатора с более низким приоритетом. | `esr(config-if-gi)# vrrp preemption disable`<br>`esr(config-if-gi)# ipv6 vrrp preemption disable` | |
| 15 | Установить временной интервал, по истечении которого Backup-маршрутизатор с более высоким приоритетом будет пытаться перехватить на себя роль Master у текущего Master-маршрутизатора с более низким приоритетом. | `esr(config-if-gi)# vrrp preemption delay <TIME>`<br>`esr(config-if-gi)# ipv6 vrrp preemption delay <TIME>` | <TIME> – время ожидания, определяется в секундах [1..1000].<br><br>Значение по умолчанию: 0 |
| 16 | Установить пароль для аутентификации с соседом. | `esr(config-if-gi)# vrrp authentication key ascii-text { <CLEAR-TEXT> \| encrypted <ENCRYPTED-TEXT> }` | <CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов;<br><br><ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...). |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 17 | Определить алгоритм аутентификации. | `esr(config-if-gi)# vrrp authentication algorithm <ALGORITHM>` | <ALGORITHM> – алгоритм аутентификации:<br>• **cleartext** – пароль, передается открытым текстом;<br>• **md 5** – пароль хешируется по алгоритму md5. |
| 18 | Задать версию VRRP-протокола. | `esr(config-if-gi)# vrrp version <VERSION>` | <VERSION> – версия VRRP-протокола: 2, 3. |
| 19 | Установить режим, когда vrrp IP-адрес остается в состоянии UP вне зависимости от состояния самого интерфейса. (не обязательно) | `esr(config-if-gi)# vrrp force-up` | |
| 20 | Определить задержку между установлением ipv6 vrrp состояния MASTER и началом рассылки ND сообщений. | `esr(config-if-gi)# ipv6 vrrp timers nd delay <TIME>` | <TIME> – время в секундах, принимает значения [1..60].<br><br>Значение по умолчанию: 5 |
| 21 | Определить период обновления информации протокола ND для ipv6 vrrp в состоянии MASTER. | `esr(config-if-gi)# ipv6 vrrp timers nd refresh <TIME>` | <TIME> – время в секундах, принимает значения [1..65535].<br><br>Значение по умолчанию: 5 |
| 22 | Определить количество ND сообщений отправляемых за период обновления для ipv6 vrrp в состоянии MASTER. | `esr(config-if-gi)# ipv6 vrrp timers nd refresh-repeat <NUM>` | <NUM> – количество, принимает значения [1..60].<br><br>Значение по умолчанию: 0 |
| 23 | Определить количество отправок ND пакетов после установки ipv6 vrrp в состоянии MASTER. | `esr(config-if-gi)# ipv6 vrrp timers nd repeat <NUM>` | <NUM> – количество, принимает значения [1..60].<br><br>Значение по умолчанию: 1 |

### 8.1.2 Пример настройки 1

**Задача:**

Организовать виртуальный шлюз для локальной сети в VLAN 50, используя протокол VRRP. В качестве локального виртуального шлюза используется IP-адрес 192.168.1.1.




**Решение:**

Предварительно нужно выполнить следующие действия:

- создать соответствующий саб-интерфейс;
- настроить зону для саб-интерфейса;
- указать IP-адрес для саб-интерфейса.

Основной этап конфигурирования:

*Настроим маршрутизатор R1.*

В созданном саб-интерфейсе настроим VRRP. Укажем уникальный идентификатор VRRP:

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

Укажем IP-адрес виртуального шлюза 192.168.1.1/24:

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

Включим VRRP:

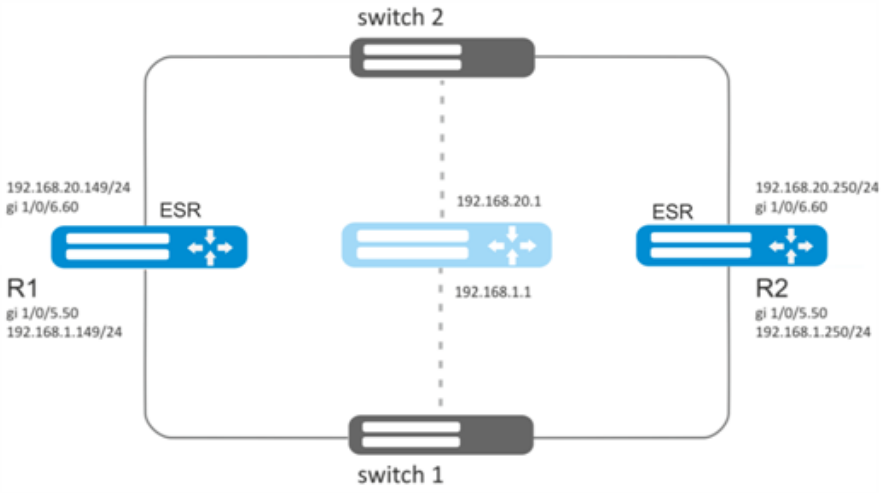
```
R1(config-subif)# vrrp
R1(config-subif)# exit
```

*Произвести аналогичные настройки на R2.*

### 8.1.3 Пример настройки 2

**Задача:**

Организовать виртуальные шлюзы для подсети 192.168.1.0/24 в VLAN 50 и подсети 192.168.20.0/24 в VLAN 60, используя протокол VRRP с функцией синхронизации Мастера. Для этого используем объединение VRRP-процессов в группу. В качестве виртуальных шлюзов используются IP-адреса 192.168.1.1 и 192.168.20.1.




**Решение:**

Предварительно нужно выполнить следующие действия:

- создать соответствующие саб-интерфейсы;
- настроить зону для саб-интерфейсов;
- указать IP-адреса для саб-интерфейсов.

Основной этап конфигурирования:

Настроим маршрутизатор R1.

Настроим VRRP для подсети 192.168.1.0/24 в созданном саб-интерфейсе.

Укажем уникальный идентификатор VRRP:

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

Укажем IP-адрес виртуального шлюза 192.168.1.1:

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

Укажем идентификатор VRRP-группы:

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

Включим VRRP:

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

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

Укажем уникальный идентификатор VRRP:

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

Укажем IP-адрес виртуального шлюза 192.168.20.1:

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

Укажем идентификатор VRRP-группы:

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

Включим VRRP:

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

*Произвести аналогичные настройки на R2.*

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

## 8.2 Настройка VRRP tracking

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

### 8.2.1 Алгоритм настройки

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

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 5 | Создать статический IP-маршрут к указанной подсети с указанием Tracking-объекта. | `esr(config)# ip route [ vrf <VRF> ] <SUBNET> { <NEXTHOP> [ resolve ] \| interface <IF> \| tunnel <TUN> \| wan load-balance rule <RULE> \| blackhole \| unreachable \| prohibit } [ <METRIC> ] [ track <TRACK-ID> ]` | <VRF> – имя экземпляра VRF, задается строкой до 31 символа;<br><br><SUBNET> – адрес назначения, может быть задан в следующих видах:<br><br>AAA.BBB.CCC.DDD – IP-адрес хоста, где каждая часть принимает значения [0..255];<br><br>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].<br><br><NEXTHOP> – IP-адрес шлюза задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];<br><br>• **resolve** – при указании данного параметра IP-адрес шлюза будет рекурсивно вычислен через таблицу маршрутизации. Если при рекурсивном вычислении не удастся найти шлюз из напрямую подключенной подсети, то данный маршрут не будет установлен в систему;<br><br><IF> – имя IP-интерфейса, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора;<br><br><TUN> – имя туннеля, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора;<br><br><RULE> – номер правила wan, задаётся в диапазоне [1..50]; |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| | | | • **blackhole** – при указании команды пакеты до данной подсети будут удаляться устройством без отправки уведомлений отправителю;<br>• **unreachable** – при указании команды пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Host unreachable, code 1);<br>• **prohibit** – при указании команды, пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Communication administratively prohibited, code 13);<br>[METRIC] – метрика маршрута, принимает значения [0..255];<br><br><TRACK-ID> – идентификатор Tracking объекта. Если маршрут привязан к Tracking объекту, то он появится в системе только при выполнении всех условий, заданных в объекте. |
| 6 | Настройка IP адреса, доступность которого проверяется отправкой пингов. Необходимо разрешить ICMP в Firewall. | esr(config-bridge)# vrrp track-ip <AAA.BBB.CCC.DDD> | AAA.BBB.CCC.DDD – IP-адрес хоста, где каждая часть принимает значения [0..255]. |
| 7 | Интервал, через который осуществляется отправка пингов. | esr(config-bridge)# vrrp track-ip <seconds> | <seconds> – интервал времени в секундах [3..60]. Значение по умолчанию 10. |

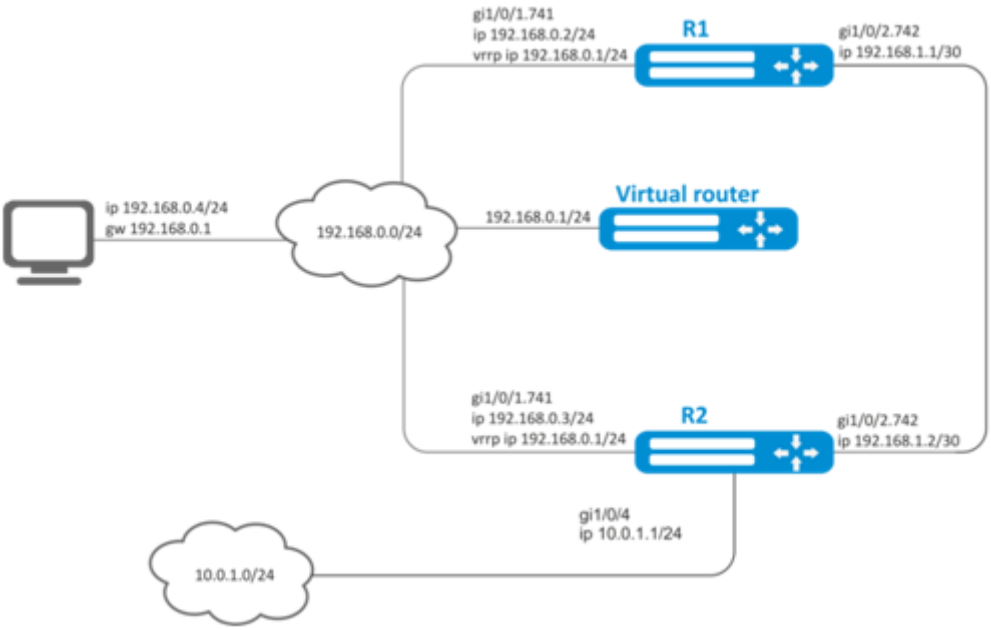
| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 8 | Количество пингов, которое отправляется при мониторинге удаленного адреса. | esr(config-bridge)# vrrp track-ip packets <packets> | <packets> – количество отправляемых пакетов [1..5]. Значение по умолчанию 5. |

### 8.2.2 Пример настройки

**Задача:**

Для подсети 192.168.0.0/24 организован виртуальный шлюз 192.168.0.1/24 с использованием протокола VRRP на основе аппаратных маршрутизаторов R1 и R2. Так же между маршрутизаторами R1 и R2 есть линк с вырожденной подсетью 192.168.1.0/30. Подсеть 10.0.1.0/24 терминируется только на маршрутизаторе R2. ПК имеет IP-адрес 192.168.0.4/24 и шлюз по умолчанию 192.168.0.1

Когда маршрутизатор R1 находится в состоянии vrrp backup, трафик от ПК в подсеть 10.0.1.0/24 пойдет без дополнительных настроек. Когда маршрутизатор R1 находится в состоянии vrrp master, необходим дополнительный маршрут для подсети 10.0.1.0/24 через интерфейс 192.168.1.2.



**Исходные конфигурации маршрутизаторов:**

1 Маршрутизатор R1

```
hostname R1
interface gigabitethernet 1/0/1
  switchport forbidden default-vlan
exit
interface gigabitethernet 1/0/1.741
  ip firewall disable
  ip address 192.168.0.2/24
  vrrp id 10
  vrrp ip 192.168.0.1/24
  vrrp
exit
interface gigabitethernet 1/0/2
  switchport forbidden default-vlan
exit
interface gigabitethernet 1/0/2.742
  ip firewall disable
  ip address 192.168.1.1/30
exit
```

2 Маршрутизатор R2

```
hostname R2
interface gigabitethernet 1/0/1
  switchport forbidden default-vlan
exit
interface gigabitethernet 1/0/1.741
  ip firewall disable
  ip address 192.168.0.3/24
  vrrp id 10
  vrrp ip 192.168.0.1/24
  vrrp
exit
interface gigabitethernet 1/0/2
  switchport forbidden default-vlan
exit
interface gigabitethernet 1/0/2.742
  ip firewall disable
  ip address 192.168.1.2/30
exit
interface gigabitethernet 1/0/4
  ip firewall disable
  ip address 10.0.1.1/24
exit
```

**Решение:**

На маршрутизаторе R2 никаких изменений не требуется так как подсеть 10.0.1.0/24 терминируется на нем, и в момент, когда R2 выступает в роли vrrp master, пакеты будут переданы в соответствующий

интерфейс. На маршрутизаторе необходимо создать маршрут для пакетов с IP-адресом назначения из сети 10.0.1.0/24 в момент, когда R1 выступает в роли vrrp master.

Для этого создадим tracking-object с соответствующим условием:

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

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

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

# 9 Управление удаленным доступом



## 9.1 Настройка сервера удаленного доступа к корпоративной сети по PPTP-протоколу

PPTP (англ. Point-to-Point Tunneling Protocol) – туннельный протокол типа точка-точка, позволяющий компьютеру устанавливать защищённое соединение с сервером за счёт создания специального туннеля в обычной незащищенной сети. PPTP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например, Интернет. PPTP может также использоваться для организации туннеля между двумя локальными сетями. PPTP использует дополнительное TCP-соединение для обслуживания туннеля.

### 9.1.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Создать профиль PPTP-сервера. | `esr(config)# remote-access pptp <NAME>` | <NAME> – имя профиля PPTP-сервера, задаётся строкой до 31 символа. |
| 2 | Указать описание конфигурируемого сервера (не обязательно). | `esr(config-pptp-server)# description <DESCRIPTION>` | <DESCRIPTION> – описание PPTP-сервера, задаётся строкой до 255 символов. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 3 | Указать IP-адрес, который должен обрабатывать PPTP-сервер. | `esr(config-pptp-server)# outside-address { object-group <OBJ-GROUP-NETWORK-NAME> \| ip-address <ADDR> \| interface { <IF> \| <TUN> } }` | <OBJ-GROUP-NETWORK-NAME> – имя профиля содержащего IP-адрес, который должен слушать PPTP-сервер, задаётся строкой до 31 символа;<br><br><ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];<br><br><IF> – тип и идентификатор интерфейса маршрутизатора;<br><br><TUN> – тип и номер туннеля маршрутизатора. |
| 4 | Указать IP-адрес локального шлюза. | `esr(config-pptp-server)# local-address { object-group <OBJ-GROUP-NETWORK-NAME > \| ip-address <ADDR> }` | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит IP-адрес локального шлюза, задаётся строкой до 31 символа;<br><br><ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 5 | Указать список IP-адресов, из которого PPTP выдаются динамические IP-адреса удаленным пользователям. | `esr(config-pptp-server)# remote-address { object-group <OBJ-GROUP-NETWORK-NAME > \| address-range <FROM-ADDR>-<TO-ADDR> }` | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит список IP-адресов удаленных пользователей, задаётся строкой до 31 символа;<br><br><FROM-ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];<br><br><TO-ADDR> – конечный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 6 | Выбрать режим аутентификации PPTP-клиентов. | `esr(config-pptp-server)# authentication mode { local \| radius }` | • local – аутентификация пользователя по локальной базе.<br>• radius – аутентификация пользователя по базе RADIUS-сервера. На маршрутизаторе должен быть сконфигурирован механизм взаимодействия с RADIUS-сервером см. раздел Алгоритм настройки AAA по протоколу RADIUS |
| 7 | Разрешить необходимые методы аутентификации удаленных пользователей | `esr(config-pptp-server)# authentication method <METHOD>` | <METHOD> - метод аутентификации, принимает значения [chap, mschap, mschap-v2, eap, pap].<br><br>По умолчанию разрешен только chap |
| 8 | Указать имя пользователя (при использовании локальной аутентификации пользователей). | `esr(config-pptp-server) username < NAME >` | <NAME> – имя пользователя, задаётся строкой до 12 символов. |
| 9 | Указать пароль пользователя(при использовании локальной аутентификации пользователей). | `esr(config-pptp-user) password ascii-text { <PASSWORD> \| encrypted <PASSWORD> }` | <PASSWORD> – пароль пользователя, задается строкой до 32 символов. |
| 10 | Активировать пользователя(при использовании локальной аутентификации пользователей). | `esr(config-pptp-user) enable` | |
| 11 | Включить PPTP-сервер в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall (см. раздел Конфигурирование Firewall). | `esr(config-pptp-server)# security-zone <NAME>` | <NAME> – имя зоны безопасности, задаётся строкой до 31 символа. |
| 12 | Включить сервер. | `esr(config-pptp-server)# enable` | |
| 13 | Указать DSCP-приоритет исходящих пакетов (не обязательно). | `esr(config-pptp-server)# dscp <DSCP>` | <DSCP>– dscp приоритет исходящих пакетов [0..63]. |

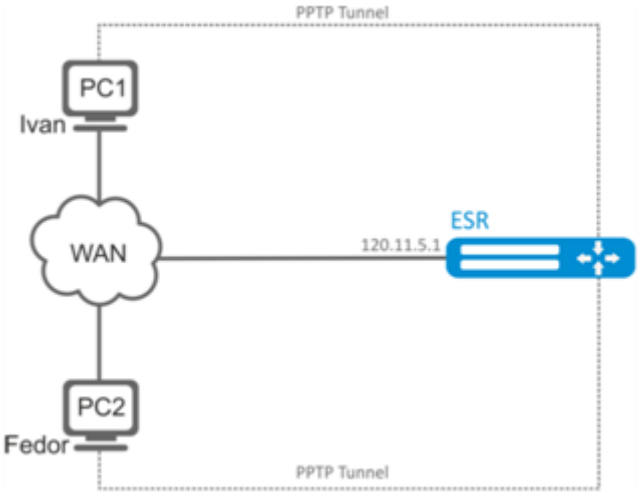
| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 14 | Включить шифрование MPPE для PPTP-соединений (не обязательно). | `esr(config-pptp-server)# encryption mppe` | |
| 15 | Указать размер MTU (MaximumTransmitionUnit) для сервера (не обязательно).<br>MTU более 1500 будет активно только в случае применения команды "system jumbo-frames" | `esr(config-pptp-server) mtu <MTU>` | <MTU> – значение MTU, принимает значения в диапазоне [1280..1500].<br><br>Значение по умолчанию: 1500. |
| 16 | Указать список DNS-серверов, которые будут использовать удаленные пользователи (не обязательно). | `esr(config-pptp-server)# dns-servers object-group <OBJ-GROUP-NETWORK -NAME >` | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, содержащего, который содержит адреса необходимых DNS-серверов, задаётся строкой до 31 символа. |
| 17 | Указать список WINS-серверов, которые будут использовать удаленные пользователи (не обязательно). | `esr(config-pptp-server)# wins-servers object-group <OBJ-GROUP-NETWORK -NAME >` | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит адреса необходимых WINS-серверов, задаётся строкой до 31 символа. |

### 9.1.2 Пример настройки

**Задача:**

Настроить PPTP-сервер на маршрутизаторе.

- адрес PPTP-сервера – 120.11.5.1;
- шлюз внутри туннеля для подключающихся клиентов – 10.10.10.1;
- пул IP-адресов для выдачи 10.10.10.5-10.10.10.25;
- DNS-серверы: 8.8.8.8, 8.8.8.4;
- учетные записи для подключения – fedor, ivan.



**Решение:**

Создадим профиль адресов, содержащий адрес, который должен слушать сервер:

```
esr# configure
esr(config)# object-group network pptp_outside
esr(config-object-group-network)# ip address-range 120.11.5.1
esr(config-object-group-network)# exit
```

Создадим профиль адресов, содержащий адрес локального шлюза:

```
esr(config)# object-group network pptp_local
esr(config-object-group-network)# ip address-range 10.10.10.1
esr(config-object-group-network)# exit
```

Создадим профиль адресов, содержащий адреса клиентов:

```
esr(config)# object-group network pptp_remote
esr(config-object-group-network)# ip address-range 10.10.10.5-10.10.10.25
esr(config-object-group-network)# exit
```

Создадим PPTP-сервер и привяжем вышеуказанные профили:

```
esr(config)# remote-access pptp remote-workers
esr(config-pptp)# local-address object-group pptp_local
esr(config-pptp)# remote-address object-group pptp_remote
esr(config-pptp)# outside-address object-group pptp_outside
esr(config-pptp)# dns-servers object-group pptp_dns
```

Выберем метод аутентификации пользователей PPTP-сервера:

```
esr(config-pptp)# authentication mode local
```

Укажем зону безопасности, к которой будут относиться сессии пользователей:

```
esr(config-pptp)# security-zone VPN
```

Создадим PPTP-пользователей *Ivan* и *Fedor* для PPTP-сервера:

```
esr(config-pptp)# username ivan
esr(config-pptp-user)# password ascii-text password1
esr(config-pptp-user)# enable
esr(config-pptp-user)# exit
esr(config-pptp)# username fedor
esr(config-pptp-user)# password ascii-text password2
esr(config-pptp-user)# enable
esr(config-pptp-user)# exit
esr(config-pptp)# exit
```

Включим PPTP-сервер:

```
esr(config-pptp)# enable
```

После применения конфигурации маршрутизатор будет прослушивать 120.11.5.1:1723. Состояние сессий PPTP-сервера можно посмотреть командой:

```
esr# show remote-access status pptp server remote-workers
```

Счетчики сессий PPTP-сервера можно посмотреть командой:

```
esr# show remote-access counters pptp server remote-workers
```

Очистить счетчики сессий PPTP-сервера можно командой:

```
esr# clear remote-access counters pptp server remote-workers
```

Завершить сессию пользователя fedor PPTP-сервера можно одной из следующих команд:

```
esr# clear remote-access session pptp username fedor
esr# clear remote-access session pptp server remote-workers username fedor
```

Конфигурацию PPTP-сервера можно посмотреть командой:

```
esr# show remote-access configuration pptp remote-workers
```

⚠ Помимо создания PPTP-сервера необходимо в firewall открыть TCP-порт 1723 для обслуживания соединений и разрешить протокол GRE(47) для туннельного трафика.

## 9.2 Настройка сервера удаленного доступа к корпоративной сети по L2TP over IPsec протоколу

L2TP (англ. Layer 2 Tunneling Protocol – протокол туннелирования второго уровня) –туннельный протокол, использующийся для поддержки виртуальных частных сетей. L2TP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например, Интернет. L2TP может также использоваться для организации туннеля между двумя локальными сетями. L2TP использует дополнительное UDP-соединение для обслуживания туннеля. L2TP-протокол не предоставляет средств шифрования данных и поэтому он обычно используется в связке с группой протоколов IPsec, которая предоставляет безопасность на пакетном уровне.

### 9.2.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Создать профиль L2TP-сервера. | `esr(config)# remote-access l2tp <NAME>` | <NAME> – имя профиля L2TP-сервера, задаётся строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 2 | Указать описание конфигурируемого сервера (не обязательно). | `esr(config-l2tp-server)# description <DESCRIPTION>` | <DESCRIPTION> – описание L2TP-сервера, задаётся строкой до 255 символов. |
| 3 | Указать IP-адрес, который должен слушать L2TP-сервер. | `esr(config-l2tp-server)# outside-address { object-group <NAME> \| ip-address <ADDR> \| interface { <IF> \| <TUN> } }` | <OBJ-GROUP-NETWORK-NAME> – имя профиля содержащего IP-адрес, который должен слушать L2TP-сервер, задаётся строкой до 31 символа;<br><br><ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];<br><br><IF> – тип и идентификатор интерфейса маршрутизатора;<br><br><TUN> – тип и номер туннеля маршрутизатора. |
| 4 | Указать IP-адрес локального шлюза либо отключить firewall для PPTP-сервера | `esr(config-l2tp-server)# local-address { object-group <OBJ-GROUP-NETWORK -NAME> \| ip-address <ADDR> }` | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит IP-адрес локального шлюза, задаётся строкой до 31 символа;<br><br><ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 5 | Указать список IP-адресов из которого L2TP выдаются динамические IP-адреса удаленным пользователям. | `esr(config-l2tp-server)# remote-address { object-group <OBJ-GROUP-NETWORK -NAME > \| address-range <FROM-ADDR>-<TO-ADDR> }` | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит список IP-адресов удаленных пользователей, задаётся строкой до 31 символа;<br><br><FROM-ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];<br><br><TO-ADDR> – конечный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 6 | Выбрать режим аутентификации L2TP-клиентов. | `esr(config-l2tp-server)# authentication mode { local \| radius }` | • local – аутентификация пользователя по локальной базе.<br>• radius – аутентификация пользователя по базе RADIUS-сервера. На маршрутизаторе должен быть сконфигурирован механизм взаимодействия с RADIUS-сервером см. раздел Алгоритм настройки AAA по протоколу RADIUS |
| 7 | Разрешить необходимые методы аутентификации удаленных пользователей | `esr(config-l2tp-server)# authentication method <METHOD>` | <METHOD> - метод аутентификации, принимает значения [chap, mschap, mschap-v2, eap, pap].<br><br>По умолчанию разрешен только chap. |
| 8 | Включить L2TP-сервер в зону безопасности и настроить правила взаимодействия между зонами (см. раздел Конфигурирование Firewall). | `esr(config-l2tp-server)# security-zone <NAME>` | <NAME> – имя зоны безопасности, задаётся строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 9 | Указать имя пользователя (при использовании локальной базы аутентификации). | `esr(config-l2tp-server) username < NAME >` | <NAME> – имя пользователя, задаётся строкой до 12 символов. |
| 10 | Указать пароль пользователя (при использовании локальной базы аутентификации). | `esr(config-l2tp-user) password ascii-text { <PASSWORD> \| encrypted <PASSWORD> }` | <PASSWORD> – пароль пользователя, задается строкой до 32 символов. |
| 11 | Включить пользователя (при использовании локальной базы аутентификации). | `esr(config-l2tp-user) enable` | |
| 12 | Выбрать метод аутентификации по ключу для IKE-соединения (). | `esr(config-l2tp-server)# ipsec authentication method pre-shared-key` | |
| 13 | Указать общий секретный ключ для аутентификации, который должен совпадать у обоих сторон, устанавливающих туннель. | `esr(config-l2tp-server)# ipsec authentication pre-shared-key { ascii-text { <TEXT> \| encrypted <ENCRYPTED-TEXT> } \| hexadecimal {<HEX> \| encrypted <ENCRYPTED-HEX> } }` | <TEXT> – строка [1..64] ASCII символов;<br><br><HEX> – число размером [1..32] байт задаётся строкой [2..128] символов в шестнадцатеричном формате (0xYYYY...) или (YYYY...).<br><br><ENCRYPTED-TEXT> – зашифрованный пароль размером [1..32] байт, задаётся строкой [2..128] символов;<br><br><ENCRYPTED-HEX> – зашифрованное число размером [2..64] байт, задаётся строкой [2..256] символов. |
| 14 | Включить сервер. | `esr(config-l2tp-server)# enable` | |
| 15 | Указать DSCP приоритет исходящих пакетов. | `esr(config-l2tp-server)# dscp <DSCP>` | <DSCP> – dscp приоритет исходящих пакетов [0..63]. |
| 16 | Указать размер MTU (MaximumTransmitionUnit) для сервера (не обязательно).<br>MTU более 1500 будет активно только в случае применения команды "system jumbo-frames" | `esr(config-l2tp-server) mtu <MTU>` | <MTU> – значение MTU, принимает значения в диапазоне [1280..1500].<br><br>Значение по умолчанию: 1500. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 17 | Указать список DNS-серверов, которые будут использовать удаленные пользователи (не обязательно). | `esr(config-l2tp-server)# dns-servers object-group <OBJ-GROUP-NETWORK -NAME >` | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, содержащего, который содержит адреса необходимых DNS-серверов, задаётся строкой до 31 символа. |
| 18 | Указать список WINS-серверов, которые будут использовать удаленные пользователи (не обязательно). | `esr(config-l2tp-server)# wins-servers object-group <OBJ-GROUP-NETWORK -NAME >` | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит адреса необходимых WINS-серверов, задаётся строкой до 31 символа. |

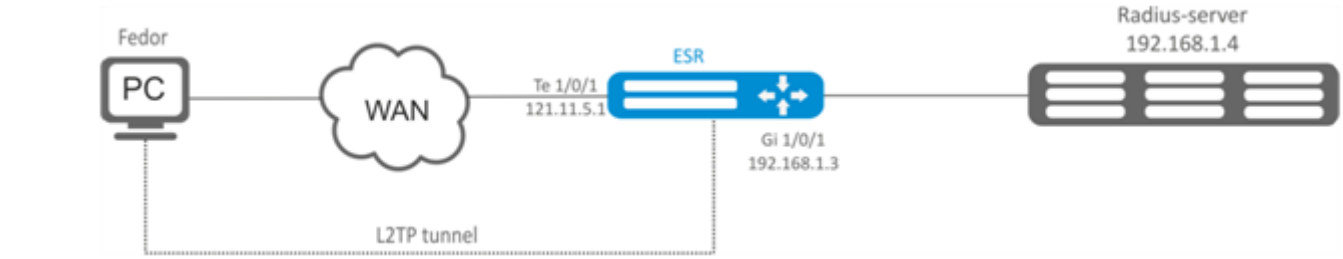
### 9.2.2 Пример настройки

**Задача:**

Настроить L2TP-сервер на маршрутизаторе для подключения удаленных пользователей к ЛВС. Аутентификация пользователей проходит на RADIUS-сервере.

- адрес L2TP-сервера – 120.11.5.1;
- шлюз внутри туннеля – 10.10.10.1;
- адрес Radius-сервера – 192.168.1.4;

Для IPsec используется метод аутентификации по ключу: ключ — «password».




**Решение:**

Предварительно нужно выполнить следующие действия:

- Настроить подключение к RADIUS-серверу;
- Настроить зоны для интерфейсов te1/0/1 и gi1/0/1;
- Указать IP-адреса для интерфейсов te1/0/1 и te1/0/1.

Создадим профиль адресов, содержащий адрес локального шлюза:

```
esr(config)# object-group network l2tp_local
esr(config-object-group-network)# ip address-range 10.10.10.1
esr(config-object-group-network)# exit
```

Создадим профиль адресов, содержащий DNS-серверы:

```
esr(config)# object-group network pptp_dns
esr(config-object-group-network)# ip address-range 8.8.8.8
esr(config-object-group-network)# ip address-range 8.8.4.4
esr(config-object-group-network)# exit
```

Создадим L2TP-сервер и привяжем к нему вышеуказанные профили:

```
esr(config)# remote-access l2tp remote-workers
esr(config-l2tp)# local-address ip-address 10.10.10.1
esr(config-l2tp)# remote-address address-range 10.10.10.5-10.10.10.15
esr(config-l2tp)# outside-address ip-address 120.11.5.1
esr(config-l2tp)# dns-server object-group l2tp_dns
```

Выберем метод аутентификации пользователей L2TP-сервера:

```
esr(config-l2tp)# authentication mode radius
```

Укажем зону безопасности, к которой будут относиться сессии пользователей:

```
esr(config-l2tp)# security-zone VPN
```

Выберем метод аутентификации первой фазы IKE и зададим ключ аутентификации:

```
esr(config-l2tp)# ipsec authentication method psk
esr(config-l2tp)# ipsec authentication pre-shared-key ascii-text password
```

Включим L2TP-сервер:

```
esr(config-l2tp)# enable
```

После применения конфигурации маршрутизатор будет прослушивать IP-адрес 120.11.5.1 и порт 1701.
Состояние сессий L2TP-сервера можно посмотреть командой:

```
esr# show remote-access status l2tp server remote-workers
```

Счетчики сессий L2TP-сервера можно посмотреть командой:

```
esr# show remote-access counters l2tp server remote-workers
```

Очистить счетчики сессий L2TP-сервера можно командой:

```
esr# clear remote-access counters l2tp server remote-workers
```

Завершить сессию пользователя fedor L2TP-сервера можно одной из следующих команд:

```
esr# clear remote-access session l2tp username fedor
esr# clear remote-access session l2tp server remote-workers username fedor
```

Конфигурацию L2TP-сервера можно посмотреть командой:

```
esr# show remote-access configuration l2tp remote-workers
```

⚠ Помимо создания L2TP-сервера необходимо в firewall открыть UDP-порты 500, 1701, 4500 для обслуживания соединений и разрешить протоколы ESP(50) и GRE(47) для туннельного трафика.

## 9.3 Настройка сервера удаленного доступа к корпоративной сети по OpenVPN протоколу

OpenVPN — полнофункциональное средство для построения виртуальных частных сетей (Virtual Private Networks, VPN), организации удалённого доступа, и решения ряда других задач, связанных с безопасностью передачи данных, базирующееся на SSL.

### 9.3.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Создать профиль OpenVPN-сервера. | `esr(config)# remote-access openvpn <NAME>` | <NAME> – имя профиля OpenVPN-сервера, задаётся строкой до 31 символа. |
| 2 | Указать описание конфигурируемого сервера (не обязательно). | `esr(config-openvpn-server)# description <DESCRIPTION>` | <DESCRIPTION> – описание OpenVPN-сервера, задаётся строкой до 255 символов. |
| 3 | Определим подсеть, из которой выдаются IP-адреса пользователям. (только для tunnel ip) | `esr(config-openvpn-server)# network <ADDR/LEN>` | <ADDR/LEN> – адрес подсети, имеет следующий формат:<br><br>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]; |
| 4 | Указать инкапсулируемый протокол. | `esr(config-openvpn-server)# protocol <PROTOCOL>` | <PROTOCOL> – тип инкапсуляции, возможные значения:<br><br>• TCP-инкапсуляция в TCP-сегменты;<br>• UDP-инкапсуляция в UDP-дейтаграммы. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 5 | Определить тип соединения с частной сетью через OpenVPN-сервер. | `esr(config-openvpn-server)# tunnel <TYPE>` | <TYPE> – инкапсулирующий протокол, принимает значения:<br>• ip – соединение точка-точка;<br>• ethernet – подключение к L2 домену. |
| 6 | Указать список IP-адресов, из которого OpenVPN сервером выдаются динамические IP-адреса удаленным пользователям в режиме L2. (только для tunnel ethernet) | `esr(config-openvpn-server)# address-range <FROM-ADDR>-<TO-ADDR>` | <FROM-ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];<br><TO-ADDR> – конечный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 7 | Включить клиентские соединения по OpenVPN в L2 домен (только для tunnel ethernet). | `esr(config-openvpn-server)# bridge-group <BRIDGE-ID>` | <BRIDGE-ID> – идентификационный номер моста. |
| 8 | Указать сертификаты и ключи. | `esr(config-openvpn-server)# certificate <CERTIFICATE-TYPE> <NAME>` | <CERTIFICATE-TYPE> – тип сертификата или ключа, может принимать следующие значения:<br>• ca – сертификат удостоверяющего сервера;<br>• crl – список отозванных сертификатов;<br>• dh – ключ Диффи-Хеллмана;<br>• server - crt – публичный сертификат сервера;<br>• server - key – приватный ключ сервера;<br>• ta – HMAC ключ.<br><NAME> – имя сертификата или ключа, задаётся строкой до 31 символа. |
| 9 | Выбрать алгоритм шифрования, используемый при передачи данных. | `esr(config-openvpn-server)# encryption algorithm <ALGORITHM>` | <ALGORITHM> – идентификатор протокола шифрования, принимает значения: 3des,blowfish128, aes128. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 10 | Включить OpenVPN-сервер в зону безопасности и настроить правила взаимодействия между зонами (см. раздел Конфигурирование Firewall). | `esr(config-openvpn-server)# security-zone <NAME>` | <NAME> – имя зоны безопасности, задаётся строкой до 31 символа. |
| 11 | Определить дополнительные параметры для указанного пользователя OpenVPN-сервера (при использовании локальной базы для аутентификации пользователей). | `esr(config-openvpn-server)# username < NAME >` | <NAME> – имя пользователя, задаётся строкой до 31 символа. |
| 12 | Определить подсеть для указанного пользователя OpenVPN-сервера. | `esr(config-openvpn-user)# subnet <ADDR/LEN>` | <ADDR/LEN> – адрес подсети, имеет следующий формат: AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32]. |
| 13 | Определить статический ip-адрес для указанного пользователя OpenVPN-сервера | `esr(config-openvpn-user)# ip address <ADDR>` | <ADDR> – адрес имеет следующий формат: AAA.BBB.CCC.DDD – IP-адрес подсети, где AAA-DDD принимают значения [0..255]. |
| 14 | Включить профиль OpenVPN-сервера. | `esr(config-openvpn-server)# enable` | |
| 15 | Включить блокировку передачи данных между клиентами (не обязательно). | `esr(config-openvpn-server)# client-isolation` | |
| 16 | Устанавливается максимальное количество одновременных пользовательских сессий (не обязательно). | `esr(config-openvpn-server)# client-max <VALUE>` | <VALUE> – максимальное количество пользователей, принимает значения [1..65535]. |
| 17 | Включается механизм сжатия передаваемых данных между клиентами и сервером OpenVPN (не обязательно). | `esr(config-openvpn-server)# compression` | |
| 18 | Указать список DNS-серверов, которые будут использовать удаленные пользователи (не обязательно). | `esr(config-openvpn-server)# dns-server <ADDR>` | <ADDR> – IP-адрес DNS сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 19 | Указать TCP/UDP порт, который будет прослушиваться OpenVPN –сервером (не обязательно). | `esr(config-openvpn-server)# port <PORT>` | <PORT> – TCP/UDP порт, принимает значения [1..65535].<br><br>Значение по умолчанию: 1194 |
| 20 | Включить анонсирование маршрута по умолчанию для OpenVPN соединений, что приводит к замене маршрута по умолчанию на клиентской стороне (не обязательно). | `esr(config-openvpn-server)# redirect-gateway` | |
| 21 | Включить анонсирование указанных подсетей, шлюзом является IP-адрес OpenVPN-сервера (не обязательно). | `esr(config-openvpn-server)# route <ADDR/LEN>` | <ADDR/LEN> – адрес подсети, имеет следующий формат:<br><br>AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32]; |
| 22 | Указать временной интервал, по истечению которого встречная сторона считается недоступной (не обязательно). | `esr(config-openvpn-server)# timers holdtime <TIME>` | <TIME> – время в секундах, принимает значения [1..65535].<br><br>Значение по умолчанию: 120 |
| 23 | Указать временной интервал, по истечению которого идет проверка соединения со встречной стороной (не обязательно). | `esr(config-openvpn-server)# timers keepalive <TIME>` | <TIME> – время в секундах, принимает значения [1..65535].<br><br>Значение по умолчанию: 10 |
| 24 | Разрешить подключаться к OpenVPN-серверу нескольким пользователям с одним сертификатом. | `esr(config-openvpn-server)# duplicate-cn` | |
| 25 | Указать список WINS-серверов, которые будут использовать удаленные пользователи (не обязательно). | `esr(config-openvpn-server)# wins-server <ADDR>` | <ADDR> – IP-адрес WINS сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 26 | Изменить алгоритм аутентификации OpenVPN-клиентов (не обязательно). | `esr(config-openvpn-server)# authentication algorithm <ALGORITHM>` | <ALGORITHM> – алгоритм аутентификации:<br>• 8-128 bits key size: md4, rsa-md4, md5, rsa-md5, mdc2, rsa-mdc2<br>• 8-160 bits key size: sha, sha1, rsa-sha, rsa-sha1, rsa-sha1-2, dsa, dsa-sha, dsa-sha1, dsa-sha1-old, ripemd160, rsa-ripemd160, ecdsa-with-sha1<br>• 8-224 bits key size: sha-224, rsa-sha-224<br>• 8-256 bits key size: sha-256, rsa-sha-256<br>• 8-384 bits key size: sha-384, rsa-sha-384<br>• 8-512 bits key size: sha-512, rsa-sha-512, whirlpool<br>Значение по умолчанию: sha |

### 9.3.2 Пример настройки

**Задача:**

Настроить OpenVPN-сервер в режиме L3 на маршрутизаторе для подключения удаленных пользователей к ЛВС.

- подсеть OpenVPN-сервера – 10.10.100.0/24;
- режим – L3;
- аутентификация на основе сертификатов.


**Решение:**

Предварительно нужно выполнить следующие действия:

- Подготовить сертификаты и ключи:
  - Сертификат Удостоверяющего Центра (CA)
  - Ключ и сертификат для OpenVPN сервера
  - Ключ Диффи-Хелмена и HMAC для TLS

- Настроить зону для интерфейса te1/0/1
- Указать IP-адреса для интерфейса te1/0/1.

Импортируем по tftp сертификаты и ключи:

```
esr# copy tftp://192.168.16.10:/ca.crt certificate:ca/ca.crt
esr# copy tftp://192.168.16.10:/dh.pem certificate:dh/dh.pem
esr# copy tftp://192.168.16.10:/server.key certificate:server-key/server.key
esr# copy tftp://192.168.16.10:/server.crt certificate:server-crt/server.crt
esr# copy tftp://192.168.16.10:/ta.key certificate:ta/ta.key
```

Создадим OpenVPN-сервер и подсеть, в которой он будет работать:

```
esr(config)# remote-access openvpn AP
esr(config-openvpn)# network 10.10.100.0/24
```

Укажем тип соединения L3 и протокол инкапсуляции.

```
esr(config-openvpn)# tunnel ip
esr(config-openvpn)# protocol tcp
```

Объявим подсети ЛВС которые будут доступны через OpenVPN соединение и укажем DNS сервер

```
esr(config-)# route 10.10.0.0/20
esr(config-openvpn)# dns-server 10.10.1.1
```

Укажем ранее импортированные сертификаты и ключи, которые будет использоваться OpenVPN-сервером:

```
esr(config-openvpn)# certificate ca ca.crt
esr(config-openvpn)# certificate dh dh.pem
esr(config-openvpn)# certificate server-key server.key
esr(config-openvpn)# certificate server-crt server.crt
esr(config-openvpn)# certificate ta ta.key
```

Укажем зону безопасности, к которой будут относиться сессии пользователей:

```
esr(config-openvpn)# security-zone VPN
```

Выберем алгоритм шифрования aes128:

```
esr(config-openvpn)# encryption algorithm aes128
```

Включим OpenVPN-сервер:

```
esr(config-openvpn)# enable
```

После применения конфигурации маршрутизатор будет прослушивать порт 1194 (используется по умолчанию).

Состояние сессий OpenVPN-сервера можно посмотреть командой:

```
esr# show remote-access status openvpn server AP
```

Счетчики сессий OpenVPN-сервера можно посмотреть командой:

```
esr# show remote-access counters openvpn server AP
```

Очистить счетчики сессий OpenVPN-сервера можно командой:

```
esr# clear remote-access counters openvpn server AP
```

Завершить сессию пользователя fedor OpenVPN-сервера можно одной из следующих команд:

```
esr# clear remote-access session openvpn username fedor
esr# clear remote-access session openvpn server AP username fedor
```

Конфигурацию OpenVPN-сервера можно посмотреть командой:

```
esr# show remote-access configuration openvpn AP
```

⚠ Помимо создания OpenVPN-сервера необходимо в firewall открыть TCP-порт 1194.

## 9.4 Настройка клиента удаленного доступа по протоколу PPPoE

PPPoE — это туннелирующий протокол (tunneling protocol), который позволяет инкапсулировать IP PPP через соединения Ethernet и обладает программными возможностями PPP-соединений, что позволяет использовать его для виртуальных соединений на соседнюю Ethernet-машину и устанавливать соединение точка-точка, которое используется для транспортировки IP-пакетов, а также работает с возможностями PPP. Это позволяет применять традиционное PPP-ориентированное ПО для настройки соединения, которое использует не последовательный канал, а пакетно-ориентированную сеть (например, Ethernet), чтобы организовать классическое соединение с логином и паролем для Интернет-соединений. Кроме того, IP-адрес по другую сторону соединения назначается только когда PPPoE-соединение открыто, позволяя динамическое переиспользование IP-адресов.

### 9.4.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Создать PPPoE-туннель и перейти в режим конфигурирования PPPoE-клиента. | `esr(config)# tunnel pppoe <PPPoE>` | <PPPoE> – порядковый номер туннеля от 1 до 10. |
| 2 | Указать описание конфигурируемого клиента (не обязательно). | `esr(config-pppoe)# description <DESCRIPTION>` | <DESCRIPTION> – описание PPPoE-сервера, задаётся строкой до 255 символов. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 3 | Указать имя экземпляра VRF, в котором будут использоваться PPPoE-клиент. (не обязательно) | `esr(config-pppoe)# ip vrf forwarding <VRF>` | <VRF> – имя VRF, задается строкой до 31 символа. |
| 4 | Указать интерфейс через который будет устанавливаться PPPoE соединение. | `esr(config-pppoe)# interface <IF>` | <IF> – интерфейс или группа интерфейсов. |
| 5 | Указать имя пользователя и пароль для подключения к PPPoE-серверу | `esr(config-pppoe)# username <NAME> password ascii-text { <CLEAR-TEXT> \| encrypted <ENCRYPTED-TEXT> }` | <NAME> – имя пользователя, задаётся строкой до 31 символа;<br><CLEAR-TEXT> – пароль, задаётся строкой [8 .. 64] символов;<br><ENCRYPTED-TEXT> – зашифрованный пароль, задаётся строкой [16..128] символов. |
| 6 | Включить PPPoE-туннель в зону безопасности и настроить правила взаимодействия между зонами (см. раздел Конфигурирование Firewall). | `esr(config-pppoe)# security-zone <NAME>` | <NAME>-имя зоны безопасности, задаётся строкой до 31 символа. |
| 7 | Активировать конфигурируемый профиль | `esr(config-pppoe)# enable` | |
| 8 | Указать метод аутентификации (не обязательно). | `esr(config-pppoe)# authentication method <METHOD>` | <METHOD> – метод аутентификации, возможные значения: chap, mschap, mschap-v2, eap, pap<br><br>Значение по умолчанию: chap |
| 9 | Включить отказ от получения маршрута по умолчанию от PPPoE-сервера (не обязательно). | `esr(config-pppoe)# ignore-default-route` | |
| | | | |
| 10 | Указать интервал времени, за который усредняется статистика о нагрузке (не обязательно). | `esr(config-pppoe)# load-average <TIME>` | <TIME> – интервал времени в секундах от 5 до 150 (по умолчанию 5 сек) |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 11 | Указать размер MTU (MaximumTransmitionUnit) для PPPOE-туннеля.<br>MTU более 1500 будет активно только если применена команда "system jumbo-frames"<br>(не обязательно). | `esr(config-pppoe)# mtu <MTU>` | <MTU> – значение MTU, принимает значения в диапазоне:<br>• для ESR-10/12V(F)/14VF – [1280..9600];<br>• для ESR-20/21 – [1280..9500];<br>• для ESR-100/200/1000/1200/1500/1700 [1280..10000].<br>Значение по умолчанию: 1500. |
| 12 | Изменить количество неудачных data-link тестов перед разрывом сессии (не обязательно). | `esr(config-pppoe)# ppp failure-count <NUM>` | <NUM> – количество неудачных data-link тестов, задается в диапазоне [1..100].<br>Значение по умолчанию: 10 |
| 13 | Изменить интервал времени в секундах, по истечении которого маршрутизатор отправляет keepalive-сообщение (не обязательно). | `esr(config-pppoe)# ppp timeout keepalive <TIME >` | <TIME> – время в секундах, задается в диапазоне [1..32767].<br>Значение по умолчанию: 10 |
| 14 | Переопределить значение поля MSS (Maximum segment size) во входящих TCP-пакетах (не обязательно). | `esr(config-pppoe)# ip tcp adjust-mss <MSS>` | <MSS> – значение MSS, принимает значения в диапазоне [500..1460].<br>Значение по умолчанию: 1460 |
| 15 | Включить запись статистики использования текущего туннеля (не обязательно). | `esr(config-pppoe)# history statistics` | |

Также для PPPoE-клиента возможно настроить:

- QoS в базовом или расширенном режимах (см. раздел Управление QoS);
- Proxy (см. раздел Проксирование HTTP/HTTPS-трафика);
- Мониторинг траффика (см. разделы Настройка Netflow и Настройка sFlow).

### 9.4.2 Пример настройки

**Задача:**

Настроить PPPoE-клиент на маршрутизаторе.

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


**Решение:**

Предварительно настроить PPPoE-сервер с учетными записями.

Зайдем в режим конфигурирования PPPoE-клиента и отключим межсетевой экран:

```
esr# configure
esr(config)# tunnel pppoe 1
esr(config-pppoe)# ip firewall disable
```

Укажем пользователя и пароль для подключения к PPPoE-серверу:

```
esr(config-pppoe)# username tester password ascii-text password
```

Укажем интерфейс через который будет устанавливаться PPPoE-соединение:

```
esr(config-pppoe)# interface gigabitethernet 1/0/7
esr(config- pppoe)# enable
```

Состояние PPPoE-туннеля можно посмотреть командой:

```
esr# show tunnels configuration pppoe 1
```

Счетчики сессий PPPoE-клиента можно посмотреть командой:

```
esr# show tunnels counters pppoe 1
```

## 9.5 Настройка клиента удаленного доступа по протоколу PPTP

PPTP (англ. Point-to-Point Tunneling Protocol) – туннельный протокол типа точка-точка, позволяющий устанавливать защищённое соединение за счёт создания специального туннеля в обычной незащищенной сети. PPTP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например, Интернет. PPTP может также использоваться для организации туннеля между двумя локальными сетями. PPTP использует дополнительное TCP-соединение для обслуживания туннеля.

### 9.5.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Создать PPTP-туннель и перейти в режим его конфигурирования. | `esr(config)# tunnel pptp <INDEX>` | <INDEX> – идентификатор туннеля в диапазоне: [1..10]. |
| 2 | Указать описание конфигурируемого туннеля (не обязательно). | `esr(config-pptp)# description <DESCRIPTION>` | <DESCRIPTION> – описание туннеля, задается строкой до 255 символов. |
| 3 | Указать экземпляр VRF, в котором будет работать данный PPTP-туннель (не обязательно). | `esr(config-pptp)# ip vrf forwarding <VRF>` | <VRF> – имя VRF, задается строкой до 31 символа. |
| 4 | Включить PPTP-туннель в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall (см. раздел Конфигурирование Firewall). | `esr(config-pptp)# security-zone <NAME>` | <NAME> – имя зоны безопасности, задаётся строкой до 31 символа. |
| | | `esr(config-pptp)# ip firewall disable` | |
| 5 | Установить удаленный IP-адрес для установки туннеля. | `esr(config-pptp)# remote address <ADDR>` | <ADDR> – IP-адрес локального шлюза, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 6 | Установить размер MTU (MaximumTransmitionUnit) для туннеля (не обязательно) | `esr(config-pptp)# mtu <MTU>` | <MTU> – значение MTU, принимает значения в диапазоне:<br>• для ESR-10/12V(F)/14VF – [552..9600];<br>• для ESR-20/21 – [552..9500];<br>• для ESR-100/200/1000/1200/1500/1700 [552..10000].<br>Значение по умолчанию: 1500. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 7 | Указать пользователя и установить пароль в открытой или зашифрованной форме для аутентификации удаленной стороны. | `esr(config-pptp)# username <NAME> password ascii-text { <WORD> \| encrypted <HEX> }` | <NAME> – имя пользователя, задается строкой до 31 символа.<br><br><WORD> – пароль в открытой форме, задается строкой [8..64] символов, может включать символы [0-9a-fA-F].<br><br><HEX> – пароль в зашифрованной форме, задается строкой [16..128] символов. |
| 8 | Активировать туннель | `esr(config-pptp)# enable` | |
| 9 | Переопределить значение поля MSS (Maximum segment size) во входящих TCP-пакетах (не обязательно). | `esr(config-pptp)# ip tcp adjust-mss <MSS>` | <MSS> – значение MSS, принимает значения в диапазоне [500..1460].<br>Значение по умолчанию: 1460 |
| 10 | Игнорировать маршрут по умолчанию через данный PPTP-туннель (не обязательно) | `esr(config-pptp)# ignore-default-route` | |
| 11 | Задать интервал времени, за который усредняется статистика о нагрузке на туннель (не обязательно). | `esr(config-pptp)# load-average <TIME>` | <TIME> – интервал в секундах, принимает значения [5..150]<br><br>Значение по умолчанию: 5 |
| 12 | Указать метод аутентификации (не обязательно). | `esr(config-pptp)# authentication method <METHOD>` | <METHOD> – метод аутентификации, возможные значения: chap, mschap, mschap-v2, eap, pap<br>Значение по умолчанию: chap |
| 13 | Включить запись статистики использования текущего туннеля (не обязательно). | `esr(config-pptp)# history statistics` | |
| 14 | Изменить интервал времени в секундах, по истечении которого маршрутизатор отправляет keepalive-сообщение (не обязательно). | `esr(config-pptp)# ppp timeout keepalive <TIME >` | <TIME> – время в секундах, задается в диапазоне [1..32767].<br>Значение по умолчанию: 10 |
| 15 | Изменить количество неудачных data-link тестов перед разрывом сессии (не обязательно). | `esr(config-pptp)# ppp failure-count <NUM>` | <NUM> – количество неудачных data-link тестов, задается в диапазоне [1..100].<br>Значение по умолчанию: 10 |

### 9.5.2 Пример настройки

**Задача:**

Настроить PPTP-туннель на маршрутизаторе:

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


**Решение:**

Создадим туннель PPTP:

```
esr(config)# tunnel pptp 1
```

Укажем учетную запись (пользователя Ivan) для подключения к серверу:

```
esr(config-pptp)# username ivan password ascii-text simplepass
```

Укажем удаленный шлюз:

```
esr(config-pptp)# remote address 20.20.0.1
```

Укажем зону безопасности:

```
esr(config-pptp)# security-zone VPN
```

Включим туннель PPTP:

```
esr(config-pptp)# enable
```

Состояние туннеля можно посмотреть командой:

```
esr# show tunnels status pptp
```

Счетчики входящих и отправленных пакетов можно посмотреть командой:

```
esr# show tunnels counters pptp
```

Конфигурацию туннеля можно посмотреть командой:

```
esr# show tunnels configuration pptp
```

## 9.6 Настройка клиента удаленного доступа по протоколу L2TP

L2TP (англ. Layer 2 Tunneling Protocol – протокол туннелирования второго уровня) –туннельный протокол, использующийся для поддержки виртуальных частных сетей. L2TP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например, Интернет. L2TP может также использоваться для организации туннеля между двумя локальными сетями. L2TP использует дополнительное UDP-соединение для обслуживания туннеля. L2TP-протокол не предоставляет средств шифрования данных и поэтому он обычно используется в связке с группой протоколов IPsec, которая предоставляет безопасность на пакетном уровне.

### 9.6.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Создать L2TP-туннель и перейти в режим его конфигурирования. | `esr(config)# tunnel l2tp <INDEX>` | <INDEX> – идентификатор туннеля в диапазоне: [1..10]. |
| 2 | Указать экземпляр VRF, в котором будет работать данный L2TP-туннель (не обязательно). | `esr(config-l2tp)# ip vrf forwarding <VRF>` | <VRF> – имя VRF, задаётся строкой до 31 символа. |
| 3 | Указать описание конфигурируемого туннеля (не обязательно). | `esr(config-l2tp)# description <DESCRIPTION>` | <DESCRIPTION> – описание туннеля, задается строкой до 255 символов. |
| 4 | Включить L2TP-туннель в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall (см. раздел Конфигурирование Firewall). | `esr(config-l2tp)# security-zone <NAME>` | <NAME> – имя зоны безопасности, задаётся строкой до 31 символа. |
| | | `esr(config-l2tp)# ip firewall disable` | |
| 5 | Установить удаленный IP-адрес для установки туннеля. | `esr(config-l2tp)# remote address <ADDR>` | <ADDR> – IP-адрес локального шлюза, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 6 | Указать пользователя и установить пароль в открытой или зашифрованной форме для аутентификации удалённой стороны. | `esr(config-l2tp)# username <NAME> password ascii-text { <WORD> \| encrypted <HEX> }` | <NAME>– имя пользователя, задается строкой до 31 символа.<br><br><WORD> – пароль в открытой форме, задается строкой [8..64] символов, может включать символы [0-9a-fA-F].<br><br><HEX> – пароль в зашифрованной форме, задается строкой [16..128] символов. |
| 7 | Выбрать метод аутентификации по ключу для IKE-соединения. | `esr(config-l2tp)# ipsec authentication method pre-shared-key` | |
| 8 | Указать общий секретный ключ для аутентификации, который должен совпадать у обоих сторон, устанавливающих туннель. | `esr(config-l2tp)# ipsec authentication pre-shared-key { ascii-text { <TEXT> \| encrypted <ENCRYPTED-TEXT> } \| hexadecimal {<HEX> \| encrypted <ENCRYPTED-HEX> } }` | <TEXT> – строка [1..64] ASCII символов;<br><HEX> – число размером [1..32] байт задаётся строкой [2..128] символов в шестнадцатеричном формате (0xYYYY...) или (YYYY...);<br><ENCRYPTED-TEXT> – зашифрованный пароль размером [1..32] байт, задаётся строкой [2..128] символов;<br><ENCRYPTED-HEX> – зашифрованное число размером [2..64] байт, задаётся строкой [2..256] символов. |
| 9 | Активировать туннель | `esr(config-l2tp)# enable` | |
| 10 | Установить размер MTU (MaximumTransmitionUnit) для туннеля (не обязательно). | `esr(config-l2tp)# mtu <MTU>` | <MTU> – значение MTU, принимает значения в диапазоне:<br><br>• для ESR-10/12V(F)/14VF – [552..9600];<br>• для ESR-20/21 – [552..9500];<br>• для ESR-100/200/1000/1200/1500/1700 [552..10000].<br><br>Значение по умолчанию: 1500. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 11 | Игнорировать маршрут по умолчанию через данный L2TP-туннель (не обязательно) | `esr(config-l2tp)# ignore-default-route` | |
| 12 | Указать метод аутентификации (не обязательно). | `esr(config-l2tp)# authentication method <METHOD>` | <METHOD> – метод аутентификации, возможные значения: chap, mschap, mschap-v2, eap, pap<br><br>Значение по умолчанию: chap |
| 13 | Задать интервал времени, за который усредняется статистика о нагрузке на туннель (не обязательно). | `esr(config-l2tp)# load-average <TIME>` | <TIME> – интервал в секундах, принимает значения [5..150]<br><br>Значение по умолчанию: 5 |
| 14 | Изменить интервал времени в секундах, по истечении которого маршрутизатор отправляет keepalive-сообщение (не обязательно). | `esr(config-l2tp)# ppp timeout keepalive <TIME >` | <TIME> – время в секундах, задается в диапазоне [1..32767].<br>Значение по умолчанию: 10 |
| 15 | Изменить количество неудачных data-link тестов перед разрывом сессии (не обязательно). | `esr(config-l2tp)# ppp failure-count <NUM>` | <NUM> – количество неудачных data-link тестов, задается в диапазоне [1..100].<br>Значение по умолчанию: 10 |
| Также для PPPoE-клиента возможно настроить QoS в базовом или расширенном режимах (см. раздел Управление QoS). | | | |

### 9.6.2 Пример настройки

**Задача:**

Настроить PPTP-туннель на маршрутизаторе:

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

**Решение:**

Создадим туннель L2TP:

```
esr(config)# tunnel l2tp 1
```

Укажем учетную запись (пользователя Ivan) для подключения к серверу:

```
esr(config-l2tp)# username ivan password ascii-text simplepass
```

Укажем удаленный шлюз:

```
esr(config-l2tp)# remote address 20.20.0.1
```

Укажем зону безопасности:

```
esr(config-l2tp)# security-zone VPN
```

Укажем метод аутентификации ipsec:

```
esr(config-l2tp)# ipsec authentication method pre-shared-key
```

Укажем ключ безопасности для ipsec:

```
esr(config-l2tp)# ipsec authentication pre-shared-key ascii-text password
```

Включим туннель L2TP:

```
esr(config-l2tp)# enable
```

Состояние туннеля можно посмотреть командой:

```
esr# show tunnels status l2tp
```

Счетчики входящих и отправленных пакетов можно посмотреть командой:

```
esr# show tunnels counters l2tp
```

Конфигурацию туннеля можно посмотреть командой:

```
esr# show tunnels configuration l2tp
```

# 10 Управление сервисами



## 10.1 Настройка DHCP-сервера

Встроенный DHCP-сервер маршрутизатора может быть использован для настройки сетевых параметров устройств в локальной сети. DHCP-сервер маршрутизаторов способен передавать дополнительные опции на сетевые устройства, например:

- default-router – IP-адрес маршрутизатора, используемого в качестве шлюза по умолчанию;
- domain-name – доменное имя, которое должен будет использовать клиент при разрешении имен хостов через Систему Доменных Имен (DNS);
- dns-server – список адресов серверов доменных имен в данной сети, о которых должен знать клиент. Адреса серверов в списке располагаются в порядке убывания предпочтения.

### 10.1.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Включить IPv4/IPv6 DHCP-сервер. | `esr(config)# ip dhcp-server [vrf <VRF>]` | <VRF> – имя экземпляра VRF, в рамках которого будет работать DHCP-сервер. Задается строкой до 31 символа. |
| | | `esr(config)# ipv6 dhcp-server [vrf <VRF>]` | |
| 2 | Задать значение кода DSCP для использования в IP-заголовке исходящих пакетов DHCP-сервера (не обязательно). | `esr(config)# ip dhcp-server dscp <DSCP>` | <DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].<br><br>Значение по умолчанию: 61. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 3 | Создать пул IPv4/IPv6-адресов DHCP-сервера и перейти в режим его конфигурирования. | `esr(config)# ip dhcp-server pool <NAME> [vrf <VRF>]` | <NAME> – имя пула IPv4/IPv6-адресов DHCP-сервера, задаётся строка до 31 символа.<br><br><VRF> – имя экземпляра VRF, в рамках которого будет работать данный пул IP-адресов DHCP-сервера. Задается строкой до 31 символа |
| | | `esr(config)# ipv6 dhcp-server pool <NAME> [vrf <VRF>]` | |
| 4 | Задать IPv4/IPv6-адрес и маску для подсети, из которой будет выделен пул IPv4/IPv6-адресов. | `esr(config-dhcp-server)# network <ADDR/LEN>` | <ADDR/LEN> – IP-адрес и префикс подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. |
| | | `esr(config-ipv6-dhcp-server)# network <IPV6-ADDR/LEN>` | <IPV6-ADDR/LEN> – IP-адрес и префикс подсети, задаётся в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128]. |
| 5 | Добавить диапазон IPv4/IPv6-адресов к пулу адресов, конфигурируемого DHCP-сервера. | `esr(config-dhcp-server)# address-range <FROM-ADDR>-<TO-ADDR>` | <FROM-ADDR> – начальный IP-адрес диапазона;<br><br><TO-ADDR> – конечный IP-адрес диапазона,<br><br>Адреса задаются в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].<br><br>Можно указать до 32 диапазонов IP-адресов, список задаётся через запятую. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| | | `esr(config-ipv6-dhcp-server)# address-range <FROM-ADDR>-<TO-ADDR>` | <FROM-ADDR> – начальный IPv6-адрес диапазона;<br><br><TO-ADDR> – конечный IP-адрес диапазона;<br><br>Адреса задаются в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. |
| 6 | Добавить IPv4/IPv6-адрес для определенного физического адреса к пулу адресов конфигурируемого DHCP-сервера (не обязательно). | `esr(config-dhcp-server)# address <ADDR> {mac-address <MAC> \| client-identifier <CI>}` | <ADDR> – IP-адрес клиента, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];<br><br><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].<br><br><CI> – идентификатор клиента согласно DHCPOption61. Может быть задан в одном из следующих видов:<br>• HH:HH:HH:HH:HH:HH:HH: – идентификатор клиента в шестнадцатеричной форме и mac-адрес клиента;<br>• STRING – текстовая строка длиной от 1 до 64 символов. |
| | | `esr(config-ipv6-dhcp-server)# address <ADDR> mac-address <MAC>` | <IPV6-ADDR> – IPv6-адрес клиента, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];<br><br><MAC> – MAC-адрес клиента, которому будет выдан IPv6-адрес, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF] |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 7 | Задать список IPv4-адресов шлюзов по умолчанию, которые DHCP-сервер будет сообщать клиентам, используя DHCP-опцию 3. | `esr(config-dhcp-server)# default-router <ADDR>` | <ADDR> – IP-адрес шлюза по умолчанию, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Можно указать до 8 IP-адресов, список задаётся через запятую. |
| 8 | Задать DNS-имя сетевого домена. Имя домена передаётся клиентам в составе DHCP-опции 15 (не обязательно). | `esr(config-dhcp-server)# domain-name <NAME>` | <NAME> – DNS-имя домена клиента, задаётся строкой до 255 символов. |
| | | `esr(config-ipv6-dhcp-server)# domain-name <NAME>` | |
| 9 | Задать список IPv4/IPv6-адресов DNS-серверов. Список передаётся клиентам в составе DHCP-опции 6 (не обязательно). | `esr(config-dhcp-server)# dns-server <ADDR>` | <ADDR> – IP-адрес DNS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Можно указать до 8 IP-адресов, список задаётся через запятую. |
| | | `esr(config-ipv6-dhcp-server)# dns-server <IPV6-ADDR>` | <IPV6-ADDR> – IPv6-адрес DNS-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. Можно указать до 8 IPv6-адресов, список задаётся через запятую. |
| 10 | Задать максимальное время аренды IP-адресов (не обязательно).<br><br>Если DHCP-клиент запрашивает время аренды, превосходящее максимальное значение, то будет установлено время, заданное этой командой. | `esr(config-dhcp-server)# max-lease-time <TIME>` | <TIME> – максимальное время аренды IP-адреса, задаётся в формате DD:HH:MM, где:<br>• DD – количество дней, принимает значения [0..364];<br>• HH – количество часов, принимает значения [0..23];<br>• MM – количество минут, принимает значения [0..59]<br><br>Значение по умолчанию: 1 день |
| | | `esr(config-ipv6-dhcp-server)# max-lease-time <TIME>` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 11 | Задать время аренды, на которое клиенту будет выдан IP-адрес (не обязательно).<br><br>Данное время будет использоваться если клиент не запрашивал определенное время аренды. | `esr(config-dhcp-server)# default-lease-time <TIME>`<br><br>`esr(config-ipv6-dhcp-server)# default-lease-time <TIME>` | <TIME> – максимальное время аренды IP-адреса, задаётся в формате DD:HH:MM, где:<br>• DD – количество дней, принимает значения [0..364];<br>• HH – количество часов, принимает значения [0..23];<br>• MM – количество минут, принимает значения [0..59]<br>Значение по умолчанию: 12 часов. |
| 12 | Создать идентификатор класса поставщика (DHCP Опция 60) (не обязательно). | `esr(config)# ip dhcp-server vendor-class-id <NAME>`<br><br>`esr(config)# ipv6 dhcp-server vendor-class-id <NAME>` | <NAME> – идентификатор класса поставщика, задаётся строкой до 31 символа. |
| 13 | Задать специфическую информацию поставщика (DHCP Опция 43). | `esr(config-dhcp-vendor-id)# vendor-specific-options <HEX>`<br><br>`esr(config-ipv6-dhcp-vendor-id)# vendor-specific-options <HEX>` | <HEX> – специфическая информация поставщика, задаётся в шестнадцатеричном формате до 128 символов. |
| 14 | Задать IP-адрес NetBIOS-сервера (DHCP опция 44) (не обязательно). | `esr(config-dhcp-server)# netbios-name-server <ADDR>` | <ADDR> – IP-адрес NetBIOS-сервера задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Можно задать до 4 IP-адресов. |
| 15 | Задать IP-адрес tftp-сервера (DHCPOption 150) (не обязательно). | `esr(config-dhcp-server)# tftp-server <ADDR>` | <ADDR> – IP-адрес DNS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |

### 10.1.2 Пример настройки

**Задача:**

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

**Решение:**

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

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

Создадим пул адресов с именем «Simple» и добавим в данный пул адресов диапазон IP-адресов для выдачи в аренду клиентам сервера. Укажем параметры подсети, к которой принадлежит данный пул, и время аренды для выдаваемых адресов:

```
esr# configure
esr(config)# ip dhcp-server pool Simple
esr(config-dhcp-server)# network 192.168.1.0/24
esr(config-dhcp-server)# address-range 192.168.1.100-192.168.1.125
esr(config-dhcp-server)# default-lease-time 1:00:00
```

Сконфигурируем передачу клиентам дополнительных сетевых параметров:

- маршрут по умолчанию: 192.168.1.1;
- имя домена: eltex.loc;
- список DNS-серверов: DNS1: 172.16.0.1, DNS2: 8.8.8.8.

```
esr(config-dhcp-server)# domain-name "eltex.loc"
esr(config-dhcp-server)# default-router 192.168.1.1
esr(config-dhcp-server)# dns-server 172.16.0.1 8.8.8.8
esr(config-dhcp-server)# exit
```

Для того чтобы DHCP-сервер мог раздавать IP-адреса из конфигурируемого пула, на маршрутизаторе должен быть создан IP-интерфейс, принадлежащий к той же подсети, что и адреса пула.

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# security-zone trusted
esr(config-if-gi)# ip address 192.168.1.1/24
esr(config-if-gi)# exit
```

Для разрешения прохождения сообщений протокола DHCP к серверу необходимо создать соответствующие профили портов, включающие порт источника 68 и порт назначения 67, используемые протоколом DHCP, и создать разрешающее правило в политике безопасности для прохождения пакетов протокола UDP:

```
esr(config)# object-group service dhcp_server
esr(config-object-group-service)# port-range 67
esr(config-object-group-service)# exit
esr(config)# object-group service dhcp_client
esr(config-object-group-service)# port-range 68
esr(config-object-group-service)# exit
esr(config)# security zone-pair trusted self
esr(config-zone-pair)# rule 30
esr(config-zone-rule)# match protocol udp
esr(config-zone-rule)# match source-port dhcp_client
esr(config-zone-rule)# match destination-port dhcp_server
esr(config-zone-rule)# action permit
esr(config-zone-rule)# enable
esr(config-zone-rule)# exit
esr(config-zone-pair)# exit
```

Разрешим работу сервера:

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

Просмотреть список арендованных адресов можно с помощью команды:

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

Просмотреть сконфигурированные пулы адресов можно командами:

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

⚠ Конфигурирование настроек для IPv6 производится по аналогии с IPv4.

## 10.2 Конфигурирование Destination NAT

Функция Destination NAT (DNAT) состоит в преобразовании IP-адреса назначения у пакетов, проходящих через сетевой шлюз.

DNAT используется для перенаправления трафика, идущего на некоторый «виртуальный» адрес в публичной сети, на «реальный» сервер в локальной сети, находящийся за сетевым шлюзом. Эту функцию можно использовать для организации публичного доступа к серверам, находящимся в частной сети и не имеющим публичного сетевого адреса.

### 10.2.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Перейти в режим настройки сервиса трансляции адресов получателя. | `esr(config)# nat destination` | |
| 2 | Создать пул IP-адресов и/или TCP/UDP-портов с определённым именем (не обязательно). | `esr(config-dnat)# pool <NAME>` | <NAME> – имя пула NAT-адресов, задаётся строкой до 31 символа. |
| 3 | Установить внутренний IP-адрес, на который будет заменяться IP-адрес получателя. | `esr(config-dnat-pool)# ip address <ADDR>` | <ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 4 | Установить внутренний TCP/UDP порт, на который будет заменяться TCP/UDP порт получателя. | `esr(config-dnat-pool)# ip port <PORT>` | <PORT> – TCP/UDP порт, принимает значения [1..65535]. |
| 5 | Создать группу правил с определённым именем. | `esr(config-dnat)# ruleset <NAME>` | <NAME> – имя группы правил, задаётся строкой до 31 символа. |
| 6 | Указать экземпляр VRF, в котором будет работать данная группа правил (не обязательно). | `esr(config-dnat-ruleset)# ip vrf forwarding <VRF>` | <VRF> – имя VRF, задается строкой до 31 символа. |
| 7 | Задать область применения группы правил. Правила будут применяться только для трафика, идущего из определенной зоны или интерфейса. | `esr(config-dnat-ruleset)# from { zone <NAME> \| interface <IF> \| tunnel <TUN> \| default }` | <NAME> – имя зоны изоляции;<br><br><IF> – имя интерфейса устройства;<br><br><TUN> – имя туннеля устройства;<br><br>default – обозначает группу правил для всего трафика, источник которого не попал под критерии других групп правил. |
| 8 | Задать правило с определённым номером. Правила обрабатываются в порядке возрастания. | `esr(config-dnat-ruleset)# rule <ORDER>` | <ORDER> – номер правила, принимает значения [1..10000]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 9 | Задать профиль IP-адресов {отправителя \| получателя}, для которых должно срабатывать правило. | `esr(config-dnat-rule)# match [not] {source\|destination}-address <OBJ-GROUP-NETWORK-NAME>` | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.<br><br>Значение «any» указывает на любой IP-адрес отправителя. |
| 10 | Задать профиль сервисов (tcp/udp-портов) {отправителя \| получателя}, для которых должно срабатывать правило (не обязательно). | `esr(config-dnat-rule)# match [not] {source\|destination}-port <PORT-SET-NAME>` | <PORT-SET-NAME> – имя профиля порта, задаётся строкой до 31 символа. Значение «any» указывает на любой TCP/UDP-порт отправителя. |
| 11 | Установить имя или номер IP-протокола, для которого должно срабатывать правило (не обязательно). | `esr(config-dnat-rule)# match [not] {protocol <TYPE> \| protocol-id <ID> }` | <TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre. Значение «any» указывает на любой тип протокола.<br><br><ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF]. |
| 12 | Задать тип и код сообщений протокола ICMP, для которых должно срабатывать правило (если в качестве протокола выбран ICMP) (не обязательно). | `esr(config-dnat-rule)# match [not] icmp {<ICMP_TYPE><ICMP_CODE> \| <TYPE-NAME>}` | <ICMP_TYPE> – тип сообщения протокола ICMP, принимает значения [0..255].<br><br><ICMP_CODE> – код сообщения протокола ICMP, принимает значения [0..255]. Значение «any» указывает на любой код сообщения.<br><br><TYPE-NAME> – имя типа ICMP сообщения. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 13 | Задать действие «трансляция адреса и порта получателя» для трафика, удовлетворяющего критериям, заданным командами «match». | `esr(config-dnat-rule)# action destination-nat { off \| pool <NAME> \| netmap <ADDR/LEN> }` | off – трансляция отключена;<br><br>pool <NAME> – имя пула, содержащего набор IP-адресов и/или TCP/UDP портов;<br><br>netmap <ADDR/LEN> – IP-адрес и маска подсети, используемые при трансляции. Параметр задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. |
| 14 | Активировать конфигурируемое правило. | `esr(config-dnat-rule)# enable` | |

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

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

Более подробная информация о командах для настройки маршрутизатора содержится в «Справочнике команд CLI».

### 10.2.2 Пример настройки Destination NAT

**Задача:**

Организовать доступ из публичной сети, относящейся к зоне «UNTRUST», к серверу локальной сети в зоне «TRUST». Адрес сервера в локальной сети – 10.1.1.100. Сервер должен быть доступным извне по адресу 1.2.3.4, доступный порт 80.

**Решение:**

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

```
esr# configure
esr(config)# security zone UNTRUST
esr(config-zone)# exit
esr(config)# security zone TRUST
esr(config-zone)# exit
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)#   security-zone TRUST
esr(config-if-gi)#   ip address 10.1.1.1/25
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)#   security-zone TRUST
esr(config-if-gi)#   ip address 10.1.1.1/25
esr(config-if-gi)# exit
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip address 1.2.3.4/29
esr(config-if-te)# security-zone UNTRUST
esr(config-if-te)# exit
```

Создадим профили IP-адресов и портов, которые потребуются для настройки правил Firewall и правил DNAT.

- NET_UPLINK – профиль адресов публичной сети;
- SERVER_IP – профиль адресов локальной сети;
- SRV_HTTP – профиль портов.

```
esr(config)# object-group network NET_UPLINK
esr(config-object-group-network)# ip address 1.2.3.4
esr(config-object-group-network)# exit
```

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

```
esr(config)# object-group network SERVER_IP
esr(config-object-group-network)# ip address 10.1.1.100
esr(config-object-group-network)# exit
```

Войдем в режим конфигурирования функции DNAT и создадим пул адресов и портов назначения, в которые будут транслироваться адреса пакетов, поступающие на адрес 1.2.3.4 из внешней сети.

```
esr(config)# nat destination
esr(config-dnat)# pool SERVER_POOL
esr(config-dnat-pool)# ip address 10.1.1.100
esr(config-dnat-pool)# ip port 80
esr(config-dnat-pool)# exit
```

Создадим набор правил «DNAT», в соответствии с которыми будет производиться трансляция адресов. В атрибутах набора укажем, что правила применяются только для пакетов, пришедших из зоны «UNTRUST». Набор правил включает в себя требования соответствия данных по адресу и порту назначения (match destination-address, match destination-port) и по протоколу. Кроме этого в наборе задано действие, применяемое к данным, удовлетворяющим всем правилам (action destination-nat). Набор правил вводится в действие командой «enable».

```
esr(config-dnat)# ruleset DNAT
esr(config-dnat-ruleset)# from zone UNTRUST
esr(config-dnat-ruleset)# rule 1
esr(config-dnat-rule)# match destination-address NET_UPLINK
esr(config-dnat-rule)# match protocol tcp
esr(config-dnat-rule)# match destination-port SRV_HTTP
esr(config-dnat-rule)# action destination-nat pool SERVER_POOL
esr(config-dnat-rule)# enable
esr(config-dnat-rule)# exit
esr(config-dnat-ruleset)# exit
esr(config-dnat)# exit
```

Для пропуска трафика, идущего из зоны «UNTRUST» в «TRUST», создадим соответствующую пару зон. Пропускать следует только трафик с адресом назначения, соответствующим заданному в профиле «SERVER_IP» и прошедший преобразование DNAT.

```
esr(config)# security zone-pair UNTRUST TRUST
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# match destination-address SERVER_IP
esr(config-zone-pair-rule)# match destination-nat
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# exit
```

Произведенные настройки можно посмотреть с помощью команд:

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

## 10.3 Конфигурирование Source NAT

Функция Source NAT (SNAT) используется для подмены адреса источника у пакетов, проходящих через сетевой шлюз. При прохождении пакетов из локальной сети в публичную сеть, адрес источника заменяется на один из публичных адресов шлюза. Дополнительно к адресу источника может применяться замена порта источника. При прохождении пакетов из публичной сети в локальную происходит обратная подмена адреса и порта.

Функция SNAT может быть использована для предоставления доступа в Интернет компьютерам, находящимся в локальной сети. При этом не требуется назначения публичных IP-адресов этим компьютерам.

### 10.3.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Перейти в режим настройки сервиса трансляции адресов отправителя. | `esr(config)# nat source` | |
| 2 | Создать пул IP-адресов и/или TCP/UDP-портов с определённым именем (не обязательно). | `esr(config-snat)# pool <NAME>` | <NAME> – имя пула NAT-адресов, задаётся строкой до 31 символа. |
| 3 | Установить диапазон IP-адресов, для которых будет заменяться IP-адрес отправителя. | `esr(config-snat-pool)# ip address-range <IP>[-<ENDIP>]` | <IP> – IP-адрес начала диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];<br><br><ENDIP> – IP-адрес конца диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Если не указывать IP-адрес конца диапазона, то в качестве IP-адреса для трансляции используется только IP-адрес начала диапазона. |
| 4 | Задать диапазон внешних TCP/UDP портов, на которые будет заменяться TCP/UDP порт отправителя. | `esr(config-snat-pool)# ip port-range <PORT>[-<ENDPORT>]` | <PORT> – TCP/UDP порт начала диапазона, принимает значения [1..65535];<br><br><ENDPORT> – TCP/UDP порт конца диапазона, принимает значения [1..65535]. Если не указывать TCP/UDP порт конца диапазона, то в качестве TCP/UDP порта для трансляции используется только TCP/UDP порт начала диапазона. |
| 5 | Установить внутренний TCP/UDP порт, на который будет заменяться TCP/UDP порт отправителя. | `esr(config-snat-pool)# ip port <PORT>` | <PORT> – TCP/UDP порт, принимает значения [1..65535]. |
| 6 | Включить функции NAT persistent. | `esr(config-snat-pool)# persistent` | |
| 7 | Создать группу правил с определённым именем. | `esr(config-snat)# ruleset <NAME>` | <NAME> – имя группы правил, задаётся строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 8 | Указать экземпляр VRF, в котором будет работать данная группа правил (не обязательно). | esr(config-snat-ruleset)# ip vrf forwarding <VRF> | <VRF> – имя VRF, задается строкой до 31 символа. |
| 9 | Задать область применения группы правил. Правила будут применяться только для трафика, идущего в определенную зону или интерфейс. | esr(config-snat-ruleset)# to { zone <NAME> \| interface <IF> tunnel <TUN> \| \| default } | <NAME> – имя зоны изоляции;<br><br><IF> – имя интерфейса устройства;<br><br><TUN> – имя туннеля устройства<br>default – обозначает группу правил для всего трафика, источник которого не попал под критерии других групп правил. |
| 10 | Задать правило с определённым номером. Правила обрабатываются в порядке возрастания. | esr(config-snat-ruleset)# rule <ORDER> | <ORDER> – номер правила, принимает значения [1..10000]. |
| 11 | Задать профиль IP-адресов {отправителя \| получателя}, для которых должно срабатывать правило. | esr(config-snat-rule)# match [not] {source\|destination}-address <OBJ-GROUP-NETWORK-NAME> | <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.<br><br>Значение «any» указывает на любой IP-адрес отправителя. |
| 12 | Задать профиль IP-адресов {отправителя \| получателя}, для которых должно срабатывать правило (не обязательно). | esr(config-snat-rule)# match [not] {source \| destination}-port <PORT-SET-NAME> | <PORT-SET-NAME> – имя профиля порта, задаётся строкой до 31 символа. Значение «any» указывает на любой TCP/UDP-порт отправителя. |
| 13 | Установить имя или номер IP-протокола, для которого должно срабатывать правило (не обязательно). | esr(config-snat-rule)# match [not] {protocol\|protocol-id} <TYPE> | <TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre. Значение «any» указывает на любой тип протокола;<br><br><ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 14 | Задать тип и код сообщений протокола ICMP, для которых должно срабатывать правило (не обязательно). | `esr(config-snat-rule)# match [not] icmp {<ICMP_TYPE><ICMP_CODE> \| <TYPE-NAME>}` | <ICMP_TYPE> – тип сообщения протокола ICMP, принимает значения [0..255];<br><br><ICMP_CODE> – код сообщения протокола ICMP, принимает значения [0..255]. Значение «any» указывает на любой код сообщения;<br><br><TYPE-NAME> – имя типа ICMP сообщения |
| 15 | Задать действие «трансляция адреса и порта отправителя» для трафика, удовлетворяющего критериям, заданным командами «match» | `esr(config-snat-rule)# action source-nat { off \| pool <NAME> \| netmap <ADDR/LEN> [static] \| interface [FIRST_PORT – LAST_PORT] }` | off – трансляция отключена;<br><br>pool<NAME> – имя пула, содержащего набор IP-адресов и/или TCP/UDP портов;<br><br>netmap <ADDR/LEN> – IP-адрес и маска подсети, используемые при трансляции; static – опция для организации статического NAT.<br><br>Параметр задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].<br><br>interface [FIRST_PORT – LAST_PORT] – задаёт трансляцию в IP-адрес интерфейса. Если дополнительно задан диапазон TCP/UDP-портов, то трансляция будет происходить только для TCP/UDP- портов отправителя, входящих в указанный диапазон. |
| 16 | Активировать конфигурируемое правило. | `esr(config-snat-rule)# enable` | |

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

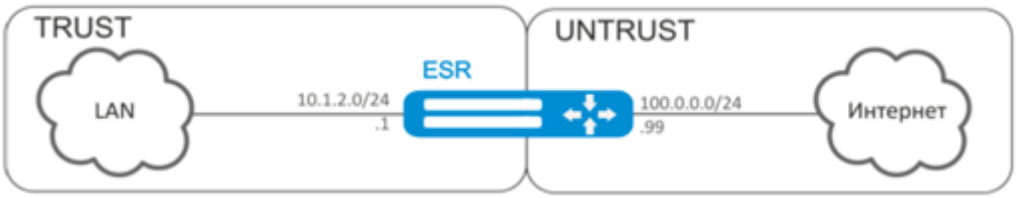
Каждая команда «match» может содержать ключ «not». При использовании данного ключа под правило будут подпадать пакеты, не удовлетворяющие заданному критерию.

Более подробная информация о командах для настройки маршрутизатора содержится в «Справочнике команд CLI».

### 10.3.2 Пример настройки 1

**Задача:**

Настроить доступ пользователей локальной сети 10.1.2.0/24 к публичной сети с использованием функции Source NAT. Задать диапазон адресов публичной сети для использования SNAT 100.0.0.100-100.0.0.249.




**Решение:**

Конфигурирование начнем с создания зон безопасности, настройки сетевых интерфейсов и определения их принадлежности к зонам безопасности. Создадим доверенную зону «TRUST» для локальной сети и зону «UNTRUST» для публичной сети.

```
esr# configure
esr(config)# security zone UNTRUST
esr(config-zone)# exit
esr(config)# security zone TRUST
esr(config-zone)# exit
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 10.1.2.1/24
esr(config-if-gi)# security-zone TRUST
esr(config-if-gi)# exit
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip address 100.0.0.99/24
esr(config-if-te)# security-zone UNTRUST
esr(config-if-te)# exit
```

Для конфигурирования функции SNAT и настройки правил зон безопасности потребуется создать профиль адресов локальной сети «LOCAL_NET», включающий адреса, которым разрешен выход в публичную сеть, и профиль адресов публичной сети «PUBLIC_POOL».

```
esr(config)# object-group network LOCAL_NET
esr(config-object-group-network)# ip address-range 10.1.2.2-10.1.2.254
esr(config-object-group-network)# exit
esr(config)# object-group network PUBLIC_POOL
esr(config-object-group-network)# ip address-range 100.0.0.100-100.0.0.249
esr(config-object-group-network)# exit
```

Для пропуска трафика из зоны «TRUST» в зону «UNTRUST» создадим пару зон и добавим правила, разрешающие проходить трафику в этом направлении. Дополнительно включена проверка адреса источника данных на принадлежность к диапазону адресов «LOCAL_NET» для соблюдения ограничения на выход в публичную сеть. Действие правил разрешается командой *enable*.

```
esr(config)# security zone-pair TRUST UNTRUST
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# match source-address LOCAL_NET
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
```

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

```
esr(config)# nat source
esr(config-snat)# pool TRANSLATE_ADDRESS
esr(config-snat-pool)# ip address-range 100.0.0.100-100.0.0.249
esr(config-snat-pool)# exit
```

Вторым шагом создаётся набор правил SNAT. В атрибутах набора укажем, что правила применяются только для пакетов, направляющихся в публичную сеть – в зону «UNTRUST». Правила включают проверку адреса источника данных на принадлежность к пулу «LOCAL_NET».

```
esr(config-snat)# ruleset SNAT
esr(config-snat-ruleset)# to zone UNTRUST
esr(config-snat-ruleset)# rule 1
esr(config-snat-rule)# match source-address LOCAL_NET
esr(config-snat-rule)# action source-nat pool TRANSLATE_ADDRESS
esr(config-snat-rule)# enable
esr(config-snat-rule)# exit
esr(config-snat-ruleset)# exit
```

Для того чтобы маршрутизатор отвечал на запросы протокола ARP для адресов, входящих в публичный пул, необходимо запустить сервис ARP Proxy. Сервис ARP Proxy настраивается на интерфейсе, которому принадлежит IP-адрес из подсети профиля адресов публичной сети «PUBLIC_POOL».

```
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip nat proxy-arp PUBLIC_POOL
```

Для того чтобы устройства локальной сети могли получить доступ к публичной сети, на них должна быть настроена маршрутизация – адрес 10.1.2.1 должен быть назначен адресом шлюза.

На самом маршрутизаторе также должен быть создан маршрут для направления на публичную сеть. Этот маршрут может быть назначен маршрутом по умолчанию с помощью следующей команды.

```
esr(config)# ip route 0.0.0.0/0 100.0.0.1
esr(config)# exit
```

### 10.3.3 Пример настройки 2

**Задача:**

Настроить доступ пользователей локальной сети 21.12.2.0/24 к публичной сети с использованием функции Source NAT без использования межсетевого экрана (firewall). Диапазон адресов публичной сети для использования SNAT 200.10.0.100-200.10.0.249.


**Решение:**

Конфигурирование начнем с настройки сетевых интерфейсов и отключения межсетевого:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 21.12.2.1/24
esr(config-if-gi)# ip firewall disable
esr(config-if-gi)# exit
```

```
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip address 200.10.0.1/24
esr(config-if-te)# ip firewall disable
esr(config-if-te)# exit
```

Для конфигурирования функции SNAT потребуется создать профиль адресов локальной сети «LOCAL_NET», включающий адреса, которым разрешен выход в публичную сеть, и профиль адресов публичной сети «PUBLIC_POOL»:

```
esr(config)# object-group network LOCAL_NET
esr(config-object-group-network)# ip address-range 21.12.2.2-21.12.2.254
esr(config-object-group-network)# exit

esr(config)# object-group network PUBLIC_POOL
esr(config-object-group-network)# ip address-range 200.10.0.100-200.10.0.249
esr(config-object-group-network)# exit
```

Конфигурируем сервис SNAT.

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

```
esr(config)# nat source
esr(config-snat)# pool TRANSLATE_ADDRESS
esr(config-snat-pool)# ip address-range 200.10.0.100-200.10.0.249
esr(config-snat-pool)# exit
```

Вторым шагом создаётся набор правил SNAT. В атрибутах набора укажем, что правила применяются только для пакетов, направляющихся в публичную сеть через порт te1/0/1. Правила включают проверку адреса источника данных на принадлежность к пулу «LOCAL_NET»:

```
esr(config-snat)# ruleset SNAT
esr(config-snat-ruleset)# to interface te1/0/1
esr(config-snat-ruleset)# rule 1
esr(config-snat-rule)# match source-address LOCAL_NET
esr(config-snat-rule)# action source-nat pool TRANSLATE_ADDRESS
esr(config-snat-rule)# enable
esr(config-snat-rule)# exit
esr(config-snat-ruleset)# exit
```

Для того чтобы маршрутизатор отвечал на запросы протокола ARP для адресов, входящих в публичный пул, необходимо запустить сервис ARP Proxy. Сервис ARP Proxy настраивается на интерфейсе, которому принадлежит IP-адрес из подсети профиля адресов публичной сети «PUBLIC_POOL»:

```
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip nat proxy-arp PUBLIC_POOL
```

Для того чтобы устройства локальной сети могли получить доступ к публичной сети, на них должна быть настроена маршрутизация – адрес 21.12.2.1 должен быть назначен адресом шлюза.

На самом маршрутизаторе также должен быть создан маршрут для направления на публичную сеть. Этот маршрут может быть назначен маршрутом по умолчанию с помощью следующей команды:

```
esr(config)# ip route 0.0.0.0/0 200.10.0.254
esr(config)# exit
```

## 10.4 Конфигурирование Static NAT

Static NAT — статический NAT задает однозначное соответствие одного адреса другому. Иными словами, при прохождении через маршрутизатор, адрес меняется на другой строго заданный адрес, один-к-одному. Запись о такой трансляции хранится неограниченно долго, пока не будет произведена перенастройка NAT на маршрутизаторе.

### 10.4.1 Алгоритм настройки

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

### 10.4.2 Пример настройки Static NAT

**Задача:**

Настроить двухстороннюю и постоянную трансляцию из локальной сети для диапазона адресов 21.12.2.100-21.12.2.150 в публичную сеть 200.10.0.0/24. Диапазон адресов публичной сети для использования трансляции – 200.10.0.100-200.10.0.150.


**Решение:**

Начнем конфигурирование с настройки сетевых интерфейсов и отключения межсетевого экрана:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 21.12.2.1/24
esr(config-if-gi)# ip firewall disable
esr(config-if-gi)# exit
```

```
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip address 200.10.0.1/24
esr(config-if-te)# ip firewall disable
esr(config-if-te)# exit
```

Для конфигурирования Static NAT потребуется создать профиль адресов локальной сети «LOCAL_NET», включающий локальную подсеть, и профиль адресов публичной сети «PUBLIC_POOL»:

```
esr(config)# object-group network LOCAL_NET
esr(config-object-group-network)# ip prefix 21.12.2.0/24
esr(config-object-group-network)# exit
```

```
esr(config)# object-group network PUBLIC_POOL
esr(config-object-group-network)# ip prefix 200.10.0.0/24
esr(config-object-group-network)# exit
```

Диапазон адресов публичной сети для использования Static NAT задаем в профиле «PROXY»:

```
esr(config)# object-group network PROXY
esr(config-object-group-network)# ip address-range 200.10.0.100-200.10.0.150
esr(config-object-group-network)# exit
```

Конфигурируем сервис Static NAT в режиме конфигурирования SNAT. В атрибутах набора укажем, что правила применяются только для пакетов, направляющихся в публичную сеть через порт te1/0/1. Правила включают проверку адреса источника данных на принадлежность к пулу «LOCAL_NET» и проверку адресов назначения на принадлежность к пулу «PUBLIC_POOL».

```
esr(config)# nat source
esr(config-snat)# ruleset SNAT
esr(config-snat-ruleset)# to interface te1/0/1
esr(config-snat-ruleset)# rule 1
esr(config-snat-rule)# match source-address LOCAL_NET
esr(config-snat-rule)# match destination-address PUBLIC_POOL
esr(config-snat-rule)# action source-nat netmap 200.10.0.0/24 static
esr(config-snat-rule)# enable
esr(config-snat-rule)# exit
esr(config-snat-ruleset)# exit
```

Для того чтобы маршрутизатор отвечал на запросы протокола ARP для адресов, входящих в пул трансляции «PROXY», необходимо запустить сервис ARP Proxy. Сервис ARP Proxy настраивается на интерфейсе, которому принадлежит IP-адрес из подсети профиля адресов «PROXY».

```
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip nat proxy-arp PROXY
```

Для того чтобы устройства локальной сети могли получить доступ к сети 200.10.0.0/24, на них должна быть настроена маршрутизация – адрес 21.12.2.1 должен быть назначен адресом шлюза.

Изменения конфигурации вступают в действие по команде применения.

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

Посмотреть активные трансляции можно с помощью команды:

```
esr# show ip nat translations
```

## 10.5 Проксирование HTTP/HTTPS-трафика

### 10.5.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Создать объект с URL | `esr(config)# object-group url <NAME>` | |
| 2 | Указать набор | `esr(config-object-group-url)# url <URL>` | <URL> – адрес веб страницы, сайта. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 3 | Создать профиль проксирования | `esr(config)# ip http profile <NAME>` | <NAME> – название профиля. |
| 4 | Выбрать действие по умолчанию | `esr(config-profile)# default action {deny\|permit\|redirect} [redirect-url <URL>]` | <URL> – адрес хоста, на который будут передаваться запросы. |
| 5 | Указать описание (не обязательно) | `esr(config-profile)# description <description>` | <description> – до 255 символов. |
| 6 | Указать удаленный или локальный список URL и тип операции (блокировка/ пропуск трафика/ перенаправление) (не обязательно) | `esr(config-profile)# urls {local\|remote} <URL_OBJ_GROUP_NAME> action {deny\|permit\|redirect} [redirect-url <URL>]` | <URL_OBJ_GROUP_NAME> – указать название объекта, содержащего набор URL. |
| 7 | Указать удаленный сервер, где лежат необходимые списки URL (не обязательно) | `esr(config)# ip http proxy server-url <URL>` | <URL> – адрес сервера, откуда будут брать удалённые списки url. |
| 8 | Указать прослушиваемый порт для проксирования (не обязательно) | `esr(config)# ip http proxy listen-ports <OBJ_GROUP_NAME>` | <OBJ_GROUP_NAME> – имя профиля порта, задаётся строкой до 31 символа. |
| 9 | Указать прослушиваемый порт для проксирования (не обязательно) | `esr(config)# ip https proxy listen-ports <OBJ_GROUP_NAME>` | <OBJ_GROUP_NAME> – имя профиля порта, задаётся строкой до 31 символа. |
| 10 | Указать базовый порт для проксирования (не обязательно) | `esr(config)# ip https proxy redirect-port <PORT>` | <PORT> – номер порта, указывается в диапазоне [1..65535].<br><br>Значение по умолчанию 3128 |
| 11 | Включить проксирование на интерфейсе на основе выбранного HTTP-профиля | `esr(config-if)# ip http proxy <PROFILE_NAME>` | <PROFILE_NAME> – название профиля |
| 12 | Включить проксирование на интерфейсе на основе выбранного HTTPS-профиля | `esr(config-if)# ip https proxy <PROFILE_NAME>` | <PROFILE_NAME> – название профиля |
| 13 | Создать списки сервисов, которые будут использоваться при фильтрации. | `esr(config)# object-group service <obj-group-name>` | <obj-group-name> – имя профиля сервисов, задается строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 14 | Задать описание списка сервисов (не обязательно). | `esr(config-object-group-service)# description <description>` | <description> – описание профиля, задается строкой до 255 символов. |
| 15 | Внести необходимые сервисы (tcp/udp порты) в список. | `esr(config-object-group-service)# port-range 3128-3135` | Прокси-сервер ESR использует для своей работы порты начиная с базового порта определённого на 10 шаге<br><br>Для http proxy используются порты начиная с базового порта по базовый порт + количество cpu данной модели ESR - 1<br><br>Для https proxy используются порты начиная с базового порта + количество cpu данной модели ESR по базовый порт + количество cpu данной модели ESR * 2 - 1 |
| 16 | Создать набор правил межзонового взаимодействия. | `esr(config)# security zone-pair <src-zone-name1> self` | <src-zone-name> – зона безопасности, в которой находятся интерфейсы с функцией ip http proxy или ip https proxy.<br><br>self – предопределенная зона безопасности для трафика, поступающего на сам ESR. |
| 17 | Создать правило межзонового взаимодействия. | `esr(config-zone-pair)# rule <rule-number>` | <rule-number> – 1..10000. |
| 18 | Задать описание правила (не обязательно). | `esr(config-zone-rule)# description <description>` | <description> – до 255 символов. |
| 19 | Указать действие данного правила. | `esr(config-zone-rule)# action <action> [ log ]` | <action> – permit<br><br>log – ключ для активации логирования сессий, которые устанавливаются согласно данному правилу. |
| 20 | Установить имя IP-протокола, для которого должно срабатывать правило | `esr(config-zone-rule)# match protocol <protocol-type>` | <protocol-type> – tcp<br><br>Прокси-сервер ESR работает по протоколу ESR. |

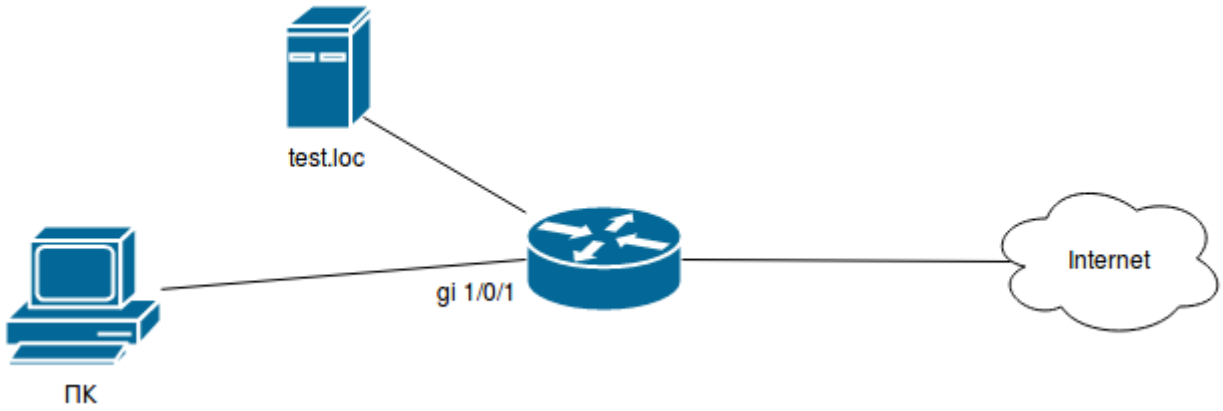
| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 21 | Установить профиль TCP/UDP-портов получателя, для которых должно срабатывать правило (если указан протокол). | `esr(config-zone-rule)# match [not] destination-port <obj-group-name>` | <obj-group-name> – имя профиля сервисов, созданного на шаге №12 |
| 22 | Включить правило межзонового взаимодействия. | `esr(config-zone-rule)# enable` | |

⚠ Если функция Firewall на ESR принудительно не отключена, необходимо создать разрешающее правило для зоны Self.

### 10.5.2 Пример настройки HTTP-прокси

**Задача:**

Организовать фильтрацию по URL для ряда адресов посредством прокси.




**Решение:**

Создадим набор URL, по которым будет осуществляться фильтрация. Настроим прокси-фильтр и укажем действия для созданного набора URL:

```
esr# configure
esr(config)# object-group url test1
esr(config-object-group-url)# url http://speedtest.net/
esr(config-object-group-url)# url http://www.speedtest.net/
esr(config-object-group-url)# url https://speedtest.net/
esr(config-object-group-url)# url https://www.speedtest.net/
esr(config-object-group-url)# exit
```

Создаем профиль:

```
esr(config)# ip http profile list1
esr(config-profile)# default action permit
esr(config-profile)# urls local test1 action redirect redirect-url http://test.loc
esr(config-profile)# exit
```

Включим проксирование на интерфейсе по профилю ‘list’:

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

Если используется Firewall, создадим для него разрешающие правила:

Допустим мы используем модель ESR-20 у которой 4 CPU.

Для http proxy нам надо открыть порты с 3128 по 3131

Для https proxy нам надо открыть порты с 3132 по 3135

Создаем профиль портов Прокси-сервера:

```
esr(config)# object-group service proxy
esr(config-object-group-service)# port-range 3128-3135
esr(config-object-group-service)# exit
```

Создаем разрешающее правило межзонового взаимодействия:

```
esr(config)# security zone-pair LAN self
esr(config-zone-pair)# rule 50
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol tcp
esr(config-zone-pair-rule)# match destination-port proxy
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
```

# 11 Мониторинг



## 11.1 Настройка Netflow

Netflow — сетевой протокол, предназначенный для учета и анализа трафика. Netflow позволяет передавать данные о трафике (адрес отправителя и получателя, порт, количество информации и др.) с сетевого оборудования (сенсора) на коллектор. В качестве коллектора может использоваться обычный сервер.

### 11.1.1 Алгоритм настройки

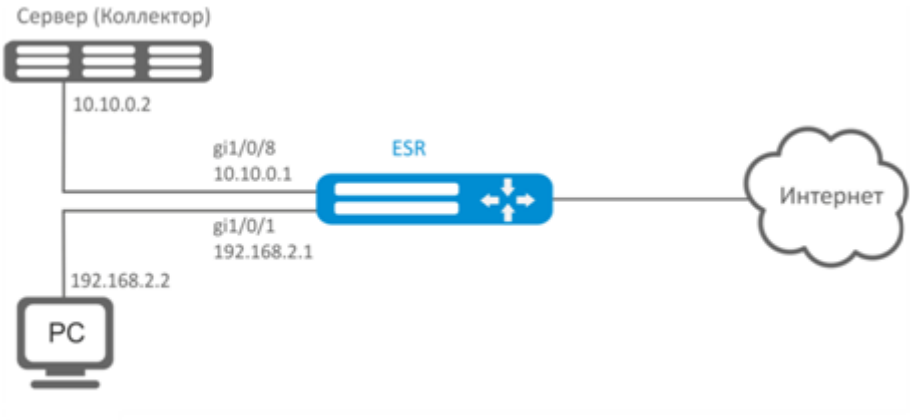
| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Задать версию Netflow-протокола. | `esr(config)# netflow version <VERSION>` | <VERSION> – версия Netflow-протокола: 5, 9 и 10. |
| 2 | Установить максимальное количество наблюдаемых сессий. | `esr(config)# netflow max-flows <COUNT>` | <COUNT> – количество наблюдаемых сессий, принимает значение [10000..2000000].<br><br>Значение по умолчанию: 512000. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 3 | Установить интервал, по истечении которого информация об устаревших сессиях экспортируются на коллектор. | `esr(config)# netflow inactive-timeout <TIMEOUT>` | <TIMEOUT> – задержка перед отправкой информации об устаревших сессиях, задается в секундах, принимает значение [0..240].<br><br>Значение по умолчанию: 15 секунд. |
| 4 | Установить частоту отправки статистики на Netflow-коллектор. | `esr(config)# netflow refresh-rate <RATE>` | <RATE> – частота отправки статистики, задается в пакетах на поток, принимает значение [1..10000].<br><br>Значение по умолчанию: 10. |
| 5 | Активировать Netflow на маршрутизаторе. | `esr(config)# netflow enable` | |
| 6 | Создать коллектор Netflow и перейти в режим его конфигурирования. | `esr(config)# netflow collector <ADDR>` | <ADDR> – IP-адрес коллектора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 7 | Установить порт Netflow-сервиса на сервере сбора статистики. | `esr(config-netflow-host)# port <PORT>` | <PORT> – номер UDP-порта, указывается в диапазоне [1..65535].<br><br>Значение по умолчанию: 2055. |
| 8 | Включить отправку статистики на Netflow-сервер в режим конфигурирования интерфейса/ туннеля/ сетевого моста. | `esr(config-if-gi)# ip netflow export` | |

### 11.1.2 Пример настройки

**Задача:**

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




**Решение:**

1 Предварительно необходимо выполнить следующие действия:

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

2 Основной этап конфигурирования:

Укажем IP-адрес коллектора:

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

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

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

Активируем netflow на маршрутизаторе:

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

Для просмотра статистики Netflow используется команда:

```
esr# show netflow statistics
```

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

## 11.2 Настройка sFlow

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

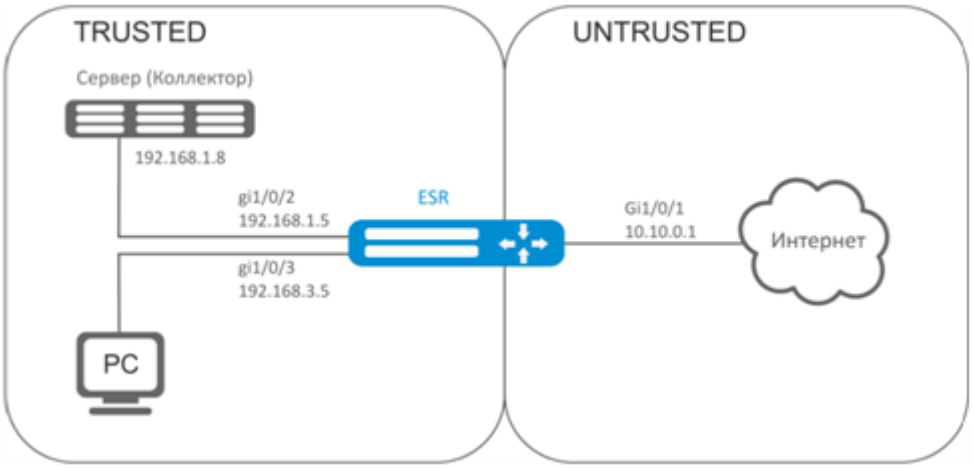
### 11.2.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Установить частоту отправки пакетов пользовательского трафика в неизменном виде на sFlow-коллектор. | `esr(config)# sflow sampling-rate <RATE>` | <RATE> – частота отправки пакетов пользовательского трафика на коллектор, принимает значение [1..10000000]. При значении частоты 10 на коллектор будет отправлен один пакет из десяти.<br><br>Значение по умолчанию: 1000. |
| 2 | Установить интервал, по истечении которого происходит получение информации о счетчиках сетевого интерфейса | `esr(config)# sflow poll-interval <TIMEOUT>` | <TIMEOUT> – интервал, по истечении которого происходит получение информации о счетчиках сетевого интерфейса, принимает значение [1..10000].<br><br>Значение по умолчанию: 10 секунд. |
| 3 | Активировать sFlow на маршрутизаторе. | `esr(config)# sflow enable` | |
| 4 | Создать коллектор sFlow и перейти в режим его конфигурирования. | `esr(config)# sflow collector <ADDR>` | <ADDR> – IP-адрес коллектора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 5 | Включить отправку статистики на sFlow-сервер в режим конфигурирования интерфейса/ туннеля/ сетевого моста. | `esr(config-if-gi)# ip sflow export` | |

### 11.2.2 Пример настройки

**Задача:**

Организовать учет трафика между зонами trusted и untrusted.




**Решение:**

Для сетей ESR создадим две зоны безопасности:

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

Настроим сетевые интерфейсы и определим их принадлежность к зонам безопасности:

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

Укажем IP-адрес коллектора:

```
esr(config)# sflow collector 192.168.1.8
```

Включим экспорт статистики по протоколу sFlow для любого трафика в правиле «rule1» для направления TRUSTED-UNTRUSTED:

```
esr(config)# security zone-pair TRUSTED UNTRUSTED
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action sflow-sample
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
```

Активируем sFlow на маршрутизаторе:

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

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

## 11.3 Настройка SNMP

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

### 11.3.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Включить SNMP-сервер | `esr(config)# snmp-server` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 2 | Определить community для доступа по протоколу SNMPv2c. | `esr(config)# snmp-server community <COMMUNITY> [ <TYPE> ] [ { <IP-ADDR> \| <IPV6-ADDR> } ] [ client-list <OBJ-GROUP-NETWORK-NAME> ] [ <VERSION> ] [ view <VIEW-NAME> ] [ vrf <VRF> ]` | <COMMUNITY> – сообщество для доступа по протоколу SNMP;<br><br><TYPE> – уровень доступа:<br>• **ro** – доступ только для чтения;<br>• **rw** – доступ для чтения и записи.<br><IP-ADDR> – IP-адрес клиента, которому предоставлен доступ, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];<br><IPV6-ADDR> – IPv6-адрес клиента, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];<br><br><OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, от которых обрабатываются snmp-запросы, задаётся строкой до 31 символа;<br><br><VERSION> – версия snmp, поддерживаемая данным community, принимает значения v1 или v2c;<br><br><VIEW-NAME> – имя профиля SNMP view, задаётся строкой до 31 символа;<br><VRF> – имя экземпляра VRF, из которого будет разрешен доступ, задается строкой до 31 символа. |
| 3 | Устанавливает значение переменной SNMP, содержащей контактную информацию | `esr(config)# snmp-server contact <CONTACT>` | <CONTACT> – контактная информация, задается строкой до 255 символов. |
| 4 | Установить значение кода DSCP для использования в IP-заголовке исходящих пакетов SNMP-сервера (не обязательно). | `esr(config)# snmp-server dscp <DSCP>` | <DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].<br><br>Значение по умолчанию: 63. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 5 | Разрешить перезагрузку маршрутизатора при помощи snmp-сообщений (не обязательно) | `esr(config)# snmp-server system-shutdown` | |
| 6 | Создать SNMPv3-пользователь. | `esr(config)# snmp-server user <NAME>` | <NAME> – имя пользователя, задаётся строкой до 31 символа. |
| 7 | Устанавливает значение переменной SNMP, содержащей информацию о расположении оборудования | `esr(config)# snmp-server location <LOCATION>` | <LOCATION> –информация о расположении оборудования, задается строкой до 255 символов. |
| 8 | Определить уровень доступа пользователя по протоколу SNMPv3. | `esr(config-snmp-user)# access <TYPE>` | <TYPE> – уровень доступа:<br>• **ro** – доступ только для чтения;<br>• **rw** – доступ для чтения и записи. |
| 9 | Определить режим безопасности пользователя по протоколу SNMPv3. | `esr(config-snmp-user)# authentication access <TYPE>` | <TYPE> – режим безопасности:<br>• **auth** – используется только аутентификация;<br>• **priv** – используется аутентификация и шифрование данных. |
| 10 | Определить алгоритм аутентификации SNMPv3-запросов. | `esr(config-snmp-user)# authentication algorithm <ALGORITHM>` | <ALGORITHM> – алгоритм шифрования:<br>• **md 5** – пароль шифруется по алгоритму md5;<br>• **sha 1** – пароль шифруется по алгоритму sha1. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 11 | Установить пароль для аутентификации SNMPv3-запросов. | `esr(config-snmp-user)# authentication key ascii-text { <CLEAR-TEXT> \| encrypted <ENCRYPTED-TEXT> }` | <CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов;<br>• **encrypted** – при указании команды задается зашифрованный пароль:<br><ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...). |
| 12 | Активировать фильтрацию и установить профиль IP-адресов, с которых могут приниматься SNMPv3 пакеты с данным именем SNMPv3 пользователя. | `esr(config-snmp-user)# client-list <NAME>` | <NAME> – имя ранее сознанной object-group, задается строкой до 31 символа. |
| 13 | Активировать фильтрацию и установить IPv4/IPv6-адрес, которому предоставлен доступ к маршрутизатору под данным SNMPv3-пользователем. | `esr(config-snmp-user)# ip address <ADDR>` | <ADDR> – IP-адрес клиента, которому предоставлен доступ, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| | | `esr(config-snmp-user)# ipv6 address <ADDR>` | <IPV6-ADDR> – IPv6-адрес клиента, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. |
| 14 | Активировать SNMPv3-пользователя. | `esr(config-snmp-user)# enable` | Значение по умолчанию: процесс выключен. |
| 15 | Определить алгоритм шифрования передаваемых данных. | `esr(config-snmp-user)# privacy algorithm <ALGORITHM>` | <ALGORITHM> – алгоритм шифрования:<br>• **aes 128** – использовать алгоритм шифрования AES-128;<br>• **des** – использовать алгоритм шифрования DES. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 16 | Установить пароль для шифрования передаваемых данных. | `esr(config-snmp-user)# privacy key ascii-text { <CLEAR-TEXT> \| encrypted <ENCRYPTED-TEXT> }` | <CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов;<br><br><ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...). |
| | Установить профиль snmp view, позволяющий разрешать или запрещать доступ к тем или иным OID для user. | `esr(config-snmp-user)# view <VIEW-NAME>` | <VIEW-NAME> – имя SNMP view профиля, на основании которого обеспечивается доступ к OID, задается строкой до 31 символа. |
| 17 | Включить передачу SNMP уведомлений на указанный IP-адрес и перейти в режим настройки SNMP уведомлений. | `esr(config)# snmp-server host { <IP-ADDR> \| <IPV6-ADDR> } [vrf <VRF>]` | <IP-ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].<br><br><IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];<br><br><VRF> – имя экземпляра VRF, в котором находится коллектор SNMP-уведомлений, задается строкой до 31 символа. |
| 18 | Определить порт коллектора SNMP уведомлений на удаленном сервере (не обязательно). | `esr(config-snmp-host)# port <PORT>` | <PORT> – номер UDP-порта, указывается в диапазоне [1..65535].<br><br>Значение по умолчанию: 162. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 19 | Установить фильтрацию на отправляемые SNMP-уведомления. | `esr(config)# snmp-server enable traps <TYPE>` | <TYPE> – тип фильтруемых сообщений. Может принимать значения:<br><br>config, entry, entry-sensor, environment, envmon, files-operations, flash, flash-operations, interfaces, links, ports, screens, snmp, syslog.<br><br>Дополнительные параметры зависят от типа фильтра. См. ESR-Series. Справочник команд CLI. |
| 20 | Создать профиль snmp view, позволяющий разрешать или запрещать доступ к тем или иным OID для community (SNMPv2) и user (SNMPv3). | `esr(config)# snmp-server enable traps <TYPE>` | <VIEW-NAME> – имя профиля SNMP view, задаётся строкой до 31 символа. |

### 11.3.2 Пример настройки

**Задача:**

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


**Решение:**

Предварительно нужно выполнить следующие действия:

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

Основной этап конфигурирования:

Включаем SNMP-сервер:

```
esr(config)# snmp-server
```

Создаем пользователя SNMPv3:

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

Определим режим безопасности:

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

Определим алгоритм аутентификации для SNMPv3-запросов:

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

Установим пароль для аутентификации SNMPv3-запросов:

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

Определим алгоритм шифрования передаваемых данных:

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

Установим пароль для шифрования передаваемых данных:

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

Активируем SNMPv3-пользователя:

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

Определяем сервер-приемник Trap-PDU сообщений:

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

## 11.4 Настройка Zabbix-agent/proxy

Zabbix-agent – агент, предназначенный для мониторинга устройства, а также выполнения удаленных команд с Zabbix сервера. Агент может работать в двух режимах: пассивный и активный. Для работы в пассивном режиме, по умолчанию, необходимо разрешающее правило в firewall – протокол tcp, порт 10050. Для активного режима – протокол tcp, порт 10051.

Zabbix-прокси - это процесс, способный собирать данные мониторинга с одного или нескольких наблюдаемых устройств и отправлять эту информацию Zabbix-серверу.

### 11.4.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Перейти в контекст настройки агента/proxy. | `esr(config)# zabbix-agent`<br>`esr(config)# zabbix-proxy` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 2 | Указать имя узла сети (опционально).<br><br>Для активного режима имя должно совпадать с именем узла сети на zabbix сервере. | `esr(config-zabbix)# hostname <WORD>`<br><br>`esr(config-zabbix-proxy)# hostname <WORD>` | <WORD> – имя узла сети, задается строкой до 255 символов. |
| 3 | Указать адрес zabbix сервера. | `esr(config-zabbix)# server <ADDR>`<br><br>`esr(config-zabbix-proxy)# server <ADDR>` | <ADDR> – IP-адрес сервера, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 4 | Указать адрес сервера для активных проверок (при использовании активного режима). | `esr(config-zabbix)# active-server <ADDR> <PORT>`<br><br>`esr(config-zabbix-proxy)# active-server <ADDR> <PORT>` | <ADDR> – IP-адрес сервера, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].<br><br><PORT> – Порт сервера, задается в диапазоне [1..65535].<br>Значение по умолчанию 10051. |
| 5 | Указать порт, который будет слушать агент/прокси (не обязательно) | `esr(config-zabbix)# port <PORT>`<br><br>`esr(config-zabbix-proxy)# port <PORT>` | <PORT> – Порт, который слушает zabbix агент/прокси, задается в диапазоне [1..65535].<br>Значение по умолчанию: 10050. |
| 6 | Разрешить выполнение удаленных команд zabbix агентом/прокси (при использовании активного режима). | `esr(config-zabbix)# remote-commands`<br><br>`esr(config-zabbix-proxy)# remote-commands` | |
| 7 | Указать адрес, с которого будет осуществляться взаимодействием с сервером (не обязательно). | `esr(config-zabbix)# source-address <ADDR>`<br><br>`esr(config-zabbix-proxy)# source-address <ADDR>` | <ADDR> – IP-адрес сервера, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].<br>Значение по умолчанию: ближайший адрес по маршрутизации. |
| 8 | Указать время обработки удаленных команд (не обязательно). | `esr(config-zabbix)# timeout <TIME>`<br><br>`esr(config-zabbix-proxy)# timeout <TIME>` | <TIME> – время ожидания, определяется в секундах [1..30].<br>Значение по умолчанию 3.<br>Рекомендуется устанавливать максимальное значение, т.к. некоторые команды могут выполняться дольше значения по умолчанию.<br>Если за указанное время команда не будет выполнена, то обработка команды будет прекращена. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 9 | Включить функционал агента/ прокси | `esr(config-zabbix)# enable`<br>`esr(config-zabbix-proxy)# enable` | |
| 10 | Разрешить из соответствующей зоны безопасности firewall обращение к маршрутизатору (в зону self) по TCP портам 10050, 10051. См. раздел Конфигурирование Firewall | | |

### 11.4.2 Пример настройки zabbix-agent


**Задача:**

Настроить взаимодействие между агентом и сервером для выполнения удаленных команд с сервера.

**Решение:**

В контексте настройки агента укажем адрес zabbix сервера, и адрес с которого будет осуществляться взаимодействие с сервером:

```
esr(config-zabbix)# server 192.168.32.101
esr(config-zabbix)# source-address 192.168.39.170
```

Для активации активного режима  укажем hostname, active-server, а также включим выполнение удаленных команд.

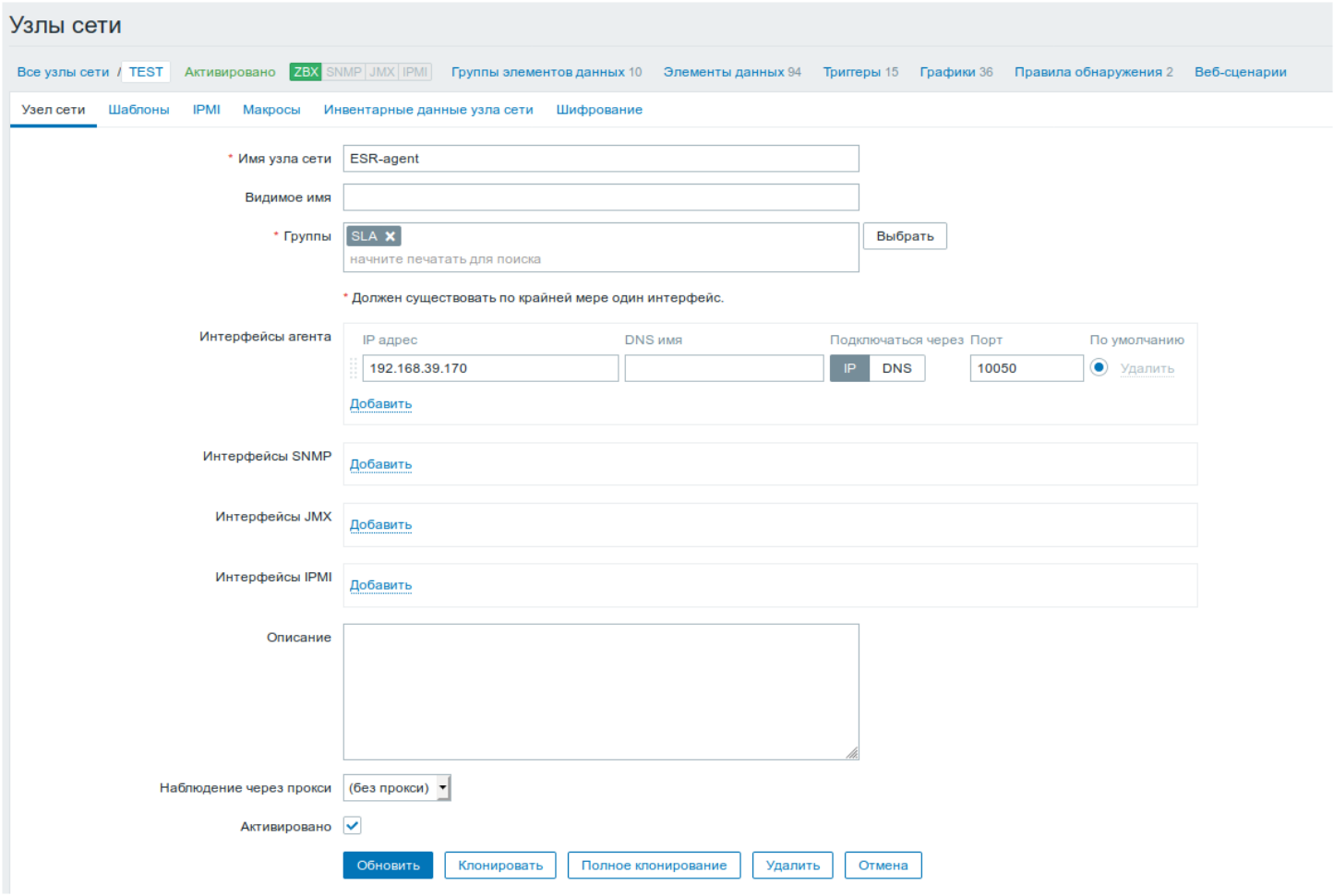
```
esr(config-zabbix)# hostname ESR-agent
esr(config-zabbix)# active-server 192.168.32.101
esr(config-zabbix)# remote-commands
```

Зададим время выполнения удаленных команд, и активируем функционал агента.

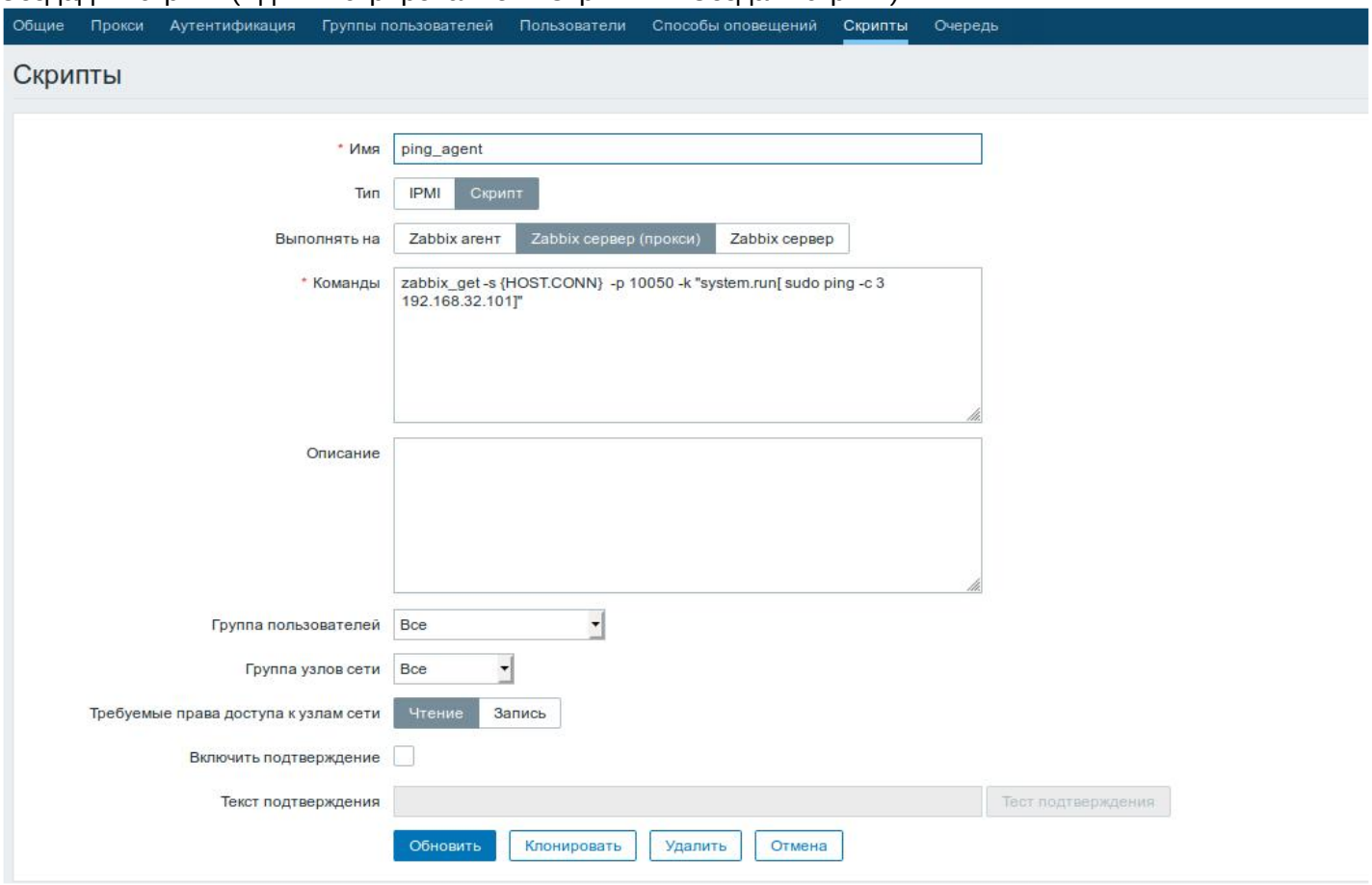
```
esr(config-zabbix)# timeout 30
esr(config-zabbix)# enable
```

### 11.4.3 Пример настройки zabbix-server

Создадим узел сети:



Создадим скрипт (Администрирование -> Скрипты-> Создать скрипт)




Маршрутизаторы ESR поддерживают выполнение следующих удаленных команд:

- **Ping:**

```
zabbix_get -s {HOST.CONN}  -p 10050 -k "system.run[ sudo ping -c 3 192.168.32.101]"
```

Клиент (ESR), получивший данную команду от сервера, выполнит ping до заданного узла (в нашем примере до 192.168.32.101), и вернет результат серверу.

Использование ключа "-c" с указанием количества пакетов в тесте - обязательно. Без данного ключа команда ping не остановится самостоятельно и тест не будет считаться завершенным.

- **Ping в VRF:**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[sudo  netns -exec -n backup sudo ping
192.168.32.101 -c 5 -W 2 ]"
```

Вышеупомянутая команда будет выполнена в заданном VRF с именем backup.

- **Fping**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[ sudo fping 192.168.32.101]"
```

Клиент (ESR), получивший данную команду от сервера, выполнит fping до заданного узла (в нашем примере до 192.168.32.101), и вернет результат серверу.

- **Fping в VRF**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[sudo  netns-exec -n backup sudo fping
192.168.32.101 ]"
```

- **Traceroute**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[ sudo traceroute 192.168.32.101]
```

Клиент (ESR), получивший данную команду от сервера, выполнит traceroute до заданного узла (в нашем примере до 192.168.32.101), и вернет результат серверу.

- **Traceroute в VRF**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[ sudo  netns-exec -n backup sudo
traceroute 192.168.32.179]"
```

- **Iperf**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[ sudo iperf -c 192.168.32.101 -u -b 100K
-i 1 -t 600]"
```

Клиент (ESR), получивший данную команду от сервера, выполнит iperf до заданного сервера (в нашем примере до 192.168.32.101), и вернет результат серверу.

- **Iperf в VRF**

```
zabbix_get -s {HOST.CONN} -p 10050 -k "system.run[ sudo  netns-exec -n backup  sudo iperf
-c 192.168.32.101 -u -b 100K -i 1 -t 600]"
```

- **Nslookup**

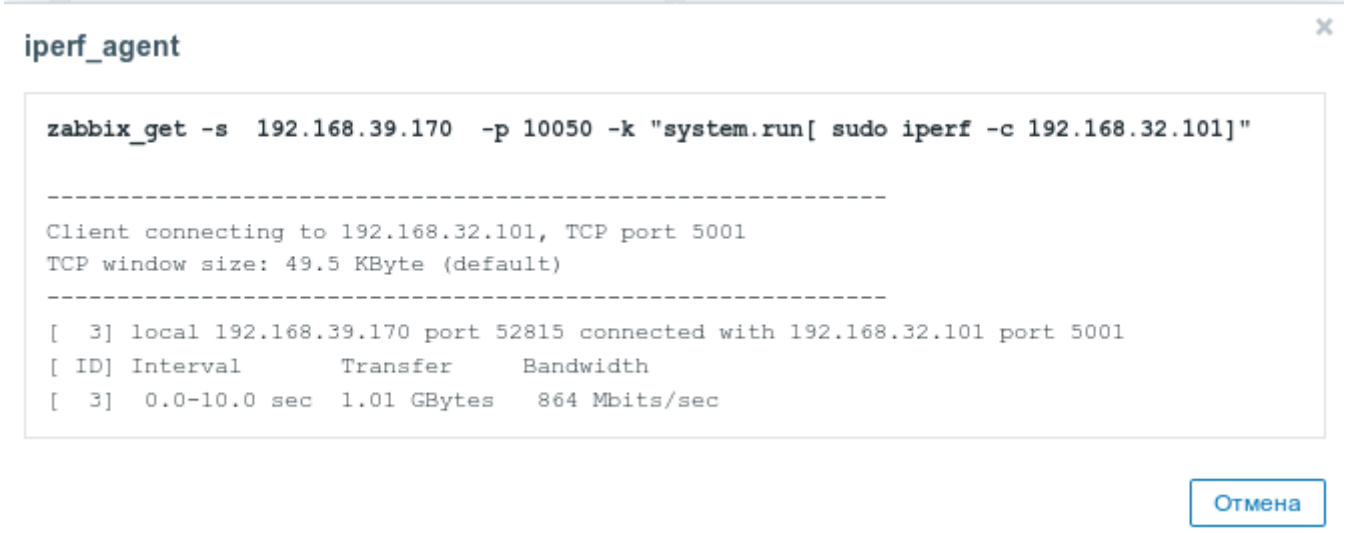
```
zabbix_get -s  {HOST.CONN} -p 10050 -k "system.run[sudo  nslookup ya.ru ]"
```

Клиент (ESR), получивший данную команду от сервера, выполнит nslookup , и вернет результат серверу.

- **Nslookup в VRF**

```
zabbix_get -s  {HOST.CONN} -p 10050 -k "system.run[sudo  netns-exec  sudo   nslookup
ya.ru ]"
```

Пример выполнения команды Iperf:




## 11.5 Настройка Syslog

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

### 11.5.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Установить уровень syslog-сообщений, которые будут отправляться на snmp-сервер в виде snmp-trap. | `esr(config)# syslog snmp <SEVERITY>` | <SEVERITY> – уровень важности сообщения, принимает значения (в порядке убывания важности):<br>• **emerg** – в системе произошла критическая ошибка, система неработоспособна;<br>• **alert** – сигналы тревоги, необходимо немедленное вмешательство персонала;<br>• **crit** – критическое состояние системы, сообщение о событии;<br>• **error** – сообщения об ошибках;<br>• **warning** – предупреждения, неаварийные сообщения;<br>• **notice** – сообщения о важных системных событиях;<br>• **info** – информационные сообщения системы;<br>• **debug** – отладочные сообщения, предоставляют пользователю информацию для корректной настройки системы;<br>• **none** – отключает вывод syslog-сообщений. |
| 2 | Задать уровень syslog-сообщений, которые будут отображаться при удаленных подключениях (Telnet, SSH) (не обязательно) | `esr(config)# syslog monitor <SEVERITY>` | |
| 3 | Включить процесс логирования введённых команд пользователя на локальный syslog-сервер (не обязательно) | `esr(config)# syslog cli-commands` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 4 | Включить сохранение сообщений syslog заданного уровня важности в указанный файл журнала | `esr(config)# syslog file <NAME> <SEVERITY>` | <NAME> – имя файла, в который будет производиться запись сообщений заданного уровня, задается строкой до 31 символа;<br><br><SEVERITY> описано в команде syslog snmp. |
| 5 | Указать максимальный размер файла журнала (не обязательно) | `esr(config)# syslog file-size <SIZE>` | <SIZE> – размер файла, принимает значение [10..10000000] кбайт |
| 6 | Задать максимальное количество файлов, сохраняемых при ротации (не обязательно) | `esr(config)# syslog max-files <NUM>` | <NUM> – максимальное количество файлов, принимает значения [1.. 1000] |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 7 | Включить передачу сообщений syslog заданного уровня важности на удаленный syslog-сервер | `esr(config)#syslog host <HOSTNAME> <ADDR> <SEVERITY> <TRANSPORT> <PORT>` | <HOSTNAME> – наименование syslog-сервера, задаётся строкой до 31 символа. Используется только для идентификации сервера при конфигурировании. Значение «all» используется в команде no syslog host для удаления всех syslog-серверов;<br><br><ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];<br><br><SEVERITY> – уровень важности сообщения, опциональный параметр, возможные значения приведены в разделе Пример настройки Syslog;<br><br><TRANSPORT> – протокол передачи данных, опциональный параметр, принимает значения:<br>• **TCP** – передача данных осуществляется по протоколу TCP;<br>• **UDP** – передача данных осуществляется по протоколу UDP;<br><PORT> – номер TCP/UDP-порта, опциональный параметр, принимает значения [1..65535], по умолчанию 514 |
| 8 | Включить вывод отладочных сообщений во время загрузки устройства (не обязательно) | `esr(config)#syslog reload debugging` | |
| 9 | Включить нумерацию сообщений (не обязательно) | `esr(config)#syslog sequence-numbers` | |
| 10 | Включить точность даты сообщений до миллисекунд (не обязательно). | `esr(config)#syslog timestamp msec` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 11 | Включить регистрацию неудачных аутентификаций (не обязательно). | `esr(config)#logging login on-failure` | |
| 12 | Включить регистрацию изменений настроек системы аудита (не обязательно). | `esr(config)#logging syslog configuration` | |
| 13 | Включить регистрацию изменений настроек пользователя (не обязательно). | `esr(config)#logging userinfo` | |

### 11.5.2 Пример настройки

**Задача:**

Настроить отправку сообщений для следующих системных событий:

- неудачная аутентификация пользователя;
- внесены изменения в конфигурацию логирования системных событий;
- старт/остановка системного процесса;
- внесены изменения в профиль пользователей.

IP-адрес маршрутизатора ESR – 192.168.52.8, ip-адрес Syslog сервера – 192.168.52.41. Использовать параметры по умолчанию для отправки сообщений – протокол UDP порт 514.


**Решение:**

Предварительно нужно выполнить следующие действия:

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

Основной этап конфигурирования:

Создаем файл на маршрутизаторе для системного журнала, уровень сообщений для журналирования – info:

```
esr(config)# syslog file ESR info
```

Указываем IP адрес и параметры удаленного Syslog-сервера:

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

Задаем логирование неудачных попыток аутентификации:

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

Задаем логирование изменений конфигурации syslog:

```
esr(config)# logging syslog configuration
```

Задаем логирование старта/остановки системных процессов:

```
esr(config)# logging service start-stop
```

Задаем логирование внесений изменений в профиль пользователей:

```
esr(config)# logging userinfo
```

Изменения конфигурации вступят в действие после применения:

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

Посмотреть текущую конфигурацию системного журнала:

```
esr# show syslog configuration
```

Посмотреть записи системного журнала:

```
esr# show syslog ESR
```

## 11.6 Проверка целостности

Проверка целостности подразумевает проверку целостности хранимых исполняемых файлов.

### 11.6.1 Процесс настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Запустить проверку целостности системы | `esr# verify filesystem <detailed>` | **detailed** – детальный вывод информации в консоль. |

### 11.6.2 Пример конфигурации

**Задача:**

Проверить целостность файловой системы:

**Решение:**

Запускаем проверку целостности:

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

## 11.7 Настройка архивации конфигурации маршрутизатора

На маршрутизаторах ESR предусмотрена функция локального и/или удаленного копирования конфигурации по таймеру или при применении конфигурации.

### 11.7.1 Процесс настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Перейти в режим настройки параметров резервирования конфигурации | `esr(config)# archive` | |
| 2 | Установить тип сохранения резервных конфигураций маршрутизатора (не обязательно) | `esr(config-ahchive)# type <TYPE>` | <TYPE> – тип сохранения резервных конфигураций маршрутизатора. Принимает значения:<br>• **local;**<br>• **remote;**<br>• **both.**<br>Значение по умолчанию: remote |
| 3 | Включить режим резервирования конфигурации по таймеру (не обязательно) | `esr(config-ahchive)# auto` | |
| 4 | Включить режим резервирования конфигурации после каждого успешного применения конфигурации (не обязательно) | `esr(config-ahchive)# by-commit` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 5 | Указать путь для удаленного копирования конфигураций маршрутизатора (обязательно для типов remote и both) | `esr(config-ahchive)# path <PATH>` | <PATH> - определяет протокол, адрес сервера, расположение и префикс имени файла на сервере |
| 6 | Задать период времени для автоматического резервирования конфигурации (не обязательно, актуально только для режима auto) | `esr(config-ahchive)# time-period <TIME>` | <TIME> – периодичность автоматического резервирования конфигурации, принимает значение в минутах [1..35791394]. Значение по умолчанию: 720 минут |
| 7 | Задать максимальное количество локально сохраняемых резервных копий конфигураций (не обязательно, актуально при типах local и both) | `esr(config-ahchive)# count-backup <NUM>` | <NUM> – максимальное количество локально сохраняемых резервных копий конфигураций. Принимает значения в диапазоне [1..100]. Значение по умолчанию: 1 |

### 11.7.2 Пример конфигурации

**Задача:**

Настроить локальное и удаленное резервное копирование конфигурации маршрутизатора 1 раз в сутки и при успешном изменении конфигурации. Удаленные копии необходимо отправлять на tftp-сервер 172.16.252.77 в подпапку esr-example. Максимальное количество локальных копий – 30.

**Решение:**

Для успешной работы удаленной архивации конфигураций, между маршрутизатором и сервером должна быть организована IP-связность, настроены разрешения на прохождение tftp-трафика по сети и сохранения файлов на сервере.

1 Основной этап конфигурирования:

Перейти в режим конфигурирования резервного копирования конфигураций:

```
esr# configure
esr(config)# archive
```

Задать режим локального и удаленного резервного копирования конфигурации:

```
esr(config)# type both
```

Настроить путь для удаленного копирования конфигураций и максимальное количество локальных резервных копий:

```
esr(config-archive)# path tftp://172.16.252.77:/esr-example/esr-example.cfg
esr(config-archive)# count-backup 30
```

Задать интервал резервного копирования конфигурации в случае отсутствия изменений:

```
esr(config-archive)# time-period 1440
```

Включить режимы архивации конфигурации маршрутизатора по таймеру и при успешном изменении конфигурации:

```
esr(config-archive)# auto
esr(config-archive)# by-commit
```

После применения данной конфигурации 1 раз в сутки и при каждом успешном изменении конфигурации маршрутизатора на tftp-сервер будет отправляться конфигурационный файл с именем вида "esr-exampleYYYYMMDD_HHMMSS.cfg". Также, на самом маршрутизаторе в разделе flash:backup/ будет создаваться файл с именем вида "config_YYYYMMDD_HHMMSS". Когда в разделе flash:backup/ накопится 30 таких файлов, при создании нового будет удаляться наиболее старый.

# 12 Управление BRAS (Broadband Remote Access Server)



## 12.1 Алгоритм настройки

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Добавить RADIUS-сервер в список используемых серверов и перейти в режим его конфигурирования. | `esr(config)# radius -server host { <IP-ADDR> \| <IPV6-ADDR> } [ vrf <VRF> ]esr(config-radius-server)#` | <IP-ADDR> – IP-адрес RADIUS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];<br><br><IPV6-ADDR> – IPv6-адрес RADIUS-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает<br><br>значения в шестнадцатеричном<br><br>формате [0..FFFF]<br><br><VRF> – имя экземпляра VRF, задается строкой до 31 символа. |
| 2 | Задать пароль для аутентификации на<br><br>удаленном RADIUS-сервере. | `esr(config-radius-server)# key ascii-text { <TEXT> \| encrypted <ENCRYPTED-TEXT> }` | <TEXT> – строка [8..16] ASCII-символов; <ENCRYPTED-TEXT> – зашифрованный пароль, размером [8..16] байт, задаётся строкой [16..32] символов. |
| 3 | Создать профиль AAA. | `esr(config)# aaa radius-profile <NAME>` | <NAME> – имя профиля сервера, задается строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 4 | В профиле AAA указать RADIUS-сервер. | `esr(config-aaa-radius-profile)# radius-server host { <IP-ADDR> \| <IPV6-ADDR> }` | <IP-ADDR> – IP-адрес RADIUS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];<br><br><IPV6-ADDR>–IPv6-адрес RADIUS-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает<br><br>значения в шестнадцатеричном<br><br>формате [0..FFFF]. |
| 5 | Создать DAS-сервер. | `esr(config)# das-server <NAME>` | <NAME> – имя DAS-сервера, задается строкой до 31 символа. |
| 6 | Задать пароль для аутентификации на удаленном DAS-сервере. | `esr(config-das-server)# key ascii-text {<TEXT>\|encrypted <ENCRYPTED-TEXT> }` | <TEXT> – строка [8..16] ASCII-символов; <ENCRYPTED-TEXT>–зашифрованный пароль, размером [8..16] байт, задаётся строкой [16..32] символов. |
| 7 | Создать AAA DAS-профиль. | `esr(config)# aaa das-profile <NAME>` | <NAME> – имя DAS-профиля, задается строкой до 31 символа. |
| 8 | Указать DAS-сервер в DAS-профиле. | `esr(config-aaa-das-profile)# das-server <NAME>` | <NAME> – имя DAS-сервера, задается строкой до 31 символа. |
| 9 | Сконфигуровать BRAS. | `esr(config)# subscriber-control [ vrf <VRF> ]` | <VRF> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет работать контроль пользователей. |
| 10 | Выбрать профиль серверов динамической авторизации (DAS), на которые будут приходить CoA-запросы от PCRF | `esr(config-subscriber-control)# aaa das-profile <NAME>` | <NAME> – имя профиля серверов динамической авторизации (DAS), задается строкой до 31 символа. |
| 11 | Выбрать профиль RADIUS-серверов для получения параметров сервисов пользователя | `esr(config-subscriber-control)# aaa services-radius-profile <NAME>` | <NAME> – имя профиля RADIUS-серверов, задается строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 12 | Выбрать профиль RADIUS-серверов для получения параметров сессии пользователя. | `esr(config-subscriber-control)# aaa sessions-radius-profile <NAME>` | <NAME> – имя профиля RADIUS-серверов, задается строкой до 31 символа. |
| 13 | Определить IP-адрес маршрутизатора, который будет использоваться в качестве IP-адреса источника в отправляемых RADIUS пакетах. | `esr(config-subscriber-control)# nas-ip-address <ADDR>` | <ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |
| 14 | Включить аутентификацию сессий по MAC-адресу<br><br>(не обязательно). | `esr(config-subscriber-control)# session mac-authentication` | |
| 15 | Организовать прозрачное пропускание служебного трафика (DHCP, DNS и т.д.) на основе фильтров. | `esr(config-subscriber-control)# bypass-traffic-ac l <NAME>` | <NAME> – имя привязываемого ACL, задается строкой до 31 символа. |
| 16 | Перейти в режим конфигурирования сервиса по умолчанию. | `esr(config-subscriber-control)# default-service` | |
| 17 | Привязать указанный QoS-класс к сервису по умолчанию. | `esr(config-subscriber-default-service)# class-map <NAME>` | <NAME> – имя привязываемого класса, задается строкой до 31 символа. |
| 18 | Указать имя списка URL, который будет использоваться для фильтрации HTTP/HTTPS трафика не аутентифицированных пользователей. | `esr(config-subscriber-default-service)# filter-name { local<LOCAL-NAME> \| remote<REMOTE-NAME> }` | <LOCAL-NAME> – имя профиля URL, задаётся строкой до 31 символа;<br><br><REMOTE-NAME> – имя списка URL на удаленном сервере, задаётся строкой до 31 символа. |
| 19 | Указать действия, которые должны быть применены для HTTP/HTTPS-пакетов, URL которых входит в список URL, назначенных командой «filter-name». | `esr(config-subscriber-default-service)# filter-action<ACT>` | <ACT> – назначаемое действие:<br>• **permit** – прохождение трафика разрешается;<br>• **deny** – прохождение трафика запрещается;<br>redirect <URL> – будет выполнен редирект на указанный URL, задается строкой до 255 символов. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 20 | Указать действия, которые должны быть применены для HTTP/HTTPS-пакетов, URL которых не входит в список URL, назначенных командой «filter-name». | `esr(config-subscriber-default-service)# default-action<ACT>` | <ACT> – назначаемое действие:<br>• **permit** – прохождение трафика разрешается;<br>• **deny** – прохождение трафика запрещается;<br>redirect <URL> – будет выполнен редирект на указанный URL, задается строкой до 255 символов. |
| 21 | Активировать профиль контроля пользователей. | `esr(config-subscriber-control)#  enable` | |
| 22 | Изменить идентификатор сетевого интерфейса (физического, саб-интерфейса или сетевого моста) (не обязательно). | `esr(config-if)# location <ID>` | <ID> – идентификатор сетевого интерфейса, задаётся строкой до 220 символов. |
| 23 | Включить контроль пользователей на интерфейсе. | `esr(config-if-gi)# service-subscriber-control {any\| object-group <NAME>}` | <NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа. |
| 24 | Включить перезапрос значения квоты при ее истечении для сервисов пользователя с настроенным ограничением по объему трафика или времени<br><br>(не обязательно). | `esr(config-subscriber-control)# quota-expired-reauth` | |
| 25 | Включить аутентификацию сессий по IP-адресу.<br><br>(не обязательно) | `esr(config-subscriber-control)# session ip-authentication` | |
| 26 | Включить прозрачное пропускание трафика в состоянии backup для BRAS<br><br>(не обязательно). | `esr(config-subscriber-control)# backup traffic-processing transparent` | |
| 27 | Задать интервал, по истечении которого с устройства будут удалены неиспользуемые в текущий момент списки URL<br><br>(не обязательно). | `esr(config)# subscriber-control unused-filters-remove-delay <DELAY>` | <DELAY> – временной интервал в секундах, принимает значения [10800..86400]. |

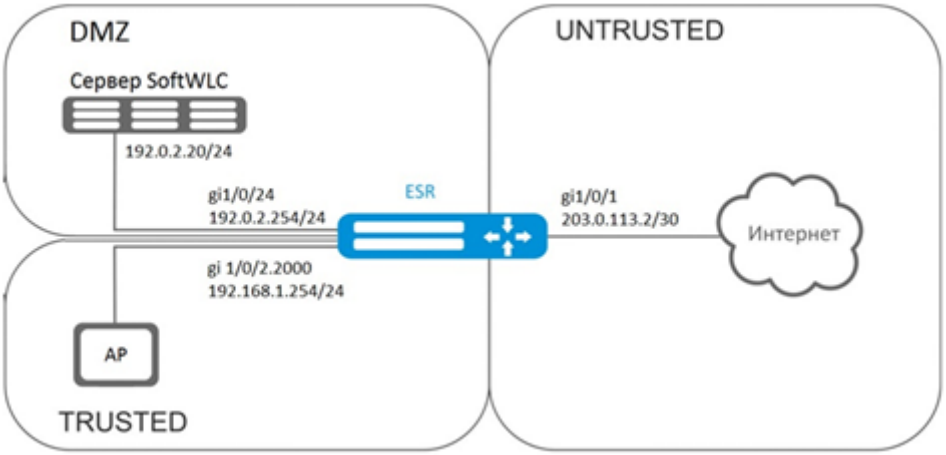
| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 28 | Задать интервал, по истечении которого, если не было пакетов от пользователя, сессия считается устаревшей и удаляется с устройства<br><br>(не обязательно). | `esr(config-subscriber-default-service)# session-timeout <SEC>` | <SEC> – период времени в секундах, принимает значения [120..3600]. |
| 29 | Определить VRRP-группу, на основе которой определяется состояние сервиса контроля абонентов (основной/резервный)<br><br>(не обязательно). | `esr(config-subscriber-control)# vrrp-group <GRID>` | <GRID> – идентификатор группы VRRP-маршрутизатора, принимает значения [1..32]. |
| 30 | Определить с каких TCP-портов назначения трафик будет перенаправлен на HTTP Proxy-сервер маршрутизатора<br><br>(не обязательно). | `esr(config-subscriber-control)# ip proxy http listen-ports <NAME>` | <NAME> – имя профиля TCP/UDP-портов, задаётся строкой до 31 символа. |
| 31 | Определить порт HTTP Proxy-сервера на маршрутизаторе<br><br>(не обязательно). | `esr(config-subscriber-control)# ip proxy http redirect-port <PORT>` | <PORT> – номер порта, указывается в диапазоне [1..65535]. |
| 32 | Определить с каких TCP-портов назначения трафик будет перенаправлен на HTTPS Proxy-сервер маршрутизатора<br><br>(не обязательно). | `esr(config-subscriber-control)# ip proxy https listen-ports <NAME>` | <NAME> – имя профиля TCP/UDP-портов, задаётся строкой до 31 символа. |
| 33 | Определить порт HTTPS Proxy-сервера на маршрутизаторе<br><br>(не обязательно). | `esr(config-subscriber-control)# ip proxy https redirect-port <PORT>` | <PORT> – номер порта, указывается в диапазоне [1..65535]. |
| 34 | Определить IP-адрес маршрутизатора, который будет использоваться в качестве IP-адреса источника в отправляемых Proxy-сервером HTTP/HTTPS пакетах<br><br>(не обязательно). | `esr(config-subscriber-control)# ip proxy source-address <ADDR>` | <ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 35 | Задать URL-адрес сервера, предоставляющего списки приложений для фильтрации трафика<br><br>(не обязательно) | `esr(config)# subscriber-control apps-server-url <URL>` | <URL> – адрес ссылки, задаётся строкой от 8 до 255 символов. |
| 36 | Включить контроль приложений на интерфейсе (не обязательно) | `esr(config-if-gi)# subscriber-control application-filter <NAME>` | <NAME> – имя профиля приложений, задаётся строкой до 31 символа. |
| 37 | Установить/ сбросить верхнюю границу количества сессий BRAS (не обязательно) | `esr(config-subscriber-control)# thresholds sessions-number high <Threshold>` | <Threshold> – количество сессий BRAS, [0-50000] – для ESR-1700<br>• [0-10000] – для ESR-1200/1000<br>• [0-1000] – для ESR-100/200 |
| 38 | Установить/ сбросить нижнюю границу количества сессий BRAS (не обязательно) | `esr(config-subscriber-control)# thresholds sessions-number low <Threshold>` | <Threshold> – количество сессий BRAS, [0-50000] – для ESR-1700<br>• [0-10000] – для ESR-1200/1000<br>• [0-1000] – для ESR-100/200 |

## 12.2 Пример настройки с SoftWLC

**Задача:**

Предоставлять доступ до ресурсов сети Интернет, только для авторизованных пользователей.



**Решение:**
За хранение учетных данных пользователей и параметров тарифных планов отвечает сервер SoftWLC. Информацию по установке и настройке сервера SoftWLC можно найти по ссылкам ниже:

v1.19_SoftWLC – общая статья о SoftWLC;

v1.19_Инструкции по установке и настройке – установка SoftWLC из репозиториев.

Для маршрутизатора необходимо наличие лицензии BRAS, после ее активации можно переходить к конфигурированию устройства.

Создадим три зоны безопасности на устройстве, согласно схеме сети:

```
esr# configure
esr(config)# security zone trusted
esr(config-zone)# exit
esr(config)# security zone untrusted
esr(config-zone)# exit
esr(config)# security zone dmz
esr(config-zone)# exit
```

Сконфигурируем параметры публичного порта и сразу пропишем шлюз по умолчанию:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# security-zone untrusted
esr(config-if-gi)# ip address 203.0.113.2/30
esr(config-if-gi)# service-policy dynamic upstream
esr(config-if-gi)# exit
esr(config)# ip route 0.0.0.0/0 203.0.113.1
```

Сконфигурируем порт в сторону сервера SoftWLC:

```
esr (config)# interface gigabitethernet 1/0/24
esr (config-if-gi)# security-zone dmz
esr (config-if-gi)# ip address 192.0.2.1/24
esr (config-if-gi)# exit
```

Сконфигурируем порт для подключения Wi-Fi точки доступа.

```
esr(config)# bridge 2
esr(config-bridge)# security-zone trusted
esr(config-bridge)# ip address 192.168.0.254/24
esr(config-bridge)# ip helper-address 192.0.2.20
esr(config-bridge)# service-subscriber-control object-group users
esr(config-bridge)# location ssid1
esr(config-bridge)# enable
esr(config-bridge)# exit
esr(config)# interface gigabitethernet 1/0/2.2000
esr(config-subif)# bridge-group 1
esr(config-subif)# exit
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# service-policy dynamic downstream
esr (config-if-gi)# exit
```

⚠ Подключать клиентов необходимо через сабинтерфейсы в бриджи, причем от параметра location (смотри конфигурацию bridge 2) зависит выбор тарифного плана.

Модуль, отвечающий за AAA-операции, основан на eltex-radius и доступен по IP-адресу сервера SoftWLC. Номера портов для аутентификации и аккаунтинга в нашем примере – это значения по умолчанию для SoftWLC.

Зададим параметры для взаимодействия с этим модулем:

```
esr(config)# radius-server host 192.0.2.20
esr(config-radius-server)#   key ascii-text password
esr(config-radius-server)#   auth-port 31812
esr (config-radius-server)#  acct-port 31813
esr (config-radius-server)# exit
```

Создадим профиль AAA:

```
esr(config)# aaa radius-profile RADIUS
esr(config-aaa-radius-profile)# radius-server host 192.0.2.20
esr(config-aaa-radius-profile)# exit
```

Укажем параметры доступа к DAS (Direct-attached storage) серверу:

```
esr(config)# object-group network server
esr(config-object-group-network)#   ip address-range 192.0.2.20
esr(config-object-group-network)# exit
esr(config)# das-server CoA
esr(config-das-server)#   key ascii-text password
esr(config-das-server)#   port 3799
esr(config-das-server)#   clients object-group server
esr(config-das-server)# exit
esr(config)# aaa das-profile CoA
esr(config-aaa-das-profile)#   das-server CoA
esr(config-aaa-das-profile)# exit
```

До аутентификации весь трафик из зоны trusted блокируется, в том числе DHCP и DNS запросы. Необходимо настроить разрешающие правила для пропуска DHCP и DNS запросов:

```
esr(config)# ip access-list extended DHCP
esr(config-acl)#  rule 10
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol udp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port 68
esr(config-acl-rule)# match destination-port 67
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# rule 11
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol udp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port any
esr(config-acl-rule)# match destination-port 53
esr(config-acl-rule)# enable
esr(config-acl-rule)#exit
esr(config-acl)# exit
```

Далее создаем правила для редиректа на портал и пропуска трафика в Интернет:

```
esr(config)# ip access-list extended WELCOME
esr(config-acl)# rule 10
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit
esr (config)# ip access-list extended INTERNET
esr(config-acl)#  rule 10
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# exit
```

Зададим web-ресурсы доступные без авторизации:

```
esr(config)# object-group url defaultservice
esr(config-object-group-url)# url http://eltex.nsk.ru
esr(config-object-group-url)# exit
```

Списки фильтрации по URL находятся на сервере SoftWLC (меняется только IP-адрес сервера SoftWLC, если используется адресация отличная от данного примера, все остальное в URL оставить без изменения):

```
esr(config)# subscriber-control filters-server-url http://192.0.2.20:7070/Filters/file/
```

Сконфигурируем и включим BRAS, в качестве NAS IP указываем адрес интерфейса на стыке с SoftWLC, в данном примере – это IP-адрес интерфейса gigabitethernet 1/0/24:

```
esr(config)# subscriber-control
esr(config-subscriber-control)#  aaa das-profile CoA
esr(config-subscriber-control)#  aaa sessions-radius-profile RADIUS
esr(config-subscriber-control)#  nas-ip-address 192.0.2.1
esr(config-subscriber-control)#  session mac-authentication
esr(config-subscriber-control)#  bypass-traffic-acl DHCP
esr(config-subscriber-control)#  default-service
esr(config-subscriber-default-service)#  class-map INTERNET
esr(config-subscriber-default-service)#  filter-name local defaultservice
esr(config-subscriber-default-service)#  filter-action permit
esr(config-subscriber-default-service)#  default-action redirect http://192.0.2.20:8080/
eltex_portal/
esr(config-subscriber-default-service)#  session-timeout 3600
esr(config-subscriber-default-service)# exit
esr(config-subscriber-control)# enable
esr(config-subscriber-control)# exit
```

Далее необходимо сконфигурировать правила перехода между зонами безопасности.

```
esr(config)# object-group service telnet
esr(config-object-group-service)#   port-range 23
esr(config-object-group-service)# exit
esr(config)# object-group service ssh
esr(config-object-group-service)#   port-range 22
esr(config-object-group-service)# exit
esr(config)# object-group service dhcp_server
esr(config-object-group-service)#   port-range 67
esr(config-object-group-service)# exit
esr(config)# object-group service dhcp_client
esr(config-object-group-service)#   port-range 68
esr(config-object-group-service)# exit
esr(config)# object-group service ntp
esr(config-object-group-service)#   port-range 123
esr(config-object-group-service)# exit
```

Разрешим доступ в Интернет из зон trusted и dmz:

```
esr(config)# security zone-pair trusted untrusted
esr(config-zone-pair)# rule 10
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# security zone-pair dmz untrusted
esr(config-zone-pair)# rule 10
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# security zone-pair dmz trusted
esr(config-zone-pair)# rule 10
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
```

Разрешим прохождение DHCP из trusted в dmz:

```
esr (config)# security zone-pair trusted dmz
esr (config-zone-pair)# rule 10
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol udp
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# match source-port dhcp_client
esr(config-zone-pair-rule)# match destination-port dhcp_server
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
```

Разрешим прохождение ICMP к устройству, для работы BRAS необходимо открыть порты для веб-проксирования – TCP 3129/3128 (NetPort Discovery Port/Active API Server Port):

```
esr(config)# object-group service bras
esr(config-object-group-service)#   port-range 3129
esr(config-object-group-service)#   port-range 3128
esr(config-object-group-service)# exit
esr(config)#  security zone-pair trusted self
esr(config-zone-pair)#  rule 10
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol tcp
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# match source-port any
esr(config-zone-pair-rule)# match destination-port bras
esr(config-zone-pair-rule)# enable
esr (config-zone-pair-rule)# exit
esr(config-zone-pair)# rule 20
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-rule)# exit
esr(config)# security zone-pair dmz self
esr(config-zone-pair)# rule 20
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-rule)# exit
esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule 20
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-rule)# exit
```

Активируем DHCP-Relay:

```
esr(config)# ip dhcp-relay
```

Настроим SNAT в порт gigabitethernet 1/0/1:

```
esr(config)# nat source
esr(config-snat)# ruleset inet
esr(config-snat-ruleset)# to interface gigabitethernet 1/0/1
esr(config-snat-ruleset)# rule 10
esr(config-snat-rule)# match source-address any
esr(config-snat-rule)# action source-nat interface
esr(config-snat-rule)# enable
esr(config-snat-rule)# end
```

## 12.3 Пример настройки без SoftWLC

**Задача:**

Настроить BRAS без поддержки SoftWLC.

**Дано:**

Подсеть с клиентами 10.10.0.0/16, подсеть для работы с FreeRADIUS-сервером 192.168.1.1/24

**Решение:**

### 12.3.1 Шаг 1:

Настройка RADIUS-сервера.

Для FreeRADIUS-сервера нужно задать подсеть, из которой могут приходить запросы и добавить список пользователей. Для этого в файл users в директории с файлами конфигурации FreeRADIUS сервера нужно добавить:

Профиль пользователя:

```
<MACADDR> Cleartext-Password := <MACADDR>
```

#Имя пользователя

```
 User-Name = <USER_NAME>,
```

#Максимальное время жизни сессии

```
 Session-Timeout = <SECONDS>,
```

#Максимальное время жизни сесиии при бездействии пользователя

```
 Idle-Timeout = <SECONDS>,
```

#Время на обновление статистики по сессии

```
 Acct-Interim-Interval = <SECONDS>,
```

#Имя сервиса для сессии (A – сервис включен, N – сервис выключен)

```
Cisco-Account-Info = "{A|N}<SERVICE_NAME>"
```

Профиль сервиса:

```
<SERVICE_NAME> Cleartext-Password := <MACADDR>
```

# Соответствует имени class-map в настройках ESR

```
Cisco-AVPair = "subscriber:traffic-class=<CLASS_MAP>",
```

# Действие, которое применяет ESR к трафику (permit, deny, redirect)

```
Cisco-AVPair = "subscriber:filter-default-action=<ACTION>",
```

# Возможность прохождения IP потоков (enabled-uplink, enabled-downlink, enabled, disabled)

```
Cisco-AVPair = "subscriber:flow-status=<STATUS>"
```

В файл clients.conf нужно добавить подсеть, в которой находится ESR:

```
client ESR {
ipaddr = <SUBNET>
secret = <RADIUS_KEY>
}
```

В нашем случае настройка RADIUS-сервера будет выглядеть так:

в файл «clients.conf» добавляем строки:

```
client BRAS {
ipaddr = 192.168.1.1
secret = password
}
```

В файл «users» добавляем строки (вместо <MAC> нужно указать MAC адрес клиента):

```
"54-E1-AD-8F-37-35" Cleartext-Password := "54-E1-AD-8F-37-35"
User-Name = "Bras_user",
Session-Timeout = 259200,
Idle-Timeout = 259200,
Cisco-AVPair += "subscriber:policer-rate-in=1000",
Cisco-AVPair += "subscriber:policer-rate-out=1000",
Cisco-AVPair += "subscriber:policer-burst-in=188",
Cisco-AVPair += "subscriber:policer-burst-out=188",
Cisco-Account-Info = "AINTERNET"
INTERNET Cleartext-Password := "INTERNET"
User-Name = "INTERNET",
Cisco-AVPair = "subscriber:traffic-class=INTERNET",
Cisco-AVPair += "subscriber:filter-default-action=permit"
```

### 12.3.2 Шаг 2:

Настройка ESR.

Для настройки функционала BRAS необходимо наличие лицензии BRAS.

```
esr(config)# do sh licence
Licence information
-------------------
Name:    Eltex
Version: 1.0
Type:    ESR-X
S/N:     NP00000000
MAC:     XX:XX:XX:XX:XX:XX
Features:
  BRAS - Broadband Remote Access Server
```

Настройка параметров для взаимодействия с RADIUS-сервером:

```
esr(config)# radius-server host 192.168.1.2
esr(config-radius-server)# key ascii-text encrypted 8CB5107EA7005AFF
esr(config-radius-server)# source-address 192.168.1.1
esr(config-radius-server)# exit
```

Создадим профиль AAA:

```
esr(config)#  aaa radius-profile bras_radius
esr(config-aaa-radius-profile)# radius-server host 192.168.1.2
esr(config-aaa-radius-profile)#  exit
esr(config)#  aaa radius-profile bras_radius_servers
esr(config-aaa-radius-profile)#  radius-server host 192.168.1.2
esr(config-aaa-radius-profile)#  exit
```

Укажем параметры к DAS-серверу:

```
esr(config)# das-server das
esr(config-das-server)# key ascii-text encrypted 8CB5107EA7005AFF
esr(config-das-server)#  exit
esr(config)#  aaa das-profile bras_das
esr(config-aaa-das-profile)#  das-server das
esr(config-aaa-das-profile)# exit
esr(config)#  vlan 10
esr(config-vlan)#  exit
```

Далее создаем правила для редиректа на портал и пропуска трафика в Интернет:

```
esr(config)#  ip access-list extended BYPASS
esr(config-acl)# rule 1
esr(config-acl-rule)#  action permit
esr(config-acl-rule)# match protocol udp
esr(config-acl-rule)#  match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)#  match source-port 68
esr(config-acl-rule)#  match destination-port 67
esr(config-acl-rule)# enable
esr(config-acl-rule)#  exit
esr(config-acl)#  rule 2
esr(config-acl-rule)#  action permit
esr(config-acl-rule)#  match protocol udp
esr(config-acl-rule)#  match source-address any
esr(config-acl-rule)#  match destination-address any
esr(config-acl-rule)#  match source-port any
esr(config-acl-rule)#  match destination-port 53
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config)# ip access-list extended INTERNET
esr(config-acl)# rule 1
esr(config-acl-rule)#  action permit
esr(config-acl-rule)# match protocol any
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# enable
esr(config-acl-rule)#  exit
esr(config)# ip access-list extended WELCOME
esr(config-acl)# rule 10
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol tcp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port any
esr(config-acl-rule)# match destination-port 443
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# rule 20
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol tcp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port any
esr(config-acl-rule)# match destination-port 8443
```

```
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# rule 30
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol tcp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port any
esr(config-acl-rule)# match destination-port 80
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
esr(config-acl)# rule 40
esr(config-acl-rule)# action permit
esr(config-acl-rule)# match protocol tcp
esr(config-acl-rule)# match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)# match source-port any
esr(config-acl-rule)# match destination-port 8080
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
```

Настройка действие фильтрации по URL обязательно, а именно, необходимо настроить фильтрацию http-proxy на BRAS для неавторизованных пользователей:

```
esr(config)# object-group url defaultserv
esr(config-object-group-url)# url http://eltex.nsk.ru
esr(config-object-group-url)# url http://ya.ru
esr(config-object-group-url)# url https://ya.ru
esr(config-object-group-url)# exit
```

Сконфигурируем и включим BRAS, в качестве NAS IP указываем адрес интерфейса на стыке с RADIUS-сервером в данном примере – это IP-адрес интерфейса gigabitethernet 1/0/2:

```
esr(config)#  subscriber-control
esr(config-subscriber-control)# aaa das-profile bras_das
esr(config-subscriber-control)# aaa sessions-radius-profile bras_radius
esr(config-subscriber-control)# aaa services-radius-profile bras_radius_servers
esr(config-subscriber-control)# nas-ip-address 192.168.1.1
esr(config-subscriber-control)# session mac-authentication
esr(config-subscriber-control)# bypass-traffic-acl BYPASS
esr(config-subscriber-control)# default-service
esr(config-subscriber-default-service)# class-map BYPASS
esr(config-subscriber-default-service)# filter-name local defaultserv
esr(config-subscriber-default-service)# filter-action permit
esr(config-subscriber-default-service)# default-action redirect http://192.
168.1.2:8080/eltex_portal
esr(config-subscriber-default-service)# session-timeout 121
esr(config-subscriber-default-service)# exit
esr(config-subscriber-control)# enable
esr(config-subscriber-control)# exit
```

На интерфейсах, для которых требуется работа BRAS настроить (для успешного запуска требуется как минимум один интерфейс):

```
esr(config)#  bridge 10
esr(config-bridge)# vlan 10
esr(config-bridge)# ip firewall disable
esr(config-bridge)#  ip address 10.10.0.1/16
esr(config-bridge)#  ip helper-address 192.168.1.2
esr(config-bridge)# service-subscriber-control any
esr(config-bridge)# location USER
esr(config-bridge)#  protected-ports
esr(config-bridge)#  protected-ports exclude vlan
esr(config-bridge)# enable
esr(config-bridge)#  exit
```

Сконфигурируем порт в сторону RADIUS-сервера:

```
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# ip firewall disable
esr(config-if-gi)# ip address 192.168.1.1/24
esr(config-if-gi)#  exit
```

Порт в сторону Клиента:

```
esr(config)#  interface gigabitethernet 1/0/3.10
esr(config-subif)#  bridge-group 10
esr(config-subif)# ip firewall disable
esr(config-subif)#  exit
```

Настройка SNAT в порт gigabitethernet 1/0/2:

```
esr(config)# nat source
esr(config-snat)# ruleset factory
esr(config-snat-ruleset)# to interface gigabitethernet 1/0/2
esr(config-snat-ruleset)# rule 10
esr(config-snat-rule)# description "replace 'source ip' by outgoing interface ip address"
esr(config-snat-rule)# match protocol any
esr(config-snat-rule)# match source-address any
esr(config-snat-rule)# match destination-address any
esr(config-snat-rule)# action source-nat interface
esr(config-snat-rule)# enable
esr(config-snat-rule)# exit
esr(config-snat-ruleset)# exit
esr(config-snat)# exit
esr(config)# ip route 0.0.0.0/0 192.168.1.2
```

Изменения конфигурации вступят в действие после применения:

```
esr(config) # do commit
esr(config) # do confirm
```

Для просмотра информации и статистики по сессиям контроля пользователей – можно воспользоваться командой:

```
esr # sh subscriber-control sessions status

Session id      User name    IP address      MAC address       Interface          Domain
--------------------   ---------------  ---------------   -----------------
1729382256910270473    Bras_user   10.10.0.3  54:e1:ad:8f:37:35     gi1/0/3.10     --
```

# 13 Управление VoIP



VoIP (англ. Voice over IP) — набор протоколов, которые позволяют передавать речевую информацию посредством IP-сетей. В рамках данного устройства VoIP используется для подключения аналоговых телефонных аппаратов к IP-сети с возможностью совершения телефонных вызовов.

## 13.1 Алгоритм настройки SIP-профиля

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Настройка SIP-профиля | `esr(config)# sip profile <NUM>` | <NUM> – номер SIP-профиля, задается в виде цифры от 1 до 5. |
| 2 | Настройка основного SIP proxy-сервера и сервера регистрации | `esr(config-sip-profile)# proxy primary` | |
| 3 | Настройка адреса SIP proxy-сервера | `esr(config-voip-sip-proxy)# ip address proxy-server <IP>` | <IP> – IP-адрес proxy-сервера |
| 4 | Настройка порта SIP proxy-сервера | `esr(config-voip-sip-proxy)# ip port proxy-server <PORT>` | <PORT> – номер UDP-порта proxy-сервера, принимает значения [1..65535]. Если используется стандартный порт 5060, то его можно не указывать. |
| 5 | Настройка адреса сервера регистрации | `esr(config-voip-sip-proxy)# ip address registration-server <IP>` | <IP> – IP-адрес сервера регистрации. |
| 6 | Настройка порта сервера регистрации: | `esr(config-voip-sip-proxy)# ip portregistration-server <PORT>` | <PORT> – номер UDP-порта сервера регистрации, принимает значения [1..65535].<br><br>Если используется стандартный порт 5060, то его можно не указывать. |
| 7 | Активация регистрации | `esr(config-voip-sip-proxy)# registration` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 8 | Активация proxy-сервера и сервера регистрации: | `esr(config-voip-sip-proxy)# enable` | |
| 9 | Настройка адреса сервера регистрации | `esr(config-voip-sip-proxy)# ip address registration-server <IP>` | <IP> – IP-адрес сервера регистрации. |
| 10 | Настройка порта сервера регистрации: | `esr(config-voip-sip-proxy)# ip portregistration-server <PORT>` | <PORT> – номер UDP-порта сервера регистрации, принимает значения [1..65535]. Если используется стандартный порт 5060, то его можно не указывать. |
| 11 | Указание SIP-домена, в котором находится устройство | `esr(config-sip-profile)# sip-domain address <ADDRESS>` | <ADDRESS> – SIP-домен, в котором находится устройство, задается ipv4-адресом или доменным именем. |
| 12 | Активация использования SIP domain при регистрации | `esr(config-sip-profile)# sip-domain registration enable` | |
| 13 | Настройка SIP-профиля | `esr(config)# sip profile <NUM>` | <NUM> – номер SIP-профиля, задается в виде цифры от 1 до 5. |
| 14 | Назначение плана нумерации текущему SIP-профилю | `esr(config-sip-profile)# dialplan pattern <DNAME>` | <DNAME> – имя план нумерации, задается стройкой до 31 символа. |
| 15 | Активация SIP-профиля | `esr(config-sip-profile)# enable` | |

## 13.2 Алгоритм настройки FXS/FXO-портов

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Переход в режим конфигурирования FXO/FXS-портов | `esr(config)# interface voice-port <NUM>` | <NUM> – номер порта, принимает значение от 1 до 4. |
| 2 | Назначение абонентского номера, закрепленного за телефонным портом | `esr(config-voice-port-fxs)# sip user phone <PHONE>` | <PHONE> – абонентский номер, закрепленный за телефонным портом, задается до 50 символов. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 3 | Назначение имя пользователя, сопоставленное с портом | `esr-12v(config-voice-port-fxs)# sip user display-name <LOGIN>` | <LOGIN> – имя пользователя, которое отображается в поле Display-Name, задается стройкой до 31 символа. |
| 4 | Выбор SIP-профиля для конкретного порта. | `esr(config-voice-port-fxs)# profile sip <PROFILE>` | <PROFILE> – номер SIP-профиля, задается от 1 до 5. |
| 5 | Настройка логина для аутентификации | `esr(config-voice-port-fxs)# authentication name <LOGIN>` | <LOGIN> – логин для аутентификации, задается строкой до 31 символа |
| 6 | Настройка пароля для аутентификации | `esr(config-voice-port-fxs)# authentication password <PASS>` | <PASS> – пароль для аутентификации, задается строкой до 16 символов. |
| 7 | Активация FXO-порта | `esr(config)# interface voice-port <NUM>` | <NUM> – номер FXO-порта принимает значение от 1 до 4. |
| 8 | Назначение абонентского номера, закрепленного за телефонным портом | `esr(config-voice-port-fxo)# sip user phone <PHONE>` | <PHONE> – абонентский номер, закрепленный за телефонным портом. |
| 9 | Указание UDP-порта, с которого и на который FXO-комплект будет отправлять и принимать SIP-сообщения | `esr(config-voice-port-fxo)# sip port <PORT>` | <PORT> – номер UDP-порта. |
| 10 | Назначение имени пользователя, сопоставленное с портом | `esr(config-voice-port-fxo)# sip user display-name <LOGIN>` | <LOGIN> – имя пользователя, которое отображается в поле Display-Name, задается строкой до 31 символа. |
| 11 | Настройка логина для аутентификации | `esr(config-voice-port-fxo)# authentication name <LOGIN>` | <LOGIN> – логин для аутентификации, задается строкой до 31 символа. |
| 12 | Настройка пароля для аутентификации | `esr(config-voice-port-fxo)# authentication password <PASS>` | <PASS> – пароль для аутентификации, задается строкой до 16 символов. |
| 13 | Разрешение передачи номера в ТфОП | `esr(config-voice-port-fxo)# pstn transmit-number` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 14 | Запретить передачу префикса | `esr(config-voice-port-fxo)# no pstn transmit-prefix` | |
| 15 | Активация услуги «Hostline PSTN to IP» | `esr(config-voice-port-fxo)# hotline ipt` | |
| 16 | Номер абонента, который будет получать вызовы с ТфОП | `esr(config-voice-port-fxo)# hotline number ipt <PHONE>` | <PHONE> – номер телефона, на который осуществляется вызов при использовании услуги, принимает значение от 1 до 50.<br><br>«Горячая/Теплая линия» в направлении из аналоговой телефонной линии в VoIP. |

## 13.3 Алгоритм настройки плана нумерации

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Создание плана нумерации | `esr(config)# dialplan pattern <DNAME>` | <DNAME> – имя плана нумерации, задается строкой до 31 символа. |
| 2 | Добавление правил нумерации | `esr(config-dial-ruleset)# pattern <REGEXP>` | <REGEXP> – регулярное выражение, задающее план нумерации. Задаётся строкой до 1024 символов. Правила составления регулярных выражений описаны в разделе Пример настройки плана нумерации. |
| 3 | Активация плана нумерации | `esr(config-dial-ruleset)# enable` | |

## 13.4 Алгоритм настройки PBX-сервера

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Настройка PBX-сервера | `esr(config)# pbx` | |
| 2 | Включение PBX-сервера | `esr(config-pbx)# enable` | |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 3 | Создание плана маршрутизации | `esr(config-pbx)# ruleset <rule_name>` | <rule_name> – имя плана маршрутизации, задается строкой до 31 символа. |
| 4 | Создание правила маршрутизации | `esr(config-pbx-ruleset)# rule <rule_index>` | <rule_index> – номер правила в плане маршрутицации, принимает значение от 1 до 1000. |
| 5 | Создание паттерна в правиле маршрутизации | `esr(config-pbx-rule)# pattern <REGEXP>` | <REGEXP> – регулярное выражение, задающее правило маршрутизации. Задаётся строкой до 256 символов. Правила составления регулярных выражений описаны в разделе Пример настройки плана нумерации. |
| 6 | Применение правила маршрутизации | `esr(config-pbx-rule)# enable` | |
| 7 | Создание SIP - профиля на PBX – сервере | `esr(config-pbx)# profile <PROFILE>` | <PROFILE> – имя SIP профиля, используемого PBX – сервером, задается строкой до 31 символа. |
| 8 | Выбор кодека, поддерживаемого SIP - профилем | `esr(config-pbx-profile)# codec allow { G711A(alaw) | G711U(ulaw) | G722 | G726 }` | |
| 9 | Выбор типа SIP - профиля | `esr(config-pbx-profile)# client { peer | user | friend }` | • **peer** – входящие и исходящие звоки разрешены без авторизации.<br>• **user** – разрешены только входящие звонки.<br>• **friend** – комбинирует типы профилей peer и user. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 10 | Выбор политики взаимодействия с NAT (не обязательно) | `esr(config-pbx-profile)# nat { comedia \| force-port \| both }` | • **comedia** – отправить медиа поток на порт PBX, независимо от указаний SDP.<br>• **force-port** – использовать rport, даже если его нет.<br>• **both** – объединяет comedia и force-port. |
| 11 | Выбор плана машрутизации, связанного с SIP - профилем | `esr(config-pbx-profile)# ruleset <NAME>` | <NAME> – Имя плана маршрутизации, задается строкой до 31 символа. |
| 12 | Создание абонента | `esr(config-pbx)# user <user>` | <user> – номер телефона или имя пользователя, задается строкой до 31 символа. |
| 13 | Создание пароля для абонента (не обязательно) | `esr(config-pbx-user)# password <password>` | <password> – пароль, который будет использоваться пользоватлем для аутентификации, задается строкой до 16 символов. |
| 14 | Применение SIP - профиля для абонента | `esr(config-pbx-user)# profile <SIPPROFILE>` | <SIPPROFILE> – SIP - профиль, используемый для данного абонента, задается строкой до 31 символа. |

## 13.5 Алгоритм создания транка регистрации

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 1 | Настройка PBX-сервера | `esr(config)# pbx` | |
| 2 | Создание транка | `esr(config-pbx)# register-server <name>` | <name> – имя транка, задается строкой до 31 символа. |
| 3 | Настройка адреса серверара гистрации | `esr(config-pbx-reg-server)# ip address <IP>` | <IP> – адрес сервера, на котором происходит регистрация, может принимать значение IP адреса или задаваться строкой до 31 символа. |

| Шаг | Описание | Команда | Ключи |
|---|---|---|---|
| 4 | Настройка порта сервера регистрации | `esr(config-pbx-reg-server)# ip port <PORT>` | <PORT> – номер UDP-порта сервера регистрации, принимает значения [1..65535]. Если используется стандартный порт 5060, то его можно не указывать. |
| 5 | Задание аутентификационного имени | `esr(config-pbx-reg-server)# username <user>` | <user> – имя пользователя для этого транка на вышестоящем домене, задается строкой до 31 символа. |
| 6 | Задание аутентификационного пароля | `esr(config-pbx-reg-server)# authentication password <password>` | <password> – пароль для этого гранка на вышестоящем домене, задается строкой до 16 символов. |
| 7 | Применение SIP - профиля для транка | `esr(config-pbx-reg-server)# profile <PROFILE>` | <PROFILE> – имя SIP профиля, используемое для данного транка, задается строкой до 31 символа. |
| 8 | Выбор транспортного протокола (не обязательно ) | `esr(config-pbx-reg-server)# protocol {tcp \| udp }` | По умолчанию используется udp. |
| 9 | Активация транка | `esr(config-pbx-reg-server)# enable` | |

## 13.6 Пример настройки VoIP

**Задача**:

Подключить аналоговые телефонные аппараты и факс-модемы к IP-сети посредством маршрутизатора ESR. В качестве proxy-сервера и сервера регистрации выступает SIP-сервер, находящийся на ESR.

**Решение:**


Настройка SIP-профиля:

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

Настройка основного SIP proxy-сервера и сервера регистрации:

```
esr(config-sip-profile)# proxy primary
```

Настройка адреса SIP proxy-сервера (в качестве SIP proxy-сервера использовать встроенный SIP-сервер):

```
esr(config-voip-sip-proxy)# ip address proxy-server 192.0.2.5
```

Настройка порта SIP proxy-сервера:

```
esr(config-voip-sip-proxy)# ip port proxy-server 5080
```

Если используется стандартный порт 5060, то его можно не указывать.

Если необходимо использовать регистрацию, то необходимо выполнить следующие пункты:

Настройка адреса сервера регистрации (в качестве сервера регистрации использовать встроенный SIP-сервер):

```
esr(config-voip-sip-proxy)# ip address registration-server 192.0.2.5
```

Настройка порта сервера регистрации:

```
esr(config-voip-sip-proxy)# ip port registration-server 5080
```

Если используется стандартный порт 5060, то его можно не указывать.

Активация регистрации:

```
esr(config-voip-sip-proxy)# registration
```

Активация proxy-сервера и сервера регистрации:

```
esr(config-voip-sip-proxy)# enable
```

На этом конфигурация SIP proxy-сервера и сервера регистрации закончена:

```
esr(config-voip-sip-proxy)# exit
```

Далее продолжается настройка SIP-профиля.

⚠ Если в качестве SIP proxy и сервера регистрации используется встроенный SIP-сервер, необходимо произвести его настройку согласно документу «Настройка SIP-сервера на маршрутизаторах серии ESR: ESR-12V, ESR-12VF, ESR-14VF».

Настройка SIP-домена:

```
esr(config-sip-profile)# sip-domain address sipdomain.com
```

Если необходимо использовать SIP Domain для регистрации:

```
esr(config-sip-profile)# sip-domain registration enable
```

В такой конфигурации все вызовы будут направлены SIP proxy-серверу. Если необходимо указать другое направление для исходящих вызовов, то необходимо проделать следующее:

Создать план нумерации, см. раздел Пример настройки плана нумерации.

Далее созданный план маршрутизации, необходимо присвоить SIP-профилю:

```
esr(config)# sip profile 1
esr(config-sip-profile)# dialplan pattern firstDialplan
```

На этом настройка плана нумерации для SIP-профиля закончена.

Активация SIP-профиля:

```
esr-12v(config-sip-profile)# enable
```

На этом минимально необходимая настройка SIP-профиля закончена:

```
esr(config-sip-profile)# exit
```

Следующим этапом является настройка абонентских портов:

```
esr(config)# interface voice-port 1
```

Указать абонентский номер:

```
esr(config-voice-port-fxs)# sip user phone 4101
```

Указать отображаемое имя:

```
esr(config-voice-port-fxs)# sip user display-name user-one
```

Используемый SIP-профиль:

```
esr(config-voice-port-fxs)# profile sip 1
```

Настройка логина и пароля для аутентификации:

```
esr(config-voice-port-fxs)# authentication name login-4101
esr(config-voice-port-fxs)# authentication password superpassword
```

На этом минимальная настройка абонентского порта закончена:

```
esr(config-voice-port-fxs)# exit
```

## 13.7 Пример настройки плана нумерации

**Задача:**

Настроить план нумерации так, чтобы вызовы на локальных (подключенных к данному ESR-12V) коммутировались локально, а вызовы на все остальные направления через SIP-proxy.

**Решение:**

Создать план нумерации:

```
esr(config)# dialplan pattern firstDialplan
```

План нумерации задается при помощи регулярных выражений:

```
esr(config-dial-ruleset)# pattern "<regular expressions>"
```

Для задачи, обозначенной выше "<*regular* expressions>" будет иметь вид:

**“S5, L5 (410[1-3]@{local} | [xABCD*#].S)”**

где:

**410[1-3]@{ local}** – вызовы на номера 4101, 4102, 4103 будут коммутироваться локально;

**[ xABCD*#]. S** – вызовы на все остальные номера будут направлены к SIP-прокси.

Активировать план нумерации:

```
esr(config-dial-ruleset)# enable
```

Настройка плана нумерации закончена.

```
esr(config-dial-ruleset)# exit
```

Структура регулярного выражения:

**Sxx, Lxx ( ),**

где:

**xx** – произвольные значения таймеров S и L;

**()** – границы плана нумерации.

Основой являются обозначения для записи последовательности набранных цифр. Последовательность цифр записывается с помощью нескольких обозначений: цифры, набираемые с клавиатуры телефона: 0, 1, 2, 3, ..., 9, # и *.

Использование символа # в плане нумерации может блокировать завершение набора с помощью этой клавиши!

Последовательность цифр, заключённая в квадратные скобки, соответствует любому из заключённых в скобки символу.

- Пример: ([1239]) – соответствует любой из цифр 1, 2, 3 или 9.
  Через тире может быть указан диапазон символов. Чаще всего используется внутри квадратных скобок.
- Пример 1: (1-5) – любая цифра от 1 до 5.
- Пример 2: ([1-39]) – пример из предыдущего пункта с иной формой записи.
  Символ X соответствует любой цифре от 0 до 9.
- Пример: (1XX) – любой трёхзначный номер, начинающийся на 1.
  «.» – повторение предыдущего символа от 0 до бесконечности раз.
  «+» – повторение предыдущего символа от 1 до бесконечности раз.
  {a,b} – повторение предыдущего символа от a до b раз;
  {a,} – повторение предыдущего символа не меньше a раз;
  {,b} – повторение предыдущего символа не больше b раз.
- Пример: (810X.) – международный номер с любым количеством цифр.
  Настройки, влияющие на обработку плана нумерации:
- Interdigit Long Timer (буква «L» в записи плана нумерации) – время ожидания ввода следующей цифры в том случае, если нет шаблонов, подходящих под набранную комбинацию;
- Interdigit Short Timer (буква «S» в записи плана нумерации) – время ожидания ввода следующей цифры, если с набранной комбинацией полностью совпадает хотя бы один шаблон и при этом имеется еще хотя бы один шаблон, до полного совпадения с которым необходимо осуществить донабор номера.

Дополнительные возможности:

1. Замена набранной последовательности
   Синтаксис: *<arg1:arg2>*
   Данная возможность позволяет заменить набранную последовательность на любую последовательность набираемых символов. При этом второй аргумент должен быть указан определённым значением, оба аргумента могут быть пустыми.
   - Пример: (<83812:> XXXXXX) – данная запись будет соответствовать набранным цифрам 83812, но эта последовательность будет опущена и не будет передана на SIP-сервер.
2. Вставка тона в набор
   При выходе на межгород (в офисных станциях – на город) привычно слышать ответ станции, что можно реализовать вставкой запятой в нужную позицию последовательности цифр.
   - Пример: (8, 770) – при наборе номера 8770 после цифры 8 будет выдан непрерывный тон.
3. Запрет набора номера
   Если в конце шаблона номера добавить восклицательный знак ‘!’, то набор номеров, соответствующих шаблону, будет заблокирован.
   - Пример: (8 10X xxxxxxx ! | 8 xxx xxxxxxx ) – выражение разрешает набор только междугородних номеров и исключает международные вызовы.
4. Замена значений таймеров набора номера
   Значения таймеров могут быть назначены как для всего плана нумерации, так и для определённого шаблона. Буква «S» отвечает за установку *«Interdigit Short Timer»* , а «L» – за *«Interdigit Long Timer»* . Значения таймеров может быть указано для всех шаблонов в плане нумерации, если значения перечислены до открывающейся круглой скобки.
   - Пример: S4 (8XXX.) или S4,L8 (XXX)
     Если эти значения указаны только в одной из последовательностей, то действуют только для неё. Также в этом случае не надо ставить двоеточие между ключом и значением таймаута, значение может быть расположено в любом месте шаблона.
   - Пример: (S4 8XXX. | XXX) или ([1-5] XX S0) – запись вызовет мгновенную передачу вызова при наборе трехзначного номера, начинающегося на 1,2, … , 5.
5. Набор по прямому адресу (IP Dialing)
   Символ «@», поставленный после номера, означает, что далее будет указан адрес сервера, на который будет отправлен вызов на набранный номер. Рекомендуется использовать *«IP Dialing»*, а

также приём и передачу вызовов без регистрации *(« Call Without Reg », « Answer Without Reg »*). Это может помочь в случае отказа сервера.
Кроме того, формат адреса с IP Dialing может быть использован в номерах, предназначенных для переадресации звонков.

- Пример 1: ( 8 xxx xxxxxxx ) – 11-значный номер, начинающийся на 8.
- Пример 2: ( 8 xxx xxxxxxx | <:8495> xxxxxxx ) – 11-значный номер, начинающийся на 8, если введён семизначный, то добавить к передаваемому номеру 8495.
- Пример 3: (0[123] | 8 [2-9]xx [2-9]xxxxxx) – набор номеров экстренных служб, а так же некоторого странного набора междугородних номеров.
- Пример 4: (S0 <:82125551234>) – быстрый набор указанного номера, аналог режима «Hotline» на других шлюзах.
- Пример 5: (S5 <:1000> | xxxx) – данный план нумерации позволяет набрать любой номер, состоящий из цифр, а если ничего не введено в течение 5 секунд, вызвать номер 1000 (допустим, это секретарь).
- Пример 6: (8, 10x.|1xx@10.110.60.51:5060) – данный план нумерации позволяет набирать номера начинающиеся на 810 и содержащие как минимум одну цифру после "810". После ввода 8 будет выдан сигнал "ответ станции". А также набор трехзначных номеров, начинающихся на "1", Invite на которые будет отправлен на IP-адрес 10.110.60.51 и порт 5060.
- Пример 7: (S3 *xx#|#xx#|#xx#|*xx*x+#) – управление и использование ДВО.
  Иногда может потребоваться совершать звонки локально внутри устройства. При этом, если IP-адрес устройства не известен или периодически изменяется, удобно использовать в качестве адреса сервера зарезервированное слово «{local}», что означает отправку соответствующей последовательности цифр на собственный адрес устройства.
- Пример: (123@{local}) – вызов на номер 123 будет обработан локально внутри устройства.

## 13.8 Настройка FXO-порта

**Задача:**

Добавить возможность совершения вызова абонента ТфОП через FXO-порт ESR-12V.

**Решение:**

Активировать FXO-порт:

```
esr(config)# interface voice-port 4
```

Указать номер FXO-порта, он же префикс выхода на ТфОП:

```
esr(config-voice-port-fxo)# sip user phone 9
```

Указать UDP-порт, с которого и на который FXO-комплект будет отправлять и принимать SIP-сообщения:

```
esr(config-voice-port-fxo)# sip port 5064
```

Указать отображаемое имя:

```
esr(config-voice-port-fxo)# sip user display-name user-one
```

Настройка логина и пароля для аутентификации:

```
esr(config-voice-port-fxo)# authentication name login-9
esr(config-voice-port-fxo)# authentication password superpassword
```

Назначить SIP-профиль FXO-порту:

```
esr(config-voice-port-fxo)# profile sip 1
```

Разрешить передачу номера в ТфОП:

```
esr(config-voice-port-fxo)# pstn transmit-number
```

Запретить передачу префикса:

```
esr(config-voice-port-fxo)# no pstn transmit-prefix
```

Для работы исходящих вызовов необходимо в настройках плана нумерации указать следующее правило, которое означает, что исходящие вызовы на номера имеющие префикс 9, маршрутизируются локально на FXO-комплект:

**9x.@{local}:5064**

На этом минимальная настройка исходящих вызовов на ТфОП закончена. Для того чтобы совершить вызов в ТфОП, нужно набрать номер вызываемого абонента с указанным префиксом (телефонный номер FXO-комплекта).

Для того чтобы принимать вызовы с ТфОП необходимо выбрать абонента, на которого будут поступать все вызовы их ТфОП, допустим, это будет абонент с номером 305.

Активировать услугу «Hostline PSTN to IP»:

```
esr(config-voice-port-fxo)# hotline ipt
```

Указать номер абонента, который будет получать вызовы с ТфОП:

```
esr(config-voice-port-fxo)# hotline number ipt 305
```

# 14 Часто задаваемые вопросы

- **Не удалось получить маршруты по BGP и/или OSPF , сконфигурированных в VRF . Соседство успешно устанавливается, но в записи маршрутов в RIB отказано %ROUTING-W-KERNEL: Can not install route. Reached the maximum number of BGP routes in the RIB**
  Необходимо выделить ресурс RIB для VRF, по умолчанию он равен нулю. Делаем это в режиме конфигурирования VRF:

```
esr(config)# ip vrf <NAME>
esr(config-vrf)# ip protocols ospf max-routes 12000
esr(config-vrf)# ip protocols bgp max-routes 1200000
esr(config-vrf)# end
```

- **Закрываются сессии SSH/Telnet проходящие через маршрутизатор ESR.**
  Для поддержания сессии активной необходимо настроить передачу keepalive пакетов. Опция отправки keepalive настраивается в клиенте SSH, например, для клиента PuTTY раздел “Соединение”.
  В свою очередь, на маршрутизаторе можно выставить время ожидания до закрытия неактивных сессий TCP (в примере выставлен 1 час):

```
esr(config)# ip firewall sessions tcp-estabilished-timeout 3600
```

- **На интерфейсе был отключен firewall ( ip firewall disable ), после внесения этого интерфейса в security zone , удаления из конфигурации ip firewall disable и применения изменений – доступ для активных сессий с данного порта не закрылся, согласно правилам security zone - pair .**
  Изменения в конфигурации Firewall будут действовать только для новых сессий, сброса активных сессий в Firewall не происходит. Отчистить активные сессии в firewall можно командой:

```
esr# clear ip firewall session
```

- **Не поднимается LACP на портах XG ESR-1000/1200/1500/1700**
  По умолчанию на port-channel режим speed 1000M, необходимо выставить speed 10G.

```
esr(config)# interface port-channel 1
esr(config-port-channel)# speed 10G
```

- **Как полностью очистить конфигурация ESR, и как сбросить на заводскую конфигурацию?**
  Очистка конфигурации происходит путем копирования пустой конфигурации в candidate-config и применения его в running-config.

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

  Процесс сброса на заводскую конфигурацию аналогичен.

```
esr# copy system:factory-config system:candidate-config
```

- **Как привязать subinterface к созданным VLAN ?**
  При создании саб-интерфейса, VLAN создается и привязывается автоматически (прямая зависимость индекс sub – VID).

```
esr(config)# interface gigabitethernet 1/0/1.100
```

  После применения можно наблюдать информационные сообщения:

```
2016-07-14T012:46:24+00:00 %VLAN: creating VLAN 100
```

- **Есть ли функционал в маршрутизаторах серии ESR для анализа трафика?**
  В маршрутизаторах серии ESR реализована возможность анализировать трафик на интерфейсах из CLI. Сниффер запускается командой monitor.

```
esr# monitor gigabitethernet 1/0/1
```

- **Как настроить ip prefix-list 0.0.0.0/0?**
  Ниже приведен пример конфигурации префикс листа, разрешающего прием маршрута по умолчанию.

```
esr(config)# ip prefix-list eltex
esr(config-pl)# permit default-route
```

- **Проблема прохождения асинхронного трафика .**
  В случае организации сети с асинхронной маршрутизацией, Firewall будет запрещать "неправильный (ошибочный)" входящий трафик (не открывающий новое соединение и не принадлежащий никакому установленному соединению) из соображений безопасности. Разрешающее правило в Firewall не решит поставленную задачу для подобных схем. Решить задачу можно, отключив Firewall на входном интерфейсе:

```
esr(config-if-gi)# ip firewall disable
```

- **Как можно сохранить локальную копию конфигурации маршрутизатора?**
  Если необходимо скопировать текущую running или candidate -конфигурацию на самом маршрутизаторе – можно воспользоваться командой copy с указанием в качестве источника копирования "system:running-config" или " system:candidate-config", а в качестве назначения – файл в разделе "flash:data/"

```
esr# copy system:candidate-config flash:data/temp.txt
```

  Также, существует возможность копирования ранее сохраненных конфигурационных файлов (автоматически из раздела flash:backup/ или вручную из раздела flash:data/) в candidate-конфигурацию:

```
esr# copy flash:data/temp.txt system:candidate-config
esr# copy flash:backup/config_20190918_164455 system:candidate-config
```

# 15 Техническая поддержка ESR

Для получения технической консультации по вопросам эксплуатации оборудования ООО «Предприятие «ЭЛТЕКС» Вы можете обратиться в Сервисный центр компании.

Форма обратной связи на сайте: http://eltex-co.ru/support/

Sevicedesk: https://servicedesk.eltex-co.ru/

На официальном сайте компании Вы можете найти техническую документацию и программное обеспечение для продукции ООО «Предприятие «ЭЛТЕКС», обратиться к базе знаний, оставить интерактивную заявку или проконсультироваться у инженеров Сервисного центра на техническом форуме:

Официальный сайт компании: http://eltex-co.ru/

База знаний: https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base

Центр загрузок: http://eltex-co.ru/support/downloads