Сервисные маршрутизаторы серии ESR

ESR-10, ESR-12V, ESR-12VF, ESR-15, ESR-15R, ESR-15VF, ESR-20, ESR-21, ESR-30, ESR-31, ESR-100, ESR-200, ESR-1000, ESR-1200, ESR-1500, ESR-1511, ESR-1511 rev.B, ESR-1700, ESR-3100, ESR-3150, ESR-3200, ESR-3200L, ESR-3250, ESR-3300, ESR-3350

Руководство по эксплуатации

Версия ПО 1.40

Содержание

1 Введение ... 15
1.1 Аннотация ... 15
1.2 Целевая аудитория ... 15
1.3 Условные обозначения ... 16
1.4 Примечания и предупреждения ... 16
2 Описание изделий ... 17
2.1 Назначение ... 17
2.2 Функции ... 18
2.2.1 Функции интерфейсов ... 18
2.2.2 Функции при работе с MAC-адресами ... 18
2.2.3 Функции второго уровня сетевой модели OSI ... 19
2.2.4 Функции третьего уровня сетевой модели OSI ... 19
2.2.5 Функции туннелирования трафика ... 20
2.2.6 Функции управления и конфигурирования ... 21
2.2.7 Функции сетевой защиты ... 22
2.3 Основные технические характеристики ... 23
2.4 Конструктивное исполнение ... 42
2.4.1 Конструктивное исполнение ESR-3350 ... 42
2.4.2 Конструктивное исполнение ESR-3300 ... 44
2.4.3 Конструктивное исполнение ESR-3250 ... 47
2.4.4 Конструктивное исполнение ESR-3200L ... 49
2.4.5 Конструктивное исполнение ESR-3200 ... 52
2.4.6 Конструктивное исполнение ESR-3150 ... 54
2.4.7 Конструктивное исполнение ESR-3100 ... 56
2.4.8 Конструктивное исполнение ESR-1700 ... 59
2.4.9 Конструктивное исполнение ESR-1511 rev.B, ESR-1511, ESR-1500 ... 61
2.4.10 Конструктивное исполнение ESR-1200, ESR-1000 ... 66
2.4.11 Конструктивное исполнение ESR-200, ESR-100 ... 70
2.4.12 Конструктивное исполнение ESR-31 ... 72
2.4.13 Конструктивное исполнение ESR-21 ... 74
2.4.14 Конструктивное исполнение ESR-30, ESR-20 ... 76
2.4.15 Конструктивное исполнение ESR-15VF ... 80
2.4.16 Конструктивное исполнение ESR-15R ... 82
2.4.17 Конструктивное исполнение ESR-15 ... 84
2.4.18 Конструктивное исполнение ESR-12VF ... 87

2.4.19 Конструктивное исполнение ESR-12V ... 89
2.4.20 Конструктивное исполнение ESR-10 ... 91
2.4.21 Световая индикация ... 94
2.5 Комплект поставки ... 112
3 Установка и подключение ... 117
3.1 Установка устройства в стойку (кроме ESR-3300, ESR-3350) ... 117
3.2 Установка ESR-3300, ESR-3350 в стойку ... 118
3.3 Подключение к vESR ... 120
3.4 Установка модулей питания ESR-31, 1000, ESR-1200, ESR-1500, ESR-1511, ESR-1511 rev.B, ESR-1700, ESR-3100, ESR-3150, ESR-3200, ESR-3200L, ESR-3250, ESR-3300, ESR-3350 ... 120
3.5 Подключение питающей сети ... 121
3.6 Установка и удаление SFP-трансиверов ... 122
3.6.1 Установка трансивера ... 122
3.6.2 Удаление трансивера ... 122
4 Интерфейсы управления ... 123
4.1 Интерфейс командной строки (CLI) ... 123
4.2 Типы и порядок именования интерфейсов маршрутизатора ... 124
4.3 Типы и порядок именования туннелей маршрутизатора ... 128
5 Начальная настройка маршрутизатора ... 130
5.1 Заводская конфигурация маршрутизатора ESR ... 130
5.1.1 Описание заводской конфигурации ... 130
5.2 Подключение и конфигурирование маршрутизатора ... 132
5.2.1 Подключение к маршрутизатору ... 132
5.2.2 Применение изменения конфигурации ... 133
5.2.3 Базовая настройка маршрутизатора ... 133
6 Рекомендации по безопасной настройке ... 138
6.1 Общие рекомендации ... 138
6.2 Настройка системы логирования событий ... 139
6.2.1 Рекомендации ... 139
6.2.2 Предупреждения ... 139
6.2.3 Пример настройки ... 139
6.3 Настройка политики использования паролей ... 140
6.3.1 Рекомендации ... 140
6.3.2 Пример настройки ... 140
6.4 Настройка политики AAA ... 141
6.4.1 Рекомендации ... 141
6.4.2 Предупреждения ... 141

6.4.3 Пример настройки ... 142
6.5 Настройка удалённого управления ... 143
6.5.1 Рекомендации ... 143
6.5.2 Пример настройки ... 143
6.6 Настройка механизмов защиты от сетевых атак ... 144
6.6.1 Рекомендации ... 144
6.6.2 Пример настройки ... 145
7 Управление интерфейсами ... 146
7.1 Настройка физического интерфейса ... 146
7.1.1 Алгоритм настройки ... 146
7.1.2 Алгоритм настройки режима L3 ... 147
7.1.3 Пример настройки в режиме L3 ... 148
7.2 Настройка терминации на саб-интерфейсе ... 149
7.2.1 Алгоритм настройки ... 149
7.2.2 Пример настройки саб-интерфейса ... 152
7.3 Настройка терминации на Q-in-Q интерфейсе ... 152
7.3.1 Алгоритм настройки ... 152
7.3.2 Пример настройки Q-in-Q интерфейса ... 155
7.4 Настройка USB-модемов ... 156
7.4.1 Алгоритм настройки USB-модемов ... 156
7.4.2 Пример настройки ... 159
7.5 Настройка PPP через E1 ... 160
7.5.1 Алгоритм настройки ... 160
7.5.2 Пример конфигурации ... 163
7.6 Настройка MLPPP ... 165
7.6.1 Алгоритм настройки ... 165
7.6.2 Пример настройки ... 168
7.6.3 Фрагментация трафика ... 170
7.7 Настройка AUX ... 171
7.7.1 Алгоритм настройки ... 171
7.7.2 Примеры настроек ... 173
7.7.3 Схемы распайки переходников ... 179
8 Управление туннелированием ... 181
8.1 Настройка GRE-туннелей ... 181
8.1.1 Алгоритм настройки ... 181
8.1.2 Пример настройки IP-GRE-туннеля ... 187
8.2 Настройка DMVPN ... 189
8.2.1 Алгоритм настройки ... 189

8.2.2 Пример настройки 1 ... 192
8.2.3 Пример настройки 2 ... 198
8.3 Настройка L2TPv3-туннелей ... 204
8.3.1 Алгоритм настройки ... 204
8.3.2 Пример настройки L2TPv3-туннеля ... 207
8.4 Настройка IPsec VPN ... 209
8.4.1 Алгоритм настройки Route-based IPsec VPN ... 209
8.4.2 Пример настройки Route-based IPsec VPN ... 218
8.4.3 Алгоритм настройки Policy-based IPsec VPN ... 223
8.4.4 Пример настройки Policy-based IPsec VPN с аутентификацией по общему известному ключу ... 232
8.4.5 Пример настройки Policy-based IPsec VPN с аутентификацией сертификатам X.509, выписываемых PKI-клиентом ... 236
8.4.6 Алгоритм настройки Remote Access IPsec VPN ... 242
8.4.7 Пример настройки Remote Access IPsec VPN ... 253
8.4.8 Пример настройки DPD (Dead Peer Detection) ... 258
8.5 Настройка LT-туннелей ... 259
8.5.1 Алгоритм настройки ... 259
8.5.2 Пример настройки ... 261
9 Управление функциями второго уровня (L2) ... 263
9.1 Настройка физического интерфейса ... 264
9.1.1 Алгоритм настройки ... 264
9.1.2 Пример настройки режима L2 ... 265
9.2 Настройка VLAN ... 266
9.2.1 Алгоритм настройки ... 266
9.2.2 Удаление и назначение VLAN ... 269
9.2.3 Пример настройки 1 ... 269
9.2.4 Пример настройки 2 ... 270
9.2.5 Разрешение обработки VLAN в тегированном и нетегированном режимах ... 272
9.2.6 Пример настройки 1 ... 272
9.2.7 Пример настройки 2 ... 273
9.2.8 Пример настройки Private Vlan ... 274
9.3 Настройка LLDP ... 276
9.3.1 Алгоритм настройки ... 276
9.3.2 Пример настройки ... 277
9.4 Настройка LLDP MED ... 278
9.4.1 Алгоритм настройки ... 278
9.4.2 Пример настройки Voice VLAN ... 280

9.5 Настройка протоколов семейства STP ... 281
9.5.1 Настройка протоколов STP и RSTP ... 281
9.5.2 Настройка протокола STP и RSTP в рамках bridge ... 284
9.5.3 Настройка протокола MSTP ... 290
9.5.4 Настройка BPDU Guard ... 293
9.6 Настройка Bridge ... 295
9.6.1 Алгоритм настройки ... 295
9.6.2 Пример настройки bridge для VLAN и L2TPv3-туннеля ... 300
9.6.3 Пример настройки bridge для VLAN ... 301
9.6.4 Пример настройки добавления/удаления второго VLAN-тега ... 302
9.7 Настройка Dual-Homing ... 303
9.7.1 Алгоритм настройки ... 303
9.7.2 Пример настройки ... 304
9.8 Настройка зеркалирования (SPAN/RSPAN) ... 305
9.8.1 Алгоритм настройки ... 305
9.8.2 Пример настройки ... 306
9.9 Настройка LACP ... 306
9.9.1 Алгоритм настройки ... 307
9.9.2 Пример настройки ... 310
10 Управление QoS ... 312
10.1 Базовый QoS ... 312
10.1.1 Алгоритм настройки ... 312
10.1.2 Пример настройки ... 316
10.1.3 Пример расчета пропускной способности для взвешенных очередей ... 317
10.2 Расширенный QoS ... 319
10.2.1 Алгоритм настройки ... 319
10.2.2 Пример настройки ... 331
10.2.3 Механизм работы полисера ... 334
10.3 MPLS QoS ... 335
11 Управление маршрутизацией ... 336
11.1 Политика фильтрации маршрутной информации ... 337
11.1.1 Протокол RIP ... 340
11.1.2 Протокол OSPF ... 341
11.1.3 Протокол IS-IS ... 342
11.1.4 Протокол iBGP ... 342
11.1.5 Протокол eBGP ... 343
11.2 Конфигурирование статических маршрутов ... 344
11.2.1 Алгоритм настройки ... 344

11.2.2 Пример настройки ... 345
11.3 Конфигурирование статических multipath-маршрутов ... 347
11.3.1 Алгоритм настройки ... 347
11.3.2 Пример настройки ... 349
11.4 Настройка RIP ... 351
11.4.1 Алгоритм настройки ... 351
11.4.2 Пример настройки ... 357
11.5 Настройка RIPng ... 359
11.5.1 Алгоритм настройки ... 359
11.5.2 Пример настройки ... 364
11.6 Настройка OSPF ... 365
11.6.1 Алгоритм настройки ... 365
11.6.2 Пример настройки ... 378
11.6.3 Пример настройки OSPF stub area ... 379
11.6.4 Пример настройки Virtual link ... 380
11.7 Настройка BGP ... 381
11.7.1 Алгоритм настройки ... 381
11.7.2 Пример настройки ... 397
11.7.3 Политика выбора лучшего маршрута в протоколе BGP ... 399
11.7.4 Условное анонсирование маршрутной информации (Conditional Advertisement) ... 402
11.7.5 Быстрая деактивация пиринговых сессий ... 414
11.7.6 Настройка политик маршрутизации Route-map ... 421
11.7.7 Конфедерация ... 444
11.8 Настройка Policy-Based Routing ... 453
11.8.1 Алгоритм настройки ... 454
11.8.2 Пример настройки ... 455
11.9 Настройка BFD ... 456
11.9.1 Настройка таймеров ... 459
11.9.2 Алгоритм настройки ... 460
11.9.3 Пример настройки ... 466
11.10 Настройка VRF ... 468
11.10.1 Алгоритм настройки ... 468
11.10.2 Пример настройки ... 470
11.11 Настройка MultiWAN ... 471
11.11.1 Алгоритм настройки ... 471
11.11.2 Пример настройки ... 474
11.12 Настройка IS-IS ... 476

11.12.1 Алгоритм настройки ... 476
11.12.2 Пример настройки ... 485
12 Управление технологией MPLS ... 487
12.1 Настройка протокола LDP ... 488
12.1.1 Алгоритм настройки ... 488
12.1.2 Пример настройки ... 490
12.2 Конфигурирование параметров сессии в протоколе LDP ... 492
12.2.1 Алгоритм настройки параметров Hello holdtime и Hello interval в глобальной конфигурации LDP ... 495
12.2.2 Алгоритм настройки параметров Hello holdtime и Hello interval для address family ... 495
12.2.3 Алгоритм настройки параметра Keepalive holdtime в глобальной конфигурации LDP ... 495
12.2.4 Алгоритм настройки параметра Keepalive holdtime для определенного соседа ... 496
12.2.5 Пример настройки ... 496
12.3 Конфигурирование параметров сессии в протоколе targeted-LDP ... 497
12.3.1 Алгоритм настройки параметров Hello holdtime, Hello interval и Keepalive holdtime для процесса LDP ... 499
12.3.2 Алгоритм настройки параметров Hello holdtime, Hello interval и Keepalive holdtime для определенного соседа ... 500
12.3.3 Пример настройки ... 500
12.4 Настройка фильтрации LDP-меток ... 501
12.4.1 Метод на основе Advertise-labels ... 501
12.4.2 Метод на основе Prefix-list ... 503
12.5 Настройка сервиса L2VPN Martini mode ... 505
12.5.1 Алгоритм настройки L2VPN VPWS ... 506
12.5.2 Пример настройки L2VPN VPWS ... 507
12.5.3 Алгоритм настройки L2VPN VPLS ... 510
12.5.4 Пример настройки L2VPN VPLS ... 512
12.6 Настройка сервиса L2VPN Kompella mode (BGP Autodiscovery and Signaling) ... 517
12.6.1 Алгоритм настройки L2VPN VPLS ... 517
12.6.2 Пример настройки L2VPN VPLS ... 519
12.7 Настройка сервиса L3VPN ... 533
12.7.1 Алгоритм настройки ... 534
12.7.2 Пример настройки ... 536
12.8 Балансировка трафика MPLS ... 551
12.8.1 Пример настройки ... 553
12.9 Работа с бридж-доменом в рамках MPLS ... 553
12.10 Назначение MTU при работе с MPLS ... 555

12.11 Inter-AS Option A ... 561
12.11.1 L2VPN ... 561
12.11.2 L3VPN ... 572
12.12 Inter-AS Option B ... 587
12.12.1 L3VPN ... 587
12.13 Inter-AS Option C ... 601
12.13.1 L3VPN ... 602
12.14 MPLS over GRE ... 605
12.14.1 L2VPN ... 605
12.14.2 L3VPN ... 612
13 Управление безопасностью ... 621
13.1 Настройка AAA ... 622
13.1.1 Алгоритм настройки локальной аутентификации ... 622
13.1.2 Алгоритм настройки AAA по протоколу RADIUS ... 628
13.1.3 Алгоритм настройки AAA по протоколу TACACS ... 631
13.1.4 Алгоритм настройки AAA по протоколу LDAP ... 636
13.1.5 Пример настройки аутентификации по Telnet через RADIUS-сервер ... 640
13.2 Настройка привилегий команд ... 641
13.2.1 Алгоритм настройки ... 641
13.2.2 Пример настройки привилегий команд ... 642
13.3 Настройка логирования и защиты от ARP-spoofing атак ... 642
13.3.1 Алгоритм настройки ... 642
13.3.2 Пример настройки защиты от ARP-spoofing атак ... 642
13.4 Настройка логирования и защиты от сетевых атак ... 643
13.4.1 Алгоритм настройки ... 643
13.4.2 Описание механизмов защиты от атак ... 646
13.4.3 Пример настройки логирования и защиты от сетевых атак ... 649
13.5 Конфигурирование Firewall ... 651
13.5.1 Алгоритм настройки ... 651
13.5.2 Пример настройки Firewall ... 662
13.5.3 Пример настройки Firewall по доменным именам ... 665
13.5.4 Пример настройки фильтрации приложений (DPI) ... 667
13.5.5 Пример настройки Firewall по расписанию ... 669
13.6 Настройка списков доступа (IP ACL) ... 671
13.6.1 Алгоритм настройки ... 671
13.6.2 Пример настройки списка доступа ... 674
13.7 Настройка списков доступа (MAC ACL) ... 674
13.7.1 Алгоритм настройки ... 675

13.7.2 Пример настройки списка доступа ... 676
13.8 Проксирование HTTP/HTTPS-трафика ... 677
13.8.1 Алгоритм настройки ... 677
13.8.2 Пример настройки HTTP-прокси ... 680
13.9 Настройка IPS/IDS ... 684
13.9.1 Алгоритм базовой настройки ... 684
13.9.2 Алгоритм настройки автообновления правил IPS/IDS из внешних источников ... 687
13.9.3 Рекомендуемые открытые источники обновления правил ... 688
13.9.4 Пример настройки IPS/IDS с автообновлением правил ... 690
13.9.5 Алгоритм настройки базовых пользовательских правил ... 691
13.9.6 Пример настройки базовых пользовательских правил ... 701
13.9.7 Алгоритм настройки расширенных пользовательских правил ... 703
13.9.8 Пример настройки расширенных пользовательских правил ... 704
13.10 Настройка взаимодействия с Eltex Distribution Manager ... 704
13.10.1 Алгоритм базовой настройки ... 705
13.10.2 Пример настройки ... 711
13.11 Настройка сервиса контентной фильтрации ... 715
13.11.1 Алгоритм базовой настройки ... 715
13.11.2 Пример настройки правил контентной фильтрации ... 723
14 Управление сертификатами и ключами ... 727
14.1 Автоматическое распространение ключей и сертификатов X.509 ... 727
14.1.1 Общее описание инфраструктуры открытых ключей ... 727
14.1.2 Планирование инфраструктуры открытых ключей ... 728
14.1.3 Настройка PKI-сервера в роли корневого удостоверяющего центра ... 729
14.1.4 Настройка PKI-клиента ... 737
14.1.5 Процесс автоматического перевыпуска сертификата PKI-клиента ... 745
14.1.6 Процесс автоматического перевыпуска сертификата PKI-сервера ... 747
14.2 Ручная генерация и распространение ключей и сертификатов X.509 ... 751
14.2.1 Алгоритм генерации ключей и запросов на сертификацию ... 751
14.2.2 Пример ручного выпуска сертификата через внешний удостоверяющий центр ... 755
15 Управление резервированием ... 761
15.1 Настройка VRRP ... 761
15.1.1 Алгоритм настройки ... 761
15.1.2 Пример настройки 1 ... 765
15.1.3 Пример настройки 2 ... 766
15.2 Настройка tracking ... 768

15.2.1 Алгоритм настройки ... 768
15.2.2 Пример настройки ... 775
15.3 Настройка Firewall/NAT failover ... 777
15.3.1 Алгоритм настройки ... 778
15.3.2 Пример настройки ... 779
15.4 Настройка DHCP failover ... 784
15.4.1 Алгоритм настройки ... 784
15.4.2 Пример настройки ... 785
16 Управление кластеризацией ... 790
16.1 Настройка кластера ... 790
16.1.1 Алгоритм настройки ... 790
16.1.2 Пример настройки кластера ... 794
16.2 Подключение сервисов ... 801
16.2.1 Настройка System prompt ... 801
16.2.2 Настройка Port-channel U/N ... 805
16.2.3 Настройка MultiWAN ... 809
16.2.4 Настройка IPsec VPN ... 814
16.2.5 Настройка firewall/NAT failover ... 828
16.2.6 Настройка DHCP failover ... 853
16.2.7 Настройка SNMP ... 865
16.2.8 Настройка Source NAT ... 868
16.2.9 Настройка Destination NAT ... 873
16.2.10 Настройка BGP ... 877
16.2.11 Настройка DMVPN ... 890
17 Управление удаленным доступом ... 918
17.1 Настройка сервера удаленного доступа к корпоративной сети по PPTP-протоколу ... 918
17.1.1 Алгоритм настройки ... 918
17.1.2 Пример настройки ... 921
17.2 Настройка сервера удаленного доступа к корпоративной сети по L2TP over IPsec протоколу ... 923
17.2.1 Алгоритм настройки ... 923
17.2.2 Пример настройки ... 927
17.3 Настройка сервера удаленного доступа к корпоративной сети по OpenVPN-протоколу ... 929
17.3.1 Алгоритм настройки ... 929
17.3.2 Пример настройки ... 933
17.4 Настройка сервера удаленного доступа к корпоративной сети по WireGuard-протоколу ... 935

17.4.1 Алгоритм настройки ... 936
17.4.2 Пример настройки ... 938
17.4.3 Пример настройки правил Firewall для совместной работы с WireGuard-сервером ... 940
17.5 Настройка клиента удаленного доступа по протоколу PPPoE ... 941
17.5.1 Алгоритм настройки ... 942
17.5.2 Пример настройки ... 944
17.6 Настройка клиента удаленного доступа по протоколу PPTP ... 946
17.6.1 Алгоритм настройки ... 946
17.6.2 Пример настройки ... 948
17.7 Настройка клиента удаленного доступа по протоколу L2TP ... 949
17.7.1 Алгоритм настройки ... 949
17.7.2 Пример настройки ... 952
17.8 Настройка клиента удаленного доступа по протоколу WireGuard ... 953
17.8.1 Алгоритм настройки ... 953
17.8.2 Пример настройки ... 956
18 Управление сервисами ... 959
18.1 Настройка DHCP-сервера ... 959
18.1.1 Алгоритм настройки ... 959
18.1.2 Пример настройки ... 964
18.2 Конфигурирование Destination NAT ... 965
18.2.1 Алгоритм настройки ... 966
18.2.2 Пример настройки Destination NAT ... 969
18.3 Конфигурирование Source NAT ... 971
18.3.1 Алгоритм настройки ... 972
18.3.2 Пример настройки 1 ... 977
18.3.3 Пример настройки 2 ... 979
18.4 Конфигурирование Static NAT ... 980
18.4.1 Алгоритм настройки ... 980
18.4.2 Пример настройки Static NAT ... 980
18.5 Настройка NTP ... 982
18.5.1 Алгоритм настройки ... 982
18.5.2 Пример настройки ... 985
19 Мониторинг ... 987
19.1 Настройка Netflow ... 987
19.1.1 Алгоритм настройки ... 987
19.1.2 Пример настройки ... 989
19.2 Настройка sFlow ... 990

19.2.1 Алгоритм настройки ... 990
19.2.2 Пример настройки ... 991
19.3 Настройка SNMP ... 992
19.3.1 Алгоритм настройки ... 992
19.3.2 Пример настройки ... 996
19.4 Настройка Zabbix-agent/proxy ... 998
19.4.1 Алгоритм настройки ... 998
19.4.2 Пример настройки zabbix-agent ... 1000
19.4.3 Пример настройки zabbix-server ... 1001
19.5 Настройка Syslog ... 1004
19.5.1 Алгоритм настройки ... 1004
19.5.2 Пример настройки ... 1009
19.6 Проверка целостности ... 1010
19.6.1 Процесс настройки ... 1010
19.6.2 Пример конфигурации ... 1011
19.7 Настройка архивации конфигурации маршрутизатора ... 1011
19.7.1 Процесс настройки ... 1011
19.7.2 Пример конфигурации ... 1012
19.8 Настройка SLA ... 1013
19.8.1 Алгоритм настройки SLA-теста ... 1013
19.8.2 Настройка SLA-responder ... 1022
19.8.3 Пример настройки ICMP-режима тестирования ... 1023
19.8.4 Пример настройки UDP-режима тестирования ... 1024
19.8.5 Алгоритм настройки параметров аутентификации ... 1026
19.8.6 Пример конфигурации UDP-теста с аутентификацией по ключ-строке ... 1032
19.8.7 Пример конфигурации UDP-теста с аутентификацией по связке ключей ... 1034
19.8.8 Настройка пороговых значений ... 1036
19.8.9 Измерение характеристик канала связи ... 1037
20 Управление BRAS (Broadband Remote Access Server) ... 1039
20.1 Алгоритм настройки ... 1039
20.2 Пример настройки с SoftWLC ... 1044
20.3 Пример настройки без SoftWLC ... 1050
21 Управление VoIP ... 1057
21.1 Алгоритм настройки SIP-профиля ... 1057
21.2 Алгоритм настройки FXS/FXO-портов ... 1059
21.3 Алгоритм настройки плана нумерации ... 1060
21.4 Алгоритм настройки PBX-сервера ... 1060
21.5 Алгоритм создания транка регистрации ... 1063

21.6 Пример настройки VoIP ... 1064
21.7 Пример настройки плана нумерации ... 1066
21.8 Настройка FXO-порта ... 1068
21.9 Пример настройки VoIP для регистрации FXS-портов на внешнем SIP-сервере ... 1070
21.10 Пример настройки VoIP на внутреннем pbx-сервере ... 1071
22 Управление лицензированием ... 1074
22.1 Лицензирование через ELM ... 1074
22.1.1 Периодичность обращений к ELM ... 1074
22.1.2 Условия преждевременного сброса лицензии ... 1075
22.1.3 Алгоритм настройки ... 1075
22.1.4 Пример настройки ... 1076
22.2 Файловое лицензирование ... 1077
22.3 Лицензирование в кластере ... 1078
22.3.1 Синхронизация файловых лицензий ... 1078
22.3.2 Установка файловых лицензий ... 1079
23 Автоматическое развертывание ... 1080
23.1 Примеры использования автоматического развертывания ... 1080
23.1.1 Автоматическое развертывание с использованием внешнего DHCP-сервера ... 1080
23.1.2 Алгоритм настройки ... 1080
23.1.3 Пример настройки ... 1080
23.1.4 Автоматическое развертывание с загрузочного носителя ... 1082
23.1.5 Пример настройки ... 1083
23.1.6 Автоматическое развертывание нового юнита в кластере ... 1083
23.1.7 Пример настройки ... 1083
24 Часто задаваемые вопросы ... 1087
25 Приложение A. Packet Flow ... 1090
25.1 Порядок обработки входящего/исходящего трафика сетевыми службами маршрутизаторов ESR ... 1090
25.2 Порядок обработки транзитного трафика сетевыми службами маршрутизаторов ESR ... 1092

1 Введение

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

1.1 Аннотация

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

Сервисные маршрутизаторы 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 по эксплуатации изложены назначение, технические характеристики, конструктивное исполнение, порядок установки, рекомендации по начальной настройке и обновлению программного обеспечения 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 Условные обозначения

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

1.4 Примечания и предупреждения

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

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

Информация содержит справочные данные об использовании устройства.

2 Описание изделий

- Назначение
- Функции
  - Функции интерфейсов
  - Функции при работе с MAC-адресами
  - Функции второго уровня сетевой модели OSI
  - Функции третьего уровня сетевой модели OSI
  - Функции туннелирования трафика
  - Функции управления и конфигурирования
  - Функции сетевой защиты
- Основные технические характеристики
- Конструктивное исполнение
  - Конструктивное исполнение ESR-3350
  - Конструктивное исполнение ESR-3300
  - Конструктивное исполнение ESR-3250
  - Конструктивное исполнение ESR-3200L
  - Конструктивное исполнение ESR-3200
  - Конструктивное исполнение ESR-3150
  - Конструктивное исполнение ESR-3100
  - Конструктивное исполнение ESR-1700
  - Конструктивное исполнение ESR-1511 rev.B, ESR-1511, ESR-1500
  - Конструктивное исполнение ESR-1200, ESR-1000
  - Конструктивное исполнение ESR-200, ESR-100
  - Конструктивное исполнение ESR-31
  - Конструктивное исполнение ESR-21
  - Конструктивное исполнение ESR-30, ESR-20
  - Конструктивное исполнение ESR-15VF
  - Конструктивное исполнение ESR-15R
  - Конструктивное исполнение ESR-15
  - Конструктивное исполнение ESR-12VF
  - Конструктивное исполнение ESR-12V
  - Конструктивное исполнение ESR-10
  - Световая индикация
- Комплект поставки

2.1 Назначение

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

Устройства поддерживают функции межсетевого экрана для защиты сети организации и своей сетевой инфраструктуры, а также сочетают в себе новейшие средства обеспечения безопасности данных, шифрования, аутентификации и защиты от вторжений. Маршрутизаторы содержат в себе средства для программной и аппаратной обработки данных.

2.2 Функции

2.2.1 Функции интерфейсов

В таблице 1 приведен список функций интерфейсов устройства.

Таблица 1 – Функции интерфейсов устройства

Определение полярности подключения кабеля (Auto MDI/MDIX)	Автоматическое определение типа кабеля – перекрестный кабель или кабель прямого подключения. • MDI (Medium Dependent Interface – прямой) – стандарт кабелей для подключения оконечных устройств; • MDIX (Medium Dependent Interface with Crossover – перекрестный) – стандарт кабелей для подключения концентраторов и коммутаторов.
Поддержка обратного давления (Back pressure)	Метод обратного давления используется на полудуплексных соединениях для регулирования потока данных от встречного устройства путем создания коллизий. Метод позволяет избежать переполнения буферной памяти устройства и потери данных.
Агрегирование каналов (LAG, Link aggregation)	Агрегирование (объединение) каналов позволяет увеличить пропускную способность канала связи и повысить его надежность. Маршрутизатор поддерживает статическое и динамическое агрегирование каналов. При динамическом агрегировании используется протокол LACP для управления группой каналов.

2.2.2 Функции при работе с MAC-адресами

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

Таблица 2 – Функции работы с MAC-адресами

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

2.2.3 Функции второго уровня сетевой модели OSI

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

Таблица 3 – Описание функций второго уровня (уровень 2 OSI)

Поддержка VLAN	VLAN (Virtual Local Area Network) – это средство разделения сети на изолированные сегменты на уровне L2. Использование VLAN позволяет повысить устойчивость работы крупных сетей за счет деления их на более мелкие сети, изолировать разнородный трафик данных между собой и решить многие другие задачи. Маршрутизаторы поддерживают различные способы организации VLAN: • VLAN на базе меток пакетов данных, в соответствии с IEEE 802.1Q; • VLAN на базе портов устройства (port-based); • VLAN на базе использования правил классификации данных (policy-based).
Протокол связующего дерева (Spanning Tree Protocol)	Задачей протокола Spanning Tree является исключение избыточных сетевых соединений и приведение топологии сети к древовидной. Основные применения протокола связаны с предотвращением зацикливания сетевого трафика и с организацией резервных каналов связи.

2.2.4 Функции третьего уровня сетевой модели OSI

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

Таблица 4 – Описание функций третьего уровня (Layer 3)

Статические IP-маршруты	Администратор маршрутизатора имеет возможность добавлять и удалять статические записи в таблицу маршрутизации.
Динамическая маршрутизация	Протоколы динамической маршрутизации позволяют устройству обмениваться маршрутной информацией с соседними маршрутизаторами и автоматически составлять таблицу маршрутов. Маршрутизатор поддерживает следующие протоколы: RIPv2, RIPng, OSPFv2, OSPFv3, IS-IS, BGP.
Таблица ARP	ARP (Address Resolution Protocol) – протокол для выяснения соответствия адресов сетевого и канального уровней. Таблица ARP содержит информацию об изученном соответствии. Соответствие устанавливается на основе анализа ответов от сетевых устройств, адреса устройств запрашиваются с помощью широковещательных пакетов.
Клиент DHCP	Протокол DHCP (Dynamic Host Configuration Protocol) даёт возможность автоматизировать управление сетевыми устройствами. Клиент DHCP позволяет маршрутизатору получать сетевой адрес и дополнительные параметры от внешнего DHCP-сервера. Как правило, этот способ используется для получения сетевых настроек оператора публичной сети (WAN).

Сервер DHCP	Сервер DHCP предназначен для автоматизации и централизации конфигурирования сетевых устройств. Размещение DHCP-сервера на маршрутизаторе позволяет получить законченное решение для поддержки локальной сети. DHCP-сервер, входящий в состав маршрутизатора, позволяет назначать IP-адреса сетевым устройствам и передавать дополнительные сетевые параметры – адреса серверов, адреса шлюзов сети и другие необходимые параметры.
DHCP Relay	Функция DHCP Relay предназначена для перенаправления широковещательных DHCP Discover-пакетов из одного широковещательного домена в одноадресные (unicast) DHCP Discover-пакеты в другом широковещательном домене.
Трансляция сетевых адресов (NAT, Network Address Translation)	Трансляция сетевых адресов – это механизм, который позволяет преобразовывать IP-адреса и номера портов транзитных пакетов. Функция NAT позволяет использовать меньшее количество IP-адресов, транслируя несколько IP-адресов внутренней сети в один внешний публичный IP-адрес. Использование NAT позволяет увеличить защищённость локальной сети за счёт скрытия её внутренней структуры. Маршрутизаторы поддерживают следующие варианты NAT: • Source NAT (SNAT) – выполняется замена адреса, а также номера порта источника при прохождении пакета в одну сторону и обратной замене адреса назначения в ответном пакете; • Destination NAT (DNAT) – когда обращения извне транслируются маршрутизатором на компьютер пользователя в локальной сети, имеющий внутренний адрес и потому недоступный извне сети непосредственно (без NAT).

2.2.5 Функции туннелирования трафика

Таблица 5 – Функции туннелирования трафика

Протоколы туннелирования	Туннелирование – это способ преобразования пакетов данных при передаче их по сети, при котором происходит замена, модификация или добавление нового сетевого заголовка пакета. Такой способ может быть использован для согласования транспортных протоколов при прохождении данных через транзитную сеть, для создания защищенных соединений, при которых туннелированные данные подвергаются шифрованию. Маршрутизаторы поддерживают следующие виды туннелей: • GRE – инкапсуляция IP-пакета/Ethernet-кадра в другой IP-пакет с добавлением GRE (General Routing Encapsulation)-заголовка; • IPv4-IPv4 – туннель, использующий инкапсуляцию исходных IP-пакетов в IP-пакеты с другими сетевыми параметрами; • L2TPv3 – туннель для передачи L2-трафика с помощью IP-пакетов; • IPsec – туннель с шифрованием передаваемых данных; • L2TP, PPTP, PPPoE, OpenVPN, WireGuard – туннели, использующиеся для организации удаленного доступа клиент-сервер.

2.2.6 Функции управления и конфигурирования

Таблица 6 – Основные функции управления и конфигурирования

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

2.2.7 Функции сетевой защиты

В таблице 7 приведены функции сетевой защиты, выполняемые устройством.

Таблица 7 − Функции сетевой защиты

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

2.3 Основные технические характеристики

Основные технические параметры маршрутизатора приведены в таблице 8.

Таблица 8 – Основные технические характеристики

Общие параметры		
Интерфейсы	ESR-3350	8 × Combo Ethernet 10/100/1000BASE-T/1000BASE-X (SFP) 4 × 1000BASE-X (SFP)/10GBASE-R (SFP+)/25GBASE-R (SFP28) 1 × Консольный порт RS-232 (RJ-45) 2 × USB 3.0 1 × Слот для microSD-карты
	ESR-3300	4 × 1000BASE-X/10GBASE-R/25GBASE-R 4 × 40GBASE-R (QSFP+)/100GBASE-R (QSFP28) 1 × Консольный порт RS-232 (RJ-45) 1 × Порт OOB 1 × USB 3.0 1 × Слот для microSD-карты
	ESR-3250	8 × Combo Ethernet 10/100/1000BASE-T/1000BASE-X (SFP) 4 × 1000BASE-X (SFP)/10GBASE-R (SFP+)/25GBASE-R (SFP28) 1 × Консольный порт RS-232 (RJ-45) 2 × USB 3.0 1 × Слот для microSD-карты
	ESR-3200L	4 × 1000BASE-X/10GBASE-R/25GBASE-R 8 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) 1 × Порт OOB 1 × USB 2.0 1 × Слот для microSD-карты
	ESR-3200	12 × 1000BASE-X/10GBASE-R/25GBASE-R 1 × Консольный порт RS-232 (RJ-45) 1 × Порт OOB 1 × USB 2.0 1 × Слот для microSD-карты

ESR-3150	8 × Combo Ethernet 10/100/1000BASE-T/1000BASE-X (SFP) 4 ×10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) 2 × USB 3.0 1 × Слот для microSD-карты
ESR-3100	8 × Ethernet 10/100/1000BASE-T/1000BASE-X 8 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) 2 × USB 3.0 1 × Слот для SD-карты
ESR-1700	4 × Combo Ethernet 10/100/1000BASE-T/1000BASE-X (SFP) 8 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 2 × Разъем для установки жесткого диска (будут поддержаны в будущих версиях) 1 × Консольный порт RS-232 (RJ-45) 1 × Порт OOB 2 × USB 2.0
ESR-1511 rev.B	4 × Combo Ethernet 10/100/1000BASE-T/1000BASE-X (SFP) 4 × Ethernet 10/100/1000BASE-T (RJ-45) 4 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 2 × 40GBASE-R (QSFP+) 1 × Консольный порт RS-232 (RJ-45) 1 × Порт OOB 1 × USB 2.0 1 × Слот для SD-карты
ESR-1511	4 × Combo Ethernet 10/100/1000BASE-T/1000BASE-X (SFP) 4 × Ethernet 10/100/1000BASE-T (RJ-45) 4 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 2 × 40GBASE-R (QSFP+) 1 × Консольный порт RS-232 (RJ-45) 1 × Порт OOB 2 × USB 2.0 1 × Слот для SD-карты

ESR-1500	4 × Combo Ethernet 10/100/1000BASE-T/1000BASE-X (SFP) 4 × Ethernet 10/100/1000BASE-T (RJ-45) 4 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) 1 × Порт OOB 2 × USB 2.0 1 × Слот для SD-карты
ESR-1200	4 × Combo Ethernet 10/100/1000BASE-T/1000BASE-X (SFP) 12 × Ethernet 10/100/1000BASE-T (RJ-45) 8 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) 2 × USB 2.0 1 × Слот для SD-карты
ESR-1000	24 × Ethernet 10/100/1000BASE-T (RJ-45) 2 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) 2 × USB 2.0 1 × Слот для SD-карты
ESR-200	4 × Combo Ethernet 10/100/1000BASE-T/1000BASE-X (SFP) 4 × Ethernet 10/100/1000BASE-T (RJ-45) 1 × Консольный порт RS-232 (RJ-45) 1 × USB 3.0 1 × USB 2.0 1 × Слот для SD-карты
ESR-100	4 × Combo Ethernet 10/100/1000BASE-T/1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) 1 × USB 3.0 1 × USB 2.0 1 × Слот для SD-карты

ESR-31	8 × Ethernet 10/100/1000BASE-T (RJ-45) 6 × Ethernet 1000BASE-X (SFP) 2 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 3 × Последовательный порт RS-232 1 × Консольный порт RS-232 (RJ-45) 1 × USB 3.0 1 × USB 2.0 1 × Слот для microSD-карты
ESR-30	4 × Ethernet 10/100/1000BASE-T (RJ-45) 2 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) 1 × USB 3.0 1 × USB 2.0 1 × Слот для microSD-карты
ESR-21	8 × Ethernet 10/100/1000BASE-T (RJ-45) 4 × 1000BASE-X (SFP) 3 × Последовательный порт RS-232 1 × Консольный порт RS-232 (RJ-45) 1 × USB 3.0 1 × USB 2.0 1 × Слот для SD-карты
ESR-20	2 × Combo Ethernet 10/100/1000BASE-T/1000BASE-X (SFP) 2 × Ethernet 10/100/1000BASE-T (RJ-45) 1 × Консольный порт RS-232 (RJ-45) 1 × USB 3.0 1 × USB 2.0 1 × Слот для SD-карты
ESR-15VF	8 × Ethernet 10/100/1000BASE-T (RJ-45) 2 × 1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) 4 × FXS 2 × USB 2.0

	ESR-15R	4 × Ethernet 10/100/1000BASE-T (RJ-45) 2 × 1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) 2 × USB 2.0
	ESR-15	4 × Ethernet 10/100/1000BASE-T (RJ-45) 2 × 1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) 2 × USB 2.0
	ESR-12VF	8 × Ethernet 10/100/1000BASE-T (RJ-45) 1 × 1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) 3 × FXS 1 × FXO 2 × USB 2.0
	ESR-12V	8 × Ethernet 10/100/1000BASE-T (RJ-45) 1 × Консольный порт RS-232 (RJ-45) 3 × FXS 1 × FXO 2 × USB 2.0
	ESR-10	4 × Ethernet 10/100/1000BASE-T (RJ-45) 2 × 1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) 2 × USB 2.0
Типы оптических трансиверов	ESR-3300	1000BASE-X SFP 10GBASE-R SFP+ 25GBASE-R SFP28 40GBASE-R QSFP+ 100GBASE-R QSFP28
	ESR-3350 ESR-3250 ESR-3200L ESR-3200	1000BASE-X SFP 10GBASE-R SFP+ 25GBASE-R SFP28

	ESR-1511 rev.B ESR-1511	1000BASE-X SFP 10GBASE-R SFP+ 40GBASE-X QSFP+
	ESR-3150 ESR-3100 ESR-1700 ESR-1500 ESR-1200 ESR-1000 ESR-31 ESR-30	1000BASE-X SFP 10GBASE-R SFP+
	ESR-200 ESR-100 ESR-21 ESR-20 ESR-15VF ESR-15R ESR-15 ESR-12VF ESR-10	1000BASE-X SFP
Дуплексный и полудуплексный режимы интерфейсов		• дуплексный и полудуплексный режимы для электрических портов • дуплексный режим для оптических портов
Максимальная пропускная способность маршрутизатора в L2-режиме (при аппаратной коммутации)	ESR-1700 ESR-1511 rev.B ESR-1511 ESR-1500 ESR-1200	160 Гбит/с
	ESR-1000	88 Гбит/с
Скорость передачи данных	ESR-3350 ESR-3250	• электрические интерфейсы 10/100/1000 Мбит/с • оптические интерфейсы 1/10/25 Гбит/с
	ESR-3300	• оптические интерфейсы 1/10/25/40/100 Гбит/с
	ESR-3200L ESR-3200	• оптические интерфейсы 1/10/25 Гбит/с

	ESR-1511 rev.B ESR-1511	• электрические интерфейсы 10/100/1000 Мбит/с • оптические интерфейсы 1/10/40 Гбит/с
	ESR-3150 ESR-3100 ESR-1700 ESR-1500 ESR-1200 ESR-1000 ESR-31 ESR-30	• электрические интерфейсы 10/100/1000 Мбит/с • оптические интерфейсы 1/10 Гбит/с
	ESR-200 ESR-100 ESR-21 ESR-20 ESR-15VF ESR-15R ESR-15 ESR-12VF ESR-10	• электрические интерфейсы 10/100/1000 Мбит/с • оптические интерфейсы 1 Гбит/с
	ESR-12V	• электрические интерфейсы 10/100/1000 Мбит/с
Количество VPN-туннелей	ESR-1700	3200
	ESR-3350 ESR-3300 ESR-3250 ESR-3200L ESR-3200 ESR-3150 ESR-3100 ESR-1511 rev.B ESR-1511 ESR-1500 ESR-1200 ESR-1000	500

	ESR-200 ESR-100 ESR-31 ESR-30 ESR-21 ESR-20	250
	ESR-15VF ESR-15R ESR-15 ESR-12V(F) ESR-10	10
Количество статических маршрутов	ESR-3350 ESR-3300 ESR-3250 ESR-3200L ESR-3200 ESR-3150 ESR-3100 ESR-1700 ESR-1511 rev.B ESR-1511 ESR-1500 ESR-1200 ESR-1000 ESR-200 ESR-100 ESR-31 ESR-30 ESR-21 ESR-20	11k
	ESR-15VF ESR-15R ESR-15 ESR-12V(F) ESR-10	1k

Максимальное количество конкурентных сессий	ESR-3350 ESR-3300 ESR-3250 ESR-3200L ESR-3200 ESR-3150 ESR-3100 ESR-1700 ESR-1511 rev.B ESR-1511	8,5M
	ESR-1500	2,43M
	ESR-1200 ESR-1000	3,13M
	ESR-200	2,250M
	ESR-31 ESR-30	3,26M
	ESR-100	1,570M
	ESR-21 ESR-20	2,940M
	ESR-15VF ESR-15R ESR-15	300k
	ESR-12V(F) ESR-10	440k
Таблица VLAN		4094

Количество маршрутов BGPv4/BGPv6	ESR-3350 ESR-3300 ESR-3250 ESR-3200L ESR-3200 ESR-3150 ESR-3100 ESR-1700 ESR-1511 rev.B ESR-1511 ESR-1500 ESR-1200 ESR-1000	5M
	ESR-200 ESR-100 ESR-31 ESR-30 ESR-21 ESR-20	2,5M
	ESR-15VF ESR-15R ESR-15 ESR-12V(F) ESR-10	1M

Количество маршрутов OSPFv2/ OSPFv3/IS-IS	ESR-3350 ESR-3300 ESR-3250 ESR-3200L ESR-3200 ESR-3150 ESR-3100 ESR-1700 ESR-1511 rev.B ESR-1511 ESR-1500 ESR-1200 ESR-1000	500k
	ESR-200 ESR-100 ESR-31 ESR-30 ESR-20 ESR-21	300k
	ESR-15VF ESR-15R ESR-15 ESR-12V(F) ESR-10	30k

Количество маршрутов RIP/RIPng	ESR-3350 ESR-3300 ESR-3250 ESR-3200L ESR-3200 ESR-3150 ESR-3100 ESR-1700 ESR-1511 rev.B ESR-1511 ESR-1500 ESR-1200 ESR-1000 ESR-200 ESR-100 ESR-31 ESR-30 ESR-21 ESR-20	10k
	ESR-15VF ESR-15R ESR-15 ESR-12V(F) ESR-10	1k
Таблица MAC-адресов	ESR-1700 ESR-1511 rev.B ESR-1511 ESR-1500 ESR-1200	128k записей
	ESR-1000	16k записей

Размер базы FIB	ESR-1700	3,0M
	ESR-3350 ESR-3300 ESR-3250 ESR-3200L ESR-3200 ESR-3150 ESR-3100 ESR-1511 rev.B ESR-1511 ESR-1500 ESR-1200 ESR-1000	1,7M
	ESR-200 ESR-100 ESR-31 ESR-30 ESR-21 ESR-20	1,4M
	ESR-15VF ESR-15R ESR-15 ESR-12V(F) ESR-10	1M
VRF		32

Количество L3-интерфейсов	ESR-1700	10000
	ESR-3350 ESR-3300 ESR-3250 ESR-3200L ESR-3200 ESR-3150 ESR-3100 ESR-1511 rev.B ESR-1511 ESR-1500 ESR-1200 ESR-1000 ESR-200 ESR-100 ESR-31 ESR-30 ESR-21 ESR-20	4000
	ESR-15VF ESR-15R ESR-15 ESR-12V(F) ESR-10	200

Соответствие стандартам		IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-T Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z Fiber Gigabit Ethernet IEEE 802.3cc 25GBASE-LR Ethernet IEEE 802.3by 25GBASE-SR Ethernet IEEE 802.3ba 40GBASE-SR4, 40GBASE-LR4 ANSI/IEEE 802.3 автоопределение скорости IEEE 802.3x контроль потоков данных IEEE 802.3ad объединение каналов LACP IEEE 802.1Q виртуальные локальные сети VLAN IEEE 802.1v, IEEE 802.3ac, IEEE 802.3ae, IEEE 802.1D, IEEE 802.1w, IEEE 802.1s
Управление		
Локальное управление		CLI
Удаленное управление		Telnet, SSH
Физические характеристики и условия окружающей среды		
Источники питания	ESR-3350 ESR-3300 ESR-1700	Сеть переменного тока: 200–240 В, 50–60 Гц Сеть постоянного тока: 36–72 В Варианты питания: • один источник питания постоянного или переменного тока; • два источника питания постоянного или переменного тока с возможностью горячей замены.
	ESR-3250 ESR-3200L ESR-3200 ESR-3150 ESR-3100 ESR-1511 rev.B ESR-1511 ESR-1500 ESR-1200 ESR-1000 ESR-31	Сеть переменного тока: 100–240 В, 50–60 Гц Сеть постоянного тока: 36–72 В Варианты питания: • один источник питания постоянного или переменного тока; • два источника питания постоянного или переменного тока с возможностью горячей замены.

	ESR-200 ESR-100 ESR-30 ESR-21 ESR-20 ESR-15VF ESR-15R ESR-12V(F)	Сеть переменного тока: 100–264 В, 50–60 Гц
	ESR-15	Сеть переменного тока 220 В (через адаптер питания 12 В, 2 А)
	ESR-10	Сеть переменного тока 220 В (через адаптер питания 12 В, 1,5 А)
Максимальная потребляемая мощность	ESR-3350	110 Вт
	ESR-3300	184 Вт
	ESR-3250	74 Вт
	ESR-3200L	105 Вт
	ESR-3200	117 Вт
	ESR-3150	74 Вт
	ESR-3100	111 Вт
	ESR-1700	235 Вт
	ESR-1511 rev.B ESR-1511	130 Вт
	ESR-1500	125 Вт
	ESR-1200	78 Вт
	ESR-1000	78 Вт
	ESR-200	35 Вт
	ESR-100	22 Вт
	ESR-31	44 Вт
	ESR-30	29 Вт

	ESR-21	32 Вт
	ESR-20	25 Вт
	ESR-15R	18 Вт
	ESR-15	19 Вт
	ESR-15VF	28 Вт
	ESR-12V(F)	22 Вт
	ESR-10	9 Вт
Масса	ESR-3350	5,638 кг
	ESR-3300	7 кг
	ESR-3250	4,232 кг
	ESR-3200L ESR-3200	5 кг
	ESR-3150	4,291 кг
	ESR-3100	4,34 кг
	ESR-1700	11,635 кг
	ESR-1511 rev.B ESR-1511	5,929 кг
	ESR-1500	7 кг
	ESR-1200	4,861 кг
	ESR-1000	4,319 кг
	ESR-200 ESR-100	2,5 кг
	ESR-31	3,425 кг
	ESR-30	1,881 кг
	ESR-21	3,13 кг
	ESR-20	2 кг

	ESR-15VF	1,536 кг
	ESR-15R	1,405 кг
	ESR-15	0,369 кг
	ESR-12V(F)	1,23 кг
	ESR-10	0,28 кг
Габаритные размеры (Ш × В × Г)	ESR-3350	430 × 43,6 × 424 мм
	ESR-3300	430 × 44 × 425 мм
	ESR-3250 ESR-3150	430 × 43,6 × 329 мм
	ESR-3200L ESR-3200 ESR-3100	430 × 44 × 330 мм
	ESR-1700	440 × 88 × 490 мм
	ESR-1511 rev.B ESR-1511 ESR-1500	430 × 44 × 425 мм
	ESR-1200 ESR-1000	430 × 44 × 352 мм
	ESR-200 ESR-100	310 × 44 × 240 мм
	ESR-31	430 × 43,6 × 275 мм
	ESR-21	430 × 44 × 225 мм
	ESR-30 ESR-20	267 × 44 × 212 мм
	ESR-15VF ESR-15R	267 × 44 × 160 мм
	ESR-15	230 × 32 × 133 мм
	ESR-12V(F)	267 × 43,6 × 160,5 мм

	ESR-10	185 × 32 × 118 мм
Интервал рабочих температур	ESR-3350 ESR-3300 ESR-3250 ESR-3200L ESR-3200 ESR-3150 ESR-3100 ESR-1700 ESR-1511 rev.B ESR-1511 ESR-1500 ESR-1200 ESR-1000 ESR-200 ESR-100 ESR-31 ESR-30 ESR-21 ESR-20	от -10 до +45 °C
	ESR-15VF ESR-15R ESR-15 ESR-12V(F) ESR-10	от -0 до +40 °C
Интервал температуры хранения	от -40 до +70 °C	
Относительная влажность при эксплуатации (без образования конденсата)	не более 80 %	
Относительная влажность при хранении (без образования конденсата)	от 10 до 95 %	
Срок службы	не менее 15 лет	

2.4 Конструктивное исполнение

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

2.4.1 Конструктивное исполнение ESR-3350

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

Передняя панель устройства ESR-3350

Внешний вид передней панели ESR-3350 показан на рисунке 1.

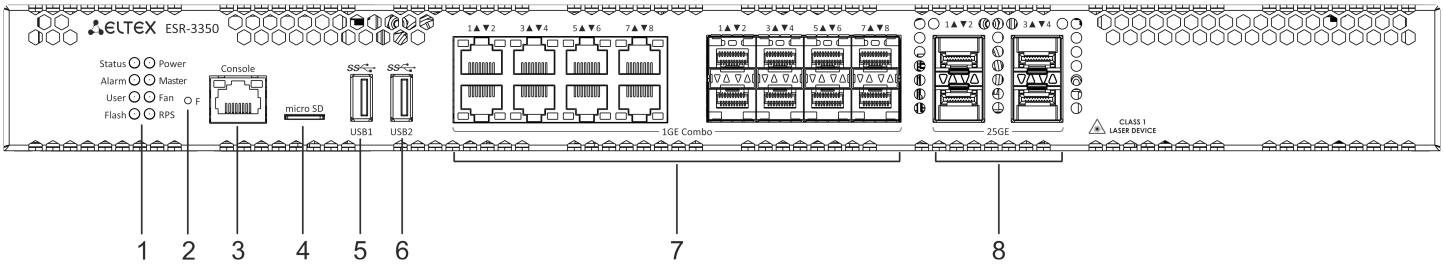


Рисунок 1 – Передняя панель ESR-3350

В таблице 9 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели ESR-3350.

Таблица 9 – Описание разъемов, индикаторов и органов управления передней панели ESR-3350

№	Элемент передней панели	Описание
1	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	User	Индикатор, использующийся для пользовательских сценариев, которые можно назначить в режиме конфигурирования устройства.
	Flash	Индикатор активности обмена с накопителем данных – microSD-картой или USB Flash.
	Power	Индикатор питания устройства.
	Master	Индикатор работы устройства в failover-режимах (не используется в текущей версии).
	Fan	Индикатор аварии вентиляторов.
	RPS	Индикатор резервного источника электропитания.

№	Элемент передней панели	Описание
2	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при удержании кнопки менее 10 секунд происходит перезагрузка устройства; • при удержании кнопки более 10 секунд происходит перезагрузка устройства и сброс к заводским настройкам.
3	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
4	microSD	Разъем для установки microSD-карт памяти.
5	USB 1	Порт USB 3.0 для подключения USB-устройств.
6	USB 2	Порт USB 3.0 для подключения USB-устройств.
7	1GE Combo [1 .. 8]	8 портов Gigabit Ethernet 10/100/1000BASE-X (SFP).
8	25GE [1 .. 4]	4 порта 1000BASE-X/10GBASE-R/25GBASE-R.

Задняя панель устройства ESR-3350

Внешний вид задней панели ESR-3350 приведен на рисунке ниже.

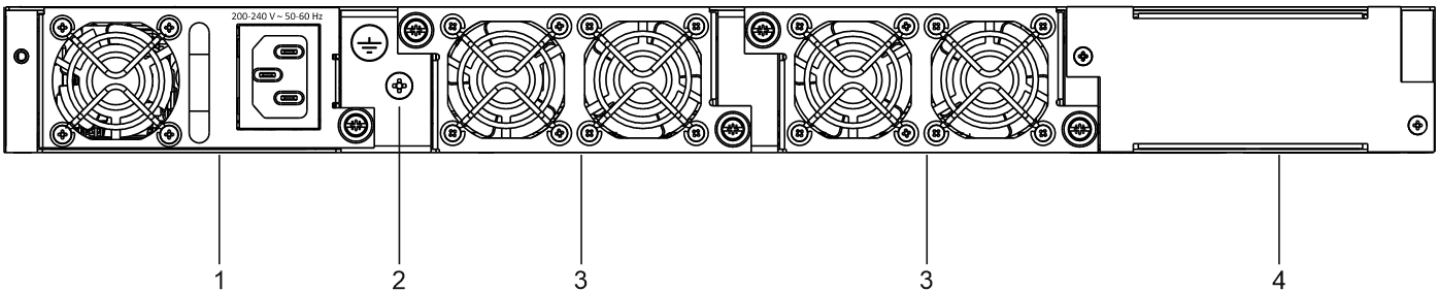


Рисунок 2 – Задняя панель ESR-3350

В таблице 10 приведен перечень разъемов, расположенных на задней панели ESR-3350.

Таблица 10 – Описание разъемов задней панели ESR-3350

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

Боковые панели устройства ESR-3350

Внешний вид боковых панелей ESR-3350 приведен на рисунках ниже.

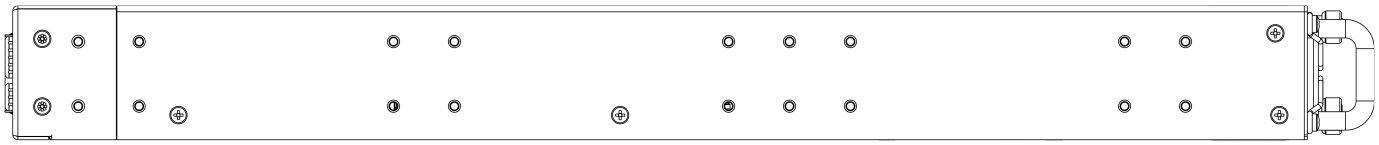


Рисунок 3 – Правая боковая панель ESR-3350

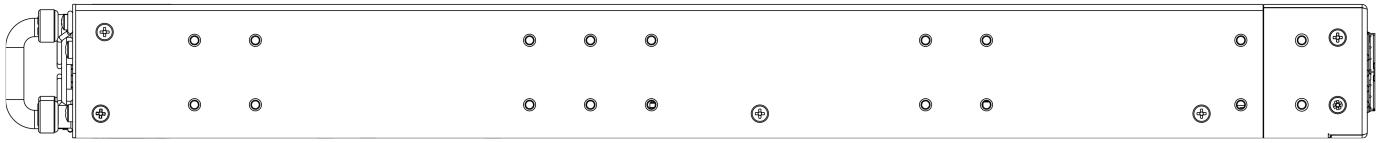


Рисунок 4 – Левая боковая панель ESR-3350

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

2.4.2 Конструктивное исполнение ESR-3300

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

Передняя панель устройства ESR-3300

Внешний вид передней панели ESR-3300 показан на рисунке 5.

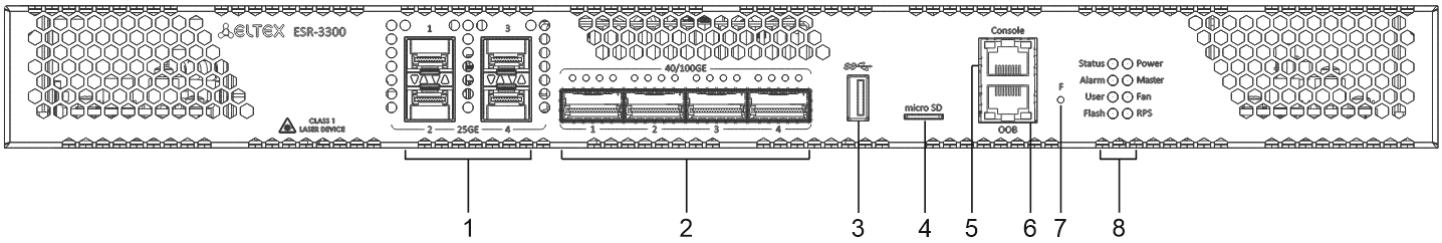


Рисунок 5 – Передняя панель ESR-3300

В таблице 11 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели ESR-3300.

Таблица 11 – Описание разъемов, индикаторов и органов управления передней панели ESR-3300

№	Элемент передней панели	Описание
1	25GE [1 .. 4]	4 порта 1000BASE-X/10GBASE-R/25GBASE-R
2	40/100GE [1 .. 4]	4 порта Ethernet 40GBASE-R (QSFP+)/100GBASE-R (QSFP28)
3	USB	Порт USB 3.0 для подключения USB-устройств.
4	microSD	Разъем для установки microSD-карт памяти.

№	Элемент передней панели	Описание
5	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
6	OOB	Ethernet-интерфейс используется для удаленного доступа и управления и обновления программного обеспечения через вторичный загрузчик U-Boot. Данный интерфейс не может участвовать в маршрутизации транзитного трафика.
7	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при удержании кнопки менее 10 секунд происходит перезагрузка устройства; • при удержании кнопки более 10 секунд происходит перезагрузка устройства и сброс к заводским настройкам.
8	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	User	Индикатор, использующийся для пользовательских сценариев, которые можно назначить в режиме конфигурирования устройства.
	Flash	Индикатор активности обмена с накопителем данных – microSD-картой или USB Flash.
	Power	Индикатор питания устройства.
	Master	Индикатор работы устройства в failover-режимах (не используется в текущей версии).
	Fan	Индикатор аварии вентиляторов.
	RPS	Индикатор резервного источника электропитания.

Задняя панель устройства ESR-3300

Внешний вид задней панели ESR-3300 приведен на рисунке ниже.

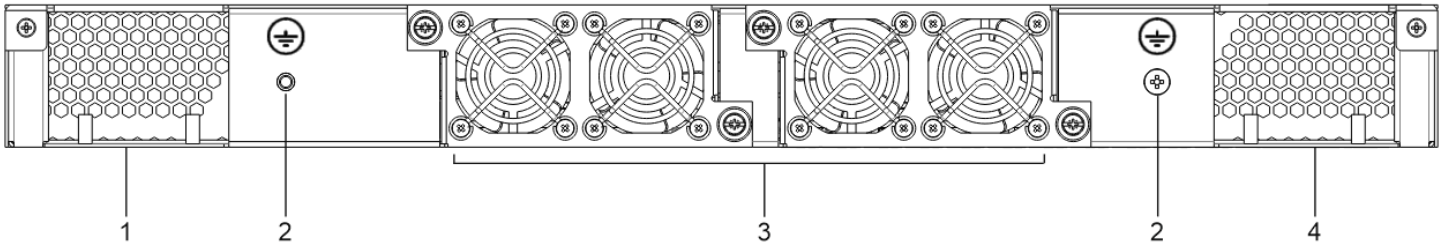


Рисунок 6 – Задняя панель ESR-3300

В таблице 12 приведен перечень разъемов, расположенных на задней панели ESR-3300.

Таблица 12 – Описание разъемов задней панели ESR-3300

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

Боковые панели устройства ESR-3300

Внешний вид боковых панелей ESR-3300 приведен на рисунках ниже.

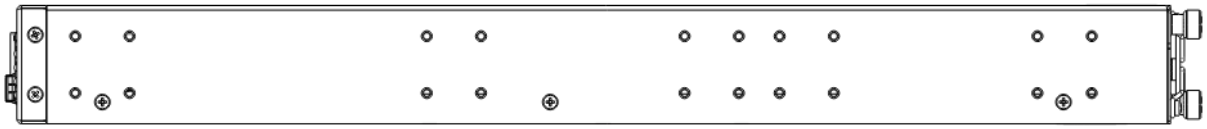


Рисунок 7 – Правая боковая панель ESR-3300

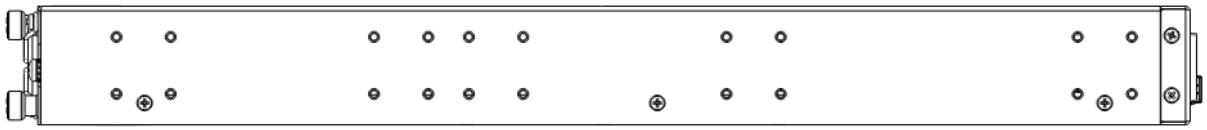


Рисунок 8 – Левая боковая панель ESR-3300

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

2.4.3 Конструктивное исполнение ESR-3250

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

Передняя панель устройства ESR-3250

Внешний вид передней панели ESR-3250 показан на рисунке 9.

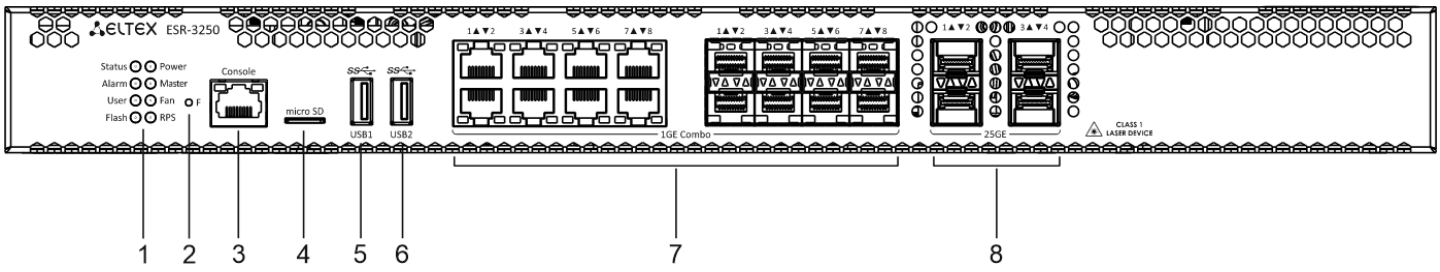


Рисунок 9 – Передняя панель ESR-3250

В таблице 13 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели ESR-3250.

Таблица 13 – Описание разъемов, индикаторов и органов управления передней панели ESR-3250

№	Элемент передней панели	Описание
1	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	User	Индикатор, использующийся для пользовательских сценариев, которые можно назначить в режиме конфигурирования устройства.
	Flash	Индикатор активности обмена с накопителем данных – microSD-картой или USB Flash.
	Power	Индикатор питания устройства.
	Master	Индикатор работы устройства в failover-режимах (не используется в текущей версии).
	Fan	Индикатор аварии вентиляторов.
	RPS	Индикатор резервного источника электропитания.
2	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при удержании кнопки менее 10 секунд происходит перезагрузка устройства; • при удержании кнопки более 10 секунд происходит перезагрузка устройства и сброс к заводским настройкам.
3	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.

№	Элемент передней панели	Описание
4	microSD	Разъем для установки microSD-карт памяти.
5	USB 1	Порт USB 3.0 для подключения USB-устройств.
6	USB 2	Порт USB 3.0 для подключения USB-устройств.
7	1GE Combo [1 .. 8]	8 портов Gigabit Ethernet 10/100/1000BASE-X (SFP).
8	25 GE [1 .. 4]	4 порта 1000BASE-X/10GBASE-R/25GBASE-R.

Задняя панель устройства ESR-3250

Внешний вид задней панели ESR-3250 приведен на рисунке ниже.

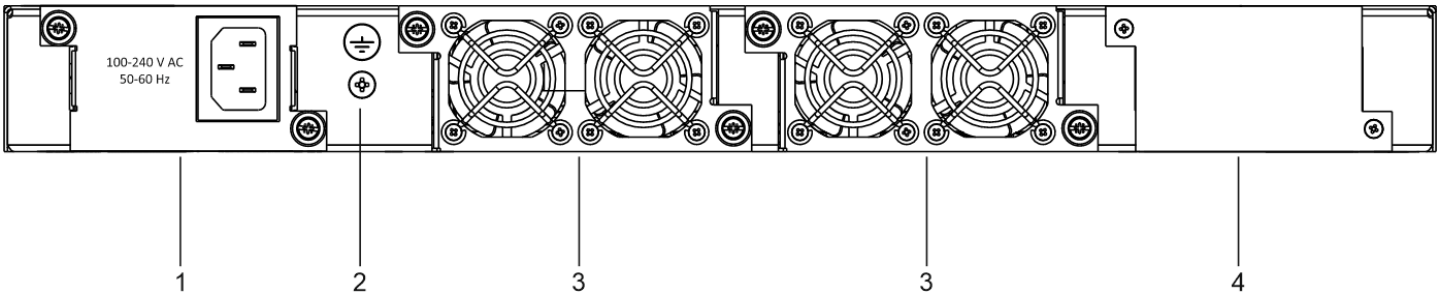


Рисунок 10 – Задняя панель ESR-3250

В таблице 14 приведен перечень разъемов, расположенных на задней панели ESR-3250.

Таблица 14 – Описание разъемов задней панели ESR-3250

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

Боковые панели устройства ESR-3250

Внешний вид боковых панелей ESR-3250 приведен на рисунках ниже.

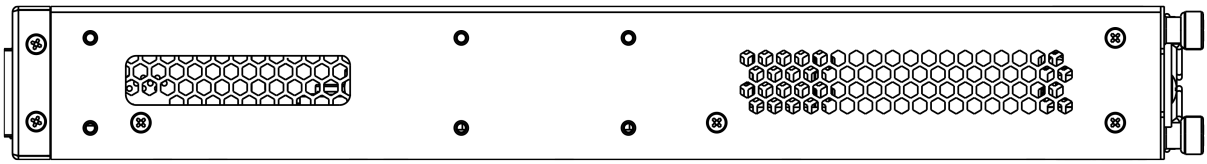


Рисунок 11 – Правая боковая панель ESR-3250

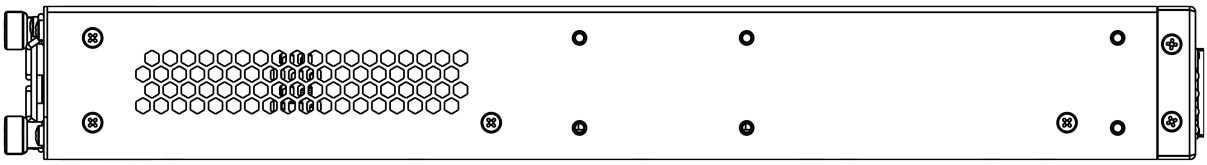


Рисунок 12 – Левая боковая панель ESR-3250

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

2.4.4 Конструктивное исполнение ESR-3200L

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

Передняя панель устройства ESR-3200L

Внешний вид передней панели ESR-3200L показан на рисунке 13.

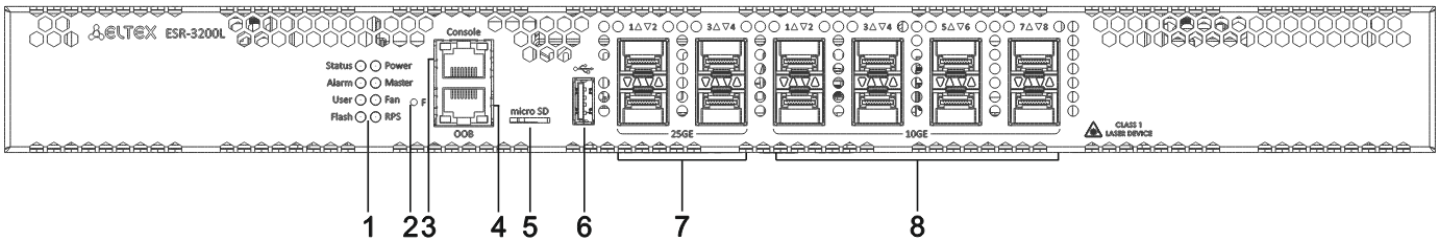


Рисунок 13 – Передняя панель ESR-3200L

В таблице 15 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели ESR-3200L.

Таблица 15 – Описание разъемов, индикаторов и органов управления передней панели ESR-3200L

№	Элемент передней панели	Описание
1	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	User	Индикатор, использующийся для пользовательских сценариев, которые можно назначить в режиме конфигурирования устройства.

№	Элемент передней панели	Описание
	Flash	Индикатор активности обмена с накопителем данных – microSD-картой или USB Flash.
	Power	Индикатор питания устройства.
	Master	Индикатор работы устройства в failover-режимах (не используется в текущей версии).
	Fan	Индикатор аварии вентиляторов.
	RPS	Индикатор резервного источника электропитания.
2	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при удержании кнопки менее 10 секунд происходит перезагрузка устройства; • при удержании кнопки более 10 секунд происходит перезагрузка устройства и сброс к заводским настройкам.
3	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
4	OOB	Ethernet-интерфейс используется для удаленного доступа и управления и обновления программного обеспечения через вторичный загрузчик U-Boot. Данный интерфейс не может участвовать в маршрутизации транзитного трафика.
5	microSD	Разъем для установки microSD-карт памяти.
6	USB	Порт USB 2.0 для подключения USB-устройств.
7	[1 .. 4]	4 порта Gigabit Ethernet 1000BASE-X/10GBASE-R/25GBASE-R.
8	[1 .. 8]	Слоты для установки трансиверов 10G SFP+/1G SFP.

Задняя панель устройства ESR-3200L

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

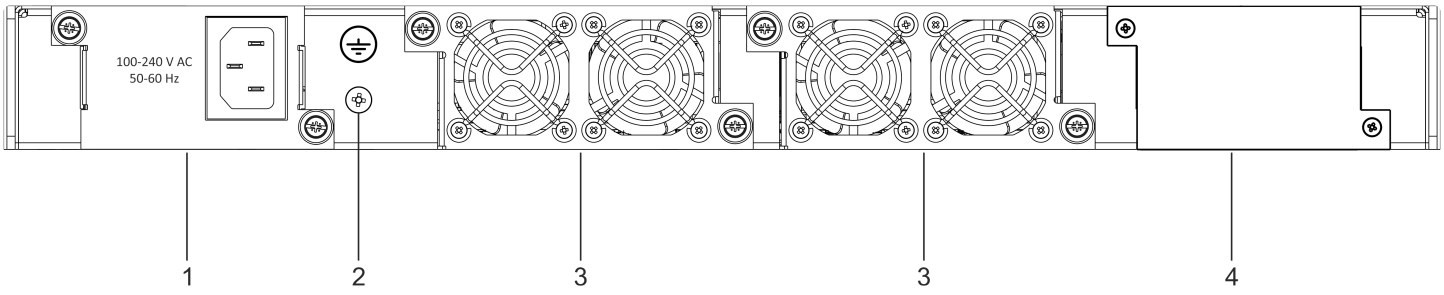


Рисунок 14 – Задняя панель ESR-3200L

В таблице 16 приведен перечень разъемов, расположенных на задней панели ESR-3200L.

Таблица 16 – Описание разъемов задней панели ESR-3200L

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

Боковые панели устройства ESR-3200L

Внешний вид боковых панелей ESR-3200L приведен на рисунках ниже.

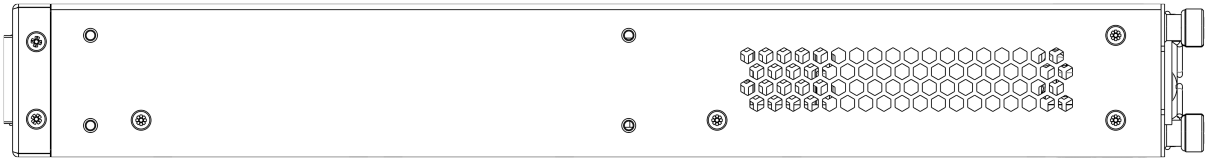


Рисунок 15 – Правая боковая панель ESR-3200L

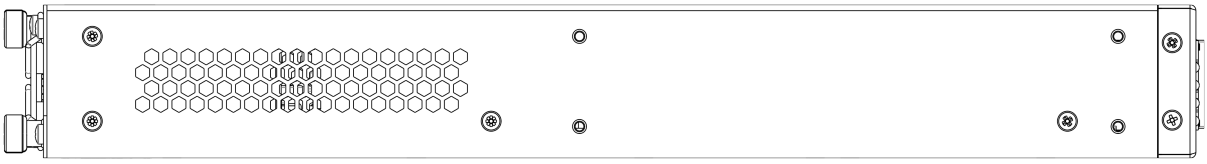


Рисунок 16 – Левая боковая панель ESR-3200L

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

2.4.5 Конструктивное исполнение ESR-3200

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

Передняя панель устройства ESR-3200

Внешний вид передней панели ESR-3200 показан на рисунке 17.

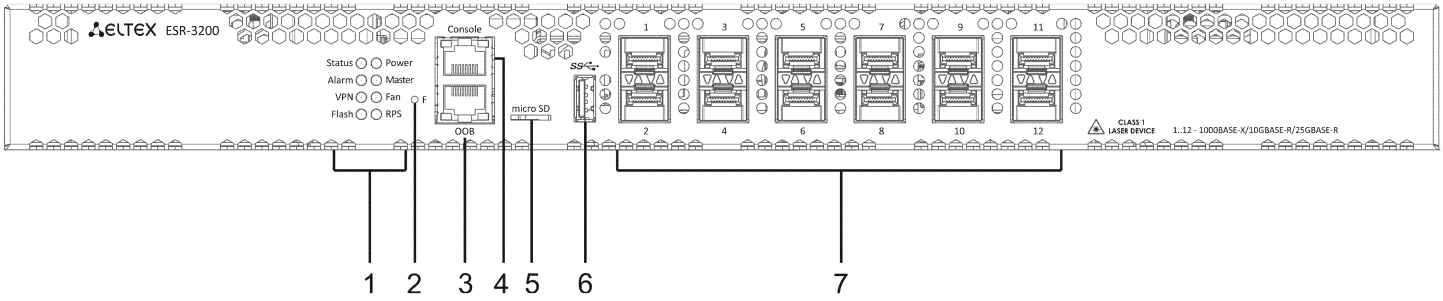


Рисунок 17 – Передняя панель ESR-3200

В таблице 17 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели ESR-3200.

Таблица 17 – Описание разъемов, индикаторов и органов управления передней панели ESR-3200

№	Элемент передней панели	Описание
1	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	VPN	Индикатор режима работы в режиме VPN-шлюза (не используется в текущей версии).
	Flash	Индикатор активности обмена с накопителем данных – microSD-картой или USB Flash.
	Power	Индикатор питания устройства.
	Master	Индикатор работы устройства в failover-режимах (не используется в текущей версии).
	Fan	Индикатор аварии вентиляторов.
	RPS	Индикатор резервного источника электропитания.
2	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при удержании кнопки менее 10 секунд происходит перезагрузка устройства; • при удержании кнопки более 10 секунд происходит перезагрузка устройства и сброс к заводским настройкам.

№	Элемент передней панели	Описание
3	OOB	Ethernet-интерфейс используется для удаленного доступа и управления и обновления программного обеспечения через вторичный загрузчик U-Boot. Данный интерфейс не может участвовать в маршрутизации транзитного трафика.
4	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
5	microSD	Разъем для установки microSD-карт памяти.
6	USB1	Порт USB 2.0 для подключения USB-устройств.
7	[1 .. 12]	Слоты для установки трансиверов 25G SFP28/10G SFP+/1G SFP.

Задняя панель устройства ESR-3200

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

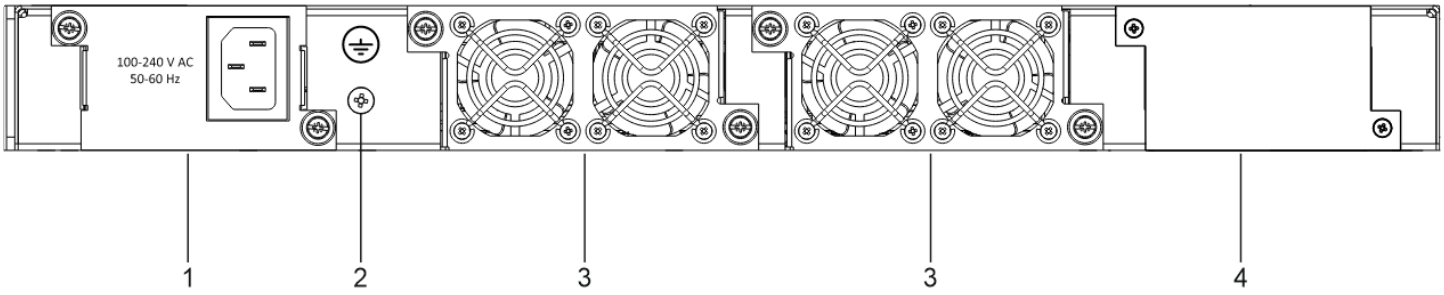


Рисунок 18 – Задняя панель ESR-3200

В таблице 18 приведен перечень разъемов, расположенных на задней панели ESR-3200.

Таблица 18 – Описание разъемов задней панели ESR-3200

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

Боковые панели устройства ESR-3200

Внешний вид боковых панелей приведен на рисунках ниже.

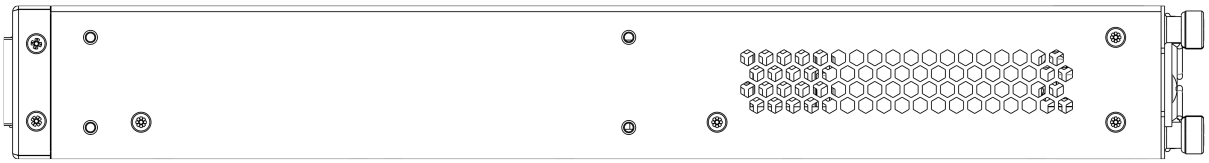


Рисунок 19 – Правая боковая панель ESR-3200

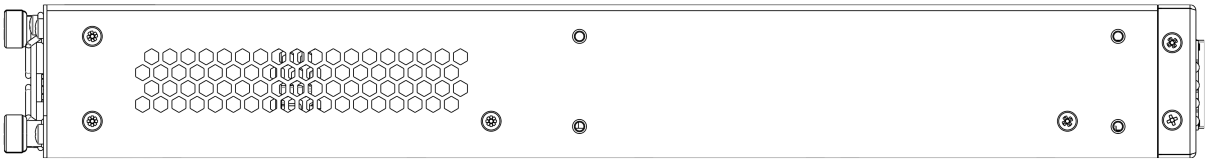


Рисунок 20 – Левая боковая панель ESR-3200

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

2.4.6 Конструктивное исполнение ESR-3150

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

Передняя панель устройства ESR-3150

Внешний вид передней панели ESR-3150 показан на рисунке 21.

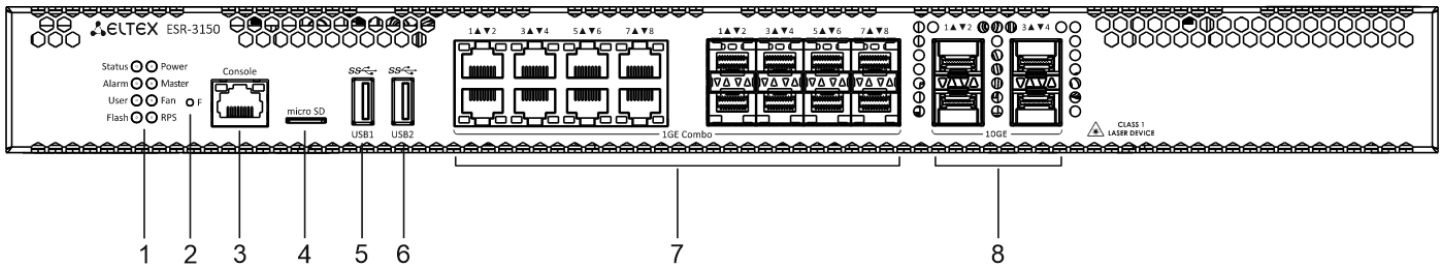


Рисунок 21 – Передняя панель ESR-3150

В таблице 19 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели ESR-3150.

Таблица 19 – Описание разъемов, индикаторов и органов управления передней панели ESR-3150

№	Элемент передней панели	Описание
1	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.

№	Элемент передней панели	Описание
	User	Индикатор, использующийся для пользовательских сценариев, которые можно назначить в режиме конфигурирования устройства.
	Flash	Индикатор активности обмена с накопителем данных – microSD-картой или USB Flash.
	Power	Индикатор питания устройства.
	Master	Индикатор работы устройства в failover-режимах (не используется в текущей версии).
	Fan	Индикатор аварии вентиляторов.
	RPS	Индикатор резервного источника электропитания.
2	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при удержании кнопки менее 10 секунд происходит перезагрузка устройства; • при удержании кнопки более 10 секунд происходит перезагрузка устройства и сброс к заводским настройкам.
3	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
4	microSD	Разъем для установки microSD-карт памяти.
5	USB 1	Порт USB 3.0 для подключения USB-устройств.
6	USB 2	Порт USB 3.0 для подключения USB-устройств.
7	1GE Combo [1 .. 8]	8 портов Gigabit Ethernet 10/100/1000BASE-X (SFP).
8	10 GE [1 .. 4]	4 порта 10GBASE-R (SFP+)/1000BASE-X (SFP).

Задняя панель устройства ESR-3150

Внешний вид задней панели ESR-3150 приведен на рисунке ниже.

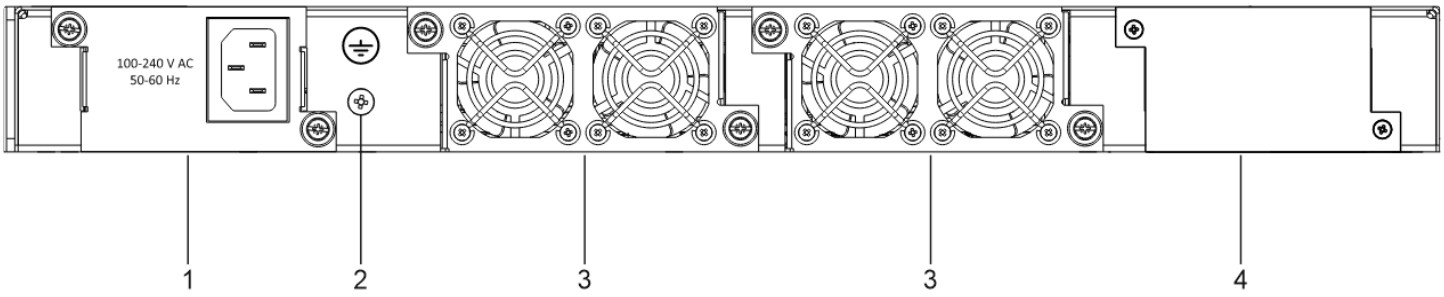


Рисунок 22 – Задняя панель ESR-3150

В таблице 20 приведен перечень разъемов, расположенных на задней панели ESR-3150.

Таблица 20 – Описание разъемов задней панели ESR-3150

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

Боковые панели устройства ESR-3150

Внешний вид боковых панелей ESR-3150 приведен на рисунках ниже.

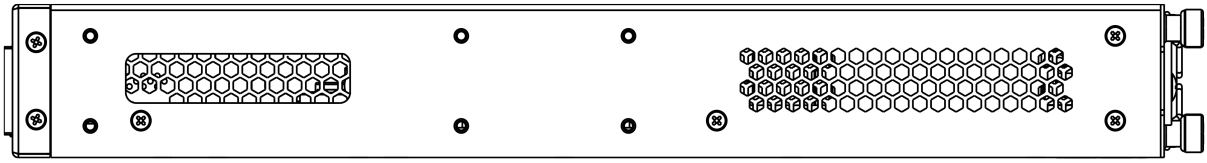


Рисунок 23 – Правая боковая панель ESR-3150

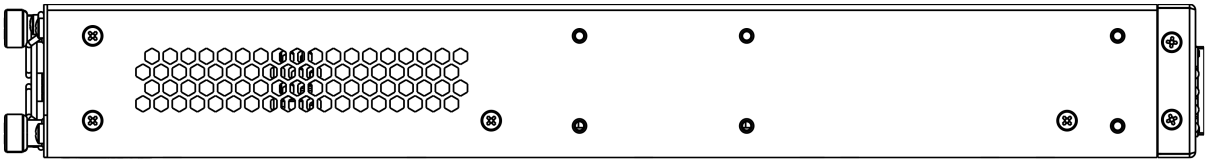


Рисунок 24 – Левая боковая панель ESR-3150

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

2.4.7 Конструктивное исполнение ESR-3100

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

Передняя панель устройства ESR-3100

Внешний вид передней панели ESR-3100 показан на рисунке 25.

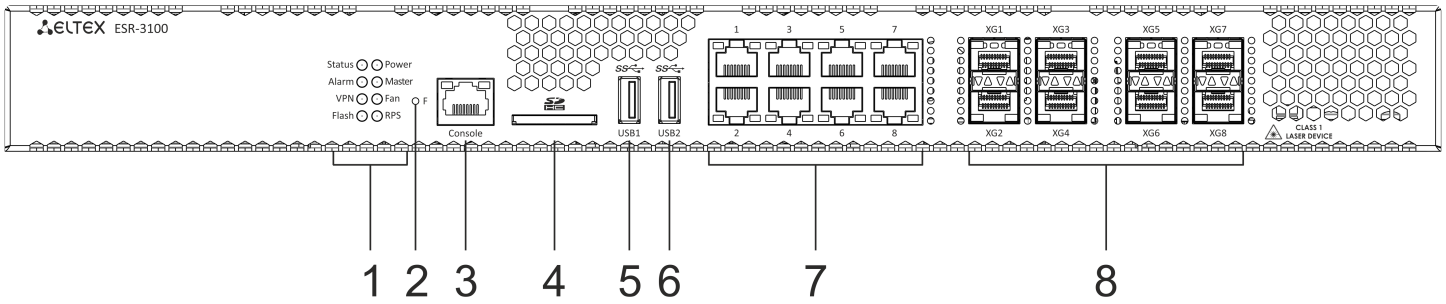


Рисунок 25 – Передняя панель ESR-3100

В таблице 21 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели ESR-3100.

Таблица 21 – Описание разъемов, индикаторов и органов управления передней панели ESR-3100

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

Задняя панель устройства ESR-3100

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

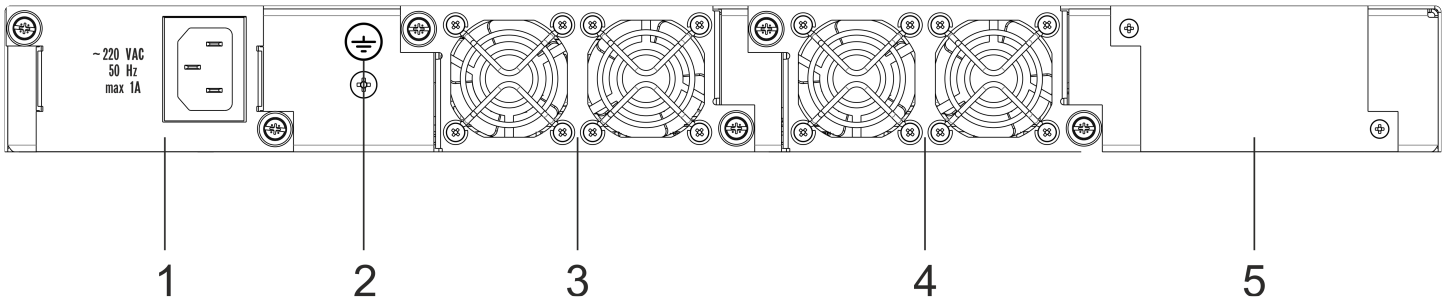


Рисунок 26 – Задняя панель ESR-3100

В таблице 22 приведен перечень разъемов, расположенных на задней панели ESR-3100.

Таблица 22 – Описание разъемов задней панели ESR-3100

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

Боковые панели устройства ESR-3100

Внешний вид боковых панелей ESR-3100 приведен на рисунках ниже.

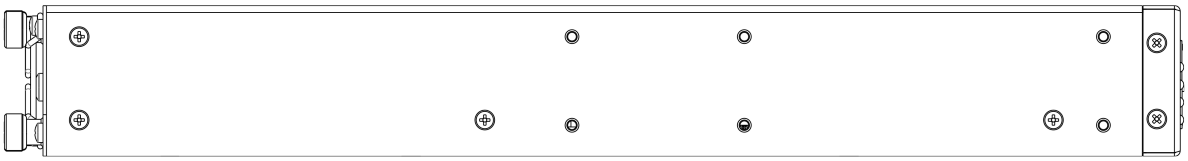


Рисунок 27 – Правая боковая панель ESR-3100

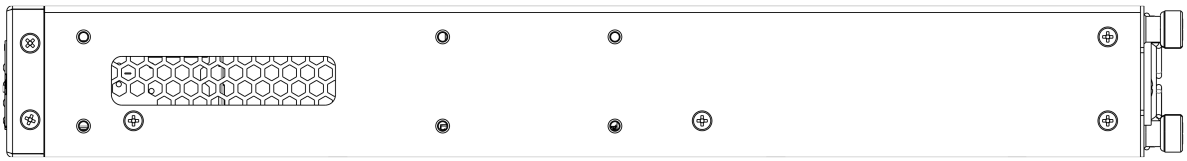


Рисунок 28 – Левая боковая панель ESR-3100

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

2.4.8 Конструктивное исполнение ESR-1700

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

Передняя панель устройства ESR-1700

Внешний вид передней панели ESR-1700 показан на рисунке 29.

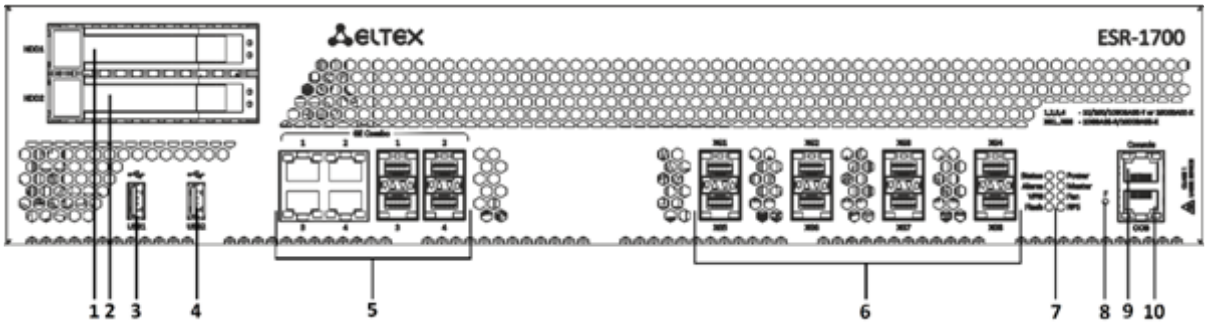


Рисунок 29 – Передняя панель ESR-1700

В таблице 23 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели ESR-1700.

Таблица 23 – Описание разъемов, индикаторов и органов управления передней панели ESR-1700

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

№	Элемент передней панели	Описание
	Master	Индикатор работы устройства в failover-режимах (не используется в текущей версии).
	Fan	Индикатор аварии вентиляторов.
	RPS	Индикатор резервного источника электропитания.
8	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при удержании кнопки менее 10 секунд происходит перезагрузка устройства; • при удержании кнопки более 10 секунд происходит перезагрузка устройства и сброс к заводским настройкам.
9	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
10	OOB	Ethernet-порт используется только для обновления программного обеспечения через загрузчик U-Boot. Данный порт не используется для удаленного доступа и управления.

Задняя панель устройства ESR-1700

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

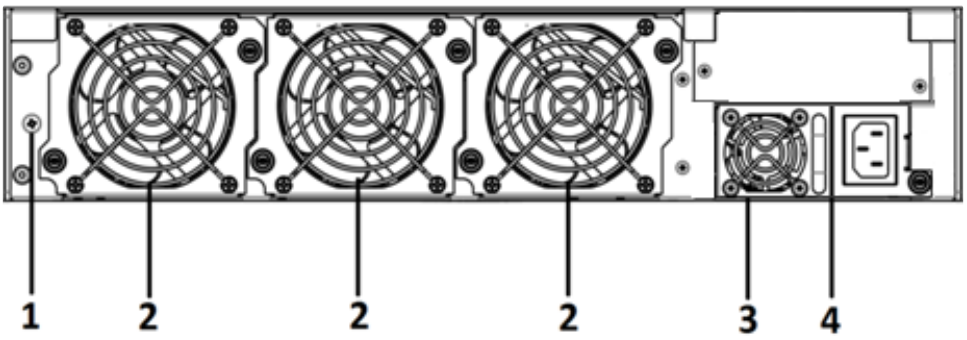


Рисунок 30 – Задняя панель ESR-1700

В таблице 24 приведен перечень разъемов, расположенных на задней панели ESR-1700.

Таблица 24 – Описание разъемов задней панели ESR-1700

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

Боковые панели устройства ESR-1700

Внешний вид боковых панелей ESR-1700 приведен на рисунках ниже.



Рисунок 31 – Правая боковая панель ESR-1700



Рисунок 32 – Левая боковая панель ESR-1700

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

2.4.9 Конструктивное исполнение ESR-1511 rev.B, ESR-1511, ESR-1500

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

Передняя панель устройства ESR-1511 rev.B

Внешний вид передней панели ESR-1511 rev.B показан на рисунке 33.

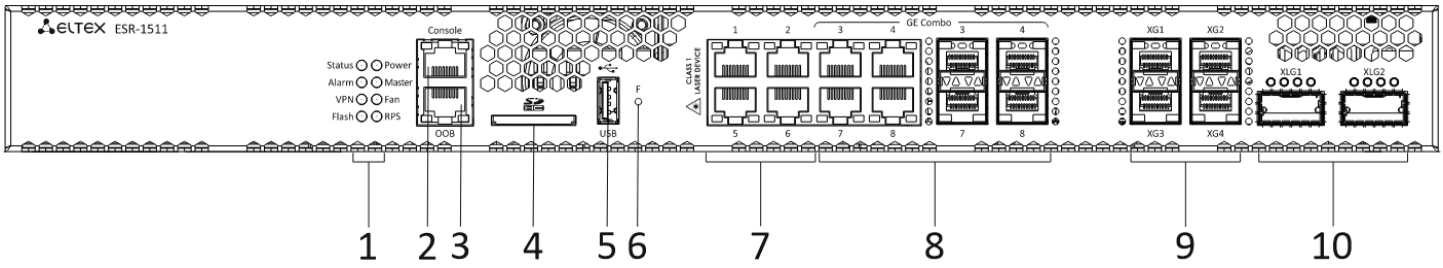


Рисунок 33 – Передняя панель ESR-1511 rev.B

В таблице 25 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели ESR-1511 rev.B.

Таблица 25 – Описание разъемов, индикаторов и органов управления передней панели ESR-1511

№	Элемент передней панели	Описание
1	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	VPN	Индикатор режима работы в режиме VPN-шлюза (не используется в текущей версии).
	Flash	Индикатор активности обмена с накопителем данных – SD-картой или USB Flash.
	Power	Индикатор питания устройства.
	Master	Индикатор работы устройства в failover-режимах (не используется в текущей версии).
	Fan	Индикатор аварии вентиляторов.
	RPS	Индикатор резервного источника электропитания.
2	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
3	OOB	Ethernet-порт используется только для обновления программного обеспечения через загрузчик U-Boot. Данный порт не используется для удаленного доступа и управления.
4	SD	Разъем для установки SD-карт памяти.
5	USB	Порт для подключения USB-устройств.
6	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при удержании кнопки менее 10 секунд происходит перезагрузка устройства; • при удержании кнопки более 10 секунд происходит перезагрузка устройства и сброс к заводским настройкам.
7	Ethernet	4 порта Ethernet 10/100/1000BASE-T.
8	Combo Ports [1 .. 4]	4 порта Gigabit Ethernet 10/100/1000BASE-X (SFP).
9	XG1–XG4	Слоты для установки трансиверов 10G SFP+/1G SFP.
10	XLG1–XLG2	Слоты для установки трансиверов 40G QSFP+.

Передняя панель устройства ESR-1511

Внешний вид передней панели ESR-1511 показан на рисунке 34.

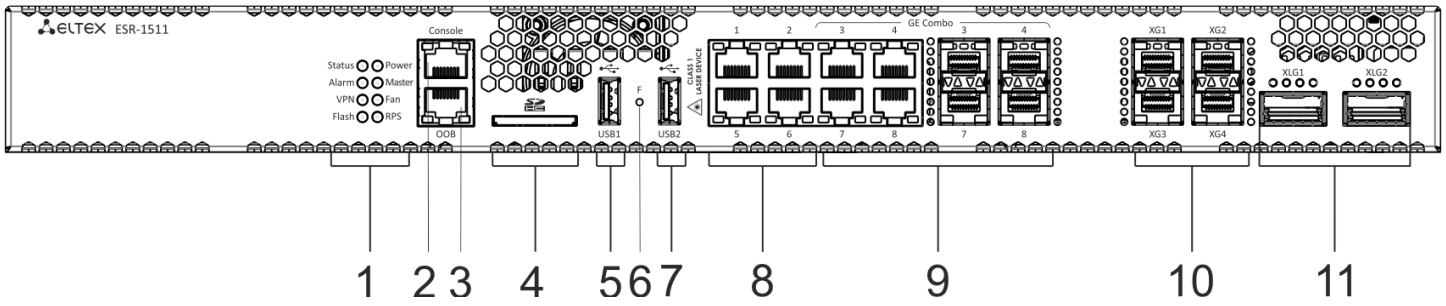


Рисунок 34 – Передняя панель ESR-1511

В таблице 26 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели ESR-1511.

Таблица 26 – Описание разъемов, индикаторов и органов управления передней панели ESR-1511

№	Элемент передней панели	Описание
1	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	VPN	Индикатор режима работы в режиме VPN-шлюза (не используется в текущей версии).
	Flash	Индикатор активности обмена с накопителем данных – SD-картой или USB Flash.
	Power	Индикатор питания устройства.
	Master	Индикатор работы устройства в failover-режимах (не используется в текущей версии).
	Fan	Индикатор аварии вентиляторов.
	RPS	Индикатор резервного источника электропитания.
2	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
3	OOB	Ethernet-порт используется только для обновления программного обеспечения через загрузчик U-Boot. Данный порт не используется для удаленного доступа и управления.
4	SD	Разъем для установки SD-карт памяти.
5	USB1	Порт для подключения USB-устройств.
6	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при удержании кнопки менее 10 секунд происходит перезагрузка устройства; • при удержании кнопки более 10 секунд происходит перезагрузка устройства и сброс к заводским настройкам.

№	Элемент передней панели	Описание
7	USB2	Порт для подключения USB-устройств.
8	Ethernet	4 порта Ethernet 10/100/1000BASE-T.
9	Combo Ports [1 .. 4]	4 порта Gigabit Ethernet 10/100/1000BASE-X (SFP).
10	XG1–XG4	Слоты для установки трансиверов 10G SFP+/1G SFP.
11	XLG1–XLG2	Слоты для установки трансиверов 40G QSFP+.

Передняя панель устройства ESR-1500

Внешний вид передней панели ESR-1500 показан на рисунке 35.

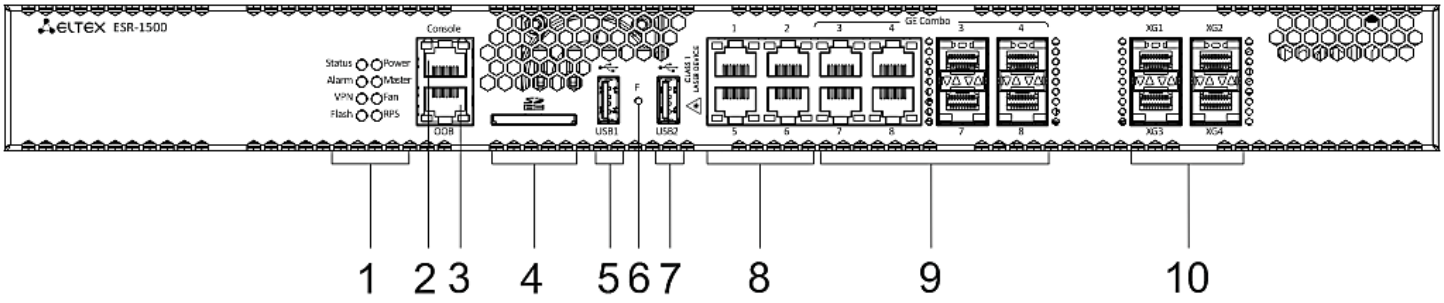


Рисунок 35 – Передняя панель ESR-1500

В таблице 27 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели ESR-1500.

Таблица 27 – Описание разъемов, индикаторов и органов управления передней панели ESR-1500

№	Элемент передней панели	Описание
1	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	VPN	Индикатор режима работы в режиме VPN-шлюза (не используется в текущей версии).
	Flash	Индикатор активности обмена с накопителем данных – SD-картой или USB Flash.
	Power	Индикатор питания устройства.
	Master	Индикатор работы устройства в failover-режимах (не используется в текущей версии).
	Fan	Индикатор аварии вентиляторов.

№	Элемент передней панели	Описание
	RPS	Индикатор резервного источника электропитания.
2	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
3	OOB	Ethernet-порт используется только для обновления программного обеспечения через загрузчик U-Boot. Данный порт не используется для удаленного доступа и управления.
4	SD	Разъем для установки SD-карт памяти.
5	USB1	Порт для подключения USB-устройств.
6	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при удержании кнопки менее 10 секунд происходит перезагрузка устройства; • при удержании кнопки более 10 секунд происходит перезагрузка устройства и сброс к заводским настройкам.
7	USB2	Порт для подключения USB-устройств.
8	Ethernet	4 порта Ethernet 10/100/1000BASE-T.
9	Combo Ports [1 .. 4]	4 порта Gigabit Ethernet 10/100/1000BASE-X (SFP).
10	XG1–XG4	Слоты для установки трансиверов 10G SFP+/1G SFP.

Задняя панель устройств ESR-1511 rev.B, ESR-1511, ESR-1500

Внешний вид задней панели ESR-1511 rev.B, ESR-1511, ESR-1500 приведен на рисунке 36.

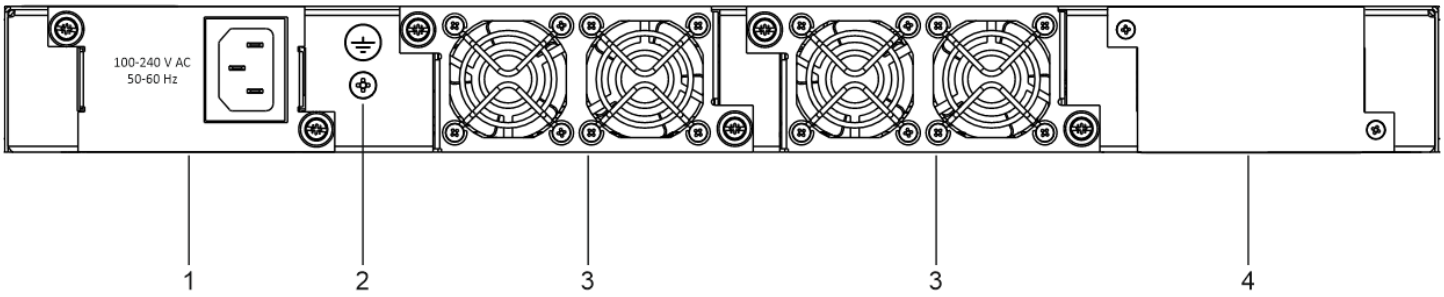


Рисунок 36 – Задняя панель ESR-1511 rev.B, ESR-1511, ESR-1500

В таблице 28 приведен перечень разъемов, расположенных на задней панели ESR-1511 rev.B, ESR-1511, ESR-1500.

Таблица 28 – Описание разъемов задней панели ESR-1511 rev.B, ESR-1511, ESR-1500

№	Описание
1	Основной источник питания.

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

Боковые панели устройств ESR-1511 rev.B, ESR-1511, ESR-1500

Внешний вид боковых панелей ESR-1511 rev.B, ESR-1511, ESR-1500 приведен на рисунках ниже.

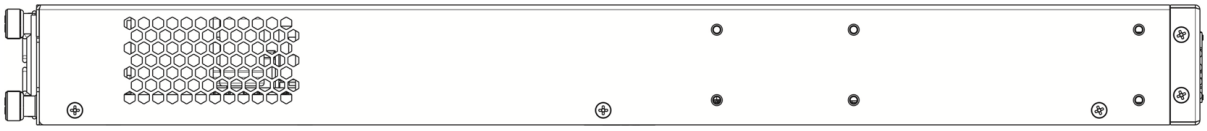


Рисунок 37 – Правая боковая панель ESR-1511 rev.B, ESR-1511, ESR-1500

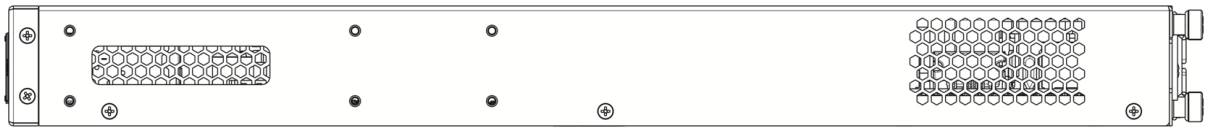


Рисунок 38 – Левая боковая панель ESR-1511 rev.B, ESR-1511, ESR-1500

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

2.4.10 Конструктивное исполнение ESR-1200, ESR-1000

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

Передняя панель устройства ESR-1200

Внешний вид передней панели ESR-1200 показан на рисунке 39.

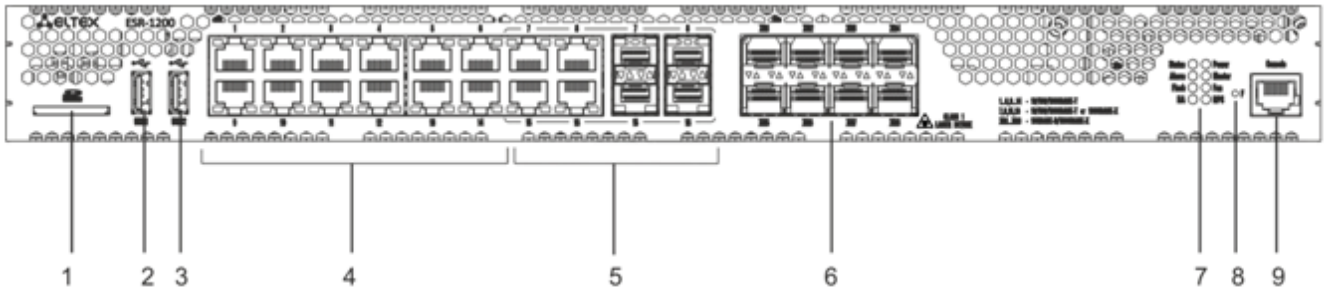


Рисунок 39 – Передняя панель ESR-1200

В таблице 29 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели ESR-1200.

Таблица 29 – Описание разъемов, индикаторов и органов управления передней панели ESR-1200

№	Элемент передней панели	Описание
1	SD	Разъем для установки SD-карт памяти.
2	USB1	Порт для подключения USB-устройств.
3	USB2	Порт для подключения USB-устройств.
4	[1 .. 12]	12 портов Gigabit Ethernet 10/100/1000BASE-T (RJ-45).
5	Combo Ports	4 порта Gigabit Ethernet 10/100/1000BASE-X (SFP).
6	XG1–XG8	Слоты для установки трансиверов 10G SFP+/1G SFP.
7	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	HA	Индикатор режима работы в режиме HA.
	Flash	Индикатор активности обмена с накопителем данных – SD-картой или USB Flash.
	Power	Индикатор питания устройства.
	Master	Индикатор работы устройства в failover-режимах.
	Fan	Индикатор аварии вентиляторов.
	RPS	Индикатор резервного источника электропитания.
8	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при удержании кнопки менее 10 секунд происходит перезагрузка устройства; • при удержании кнопки более 10 секунд происходит перезагрузка устройства и сброс к заводским настройкам.
9	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.

Передняя панель устройства ESR-1000

Внешний вид передней панели ESR-1000 показан на рисунке 40.

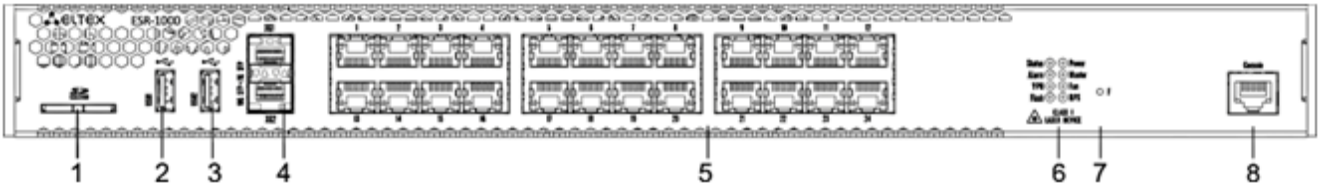


Рисунок 41 – Передняя панель ESR-1000

В таблице 30 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели ESR-1000.

Таблица 30 – Описание разъемов, индикаторов и органов управления передней панели ESR-1000

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

Задняя панель устройств ESR-1200, ESR-1000

Внешний вид задней панели ESR-1200, ESR-1000 приведен на рисунке ниже.

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

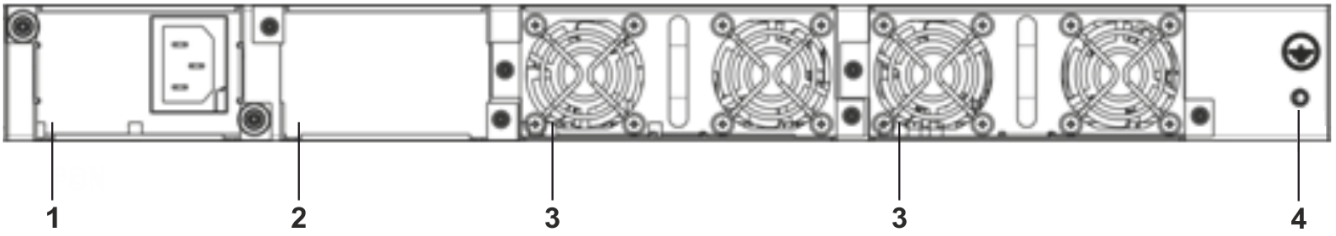


Рисунок 42 – Задняя панель ESR-1200, ESR-1000

В таблице 31 приведен перечень разъемов, расположенных на задней панели ESR-1200, ESR-1000.

Таблица 31 – Описание разъемов задней панели ESR-1200, ESR-1000

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

Боковые панели устройств ESR-1200, ESR-1000

Внешний вид боковых панелей ESR-1200, ESR-1000 приведен на рисунках ниже.

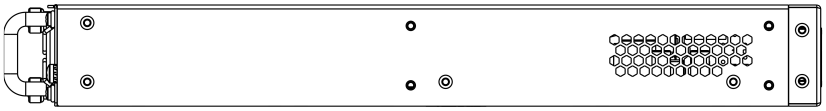


Рисунок 43 – Правая боковая панель ESR-1200, ESR-1000

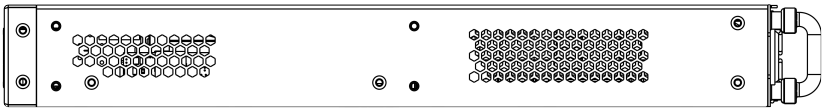


Рисунок 44 – Левая боковая панель ESR-1200, ESR-1000

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

2.4.11 Конструктивное исполнение ESR-200, ESR-100

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

Передняя панель устройств ESR-200, ESR-100

Внешний вид передней панели ESR-200 показан на рисунке 45.

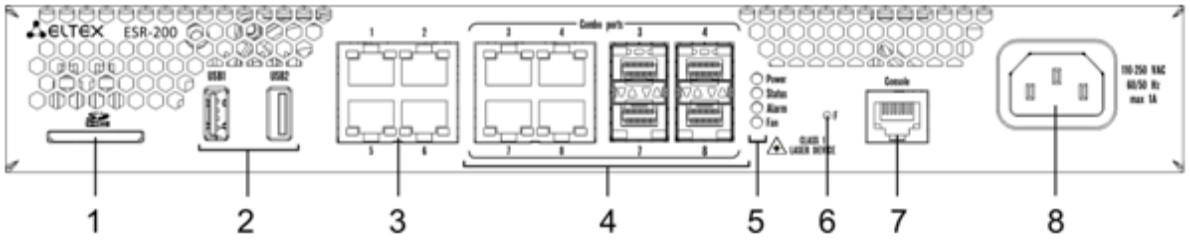


Рисунок 45 – Передняя панель ESR-200

Внешний вид передней панели ESR-100 показан на рисунке 46.

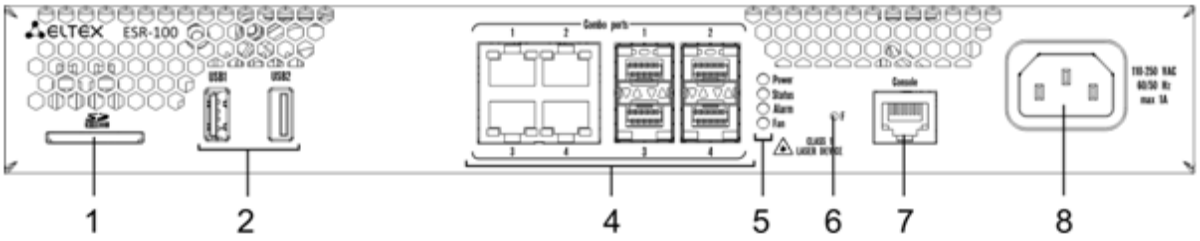


Рисунок 46 – Передняя панель ESR-100

В таблице 32 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели ESR-200, ESR-100.

Таблица 32 – Описание разъемов, индикаторов и органов управления передней панели ESR-200, ESR-100

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

№	Элемент передней панели	Описание
	Fan	Индикатор аварии вентиляторов.
6	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при удержании кнопки менее 10 секунд происходит перезагрузка устройства; • при удержании кнопки более 10 секунд происходит перезагрузка устройства и сброс к заводским настройкам.
7	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
8	110-250 VAC 60/50 Hz max 1A	Источник питания.

Задняя панель устройств ESR-200, ESR-100

Внешний вид задней панели ESR-200, ESR-100 приведен на рисунке 47.

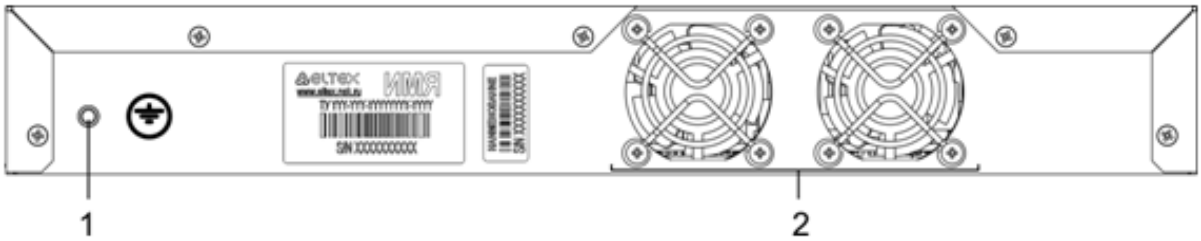


Рисунок 47 – Задняя панель ESR-200, ESR-100

В таблице 33 приведен перечень разъемов, расположенных на задней панели ESR-200, ESR-100.

Таблица 33 – Описание разъемов задней панели ESR-200, ESR-100

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

Боковые панели устройств ESR-200, ESR-100

Внешний вид боковых панелей ESR-200, ESR-100 приведен на рисунках ниже.



Рисунок 48 – Правая боковая панель ESR-200, ESR-100



Рисунок 49 – Левая боковая панель ESR-200, ESR-100

2.4.12 Конструктивное исполнение ESR-31

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

Передняя панель устройства ESR-31

Внешний вид передней панели ESR-31 показан на рисунке 50.

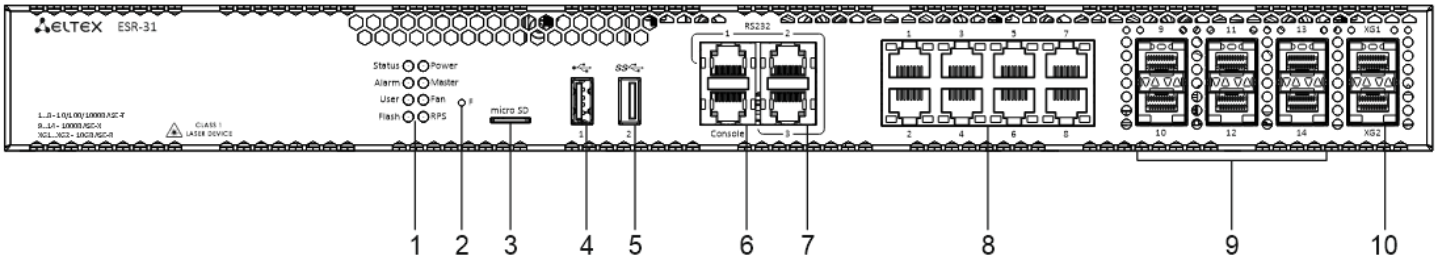


Рисунок 51 – Передняя панель ESR-31

В таблице 34 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели ESR-31.

Таблица 34 – Описание разъемов, индикаторов и органов управления передней панели ESR-31

№	Элемент передней панели	Описание
1	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	User	Индикатор, использующийся для пользовательских сценариев, которые можно назначить в режиме конфигурирования устройства.
	Flash	Индикатор активности обмена с накопителем данных – microSD-картой или USB Flash.
	Power	Индикатор питания устройства.

№	Элемент передней панели	Описание
	Master	Индикатор работы устройства в failover-режимах (не используется в текущей версии).
	Fan	Индикатор аварии вентиляторов.
	RPS	Индикатор резервного источника электропитания.
2	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при удержании кнопки менее 10 секунд происходит перезагрузка устройства; • при удержании кнопки более 10 секунд происходит перезагрузка устройства и сброс к заводским настройкам.
3	microSD	Разъем для установки microSD-карты памяти.
4	USB1	Порт USB 2.0 для подключения USB-устройств.
5	USB2	Порт USB 3.0 для подключения USB-устройств.
6	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
7	RS-232	3 последовательных порта.
8	[1 .. 8]	8 портов Gigabit Ethernet 10/100/1000BASE-T (RJ-45).
9	Optical Port	6 портов Gigabit Ethernet 10/100/1000BASE-X (SFP).
10	XG1 – XG2	Слоты для установки трансиверов 10G SFP+/1G SFP.

Задняя панель устройств ESR-31

Внешний вид задней панели ESR-31 показан на рисунке 52.

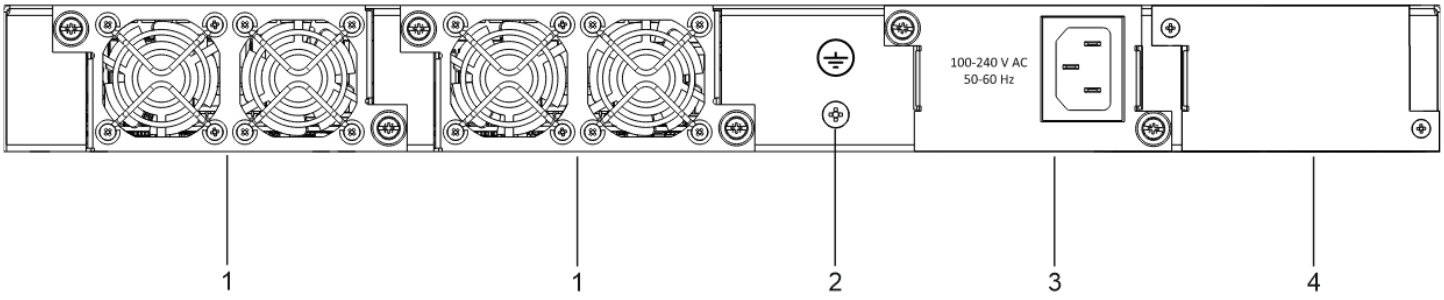


Рисунок 52 – Задняя панель ESR-31

В таблице 35 приведен перечень разъемов, расположенных на задней панели ESR-31.

Таблица 35 – Описание разъемов задней панели ESR-31

№	Описание
1	Съемные вентиляционные модули с возможностью горячей замены.

№	Описание
2	Клемма для заземления устройства.

Боковые панели устройства ESR-31

Внешний вид боковых панелей ESR-31 приведен на рисунках ниже.

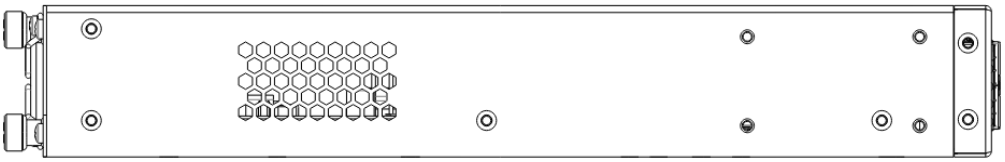


Рисунок 53 – Левая панель ESR-31

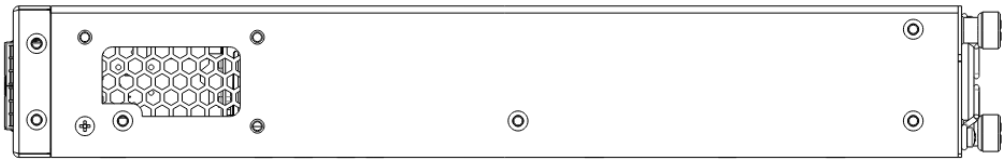


Рисунок 54 – Правая панель ESR-31

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

2.4.13 Конструктивное исполнение ESR-21

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

Передняя панель устройства ESR-21

Внешний вид передней панели ESR-21 показан на рисунке 55.

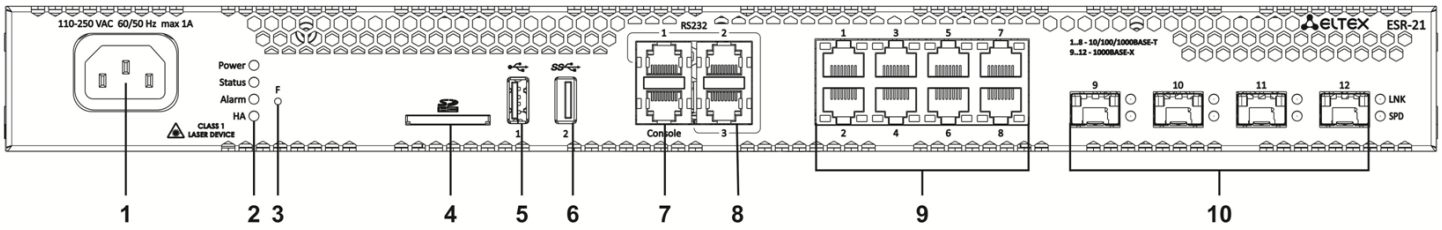


Рисунок 55 – Передняя панель ESR-21

В таблице 36 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели ESR-21.

Таблица 36 – Описание разъемов, индикаторов и органов управления передней панели ESR-21

№	Элемент передней панели	Описание
1	220V AC	Источник питания.

№	Элемент передней панели	Описание
2	Power	Индикатор питания устройства.
	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	HA	Индикатор работы в режиме HA (не используется в текущей версии).
3	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при удержании кнопки менее 10 секунд происходит перезагрузка устройства; • при удержании кнопки более 10 секунд происходит перезагрузка устройства и сброс к заводским настройкам.
4	SD	Разъем для установки SD-карт памяти.
5	USB1	Разъем USB 2.0 для подключения внешних USB-устройств.
6	USB2	Разъем USB 3.0 для подключения внешних USB-устройств.
7	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
8	RS-232	3 последовательных порта.
9	[1 .. 8]	8 портов Gigabit Ethernet 10/100/1000BASE-T (RJ-45).
10	Optical Port	4 порта Gigabit Ethernet 10/100/1000BASE-X (SFP).

Задняя панель устройств ESR-21

Внешний вид задней панели ESR-21 показан на рисунке 56.

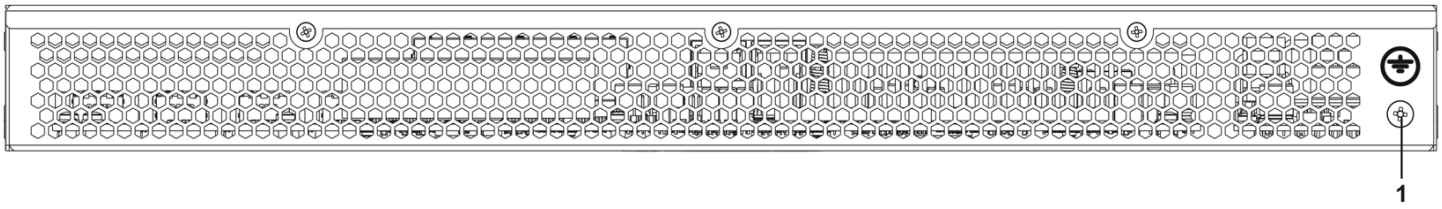


Рисунок 56 – Задняя панель ESR-21

В таблице 37 приведен перечень разъемов, расположенных на задней панели ESR-21.

Таблица 37 – Описание разъемов задней панели ESR-21

№	Описание
1	Клемма для заземления устройства.

Боковые панели устройства ESR-21

Внешний вид боковых панелей ESR-21 приведен на рисунках ниже.

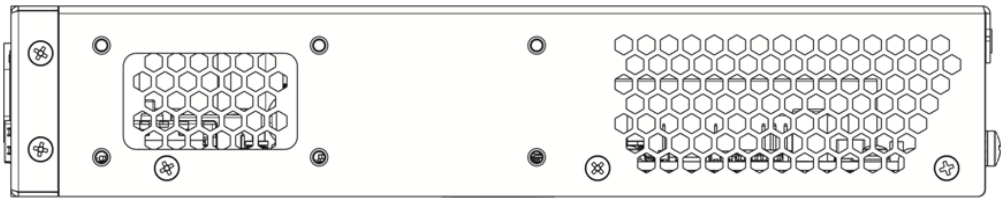


Рисунок 57 – Левая боковая панель ESR-21

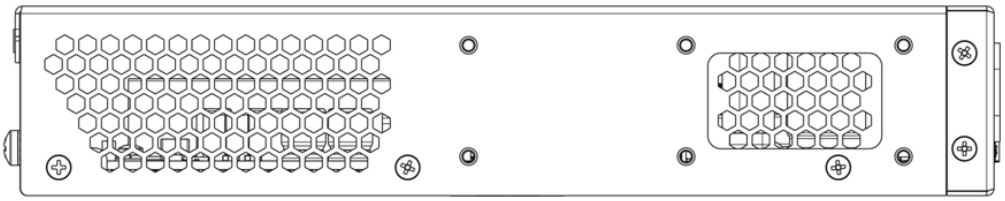


Рисунок 58 – Правая боковая панель ESR-21

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

2.4.14 Конструктивное исполнение ESR-30, ESR-20

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

Передняя панель устройства ESR-30

Внешний вид передней панели ESR-30 показан на рисунке 59.

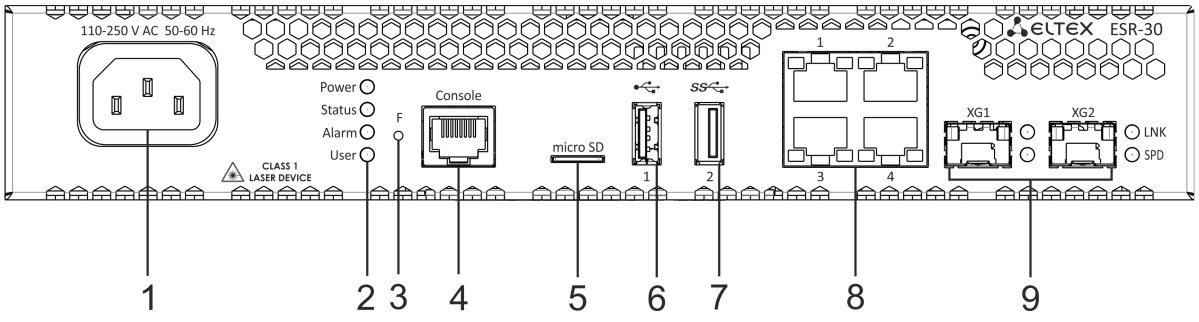


Рисунок 59 – Передняя панель ESR-30

В таблице 38 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели ESR-30.

Таблица 38 – Описание разъемов, индикаторов и органов управления передней панели ESR-30

№	Элемент передней панели	Описание
1	110-250 V AC	Источник питания.
2	Power	Индикатор питания устройства.
	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	User	Индикатор, использующийся для пользовательских сценариев, которые можно назначить в режиме конфигурирования устройства.
3	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при удержании кнопки менее 10 секунд происходит перезагрузка устройства; • при удержании кнопки более 10 секунд происходит перезагрузка устройства и сброс к заводским настройкам.
4	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
5	microSD	Разъем для установки microSD-карт памяти.
6	USB1	Разъем USB 2.0 для подключения внешних USB-устройств.
7	USB2	Разъем USB 3.0 для подключения внешних USB-устройств.
8	[1 .. 4]	4 порта Ethernet 10/100/1000BASE-T.
9	1, 2	2 порта 10GBASE-R (SPF+)/1000BASE-X.

Передняя панель устройства ESR-20

Внешний вид передней панели ESR-20 показан на рисунке 60.

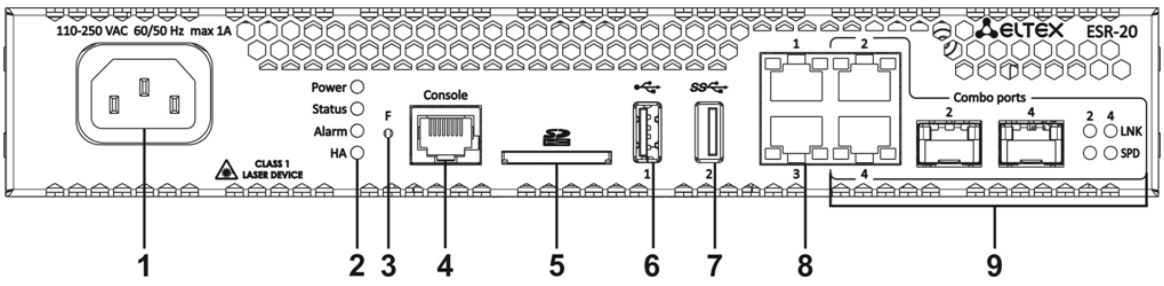


Рисунок 60 – Передняя панель ESR-20

В таблице 39 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели ESR-20.

Таблица 39 – Описание разъемов, индикаторов и органов управления передней панели ESR-20

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

Задняя панель устройств ESR-30, ESR-20

Внешний вид задней панели ESR-30, ESR-20 показан на рисунке 61.

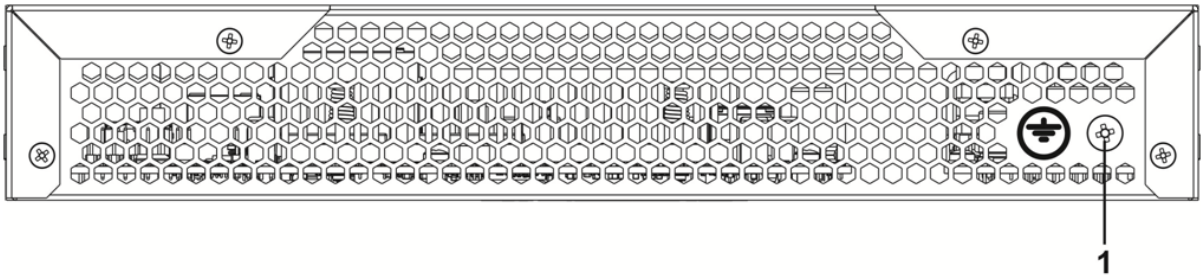


Рисунок 61 – Задняя панель ESR-30, ESR-20

В таблице 40 приведен перечень разъемов, расположенных на задней панели ESR-30, ESR-20.

Таблица 40 – Описание разъемов задней панели ESR-30, ESR-20

№	Описание
1	Клемма для заземления устройства.

Боковые панели устройств ESR-30, ESR-20

Внешний вид боковых панелей ESR-30, ESR-20 приведен на рисунках ниже.

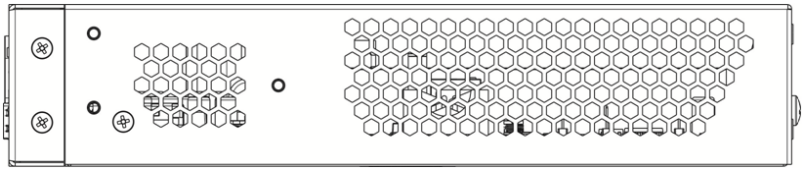


Рисунок 62 – Левая боковая панель ESR-30, ESR-20

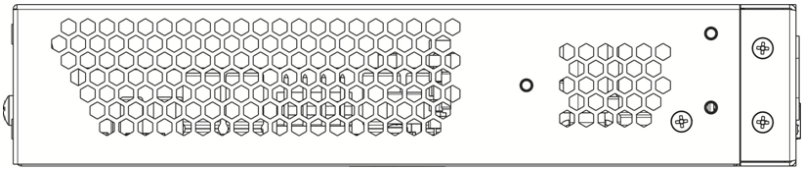


Рисунок 63 – Правая боковая панель ESR-30, ESR-20

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

2.4.15 Конструктивное исполнение ESR-15VF

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

Передняя панель устройства ESR-15VF

Внешний вид передней панели ESR-15VF показан на рисунке 64.

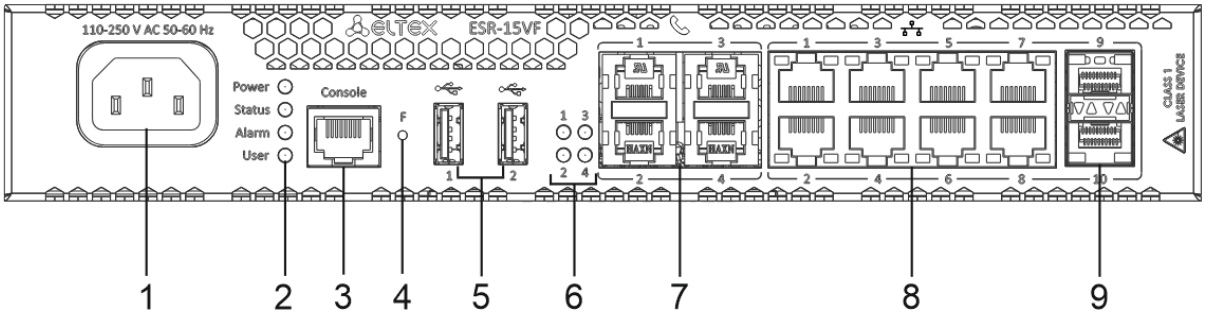


Рисунок 64 – Передняя панель ESR-15VF

В таблице 41 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели ESR-15VF.

Таблица 41 – Описание разъемов, индикаторов и органов управления передней панели ESR-15VF

№	Элемент передней панели	Описание
1	110-250 V AC	Источник питания.
2	Power	Индикатор питания устройства.
	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	User	Индикатор, использующийся для пользовательских сценариев, которые можно назначить в режиме конфигурирования устройства.
3	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
4	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при длительности нажатия на кнопку менее 10 секунд происходит перезагрузка устройства; • при длительности нажатия на кнопку более 10 секунд происходит сброс устройства к заводской конфигурации.
5	USB1	Разъем для подключения внешних USB-устройств.
	USB2	Разъем для подключения внешних USB-устройств.

№	Элемент передней панели	Описание
6	1, 2, 3, 4	Индикатор для внутренних абонентских терминалов.
7	FXS	4 разъема для внутренних абонентских терминалов.
8	[1 .. 8]	4 порта Gigabit Ethernet 10/100/1000BASE-T (RJ-45).
9	9, 10	2 порта Gigabit Ethernet 1000BASE-X SFP.

Задняя панель устройств ESR-15VF

Внешний вид задней панели ESR-15VF показан на рисунке 65.

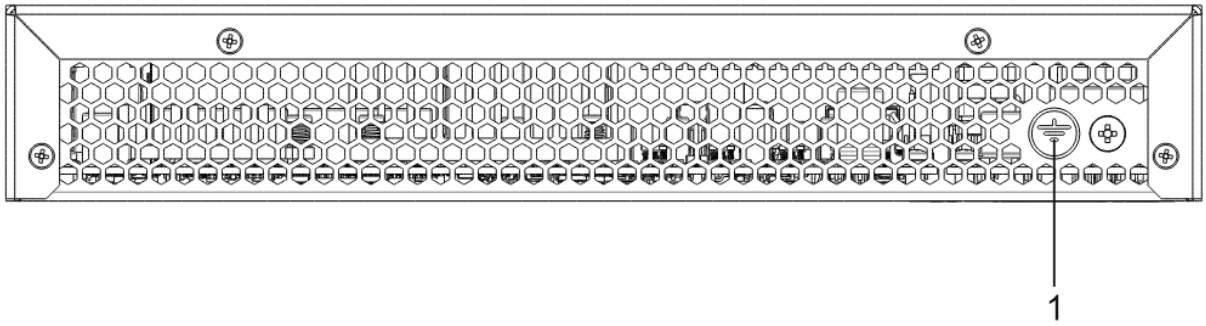


Рисунок 65 – Задняя панель ESR-15VF

В таблице 42 приведен перечень разъемов, расположенных на задней панели ESR-15VF.

Таблица 42 – Описание разъемов задней панели ESR-15VF

№	Описание
1	Клемма для заземления устройства.

Боковые панели устройства ESR-15VF

Внешний вид боковых панелей ESR-15VF приведен на рисунках ниже.

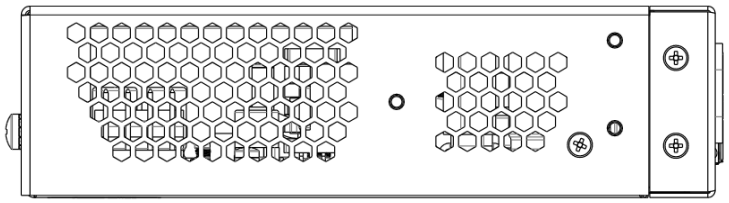


Рисунок 66 – Левая панель ESR-15VF

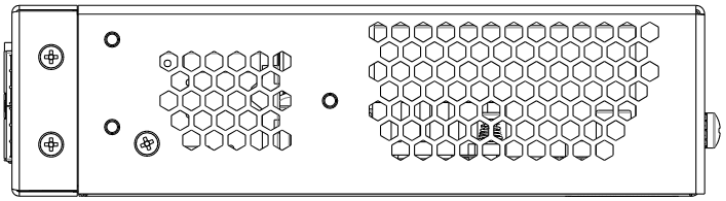


Рисунок 67 – Правая панель ESR-15VF

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

2.4.16 Конструктивное исполнение ESR-15R

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

Передняя панель устройства ESR-15R

Внешний вид передней панели ESR-15R показан на рисунке 68.

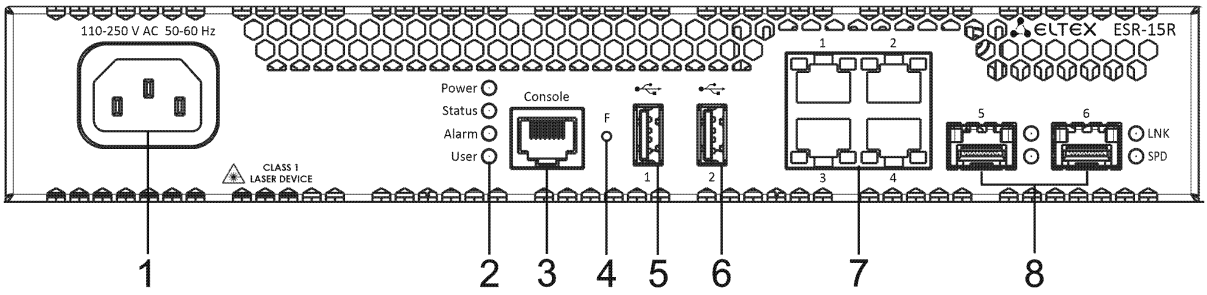


Рисунок 68 – Передняя панель ESR-15R

В таблице 43 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели ESR-15R.

Таблица 43 – Описание разъемов, индикаторов и органов управления передней панели ESR-15R

№	Элемент передней панели	Описание
1	110-250V AC	Источник питания.
2	Power	Индикатор питания устройства.
	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	User	Индикатор, использующийся для пользовательских сценариев, которые можно назначить в режиме конфигурирования устройства.
3	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
4	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при длительности нажатия на кнопку менее 10 секунд происходит перезагрузка устройства; • при длительности нажатия на кнопку более 10 секунд происходит сброс устройства к заводской конфигурации.

№	Элемент передней панели	Описание
5	USB1	Разъем для подключения внешних USB-устройств.
6	USB2	Разъем для подключения внешних USB-устройств.
7	[1 .. 4]	4 порта Gigabit Ethernet 10/100/1000BASE-T (RJ-45).
8	5, 6	2 порта Gigabit Ethernet 1000BASE-X SFP.

Задняя панель устройств ESR-15R

Внешний вид задней панели ESR-15R показан на рисунке 69.

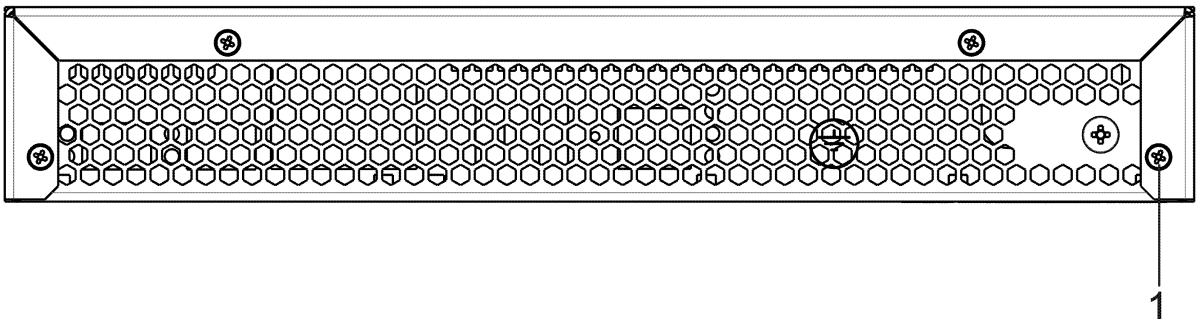


Рисунок 69 – Задняя панель ESR-15R

В таблице 44 приведен перечень разъемов, расположенных на задней панели ESR-15R.

Таблица 44 – Описание разъемов задней панели ESR-15R

№	Описание
1	Клемма для заземления устройства.

Боковые панели устройства ESR-15R

Внешний вид боковых панелей ESR-15R приведен на рисунках ниже.

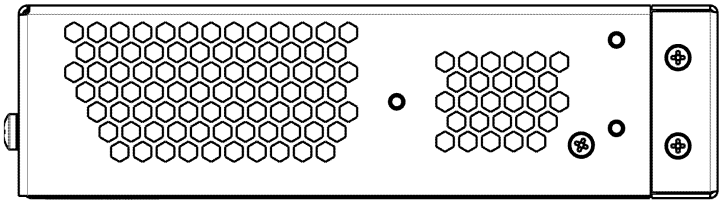


Рисунок 70 – Левая боковая панель ESR-15R

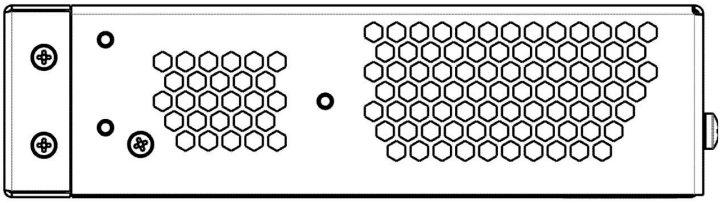


Рисунок 71 – Правая боковая панель ESR-15R

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

2.4.17 Конструктивное исполнение ESR-15

Задняя панель устройства ESR-15

Внешний вид задней панели ESR-15 показан на рисунке 72.

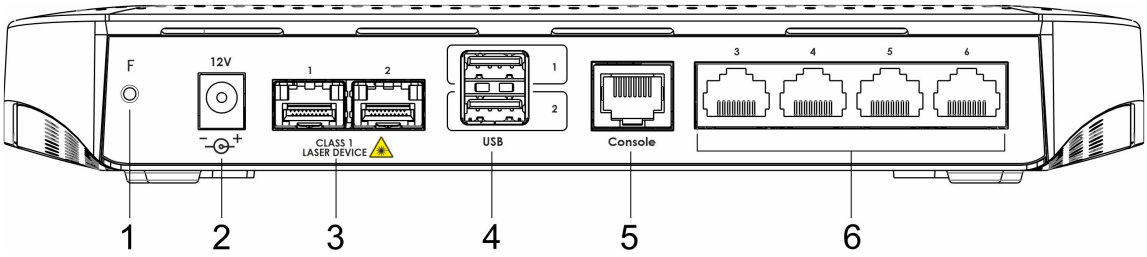


Рисунок 72 – Задняя панель ESR-15

В таблице 45 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на задней панели ESR-15.

Таблица 45 – Описание разъемов, индикаторов и органов управления задней панели ESR-15

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

Верхняя панель устройства ESR-15

Внешний вид верхней панели ESR-15 показан на рисунке 73.

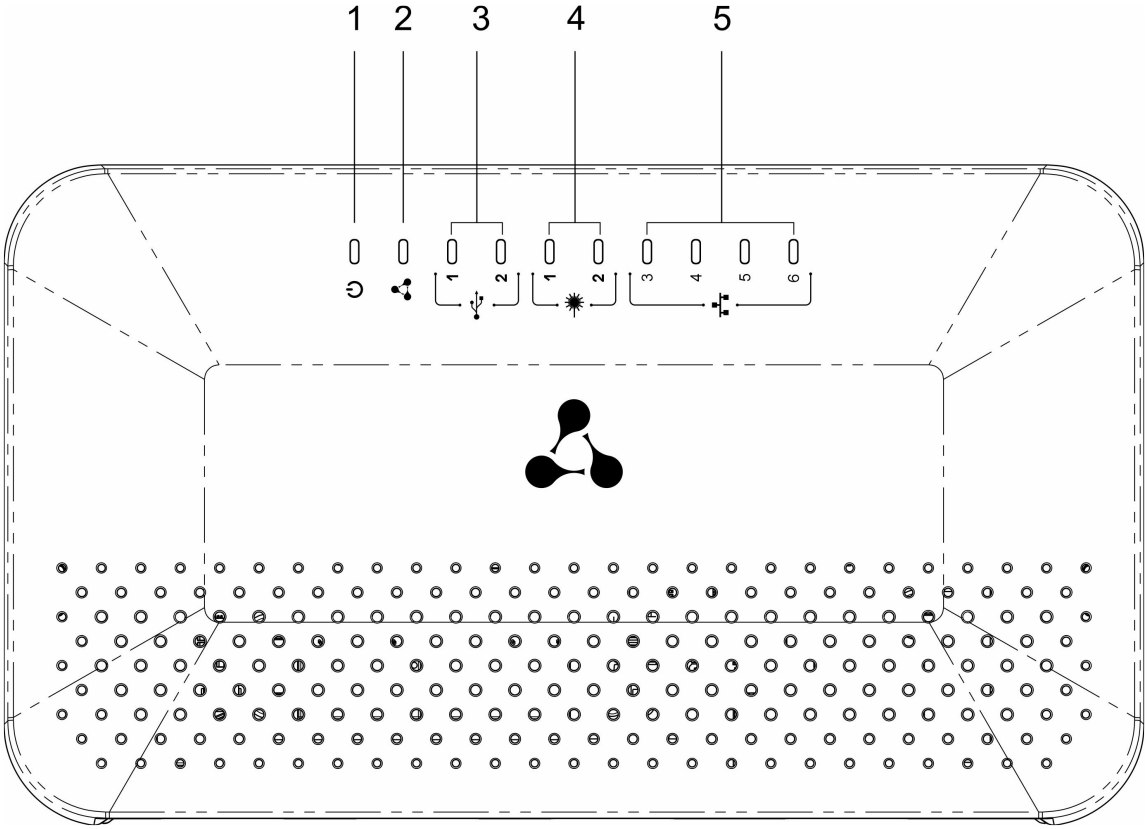


Рисунок 73 – Верхняя панель ESR-15

В таблице 46 приведен перечень светодиодных индикаторов, расположенных на верхней панели ESR-15.

Таблица 46 – Описание индикаторов верхней панели ESR-15

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

2.4.18 Конструктивное исполнение ESR-12VF

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

Передняя панель устройства ESR-12VF

Внешний вид передней панели ESR-12VF показан на рисунке 74.

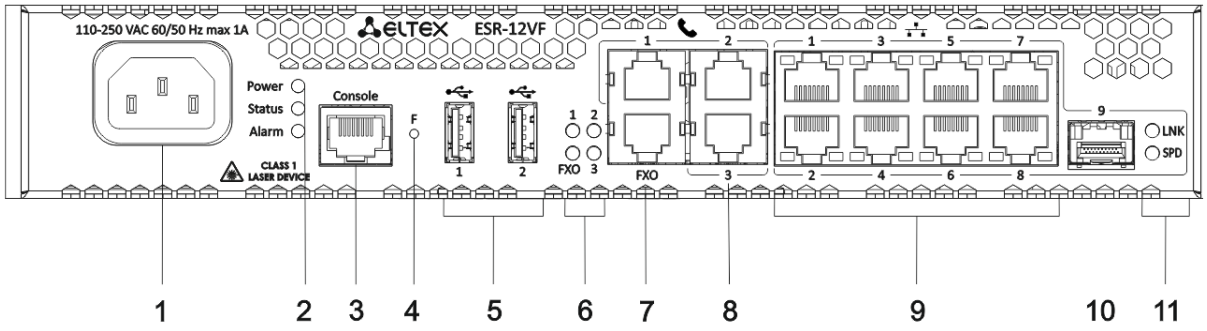


Рисунок 74 – Передняя панель ESR-12VF

В таблице 47 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели ESR-12VF.

Таблица 47 – Описание разъемов, индикаторов и органов управления передней панели ESR-12VF

№	Элемент передней панели	Описание
1	220 V AC	Источник питания.
2	Power	Индикатор питания устройства.
3	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
4	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при удержании кнопки менее 10 секунд происходит перезагрузка устройства; • при удержании кнопки более 10 секунд происходит перезагрузка устройства и сброс к заводским настройкам.
5	USB1, USB2	2 разъема USB для подключения внешних USB-устройств.
6	FXO	Индикатор внешней абонентской линии от ТфОП.
	1, 2, 3	Индикатор для внутренних абонентских терминалов.
7	FXO	1 разъем FXO для подключения внешней абонентской линии от ТфОП.
8	FXS 1, FXS 2, FXS 3	3 разъема для внутренних абонентских терминалов.
9	[1 .. 8]	8 портов Gigabit Ethernet 10/100/1000BASE-T (RJ-45).

№	Элемент передней панели	Описание
10	Optical Port	1 порт Gigabit Ethernet-100/1000BASE-X (SFP).
11	1, 2	Индикаторы работы оптических интерфейсов.

Задняя панель устройства ESR-12VF

Внешний вид задней панели ESR-12VF показан на рисунке 75.

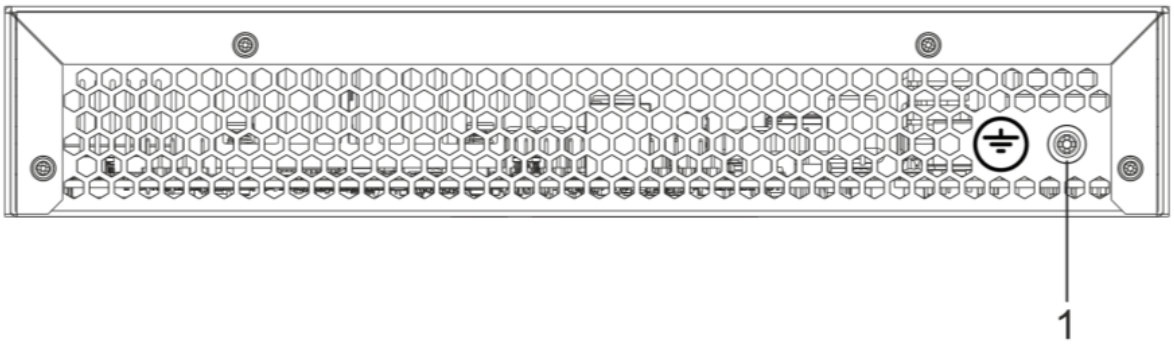


Рисунок 75 – Задняя панель ESR-12VF

В таблице 48 приведен перечень разъемов, расположенных на задней панели ESR-12VF.

Таблица 48 – Описание разъемов задней панели ESR-12VF

№	Описание
1	Клемма для заземления устройства.

Боковые панели устройства ESR-12VF

Внешний вид боковых панелей ESR-12VF приведен на рисунках ниже.

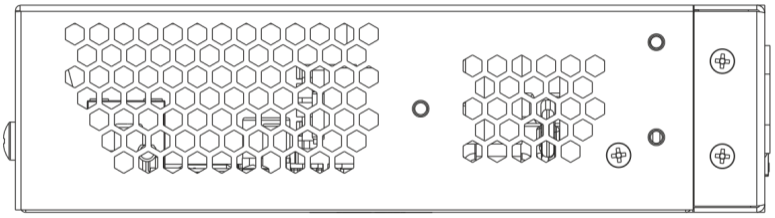


Рисунок 76 – Левая боковая панель ESR-12VF

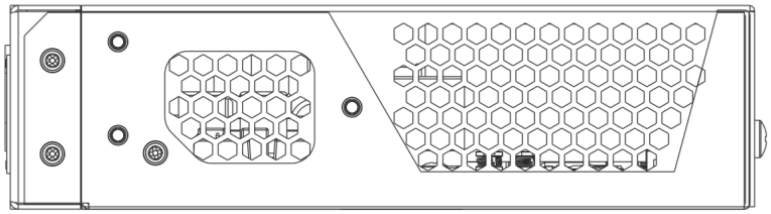


Рисунок 77 – Правая боковая панель ESR-12VF

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

2.4.19 Конструктивное исполнение ESR-12V

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

Передняя панель устройства ESR-12V

Внешний вид передней панели ESR-12V показан на рисунке 78.

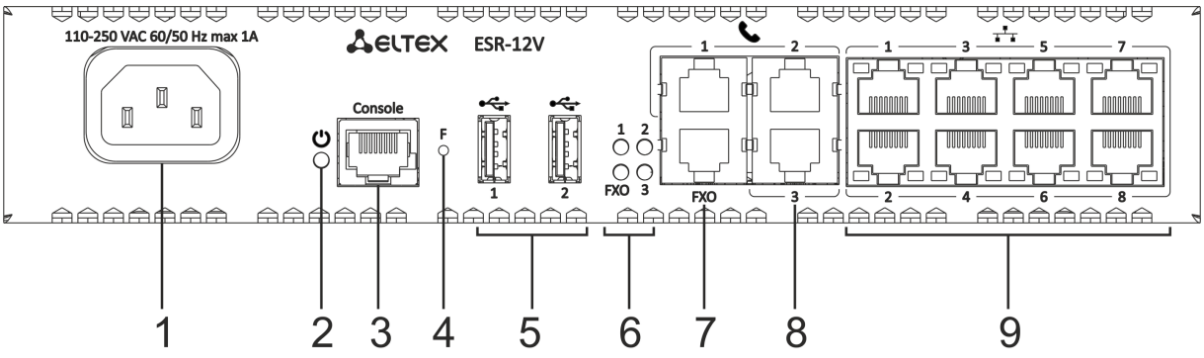


Рисунок 78 – Передняя панель ESR-12V

В таблице 49 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели ESR-12V.

Таблица 49 – Описание разъемов, индикаторов и органов управления передней панели ESR-12V

№	Элемент передней панели	Описание
1	220V AC	Источник питания.
2	Power	Индикатор питания устройства.
3	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
4	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при удержании кнопки менее 10 секунд происходит перезагрузка устройства; • при удержании кнопки более 10 секунд происходит перезагрузка устройства и сброс к заводским настройкам.
5	USB1, USB2	2 разъема USB для подключения внешних USB-устройств.
6	FXO	Индикатор внешней абонентской линии от ТфОП.
	1,2,3	Индикатор для внутренних абонентских терминалов.
7	FXO	1 разъем FXO для подключения внешней абонентской линии от ТфОП.
8	FXS 1, FXS 2, FXS 3	3 разъема для внутренних абонентских терминалов.
9	[1 .. 8]	8 портов Gigabit Ethernet 10/100/1000BASE-T (RJ-45).

Задняя панель устройств ESR-12V

Внешний вид задней панели ESR-12V показан на рисунке 79.

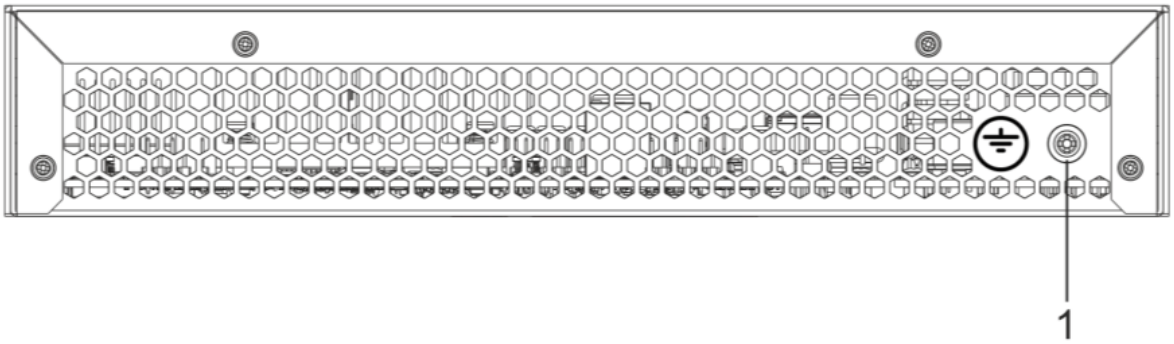


Рисунок 79 – Задняя панель ESR-12V

В таблице 50 приведен перечень разъемов, расположенных на задней панели ESR-12V.

Таблица 50 – Описание разъемов задней панели ESR-12V

№	Описание
1	Клемма для заземления устройства.

Боковые панели устройства ESR-12V

Внешний вид боковых панелей ESR-12V приведен на рисунках ниже.

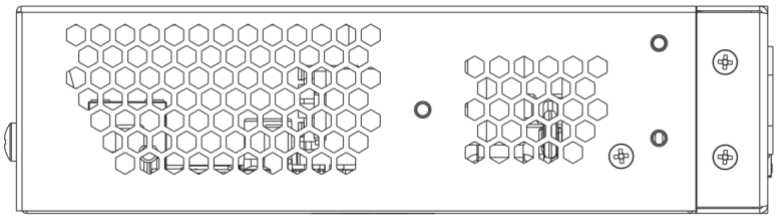


Рисунок 80 – Левая боковая панель ESR-12V

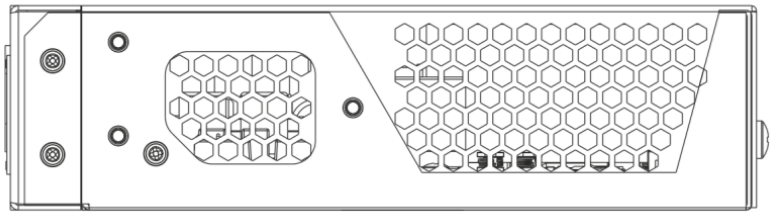


Рисунок 81 – Правая боковая панель ESR-12V

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

2.4.20 Конструктивное исполнение ESR-10

Задняя панель устройства ESR-10

Внешний вид задней панели ESR-10 показан на рисунке 82.

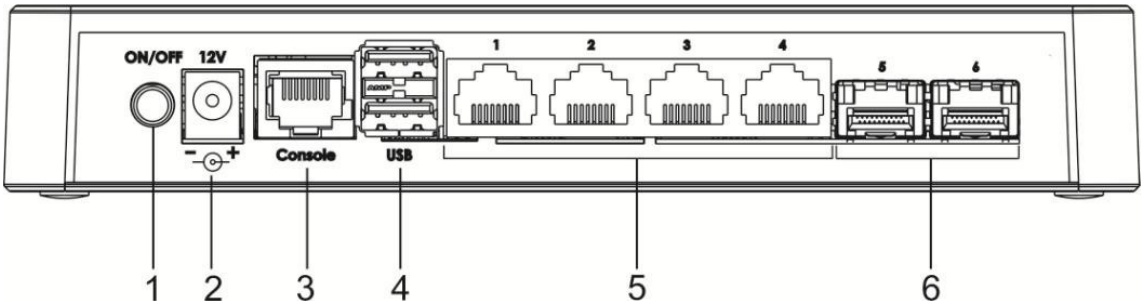


Рисунок 82 – Задняя панель ESR-10

В таблице 51 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на задней панели ESR-10.

Таблица 51 – Описание разъемов, индикаторов и органов управления задней панели ESR-10

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

Боковые панели устройства ESR-10

Внешний вид боковой панели ESR-10 показан на рисунке 83.

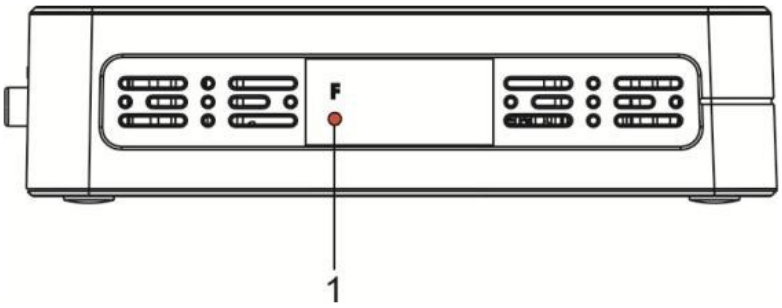


Рисунок 83 – Боковая панель ESR-10

В таблице 52 приведен перечень органов управления, расположенных на боковой панели ESR-10.

Таблица 52 – Описание разъемов боковой панели ESR-10

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

Верхняя панель устройства ESR-10

Внешний вид верхней панели ESR-10 показан на рисунке 84.

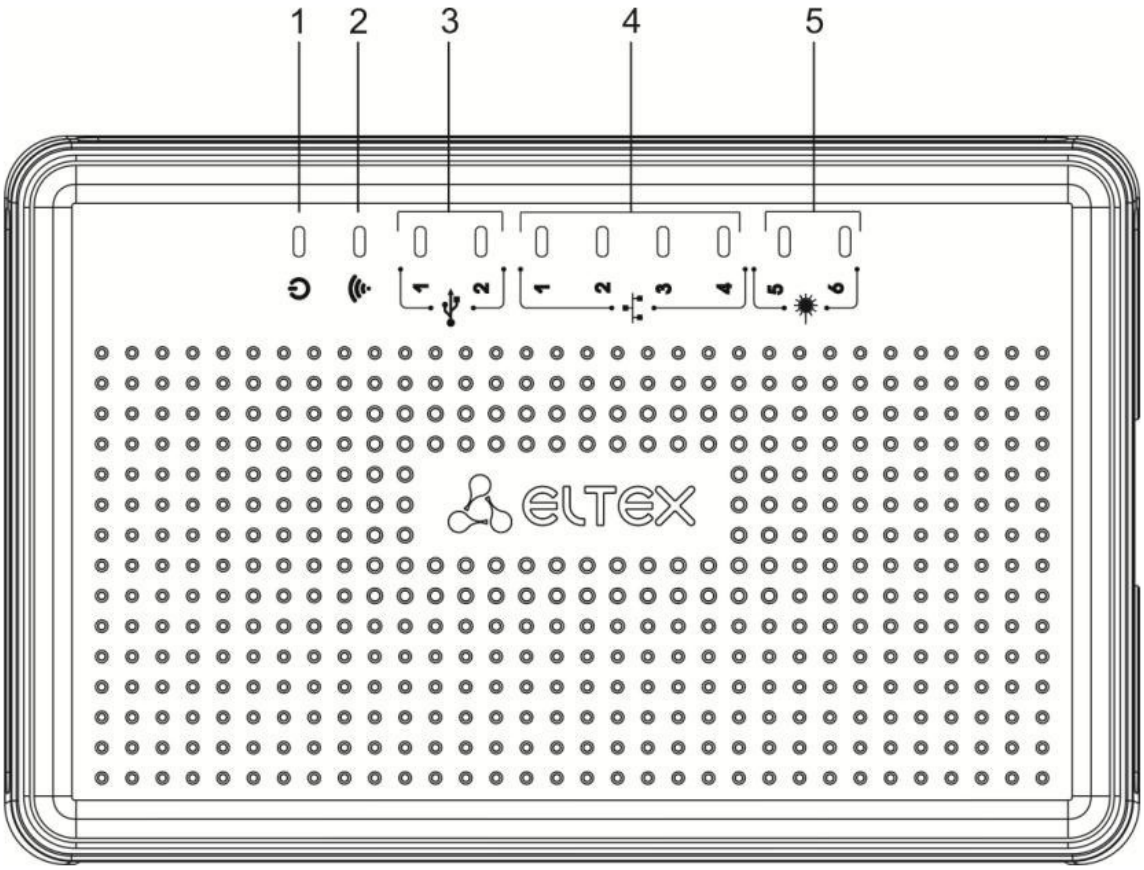


Рисунок 84 – Верхняя панель маршрутизатора ESR-10

В таблице 53 приведен перечень светодиодных индикаторов, расположенных на верхней панели ESR-10.

Таблица 53 – Описание индикаторов верхней панели ESR-10

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

2.4.21 Световая индикация

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

Состояние интерфейсов Ethernet отображается двумя светодиодными индикаторами – *LINK/ACT* зеленого цвета и *SPEED* янтарного цвета. Расположение светодиодных индикаторов интерфейсов показано ниже на рисунках 85 и 86. Значения световой индикации описаны в таблицах 54 и 55 соответственно.

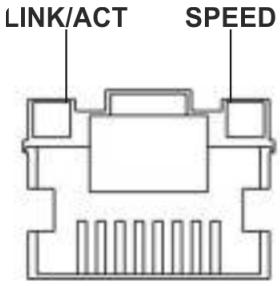


Рисунок 85 – Расположение индикаторов разъема RJ-45

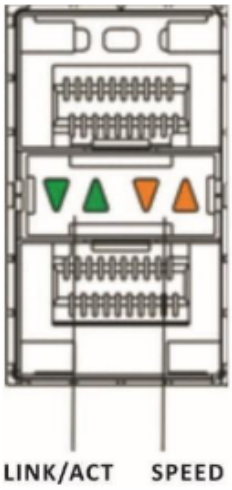


Рисунок 86 – Расположение индикаторов SFP/SFP+/SFP28-интерфейсов

Таблица 54 – Световая индикация состояния RJ-45 интерфейсов

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

Таблица 55 – Световая индикация состояния SFP/SFP+/SFP28-интерфейсов

Свечение индикатора SPEED	Свечение индикатора LINK/ACT	Состояние интерфейса Ethernet
Выключен	Выключен	Порт выключен или соединение не установлено.
Выключен	Горит постоянно зелёным	Установлено соединение на скорости 1 Гбит/с.
Горит постоянно янтарным	Горит постоянно зелёным	Установлено соединение на скорости 10 Гбит/с.
X	Мигает	Идет передача данных.

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

Таблица 56 – Состояния системных индикаторов

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

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
		Красный	Отказ одного или более вентиляторов. Причиной возникновения аварии может быть неработоспособность хотя бы одного из вентиляторов – остановка или пониженная частота оборотов.
RPS	Режим работы резервного источника питания.	Зеленый	Резервный источник установлен и исправен.
		Выключен	Резервный источник не установлен.
		Красный	Отсутствие первичного питания резервного источника или его неисправность.

Световая индикация ESR-3350, ESR-3300, ESR-3250, ESR-3200L, ESR-3200, ESR-3150, ESR-3100, ESR-1511, ESR-1500

Состояние интерфейсов Ethernet отображается двумя светодиодными индикаторами – *LINK/ACT* зеленого цвета и *SPEED* янтарного цвета. Расположение светодиодных индикаторов интерфейсов показано ниже на рисунках 87 и 88. Значения световой индикации описаны в таблицах 57 и 58 соответственно.

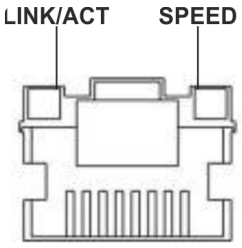


Рисунок 87 – Расположение индикаторов разъема RJ-45

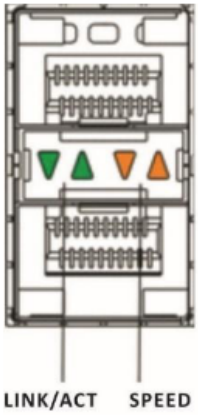


Рисунок 88 – Расположение индикаторов состояния SFP/SFP+/SFP28-интерфейсов

Для модели ESR-3300 состояние интерфейсов QSFP+/QSFP28 отображается четырьмя светодиодными индикаторами зеленого и янтарного цветов, состояние интерфейсов 100G-портов индицируется четырьмя светодиодными индикаторами, *LINK/ACT* зеленого цвета и *SPEED* янтарного цвета. Расположение светодиодов показано на рисунке 89. Значения световой индикации описаны в таблице 59.

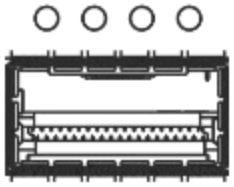


Рисунок 89 – Расположение индикаторов QSFP+/QSFP28 интерфейса для ESR-3300

Таблица 57 – Световая индикация состояния RJ-45 интерфейсов

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

Таблица 58 – Световая индикация состояния состояния SFP/SFP+/SFP28-интерфейсов

Свечение индикатора SPEED	**Свечение индикатора LINK/ ACT**	**Состояние интерфейса Ethernet**
Выключен	Выключен	Порт выключен или соединение не установлено.
Выключен	Горит постоянно зелёным	Установлено соединение на скорости 1 Гбит/с.
Горит постоянно янтарным	Горит постоянно зелёным	Установлено соединение на скорости 10/25 Гбит/с.
X	Мигает	Идет передача данных.

Таблица 59 – Световая индикация состояния QSFP+/QSFP28-интерфейсов

Состояние индикатора				Состояние интерфейса Ethernet
Выключен	Выключен	Выключен	Выключен	Порт выключен или соединение не установлено.
Горит постоянно зелёным	Выключен	Выключен	Выключен	Установлено соединение на скорости 40 Гбит/с.
Горит постоянно зелёным	Выключен	Выключен	Горит постоянно янтарным	Установлено соединение на скорости 100 Гбит/с.
Мигание	X	X	X	Идет передача данных.

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

Таблица 60 – Состояния системных индикаторов

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

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Master	Индикатор работы устройства в failover-режимах.	-	-
Fan	Состояние вентилятора охлаждения.	Зеленый	Все вентиляторы исправны.
		Красный	Отказ одного или более вентиляторов. Причиной возникновения аварии может быть неработоспособность хотя бы одного из вентиляторов – остановка или пониженная частота оборотов.
RPS	Режим работы резервного источника питания.	Зеленый	Резервный источник установлен и исправен.
		Выключен	Резервный источник не установлен.
		Красный	Отсутствие первичного питания резервного источника или его неисправность.

Световая индикация ESR-200, ESR-100

Состояние интерфейсов Ethernet отображается двумя светодиодными индикаторами – *LINK/ACT* зеленого цвета и *SPEED* янтарного цвета. Расположение индикаторов RJ-45-интерфейса показано на рисунке 87. Расположение индикаторов SFP/SFP+-интерфейсов указано на рисунке 90. Значения световой индикации описаны в таблице 61.

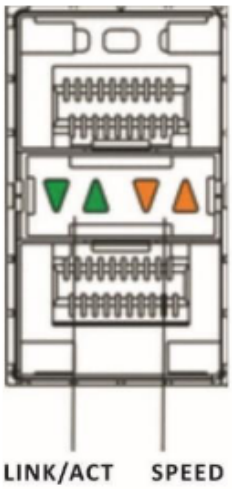


Рисунок 90 – Расположение индикаторов состояния SFP/SFP+-интерфейсов

Таблица 61 – Световая индикация состояния интерфейсов Ethernet

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

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

Таблица 62 – Состояния системных индикаторов

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Status	Индикатор текущего состояния устройства.	Зеленый	Устройство работает нормально.
		Красный	Устройство находится в состоянии загрузки ПО.
Alarm	Индикатор наличия и уровня аварии устройства(не поддерживается в текущей версии ПО).	-	-
Power	Индикатор питания устройства.	Зеленый	Питание устройства в норме. Основной источник питания, если он установлен, работает нормально.
		Красный	Неработоспособность основного источника питания, авария или отсутствие первичной сети.
		Выключен	Отказ внутренних источников питания устройства.
Fan	Состояние вентилятора охлаждения.	Выключен	Все вентиляторы исправны.
		Красный	Отказ одного или более вентиляторов. Причиной возникновения аварии может быть неработоспособность хотя бы одного из вентиляторов – остановка или пониженная частота оборотов.

Световая индикация ESR-31, ESR-30

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

Таблица 63 – Световая индикация состояния интерфейсов Ethernet

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

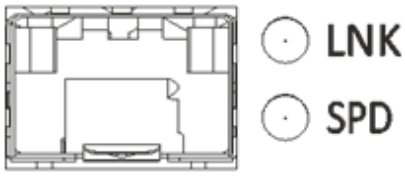


Рисунок 91 – Расположение индикаторов состояния SFP/SFP+-интерфейсов

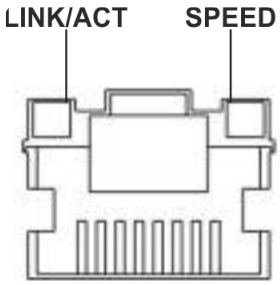


Рисунок 92 – Расположение индикаторов разъема RJ-45

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

Таблица 64 – Состояния системных индикаторов

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Power	Индикатор питания устройства.	Зеленый	Питание устройства в норме. Источник питания работает нормально, основное ПО прогружено.
		Красный	Не прогружено основное ПО.

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
		Выключен	Отказ внутренних источников питания устройства.
Status	Индикатор текущего состояния устройства.	Зеленый	Устройство работает нормально.
		Мигает зеленым	Устройство находится в состоянии загрузки ПО.
Alarm	Индикатор наличия и уровня аварии устройства.	-	-
User	Индикатор, использующийся для пользовательских сценариев, которые можно назначить в режиме конфигурирования устройства.	-	-
Flash	Индикатор активности обмена с накопителем данных: SD-картой или USB Flash.	Зеленый	Выполнение операций чтения/записи по команде «copy».
Master	Индикатор работы устройства в failover-режимах (только для ESR-31).	-	-
Fan	Состояние вентилятора охлаждения (только для ESR-31).	Зеленый	Все вентиляторы исправны.
		Красный	Отказ одного или более вентиляторов. Причиной возникновения аварии может быть неработоспособность хотя бы одного из вентиляторов – остановка или пониженная частота оборотов.
RPS	Режим работы резервного источника питания (только для ESR-31).	Зеленый	Резервный источник установлен и исправен.
		Выключен	Резервный источник не установлен.
		Красный	Отсутствие первичного питания резервного источника или его неисправность.

Световая индикация ESR-21, ESR-20

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

Таблица 65 – Световая индикация состояния интерфейсов Ethernet

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

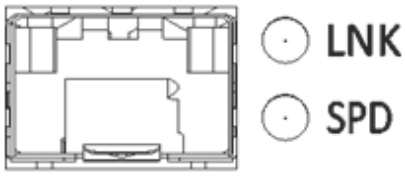


Рисунок 93 – Расположение индикаторов состояния SFP/SFP+-интерфейсов

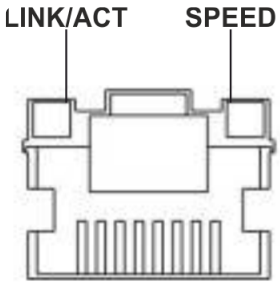


Рисунок 94 – Расположение индикаторов разъема RJ-45

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

Таблица 66 – Состояния системных индикаторов

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Power	Индикатор питания устройства.	Зеленый	Питание устройства в норме. Источник питания работает нормально, основное ПО прогружено.
		Красный	Не прогружено основное ПО.
		Выключен	Отказ внутренних источников питания устройства.

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Status	Индикатор текущего состояния устройства.	Зеленый	Устройство работает нормально.
		Красный	Устройство находится в состоянии загрузки ПО.
Alarm	Индикатор наличия и уровня аварии устройства.	-	-
HA	Индикатор работы в режиме HA (не используется в текущей версии)	-	-

Световая индикация ESR-15VF

Состояние интерфейсов Ethernet отображается двумя светодиодными индикаторами – *LINK/ACT* зеленого цвета и *SPEED* янтарного цвета. Состояние интерфейсов FXS отображается одним светодиодным индикатором зелёного цвета.

Таблица 67 – Световая индикация состояния медных интерфейсов

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

Таблица 68 – Световая индикация состояния SFP-интерфейсов

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

Таблица 69 − Световая индикация FXS-интерфейсов

Свечение индикатора	Состояние устройства
Зеленый, горит постоянно	Телефонная трубка поднята (линия активна).
Не горит	Телефонная трубка положена, нормальная работа.
Зеленый, в течение секунды мигает с частотой 20 Гц, затем 4 секунды пауза	На телефонный порт поступает входящий вызов.
Зеленый, периодическое редкое мигание	Отсутствует регистрация абонентского порта на SIP-сервере.

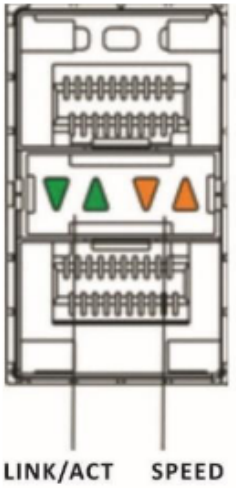


Рисунок 95 − Расположение индикаторов оптических интерфейсов

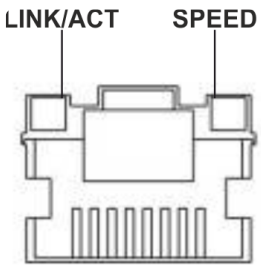


Рисунок 96 − Расположение индикаторов разъема RJ-45

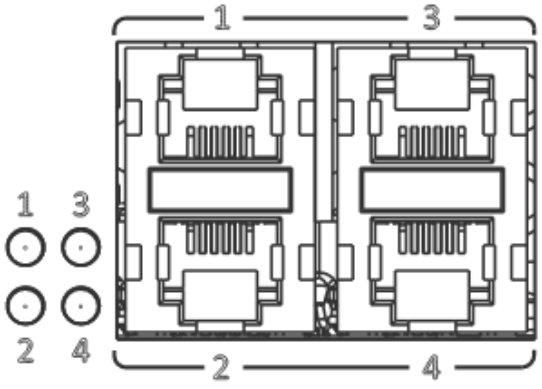


Рисунок 97 − Расположение индикаторов FXS-интерфейсов

В таблице 70 приведено описание состояний системных индикаторов устройства и их значений.

Таблица 70 – Состояния системных индикаторов

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Power	Индикатор питания устройства.	Зеленый	Питание устройства в норме. Источник питания работает нормально, основное ПО прогружено.
		Красный	Не прогружено основное ПО.
		Выключен	Отказ внутренних источников питания устройства.
Status	Индикатор текущего состояния устройства.	Зеленый	Устройство работает нормально.
		Красный	Устройство находится в состоянии загрузки ПО.
Alarm	Индикатор наличия и уровня аварии устройства.	-	-
User	Индикатор, использующийся для пользовательских сценариев, которые можно назначить в режиме конфигурирования устройства (не используется в текущей версии).	-	-

Световая индикация ESR-15R

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

Таблица 71 – Световая индикация состояния интерфейсов Ethernet

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

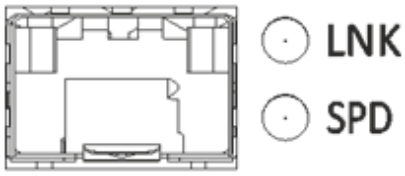


Рисунок 98 – Расположение индикаторов разъема SFP

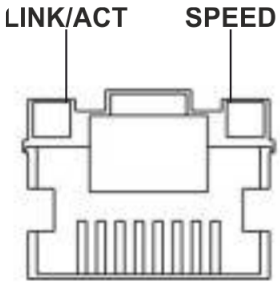


Рисунок 99 – Расположение индикаторов разъема RJ-45

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

Таблица 72 – Состояния системных индикаторов

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Power	Индикатор питания устройства.	Зеленый	Питание устройства в норме. Источник питания работает нормально, основное ПО прогружено.
		Красный	Не прогружено основное ПО.

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
		Выключен	Отказ внутренних источников питания устройства.
Status	Индикатор текущего состояния устройства.	Зеленый	Устройство работает нормально.
		Красный	Устройство находится в состоянии загрузки ПО.
Alarm	Индикатор наличия и уровня аварии устройства.	-	-
User	Индикатор, использующийся для пользовательских сценариев, которые можно назначить в режиме конфигурирования устройства.	-	-

Световая индикация ESR-15

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

Таблица 73 – Световая индикация состояния интерфейсов Ethernet

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

В таблице 74 приведено описание состояний системных индикаторов устройства и их значений.

Таблица 74 – Состояния системных индикаторов

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Power	Индикатор питания устройства.	Зеленый	Питание устройства в норме. Источник питания работает нормально, основное ПО прогружено.
		Красный	Не прогружено основное ПО.
		Выключен	Отказ внутренних источников питания устройства.

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
USB1, USB2	Индикаторы работы внешних USB-устройств.	Зеленый	Подключено USB-устройство.
		Мигает зеленым	Выполнение операций чтения/записи.
		Выключен	Нет подключенных устройств или проблемы с подключением.

Световая индикация ESR-12V(F)

Состояние интерфейсов Ethernet отображается двумя светодиодными индикаторами – LINK/ACT зеленого цвета и SPEED янтарного цвета. Состояние интерфейсов FXS и FXO отображается одним светодиодным индикатором зелёного цвета.

Таблица 75 – Световая индикация состояния интерфейсов Ethernet

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

Таблица 76 – Световая индикация FXS/FXO-интерфейсов

Название индикатора	Состояние индикатора	Состояние устройства
[1–3] FXS	Зеленый, горит постоянно	Телефонная трубка поднята (линия активна).
	Не горит	Телефонная трубка положена, нормальная работа.
	Зеленый, в течение секунды мигает с частотой 20 Гц, затем 4 секунды пауза	На телефонный порт поступает входящий вызов.
	Зеленый, периодическое редкое мигание	Отсутствует регистрация абонентского порта на SIP-сервере.
FXO	Не горит	Канал не занят (шлейф разомкнут).
	Зеленый, горит постоянно	Канал занят (шлейф замкнут).

Название индикатора	Состояние индикатора	Состояние устройства
	Зеленый, в течение секунды мигает с частотой 20 Гц, затем 4 секунды пауза	Поступает вызов со встречной АТС.

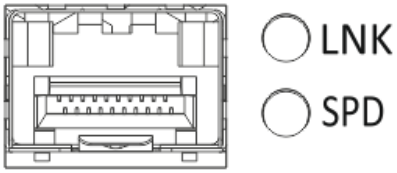


Рисунок 100 – Расположение индикаторов разъема SFP

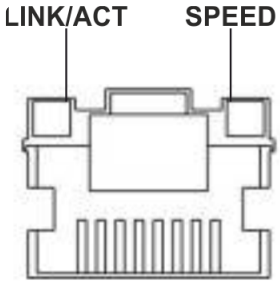


Рисунок 101 – Расположение индикаторов разъема RJ-45

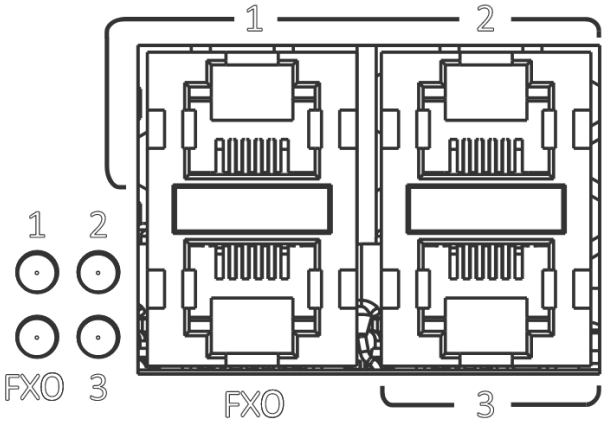


Рисунок 102 – Расположение индикаторов FXS/FXO-интерфейсов

В таблице 77 приведено описание состояний системных индикаторов устройства и их значений.

Таблица 77 – Состояния системных индикаторов

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Power	Индикатор питания устройства.	Зеленый	Питание устройства в норме. Источник питания работает нормально, основное ПО прогружено.
		Красный	Не прогружено основное ПО.
		Выключен	Отказ внутренних источников питания устройства.

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Status	Индикатор текущего состояния устройства.	Зеленый	Устройство работает нормально.
		Красный	Устройство находится в состоянии загрузки ПО.
Alarm	Индикатор наличия и уровня аварии устройства.	-	-

Световая индикация ESR-10

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

Таблица 78 – Световая индикация состояния интерфейсов Ethernet

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

В таблице 79 приведено описание состояний системных индикаторов устройства и их значений.

Таблица 79 – Состояния системных индикаторов

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Power	Индикатор питания устройства.	Зеленый	Питание устройства в норме. Источник питания работает нормально, основное ПО прогружено.
		Красный	Не прогружено основное ПО.
		Янтарный	Устройство находится в состоянии загрузки ПО.
		Выключен	Отказ внутренних источников питания устройства.
USB1, USB2	Индикаторы работы внешних USB-устройств.	Зеленый	Подключено USB-устройство.
		Мигает зеленым	Выполнение операций чтения/записи.
		Выключен	Нет подключенных устройств или проблемы с подключением.

2.5 Комплект поставки

В базовый комплект поставки ESR-10 входят:

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

В базовый комплект поставки ESR-12V входят:

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

В базовый комплект поставки ESR-12VF входят:

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

В базовый комплект поставки ESR-15 входят:

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

В базовый комплект поставки ESR-15R входят:

- маршрутизатор ESR-15R;
- кабель питания;
- консольный кабель;
- комплект для крепления устройства в стойку 19”;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки ESR-15VF входят:

- маршрутизатор ESR-15VF;
- кабель питания;
- консольный кабель;
- комплект для крепления устройства в стойку 19”;
- сертификат соответствия;

- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки ESR-20 входят:

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

В базовый комплект поставки ESR-21 входят:

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

В базовый комплект поставки ESR-30 входят:

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

В базовый комплект поставки ESR-31 входят:

- маршрутизатор ESR-31;
- консольный кабель;
- комплект для крепления устройства в стойку 19”;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки ESR-100 входят:

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

В базовый комплект поставки ESR-200 входят:

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

В базовый комплект поставки ESR-1000 входят:

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

В базовый комплект поставки ESR-1200 входят:

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

В базовый комплект поставки ESR-1500 входят:

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

В базовый комплект поставки ESR-1511 входят:

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

В базовый комплект поставки ESR-1511 rev.B входят:

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

В базовый комплект поставки ESR-1700 входят:

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

В базовый комплект поставки ESR-3100 входят:

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

В базовый комплект поставки ESR-3150 входят:

- маршрутизатор ESR-3150;
- консольный кабель;
- комплект для крепления устройства в стойку 19”;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки ESR-3200L входят:

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

В базовый комплект поставки ESR-3250 входят:

- маршрутизатор ESR-3250;
- консольный кабель;
- комплект для крепления устройства в стойку 19”;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки ESR-3300 входят:

- маршрутизатор ESR-3300;
- консольный кабель;
- комплект для крепления устройства в стойку 19”;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки ESR-3350 входят:

- маршрутизатор ESR-3350;
- консольный кабель;
- комплект для крепления устройства в стойку 19”;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

⚠ По заказу покупателя для ESR-31 в комплект поставки может быть включен модуль питания (PM160-220/12 или PM100-48/12 rev.B).
По заказу покупателя для ESR-1000, ESR-1200 в комплект поставки может быть включен модуль питания (PM160-220/12 или PM100-48/12).
По заказу покупателя для ESR-1500, ESR-1511, ESR-1511 rev.B, ESR-3100, ESR-3150, ESR-3200, ESR-3200L, ESR-3250 в комплект поставки может быть включен модуль питания (PM160-220/12 или PM160-48/12).
По заказу покупателя для ESR-1700 в комплект поставки может быть включен модуль питания (PM350-220/12 или PM350-48/12).
По заказу покупателя для ESR-3300 в комплект поставки может быть включен модуль питания (PM600-220/12 или PM600-48/12).
По заказу покупателя для ESR-3350 в комплект поставки может быть включен модуль питания (PM350-220/12 PM350-48/12).

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

3 Установка и подключение

- Установка устройства в стойку (кроме ESR-3300, ESR-3350)
- Установка ESR-3300, ESR-3350 в стойку
- Подключение к vESR
- Установка модулей питания ESR-31, 1000, ESR-1200, ESR-1500, ESR-1511, ESR-1511 rev.B, ESR-1700, ESR-3100, ESR-3150, ESR-3200, ESR-3200L, ESR-3250, ESR-3300, ESR-3350
- Подключение питающей сети
- Установка и удаление SFP-трансиверов
    - Установка трансивера
    - Удаление трансивера

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

3.1 Установка устройства в стойку (кроме ESR-3300, ESR-3350)

Для установки устройства в стойку:

1. Выберите необходимое положение кронштейна (рисунок 103). Совместите четыре отверстия кронштейна с четырьмя отверстиями на боковой панели устройства. С помощью отвертки прикрепите кронштейн винтами к корпусу.
2. Повторите шаг 1 для другой боковой панели устройства.
3. Совместите отверстия кронштейнов с отверстиями на передних вертикальных направляющих стойки. Используйте отверстия в направляющих на одном уровне с обеих сторон стойки, для того чтобы устройство располагалось горизонтально.
4. С помощью отвертки прикрепите маршрутизатор к стойке винтами.

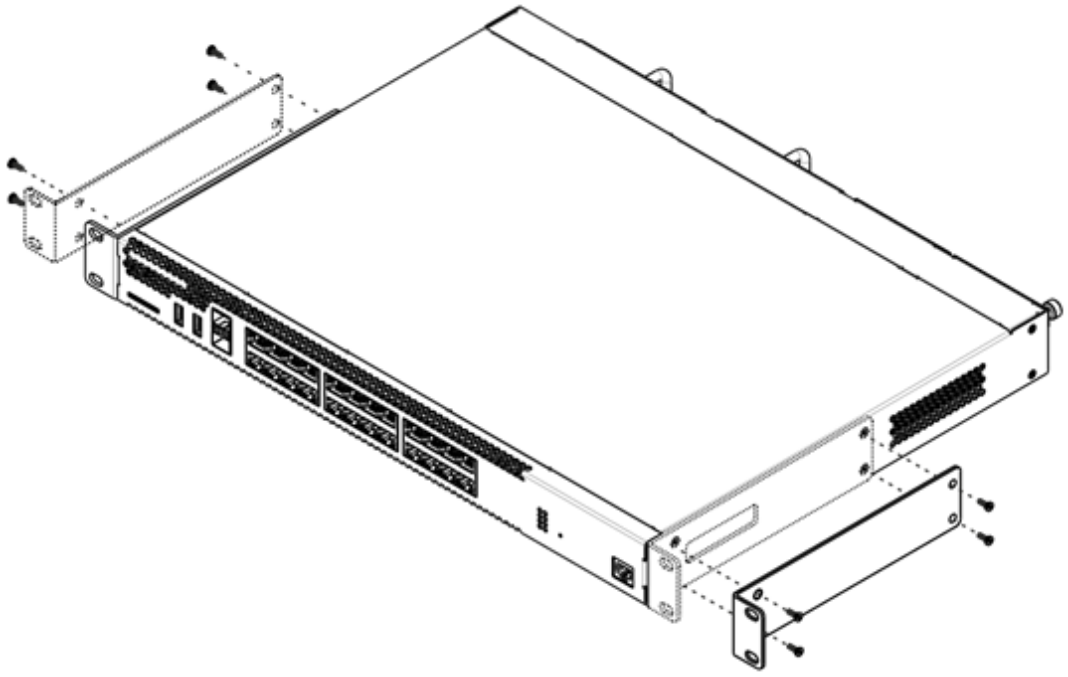


Рисунок 103 – Крепление кронштейнов к устройству

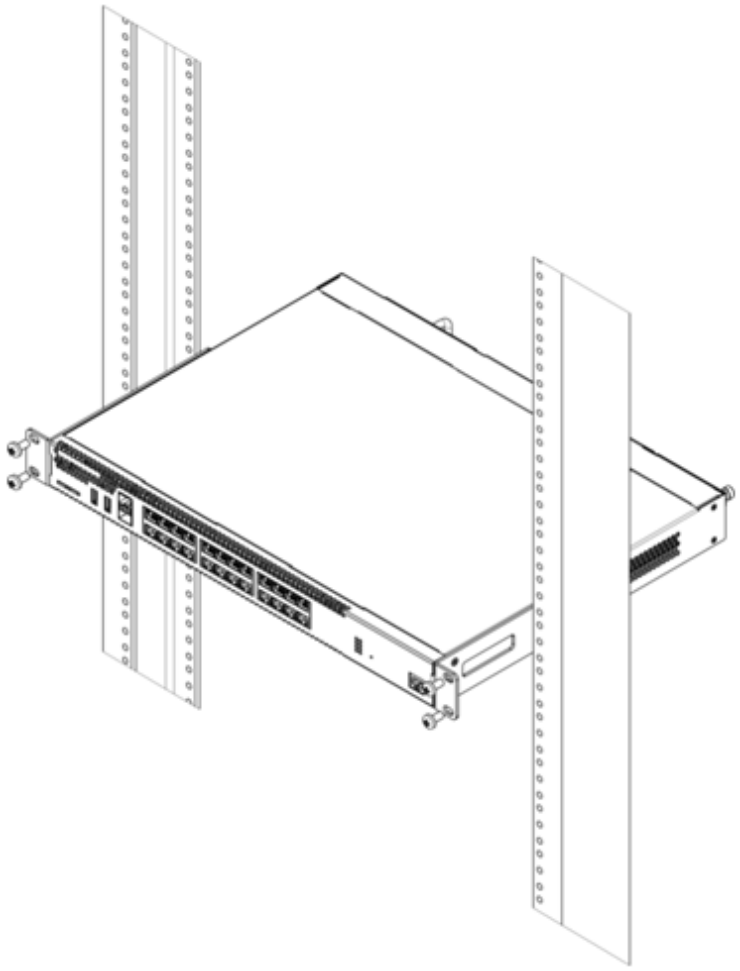


Рисунок 104 – Установка устройства в стойку

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

3.2 Установка ESR-3300, ESR-3350 в стойку

Для деталей длинного кронштейна предусмотрено несколько положений: в каждом случае необходимое положение определяется глубиной используемой стойки. Минимальная глубина, на которую рассчитан кронштейн — 537.5 мм, максимальная — 787.5 мм.

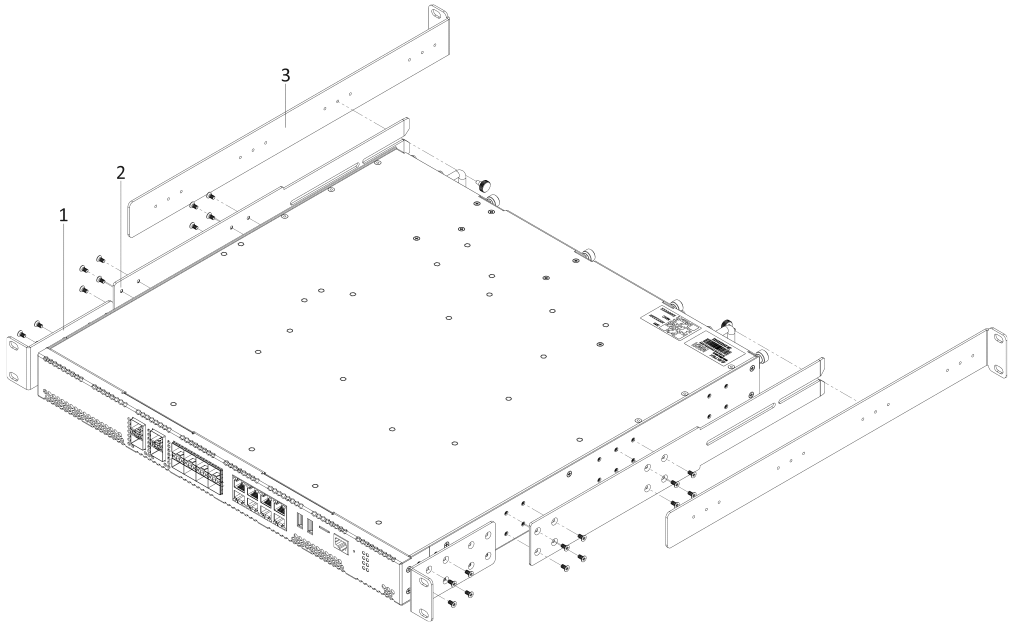


Рисунок 105 – Крепление кронштейнов к ESR-3300, ESR-3350

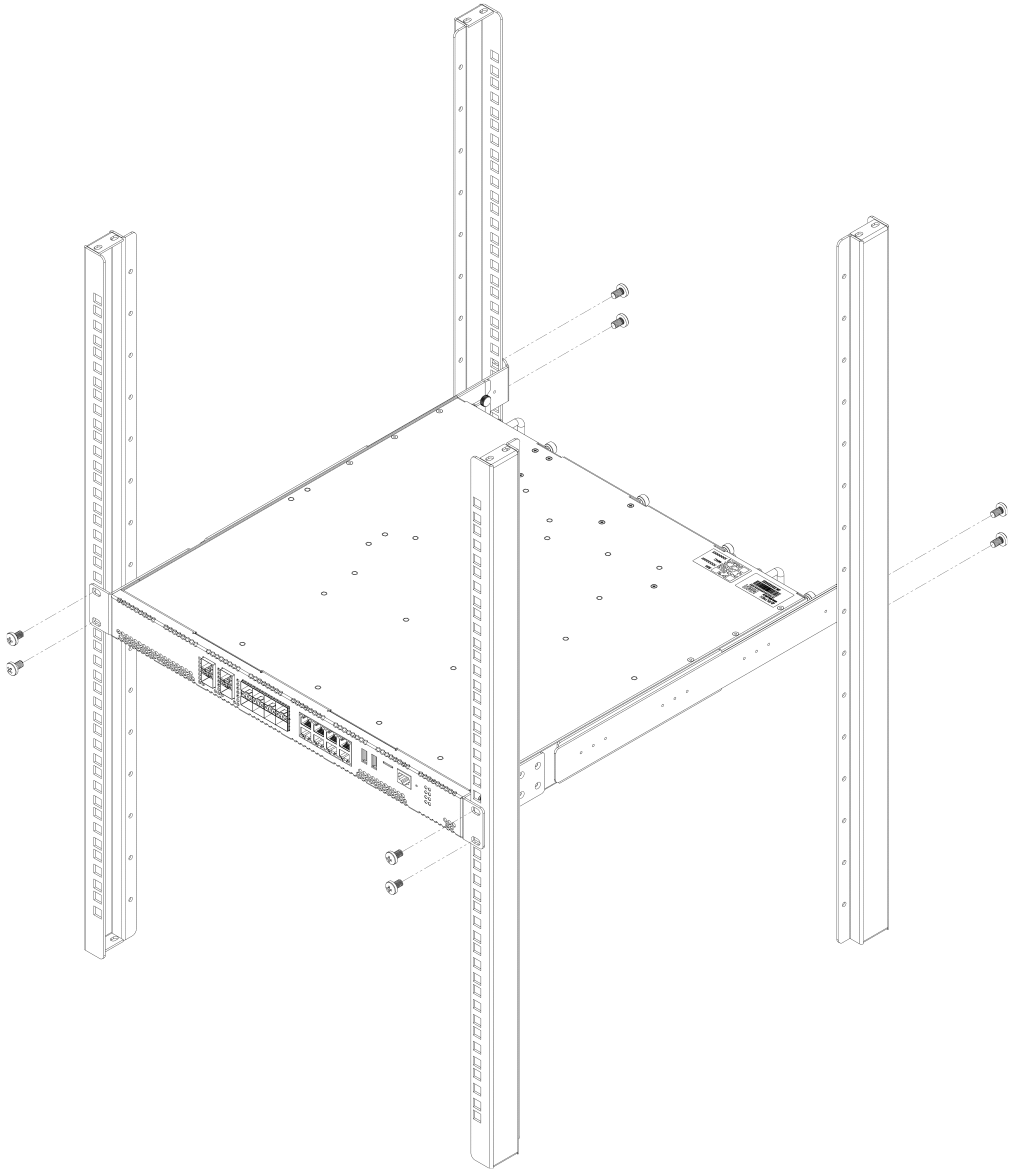


Рисунок 106 – Установка ESR-3300, ESR-3350 в стойку

Для установки устройства в стойку:

1. Выберите необходимое положение детали 1. Совместите четыре отверстия на детали 1 с четырьмя отверстиями на боковой панели устройства. С помощью отвертки прикрепите деталь 1 винтами к корпусу.
2. (Если необходимо) С помощью отвертки извлеките направляющий винт, соединяющий детали 2 и 3, и разъедините их.
3. Выберите необходимое положение детали 2. Совместите восемь отверстий на детали 2 с восемью отверстиями на боковой панели устройства. С помощью отвертки прикрепите деталь 2 винтами к корпусу.
4. Повторите шаги 1–3 для другой боковой панели устройства.
5. Совместите отверстия кронштейна на деталях 3 с отверстиями на задних вертикальных направляющих стойки и прикрепите детали к стойке винтами (рисунок 106). В зависимости от глубины стойки вкрутите направляющие винты в детали 3.
6. Совместите отверстия на деталях 1 с отверстиями на передних вертикальных направляющих стойки (рисунок 106). Используйте отверстия в направляющих на одном уровне с обеих сторон стойки, для того чтобы устройство располагалось горизонтально.
7. Установите устройство в стойку, совместив прорезь детали 2 с направляющим винтом в детали 3.
8. С помощью отвертки прикрепите устройство к стойке винтами.

3.3 Подключение к vESR

Для получения информации о установке и подключении к vESR перейдите в раздел документации ESR-Series. Руководство по установке и настройке vESR. Версия 1.40.

3.4 Установка модулей питания ESR-31, 1000, ESR-1200, ESR-1500, ESR-1511, ESR-1511 rev.B, ESR-1700, ESR-3100, ESR-3150, ESR-3200, ESR-3200L, ESR-3250, ESR-3300, ESR-3350

Маршрутизаторы ESR-31/1000/1200/1500/1511(rev.B)/1700/3100/3150/3200/3200L/3250/3300/3350 могут работать с одним или двумя модулями питания. Установка второго модуля питания необходима в случае использования устройства в условиях, требующих повышенной надежности.

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

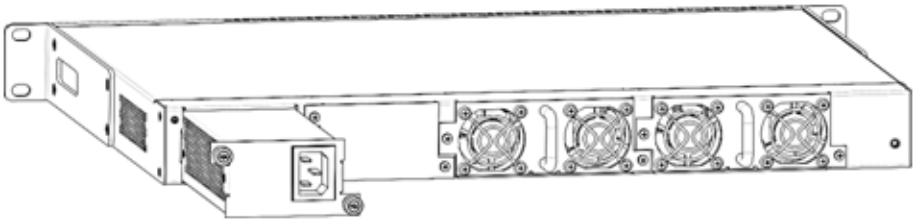


Рисунок 107 – Установка модулей питания

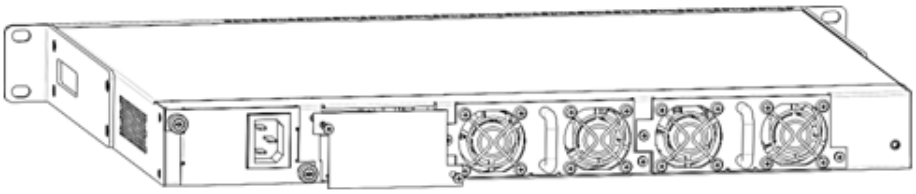


Рисунок 108 – Установка заглушки

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

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

3.5 Подключение питающей сети

1. Прежде чем к устройству будет подключена питающая сеть, необходимо заземлить корпус устройства через заземляющий винт M4. Заземление необходимо выполнять изолированным многожильным проводом. Устройство заземления и сечение заземляющего провода должны соответствовать требованиями Правил устройства электроустановок (ПУЭ).
2. Если предполагается подключение компьютера или иного оборудования к консольному порту маршрутизатора, это оборудование также должно быть надежно заземлено.
3. Подключите к устройству кабель питания. В зависимости от комплектации устройства, питание может осуществляться от сети переменного тока либо от сети постоянного тока. При подключении сети переменного тока следует использовать кабель, входящий в комплект устройства. Для подключения к сети постоянного тока используйте провод сечением не менее 1 мм^2.
4. Включите питание устройства и убедитесь в отсутствии аварий по состоянию индикаторов на передней панели.

3.6 Установка и удаление SFP-трансиверов

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

3.6.1 Установка трансивера

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

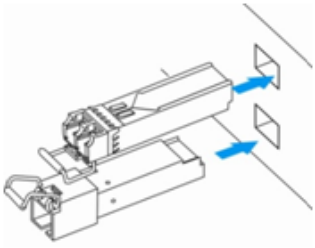


Рисунок 109 – Установка SFP-трансиверов

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

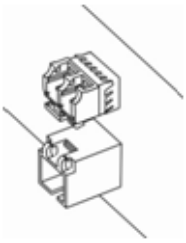


Рисунок 110 – Установленные SFP-трансиверы

3.6.2 Удаление трансивера

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

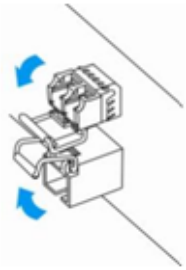


Рисунок 111 – Открытие защелки SFP-трансиверов

2. Извлеките модуль из слота.

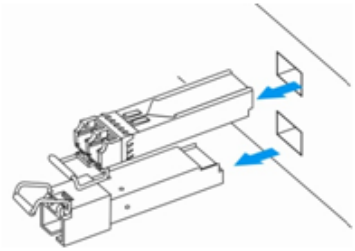


Рисунок 112 – Извлечение SFP-трансиверов

4 Интерфейсы управления

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

Настройка и мониторинг устройства могут осуществляться через различные интерфейсы управления.

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

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

- для ESR-10: GigabitEthernet 1/0/2-6;
- для ESR-12V(F): GigabitEthernet 1/0/2-8;
- для ESR-15(R): GigabitEthernet 1/0/2-5;
- для ESR-15VF: GigabitEthernet 1/0/2-9;
- для ESR-20: GigabitEthernet 1/0/2-4;
- для ESR-21: GigabitEthernet 1/0/2-12;
- для ESR-30: GigabitEthernet 1/0/2-4;
- для ESR-31: GigabitEthernet 1/0/2-14;
- для ESR-100: GigabitEthernet 1/0/2-4;
- для ESR-200: GigabitEthernet 1/0/2-8;
- для ESR-1000: GigabitEthernet 1/0/2-24;
- для ESR-1200: GigabitEthernet 1/0/2-16, TengigabitEthernet 1/0/3-8;
- для ESR-1500: GigabitEthernet 1/0/2-8, TengigabitEthernet 1/0/2-4;
- для ESR-1511: GigabitEthernet 1/0/2-8, TengigabitEthernet 1/0/1-4;
- для ESR-1700: GigabitEthernet 1/0/2-4, TengigabitEthernet 1/0/3-12;
- для ESR-3100: GigabitEthernet 1/0/2-8, TengigabitEthernet 1/0/3-8;
- для ESR-3150: GigabitEthernet 1/0/2-8, Tenegigabitethernet 1/0/3-4;
- для ESR-3200: Twentyfivegigabitethernet 1/0/3-12;
- для ESR-3200L: TengigabitEthernet 1/0/3-8, TwentyfivegigabitEthernet 1/0/3-4;
- для ESR-3250, ESR-3350: GigabitEthernet 1/0/2-8, Twentyfivegigabitethernet 1/0/3-4
- для ESR-3300: TwentyfivegigabitEthernet 1/0/3-4, HundredgigabitEthernet 1/0/3-4.

В заводской конфигурации по умолчанию создан пользователь «admin» с паролем «password». Протоколы семейства STP (STP, RSTP, VSTP) отключены.

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

4.1 Интерфейс командной строки (CLI)

Интерфейс командной строки (Command Line Interface, CLI) – интерфейс, предназначенный для управления, просмотра состояния и мониторинга устройства. Для работы потребуется любая установленная на ПК программа, поддерживающая работу по протоколам Telnet, SSH или прямое подключение через консольный порт (например, HyperTerminal).

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

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

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

Система позволяет нескольким пользователям одновременно подключаться к устройству.

4.2 Типы и порядок именования интерфейсов маршрутизатора

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

Таблица 80 – Типы и порядок именования интерфейсов маршрутизатора

Тип интерфейса	Обозначение
Физические интерфейсы	Обозначение физического интерфейса включает в себя его тип и идентификатор. Идентификатор физических интерфейсов имеет вид **<UNIT>/<SLOT>/<PORT>**, где: • **<UNIT>** – номер устройства в группе устройств [1..4], • **<SLOT>** – номер модуля в составе устройства или 0 при отсутствии деления устройства на модули, • **<PORT>** – порядковый номер порта.
Порты 1 Гбит/с	**gigabitethernet <UNIT>/<SLOT>/<PORT>** Пример обозначения: **gigabitethernet 1/0/12** ⚠ Допускается использовать сокращенное наименование, например gi1/0/12.
Порты 10 Гбит/с	**tengigabitethernet <UNIT>/<SLOT>/<PORT>** Пример обозначения: **tengigabitethernet 1/0/2** ⚠ Допускается использовать сокращенное наименование, например te1/0/2.
Порты 25 Гбит/с	**twentyfivegigabitethernet <UNIT>/<SLOT>/<PORT>** Пример обозначения: **twentyfivegigabitethernet 1/0/2** ⚠ Допускается использовать сокращенное наименование, например twe1/0/2.

Тип интерфейса	Обозначение
Порты 40 Гбит/с	**fortygigabitethernet <UNIT>/<SLOT>/<PORT>** Пример обозначения: **fortygigabitethernet 1/0/2** ⚠ Допускается использовать сокращенное наименование, например fo1/0/2.
Порты 100 Гбит/с	**hundredgigabitethernet <UNIT>/<SLOT>/<PORT>** Пример обозначения: **hundredgigabitethernet 1/0/2** ⚠ Допускается использовать сокращенное наименование, например hu1/0/2.
Группы агрегации каналов	Обозначение группы агрегации каналов включает в себя его тип и идентификатор. Идентификатор port-channel-интерфейсов может иметь вид **{ <CHANNEL_ID> | <UNIT>/<CHANNEL_ID> }**, где • **<UNIT>** – номер устройства в группе устройств [1..4], • **<CHANNEL_ID>** – порядковый номер группы агрегации каналов [1..12] Примеры обозначений: **port-channel 6** **port-channel 1/6** ⚠ Допускается использовать сокращенное наименование, например, po1.
Саб-интерфейсы	Обозначение саб-интерфейса образуется из обозначения базового интерфейса и идентификатора (VLAN) саб-интерфейса, разделенных точкой. Примеры обозначений: • **gigabitethernet 1/0/12.100** • **tengigabitethernet 1/0/2.123** • **twentyfivegigabitethernet 1/0/2.200** • **fortygigabitethernet 1/0/2.1024** • **port-channel 1.6** • **port-channel 1/6.6** ⚠ Идентификатор саб-интерфейса может принимать значения [2..4094].

Тип интерфейса	Обозначение
Q-in-Q интерфейсы	Обозначение Q-in-Q интерфейса образуется из обозначения базового интерфейса, идентификатора сервисного VLAN и идентификатора пользовательского VLAN, разделенных точкой. Примеры обозначений: • **gigabitethernet 1/0/12.100.10** • **tengigabitethernet 1/0/2.45.12** • **twentyfivegigabitethernet 1/0/2.100.200** • **fortygigabitethernet 1/0/2.408.507** • **port-channel 1.6.34** • **port-channel 1/6.6.34** ⚠ Идентификатор сервисного и пользовательского VLAN может принимать значения [1..4094].
E1-интерфейсы	Обозначение E1-интерфейса включает в себя его тип и идентификатор. Идентификатор E1-интерфейсов имеет вид **<UNIT>/<SLOT>/<STREAM>**, где • **<UNIT>** – номер устройства в группе устройств [1..4], • **<SLOT>** – номер E1-модуля в составе устройства, • **<STREAM>** – порядковый номер E1-потока. Пример обозначения: **e1 1/0/1**
Группы агрегации E1-каналов	Обозначение группы агрегации E1-каналов включает в себя его тип и порядковый номер интерфейса: **multilink <CHANNEL_ID>** Пример обозначения: **multilink <CHANNEL_ID>**
Логические интерфейсы	Обозначение логического интерфейса является порядковым номером интерфейса: Примеры обозначений: • **loopback 4** • **bridge 60** • **service-port 1**
Последовательные интерфейсы	Обозначение последовательного интерфейса включает в себя его тип и идентификатор. Идентификатор последовательного интерфейса имеет вид **<UNIT>/<SLOT>/<STREAM>**, где • **<UNIT>** – номер устройства в группе устройств [1..4], • **<SLOT>** – номер модуля в составе устройства или 0 при отсутствии деления устройства на модули, • **<PORT>** – порядковый номер порта. Пример обозначения: **serial 1/0/1**

Тип интерфейса	Обозначение
USB-модемы	Обозначение USB-модема включает в себя его тип и порядковый номер: **cellular modem <MODEM-NUM>** Пример обозначения: **cellular modem 1**
FXS/FXO-порты	Обозначение FXS/FXO-портов включает в себя его тип и порядковый номер: **interface voice-port <NUM>** Пример обозначения: **voice-port 1**

1. Количество интерфейсов каждого типа зависит от модели маршрутизатора.
2. Текущая версия ПО поддерживает кластеризацию устройств единой модели. Номер unit в группе устройств может принимать значение в диапазоне от 1 до 4.
3. Некоторые команды поддерживают одновременную работу с группой интерфейсов. Для указания группы интерфейсов может быть использовано перечисление через запятую или указание диапазона идентификаторов через дефис «-».
Примеры указания групп интерфейсов:

```
interface gigabitethernet 1/0/1, gigabitethernet 1/0/5
interface tengigabitethernet 1/0/1-2
interface twentyfivegigabitethernet 1/0/3-4
interface fortygigabitethernet 1/0/1-2
interface gi1/0/1-3,gi1/0/7,te1/0/1,fo1/0/1
```

4.3 Типы и порядок именования туннелей маршрутизатора

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

Таблица 81 – Типы и порядок именования туннелей маршрутизатора

Тип туннеля	Обозначение
L2TP-туннель	Обозначение L2TP-туннеля состоит из обозначения типа и порядкового номера туннеля: **l2tp <L2TP_ID>** Пример обозначения: **l2tp 1**
L2TPv3-туннель	Обозначение L2TPv3-туннеля состоит из обозначения типа и порядкового номера туннеля: **l2tpv3 <L2TPV3_ID>** Пример обозначения: **l2tpv3 1**
GRE-туннель	Обозначение GRE-туннеля состоит из обозначения типа и порядкового номера туннеля: **gre <GRE_ID>** Пример обозначения: **gre 1**
SoftGRE-туннель	Обозначение SoftGRE-туннеля состоит из обозначения типа, порядкового номера туннеля и, опционально, VLAN ID виртуального интерфейса: **softgre <GRE_ID>[.<VLAN>]** Примеры обозначения: **softgre 1, softgre 1.10**
IPv4-over-IPv4-туннель	Обозначение IPv4-over-IPv4-туннеля состоит из обозначения типа и порядкового номера туннеля: **ip4ip4 <IPIP_ID>** Пример обозначения: **ip4ip4 1**
IPsec-туннель	Обозначение виртуального IPsec-туннеля состоит из обозначения типа и порядкового номера туннеля: **vti <VTI_ID>** Пример обозначения: **vti 1**
Логический туннель (туннель между VRF)	Обозначение логического туннеля состоит из обозначения типа и порядкового номера туннеля: **lt <LT_ID>** Пример обозначения: **lt 1**

Тип туннеля	Обозначение
PPPoE-туннель	Обозначение PPPoE-туннеля состоит из обозначения типа и порядкового номера туннеля: **pppoe <PPPOE_ID>** Пример обозначения: **pppoe 1**
OpenVPN-туннель	Обозначение OpenVPN-туннеля состоит из обозначения типа и порядкового номера туннеля: **openvpn <OPENVPN_ID>** Пример обозначения: **openvpn 1**
PPTP-туннель	Обозначение PPTP-туннеля состоит из обозначения типа и порядкового номера туннеля: **pptp <PPTP_ID>** Пример обозначения: **pptp 1**
Wireguard-туннель	Обозначение Wireguard-туннеля состоит из обозначения типа и порядкового номера туннеля: **wireguard <WG_ID>** Пример обозначения: **wireguard 1**

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

5 Начальная настройка маршрутизатора

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

5.1 Заводская конфигурация маршрутизатора ESR

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

5.1.1 Описание заводской конфигурации

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

1. **Зона «Untrusted»** предназначена для подключения к публичной сети (WAN). В этой зоне открыты порты DHCP-протокола для получения динамического IP-адреса от провайдера. Все входящие соединения из данной зоны на маршрутизатор запрещены.
   В данную зону безопасности входят интерфейсы:
   - для ESR-10/12V: GigabitEthernet 1/0/1;
   - для ESR-12VF: GigabitEthernet 1/0/1; GigabitEthernet 1/0/9;
   - для ESR-15(R): GigabitEthernet1/0/1; GigabitEthernet1/0/6;
   - для ESR-15VF: GigabitEthernet 1/0/1; GigabitEthernet 1/0/10;
   - для ESR-20: GigabitEthernet 1/0/1;
   - для ESR-21: GigabitEthernet 1/0/1;
   - для ESR-30/31: GigabitEthernet 1/0/1; TengigabitEthernet 1/0/1-2;
   - для ESR-100/200: GigabitEthernet 1/0/1;
   - для ESR-1000/1500/3100: GigabitEthernet 1/0/1, TengigabitEthernet 1/0/1-2;
   - для ESR-1200/1700: GigabitEthernet 1/0/1, TengigabitEthernet 1/0/1, TengigabitEthernet 1/0/2;
   - для ESR-1511: GigabitEthernet 1/0/1, FortygigabitEthernet 1/0/1-2;
   - для ESR-3150: GigabitEthernet 1/0/1, TengigabitEthernet 1/0/1-2;
   - для ESR-3200: Twentyfivegigabitethernet 1/0/1-2;
   - для ESR-3200L: TengigabitEthernet 1/0/1-2, TwentyfivegigabitEthernet 1/0/1-2;
   - для ESR-3250/3350: GigabitEthernet 1/0/1, TwentyfivegigabitEthernet 1/0/1-2;
   - для ESR-3300: TwentyfivegigabitEthernet 1/0/1-2, HundredgigabitEthernet 1/0/1-2.

   Интерфейсы зоны объединены в один L2-сегмент через сетевой мост Bridge 2.

2. **Зона «Trusted»** предназначена для подключения к локальной сети (LAN). В этой зоне открыты порты протоколов SSH для удаленного доступа, ICMP-протокола для проверки доступности маршрутизатора, DHCP-протокола для получения клиентами IP-адресов от маршрутизатора. Исходящие соединения из данной зоны в зону «Untrusted» разрешены.
   В данную зону безопасности входят интерфейсы:
   - для ESR-10: GigabitEthernet 1/0/2-6;
   - для ESR-12V(F): GigabitEthernet 1/0/2-8;
   - для ESR-15(R): GigabitEthernet 1/0/2-5;
   - для ESR-15VF: GigabitEthernet 1/0/2-9;
   - для ESR-20: GigabitEthernet 1/0/2-4;
   - для ESR-21: GigabitEthernet 1/0/2-12;
   - для ESR-30: GigabitEthernet 1/0/2-4;
   - для ESR-31: GigabitEthernet 1/0/2-14;
   - для ESR-100: GigabitEthernet 1/0/2-4;
   - для ESR-200: GigabitEthernet 1/0/2-8;
   - для ESR-1000: GigabitEthernet 1/0/2-24;
   - для ESR-1200: GigabitEthernet 1/0/2-16, TengigabitEthernet 1/0/3-8;
   - для ESR-1500: GigabitEthernet 1/0/2-8, TengigabitEthernet 1/0/3-4;
   - для ESR-1511: GigabitEthernet 1/0/2-8, TengigabitEthernet 1/0/1-4;
   - для ESR-1700: GigabitEthernet 1/0/2-4, TengigabitEthernet 1/0/3-12;
   - для ESR-3100: GigabitEthernet 1/0/2-8, TengigabitEthernet 1/0/3-8;
   - для ESR-3150: GigabitEthernet 1/0/2-8, Tenegigabitethernet 1/0/3-4;
   - для ESR-3200: Twentyfivegigabitethernet 1/0/3-12;
   - для ESR-3200L: TengigabitEthernet 1/0/3-8, TwentyfivegigabitEthernet 1/0/3-4;
   - для ESR-3250/3350: GigabitEthernet 1/0/2-8, Twentyfivegigabitethernet 1/0/3-4;
   - для ESR-3300: TwentyfivegigabitEthernet 1/0/3-4, HundredgigabitEthernet 1/0/3-4.

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

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

Политики зон безопасности настроены следующим образом:

Таблица 82 – Описание политик зон безопасности

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

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

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

5.2 Подключение и конфигурирование маршрутизатора

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

Базовая настройка маршрутизатора должна включать:

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

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

5.2.1 Подключение к маршрутизатору

Предусмотрены следующие способы подключения к устройству:

Подключение по локальной сети Ethernet

При первоначальном старте маршрутизатор загружается с заводской конфигурацией. Описание заводской конфигурации приведено в разделе Заводская конфигурация маршрутизатора ESR данного руководства.

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

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

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

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

Подключение через консольный порт RS-232

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

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

Выполните следующие настройки интерфейса RS-232:

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

5.2.2 Применение изменения конфигурации

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

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

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

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

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

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

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

5.2.3 Базовая настройка маршрутизатора

Процедура настройки маршрутизатора при первом включении состоит из следующих этапов:

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

Изменение пароля пользователя «admin» при первой авторизации

При первом входе в систему необходимо сменить пароль по умолчанию привилегированного пользователя «admin». До смены пароля пользовательская настройка устройства недоступна.

После указания нового пароля необходимо применить изменения в конфигурации командой **commit** и подтвердить изменения командой **confirm**:

```
esr(change-expired-password)# password <new password>
esr(change-expired-password)# commit
Configuration has been successfully applied and saved to flash. Commit timer started, changes
will be reverted in 600 seconds.
esr(change-expired-password)# confirm
Configuration has been confirmed. Commit timer canceled.
esr#
```

Создание новых пользователей

Для управления устройством на сервисных маршрутизаторах ESR существует возможность создавать пользовательские учетные записи, у которых администратор может индивидуально задать:

- пароль;
- уровень привилегий;
- режим работы учетной записи.

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

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

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

⚠ У учетных записей есть несколько режимов работы:

- cli – режим работы по умолчанию, пользователь получает доступ к интерфейсу командной строки, предназначенному для управления, просмотра состояния и мониторинга устройства;
- techsupport – пользователь получает доступ к командной оболочке, в которой выполняется процедура отладки устройства совместно с специалистами технической поддержки;
- sftp – пользователь используется для организации доступа к встроенному SFTP-серверу, возможность работы в какой-либо командой оболочке при этом у пользователя отсутствует.

Пользователь «admin» является единственным предустановленным пользователем в конфигурации устройства. Это приводит к определенным особенностям работы с ним:
1) Применение команды **no username admin** не удаляет пользователя «admin» из конфигурации, а приводит его к настройкам по умолчанию – паролю «password» и 15 уровню привилегий.
2) Отключить возможность авторизации пользователя «admin» можно командой **no admin login enable**.
3) Пользователь «admin» с настройками по умолчанию (пароль «password», уровень привилегий 15) не отображается в выводах команд **show running-config** и **show candidate-config** без модификатора «full».

Пример команд для создания нескольких учетных записей – пользователя «**netmaster**» с уровнем привилегий **15** для управления оборудованием, пользователя «**watcher**» с уровнем привилегий **1** для ограниченного просмотра оперативной информации, а также пользователя «**techsup**» для отладки устройства совместно с сотрудниками технической поддержки:

```
esr# configure
esr(config)# username netmaster
esr(config-user)# password P@ssW0rd
esr(config-user)# privilege 15
esr(config-user)# exit
esr(config)# username watcher
esr(config-user)# password password
esr(config-user)# privilege 1
esr(config-user)# exit
esr(config)# username techsup
esr(config-user)# password PsWdTs
esr(config-user)# mode techsupport
esr(config-user)# exit
esr(config)#
```

Назначение имени устройства

Для назначения имени устройства используются следующие команды:

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

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

Настройка параметров публичной сети

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

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

Параметры интерфейса:

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

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

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

```
esr# show ip interfaces
IP address                                          Interface             Admin   Link
Type      Precedence
----------------------------------------------------   -------------------   -----   -----
-------   -----------
192.168.16.144/24                                   gi1/0/2.150           Up      Up
static    primary
```

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

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

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

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

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

Настройка удаленного доступа к маршрутизатору

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

При конфигурировании доступа к маршрутизатору правила создаются для пары зон:

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

Для создания разрешающего правила используются следующие команды:

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

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

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

6 Рекомендации по безопасной настройке

- Общие рекомендации
- Настройка системы логирования событий
  - Рекомендации
  - Предупреждения
  - Пример настройки
- Настройка политики использования паролей
  - Рекомендации
  - Пример настройки
- Настройка политики AAA
  - Рекомендации
  - Предупреждения
  - Пример настройки
- Настройка удалённого управления
  - Рекомендации
  - Пример настройки
- Настройка механизмов защиты от сетевых атак
  - Рекомендации
  - Пример настройки

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

6.1 Общие рекомендации

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

6.2 Настройка системы логирования событий

Алгоритмы настройки системы логирования событий приведены в подразделе «Настройка Syslog» раздела Мониторинг настоящего руководства.

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

6.2.1 Рекомендации

- Рекомендуется настроить хранение сообщений о событиях в файл syslog на устройстве и передачу этих событий на внешний syslog-сервер.
- Рекомендуется ограничивать размер syslog-файла на устройстве.
- Рекомендуется настраивать ротацию syslog-файлов на устройстве.
- Рекомендуется включать нумерацию сообщений syslog.
- Рекомендуется включать добавление меток timestamp msec к syslog-сообщениям на устройствах ESR-1500 и ESR-1511.

6.2.2 Предупреждения

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

6.2.3 Пример настройки

Задача:

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

Решение:

Настраиваем хранение syslog-сообщений в файле:

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

Настраиваем ограничение размера и ротацию файлов:

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

Настраиваем передачу сообщений на внешний сервер:

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

Включаем нумерацию сообщений syslog:

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

6.3 Настройка политики использования паролей

Алгоритмы настройки политики использования паролей приведены в разделе Настройка AAA настоящего руководства.

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

6.3.1 Рекомендации

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

6.3.2 Пример настройки

Задача:

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

Решение:

Включаем запрос на смену пароля по умолчанию для пользователя admin:

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

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

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

Устанавливаем ограничения на длину пароля:

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

Устанавливаем ограничения по минимальному количеству символов соответствующих типов:

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

6.4 Настройка политики AAA

Алгоритмы настройки политики AAA приведены в разделе Настройка AAA настоящего руководства.

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

6.4.1 Рекомендации

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

6.4.2 Предупреждения

- Встроенную учётную запись **admin** удалить нельзя, только отключить авторизацию для неё командой **no admin login enable**.
- Команда **no username admin** не удаляет пользователя **admin**, сбрасывает его конфигурацию в значения по умолчанию. После применения этой команды пользователь **admin** не будет отображаться в конфигурации.
- Команда **no password** для пользователя **admin** также не удаляет пароль пользователя **admin**, а сбрасывает его в значение по умолчанию. После применения этой команды пароль пользователя **admin** перестаёт отображаться в конфигурации и становится ‘password'.
- Перед отключением авторизации для пользователя **admin** в конфигурацию устройства необходимо настроить пользователя с уровнем привилегий 15 или задать ENABLE-пароль для уровня привилегий 15.

6.4.3 Пример настройки

Задача:

Настроить политику AAA:

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

Решение:

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

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

Задаём локальный ENABLE-пароль:

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

Далее необходимо отключить авторизацию у пользователя admin:

```
esr(config)# no admin login enable
```

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

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

Настраиваем политику AAA:

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

Настраиваем логирование:

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

6.5 Настройка удалённого управления

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

6.5.1 Рекомендации

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

6.5.2 Пример настройки

Задача:

Сгенерировать новые ключи шифрования. Использовать криптостойкие алгоритмы.

Решение:

Отключаем устаревшие и не криптостойкие алгоритмы:

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

Генерируем новые ключи шифрования:

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

6.6 Настройка механизмов защиты от сетевых атак

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

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

6.6.1 Рекомендации

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

- Рекомендуется включать логирование механизма защиты от сетевых атак.

6.6.2 Пример настройки

Задача:

Настроить механизм защиты от сетевых атак в соответствии с рекомендациями.

Решение:

Включаем защиту от ip spoofing и логирование механизма защиты:

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

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

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

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

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

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

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

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

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

7 Управление интерфейсами

- Настройка физического интерфейса
  - Алгоритм настройки
  - Алгоритм настройки режима L3
  - Пример настройки в режиме L3
- Настройка терминации на саб-интерфейсе
  - Алгоритм настройки
  - Пример настройки саб-интерфейса
- Настройка терминации на Q-in-Q интерфейсе
  - Алгоритм настройки
  - Пример настройки Q-in-Q интерфейса
- Настройка USB-модемов
  - Алгоритм настройки USB-модемов
  - Пример настройки
- Настройка PPP через E1
  - Алгоритм настройки
  - Пример конфигурации
- Настройка MLPPP
  - Алгоритм настройки
  - Пример настройки
  - Фрагментация трафика
- Настройка AUX
  - Алгоритм настройки
  - Примеры настроек
  - Схемы распайки переходников

7.1 Настройка физического интерфейса

7.1.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
	Переход в режим конфигурирования функционала.	**esr(config)# interface gigabitethernet** **esr(config)# interface tengigabitethernet** **esr(config)# interface fourtygigabitethernet** **esr(config)# interface twentyfivegigabitethernet** **esr(config)# interface hundredgigabitethernet** **esr(config)# interface port-channel { <ID> | <UNIT>/<ID> }**	<UNIT> – номер устройства в группе устройств [1..4]. <ID> – порядковый номер группы агрегации каналов, принимает значения [1..12].
2	Включить/отключить интерфейс.	**esr(config-if-gi)# shutdown/ no shutdown**	

Шаг	Описание	Команда	Ключи
3	Задать описание (необязательно).	**esr(config-if-gi)# description <text>**	<text> – до 255 символов.
4	Задать MTU (необязательно).	**esr(config-if-gi)# mtu <count>**	<count> – 552–10000. Значение по умолчанию: 1500.
5	Задать скорость (необязательно).	**esr(config-if-gi)# speed 1000M/100M/10M/10G/auto**	Значение по умолчанию: auto.
6	Задать MAC-адрес (необязательно).	**esr(config-if-gi)# mac-address <ADDR>**	<ADDR> – MAC-адрес сетевого моста, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF].

7.1.2 Алгоритм настройки режима L3

Шаг	Описание	Команда	Ключи
1.1	Задать IP-адрес. Получить IP-адрес от DHCP-сервера.	**esr(config-if-gi)# ip address <ADDR/LEN>** или **esr(config-if-gi)# ip address <ADDR/LEN> secondary**	<ADDR/LEN> – IP-адрес и длина маски подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. Ключ secondary указывает, что настроенный адрес является дополнительным IP-адресом. Если это ключевое слово отсутствует, настроенный адрес является основным IP-адресом. Возможно указать до 7 дополнительных IP-адресов.
1.2		**esr(config-if-gi)# ip address dhcp**	

Шаг	Описание	Команда	Ключи
2.1	Задать IPv6-адрес. Получить IPv6-адрес от DHCP-сервера.	**esr(config-if-gi)# ipv6 address <ADDR/P>**	<ADDR/P> – IP-адрес и длина маски подсети, задаётся в виде <X:X:X:X::X/N> – где каждая буква X – это шестнадцатеричные значения шести 16-битных элементов адреса и N – длина префикса, принимает значения [1..128].
2.2		**esr(config-if-gi)# ipv6 address dhcp**	

Также для физического интерфейса в режиме L3 возможно настроить:

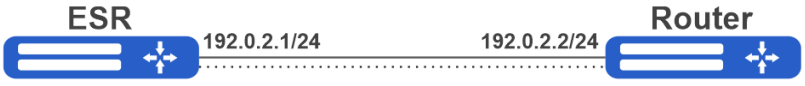
- QoS в базовом или расширенном режимах (см. раздел Управление QoS);
- proxy (см. раздел Проксирование HTTP/HTTPS-трафика);
- мониторинг трафика (см. разделы Настройка Netflow и Настройка sFlow);
- функционал протоколов маршрутизации (см. раздел Управление маршрутизацией);
- протокол VRRF (см. раздел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

⚠ Для использования firewall необходимо произвести его настройку (см. в разделе Конфигурирование Firewall).

7.1.3 Пример настройки в режиме L3

Задача:

Настроить интерфейс для прохождения трафика.



Решение:

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

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

Сохраните изменения:

```
esr(config)# commit
esr(config)# confirm
```

На противоположной стороне выдается адрес из той же подсети.

7.2 Настройка терминации на саб-интерфейсе

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

7.2.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать саб-интерфейс физического интерфейса (возможно только если физический интерфейс в режиме routeport или hybrid).	**esr(config)# interface gigabitethernet <PORT>.<S-VLAN>** или **interface tengigabitethernet <PORT>.<S-VLAN>** или **interface port-channel { <CH> | <UNIT>/<CH> }.<S-VLAN>**	<PORT> – номер физического интерфейса. <UNIT> – номер устройства в группе устройств [1..4]. <CH> – номер агрегированного интерфейса. <S-VLAN> – идентификатор создаваемого S-VLAN. Если физический интерфейс включен в bridge-group, создать саб-интерфейс будет невозможно.
2	Задать описание саб-интерфейса (необязательно).	**esr(config-if-sub)# description <DESCRIPTION>**	<DESCRIPTION> – описание интерфейса, задаётся строкой до 255 символов.
3	Указать экземпляр VRF, в котором будет работать данный саб-интерфейс (необязательно).	**esr(config-if-sub)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.

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

Шаг	Описание	Команда	Ключи
		esr(config-if-sub)# security-zone <NAME>	<NAME> – имя зоны безопасности, задаётся строкой до 31 символа.
6	Установить интервал времени, в течение которого собирается статистика о нагрузке на саб-интерфейс (необязательно).	**esr(config-if-sub)# load-average <TIME>**	<TIME> – интервал в секундах, принимает значения [5..150].
7	Установить время жизни IPv4/IPv6 записей в ARP-таблице, изученных на данном интерфейсе (необязательно).	**esr(config-if-sub)# ip arp reachable-time <TIME>** или **esr(config-if-sub)# ipv6 nd reachable-time <TIME>**	<TIME> – время жизни динамических MAC-адресов, в миллисекундах. Допустимые значения от 5000 до 100000000 миллисекунд. Реальное время обновления записи варьируется от [0,5;1,5]*<TIME>.
8	Изменить размер MTU (MaximumTransmitionUnit). MTU более 1500 будет активно только если применена команда "system jumbo-frames" (необязательно).	**esr(config-if-sub)# mtu <MTU>**	<MTU> – значение MTU в байтах. Значение по умолчанию: 1500.
9	Включить запись статистики использования текущего интерфейса (необязательно).	**esr(config-if-sub)# history statistics**	
10	Переопределить значение поля MSS (Maximum segment size) во входящих TCP-пакетах (необязательно).	**esr(config-if-sub)# ip tcp adjust-mss <MSS>** **esr(config-if-sub)# ipv6 tcp adjust-mss <MSS>**	<MSS> – значение MSS, принимает значения в диапазоне [500..1460]. Значение по умолчанию: 1460.

Также для саб-интерфейса возможно настроить:

- QoS в базовом или расширенном режимах (см. раздел Управление QoS);
- proxy (см. раздел Проксирование HTTP/HTTPS-трафика);
- мониторинг трафика (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).

7.2.2 Пример настройки саб-интерфейса

Задача:

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

Решение:

Создадим саб-интерфейс для VLAN: 828:

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

Настроим IP-адрес из необходимой подсети:

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

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

7.3 Настройка терминации на Q-in-Q интерфейсе

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

7.3.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать саб-интерфейс физического интерфейса (возможно только если физический интерфейс в режиме routeport или hybrid).	**esr(config)# interface gigabitethernet <PORT>.<S-VLAN>** или **interface tengigabitethernet <PORT>.<S-VLAN>** или **interface port-channel { <CH> | <UNIT>/<CH> }.<S-VLAN>**	<PORT> – номер физического интерфейса. <UNIT> – номер устройства в группе устройств [1..4]. <CH> – номер агрегированного интерфейса. <S-VLAN> – идентификатор создаваемого S-VLAN. Если физический интерфейс включен в bridge-group, создать саб-интерфейс будет невозможно.

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

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

Шаг	Описание	Команда	Ключи
9	Изменить размер MTU (MaximumTransmitionUnit). MTU более 1500 будет активно только если применена команда "system jumbo-frames" (необязательно).	**esr(config-if-sub)# mtu <MTU>**	<MTU> – значение MTU в байтах. Значение по умолчанию: 1500.
10	Включить запись статистики использования текущего интерфейса (необязательно).	**esr(config-if-sub)# history statistics**	
11	Переопределить значение поля MSS (Maximum segment size) во входящих TCP-пакетах (необязательно).	**esr(config-if-sub)# ip tcp adjust-mss <MSS>** **esr(config-if-sub)# ipv6 tcp adjust-mss <MSS>**	<MSS> – значение MSS, принимает значения в диапазоне [500..1460]. Значение по умолчанию: 1460.
Также для Q-in-Q интерфейса возможно настроить: • QoS в базовом или расширенном режимах (см. раздел Управление QoS); • proxy (см. раздел Проксирование HTTP/HTTPS-трафика); • мониторинг трафика (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).			

7.3.2 Пример настройки Q-in-Q интерфейса

Задача:

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

Решение:

Создадим саб-интерфейс для S-VLAN: 828:

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

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

7.4 Настройка USB-модемов

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

На маршрутизаторах ESR-1700 работа беспроводных модемов не поддержана.

7.4.1 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 cellular 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 (необязательно).	**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 пароль для пользователя мобильной сети (если мобильный оператор требует аутентификации по логину/паролю).	**esr(config-user)# password ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<CLEAR-TEXT> – пароль в открытой форме, задаётся строкой [1 .. 64] символов, может включать символы [0-9a-fA-F]; <ENCRYPTED-TEXT> – пароль в зашифрованной форме, задаётся строкой [2..128] символов.
8	Активировать пользователя (если мобильный оператор требует аутентификации по логину/паролю).	**esr(config-user)# enable**	

Шаг	Описание	Команда	Ключи
9	Установить номер дозвона для подключения к мобильной сети.	**esr(config-cellular-profile)# number <WORD>**	<WORD> – номер дозвона для подключения к мобильной сети, задаётся строкой до 15 символов.
10	Задать метод аутентификации пользователя в мобильной сети (необязательно).	**esr(config-cellular-profile)# allowed-auth <TYPE>**	<TYPE> – метод аутентификации пользователя в мобильной сети [none, PAP, CHAP, MSCHAP, MSCHAPv2, EAP]. Значение по умолчанию: PAP.
11	Ограничить возможность использования семейств IP-адресов в мобильной сети.	**esr(config-cellular-profile)# ip-version { ipv4 | ipv6 }**	ipv4 – семейство IPv4; ipv6 – семейство IPv6.
12	Создать USB-модем в конфигурации маршрутизатора и перейти в режим конфигурирования модема.	**esr(config)# cellular modem <ID>**	<ID> – идентификатор USB-модема в системе [1..10].
13	Установить режим работы беспроводного модема.	**esr(config)# mode <MODE>**	<MODE> – режим работы USB-модема [stick, hilink].
14	Задать описание модема (необязательно).	**esr(config-cellular-modem)# description <DESCRIPTION>**	<DESCRIPTION> – описание модема, задаётся строкой до 255 символов.
15	Указать экземпляр VRF, в котором будет работать данный модем (необязательно).	**esr(config-cellular-modem)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.
16	Задать идентификатор USB-модема, назначенного системой (определен в пункте 2).	**esr(config-cellular-modem)# device <WORD>**	<WORD> – идентификатор USB-порта подключенного модема, задаётся строкой до 12 символов.
17	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].
18	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.
19	Разрешить использование того или иного режима работы сети USB-модема (необязательно).	**esr(config-cellular-modem)# allowed-mode <MODE>**	<MODE> – допустимый режим работы сети USB-модема [2g, 3g, 4g]. По умолчанию: разрешены все режимы, поддерживаемые модемом.

Шаг	Описание	Команда	Ключи
20	Задать размер максимального принимаемого пакета (необязательно).	**esr(config-cellular-modem)# mru { <MRU> }**	<MRU> – значение MRU, принимает значения в диапазоне [128..16383]. Значение по умолчанию: 1500.
21	Изменить максимальный размер обрабатываемых пакетов MTU (MaximumTransmitionUnit). MTU более 1500 будет активно, только если применена команда "system jumbo-frames" (необязательно).	**esr(config-cellular-modem)# mtu <MTU>**	<MTU> – значение MTU в байтах. Значение по умолчанию: 1500.
22	Задать предпочтительный режим работы USB-модема в мобильной сети (необязательно).	**esr(config-cellular-modem)# preferred-mode { <MODE> }**	<MODE> – предпочтительный режим работы USB-модема [2g, 3g, 4g].
23	Отключить на интерфейсе функции Firewall или включить интерфейс в зону безопасности (см. раздел Конфигурирование Firewall).	**esr(config-if-sub)# ip firewall disable**	
		esr(config-if-sub)# security-zone <NAME>	<NAME> – имя зоны безопасности, задаётся строкой до 31 символа.
24	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 трафика (см. разделы Настройка Netflow и Настройка sFlow);
- функционал протоколов маршрутизации (см. разделы Policy-based routing и MultiWAN).

Список поддерживаемых устройств, предоставленный производителем интегрированного драйвера см. по ссылке.

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

7.4.2 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
```

7.5 Настройка PPP через E1

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

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

На маршрутизаторах ESR-1000 не поддерживается работа модулей ToPGATE-WAN-E1 с аппаратной версией (hardware revision) 812.

7.5.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
Предварительная настройка:			
1	Необходимо включить поддержку Jumbo-фреймов. Для вступления изменений в силу требуется перезагрузка устройства.	**esr(config)# system jumbo-frames**	
Настройка физического интерфейса:			
2	Необходимо выбрать интерфейс, в котором установлен TOPGATE-WAN-E1.	**esr(config)# interface gigabitethernet 1/0/3**	
3	Перевести физический интерфейс в режим коммутации.	**esr(config-if-gi)# mode switchport**	
4	Задать режим работы интерфейса E1.	**esr(config-if-gi)# switchport mode e1**	
5	Задать источник синхронизации (необязательно).	**esr(config-if-gi)# switchport e1 clock source <SOURCE>**	<SOURCE> – источник синхронизации: • **internal** (по умолчанию) – синхронизироваться с внутренним источником; • **line** – синхронизироваться с линейным сигналом.
6	Указать размер MTU (Maximum Transmition Unit) для физических интерфейсов.	**esr(config-if-gi)# mtu <MTU>**	<MTU> – значение MTU, для E1- и Multilink-интерфейсов необходимо указать значения в диапазоне [1510..9600].

Шаг	Описание	Команда	Ключи
7	Задать хэш-алгоритм проверки кадра (необязательно).	**esr(config-if-gi)# switchport e1 crc <FCS>**	<FCS> – последовательность проверки кадра: • **16** (по умолчанию) – FCS16; • **32** – FCS32.
8	Задать проверку на наличие ошибок при передаче (необязательно).	**esr(config-if-gi)# switchport e1 framing <CRC>**	<CRC> – проверка циклической избыточности: • **crc-4** – использовать алгоритм CRC-4; • **no-crc4** (по умолчанию) – не использовать проверку.
9	Задать инвертирование передаваемых бит (необязательно).	**esr(config-if-gi)# switchport e1 invert data**	
10	Задать тип линейного кодирования (необязательно).	**esr(config-if-gi)# switchport e1 linecode <CODE>**	<CODE> – тип линейного кодирования; • **ami** – чередующейся полярностью импульсов; • **hdb3** (по умолчанию) – двухполярный код высокой плотности порядка 3.
11	Задать количество тайм-слотов.	**esr(config-if-gi)# switchport e1 timeslots <RANGE>**	<RANGE> – количество тайм-слотов.
12	Использовать E1 как единую сущность, без тайм-слотов (необязательно).	**esr(config-if-gi)# switchport e1 unframed**	
Настройка интерфейса E1:			
13	Необходимо выбрать интерфейс E1.	**esr(config)# interface e1 1/<SLOT>/1**	<SLOT> – номер слота.
14	Указать IPv4 и маску подсети для конфигурируемого интерфейса.	**esr(config-if-e1)# ip address <ADDR/LEN>**	<ADDR/LEN> – IP-адрес и длина маски подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].

Шаг	Описание	Команда	Ключи
15	Отключить на интерфейсе функции Firewall или включить интерфейс в зону безопасности (см. раздел Конфигурирование Firewall).	**esr(config-if-e1)# ip firewall disable**	
		esr(config-if-e1)# security-zone <NAME>	<NAME> – имя зоны безопасности, задаётся строкой до 31 символа.
Дополнительные настройки PPP для E1:			
16	Включить CHAP-аутентификацию для PPP (необязательно).	**esr(config-if-e1)# ppp authentication chap**	
17	Задать имя маршрутизатора, которое отправляется удаленной стороне для прохождения CHAP-аутентификации (необязательно).	**esr(config-if-e1)# ppp chap hostname <NAME>**	<NAME> – имя маршрутизатора.
18	Задать пароль для аутентификации (необязательно).	**esr(config-if-e1)# ppp chap password ascii-text <CLEAR-TEXT>**	<CLEAR-TEXT> – пароль в открытой форме, задаётся строкой [1 .. 64] символов, может включать символы [0-9a-fA-F].
19	Включить игнорирование аутентификации (необязательно).	**esr(config-if-e1)# ppp chap refuse**	
20	Задать имя пользователя для аутентификации (необязательно).	**esr(config-if-e1)# ppp chap username <NAME>**	<NAME> – имя пользователя.
21	Разрешается принимать от соседа любой ненулевой IP-адрес в качестве локального IP-адреса (необязательно).	**esr(config-if-e1)# ppp ipcp accept-address**	
22	Задать IP-адрес, который отправляется удаленной стороне для последующего его присвоения (необязательно).	**esr(config-if-e1)# ppp ipcp remote-address <ADDR>**	<ADDR> – IP-адрес удаленного шлюза.
23	Задать количество попыток отправки Configure-Request пакетов, прежде чем удаленный пир будет признан неспособным ответить (необязательно).	**esr(config-if-e1)# ppp max-configure <VALUE>**	<VALUE> – количество попыток.
24	Задать количество попыток отправки Configure-NAK пакетов, прежде чем будут подтверждены все опции (необязательно).	**esr(config-if-e1)# ppp max-failure <VALUE>**	<VALUE> – количество попыток.
25	Задать количество попыток отправки Terminate-Request пакетов, прежде чем сессия будет прервана (необязательно).	**esr(config-if-e1)# ppp max-terminate <VALUE>**	<VALUE> – количество попыток.

Шаг	Описание	Команда	Ключи
26	Задать размер MRU (Maximum Receive Unit) для интерфейса (необязательно).	**esr(config-if-e1)# ppp mru <MRU>**	<MRU> – значение MRU.
27	Задается интервал времени в секундах, по истечении которого маршрутизатор отправляет keepalive-сообщение (необязательно).	**esr(config-if-e1)# ppp timeout keepalive <TIME>**	<TIME> – время в секундах.
28	Задается интервал, по истечении которого маршрутизатор повторяет запрос на установление сессии (необязательно).	**esr(config-if-e1)# ppp timeout retry <TIME>**	<TIME> – время в секундах.
Включение интерфейса E1 в Multilink PPP:			
29	Добавить в MLPPP-группу (необязательно).	**esr(config-if-e1)# ppp multilink-group <GROUP-ID>**	<GROUP-ID> – номер группы.
30	Включение режима MLPPP (необязательно).	**esr(config-if-e1)# ppp multilink**	

7.5.2 Пример конфигурации

Задача:

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



Решение:

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

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

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

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

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

Настроим интерфейс e1:

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

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

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

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

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

7.6 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.

7.6.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Настроить группу агрегации.	**esr(config)# interface multilink <IF>**	<IF> – наименование интерфейса.
2	Указать описание конфигурируемой группы агрегации (необязательно).	**esr(config-if-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 (необязательно).	**esr(config-if-multilink)# load-average <TIME>**	<TIME> – интервал в секундах, принимает значения [5..150]. Значение по умолчанию: 5.
4	Указать размер MTU (Maximum Transmition Unit) для группы агрегации (необязательно). MTU более 1500 будет активно только в случае применения команды "system jumbo-frames".	**esr(config-if-multilink)# mtu <MTU>**	<MTU> – значение MTU, принимает значения в диапазоне [1280..1500]. Значение по умолчанию: 1500.
5	Включить CHAP-аутентификацию.	**esr(config-if-multilink)# ppp authentication chap**	
6	Включить игнорирование аутентификации (необязательно).	**esr(config-if-multilink)# ppp chap refuse**	

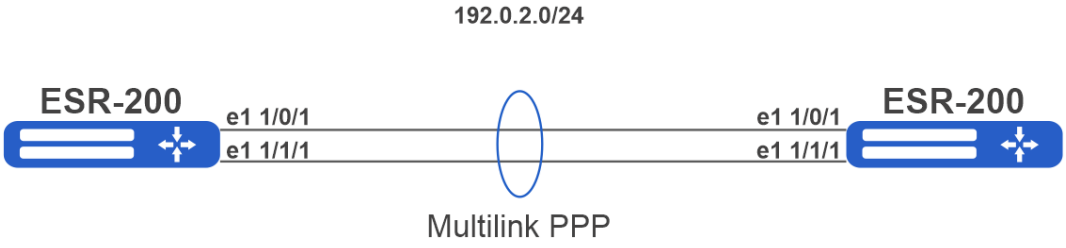
7	Указать имя маршрутизатора, которое отправляется удаленной стороне для прохождения CHAP-аутентификации.	**esr(config-if-multilink)# ppp chap hostname <NAME>**	<NAME> – имя маршрутизатора, задаётся строкой до 31 символа
8	Указать пароль, который отправляется удаленной стороне вместе с именем маршрутизатора для прохождения CHAP-аутентификации.	**esr(config-if-multilink)# ppp chap password ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<CLEAR-TEXT> – пароль в открытой форме, задаётся строкой [8 .. 64] символов, может включать символы [0-9a-fA-F]. <ENCRYPTED-TEXT> – пароль в зашифрованной форме, задаётся строкой [16..128] символов.
9	Разрешить принимать от соседа любой ненулевой IP-адрес в качестве локального IP-адреса (необязательно).	**esr(config-if-multilink)# ppp ipcp accept-address**	
10	Установить IP-адрес, который отправляется удаленной стороне для последующего его присвоения.	**esr(config-if-multilink)# ppp iccp remote-address <ADDR>**	<ADDR> – IP-адрес удаленного шлюза.
11	Указать пользователя для аутентификации удаленной стороны и перейти в режим конфигурирования указанного пользователя.	**esr(config-if-multilink)# chap username <NAME>**	<NAME> – имя пользователя, задаётся строкой до 31 символа.
12	Установить пароль в открытой или зашифрованной форме определенному пользователю для аутентификации удаленной стороны.	**esr(config-ppp-user)# password ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<CLEAR-TEXT> – пароль в открытой форме, задаётся строкой [8 .. 64] символов, может включать символы [0-9a-fA-F]. <ENCRYPTED-TEXT> – пароль в зашифрованной форме, задаётся строкой [16..128] символов.
13	Установить количество попыток отправки Configure-Request пакетов, прежде чем удаленный пир будет признан неспособным ответить (необязательно).	**esr(config-if-multilink)# ppp max-configure <VALUE>**	<VALUE> – время в секундах, принимает значения [1..255]. Значение по умолчанию: 10.
14	Установить количество попыток выслать Configure-NAK пакеты, прежде чем будут подтверждены все опции (необязательно).	**esr(config-if-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 (необязательно).	**esr(config-if-multilink)# ppp max-terminate <VALUE>**	<VALUE> – время в секундах, принимает значения [1..255]. Значение по умолчанию: 2.
16	Указать размер MRU (Maximum Receive Unit) для интерфейса.	**esr(config-if-multilink)# ppp mru <MRU>**	<MRU> – значение MRU, принимает значения в диапазоне [128..1485]. Значение по умолчанию: 1500.
17	Указать интервал времени в секундах, по истечении которого маршрутизатор отправляет keepalive-сообщение (необязательно).	**esr(config-if-multilink)# ppp timeout keepalive <TIME>**	<TIME> – время в секундах, принимает значения [1..32767]. Значение по умолчанию: 10.
18	Установить интервал времени в секундах, по истечении которого маршрутизатор повторяет запрос на установление сессии (необязательно).	**esr(config-if-multilink)# ppp timeout retry <TIME>**	<TIME> – время в секундах, принимает значения [1..255]. Значение по умолчанию: 3.
19	Определить максимальный размер пакета для MLPP-интерфейса.	**esr(config-if-multilink)# mrru <MRRU>**	<MRRU> – максимальный размер принимаемого пакета для MLPP-интерфейса, принимает значение в диапазоне [1500..10000].
20	Привязать порт e1 к физическому интерфейсу.	**esr(config-if-gi)# switchport e1 <SLOT>**	<SLOT> – идентификатор слота, принимает значение в диапазоне [0..3].
21	Перевести физический порт в режим работы с SFPe1-модулем.	**esr(config-if-gi)# switchport mode e1**	
22	Включить режим MLPPP на E1-интерфейсе.	**esr(config-if-e1)# ppp multilink**	
23	Включить E1-интерфейс в группу агрегации.	**esr(config-if-e1)# ppp multilink-group <GROUP-ID>**	<GROUP-ID> – идентификатор группы, принимает значение [1..4].

7.6.2 Пример настройки

Задача:

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



Решение:

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

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

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

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

Настроим интерфейс multilink:

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

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

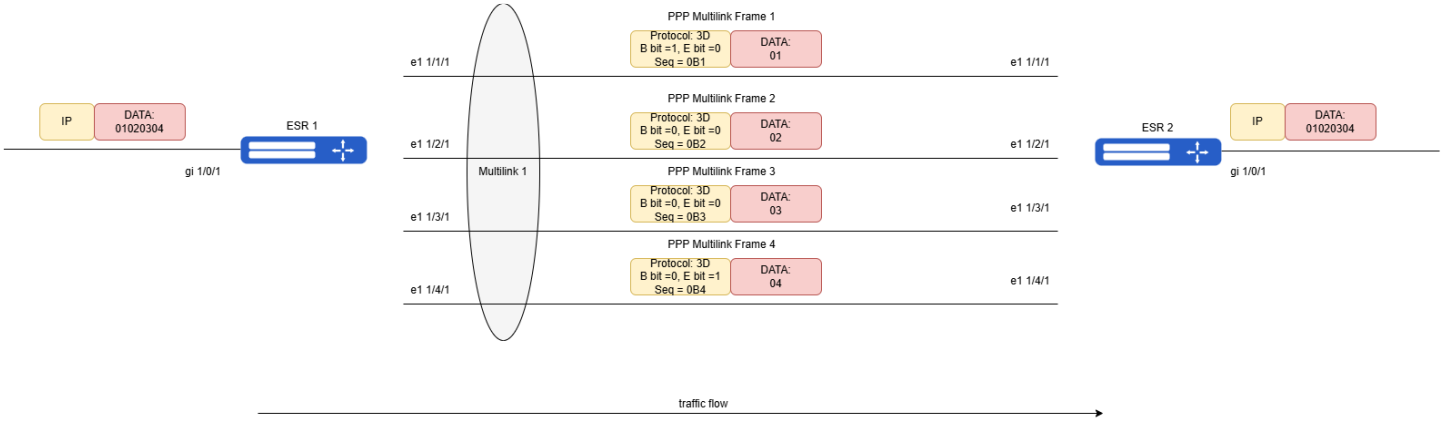
```
esr(config)# interface e1 1/0/1
esr(config-if-e1)# ppp multilink-group 3
esr(config-if-e1)# ppp multilink
esr(config-if-e1)# exit
esr(config)# interface e1 1/1/1
esr(config-if-e1)# ppp multilink-group 3
esr(config-if-e1)# ppp multilink
esr(config-if-e1)# exit
```

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

```
esr# show interfaces status multilink 3
Interface 'mu3' status information:
    Description:          --
    Operational state:    Up
    Administrative state: Up
    Track ID:             0
    Supports broadcast:   No
    Supports multicast:   Yes
    MTU:                  1492
    MAC address:          none
    Last change:          1 hour, 4 minutes and 2 seconds
    Mode:                 routerport
    Bandwidth:            3968 Kbps
    Member links:         2 active, 0 inactive
        * e1 1/0/1:       Up 23 minutes and 58 seconds ago
          e1 1/1/1:       Up 30 minutes and 36 seconds ago
```

7.6.3 Фрагментация трафика

По умолчанию каждый пакет, который будет отправлен через мультилинк, подлежит фрагментации. Пакет делится на равные части пропорционально количеству линков в мультилинке. Каждый фрагмент инкапсулируется в ML PPP. На противоположной стороне пакет собирается из фрагментов в свое первоначальное состояние.



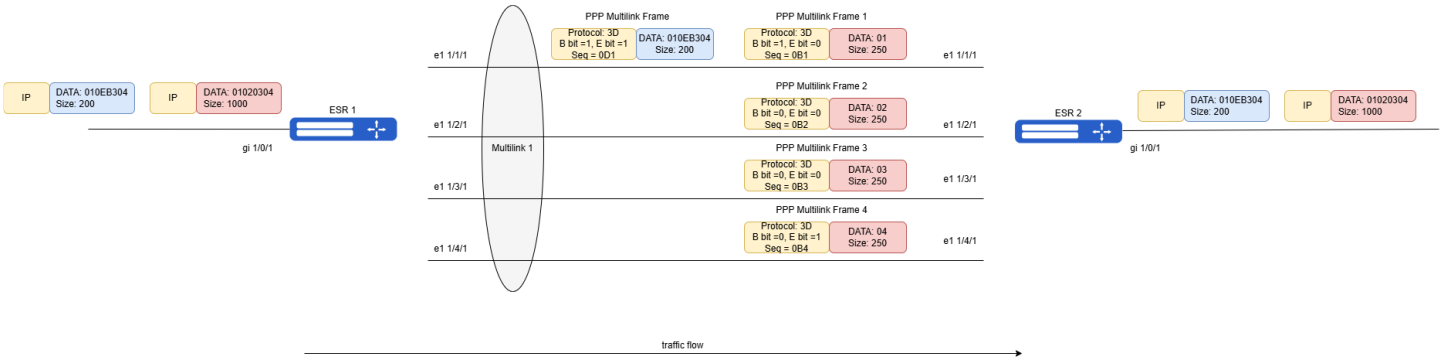
В случае передачи большого количество пакетов небольшого размера (например, голосовой трафик) такое поведение порождает избыточное количество служебного трафика, что негативно влияет на утилизацию канала, а также является одной из причин возникновения задержек при передаче.

> Например, пакет размером 80 байт, проходящий через мультилинк, в котором 8 участников, будет разделен на 8 фрагментов по 10 байт. На каждый фрагмент будет добавлен ML PPP заголовок (4 байта).

Для оптимизации такого поведения можно указать минимальный размер, все пакеты меньше которого не будут подлежать фрагментации.

```
ESR# config
esr-1200(config)# interface multilink 1
esr-1200(config-if-multilink)# min-frag-size 200
esr-1200(config)# do commit
esr-1200(config)# do confirm
```

После включения данного функционала пакеты, размер которых меньше 200 байт, не будут фрагментированы. Пакеты с большим размер будут подлежать фрагментации.



7.7 Настройка AUX

> ⚠ Для модели ESR-21, ESR-31.

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

7.7.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим конфигурирования последовательного интерфейса.	**esr(config)# line aux [<UNIT>/ <SLOT>/<PORT>]**	<UNIT> – номер устройства в группе устройств; <SLOT> – номер модуля в составе устройства или 0 при отсутствии деления устройства на модули; <PORT> – порядковый номер порта.

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

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

7.7.2 Примеры настроек

Задача 1:

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



⚠ Модемы должны быть предварительно введены в режим автоматической установки соединения.

⚠ **Проверена совместимость с модемами**

- Tainet T-336Cx
- Modem Zyxel U-336E Plus

Решение:

Сконфигурировать первый ESR-21

Настроим параметры согласования:

```
esr-21-1(config)# line aux 1/0/2
esr-21-1(config-line-aux)# flowcontrol hardware
esr-21-1(config-line-aux)# exit
esr-21-1(config)#
```

Сконфигурируем необходимые RS-232 интерфейсы:

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

Сконфигурируем firewall для зон безопасности:

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

И укажем принадлежность интерфейсов к зоне безопасности:

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

Сконфигурировать второй ESR-21

Настроим параметры согласования:

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

Сконфигурируем необходимые RS-232 интерфейсы:

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

Сконфигурируем firewall для зон безопасности:

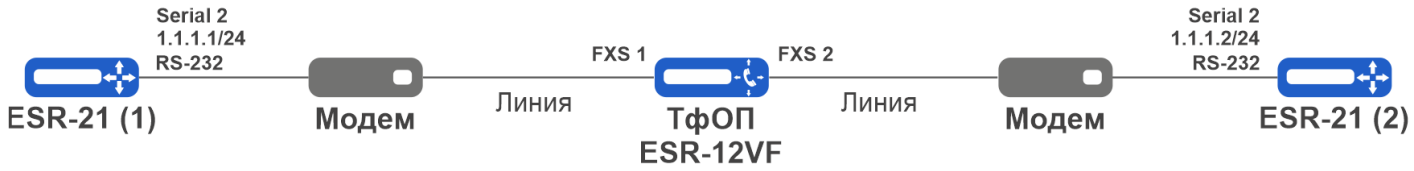
```
esr-21-2(config)# security zone xx
esr-21-2(config-zone)# exit
esr-21-2(config)# security zone-pair xx self
esr-21-2(config-zone-pair)#   rule 1
esr-21-2(config-zone-pair-rule)# action permit
esr-21-2(config-zone-pair-rule)# enable
esr-21-2(config-zone-pair-rule)# exit
esr-21-2(config-zone-pair)#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

И укажем принадлежность интерфейсов к зоне безопасности:

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

Задача 2:

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



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

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

Проверена совместимость с модемами

- Modem ZyXEL OMNI 56K (MINI).
- Modem Acorp-M56SCD.
- Tainet T-336Cx

Решение:

Сконфигурировать первый ESR-21

Настроим параметры согласования с модемом:

```
esr-21-1(config)# line aux 1/0/2
esr-21-1(config-line-aux)# flowcontrol hardware
esr-21-1(config-line-aux)# modem inout
esr-21-1(config-line-aux)# exit
esr-21-1(config)#
```

Сконфигурируем необходимые RS-232 интерфейсы:

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

Сконфигурируем firewall для зон безопасности:

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

И укажем принадлежность интерфейсов к зоне безопасности:

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

Включим дозвон по номеру:

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

Сконфигурировать второй ESR-21

Настроим параметры согласования:

```
esr-21-2(config)# line aux 1/0/2
esr-21-2(config-line-aux)# flowcontrol hardware
esr-21-2(config-line-aux)# modem inout
esr-21-2(config-line-aux)# exit
esr-21-2(config)#
```

Сконфигурируем необходимые RS-232 интерфейсы:

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

Сконфигурируем firewall для зон безопасности:

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

И укажем принадлежность интерфейсов к зоне безопасности:

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

Задача 3:

Использовать дополнительные параметры настройки модемов для задачи 2:

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

Решение

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

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

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

Включим использование строки инициализации модема:

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

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

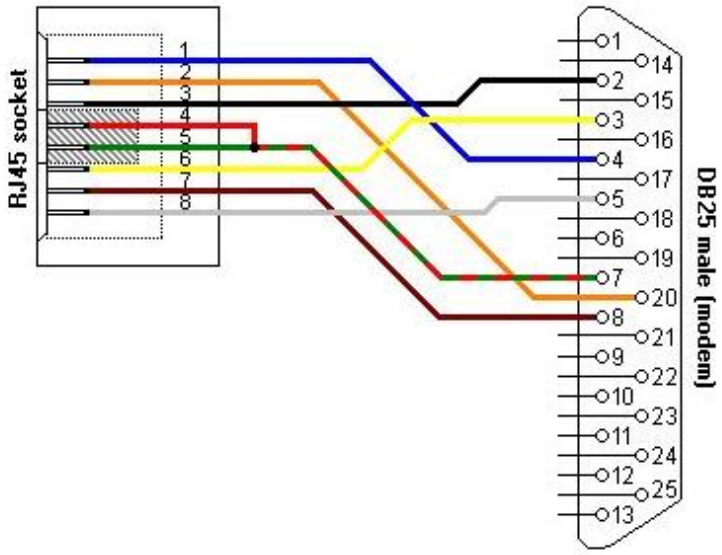
```
esr-21-2(config)# chat-script answer_test "ABORT 'BUSY' ABORT 'NO CARRIER' '' AT OK AT&F OK
ATM0L0 RING ATAr CONNECT '"
esr-21-2(config)#
```

Включим использование строки инициализации модема:

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

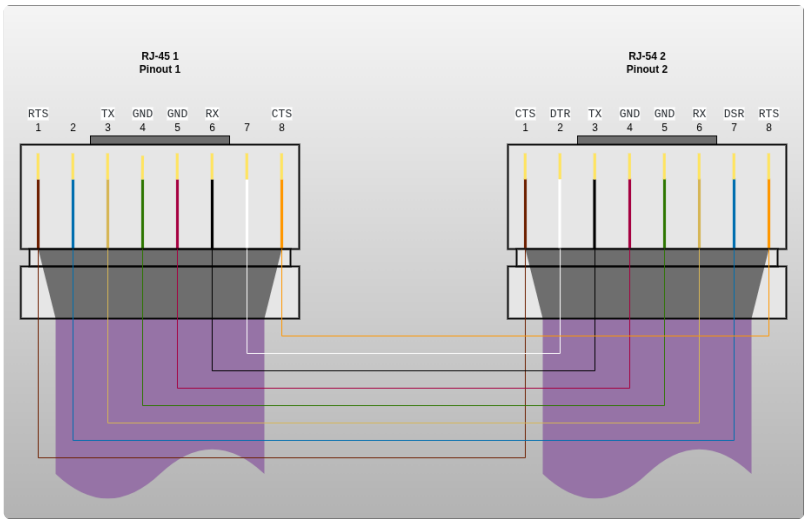
7.7.3 Схемы распайки переходников

RJ-45 <--> DB-25 pinout

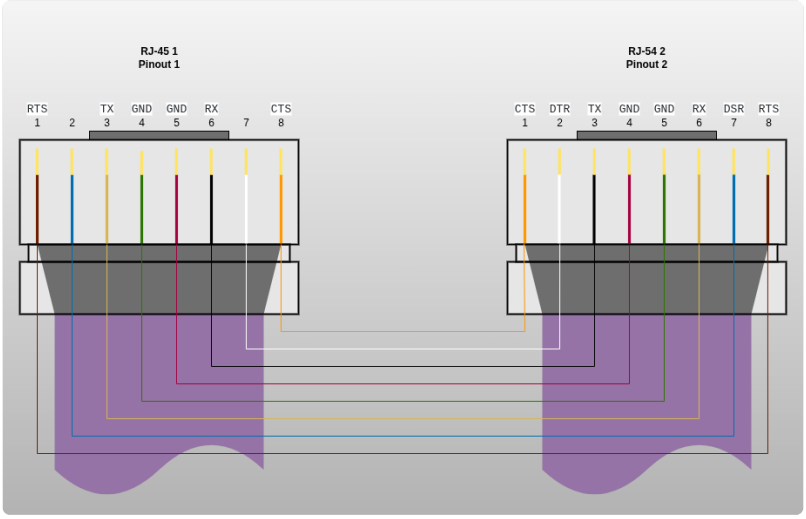


RJ-45 <--> RJ-45 pinout (rolled over cable)

Для подключения **любых** устройстве серии ESR следует выполнить кроссировку кабеля по схеме cross rollover:



Допускается использования straight rollover схемы кроссировки кабеля для всех устройств серии ESR, **кроме** моделей ESR-3xx0 (3100 / 3150 / 3200(L) / 3250 / 3300 / 3350):



8 Управление туннелированием

- Настройка GRE-туннелей
  - Алгоритм настройки
  - Пример настройки IP-GRE-туннеля
- Настройка DMVPN
  - Алгоритм настройки
  - Пример настройки 1
  - Пример настройки 2
- Настройка L2TPv3-туннелей
  - Алгоритм настройки
  - Пример настройки L2TPv3-туннеля
- Настройка IPsec VPN
  - Алгоритм настройки Route-based IPsec VPN
  - Пример настройки Route-based IPsec VPN
  - Алгоритм настройки Policy-based IPsec VPN
  - Пример настройки Policy-based IPsec VPN с аутентификацией по общему известному ключу
  - Пример настройки Policy-based IPsec VPN с аутентификацией сертификатам X.509, выписываемых PKI-клиентом
  - Алгоритм настройки Remote Access IPsec VPN
  - Пример настройки Remote Access IPsec VPN
  - Пример настройки DPD (Dead Peer Detection)
- Настройка LT-туннелей
  - Алгоритм настройки
  - Пример настройки

8.1 Настройка GRE-туннелей

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

В маршрутизаторе ESR 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.

8.1.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Сконфигурировать L3-интерфейс, от которого будет строиться GRE-туннель.		

Шаг	Описание	Команда	Ключи
2	Создать GRE-туннель и перейти в режим его конфигурирования.	**esr(config)# tunnel gre <INDEX>**	<INDEX> – идентификатор туннеля в диапазоне: • для ESR-10/12V(F)/ 15/15R/15VF – [1..10]; • для ESR-20/21/30/31/ 100/200 – [1..250]; • для ESR-1000/1200/ 1500/1511 (rev.B)/ 3100/3150/3200/ 3200L/3250/3300/3350 – [1..500]; • для ESR-1700 – [1...3200].
3	Указать экземпляр VRF, в котором будет работать данный GRE-туннель (необязательно).	**esr(config-gre)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.
4	Указать имя VRF от IP-интерфейса которого будет строиться данный GRE-туннель (необязательно).	**esr-(config-gre)# tunnel-source vrf <VRF>**	<VRF> – имя экземпляра VRF, задается строкой до 31 символа. Без указания ключа "vrf" и имени экземпляра VRF будет использоваться IP-интерфейс глобальной конфигурации.
5	Указать описание конфигурируемого туннеля (необязательно).	**esr(config-gre)# description <DESCRIPTION>**	<DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов.
6	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.
7	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].

Шаг	Описание	Команда	Ключи
8	Указать режим инкапсуляции для GRE-туннеля.	**esr(config-gre)# mode <MODE>**	<MODE> – режим инкапсуляции для GRE-туннеля: • **ip** – инкапсуляция IP-пакетов в GRE; • **ethernet** – инкапсуляция Ethernet-фреймов в GRE. Значение по умолчанию: ip
9	Установить IP-адрес локальной стороны туннеля (только в режиме ip).	**esr(config-gre)# ip address <ADDR/LEN> [unit <ID>]** или **esr(config-gre)# ip address <ADDR/LEN> secondary [unit <ID>]**	<ADDR/LEN> – IP-адрес и префикс подсети задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. <ID> – номер юнита, принимает значения [1..4]. Ключ secondary указывает, что настроенный адрес является дополнительным IP-адресом. Если это ключевое слово отсутствует, настроенный адрес является основным IP-адресом. Возможно указать до 7 дополнительных IP-адресов. Дополнительные функции IPv4-адресации см. в разделе Настройка IP-адресации.
10	Назначить широковещательный домен для инкапсуляции в GRE-пакеты данного туннеля (только в режиме ethernet).	**esr(config-gre)# bridge-group <BRIDGE-ID>**	<BRIDGE-ID> – идентификационный номер моста, принимает значения в диапазоне: • для ESR-10/12V(F)/ 15/15R/15VF – [1..50]; • для ESR-20/21/30/31/ 100/200 – [1..250]; • для ESR-1000/1200/ 1500/1511 (rev.B)/ 1700/3100/3150/3200/ 3200L/3250/3300/3350 – [1..500].

Шаг	Описание	Команда	Ключи
11	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	
12	Указать размер MTU (Maximum Transmition Unit) для туннеля (необязательно). MTU более 1500 будет активно, только если применена команда "system jumbo-frames".	**esr(config-gre)# mtu <MTU>**	<MTU> – значение MTU, принимает значения в диапазоне: • для ESR-10/12V(F)/ 15/15R/15VF – [1280..9600]; • для ESR-20/21/30/31 – [1280..9500]; • для ESR-100/200/1000/ 1200/1500/1511 (rev.B)/ 1700/3100/3150/3200/ 3200L/3250/3300/3350 – [1280..10000]. Значение по умолчанию: 1500.
13	Указать значение времени жизни TTL для туннельных пакетов (необязательно).	**esr(config-gre)# ttl <TTL>**	<TTL> – значение TTL, принимает значения в диапазоне [1..255]. Значение по умолчанию: наследуется от инкапсулируемого пакета.
14	Указать DSCP для использования в IP-заголовке инкапсулирующего пакета (необязательно).	**esr(config-gre)# dscp <DSCP>**	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: наследуется от инкапсулируемого пакета.
15	Разрешить передачу ключа (key) в туннельном заголовке GRE (в соответствии с RFC 2890) и установить значение ключа. Настраивается только с обеих сторон туннеля (необязательно).	**esr(config-gre)# key <KEY>**	<KEY> – значение KEY, принимает значения в диапазоне [1..2000000]. Значение по умолчанию: ключ не передаётся.

Шаг	Описание	Команда	Ключи
16	Включить вычисление контрольной суммы и занесение её в GRE-заголовок отправляемых пакетов. При этом на удаленной стороне необходимо включить проверку контрольной суммы (необязательно).	**esr(config-gre)# local checksum**	
17	Включить проверку наличия и соответствия значений контрольной суммы в заголовках принимаемых GRE-пакетов. При этом на удаленной стороне необходимо включить вычисление контрольной суммы (необязательно).	**esr(config-gre)# remote checksum**	
18	Включить проверку доступности удаленного шлюза туннеля (необязательно).	**esr(config-gre)# keepalive enable**	
19	Изменить время ожидания keepalive пакетов от встречной стороны (необязательно).	**esr(config-gre)# keepalive timeout <TIME>**	<TIME> – время в секундах, принимает значения в диапазоне [1..32767]. Значение по умолчанию: 10.
20	Изменить количество попыток проверки доступности удаленного шлюза туннеля (необязательно).	**esr(config-gre)# keepalive retries <VALUE>**	<VALUE> – количество попыток, принимает значения в диапазоне [1..255]. Значение по умолчанию: 5.
21	Указать IP-адрес для работы механизма keepalive (обязательно в режиме ethernet).	**esr(config-gre)# keepalive dst-address <ADDR>**	<ADDR> – IP-адрес для проверки работоспособности GRE-туннеля.
22	Изменить интервал времени, за который усредняется статистика о нагрузке на туннеле (необязательно).	**esr(config-gre)# load-average <TIME>**	<TIME> – интервал в секундах, принимает значения [5..150]. Значение по умолчанию: 5.
23	Включить отправку snmp-trap о включении/отключении туннеля.	**esr(config-gre)# snmp init-trap**	
24	Включить механизм перезапроса IP-адресов по протоколу DHCP на указанных интерфейсах при отключении GRE-туннеля по keepalive (необязательно).	**esr(config-gre)# keepalive dhcp dependent-interface <IF>**	<IF> – физический/ логический интерфейс, на котором включено получение IP-адреса по DHCP.

Шаг	Описание	Команда	Ключи
25	Задать интервал времени между отключением GRE-туннеля и перезапросом IP-адреса на интерфейсе/интерфейсах, указанных командой keepalive dhcp dependent-interface (необязательно).	**esr(config-gre)# keepalive dhcp link-timeout <SEC>**	<SEC> – интервал между отключением GRE-туннеля и перезапросом IP-адреса по DHCP на интерфейсах.
26	Переопределить значение поля MSS (Maximum segment size) во входящих TCP-пакетах (необязательно).	**esr(config-gre)# ip tcp adjust-mss <MSS>**	<MSS> – значение MSS, принимает значения в диапазоне [500..1460]. Значение по умолчанию: 1460.
27	Включить запись статистики использования текущего туннеля (необязательно).	**esr(config-gre)# history statistics**	
28	Активировать туннель.	**esr(config-gre)# enable**	

Также для GRE-туннеля возможно настроить:

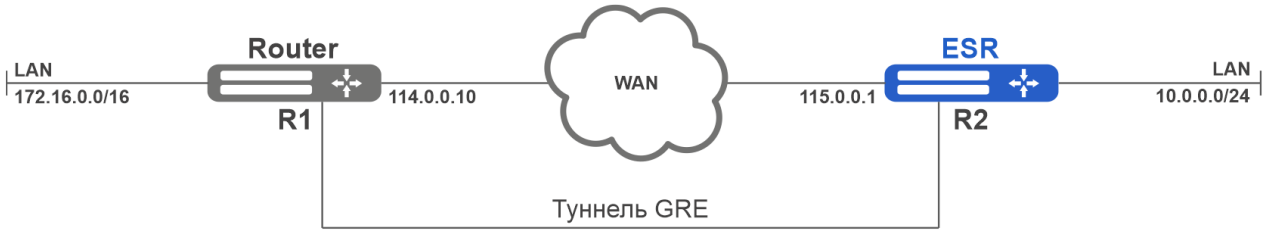
- QoS в базовом или расширенном режимах (см. раздел Управление QoS);
- proxy (см. раздел Проксирование HTTP/HTTPS-трафика);
- мониторинг трафика (см. разделы Настройка Netflow и Настройка sFlow);
- функционал протоколов маршрутизации (см. раздел Управление маршрутизацией);
- функционал BRAS (см. раздел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

8.1.2 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).

8.2 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.

8.2.1 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.
3	Создать GRE-туннель и перейти в режим его конфигурирования.	**esr(config)# tunnel gre <INDEX>**	<INDEX> – идентификатор туннеля.
4	Перевести GRE-туннель в режим multipoint.	**esr(config-gre)# multipoint**	
5	Указать экземпляр VRF, в котором будет работать данный GRE-туннель (необязательно).	**esr(config-gre)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.
6	Указать имя VRF от IP-интерфейса которого будет строиться данный GRE-туннель (необязательно).	**esr(config-gre)# tunnel-source vrf <VRF>**	<VRF> – имя экземпляра VRF, задается строкой до 31 символа. Без указания ключа "vrf" и имени экземпляра VRF, будет использоваться IP-интерфейс глобальной конфигурации.
7	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].

Шаг	Описание	Команда	Ключи
		esr(config-gre)# local interface <IF>	<IF> – интерфейс, от IP-адреса которого устанавливается туннель.
8	Задать IP-адрес на туннеле. В качестве альтернативы можно настроить DHCP-клиент для получения IP-адреса от DHCP-сервера.	**esr(config-gre)# ip address <ADDR/LEN>** или **esr(config-gre)# ip address <ADDR/LEN> secondary**	<ADDR/LEN> – IP-адрес и длина маски подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. Ключ secondary указывает, что настроенный адрес является дополнительным IP-адресом. Если это ключевое слово отсутствует, настроенный адрес является основным IP-адресом. Возможно указать до 7 дополнительных IP-адресов.
		esr(config-gre)# ip address dhcp	
9	Установить открытый пароль для NHRP-пакетов (необязательно).	**esr(config-gre)# ip nhrp authentication <WORD>**	<WORD> – пароль в открытой форме, задается строкой [1..8] символов, может включать символы [0-9a-fA-F].
10	Указать время, в течение которого на NHS будет существовать запись о данном клиенте (не обязательно).	**esr(config-gre)# ip nhrp holding-time <TIME>**	<TIME> – время в секундах, в течение которого на сервере будет существовать запись о данном клиенте, принимает значения [1..65535]. Значение по умолчанию: 7200.
11	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].
12	Задать «логический (туннельный)» адрес NHRP-сервера.	**esr(config-gre)# ip nhrp nhs <ADDR>**	<ADDR> – адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть AAA – DDD принимает значения [0..255].

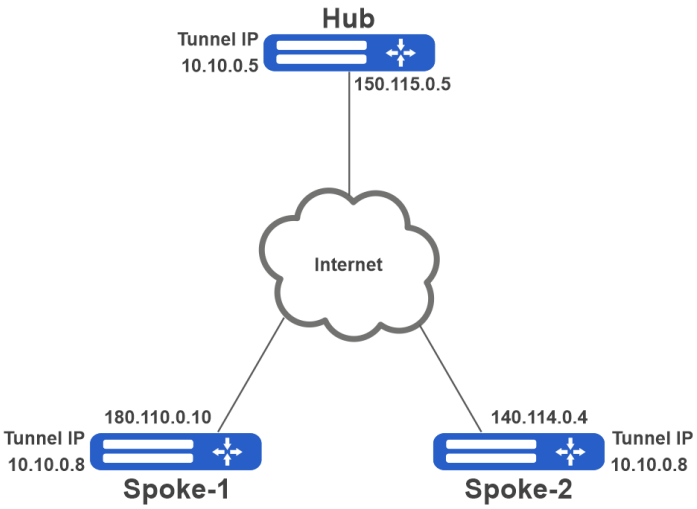
Шаг	Описание	Команда	Ключи
13	Определить адресата мультикастного трафика.	**esr(config-gre)# ip nhrp multicast { dynamic | nhs | <ADDR> }**	• **dynamic** – отправлять на все пиры, с которыми есть соединение; • **nhs** – отправлять на все статические сконфигурированные сервера; <ADDR> – отправлять на специфически сконфигурированный адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
14	Включить возможность отправки NHRP Traffic Indication пакетов. Выполняется на NHS (необязательно).	**esr(config-gre)# ip nhrp redirect**	
15	Включить возможность создания кратчайших маршрутов. Выполняется на NHC (необязательно).	**esr(config-gre)# ip nhrp shortcut**	
16	Привязать IPsec-VPN к mGRE-туннелю (необязательно).	**esr(config-gre)# ip nhrp ipsec <WORD> { static | dynamic }**	<WORD> – имя VPN, задаётся строкой до 31 символа; • **static** – статическое соединение, применятся для связи с NHS; • **dynamic** – динамически устанавливающееся соединение, конфигурируется для связи между NHC.
17	Включить передачу имени NHRP-группы NHRP-соседям в процессе обмена NHRP-сообщениями (необязательно).	**esr(config-gre)# ip nhrp attribute group <WORD>**	<WORD> – имя группы NHRP, задаётся строкой [1..40] символов, не принимает символы [^#].
18	Задать соответствие группы NHRP, полученной от NHRP-соседа в процессе обмена NHRP-сообщениями, и политики QoS, которая будет применена к исходящему в сторону этого NHRP-соседа трафика (необязательно).	**esr(config-gre)# ip nhrp map group <GROUP> service-policy output <POLICY>**	<GROUP> – имя группы NHRP, задаётся строкой [1..40] символов, не принимает символы [^#]; <POLICY> – имя QoS-политики, задается строкой [1..31] символов.
19	Включить работу протокола NHRP.	**esr(config-gre)# ip nhrp enable**	

Шаг	Описание	Команда	Ключи
20	Организовать IP-связность посредством протокола динамической маршрутизации.		
Остальные настройки аналогичны настройкам статичного GRE-туннеля (см. раздел Настройка GRE-туннелей).			

8.2.2 Пример настройки 1

Задача:

Организовать DMVPN между офисами компании, используя mGRE-туннели, NHRP (Next Hop Resolution Protocol), протокол динамической маршрутизации (BGP), IPsec. В данном примере 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.

Предварительная настройка интерфейсов:

```
esr-Hub# configure
esr-Hub(config)# int gi1/0/1
esr-Hub(config-if-gi)# ip address 150.115.0.5/24
esr-Hub(config-if-gi)# ip firewall disable
esr-Hub(config-if-gi)# exit
esr-Hub(config)# ip route 0.0.0.0/0 150.115.0.1
esr-Hub(config)# do commit
esr-Hub(config)# do confirm

esr-Spoke-1# configure
esr-Spoke-1(config)# int gi1/0/1
esr-Spoke-1(config-if-gi)# ip address 180.100.0.10/24
esr-Spoke-1(config-if-gi)# ip firewall disable
esr-Spoke-1(config-if-gi)# exit
esr-Spoke-1(config)# ip route 0.0.0.0/0 180.100.0.1
esr-Spoke-1(config)# do commit
esr-Spoke-1(config)# do confirm

esr-Spoke-2# configure
esr-Spoke-2(config)# int gi1/0/1
esr-Spoke-2(config-if-gi)# ip address 140.114.0.4/24
esr-Spoke-2(config-if-gi)# ip firewall disable
esr-Spoke-2(config)# exit
esr-Spoke-2(config)# ip route 0.0.0.0/0 140.114.0.1
esr-Spoke-2(config)# do commit
esr-Spoke-2(config)# do confirm
```

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
   ```

2. Зададим значение MTU:

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

   Установим значение ttl:

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

   Отключим firewall:

   ```
   esr(config-gre)# ip firewall disable
   ```

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 примере это будет BGP.
Поскольку в примере используется eBGP необходимо явно разрешить анонсирование подсетей:

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

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

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)# type transport
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)# tunnel gre 5
esr(config-gre)# ip nhrp ipsec IPSECVPN dynamic
```

Включим работу NHRP и сам туннель:

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

3. Конфигурирование Spoke
   Проведём стандартную настройку DMVPN на туннеле:

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

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
```

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-gre)# ip nhrp multicast nhs
```

Произведём настройку BGP для spoke. Поскольку в примере используется eBGP необходимо явно разрешить анонсирование подсетей:

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

esr(config)# router bgp 65008
esr(config-bgp)# neighbor 10.10.0.5
esr(config-bgp-neighbor)# remote-as 65005
esr(config-bgp-neighbor)# enable
esr(config-bgp-neighbor)# address-family ipv4 unicast
esr(config-bgp-neighbor-af)# route-map PERMIT_ALL out
esr(config-bgp-neighbor-af)# enable
esr(config-bgp-neighbor-af)# exit
esr(config-bgp-neighbor)# exit
esr(config-bgp)# address-family ipv4 unicast
esr(config-bgp-af)# exit
esr(config-bgp)# 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)# type transport
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-ipsec-vpn)# exit
```

```
esr(config)# security ipsec vpn IPSECVPN_SPOKE
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# type transport
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
esr(config-ipsec-vpn)# exit
```

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

```
esr(config)# tunnel gre 8
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
```

Сохраним конфигурацию:

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

> ⚠ Для использования firewall необходимо произвести его настройку. В данном примере firewall был отключён.

Состояние NHRP-записей можно посмотреть командой:

```
esr# show ip nhrp peers
```

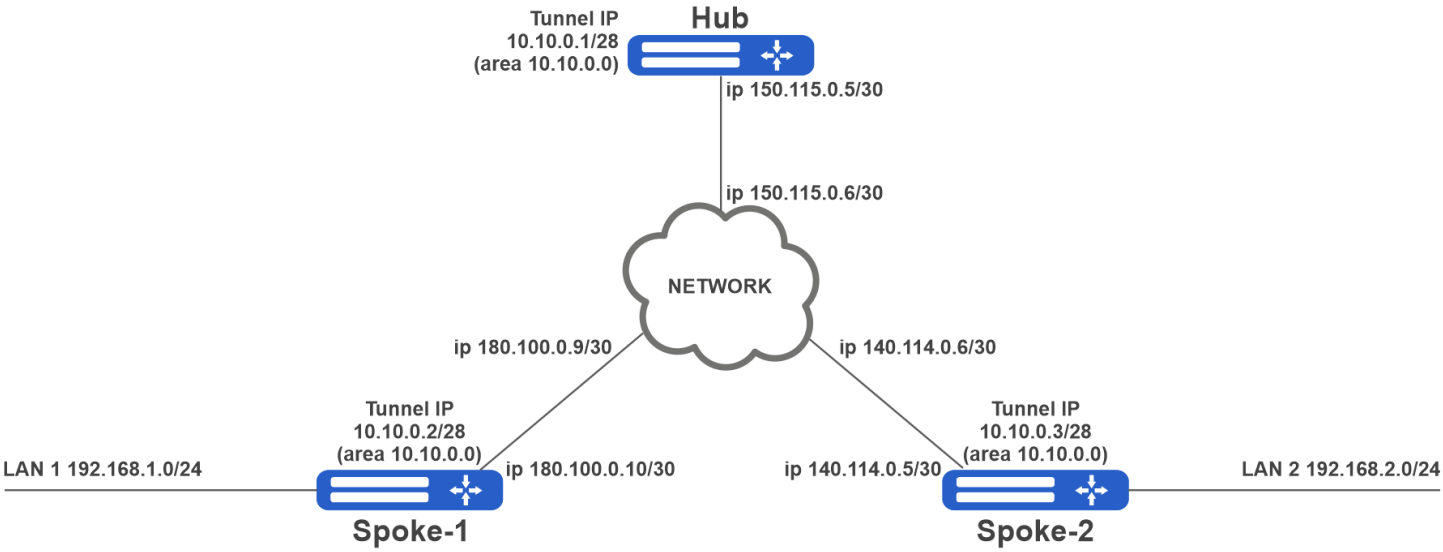
Очистить NHRP-записи можно командой:

```
esr# clear ip nhrp peers
```

8.2.3 Пример настройки 2

Задача:

Организовать DMVPN между офисами компании с соответствующими подсетями LAN1 и LAN2, используя mGRE-туннели, NHRP (Next Hop Resolution Protocol), протокол динамической маршрутизации (OSPF), IPsec. В нашем примере у нас будет HUB-маршрутизатор и два филиала. HUB – это DMVPN-сервер (NHS), а филиалы – DMPVN-клиенты (NHC).



При использовании схемы DMVPN необходимо, чтобы HUB являлся DR-маршрутизатором. Таким образом, маршруты локальных подсетей spoke 1 и spoke 2 будут ретранслироваться через hub.

HUB внешний IP-адрес — 150.115.0.5;
SPOKE-1 внешний IP-адрес — 180.100.0.10;
SPOKE-2 внешний IP-адрес — 140.114.0.4.

Параметры IPsec VPN:

IKE:

- группа Диффи-Хэллмана: 2;
- алгоритм шифрования: AES128;
- алгоритм аутентификации: MD5.

IPsec:

- группа Диффи-Хэллмана: 2;
- алгоритм шифрования: AES128;
- алгоритм аутентификации: MD5.

Решение:

1. Конфигурирование HUB:
   Предварительно настроим протокол OSPF:

```
esr(config)# router ospf log-adjacency-changes
esr(config)# router ospf 1
esr(config-ospf)# router-id 77.77.77.77
esr(config-ospf)# area 10.10.0.0
esr(config-ospf-area)# enable
esr(config-ospf-area)# exit
esr(config-ospf)# enable
esr(config-ospf)# exit
```

   Настроим интерфейс и определим принадлежность к зоне безопасности:

```
esr(config)# 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 150.115.0.5/30
esr(config-if-gi)# exit
```

   Настроим GRE-туннель, определим принадлежность к зоне безопасности, настроим OSPF на GRE-туннеле, настроим NHRP и включим туннель и NHRP командой enable. Чтобы HUB стал DR, необходимо выставить максимальный приоритет:

```
esr(config)# tunnel gre 1
esr(config-gre)# ttl 16
esr(config-gre)# mtu 1416
esr(config-gre)# multipoint
esr(config-gre)# security-zone untrusted
esr(config-gre)# local address 150.115.0.5
esr(config-gre)# ip address 10.10.0.1/28
esr(config-gre)# ip ospf instance 1
esr(config-gre)# ip ospf area 10.10.0.0
esr(config-gre)# ip ospf priority 255
esr(config-gre)# ip ospf
esr(config-gre)# ip nhrp multicast dynamic
esr(config-gre)# ip nhrp enable
esr(config-gre)# enable
esr(config-gre)# exit
```

   Создадим статические маршруты для подсетей интерфейсов spoke 180.100.0.8/30 и 140.114.0.4/30:

```
esr(config)# ip route 180.100.0.8/30 150.115.0.6
esr(config)# ip route 140.114.0.4/30 150.115.0.6
```

Произведём настройку IPsec для HUB:

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

```
esr(config)# security ike policy ike_pol1
esr(config-ike-policy)# pre-shared-key ascii-text password
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit
```

```
esr(config)# security ike gateway ike_spoke
esr(config-ike-gw)# ike-policy ike_pol1
esr(config-ike-gw)# local address 150.115.0.5
esr(config-ike-gw)# local network 150.115.0.5/32 protocol gre
esr(config-ike-gw)# remote address any
esr(config-ike-gw)# remote network any
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

```
esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# pfs dh-group 2
esr(config-ipsec-proposal)# exit
```

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

```
esr(config)# security ipsec vpn ipsec_spoke
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# type transport
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway ike_spoke
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
```

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

```
esr(config)# tunnel gre 1
esr(config-gre)# ip nhrp ipsec ipsec_spoke dynamic
esr(config-gre)# exit
```

2. Конфигурирование SPOKE:
   Предварительно настроим протокол OSPF с анонсированием подсети LAN1:

```
esr(config)# router ospf log-adjacency-changes
esr(config)# router ospf 1
esr(config-ospf)# router-id 1.1.1.1
esr(config-ospf)# area 10.10.0.0
esr(config-ospf-area)# network 192.168.1.0/24
esr(config-ospf-area)# enable
esr(config-ospf-area)# exit
esr(config-ospf)# enable
esr(config-ospf)# exit
```

   Настроим интерфейс и определим принадлежность к зоне безопасности:

```
esr(config)# 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 180.100.0.10/30
esr(config-if-gi)# exit
```

   Настроим GRE-туннель, определим принадлежность к зоне безопасности, настроим OSPF на GRE-туннеле, настроим NHRP и включим туннель и NHRP командой enable. Чтобы HUB стал DR, необходимо выставить минимальный приоритет на spoke:

```
esr(config)# tunnel gre 1
esr(config-gre)# ttl 16
esr(config-gre)# mtu 1416
esr(config-gre)# multipoint
esr(config-gre)# security-zone untrusted
esr(config-gre)# local address 180.100.0.10
esr(config-gre)# ip address 10.10.0.2/28
esr(config-gre)# ip ospf instance 1
esr(config-gre)# ip ospf area 10.10.0.0
esr(config-gre)# ip ospf priority 0
esr(config-gre)# ip ospf
esr(config-gre)# ip nhrp holding-time 300
esr(config-gre)# ip nhrp map 10.10.0.1 150.115.0.5
esr(config-gre)# ip nhrp nhs 10.10.0.1/28
esr(config-gre)# ip nhrp multicast nhs
esr(config-gre)# ip nhrp enable
esr(config-gre)# enable
esr(config-gre)# exit
```

   Создадим статические маршруты для подсетей интерфейсов spoke 180.100.0.8/30 и 140.114.0.4/30:

```
esr(config)# ip route 150.115.0.4/30 180.100.0.9
esr(config)# ip route 140.114.0.4/30 180.100.0.9
```

Произведём настройку IPsec для SPOKE:

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

```
esr(config)# security ike policy ike_pol1
esr(config-ike-policy)# pre-shared-key ascii-text password
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# exit
```

```
esr(config)# security ike gateway ike_spoke
esr(config-ike-gw)# ike-policy ike_pol1
esr(config-ike-gw)# local address 180.100.0.10
esr(config-ike-gw)# local network 180.100.0.10/32 protocol gre
esr(config-ike-gw)# remote address any
esr(config-ike-gw)# remote network any
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
esr(config)# security ike gateway ike_hub
esr(config-ike-gw)# ike-policy ike_pol1
esr(config-ike-gw)# local address 180.100.0.10
esr(config-ike-gw)# local network 180.100.0.10/32 protocol gre
esr(config-ike-gw)# remote address 150.115.0.5
esr(config-ike-gw)# remote network 150.115.0.5/32 protocol gre
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

```
esr(config)# security ipsec proposal ipsec_prop1
esr(config-ipsec-proposal)# authentication algorithm md5
esr(config-ipsec-proposal)# encryption algorithm aes128
esr(config-ipsec-proposal)# pfs dh-group 2
esr(config-ipsec-proposal)# exit
```

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

```
esr(config)# security ipsec vpn ipsec_spoke
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# type transport
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway ike_spoke
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
esr(config)# security ipsec vpn ipsec_hub
esr(config-ipsec-vpn)# mode ike
esr(config-ipsec-vpn)# type transport
esr(config-ipsec-vpn)# ike establish-tunnel route
esr(config-ipsec-vpn)# ike gateway ike_hub
esr(config-ipsec-vpn)# ike ipsec-policy ipsec_pol1
esr(config-ipsec-vpn)# enable
esr(config-ipsec-vpn)# exit
```

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

```
esr(config)# tunnel gre 1
esr(config-gre)# ip nhrp ipsec ipsec_hub static
esr(config-gre)# ip nhrp ipsec ipsec_spoke dynamic
esr(config-gre)# exit
```

3. Состояние NHRP-записей можно посмотреть командой:

```
esr# show ip nhrp
```

4. Дополнительно в security zone-pair untrusted self необходимо разрешить протоколы для GRE over IPSec-туннеля, а также для протокола OSPF:

```
esr(config)# object-group service ISAKMP_PORT
esr(config-object-group-service)# port-range 500
esr(config-object-group-service)# port-range 4500
esr(config-object-group-service)# exit
esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol udp
esr(config-zone-pair-rule)# match destination-port object-group ISAKMP_PORT
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# rule 2
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol gre
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# rule 3
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol esp
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# rule 4
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol ospf
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
```

8.3 Настройка L2TPv3-туннелей

L2TPv3 (Layer 2 Tunneling Protocol Version 3) — протокол для туннелирования пакетов 2 уровня модели OSI между двумя IP-узлами. В качестве инкапсулирующего протокола используется IP или UDP. L2TPv3 может использоваться как альтернатива MPLS P2P L2VPN (VLL) для организации VPN уровня L2. В 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.

8.3.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Сконфигурировать L3-интерфейс, от которого будет строиться L2TPv3-туннель.		

Шаг	Описание	Команда	Ключи
2	Создать L2TPv3-туннель и перейти в режим его конфигурирования.	**esr(config)# tunnel l2tpv3 <INDEX>**	<INDEX> – идентификатор туннеля в диапазоне: • для ESR-10/12V(F)/ 15/15R/15VF – [1..10]; • для ESR-20/21/30/31/ 100/200 – [1..250]; • для ESR-1000/1200/ 1500/1511 (rev.B)/1700/ 3100/3150/3200/3200L/ 3250/3300/3350 – [1..500].
3	Указать описание конфигурируемого туннеля (необязательно).	**esr(config-l2tpv3)# description <DESCRIPTION>**	<DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов.
4	Установить локальный IP-адрес для установки туннеля.	**esr(config-l2tpv3)# local address <ADDR>**	<ADDR> – IP-адрес локального шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
5	Установить удаленный IP-адрес для установки туннеля.	**esr(config-l2tpv3)# remote address <ADDR>**	<ADDR> – IP-адрес локального шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
6	Выбрать метод инкапсуляции для туннеля L2TPv3.	**esr(config-l2tpv3)# protocol <TYPE>**	<TYPE> – тип инкапсуляции, возможные значения: • **ip** – инкапсуляция в IP-пакет; • **udp** – инкапсуляция в UDP-дейтаграммы.
7	Установить локальный идентификатор сессии.	**esr(config-l2tpv3)# local session-id <SESSION-ID>**	<SESSION-ID> – идентификатор сессии, принимает значения [1..200000].
8	Установить удаленный идентификатор сессии.	**esr(config-l2tpv3)# remote session-id <SESSION-ID>**	<SESSION-ID> – идентификатор сессии, принимает значения [1..200000].
9	Определить локальный UDP-порт (если в качестве метода инкапсуляции был выбран UDP протокол).	**esr(config-l2tpv3)# local port <UDP>**	<UDP> – номер UDP-порта в диапазоне [1..65535].

Шаг	Описание	Команда	Ключи
10	Определить удаленный UDP-порт (если в качестве метода инкапсуляции был выбран UDP-протокол).	**esr(config-l2tpv3)# remote port <UDP>**	<UDP> – номер UDP-порта в диапазоне [1..65535].
11	Назначить широковещательный домен для инкапсуляции в L2TPV3-пакеты данного туннеля.	**esr(config-l2tpv3)# bridge-group <BRIDGE-ID>**	<BRIDGE-ID> – идентификационный номер моста, принимает значения в диапазоне: • для ESR-10/12V(F)/15/15R/15VF – [1..50]; • для ESR-20/21/30/31/100/200 – [1..250]; • для ESR-1000/1200/1500/1511 (rev.B)/1700/3100/3150/3200/3200L/3250/3300/3350 – [1..500].
12	Активировать туннель.	**esr(config-l2tpv3)# enable**	
13	Указать размер MTU (MaximumTransmitionUnit) для туннелей (необязательно). MTU более 1500 будет активно только в случае применения команды "system jumbo-frames".	**esr(config-l2tpv3)# mtu <MTU>**	<MTU> – значение MTU, принимает значения в диапазоне: • для ESR-10/12V(F)/15/15VF/15R – [1280..9600]; • для ESR-20/21/30/31 – [1280..9500]; • для ESR-100/200/1000/1200/1500/1511/1700/3100/3150/3200/3200L/3250/3300/3350 – [1280..10000]. Значение по умолчанию: 1500.
14	Определить локальное значение cookie для дополнительной проверки соответствия между передаваемыми данными и сессией (необязательно).	**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 (необязательно).	**esr(config-l2tpv3)# remote cookie <COOKIE>**	<COOKIE> – значение COOKIE, параметр принимает значения длиной восемь или шестнадцать символов в шестнадцатеричном виде.

Шаг	Описание	Команда	Ключи
16	Задать интервал времени, за который усредняется статистика о нагрузке на туннеле (не обязательно).	**esr(config-l2tpv3)# load-average <TIME>**	<TIME> – интервал в секундах, принимает значения [5..150]. Значение по умолчанию: 5.
17	Включить запись статистики использования текущего туннеля (необязательно).	**esr(config-if-sub)# history statistics**	

Также для L2TPv3-туннеля возможно настроить:

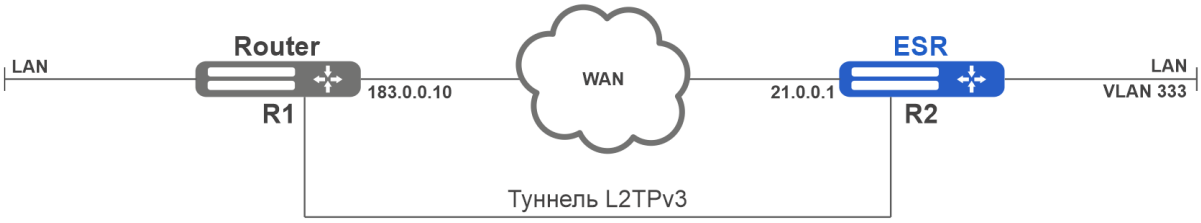
- QoS в базовом или расширенном режимах (см. раздел Управление QoS);
- функционал BRAS (см. раздел Управление BRAS (Broadband Remote Access Server)).

8.3.2 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:

> ⚠ Предварительно необходимо в firewall разрешить входящий трафик по протоколу UDP с портом отправителя 519 и портом назначения 519.

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-if-sub)# bridge-group 333
esr(config-if-sub)# 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
```

8.4 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.

8.4.1 Алгоритм настройки Route-based IPsec VPN

Шаг	Описание	Команда	Ключи
1	Создать VTI-туннель и перейти в режим его конфигурирования.	**esr(config)# tunnel vti <TUN>**	<TUN> – имя туннеля устройства.
2	Указать локальный IP-адрес VTI-туннеля.	**esr(config-vti)#local address <ADDR>**	<ADDR> – IP-адрес локального шлюза.
3	Указать удаленный IP-адрес VTI-туннеля.	**esr(config-vti)#remote address <ADDR>**	<ADDR> – IP-адрес удаленного шлюза.
4	Установить IP-адрес локальной стороны VTI-туннеля.	**esr(config-vti)# ip address <ADDR/LEN> [unit <ID>]** или **esr(config-vti)# ip address <ADDR/LEN> secondary [unit <ID>]**	<ADDR/LEN> – IP-адрес и префикс подсети задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]; <ID> – номер юнита, принимает значения [1..4]. Ключ secondary указывает, что настроенный адрес является дополнительным IP-адресом. Если это ключевое слово отсутствует, настроенный адрес является основным IP-адресом. Возможно указать до 7 дополнительных IP-адресов.

Шаг	Описание	Команда	Ключи
5	Включить VTI-туннель в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall для VTI-туннеля.	**esr(config-vti)# security-zone<NAME>** **esr(config-vti)# ip firewall disable**	<NAME> – имя зоны безопасности, задаётся строкой до 12 символов.
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 (необязательно).	**esr(config-ike-proposal)# description<DESCRIPTION>**	<DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов.
9	Определить алгоритм аутентификации для IKE (необязательно).	**esr(config-ike-proposal)# authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2-384, sha2-512. Значение по умолчанию: sha1.
10	Определить алгоритм шифрования для IKE (необязательно).	**esr(config-ike-proposal)# encryption algorithm <ALGORITHM>**	<ALGORITHM> – протокол шифрования, принимает значения: des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256. Значение по умолчанию: 3des.
11	Определить номер группы Диффи-Хэллмана (необязательно).	**esr(config-ike-proposal)# dh-group <DH-GROUP>**	<DH-GROUP> – номер группы Диффи-Хэллмана, принимает значения [1, 2, 5, 14, 15, 16, 17, 18]. Значение по умолчанию: 1.
12	Создать IKE-политику и перейти в режим её конфигурирования.	**esr(config)# security ike policy <NAME>**	<NAME> – имя политики IKE, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
13	Определить режим аутентификации IKE (необязательно).	**esr(config-ike-policy)# authentication method <METHOD>**	<METHOD> – метод аутентификации IKE-сессии. Может принимать значения: • **pre-shared-key** – метод аутентификации, использующий предварительно согласованные ключи, которые должны совпадать у обоих участников IKE-сессии; • **keyring** – метод аутентификации, использующий набор предварительно согласованных ключей; • **public-key** – метод аутентификации, использующий приватные ключи и сертификаты X.509. Файлы сертификатов и ключей должны быть загружены в локальное хранилище маршрутизатора; • **trustpoint** – метод аутентификации, использующий приватные ключи и сертификаты X.509. Файлы сертификатов и ключей предоставляются PKI-клиентом, который автоматически выписывает актуальные сертификаты у удостоверяющего центра; • **xauth-psk-key** – метод расширенной аутентификации, использующий в качестве первого фактора аутентификации предварительно согласованные ключи и пару логин-пароль пользователя в качестве второго фактора аутентификации;

Шаг	Описание	Команда	Ключи
			• **eap** – метод расширенной аутентификации, использующий приватные ключи и сертификаты X.509 для аутентификации ответчика в IKE-сессии и пару логин-пароль пользователя для аутентификации инициатора IKE-сессии.
14	Задать время жизни соединения протокола IKE (необязательно).	**esr(config-ike-policy)# lifetime seconds <SEC>**	<SEC> – период времени, принимает значения [4 ..86400] секунд. Значение по умолчанию: 10800.
15	Привязать IKE-профиль к IKE-политике.	**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 (необязательно).	**esr(config-ike-gw)# version <VERSION>**	<version> – версия IKE-протокола: v1-only или v2-only. Значение по умолчанию: v1-only.
20	Установить режим перенаправления трафика в туннель – route-based.	**esr(config-ike-gw)# mode route-based**	

Шаг	Описание	Команда	Ключи
21	Указать действие для DPD (необязательно).	**esr(config-ike-gw)# dead-peer-detection action <MODE>**	<MODE> – режим работы DPD: • **restart** – соединение переустанавливается; • **clear** – соединение останавливается; • **hold** – соединение поддерживается; • **none** – механизм выключен, никаких действий не предпринимается. Значение по умолчанию: none.
22	Указать интервал между отправкой сообщений механизмом DPD (необязательно).	**esr(config-ike-gw)# dead-peer-detection interval <SEC>**	<SEC> – интервал между отправкой сообщений механизмом DPD, принимает значения [1..180] секунд. Значение по умолчанию: 2.
23	Указать период времени ожидания ответа на сообщения механизма DPD (необязательно).	**esr(config-ike-gw)# dead-peer-detection timeout <SEC>**	<SEC> – период времени ожидания ответа на сообщения механизма DPD принимает значения [1..180] секунд. Значение по умолчанию: 30 секунд.
24	Указать базовый период времени ожидания ответа на сообщения (необязательно).	**esr(config-ike-gw)# retransmit timeout <SEC>**	<SEC> – базовый период времени ожидания ответа на сообщения принимает значения [1..30] секунд. Значение по умолчанию: 4 секунды.

Шаг	Описание	Команда	Ключи
25	Указать количество попыток повторной отправки сообщений после наступления таймаута ожидания ответа (необязательно).	**esr(config-ike-gw)# retransmit tries <TRIES>**	<TRIES> – количество попыток повторной отправки сообщений в случае наступления таймаута ожидания ответа принимает значения от 1 до 10. Для первого отправленного сообщения период времени ожидания ответа будет равен базовому периоду, указанному в команде **retransmit timeout**, а для последующих попыток интервал ожидания будет рассчитан по формуле: "retransmit timeout" * 1.8 ^ (N-1), где N - номер попытки. Значение по умолчанию: 5 попыток.
26	Указать уровень случайного разброса периода ожидания ответа на сообщения (необязательно).	**esr(config-ike-gw)# retransmit jitter <VALUE>**	<VALUE> – максимальный процент разброса значений, принимает значения [0..100]. Значение по умолчанию: 0 %
27	Указать ограничение максимального периода времени ожидания ответа на сообщения (необязательно).	**esr(config-ike-gw)# retransmit limit <SEC>**	<SEC> – максимальный период времени ожидания ответа на сообщения принимает значения [15..300] секунд. Значение по умолчанию: 0 секунд, у периода нет верхнего предела.
28	Данная команда отключает расширение MOBIKE IKEv2, которое позволяет инициатору ike-сессии изменять local address в соответствии с RFC 4555.	**esr(config-ike-gw)# mobike disable**	
29	Привязать VTI-туннель к IKE-шлюзу.	**esr(config-ike-gw)# bind-interface vti <VTI>**	<VTI> – идентификационный номер интерфейса VTI.
30	Создать в IPsec-профиль.	**esr(config)# security ipsec proposal <NAME>**	<NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа.

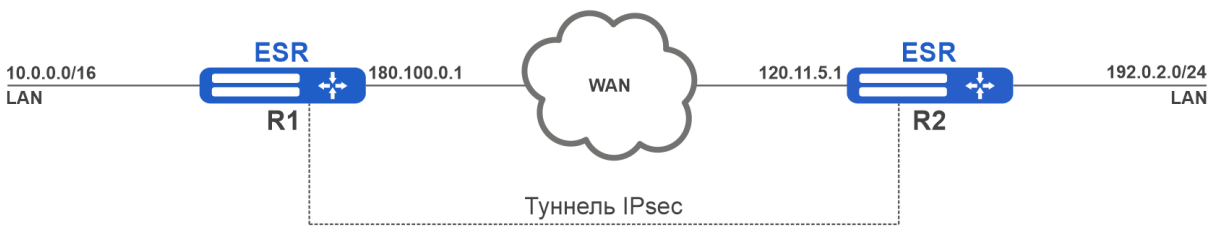
Шаг	Описание	Команда	Ключи
31	Определить алгоритм аутентификации для IPsec (необязательно).	**esr(config-ipsec-proposal)# authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2-384, sha2-512. Значение по умолчанию: sha1.
32	Определить алгоритм шифрования для IPsec (необязательно).	**esr(config-ipsec-proposal)# encryption algorithm <ALGORITHM>**	<ALGORITHM> – протокол шифрования, принимает значения: des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256. Значение по умолчанию: 3des.
33	Указать протокол инкапсуляции для IPsec (необязательно).	**esr(config-ipsec-proposal)# protocol <PROTOCOL>**	<PROTOCOL> – инкапсулирующий протокол, принимает значения: • ah – данный протокол осуществляет только аутентификацию трафика, шифрование данных не выполняется; • esp – данный протокол осуществляет аутентификацию и шифрование трафика. Значение по умолчанию: esp.
34	Создать IPsec-политику и перейти в режим её конфигурирования.	**esr(config)# security ipsec policy <NAME>**	<NAME> – имя политики IPsec, задаётся строкой до 31 символа.
35	Привязать IPsec-профиль к IPsec-политике.	**esr(config-ipsec-policy)# proposal <NAME>**	<NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
36	Задать время жизни IPsec-туннеля (необязательно).	**esr(config-ipsec- policy)# lifetime { seconds <SEC> | packets <PACKETS> | kilobytes <KB> }**	<SEC> – период времени жизни IPsec-туннеля, по истечении происходит пересогласование. Принимает значения [1140..86400] секунд. <PACKETS> – количество пакетов, после передачи которого происходит пересогласование IPsec-туннеля. Принимает значения [4..86400]. <KB> – объем трафика, после передачи которого происходит пересогласование IPsec-туннеля. Принимает значения [4..4608000] секунд. Значение по умолчанию: 28800 секунд.
37	Отключить реаутентификацию IKE-сессии (необязательно).	**esr(config-ipsec- policy)# reauthentication disable**	
38	Создать IPsec VPN и перейти в режим конфигурирования.	**esr(config)# security ipsec vpn <NAME>**	<NAME> – имя VPN, задаётся строкой до 31 символа.
39	Определить режим согласования данных, необходимых для активации VPN.	**esr(config-ipsec-vpn)# mode <MODE>**	<MODE> – режим работы VPN.
40	Привязать IPsec-политику к IPsec-VPN.	**esr(config-ipsec-vpn)# ike ipsec-policy <NAME>**	<NAME> – имя IPsec-политики, задаётся строка до 31 символа.
41	Задать значение DSCP для использования в IP-заголовке исходящих пакетов IKE-протокола (необязательно).	**esr(config-ipsec-vpn)# ike dscp <DSCP>**	DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 63.

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

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

8.4.2 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:

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

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

```
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)# ip address 10.10.10.1/30
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 500,4500
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. Поддержка MOBIKE отключается для route-based IPsec в обязательном порядке:

```
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)# mobike disable
esr(config-ike-gw)# bind-interface vti 1
esr(config-ike-gw)# version v2-only
esr(config-ike-gw)# exit
```

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

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

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

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

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

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

2. Конфигурирование R2

Настроим внешний сетевой интерфейс и определим принадлежность к зоне безопасности:

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

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

```
esr(config)# tunnel vti 1
esr(config-vti)# remote address 180.100.0.1
esr(config-vti)# local address 120.11.5.1
esr(config-vti)# ip address 10.10.10.2/30
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 500,4500
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
```

8.4.3 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 (необязательно).	**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.

Шаг	Описание	Команда	Ключи
5	Определить номер группы Диффи-Хэллмана.	**esr(config-ike-proposal)# dh-group <DH-GROUP>**	<DH-GROUP> – номер группы Диффи-Хэллмана, принимает значения [1, 2, 5, 14, 15, 16, 17, 18].
6	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
7	Определить режим аутентификации.	**esr(config-ike-policy)# authentication method <METHOD>**	<METHOD> – метод аутентификации IKE-сессии. Может принимать значения: • **pre-shared-key** – метод аутентификации, использующий предварительно согласованные ключи, которые должны совпадать у обоих участников IKE-сессии; • **keyring** – метод аутентификации, использующий набор предварительно согласованных ключей; • **public-key** – метод аутентификации, использующий приватные ключи и сертификаты X.509. Файлы сертификатов и ключей должны быть загружены в локальное хранилище маршрутизатора; • **trustpoint** – метод аутентификации, использующий приватные ключи и сертификаты X.509. Файлы сертификатов и ключей предоставляются PKI-клиентом, который автоматически выписывает актуальные сертификаты у удостоверяющего центра; • **xauth-psk-key** – метод расширенной аутентификации, использующий в качестве первого фактора аутентификации предварительно согласованные ключи и пару логин-пароль пользователя в качестве второго фактора аутентификации;

Шаг	Описание	Команда	Ключи
			• **eap** – метод расширенной аутентификации, использующий приватные ключи и сертификаты X.509 для аутентификации ответчика в IKE-сессии и пару логин-пароль пользователя для аутентификации инициатора IKE-сессии.
8	Задать время жизни соединения протокола IKE (необязательно).	**esr(config-ike-policy)# lifetime seconds <SEC>**	<SEC> – период времени, принимает значения [4 ..86400] секунд. Значение по умолчанию: 10800.
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 (необязательно).	**esr(config-ike-gw)# version <VERSION>**	<version> – версия IKE-протокола: **v1-only** или **v2-only**.

Шаг	Описание	Команда	Ключи
14	Установить режим перенаправления трафика в туннель.	**esr(config-ike-gw)#mode<MODE>**	<MODE> – режим перенаправления трафика в туннель, принимает значения: • **policy - based** – трафик перенаправляется на основе принадлежности к указанным в политиках подсетям; • **route - based** – трафик перенаправляется на основе маршрутов, шлюзом у которых является туннельный интерфейс.
15	Указать действие для DPD (необязательно).	**esr(config-ike-gw)# dead-peer-detection action <MODE>**	<MODE> – режим работы DPD: • **restart** – соединение переустанавливается; • **clear** – соединение останавливается; • **hold** – соединение поддерживается; • **none** – механизм выключен, никаких действий не предпринимается.
16	Указать интервал между отправкой сообщений механизмом DPD (необязательно).	**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 ожидания ответа на сообщения механизма DPD (необязательно).	**esr(config-ike-gw)# dead-peer-detection timeout <SEC>**	<SEC> – период времени ожидания ответа на сообщения механизма DPD принимает значения [1..180] секунд. Значение по умолчанию: 30 секунд.
18	Указать базовый период времени ожидания ответа на сообщения (необязательно).	**esr(config-ike-gw)# retransmit timeout <SEC>**	<SEC> – базовый период времени ожидания ответа на сообщения принимает значения [1..30] секунд. Значение по умолчанию: 4 секунды.

Шаг	Описание	Команда	Ключи
19	Указать количество попыток повторной отправки сообщений после наступления таймаута ожидания ответа (необязательно).	**esr(config-ike-gw)# retransmit tries <TRIES>**	<TRIES> – количество попыток повторной отправки сообщений в случае наступления таймаута ожидания ответа принимает значения от 1 до 10. Для первого отправленного сообщения период времени ожидания ответа будет равен базовому периоду, указанному в команде **retransmit timeout**, а для последующих попыток интервал ожидания будет рассчитан по формуле: "retransmit timeout" * 1.8 ^ (N-1), где N - номер попытки. Значение по умолчанию: 5 попыток.
20	Указать уровень случайного разброса периода ожидания ответа на сообщения (необязательно).	**esr(config-ike-gw)# retransmit jitter <VALUE>**	<VALUE> – максимальный процент разброса значений, принимает значения [0..100]. Значение по умолчанию: 0 %
21	Указать ограничение максимального периода времени ожидания ответа на сообщения (необязательно).	**esr(config-ike-gw)# retransmit limit <SEC>**	<SEC> – максимальный период времени ожидания ответа на сообщения принимает значения [15..300] секунд. Значение по умолчанию: 0 секунд, у периода нет верхнего предела.
22	Установить IP-адрес удаленного шлюза IPsec-туннеля.	**esr(config-ike-gw)#remote address <ADDR>**	<ADDR> – IP-адрес удаленного шлюза.

Шаг	Описание	Команда	Ключи
23	Установить IP-адрес подсети получателя, а также IP-протокол и порт.	**esr(config-ike-gw)# remote network <ADDR/LEN> [protocol { <TYPE> | <ID> } [port <PORT>]]**	<ADDR/LEN> – IP-адрес и маска подсети отправителя. Параметр задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]; <TYPE> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre; <ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF]; <PORT> – TCP/UDP-порт, принимает значения [1..65535].
	Установить		
24	Создать в профиль IPsec.	**esr(config)# security ipsec proposal <NAME>**	<NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа.
25	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.

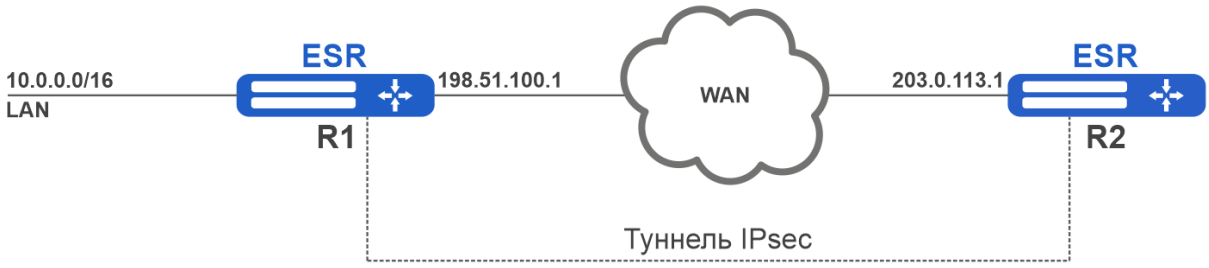
Шаг	Описание	Команда	Ключи
27	Указать протокол (необязательно).	**esr(config-ipsec-proposal)#protocol <PROTOCOL>**	<PROTOCOL> – инкапсулирующий протокол, принимает значения • ah – данный протокол осуществляет только аутентификацию трафика, шифрование данных не выполняется; • esp – данный протокол осуществляет аутентификацию и шифрование трафика. Значение по умолчанию: esp.
28	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.
29	Привязать политику к профилю.	**esr(config-ipsec-policy)# proposal <NAME>**	<NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа.
30	Задать время жизни IPsec-туннеля (необязательно).	**esr(config-ipsec-policy)# lifetime { seconds <SEC> | packets <PACKETS> | kilobytes <KB> }**	<SEC> – период времени жизни IPsec-туннеля, по истечении которого происходит пересогласование. Принимает значения [1140..86400] секунд. <PACKETS> – количество пакетов, после передачи которых происходит пересогласование IPsec-туннеля. Принимает значения [4..86400]. <KB> – объем трафика, после передачи которого происходит пересогласование IPsec-туннеля. Принимает значения [4..4608000] секунд.
31	Отключить реаутентификацию IKE-сессии (необязательно).	**esr(config-ipsec-policy)# reauthentication disable**	
32	Создать IPsec VPN и перейти в режим конфигурирования.	**esr(config)# security ipsecvpn <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 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 (необязательно).	**esr(config-ipsec-vpn)#ike dscp <DSCP>**	DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63].
36	Установить режим активации VPN.	**esr(config-ipsec-vpn)#ike establish-tunnel <MODE>**	<MODE> – режим активации VPN: • **by - request** – соединение активируется встречной стороной; • **route** – соединение активируется при появлении трафика, маршрутизируемого в туннель; • **immediate** – туннель активируется автоматически после применения конфигурации.
37	Осуществить привязка IKE-шлюза к 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 (необязательно).	**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 (необязательно).	**esr(config-ipsec-vpn)#ike rekey disable**	

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

8.4.4 Пример настройки Policy-based IPsec VPN с аутентификацией по общему известному ключу

Задача:



Настроить IPsec-туннель между R1 и R2.

R1 IP-адрес – 198.51.100.1;

R2 IP-адрес – 203.0.113.1;

IKE:

- группа Диффи-Хэллмана: 2;
- алгоритм шифрования: AES 128 bit;
- алгоритм аутентификации: MD5;
- аутентификация по общему известному ключу.

IPsec:

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

Решение:

⚠ В firewall необходимо разрешить протокол ESP, UDP-порт 500 (для протокола ISAKMP), UDP-порт 4500 (для IPsec трафика при наличии NAT между IPsec соседями).

1) Конфигурирование R1

Настроим IP-адрес на внешнем сетевом интерфейсе:

```
esr# configure
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 198.51.100.1/24
esr(config-if-gi)# exit
```

Создадим набор алгоритмов для протокола IKE. В наборе 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 укажем ранее созданный набор алгоритмов, а также укажем общий известный ключ, который будет использован при аутентификации IKE-сессии:

```
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 разделе привяжем раннее созданную политику протокола IKE, укажем IP-адреса для построения IPsec туннеля и набор локальных и удаленных сетей, трафик между которыми необходимо будет шифровать. Также укажем версию протокола IKE и "policy-based" в качестве режима перенаправления трафика в туннель:

```
esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_pol1
esr(config-ike-gw)# local address 198.51.100.1
esr(config-ike-gw)# local network 10.0.0.0/16
esr(config-ike-gw)# remote address 203.0.113.1
esr(config-ike-gw)# remote network 192.0.2.0/24
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

Создадим набор алгоритмов для IPsec-туннеля. В нем 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 раннее описанный набор алгоритмов для IPsec-туннеля.

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

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

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

2) Конфигурирование R2

Настроим IP-адрес на внешнем сетевом интерфейсе:

```
esr# configure
esr(config)# interface gi 1/0/1
esr(config-if)# ip address 203.0.113.1/24
esr(config-if)# exit
```

Создадим набор алгоритмов для протокола IKE. В наборе 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 укажем ранее созданный набор алгоритмов, а также укажем общий известный ключ, который будет использован при аутентификации IKE-сессии:

```
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 разделе привяжем раннее созданную политику протокола IKE, укажем IP-адреса для построения IPsec туннеля и набор локальных и удаленных сетей, трафик между которыми необходимо будет шифровать. Также укажем версию протокола IKE и «policy-based» в качестве режима перенаправления трафика в туннель:

```
esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_pol1
esr(config-ike-gw)# remote address 198.51.100.1
esr(config-ike-gw)# remote network 10.0.0.0/16
esr(config-ike-gw)# local address 203.0.113.1
esr(config-ike-gw)# local network 192.0.2.0/24
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

Создадим набор алгоритмов для IPsec-туннеля. В нем 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 ранее описанный набор алгоритмов для IPsec-туннеля.

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

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

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

Состояние туннеля можно посмотреть командой:

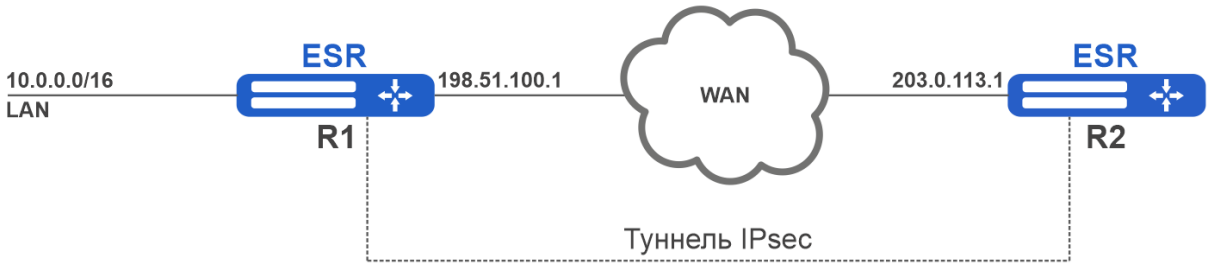
```
esr# show security ipsec vpn status ipsec1
```

Конфигурацию туннеля можно посмотреть командой:

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

8.4.5 Пример настройки Policy-based IPsec VPN с аутентификацией сертификатам X.509, выписываемых PKI-клиентом

Задача:



Настроить IPsec-туннель между R1 и R2.

R1 IP-адрес – 198.51.100.1;

R2 IP-адрес – 203.0.113.1;

PKI:

- R1 выступает в роли PKI-сервера – удостоверяющего центра с самоподписанным сертификатом;
- На R1 и R2 настраиваются PKI-клиенты, запрашивающие выпуск сертификатов для IPsec VPN на R1.

IKE:

- группа Диффи-Хэллмана: 2;
- алгоритм шифрования: AES 128 bit;
- алгоритм аутентификации: MD5;
- аутентификация по сертификатам X.509.

IPsec:

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

Решение:

⚠ В firewall необходимо разрешить протокол ESP, UDP-порт 500 (для протокола ISAKMP), UDP-порт 4500 (для IPsec трафика при наличии NAT между IPsec соседями). Также на стороне R1 необходимо разрешить TCP-порт 80 для доступа PKI-клиентов к PKI-серверу.

1) Конфигурирование R1

Настроим IP-адрес на внешнем сетевом интерфейсе:

```
esr# configure
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 198.51.100.1/24
esr(config-if-gi)# exit
```

Настроим NTP-клиента на получение точного времени от шлюза Интернет-провайдера:

```
esr(config)# ntp enable
esr(config)# ntp server 198.51.100.15
esr(config-ntp-server)# exit
esr(config)#
```

Настроим PKI-сервер. В нем заполним отличительное имя, challenge-password, время жизни выписываемых клиентских сертификатов и привяжем PKI-сервер к внешнему сетевому интерфейсу:

```
esr(config)# crypto pki server
esr(config-pki-server)# subject-name
esr(config-pki-server-subject-name)# country RU
esr(config-pki-server-subject-name)# state Moscow
esr(config-pki-server-subject-name)# locality Moscow
esr(config-pki-server-subject-name)# organization Company
esr(config-pki-server-subject-name)# common-name ca.company.loc
esr(config-pki-server-subject-name)# exit
esr(config-pki-server)# source-interface gi 1/0/1
esr(config-pki-server)# challenge-password password
esr(config-pki-server)# lifetime 7
esr(config-pki-server)# enable
esr(config-pki-server)# exit
esr(config)#
```

На этом этапе необходимо применить конфигурацию на маршрутизаторе, чтобы получить цифровой отпечаток сертификата PKI-сервера из вывода команды **show crypto pki server**, он понадобится в дальнейшей настройке PKI-клиентов:

```
esr# show crypto pki server
Status:                     Enabled
Lifetime days:              14
Certificate fingerprint:    79:D2:B6:7E:DF:77:2D:C5:27:68:99:10:BA:EC:D2:47
Source:                     gigabitethernet 1/0/1
Last issued serial number: --
Challenge password:         Active
ESR.CA#
```

Продолжим дальнейшую настройку PKI-клиента. Необходимо заполнить отличительное имя, URL для подключения к PKI-серверу (в случае маршрутизатора R1 – его собственный IP-адрес, назначенный на внешний интерфейс), ранее полученный цифровой отпечаток сертификата PKI-сервера и доменное имя маршрутизатора в качестве альтернативного имени клиентского сертификата:

```
esr(config)# crypto pki trustpoint TP_R1
esr(config-trustpoint)# subject-name
esr(config-trustpoint-subject-name)# country RU
esr(config-trustpoint-subject-name)# state Moscow
esr(config-trustpoint-subject-name)# locality Moscow
esr(config-trustpoint-subject-name)# organization Company
esr(config-trustpoint-subject-name)# common-name r1.company.loc
esr(config-trustpoint-subject-name)# exit
esr(config-trustpoint)# subject-alt-name
esr(config-trustpoint-san)# dns r1.company.loc
esr(config-trustpoint-san)# exit
esr(config-trustpoint)# url http://198.51.100.1/
esr(config-trustpoint)# fingerprint 79:D2:B6:7E:DF:77:2D:C5:27:68:99:10:BA:EC:D2:47
esr(config-trustpoint)# challenge-password password
esr(config-trustpoint)# enable
esr(config-trustpoint)# exit
esr(config)#
```

Перейдем к настройке VPN.

Создадим набор алгоритмов для протокола IKE. В наборе 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 указываем ранее созданный набор алгоритмов, в качестве метода аутентификации выбираем "trustpoint" и в команде **crypto trustpoint** указываем имя ранее созданного PKI-клиента, выписываемые им сертификаты будут использованы при аутентификации IKE-сессии:

```
esr(config)# security ike policy ike_pol1
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# authentication method trustpoint
esr(config-ike-policy)# crypto trustpoint TP_R1
esr(config-ike-policy)# exit
```

Создадим шлюз протокола IKE. В данном разделе привяжем раннее созданную политику протокола IKE, укажем IP-адреса для построения IPsec туннеля и набор локальных и удаленных сетей, трафик между которыми необходимо будет шифровать. Также укажем версию протокола IKE и «policy-based» в качестве режима перенаправления трафика в туннель:

⚠ Важным моментом при настройке аутентификации по сертификатам X.509 является указание корректных local id и remote id, присутствующих в сертификатах в качестве альтернативных имен сертификата. Поскольку ранее в настройках PKI-клиента в качестве альтернативного имени было указано полное доменное имя маршрутизатора – укажем его и в командах **local id** и **remote id**.

```
esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_pol1
esr(config-ike-gw)# local address 198.51.100.1
esr(config-ike-gw)# local network 10.0.0.0/16
esr(config-ike-gw)# remote address 203.0.113.1
esr(config-ike-gw)# remote network 192.0.2.0/24
esr(config-ike-gw)# local id dns r1.company.loc
esr(config-ike-gw)# remote id dns r2.company.loc
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

Создадим набор алгоритмов для IPsec-туннеля. В нем 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 ранее описанный набор алгоритмов для IPsec-туннеля.

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

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

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

2) Конфигурирование R2

Настроим IP-адрес на внешнем сетевом интерфейсе:

```
esr# configure
esr(config)# interface gi 1/0/1
esr(config-if)# ip address 203.0.113.1/24
esr(config-if)# exit
```

Произведем настройку настройку PKI-клиента. Необходимо заполнить отличительное имя, URL для подключения к PKI-серверу (в случае маршрутизатора R2 – внешний IP-адрес маршрутизатора R1), ранее полученный цифровой отпечаток сертификата PKI-сервера и доменное имя маршрутизатора в качестве альтернативного имени клиентского сертификата:

```
esr(config)# crypto pki trustpoint TP_R2
esr(config-trustpoint)# subject-name
esr(config-trustpoint-subject-name)# country RU
esr(config-trustpoint-subject-name)# state Moscow
esr(config-trustpoint-subject-name)# locality Moscow
esr(config-trustpoint-subject-name)# organization Company
esr(config-trustpoint-subject-name)# common-name r2.company.loc
esr(config-trustpoint-subject-name)# exit
esr(config-trustpoint)# subject-alt-name
esr(config-trustpoint-san)# dns r2.company.loc
esr(config-trustpoint-san)# exit
esr(config-trustpoint)# url http://198.51.100.1/
esr(config-trustpoint)# fingerprint 79:D2:B6:7E:DF:77:2D:C5:27:68:99:10:BA:EC:D2:47
esr(config-trustpoint)# challenge-password password
esr(config-trustpoint)# enable
esr(config-trustpoint)# exit
esr(config)#
```

Перейдем к настройке VPN.

Создадим набор алгоритмов для протокола IKE. В наборе 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 указываем ранее созданный набор алгоритмов, в качестве метода аутентификации выбираем «trustpoint» и в команде **crypto trustpoint** указываем имя ранее созданного PKI-клиента, выписываемые им сертификаты будут использованы при аутентификации IKE-сессии:

```
esr(config)# security ike policy ike_pol1
esr(config-ike-policy)# proposal ike_prop1
esr(config-ike-policy)# authentication method trustpoint
esr(config-ike-policy)# crypto trustpoint TP_R2
esr(config-ike-policy)# exit
```

Создадим шлюз протокола IKE. В данном разделе привяжем ранее созданную политику протокола IKE, укажем IP-адреса для построения IPsec туннеля и набор локальных и удаленных сетей, трафик между которыми необходимо будет шифровать. Также укажем версию протокола IKE и «policy-based» в качестве режима перенаправления трафика в туннель:

⚠ Важным моментом при настройке аутентификации по сертификатам X.509 является указание корректных «local id» и «remote id», присутствующих в сертификатах в качестве альтернативных имен сертификата. Поскольку ранее в настройках PKI-клиента в качестве альтернативного имени было указано полное доменное имя маршрутизатора – укажем его и в командах **local id** и **remote id**.

```
esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# ike-policy ike_pol1
esr(config-ike-gw)# remote address 198.51.100.1
esr(config-ike-gw)# remote network 10.0.0.0/16
esr(config-ike-gw)# local address 203.0.113.1
esr(config-ike-gw)# local network 192.0.2.0/24
esr(config-ike-gw)# local id dns r2.company.loc
esr(config-ike-gw)# remote id dns r1.company.loc
esr(config-ike-gw)# mode policy-based
esr(config-ike-gw)# exit
```

Создадим набор алгоритмов для IPsec-туннеля. В нем 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 ранее описанный набор алгоритмов для IPsec-туннеля.

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

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

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

Состояние туннеля можно посмотреть командой:

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

Конфигурацию туннеля можно посмотреть командой:

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

Состояние PKI-клиента и время следующей процедуры автоматического перевыпуска сертификата можно посмотреть командой:

```
esr# show crypto pki trustpoint TP_R1
```

8.4.6 Алгоритм настройки Remote Access IPsec VPN

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

Дополнительной особенностью RA IPsec VPN является возможность использования двухфакторной аутентификации IPsec, где первым фактором аутентификации является Extended Authentication (XAUTH)

или Extensible Authentication Protocol (EAP), а вторым фактором аутентификации является пара логин-пароль для клиента IPsec VPN.

Шаг	Описание	Команда	Ключи
1	Создать IKE-экземпляр и перейти в режим его конфигурирования.	**esr(config)# security ike proposal <NAME>**	<NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа.
2	Указать описание конфигурируемого туннеля (необязательно).	**esr(config-ike-proposal)# description <DESCRIPTION>**	<DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов.
3	Определить алгоритм аутентификации для IKE (необязательно).	**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 (необязательно).	**esr(config-vti)# ip address <ADDR/LEN> [unit <ID>]** или **esr(config-vti)# ip address <ADDR/LEN> secondary [unit <ID>]**	<ADDR/LEN> – IP-адрес и префикс подсети задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..31]; <ID> – номер юнита, принимает значения [1..4]. Ключ secondary указывает, что настроенный адрес является дополнительным IP-адресом. Если это ключевое слово отсутствует, настроенный адрес является основным IP-адресом. Возможно указать до 7 дополнительных IP-адресов.
5	Определить номер группы Диффи-Хэллмана (необязательно).	**esr(config-ike-proposal)# dh-group <DH-GROUP>**	<DH-GROUP> – номер группы Диффи-Хэллмана, принимает значения [1, 2, 5, 14, 15, 16, 17, 18]. Значение по умолчанию: 1.
6	Создать политику для профиля IKE и перейти в режим её конфигурирования.	**esr(config)# security ike policy <NAME>**	<NAME> – имя политики IKE, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
7	Определить режим аутентификации.	**esr(config-ike- policy)# authentication method <METHOD>**	<METHOD> – метод аутентификации ключа. Может принимать значения: • **xauth - psk - key** – метод двухфакторной аутентификации, использующий пару логин-пароль и предварительно полученные ключи шифрования; • **eap** - метод двухфакторной аутентификации, использующий пару логин-пароль и предварительно полученные сертификаты.
8	Задать режим клиента (только для клиента).	**esr(config-ike- policy)# authentication mode client**	
9	Задать время жизни соединения протокола IKE (необязательно).	**esr(config-ike- policy)# lifetime seconds <SEC>**	<SEC> – период времени, принимает значения [4 ..86400] секунд. Значение по умолчанию: 3600.
10	Отключить реаутентификацию IKE сессии (необязательно).	**esr(config-ipsec-policy)# reauthentication disable**	
11	Привязать политику к профилю.	**esr(config-ike-policy)# proposal <NAME>**	<NAME> – имя профиля протокола IKE, задаётся строкой до 31 символа.
12	Указать ключ аутентификации.	**esr(config-ike-policy)#pre-shared-key ascii-text <TEXT>**	<TEXT> – строка [1..64] ASCII символов.

Шаг	Описание	Команда	Ключи
13	Указать сертификаты и ключи (только для метода EAP)	**esr-10(config-ike-policy)# crypto <CERTEFICATE-TYPE> <NAME>**	<CERTIFICATE-TYPE> – тип сертификата или ключа, может принимать следующие значения: • **ca** – сертификат удостоверяющего сервера; • **crl** – список отозванных сертификатов; • **local-crt** – публичный сертификат сервера удалённого доступа; • **local-crt-key** – приватный ключ сервера удалённого доступа. <NAME> – имя сертификата или ключа, задаётся строкой до 31 символа. На стороне сервера необходимо добавить набор сертификатов (ca, local-crt, local-key). На стороне клиента необходимо указать только корневой сертификат (ca).
14	Создать профиль доступа.	**esr(config)# access profile <NAME>**	<NAME> – имя профиля доступа, задаётся строкой до 31 символа.
15	Создать имя пользователя.	**esr(config-access-profile)# user <LOGIN>**	<LOGIN> – логин клиента, задаётся строкой до 31 символа.
16	Задать пароль пользователя.	**esr(config-profile)# password ascii-text <TEXT>**	<TEXT> – строка [8..32] ASCII символов.
17	Создать пул адресов назначения (только для сервера).	**esr(config)# address-assignment pool <NAME>**	<NAME> – имя пула адресов назначения, задаётся строкой до 31 символа.
18	Задать подсеть, из которой будут выдаваться IP клиентам (только для сервера).	**esr(config-pool)# ip prefix <ADDR/LEN>**	<ADDR/LEN> – адрес подсети и префикс.
19	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.

Шаг	Описание	Команда	Ключи
20	Привязать политику IKE.	**esr(config-ike-gw)# ike-policy <NAME>**	<NAME> – имя политики протокола IKE, задаётся строкой до 31 символа.
21	Установить режим перенаправления трафика в туннель.	**esr(config-ike-gw)# mode <MODE>**	<MODE> – режим перенаправления трафика в туннель, принимает значения: • **policy - based** – трафик перенаправляется на основе принадлежности к указанным в политиках подсетям.
22	Указать действие для DPD (необязательно).	**esr(config-ike-gw)# dead-peer-detection action <MODE>**	<MODE> – режим работы DPD: • **restart** – соединение переустанавливается; • **clear** – соединение останавливается; • **hold** – соединение поддерживается; • **none** – механизм выключен, никаких действий не предпринимается. Значение по умолчанию: none.
23	Указать интервал между отправкой сообщений механизмом DPD (необязательно).	**esr(config-ike-gw)#dead-peer-detection interval <SEC>**	<SEC> – интервал между отправкой сообщений механизмом DPD, принимает значения [1..180] секунд. Значение по умолчанию: 2.
24	Указать период времени ожидания ответа на сообщения механизма DPD (необязательно).	**esr(config-ike-gw)# dead-peer-detection timeout <SEC>**	<SEC> – период времени ожидания ответа на сообщения механизма DPD принимает значения [1..180] секунд. Значение по умолчанию: 30 секунд.
25	Указать базовый период времени ожидания ответа на сообщения (необязательно).	**esr(config-ike-gw)# retransmit timeout <SEC>**	<SEC> – базовый период времени ожидания ответа на сообщения принимает значения [1..30] секунд. Значение по умолчанию: 4 секунды.

Шаг	Описание	Команда	Ключи
26	Указать количество попыток повторной отправки сообщений после наступления таймаута ожидания ответа (необязательно).	**esr(config-ike-gw)# retransmit tries <TRIES>**	<TRIES> – количество попыток повторной отправки сообщений в случае наступления таймаута ожидания ответа принимает значения от 1 до 10. Для первого отправленного сообщения период времени ожидания ответа будет равен базовому периоду, указанному в команде **retransmit timeout**, а для последующих попыток интервал ожидания будет рассчитан по формуле: "retransmit timeout" * 1.8 ^ (N-1), где N - номер попытки. Значение по умолчанию: 5 попыток.
27	Указать уровень случайного разброса периода ожидания ответа на сообщения (необязательно).	**esr(config-ike-gw)# retransmit jitter <VALUE>**	<VALUE> – максимальный процент разброса значений, принимает значения [0..100]. Значение по умолчанию: 0 %
28	Указать ограничение максимального периода времени ожидания ответа на сообщения (необязательно).	**esr(config-ike-gw)# retransmit limit <SEC>**	<SEC> – максимальный период времени ожидания ответа на сообщения принимает значения [15..300] секунд. Значение по умолчанию: 0 секунд, у периода нет верхнего предела.
29	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.
30	Задать режим динамического установления удаленной подсети (только для клиента).	**esr(config-ike-gw)# remote network dynamic client**	
31	Задать профиль доступа (только для сервера).	**esr(config-ike-gw)# access-profile <NAME>**	<NAME> – имя профиля доступа, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
32	Задать профиль доступа и логин (только для клиента).	**esr(config-ike-gw)# access-profile <NAME> client <LOGIN>**	<NAME> – имя профиля доступа, задаётся строкой до 31 символа; <LOGIN> – логин клиента, задаётся строкой до 31 символа.
33	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].
34	Создать профиль IPsec.	**esr(config)# security ipsec proposal <NAME>**	<NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа.
35	Определить алгоритм аутентификации для IPsec (необязательно).	**esr(config-ipsec-proposal)# authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм аутентификации, принимает значения: md5, sha1, sha2-256, sha2-384, sha2-512. Значение по умолчанию: sha1.
36	Определить алгоритм шифрования для IPsec (необязательно).	**esr(config-ipsec-proposal)# encryption algorithm <ALGORITHM>**	<ALGORITHM> – протокол шифрования, принимает значения: des, 3des, blowfish128, blowfish192, blowfish256, aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, camellia128, camellia192, camellia256. Значение по умолчанию: 3des.
37	Указать протокол (необязательно).	**esr(config-ipsec-proposal)#protocol <PROTOCOL>**	<PROTOCOL> – инкапсулирующий протокол, принимает значения: • ah – данный протокол осуществляет только аутентификацию трафика, шифрование данных не выполняется; • esp – данный протокол осуществляет аутентификацию и шифрование трафика. Значение по умолчанию: esp.

Шаг	Описание	Команда	Ключи
38	Задать config-ipsec-proposal конфигурирования.	**esr(config)# security ipsec policy <NAME>**	<NAME> – имя политики IPsec, задаётся строкой до 31 символа.
39	Привязать политику к профилю.	**esr(config-ipsec-policy)# proposal <NAME>**	<NAME> – имя профиля протокола IPsec, задаётся строкой до 31 символа.
40	Задать время жизни IPsec-туннеля (необязательно).	**esr(config-ipsec-policy)# lifetime { seconds <SEC> | packets <PACKETS> | kilobytes <KB> }**	<SEC> – период времени жизни IPsec-туннеля, по истечении которого происходит пересогласование. Принимает значения [1140..86400] секунд. Значение по умолчанию: 540. <PACKETS> – количество пакетов, после передачи которых происходит пересогласование IPsec-туннеля. Принимает значения [4..86400]. Значение по умолчанию: отключено. <KB> – объем трафика, после передачи которого происходит пересогласование IPsec-туннеля. Принимает значения [4..4608000] секунд. Значение по умолчанию: отключено.
41	Создать IPsec VPN и перейти в режим конфигурирования.	**esr(config)# security ipsec vpn <NAME>**	<NAME> – имя VPN, задаётся строкой до 31 символа.
42	Определить режим согласования данных, необходимых для активации VPN.	**esr(config-ipsec-vpn)# mode <MODE>**	<MODE> – режим работы VPN, принимает значения: ike, manual.
43	Привязать IPsec политику к VPN.	**esr(config-ipsec-vpn)#ike ipsec-policy <NAME>**	<NAME> – имя IPsec-политики, задаётся строка до 31 символа.

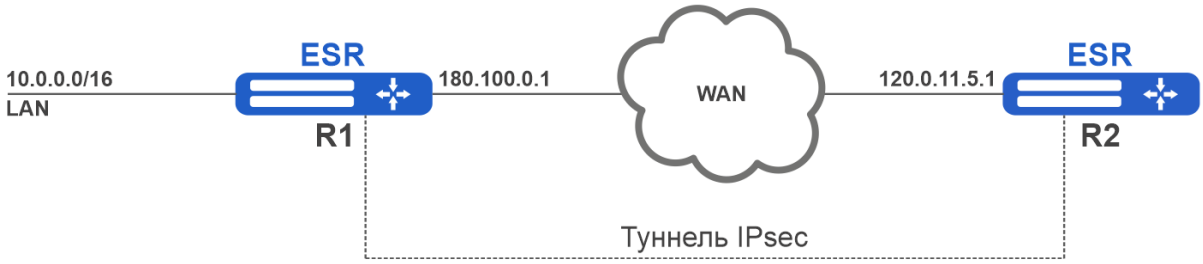
Шаг	Описание	Команда	Ключи
44	Задать значение DSCP для использования в IP-заголовке исходящих пакетов IKE-протокола (необязательно).	**esr(config-ipsec-vpn)#ike dscp <DSCP>**	DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 63.
45	Устанавливается режим активации VPN.	**esr(config-ipsec-vpn)#ike establish-tunnel <MODE>**	<MODE> – режим активации VPN: • **by - request** – соединение активируется встречной стороной, доступно для сервера; • **route** – соединение активируется при появлении трафика, маршрутизируемого в туннель, доступно для сервера; • **immediate** – туннель активируется автоматически после применения конфигурации, доступно для клиента.
46	Осуществить привязку IKE-шлюза к VPN.	**esr(config-ipsec-vpn)# ike gateway <NAME>**	<NAME> – имя IKE-шлюза, задаётся строкой до 31 символа.
47	Установить значение временного интервала в секундах, по истечению которого соединение закрывается, если не было принято или передано ни одного пакета через SA (необязательно).	**esr(config-ipsec-vpn)# ike idle-time <TIME>**	<TIME> – интервал в секундах, принимает значения [4..86400]. Значение по умолчанию: 0.
48	Отключить пересогласование ключей до разрыва IKE-соединения по истечению времени, количеству переданных пакетов или байт (необязательно).	**esr(config-ipsec-vpn)#ike rekey disable**	Значение по умолчанию: включено.

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

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

8.4.7 Пример настройки Remote Access IPsec VPN

Задача:



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

R2 IP-адрес – 120.11.5.1;

R1 IP-адрес – 180.100.0.1;

Клиентам IPsec VPN:

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

IKE:

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

IPsec:

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

XAUTH:

- логин: client1;
- пароль: password123.

Решение:

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

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

```
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)# access-profile XAUTH
esr(config-ike-gw)# exit
```

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

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

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

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

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

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

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

```
esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol udp
esr(config-zone-pair-rule)# match destination-port object-group 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)# access-profile xauth client client1
esr(config-ike-gw)# exit
```

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

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

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

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

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

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

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

```
esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol udp
esr(config-zone-pair-rule)# match destination-port object-group 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:

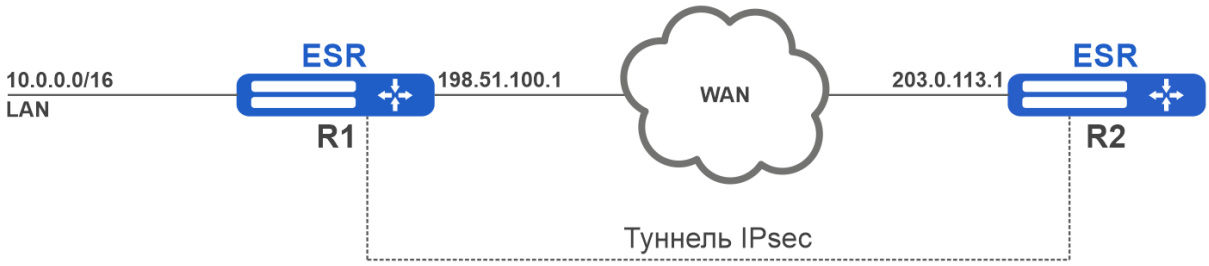
```
esr# show security ipsec vpn status IPSECVPN
```

Конфигурацию туннеля можно посмотреть командой:

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

8.4.8 Пример настройки DPD (Dead Peer Detection)

Задача:



Настроить Dead Peed Detection на R1 для Policy-based Ipsec VPN между R1 и R2.

Исходную конфигурацию можно взять из примера настройки Policy-based IPsec VPN.

Решение:

На R1 в шлюзе протокола IKE укажем: режим работы DPD – restart, интервал опроса – 1 секунду, таймаут – 4 секунды:

```
esr# configure
esr(config)# security ike gateway ike_gw1
esr(config-ike-gw)# dead-peer-detection action restart
esr(config-ike-gw)# dead-peer-detection interval 1
esr(config-ike-gw)# dead-peer-detection timeout 4
esr(config-ike-gw)# exit
```

Состояние туннеля можно посмотреть командой:

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

Конфигурацию туннеля можно посмотреть командой:

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

После разрыва соединения между R1 и R2 на R1 IPsec-туннель начнет перестраиваться спустя 4 секунды после разрыва.

```
esr# show security ipsec vpn status
Name                              Local host        Remote host       Initiator spi
Responder spi        State
-------------------------------   ---------------   ---------------   ------------------
------------------   -----------
ipsec1                            198.51.100.1      203.0.113.1       0x7a77a25a55853255
0xb62fd04f2db43d08   Established
2037-10-30T07:52:53+00:00 %CLI-I-CMD: user admin from console  input: show security ipsec vpn
status
esr# show security ipsec vpn status
Name                              Local host        Remote host       Initiator spi
Responder spi        State
-------------------------------   ---------------   ---------------   ------------------
------------------   -----------
ipsec1                            198.51.100.1      203.0.113.1       0x77706e37b4e68cce
0x0000000000000000   Connecting
2037-10-30T07:52:57+00:00 %CLI-I-CMD: user admin from console  input: show security ipsec vpn
status
```

8.5 Настройка LT-туннелей

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

8.5.1 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 (необязательно).	**esr(config-lt)# description <DESCRIPTION>**	<DESCRIPTION> – описание туннеля, задаётся строкой до 255 символов.
3	Включить каждый LT-туннель в соответствующий VFR.	**esr(config-lt)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.
4	Включить каждый LT-туннель в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall для LT-туннеля.	**esr(config-lt)# security-zone<NAME>**	<NAME> – имя зоны безопасности, задаётся строкой до 12 символов.
		esr(config-lt)# ip firewall disable	
5	Для каждого LT-туннеля задать номер противоположный LT туннель (в другом VRF).	**esr(config-lt)# peer lt <ID>**	<ID> – идентификатор туннеля в диапазоне [1..128].

Шаг	Описание	Команда	Ключи
6	Для каждого LT-туннеля указать IP-адрес для маршрутизации пакетов. Для взаимодействующих LT-туннелей, IP-адреса должны быть из одной IP-подсети.	**esr(config-lt)# ip address <ADDR/LEN> [unit <ID>]** или **esr(config-lt)# ip address <ADDR/LEN> secondary [unit <ID>]**	<ADDR/LEN> – IP-адрес и префикс подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]; <ID> – номер юнита, принимает значения [1..4]. Ключ secondary указывает, что настроенный адрес является дополнительным IP-адресом. Если это ключевое слово отсутствует, настроенный адрес является основным IP-адресом. Возможно указать до 7 дополнительных IP-адресов.
7	Включить туннели.	**esr(config-lt)# enable**	
8	Для каждого VRF настроить необходимые протоколы маршрутизации через LT-туннель.		
9	Задать интервал времени, за который усредняется статистика о нагрузке на туннеле (необязательно).	**esr(config-lt)# load-average <TIME>**	<TIME> – интервал в секундах, принимает значения [5..150]. Значение по умолчанию: 5.
10	Указать размер MTU (Maximum Transmition Unit) пакетов, которые может пропускать данный bridge (необязательно; возможно, если в bridge включен только VLAN). MTU более 1500 будет активно только в случае применения команды "system jumbo-frames".	**esr(config-lt)# mtu <MTU>**	<MTU> – значение MTU, принимает значения в диапазоне: • для ESR-10/12V(F)/15/15R/15VF – [1280..9600]; • для ESR-20/21/30/31 – [1280..9500]; • для ESR-100/200/1000/1200/1500/1511 (rev.B)/1700/3100/3150/3200/3200L/3250/3300/3350 – [1280..10000]. Значение по умолчанию: 1500.

8.5.2 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
```

9 Управление функциями второго уровня (L2)

- Настройка физического интерфейса
  - Алгоритм настройки
  - Пример настройки режима L2
- Настройка VLAN
  - Алгоритм настройки
  - Удаление и назначение VLAN
  - Пример настройки 1
  - Пример настройки 2
  - Разрешение обработки VLAN в тегированном и нетегированном режимах
  - Пример настройки 1
  - Пример настройки 2
  - Пример настройки Private Vlan
- Настройка LLDP
  - Алгоритм настройки
  - Пример настройки
- Настройка LLDP MED
  - Алгоритм настройки
  - Пример настройки Voice VLAN
- Настройка протоколов семейства STP
  - Настройка протоколов STP и RSTP
    - Алгоритм настройки
    - Пример настройки
  - Настройка протокола STP и RSTP в рамках bridge
    - Алгоритм настройки
    - Пример настройки
  - Настройка протокола MSTP
    - Алгоритм настройки
    - Пример настройки
  - Настройка BPDU Guard
    - Алгоритм настройки
    - Пример настройки
- Настройка Bridge
  - Алгоритм настройки
  - Пример настройки bridge для VLAN и L2TPv3-туннеля
  - Пример настройки bridge для VLAN
  - Пример настройки добавления/удаления второго VLAN-тега
- Настройка Dual-Homing
  - Алгоритм настройки
  - Пример настройки
- Настройка зеркалирования (SPAN/RSPAN)
  - Алгоритм настройки
  - Пример настройки
- Настройка LACP
  - Алгоритм настройки
  - Пример настройки

9.1 Настройка физического интерфейса

9.1.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Переход в режим конфигурирования функционала.	**esr(config)# interface gigabitethernet** **esr(config)# interface tengigabitethernet** **esr(config)# interface fourtygigabitethernet** **esr(config)# interface twentyfivegigabitethernet** **esr(config)# interface port-channel { <ID> | <UNIT>/<ID> }**	<UNIT> – номер устройства в группе устройств [1..4]. <ID> – порядковый номер группы агрегации каналов, принимает значения [1..12].
2	Выключить интерфейс.	**esr(config-if-gi)# shutdown**	
3	Задать описание (необязательно).	**esr(config-if-gi)# description <text>**	<text> – до 255 символов.
4	Задать MTU (необязательно).	**esr(config-if-gi)# mtu <count>**	<count> – 552–10000. Значение по умолчанию: 1500.
5	Задать скорость и режим работы приемопередатчика (необязательно).	**esr(config-if-gi)# speed <SPEED> <DUPLEX>**	<SPEED> – значение скорости: • 10M – значение скорости 10 Мбит/с; • 100M – значение скорости 100 Мбит/с; • 1000M – значение скорости 1000 Мбит/с; • 10G – значение скорости 10 Гбит/с; • auto – автоматический выбор режима (недоступно для 10G-интерфейсов). Значение по умолчанию: auto. <DUPLEX> – режим работы приемопередатчика, принимает значения: • full-duplex – дуплекс; • half-duplex – полудуплекс.
6	Задать MAC-адрес (необязательно).	**esr(config-if-gi)# mac-address <ADDR>**	<ADDR> – MAC-адрес сетевого моста, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF].

На данном этапе нет необходимости в настройке firewall.

9.1.2 Пример настройки режима L2

Задача:

Настроить интерфейс gigabitethernet 1/0/1 на прохождение трафика следующим образом:

- Задать MAC-address 68:13:e2:7e:e4:9a;
- Перевести интерфейс в режим Switchport;
- Установить значение MTU=1400;
- Перевести интерфейс в режим работы Full-duplex на скорости 10M.



Решение:

Перейдём в режим конфигурирования интерфейса gigabitethernet 1/0/1 и зададим на нём MAC-address 68:13:e2:7e:e4:9a:

```
esr# configure
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# mac-address 68:13:e2:7e:e4:9a
```

Переведём интерфейс в режим swithcport:

```
esr(config-if-gi)# mode switchport
```

Установим значение MTU на интерфейсе, равное 1400:

```
esr(config-if-gi)# mtu 1400
```

Установим на интерфейсе скорость 10M и согласуем режим работы приемопередатчика в полном дуплексе. Выйдем из режима конфигурирования, применим и сохраним настройки:

```
esr(config-if-gi)# speed 10m full-duplex
esr(config-if-gi)# end
esr# commit
esr# confirm
```

Проверим настроенные параметры на интерфейсе:

```
esr# show interfaces switch-port status gigabitethernet 1/0/1
Interface       gigabitethernet 1/0/1
  Status:       Up
  Media:        copper
  Speed:        10M
  Duplex:       full
  Flow Control: Disabled
  MDI Mode:     MDI
```

9.2 Настройка VLAN

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

9.2.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать VLAN.	**esr(config)# vlan <VID>**	<VID> – идентификатор VLAN, задаётся в диапазоне [2..4094]. Также есть возможность создания нескольких vlan (через запятую), диапазона vlan (через дефис или комбинированную запись, содержащую запятые и дефисы).
2	Задать имя vlan (необязательно).	**esr(config-vlan)# name <vlan-name>**	<vlan-name> – до 255 символов.
3	Отключить отслеживание состояния интерфейсов, на которых разрешена обработка Ethernet-фреймов данного VLAN (необязательно).	**esr(config-vlan)# force-up**	
4	Установить режим работы физического интерфейса.	**esr(config-if-gi)# mode switchport**	Допустимо для всех ESR.
		esr(config-if-gi)# mode hybrid	Допустимо только для ESR-1000/1200/1500/1511 (rev.B)/1700.

Шаг	Описание	Команда	Ключи
5	Отключить обработку входящих нетегированных Ethernet-фреймов на основе таблицы коммутации VLAN-а по умолчанию (VLAN-ID – 1) (необязательно).	**esr(config-if-gi)# switchport forbidden default-vlan**	
6	Задать режим работы L2-интерфейса.	**esr(config-if-gi)# switchport mode access**	Только для ESR-10/12V(F)/ 15/15R/15VF/20/21/30/31/ 100/200/3100/3150/3200/ 3200L/3250/3300/3350. Данный режим является режимом по умолчанию и не отображается в конфигурации.
		esr(config-if-gi)# switchport mode trunk	Только для ESR-10/12V(F)/ 15/15R/15VF/20/21/30/31/ 100/200/3100/3150/3200/ 3200L/3250/3300/3350.
		esr(config-if-gi)# switchport mode general	Только для ESR-1000/1200/1500/1511 (rev.B)/1700. Данный режим является режимом по умолчанию и не отображается в конфигурации.
7	Настроить список VLAN на интерфейсе.	**esr(config-if-gi)# switchport trunk allowed vlan <ACT> <VID>**	Для ESR-10/12V(F)/15/ 15R/15VF/20/21/30/31/ 100/200/3100/3150/3200/ 3200L/3250/3300/3350. <ACT> – назначаемое действие: **add** – включение интерфейса во VLAN; **remove** – исключение интерфейса из VLAN. <VID> – идентификационный номер VLAN, задаётся в диапазоне [2…4094]. Можно задать диапазоном через «-» или перечислением через «,».

Шаг	Описание	Команда	Ключи
		esr(config-if-gi)# switchport general allowed vlan <ACT> <VID> [<TYPE>]	Для ESR-1000/1200/1500/1511 (rev.B)/1700. <ACT> – назначаемое действие: **add** – включение интерфейса во VLAN; **remove** – исключение интерфейса из VLAN. <VID> – идентификационный номер VLAN, задаётся в диапазоне [2…4094]. Можно задать диапазоном через «-» или перечислением через «,»; <TYPE> – тип пакета: **tagged** – интерфейс будет передавать и принимать пакеты в указанных VLAN тегированными; **untagged** – интерфейс будет передавать пакеты в указанных VLAN нетегированными. VLAN, в которую будут направлены входящие нетегированные пакеты, настраивается командой switchport general pvid.
8	Настроить VLAN в качестве Default VLAN на данном интерфейсе для нетегированного трафика, поступающего на данный порт.	**esr(config-if-gi)# switchport trunk native-vlan <VID>**	Для ESR-10/12V(F)/15/15R/15VF/20/21/30/31/100/200/3100/3150/3200/3200L/3250/3300/3350. <VID> – идентификатор VLAN, задаётся в диапазоне [2..4094].
9	Установить идентификатор VLAN-порта (PVID) для входящего нетегированного трафика (необязательно).	**esr(config-if-gi)# switchport general pvid <VID>**	Для ESR-1000/1200/1500/1511 (rev.B)/1700. <VID> – идентификационный номер VLAN, задаётся в диапазоне [1…4094].
10	Разрешить на интерфейсе обработку Ethernet-фреймов всех созданных на маршрутизаторе VLAN (необязательно).	**esr(config-if-gi)# switchport trunk allowed vlan auto-all**	Только для ESR-10/12V(F)/15/15R/15VF/20/21/30/31/100/200/3100/3150/3200/3200L/3250/3300/3350.

Шаг	Описание	Команда	Ключи
		esr(config-if-gi)# switchport general allowed vlan auto-all	Только для ESR-1000/1200/1500/1511/1700.
11	Перевести интерфейс в режим изоляции по группам (необязательно).	**esr(config-if-gi)# switchport protected-port**	
12	Добавить интерфейс в группу изоляции (необязательно). Данная команда актуальна, только если порт находится в режиме изоляции по группам.	**esr(config-if-gi)# switchport community**	<ID> – идентификатор группы, принимает значение в диапазоне [1...30].
13	Включить функцию Private VLAN на интерфейсе (необязательно).	**esr(config-if-gi)# switchport protected**	<IF> – интерфейс, задается в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора.

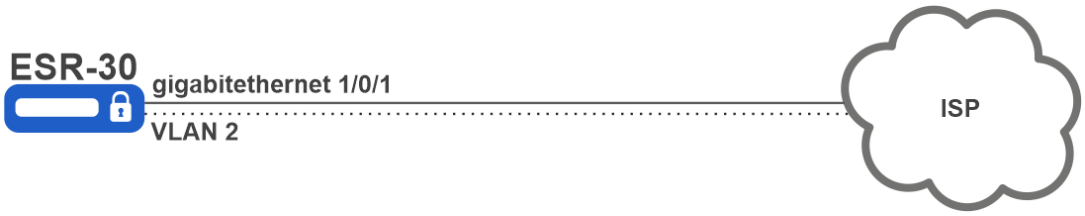
9.2.2 Удаление и назначение VLAN

9.2.3 Пример настройки 1

Данный пример предназначен для использования при конфигурировании VLAN на устройствах ESR-10/12V(F)/15/15R/15VF/20/21/30/31/100/200/3100/3150/3200/3200L/3250/3300/3350.

Задача:

На основе заводской конфигурации для ESR-30 удалить из VLAN 2 порт gigabitethernet 1/0/1 и назначить его на интерфейс gigabitethernet 1/0/2 в нетегированном режиме.



Решение:

Перейдём в режим настройки интерфейса gigabitethernet 1/0/1 и удалим его из VLAN 2:

```
esr# configure
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# no switchport access vlan
esr(config-if-gi)# exit
```

Перейдём в режим настройки интерфейса gigabitethernet 1/0/2 и назначим его в VLAN 2:

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

Применим и сохраним изменения конфигурации:

```
esr(config-if-gi)# end
esr# commit
esr# confirm
```

Проверим, что внесенные изменения вступили в силу, и теперь интерфейс gigabitethernet 1/0/2 принадлежит к VLAN 2 в нетегированном режиме:

```
esr# show vlans 2
VID    Name                  Tagged                 Untagged
----   --------------------  ---------------------  ----------------------
2      --                                           gi1/0/2, te1/0/1-2
```

9.2.4 Пример настройки 2

Данный пример предназначен для использования при конфигурировании VLAN на устройствах ESR-1000/1200/1500/1511/1700.

Задача:

На основе заводской конфигурации для ESR-1000 удалить из VLAN 2 порт gigabitethernet 1/0/1 и назначить его на интерфейс gigabitethernet 1/0/2 в нетегированном режиме.



Решение:

Перейдём в режим настройки интерфейса gigabitethernet 1/0/1 и удалим его из VLAN 2:

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

Перейдём в режим настройки интерфейса gigabitethernet 1/0/2 и назначим его в VLAN 2:

```
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# switchport general allowed vlan add 2 untagged
esr(config-if-gi)# switchport general pvid 2
esr(config-if-gi)# end
```

Применим и сохраним изменения конфигурации:

```
esr(config-if-gi)# end
esr# commit
esr# confirm
```

Проверим, что внесенные изменения вступили в силу, и теперь интерфейс gigabitethernet 1/0/2 принадлежит к VLAN 2 в нетегированном режиме:

```
esr# show vlans 2
VID    Name                    Tagged                  Untagged
----   --------------------    ----------------------  ----------------------
2      --                                              gi1/0/2, te1/0/1-2
```

9.2.5 Разрешение обработки VLAN в тегированном и нетегированном режимах

9.2.6 Пример настройки 1

Данный пример предназначен для использования при конфигурировании VLAN на устройствах ESR-10/12V(F)/15/15R/15VF/20/21/30/31/100/200/3100/3150/3200/3200L/3250/3300/3350.

Задача:

На ESR-15 настроить интерфейс gigabitethernet 1/0/1 в режиме trunk для передачи и приема фреймов в VLAN 2, VLAN 64, VLAN 2000 в тегированном режиме в сторону устройства Switch. Интерфейс gigabitethernet 1/0/2 настроить в режиме access для определения нетегированного трафика от PC в VLAN 2.



Решение:

Создадим VLAN 2, VLAN 64, VLAN 2000:

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

Перейдём в режим настройки интерфейса gigabitethernet 1/0/1. Запретим использование default-vlan (VLAN 1) и настроим его принадлежность к VLAN 2, VLAN 64, VLAN 2000 в тегированном режиме:

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

Перейдём в режим настройки интерфейса gigabitethernet 1/0/2 и определим его к VLAN 2 в режиме работы access:

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

Применим и сохраним изменения конфигурации:

```
esr(config-if-gi)# end
esr# commit
esr# confirm
```

Проверим, что внесенные изменения вступили в силу - теперь интерфейс gigabitethernet 1/0/1 принадлежит к VLAN 2, 64, 2000, настроенным в тегированном режиме, а интерфейс gigabitethernet 1/0/2 принадлежит к VLAN 2 в нетегированном режиме:

```
esr# show vlans
VID    Name                 Tagged                 Untagged
----   -------------------  ---------------------  ---------------------
2      --                   gi1/0/1                gi1/0/2
64     --                   gi1/0/1
2000   --                   gi1/0/1
```

9.2.7 Пример настройки 2

Данный пример предназначен для использования при конфигурировании VLAN на устройствах ESR-1000/1200/1500/1511/1700.

Задача:

На ESR-1000 настроить интерфейс gigabitethernet 1/0/1 в режиме "general" для передачи и приема фреймов в VLAN 2, VLAN 64, VLAN 2000 в тегированном режиме в сторону устройства Switch. Интерфейс gigabitethernet 1/0/2 настроить в этом же режиме, но для определения нетегированного трафика от PC в VLAN 2.



Решение:

Создадим VLAN 2, VLAN 64, VLAN 2000:

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

Перейдём в режим настройки интерфейса gigabitethernet 1/0/1. Запретим использование default-vlan (VLAN 1) и настроим его принадлежность к VLAN 2, VLAN 64, VLAN 2000 в тегированном режиме:

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

Перейдём в режим настройки интерфейса gigabitethernet 1/0/2, запретим использование default-vlan (VLAN 1), укажем Port-VLAN ID (PVID) 2 и определим его к VLAN 2 в нетегированном режиме:

```
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# mode switchport
esr(config-if-gi)# switchport forbidden default-vlan
esr(config-if-gi)# switchport mode general
esr(config-if-gi)# switchport general allowed vlan add 2 untagged
esr(config-if-gi)# switchport general pvid 2
```

Применим и сохраним изменения конфигурации:

```
esr(config-if-gi)# end
esr# commit
esr# confirm
```

Проверим, что внесенные изменения вступили в силу - теперь интерфейс gigabitethernet 1/0/1 принадлежит к VLAN 2, 64, 2000, настроенным в тегированном режиме, а интерфейс gigabitethernet 1/0/2 принадлежит к VLAN 2 в нетегированном режиме:

```
esr# show vlans
VID    Name                    Tagged                  Untagged
----   --------------------    ----------------------  ----------------------
2      --                      gi1/0/1                 gi1/0/2
64     --                      gi1/0/1
2000   --                      gi1/0/1
```

9.2.8 Пример настройки Private Vlan

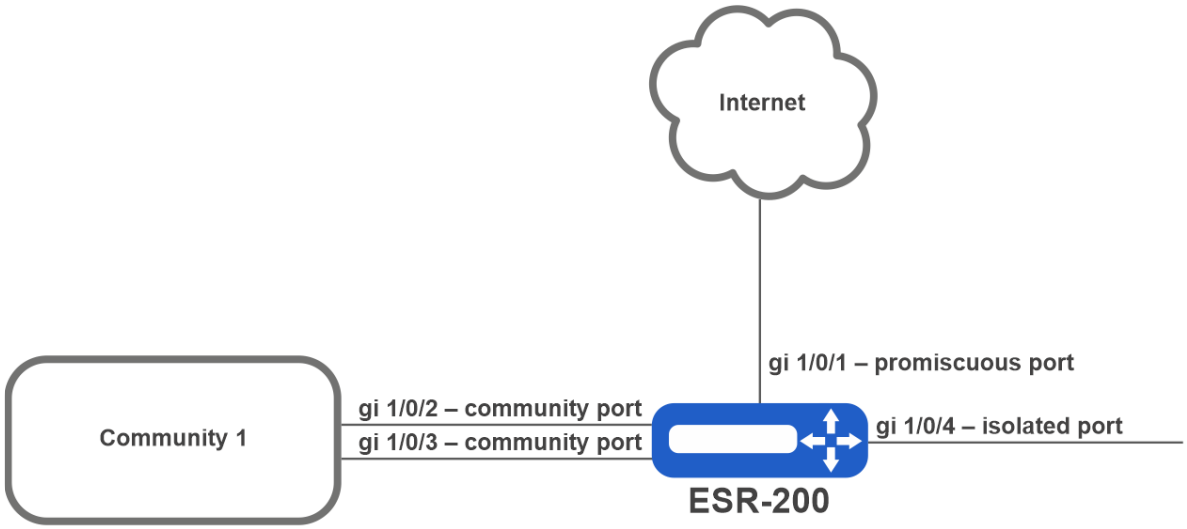
Технология Private VLAN (PVLAN) позволяет производить разграничение трафика на втором уровне модели OSI между портами маршрутизатора, которые находятся в одном широковещательном домене.

На маршрутизаторе может быть сконфигурировано три типа PVLAN-портов:

- promiscuous – это порт, который способен обмениваться данными между любыми интерфейсами, включая isolated- и community-порты PVLAN;
- isolated – это порт, который полностью изолирован от других портов внутри одного и того же PVLAN, но не от promiscuous-портов. PVLAN блокируют весь трафик, идущий в сторону isolated-портов, кроме трафика со стороны promiscuous-портов; пакеты со стороны isolated-портов могут передаваться только в сторону promiscuous-портов;
- community – это группа портов, которые могут обмениваться данными между собой и promiscuous-портами, эти интерфейсы отделены на втором уровне модели OSI от всех остальных community-интерфейсов, а также isolated-портов внутри PVLAN.

Задача:

Настроить изоляцию портов в одном широковещательном домене (PVLAN). Порты gi1/0/2 и gi1/0/3 должны относиться к community 1, порт gi1/0/4 должен быть изолирован в сторону promission port. В качестве promission port выступает gi1/0/1.



Решение:

Создадим VLAN 10:

```
esr(config)# vlan 10
esr(config-vlan)# exit
```

Настроим интерфейс gi1/0/1 в режиме «promiscuous port»:

```
esr(config)# interface gigabitethernet 1/0/1
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 10
esr(config-if-gi)# exit
```

Настроим интерфейсы gi1/0/2, gi1/0/3 в режиме «community port»:

```
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# mode switchport
esr(config-if-gi)# switchport protected-port
esr(config-if-gi)# switchport community 1
esr(config-if-gi)# switchport forbidden default-vlan
esr(config-if-gi)# switchport mode trunk
esr(config-if-gi)# switchport trunk allowed vlan add 10
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/3
esr(config-if-gi)# mode switchport
esr(config-if-gi)# switchport protected-port
esr(config-if-gi)# switchport community 1
esr(config-if-gi)# switchport forbidden default-vlan
esr(config-if-gi)# switchport mode trunk
esr(config-if-gi)# switchport trunk allowed vlan add 10
esr(config-if-gi)# exit
```

Настроим интерфейс gi1/0/4 в режиме «isolated port»:

```
esr(config)# interface gigabitethernet 1/0/4
esr(config-if-gi)# mode switchport
esr(config-if-gi)# switchport protected gigabitethernet 1/0/1
esr(config-if-gi)# switchport forbidden default-vlan
esr(config-if-gi)# switchport mode trunk
esr(config-if-gi)# switchport trunk allowed vlan add 10
esr(config-if-gi)# exit
```

Информацию о состоянии физических интерфейсов в режиме изоляции по группам можно узнать с помощью команды:

```
esr# show interfaces protected-ports
```

9.3 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.

9.3.1 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**	

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

9.3.2 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
```

9.4 Настройка LLDP MED

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

9.4.1 Алгоритм настройки

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

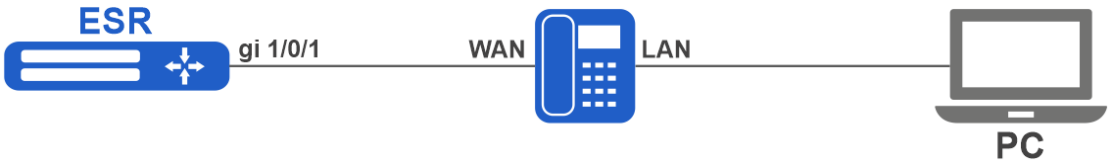
Шаг	Описание	Команда	Ключи
5	Указать тип приложения.	**esr(config-net-policy)# application <APP_TYPE>**	<APP-TYPE> – тип приложения, для которого будет срабатывать network-policy. Принимает значения: • voice; • voice-signaling; • guest-voice; • guest-voice-signaling; • softphone-voice; • video-conferencing;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

9.4.2 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
```

9.5 Настройка протоколов семейства STP

Spanning Tree Protocol – сетевой протокол, основной задачей которого является приведение сети Ethernet с избыточными соединениями к древовидной топологии, исключающей петли. Сетевые устройства обмениваются служебными сообщениями, используя кадры специального формата (BPDU), и выборочно включают/отключают интерфейсы во избежание кольцевых топологий.

Rapid (быстрый) STP (RSTP) – является усовершенствованием протокола STP, характеризуется меньшим временем сходимости за счет использования механизма предложений и соглашений (propolsal/agreement proccess) и улучшенной логикой отправки служебных BPDU-сообщений.

Ниже представлена сводная таблица по поддержке протоколов семейства xSTP.

Устройство	STP/ RSTP		MSTP
	На порту	на бридже	
ESR-10, ESR-12(V/VF), ESR-15(R,VF)	✅	✅	⛔
ESR-100/200, ESR-20/21, ESR-30/31	✅	✅	⛔
ESR-1000	⛔	✅	✅
ESR-1200, ESR-1500/1511, ESR-1700	⛔	✅	⛔
ESR-3100, ESR-3200(L), ESR-3150, ESR-3250, ESR-3300, ESR-3350	✅	✅	⛔

9.5.1 Настройка протоколов STP и RSTP

Для активации протокола необходимо перевести работу интерфейса в L2-режим (mode switchport). По умолчанию используется протокол RSTP со следующими временными параметрами: Hello Time – 2 с, Forward Delay – 15 с, Max Age – 20 с.

Алгоритм настройки

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

Шаг	Описание	Команда	Ключи
4	Установить время, в течение которого будет ожидаться получение BPDU от ROOT-коммутатора (необязательно).	**esr(config)# spanning-tree max-age <TIME>**	<TIME> – время в секундах, принимает значения [6..40]. Значение по умолчанию: 20 секунд.
5	Выбрать тип протокола: STP или RSTP.	**esr(config)# spanning-tree mode <MODE>**	<MODE> – протокол семейства STP: • STP – IEEE 802.1D Spanning Tree Protocol; • RSTP – IEEE 802.1W Rapid Spanning Tree Protocol; Значение по умолчанию: RSTP.
6	Установить метод расчет стоимости пути (необязательно).	**esr(config)# spanning-tree pathcost method <short | long>**	long – значение ценности в диапазоне [1..200000000]; short – значение ценности в диапазоне [1..65535]. Значение по умолчанию: short.
7	Настроить приоритет связующего дерева STP (необязательно).	**esr(config)# spanning-tree priority <PRIORITY>**	<PRIORITY> – приоритет, указывается в диапазоне с шагом 4096 [0..61440]. Значение по умолчанию: 32768.
8	Перевести интерфейс в L2-режим для включения в работу в STP/RSTP.	**esr(config-if-gi)# mo switchport**	
9	Установить стоимость на определенном интерфейсе (необязательно).	**esr(config-if-gi)# spanning-tree cost**	<COST> – стоимость пути, устанавливается в диапазоне [1..20000000]. Значение по умолчанию: 4.
10	Установить тип интерфейса (необязательно).	**esr(config-if-gi)# spanning-tree link-type {point-to-point|shared}**	point-to-point – команда определяет интерфейс как «точка-точка»; shared – команда определяет интерфейс как «разветвленный». Значение по умолчанию: point-to-point.

Шаг	Описание	Команда	Ключи
11	Установить приоритет интерфейса в связующем дереве STP (необязательно).	**esr(config-if-gi)# spanning-tree port-priority <PRIORITY>**	<PRIORITY> – приоритет, указывается в диапазоне с шагом 16 [0..240].

Пример настройки

Задача:

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



Решение:

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

По умолчанию на ESR включен протокол RSTP.

Перейдём в режим конфигурирования:

```
esr-20# configure
```

Зададим протокол по умолчанию STP:

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

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

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

Вывод команды **show spanning-tree bridge global active**:

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

9.5.2 Настройка протокола STP и RSTP в рамках bridge

Работа протоколов STP/RSTP также возможна в рамках выделенного bridge-домена, что дает возможность организовать кольцевую отказоустойчивую топологию в сетях с использование L2-туннелей (сервисы L2TPv3 и Ethernet over GRE), или в сетях, устройства которых не поддерживают работу протоколов семейства xSTP.

Для корректной работы устройства должны поддерживать работу протоколов STP/RSTP в bridge-домене.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим конфигурации bridge-домена для настройки протокола STP/RSTP.	**esr(config)# bridge <BR-NUM>**	<BR-NUM> – номер bridge.
2	Установить интервал времени, затрачиваемый на прослушивание и изучение состояний перед переключением в состояние передачи (необязательно).	**esr(config-bridge)# spanning-tree forward-time <TIME>**	<TIME> – время в секундах, принимает значения [4..30]. Значение по умолчанию: 15 секунд.
3	Установить интервал времени между отправкой BPDU-пакетов (необязательно).	**esr(config-bridge)# spanning-tree hello-time <TIME>**	<TIME> – время в секундах, принимает значения [1..10]. Значение по умолчанию: 2 секунды.

Шаг	Описание	Команда	Ключи
4	Установить время, в течение которого будет ожидаться получение BPDU от ROOT -коммутатора (необязательно).	**esr(config-bridge)# spanning-tree max-age <TIME>**	<TIME> – время в секундах, принимает значения [6..40]. Значение по умолчанию: 20 секунд.
5	Выбрать тип протокола: STP или RSTP.	**esr(config-bridge)# spanning-tree mode <MODE>**	<MODE> – протокол семейства STP: • STP – IEEE 802.1D Spanning Tree Protocol; • RSTP – IEEE 802.1W Rapid Spanning Tree Protocol. Значение по умолчанию: RSTP.
6	Установить метод расчета стоимости пути (необязательно).	**esr(config-bridge)# spanning-tree pathcost method <short | long>**	long – значение ценности в диапазоне [1..200000000]; short – значение ценности в диапазоне [1..65535]. Значение по умолчанию: short.
7	Настроить приоритет бриджа – используется при выборе root бриджа в топологии (необязательно).	**esr(config-bridge)# spanning-tree priority <PRIORITY>**	<PRIORITY> – приоритет, указывается в диапазоне с шагом 4096 [0..61440]. Значение по умолчанию: 32768.
8	Включить бридж в работу с соответствующим интерфейсом.	**esr(config-if-gi)# bridge-group <BR-NUM>**	<BR-NUM> – номер bridge.
9	Установить стоимость на определенном интерфейсе (необязательно).	**esr(config-if-gi)# spanning-tree cost**	<COST> – стоимость пути, устанавливается в диапазоне [1..20000000]. Значение по умолчанию: 4.
10	Установить тип интерфейса (необязательно).	**esr(config-if-gi)# spanning-tree link-type {point-to-point|shared}**	point-to-point – команда определяет интерфейс как «точка-точка»; shared – команда определяет интерфейс как «разветвленный». Значение по умолчанию: point-to-point.

Шаг	Описание	Команда	Ключи
11	Установить приоритет интерфейса в связующем дереве STP (необязательно).	**esr(config-if-gi)# spanning-tree port-priority <PRIORITY>**	<PRIORITY> – приоритет, указывается в диапазоне с шагом 16 [0..240].

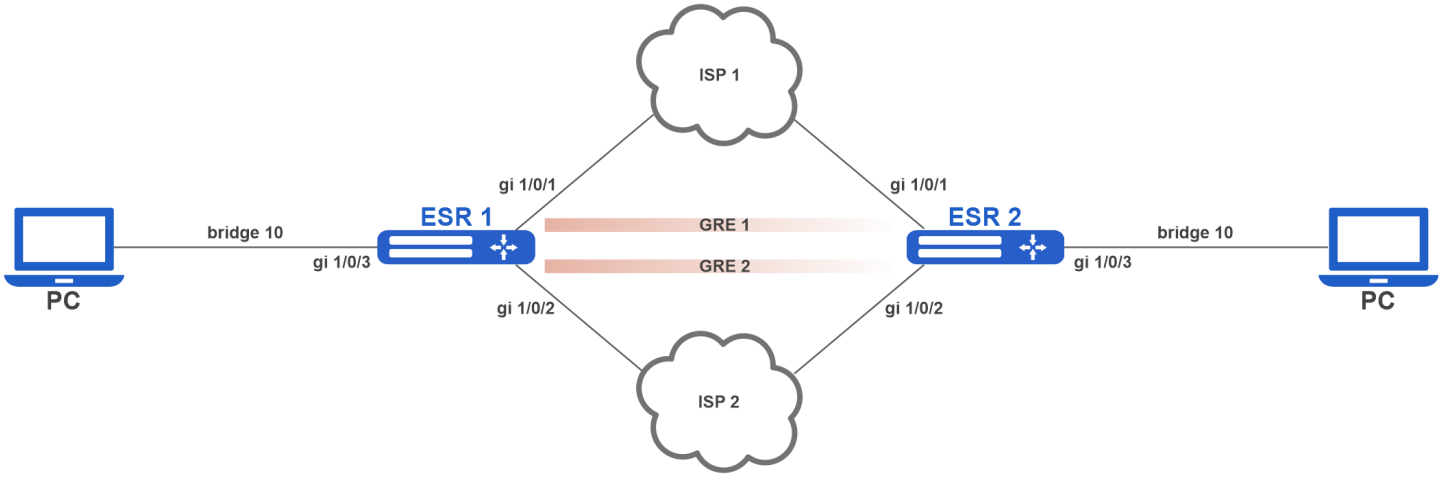
⚠ Для корректной работы STP/RSTP в рамках bridge-домена интерфейсы необходимо добавить в bridge-домен следующим образом:

```
interface gigabitethernet 1/0/3
mode switchport
bridge-group 10
exit
```

Пример настройки

Задача:

С помощью протокола RSTP организовать резервирования сервиса L2VPN, построенного с помощью Ethernet over GRE.



Решение:

Настроим адресацию на ESR1 и ESR2:

```
ESR2(config)# interface gigabitethernet 1/0/1
ESR2(config-if-gi)#   ip firewall disable
ESR2(config-if-gi)#   ip address 198.51.100.2/30
ESR2(config-if-gi)# exit
ESR2(config)# interface gigabitethernet 1/0/2
ESR2(config-if-gi)#   ip firewall disable
ESR2(config-if-gi)#   ip address 198.51.100.6/30
ESR2(config-if-gi)# exit
ESR2(config)# do commit
ESR2(config)# do confirm

ESR1(config)# interface gigabitethernet 1/0/1
ESR1(config-if-gi)#   ip firewall disable
ESR1(config-if-gi)#   ip address 198.51.100.1/30
ESR1(config-if-gi)# exit
ESR1(config)# interface gigabitethernet 1/0/2
ESR1(config-if-gi)#   ip firewall disable
ESR1(config-if-gi)#   ip address 198.51.100.5/30
ESR1(config-if-gi)# exit
ESR1(config)# do commit
ESR1(config)# do confirm
```

Настроим Ethernet over GRE. Определим GRE 1 как основной канал, GRE 2 – резервный:

```
ESR1(config)# bridge 10
ESR1(config-bridge)#   enable
ESR1(config-bridge)# exit
ESR1(config)# tunnel gre 1
ESR1(config-gre)#   mode ethernet
ESR1(config-gre)#   bridge-group 10
ESR1(config-gre)#   local address 198.51.100.1
ESR1(config-gre)#   remote address 198.51.100.2
ESR1(config-gre)#   spanning-tree cost 10
ESR1(config-gre)#   enable
ESR1(config-gre)# exit
ESR1(config)# tunnel gre 2
ESR1(config-gre)#   mode ethernet
ESR1(config-gre)#   bridge-group 10
ESR1(config-gre)#   local address 198.51.100.5
ESR1(config-gre)#   remote address 198.51.100.6
ESR1(config-gre)#   spanning-tree cost 20
ESR1(config-gre)#   enable
ESR1(config-gre)# exit
ESR1(config-if-gi)# do commit
ESR1(config-if-gi)# do confirm

ESR2(config)# bridge 10
ESR2(config-bridge)#   enable
ESR2(config-bridge)# exit
ESR2(config)# tunnel gre 1
ESR2(config-gre)#   mode ethernet
ESR2(config-gre)#   bridge-group 10
ESR2(config-gre)#   local address 198.51.100.2
ESR2(config-gre)#   remote address 198.51.100.1
ESR2(config-gre)#   spanning-tree cost 10
ESR2(config-gre)#   enable
ESR2(config-gre)# exit
ESR2(config)# tunnel gre 2
ESR2(config-gre)#   mode ethernet
ESR2(config-gre)#   bridge-group 10
ESR2(config-gre)#   local address 198.51.100.6
ESR2(config-gre)#   remote address 198.51.100.5
ESR2(config-gre)#   spanning-tree cost 20
ESR2(config-gre)#   enable
ESR2(config-gre)# exit
ESR2(config-if-gi)# do commit
ESR2(config-if-gi)# do confirm
```

Добавим клиентские интерфейсы в соответствующий bridge-домен:

```
ESR1(config)# interface gigabitethernet 1/0/3
ESR1(config-if-gi)# mode switchport
ESR1(config-if-gi)# spanning-tree portfast
ESR1(config-if-gi)# bridge-group 10
ESR1(config-if-gi)# do commit
ESR1(config-if-gi)# do confirm

ESR2(config)# interface gigabitethernet 1/0/3
ESR2(config-if-gi)# mode switchport
ESR2(config-if-gi)# spanning-tree portfast
ESR2(config-if-gi)# bridge-group 10
ESR2(config-if-gi)# do commit
ESR2(config-if-gi)# do confirm
```

Проверим статус туннелей, чтобы убедиться в сходимости протокола RSTP:

```
ESR1# sh tu status
Tunnel              Admin    Link     MTU      Local IP           Remote IP          Last change
                    state    state
-----------------   -----    -----    ------   ----------------   ----------------
-------------------------
gre 1               Up       Up       1500     198.51.100.1       198.51.100.2       4 hours, 24
 minutes and
                                                                                     58 seconds

gre 2               Up       Up       1500     198.51.100.5       198.51.100.6       4 hours, 23
 minutes and 6
                                                                                     seconds

ESR1# sh spanning-tree bridge 10 active
Instance name: bridge 10
    Protocol version: RSTP
    Root ID: [32768] a8:f9:4b:ad:fe:d1
                Root port: [128] gre 1
                Pathcost 10
                Message Age 300
                Hello time: 2 Max age time: 20 Forward delay: 15
    Bridge ID: [32768] e4:5a:d4:01:b7:ec
                Hello time: 2 Max age time: 20 Forward delay: 15
                Transmit hold count: 6 Topology change: 0
                Time since topology change: 1600 Topology change count: 7

Name            State    Prio.Num    Cost         Status      Role        PortFast    Type
------------    -----    --------    ---------    --------    --------    --------
--------------------
gi1/0/3         en       128.5       32768        FRW         Desg        Yes         RSTP
gre 1           en       128.3       10           FRW         Root        No          RSTP
gre 2           en       128.4       20           BLK         Altr        No          RSTP
```

Настройка сервиса завершена.

9.5.3 Настройка протокола MSTP

Протокол Multiple STP является современной реализацией RSTP, ключевой особенностью которой является поддержка VLAN. В MSTP каждый порт может работать с разным количеством VLAN, принадлежащих разным экземплярам (STI). Изменение состояния в одном из инстансов не оказывает влияния на состояние других экземпляров, что позволяет продолжать обработку трафика в случае блокировки одного из STI.

Протокол MSTP поддержан только на ESR-1000.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Выбрать тип протокола MSTP.	**esr(config)# spanning tree mode <MODE>**	<MODE> – протокол семейства STP: • STP – IEEE 802.1D Spanning Tree Protocol; • RSTP – IEEE 802.1W Rapid Spanning Tree Protocol; • MST -IEEE 802.1S Multiple Spanning Tree Protocol. Значение по умолчанию: RSTP.
2	Установить приоритет для соответствующего инстанса перед остальными, использующими общий экземпляр MST (необязательно).	**esr(config)# spanning-tree mst <INSTANCE> priority <PRIORITY>**	<INSTANCE> – номер экземпляра MSTP [1..15]. <PRIORITY> – приоритет, указывается в диапазоне с шагом 4096 [0..61440]. Значение по умолчанию: 32768.
3	Установить максимальное количество транзитных узлов для пакета BPDU, необходимых для формирования дерева (необязательно).	**esr(config)# spanning-tree mst max-hops <NUM>**	<NUM> – количество транзитных узлов, принимает значения [6..40]. Значение по умолчанию: 6.
4	Установить принадлежность экземпляра MST к соответствующей группе VLAN (необязательно).	**esr(config-mst)# instance <INSTANCE> vlan <VLAN>**	<INSTANCE> – номер экземпляра MSTP [1..15]. <VLAN> – номер VLAN.
5	Задать имя конфигурации MST (необязательно).	**esr(config-mst)# name <NAME>**	<NAME> – имя конфигурации MST [1..31].
6	Задать номер ревизии конфигурации MST (необязательно).	**esr(config-bridge)# revision <REVISION>**	<REVISION> – номер ревизии конфигурации MST [0..65535].

Шаг	Описание	Команда	Ключи
7	Установить стоимость интерфейса для соответствующего экземпляра MST.	**esr(config-if-gi)# spanning-tree mst <INSTANCE> cost <COST>**	<INSTANCE> – номер экземпляра MSTP [1..15]. <COST> – стоимость пути, устанавливается в диапазоне [1..20000000]. Значение по умолчанию: 4.
8	Установить приоритет порта для соответствующего интерфейса в экземпляре MST.	**esr(config-if-gi)# spanning-tree mst <INSTANCE> port-priority <PRIORITY>**	<INSTANCE> – номер экземпляра MSTP [1..15]. <PRIORITY> – приоритет, указывается в диапазоне с шагом 16 [0..240].

Пример настройки

Задача:

Настроить протокол MSTP между устройствами для VLAN 100 и VLAN 200, выделив для этого соответствующие инстансы.



Решение:

Создадим на устройствах необходимые VLAN. Настроим порт в режиме General, трафик VLAN100, 200 будет отправляться тегированным:

```
esr(config)# vlan 100
esr(config-vlan)# exit
esr(config)# vlan 200
esr(config-vlan)# exit
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# mo switchport
esr(config-if-gi)# switchport general allowed vlan add 100,200


Switch(config)#vlan 100,200
Switch(config-vlan-range)#vlan active
Switch(config-vlan-range)#exit
Switch(config)#interface gigabitethernet 0/1
Switch(config-if)#switchport general allowed vlan add 100,200
```

Включим протокол MSTP. Настроим инстансы и соответствующие им VLAN.

```
esr(config)# spanning-tree mst configuration
esr(config-mst)# name mst
esr(config-mst)# revision 1
esr(config-mst)# instance 1 vlan 100
esr(config-mst)# instance 2 vlan 200
esr(config-mst)# exit


Switch(config)#spanning-tree  mode mst
Switch(config)#spanning-tree  mst configuration
Switch(config-mst)# name mst
Switch(config-mst)#  revision 1
Switch(config-mst)#  instance 1 vlan 100
Switch(config-mst)#  instance 2 vlan 200
```

Проверим работу протокола MSTP и состояние портов:

```
esr# sh spanning-tree bridge global
###### MST instance 1. Vlans mapped: 100
        Regional Root ID: [32768] A8:F9:4B:AA:39:7B
        This switch is the Regional Root
                        Time since topology change: 0 Topology change: 0
                        Topology change count: 32 Max hops: 20
        Designated bridge ID: [32768] A8:F9:4B:AA:39:7B

###### MST instance 2. Vlans mapped: 200
        Regional Root ID: [8192] A8:F9:4B:AA:39:7B
        This switch is the Regional Root
                        Time since topology change: 0 Topology change: 1
                        Topology change count: 34 Max hops: 20
        Designated bridge ID: [8192] A8:F9:4B:AA:39:7B

esr#   sh spanning-tree gigabitethernet 1/0/1

###### MST 1. Mapped Vlans: 100
        Regional Root ID: [16384] A8:F9:4B:AA:39:7B
        This switch is the Regional Root
Name           State   Prio.Num   Cost        Status     Role       PortFast   Type
------------   -----   --------   ---------   --------   --------   --------
--------------------
gi1/0/1        en      128.2305   4           FRW        Desg       No         P2P Inter

###### MST 2. Mapped Vlans: 200
        Regional Root ID: [8192] A8:F9:4B:AA:39:7B
        This switch is the Regional Root
Name           State   Prio.Num   Cost        Status     Role       PortFast   Type
------------   -----   --------   ---------   --------   --------   --------
--------------------
gi1/0/1        en      128.2305   4           FRW        Desg       No         P2P Inter
```

Настройка протокола MSTP завершена.

9.5.4 Настройка BPDU Guard

BPDU Guard — функция, позволяющая блокировать порт при поступлении BPDU. Это предотвращает случайное или злонамеренное создание петель в сети. Рекомендуется включать BPDU Guard на портах, к которым подключены конечные устройства. Функция может быть использована на физических, sub, q-in-q интерфейсах, а также на port-channel.

⚠ Функция недоступна на устройствах ESR-1000, ESR-1200, ESR-15xx, ESR-1700.

При обнаружении входящего BPDU порт переводится в статус errdisable. В логе появятся соответствующие сообщения:

```
2025-07-01T10:45:48+00:00 %MSTPD-W-BPDUGUARD: Received BPDU on port gigabitethernet 1/0/3 with
BPDU Guard - disabling port
2025-07-01T10:45:48+00:00 %LINK-W-ERRDISABLE: gigabitethernet 1/0/3 changed state to
ErrDisable, cause 'bpduguard'
```

По умолчанию порт не будет пытаться автоматически переходить в состояние "Up". Это можно сделать командой:

```
esr# set interface active gigabitethernet 1/0/3
```

Возможна настройка автоматического восстановления. По умолчанию временной интервал составляет 300 секунд (значение меняется от 30 до 86400 секунд):

```
esr-15r(config)# errdisable recovery cause bpduguard
esr-15r(config)# errdisable recovery interval
  30-86400  Specify the timeout interval in seconds
```

При попытке восстановления порта в логе появится сообщение:

```
esr# 2025-07-02T03:25:25+00:00 %LINK-W-ERRDISABLE_RECOVERY: Attempting to recover
gigabitethernet 1/0/3 from ErrDisable state caused by 'bpduguard'
```

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	В контексте настройки интерфейса/туннеля активировать функцию BPDU Guard	**esr(config-if-gi)# spanning-tree bpduguard**	
2	Включить автоматический перевод порта из состояния errDisable (не обязательно)	**esr(config)# errdisable recovery cause bpduguard**	

Шаг	Описание	Команда	Ключи
3	Установить временной интервал, по истечении которого интерфейс будет переведен в состояние "UP"	**esr(config)# errdisable recovery interval <TIME>**	<TIME> -– время в секундах, принимает значение в диапазоне [30…86400]. Значение по умолчанию: 300.

Пример настройки

Задача:

Включить BPDU Guard на физическом интерфейсе gigabitethernet 1/0/3, к которому подключено конечное устройство. При поступлении BPDU порт должен отключаться на 60 секунд и автоматически восстанавливаться.



Решение:

Включаем на gigabitethernet 1/0/3 BPDU Guard:

```
esr(config)# interface gigabitethernet 1/0/3
esr(config-if-gi)# spanning-tree bpduguard
```

Включаем автоматическое восстановление интерфейса и задаём временной интервал 60 секунд:

```
esr(config)# errdisable recovery cause bpduguard
esr(config)# errdisable recovery interval 60
```

Проверим настройки восстановления интерфейса:

```
esr# show errdisable recovery
Timer interval: 60 seconds
Reason Automatic Recovery
---------- -------------------
bpduguard Enabled
```

После перехода интерфейса в состояние блокировки, его статус будет отображаться как ErrDisable:

```
esr# show interfaces status
Interface              Admin        Link    MTU     MAC address         Last change     Mode
                       State        State                               (d,h:m:s)
--------------------   ----------   -----   -----   -----------------   -------------
------------
gi1/0/1                Up           Up      1500    68:13:e2:7e:73:91
00,18:31:16     routerport
gi1/0/2                Up           Down    1500    68:13:e2:7e:73:92
00,18:31:22     routerport
gi1/0/3                ErrDisable   Down    1500    68:13:e2:7e:73:93
00,00:00:08     switchport
```

Подробную информацию о блокировке интерфейсов можно посмотреть командой:

```
esr-15r# show interfaces status errdisable
Interface              Err-Disable Reason    Auto-Recovery Time Left
                                             (sec)
--------------------   -------------------   ------------------------
gi1/0/3                bpduguard             56
```

9.6 Настройка Bridge

Bridge (мост) — это способ соединения двух и более сегментов Ethernet на канальном уровне без использования протоколов более высокого уровня, таких как IP. Пакеты передаются на основе Ethernet-адресов, а не IP-адресов. Поскольку передача выполняется на канальном уровне (уровень 2 модели OSI), трафик протоколов более высокого уровня прозрачно проходит через мост.

9.6.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Добавить сетевой мост (bridge) в систему и перейти в режим настройки его параметров.	**esr(config)# bridge <BRIDGE-ID>**	<BRIDGE-ID> – идентификационный номер моста, принимает значения в диапазоне: • для ESR-10/12V(F)/ 15/15R/15VF – [1..50]; • для ESR-20/21/30/31/ 100/200 – [1..250]; • для ESR-1000/1200/ 1500/1511 (rev.B)/ 1700/3100/3150/ 3200/3200L/ 3250/3250/3300/3350/ 3350 – [1..500].
2	Активировать сетевой мост.	**esr(config-bridge)# enable**	

Шаг	Описание	Команда	Ключи
3	Указать экземпляр VRF, в котором будет работать данный интерфейс (необязательно).	**esr(config-bridge)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.
4	Назначить описание конфигурируемому сетевому мосту (необязательно).	**esr(config-bridge)# description <DESCRIPTION>**	<DESCRIPTION> – описание сетевого моста, задаётся строкой до 255 символов.
5	Связать саб-интерфейс, qinq-интерфейс, L2GRE-туннель или L2TPv3-туннель с сетевым мостом. Связанные интерфейсы/туннели и сетевые мосты автоматически становятся участниками общего L2-домена (необязательно).	**esr(config-if-gi)# bridge-group <BRIDGE-ID>** **esr(config-if-l2tpv3)# bridge-group <BRIDGE-ID>**	<BRIDGE-ID> – идентификационный номер моста, принимает значения в диапазоне: • для ESR-10/12V(F)/ 15/15R/15VF – [1..50]; • для ESR-20/21/30/ 31/100/200 – [1..250]; • для ESR-1000/1200/ 1500/1511 (rev.B)/ 1700/3100/3150/ 3200/3200L/ 3250/3250/3300/3350/ 3350 – [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 (необязательно).	**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 (необязательно; возможно, если в bridge включен только VLAN). MTU более 1500 будет активно только в случае применения команды "system jumbo-frames".	**esr(config-bridge)# mtu <MTU>**	<MTU> – значение MTU, принимает значения в диапазоне: • для ESR-10/12V(F)/15/ 15R/15VF – [552..9600]; • для ESR-20/21/30/ 31 – [552..9500]; • для ESR-100/200/ 1000/1200/1500/ 1511 (rev.B)/1700/3100/ 3150/3200/3200L/ 3250/3250/3300/3350/ 3350 – [552..10000]. Значение по умолчанию: 1500.

Шаг	Описание	Команда	Ключи
8	Указать IPv4/IPv6-адрес и маску подсети для конфигурируемого интерфейса или включить получение IP-адреса динамически.	**esr(config-bridge)# ip address <ADDR/LEN> [unit <ID>]** или **esr(config-bridge)# ip address <ADDR/LEN> secondary [unit <ID>]**	<ADDR/LEN> – IP-адрес и длина маски подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. <ID> – номер юнита, принимает значения [1..4]. Ключ secondary указывает, что настроенный адрес является дополнительным IP-адресом. Если это ключевое слово отсутствует, настроенный адрес является основным IP-адресом. Возможно указать до 7 дополнительных IP-адресов. Дополнительные функции IPv4-адресации см. в разделе Настройка IP-адресации.
		esr(config-bridge)# ipv6 address <IPV6-ADDR/LEN> [unit <ID>]	<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]. <ID> – номер юнита, принимает значения [1..4]. Дополнительные функции IPv6-адресации см. в разделе Настройка IPv6-адресации. Можно указать несколько IPv4/IPv6-адресов перечислением через запятую. Может быть назначено до 8 IPv4/IPv6-адресов на интерфейс.
		esr(config-bridge)# ip address dhcp	Дополнительные функции при работе DHCP-клиента см. в разделе Управление DHCP-клиентом.

Шаг	Описание	Команда	Ключи
9	Отключить на интерфейсе функции Firewall или включить интерфейс в зону безопасности (см. раздел Конфигурирование Firewall).	**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 (необязательно).	**esr(config-bridge)# history statistics**	
11	Задать интервал времени, за который усредняется статистика о нагрузке на bridge (необязательно).	**esr(config-bridge)# load-average <TIME>**	<TIME> – интервал в секундах, принимает значения [5..150]. Значение по умолчанию: 5.
12	Задать MAC-адрес сетевого моста, отличный от системного (необязательно).	**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].
13	Включить на bridge режим изоляции интерфейсов. В данном режиме обмен трафиком между членами сетевого моста запрещен (необязательно). Командой **protected-ports exclude {<IF> | <TUN> | <VLAN>}** исключаются из списка изолируемых сущности, включенные в сетевой мост.	**esr(config-bridge)# protected-ports <MODE>**	• none – изоляция интерфейсов отключена. В данном режиме коммутация кадров между членами сетевого моста разрешена; • local – изоляция интерфейсов включена. В данном режиме коммутация кадров между членами сетевого моста запрещена; • radius – изоляция интерфейсов включена. Для использования данного режима требуется настройка Wi-Fi контроллера туннелей в режиме "radius". В данном режиме коммутация кадров между членами сетевого моста запрещена, за исключением SoftGRE DATA туннелей. Для SoftGRE DATA-туннелей параметры изоляции запрашиваются у RADIUS-сервера.

Шаг	Описание	Команда	Ключи
		esr(config-bridge)# protected-ports exclude {<IF> | <TUN> | <VLAN>}	<IF> – интерфейс, задается в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора. <TUN> – имя туннеля, задается в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора. <VLAN> – vlan, связанный с сетевым мостом.
14	Запретить коммутацию трафика unknown-unicast (когда MAC-адрес назначения не содержится в таблице коммутации) в данном bridge (необязательно; применимо только на ESR-1000/1200/1500/1511/1700/3100/3150/3200/3200L/3250/3300/3350).	**esr(config-bridge)# unknown-unicast-forwarding disable**	
15	Установить время жизни IPv4/IPv6-записей в ARP-таблице, изученных на данном bridge (необязательно).	**esr(config-bridge)# ip arp reachable-time <TIME>** или **esr(config-bridge)# ipv6 nd reachable-time <TIME>**	<TIME> – время жизни динамических MAC-адресов, в миллисекундах. Допустимые значения от 5000 до 100000000 миллисекунд. Реальное время обновления записи варьируется от [0,5;1,5]*<TIME>.

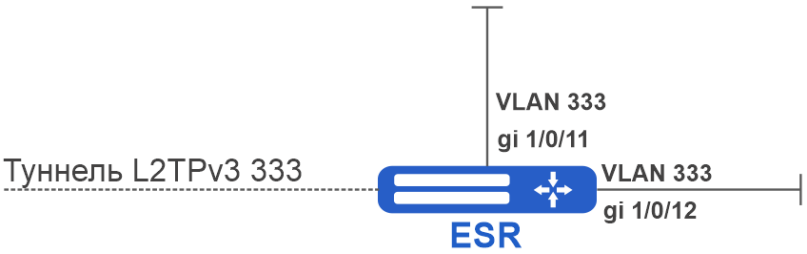
Также для bridge-интерфейса возможно настроить:

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

9.6.2 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
```

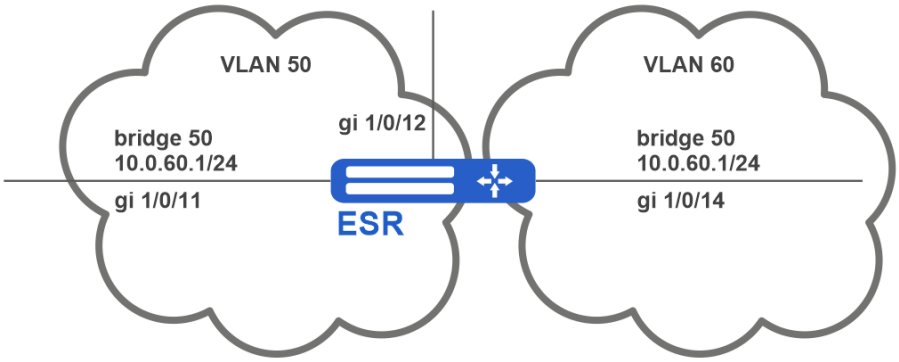
Установим принадлежность L2TPv3-туннеля к мосту, который связан с локальной сетью (настройка L2TPv3-туннеля рассматривается в разделе Настройка L2TPv3-туннелей). В общем случае идентификаторы моста и туннеля не должны совпадать с VID, как в данном примере.

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

9.6.3 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». Необходимо 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
```

9.6.4 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-if-sub)# bridge-group 1
esr(config-if-sub)# exit
```

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

9.7 Настройка Dual-Homing

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

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

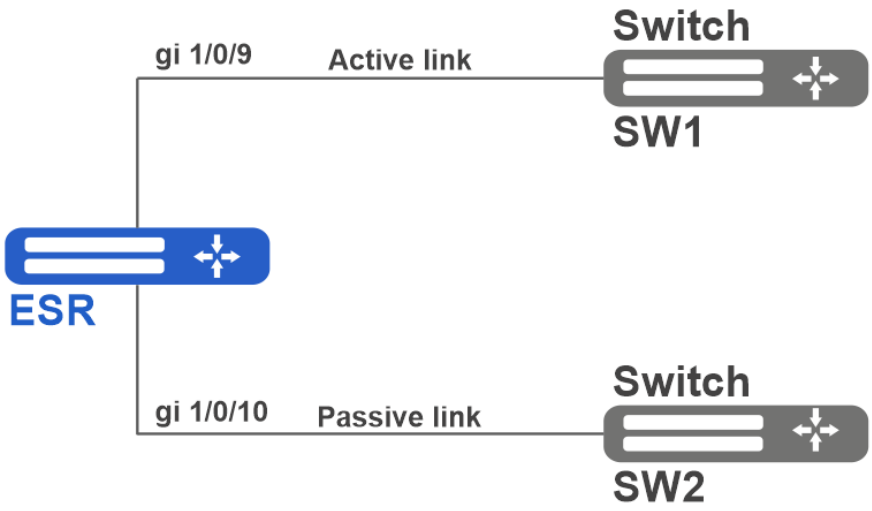
9.7.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Указать резервный интерфейс, на который будет происходить переключение при потере связи на основном.	**esr(config-if-gi)# backup interface<IF> vlan <VID>**	<IF> – интерфейс, на который будет происходить переключение. <VID> – идентификационный номер VLAN, задаётся в диапазоне [2…4094]. Можно также задать диапазоном через «-» или перечислением через «,».
2	Указать количество копий пакетов с одним и тем же MAC-адресом, которые будут отправлены в активный интерфейс при переключении (необязательно).	**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 (необязательно).	**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 (необязательно).	**esr(config)# backup-interface preemption**	

9.7.2 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
```

9.8 Настройка зеркалирования (SPAN/RSPAN)

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

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

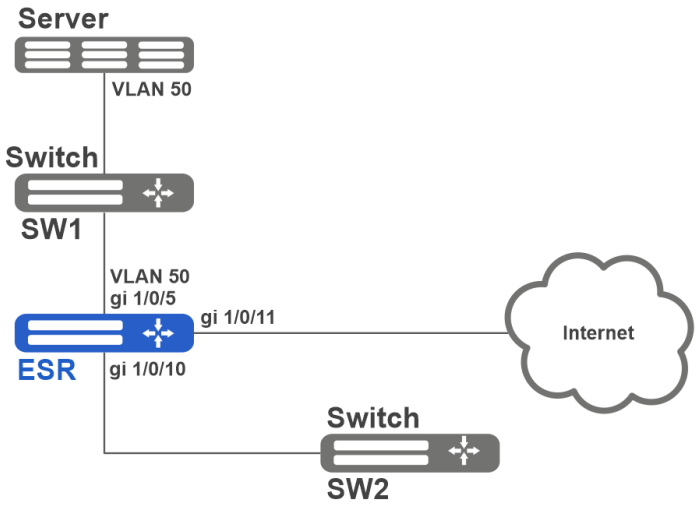
9.8.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Определить VLAN, по которому будет передаваться отзеркалированный трафик (в случае использования удаленного зеркалирования).	**esr(config)# port monitor remote vlan <VID> <DIRECTION>**	<VID> – идентификационный номер VLAN, задаётся в диапазоне [2...4094]; <DIRECTION> – направление трафика: • **tx** – зеркалирование в указанный VLAN только исходящего трафика; • **rx** – зеркалирование в указанный VLAN только входящего трафика.
2	Включить режим удаленного зеркалирования (в случае использования удаленного зеркалирования).	**esr(config)# port monitor remote**	
3	Определить режим порта, передающего отзеркалированный трафик (необязательно).	**esr(config)# port monitor mode <MODE>**	<MODE> – режим: • **network** – совмещенный режим передачи данных и зеркалирование (по умолчанию); • **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; <DIRECTION> – направление трафика: • **tx** – зеркалирование только исходящего трафика; • **rx** – зеркалирование только входящего трафика.

9.8.2 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
```

9.9 Настройка LACP

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

9.9.1 Алгоритм настройки

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

Шаг	Описание	Команда	Ключи
		esr(config)# interface port-channel { <ID> | <UNIT>/<ID> }.<S-VLAN>	**<UNIT>** – номер устройства в группе устройств [1..4]. **<CH>** – порядковый номер группы агрегации каналов, принимает значения [1..12]. **<S-VLAN>** – идентификатор создаваемого S-VLAN.
		esr(config)# interface port-channel { <ID> | <UNIT>/<ID> }.<S-VLAN>.<C-VLAN>	**<C-VLAN>** – идентификатор создаваемого C-VLAN.
5	Настроить необходимые параметры агрегированного канала.	**esr(config-if-port-channel)# mode switchport**	Установить интерфейс в режим L2
		esr(config-if-port-channel)# mode routerport	Установить интерфейс в режим L3
6	Задать скорость (необязательно).	**esr(config-if-port-channel)# speed <SPEED>**	**<SPEED>** – значение скорости: • 10M – значение скорости 10 Мбит/с; • 100M – значение скорости 100 Мбит/с; • 1000M – значение скорости 1000 Мбит/с; • 10G – значение скорости 10 Гбит/с; • 25G – значение скорости 25 Гбит/с; • 40G – значение скорости 40 Гбит/с; • 100G – значение скорости 100 Гбит/с; **Параметр наследуют все физические интерфейсы, принадлежащие данной группе агрегации каналов.** Значение по умолчанию: 1000M

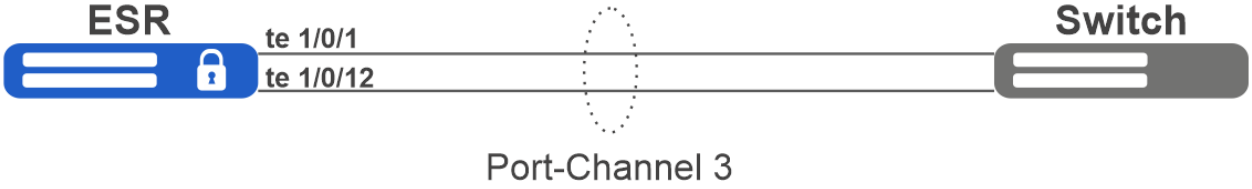
Шаг	Описание	Команда	Ключи
7	Изменить размер MTU (MaximumTransmitionUnit). MTU более 1500 будет активно, только если применена команда **system jumbo-frames** (необязательно).	**esr(config-if-port-channel)# mtu <MTU>**	**<MTU>** – значение MTU в байтах. **Параметр наследуют все физические интерфейсы, принадлежащие данной группе агрегации каналов.** Значение по умолчанию: 1500.
8	Перейти в режим конфигурирования физического интерфейса.	**esr(config)# interface <IF-TYPE><IF-NUM>**	**<IF-TYPE>** – тип интерфейса (gigabitethernet или tengigabitethernet). **<IF-NUM>** – U/S/P – U-юнит (1), S – слот (0), P – порт.
9	Включить физический интерфейс в группу агрегации каналов с указанием режима формирования группы агрегации каналов.	**esr(config-if-gi)# channel-group <ID> mode <MODE>**	**<ID>** – порядковый номер группы агрегации каналов, принимает значения [1..12]. **<MODE>** – режим формирование группы агрегации каналов: • **auto** – добавить интерфейс в динамическую группу агрегации с поддержкой протокола LACP; • **on** – добавить интерфейс в статическую группу агрегации.
10	Установить LACP-приоритет интерфейса Ethernet.	**esr(config-if-gi)# lacp port-priority <PRIORITY>**	**<PRIORITY>** – приоритет, указывается в диапазоне [1..65535]. Значение по умолчанию: 1.
11	Установить интервал времени, в течение которого собирается статистика о нагрузке на интерфейс (необязательно).	**esr(config-if-gi)# load-average <TIME>**	**<TIME>** – интервал в секундах, принимает значения [5..150].
12	Включить запись статистики использования текущего интерфейса (необязательно).	**esr(config-if-gi)# history statistics**	

Шаг	Описание	Команда	Ключи
Также для агрегированного интерфейса возможно настроить: • IPv4/IPv6-адресацию (см. в разделах Настройка IP-адресации, Настройка IPv6-адресации и Управление DHCP-клиентом); • Firewall (см. раздел Конфигурирование Firewall); • QoS в базовом или расширенном режимах (см. раздел Управление QoS); • proxy (см. раздел Проксирование HTTP/HTTPS-трафика); • мониторинг трафика (см. разделы Настройка Netflow и Настройка sFlow); • функции протоколов маршрутизации (см. раздел Управление маршрутизацией); • протокол VRRF (см. раздел Управление резервированием) • функция BRAS (см. раздел Управление BRAS (Broadband Remote Access Server)); • функции IDS/IPS (см. раздел Настройка IPS/IDS).			

9.9.2 Пример настройки

Задача:

Настроить агрегированный канал между маршрутизатором ESR и коммутатором с помощью tengigabitethernet-интерфейсов со значением MTU 9000 в режиме Trunk для передачи всех VLAN, созданных на маршрутизаторе.



Решение:

Предварительная конфигурация:

Предварительно на устройствах необходимо включить поддержку Jumbo-фреймов. Для вступления изменений в силу требуется перезагрузка устройства:

```
esr (config)# system jumbo-frames
```

Также на устройствах должны быть созданы необходимые VLAN для передачи в режиме Trunk.

Основной этап конфигурирования:

Создадим интерфейс port-channel 3:

```
esr(config)# interface port-channel 3
```

Переведём интерфейс в режим swithcport:

```
esr(config-if-port-channel)# mode switchport
```

Зададим размер MTU = 9000:

```
esr(config-if-port-channel)# mtu 9000
```

Установим значение скорости физических интерфейсов, на которых будет работать агрегированный интерфейс:

```
esr(config-if-port-channel)# speed 10G
```

Настроим работу интерфейса в режиме trunk с передачей всех VLAN, созданных на маршрутизаторе:

```
esr(config-if-port-channel)# switchport mode trunk
esr(config-if-port-channel)# switchport trunk allowed vlan auto-all
```

Перейдём к настройке физических интерфейсов. Переведём интерфейсы tengigabitethernet1/0/1 и tengigabitethernet1/0/2 в режим работы switchport:

```
esr(config)# interface tengigabitethernet 1/0/1-2
esr(config-if-te)# mode switchport
```

Включим интерфейсы в созданную группу агрегации каналов с ID 3 в режиме auto с поддержкой протокола LACP:

```
esr(config-if-te)# channel-group 3 mode auto
```

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

10 Управление QoS

- Базовый QoS
  - Алгоритм настройки
  - Пример настройки
  - Пример расчета пропускной способности для взвешенных очередей
- Расширенный QoS
  - Алгоритм настройки
  - Пример настройки
  - Механизм работы полисера
- MPLS QoS

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

10.1 Базовый QoS

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

10.1.1 Алгоритм настройки

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

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

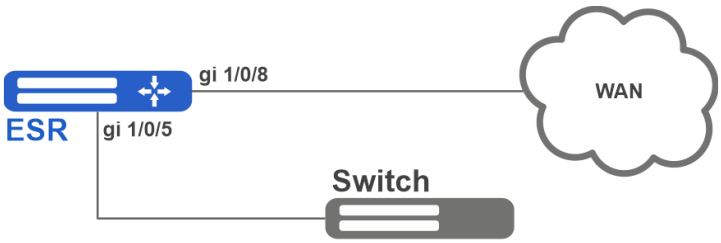
Шаг	Описание	Команда	Ключи
7	Установить номер очереди по умолчанию, в которую попадает весь трафик, кроме IP, в режиме доверия DSCP-приоритетам.	**esr(config)# qos queue default <QUEUE>**	<QUEUE> – идентификатор очереди, принимает значения [1..8].
8	Задать количество приоритетных очередей. Оставшиеся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

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

10.1.2 Пример настройки

Задача:

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



Решение:

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

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

Перенаправим трафик с DSCP 22 в первую приоритетную очередь:

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

Перенаправим трафик с DSCP 14 в седьмую взвешенную очередь:

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

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

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

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

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

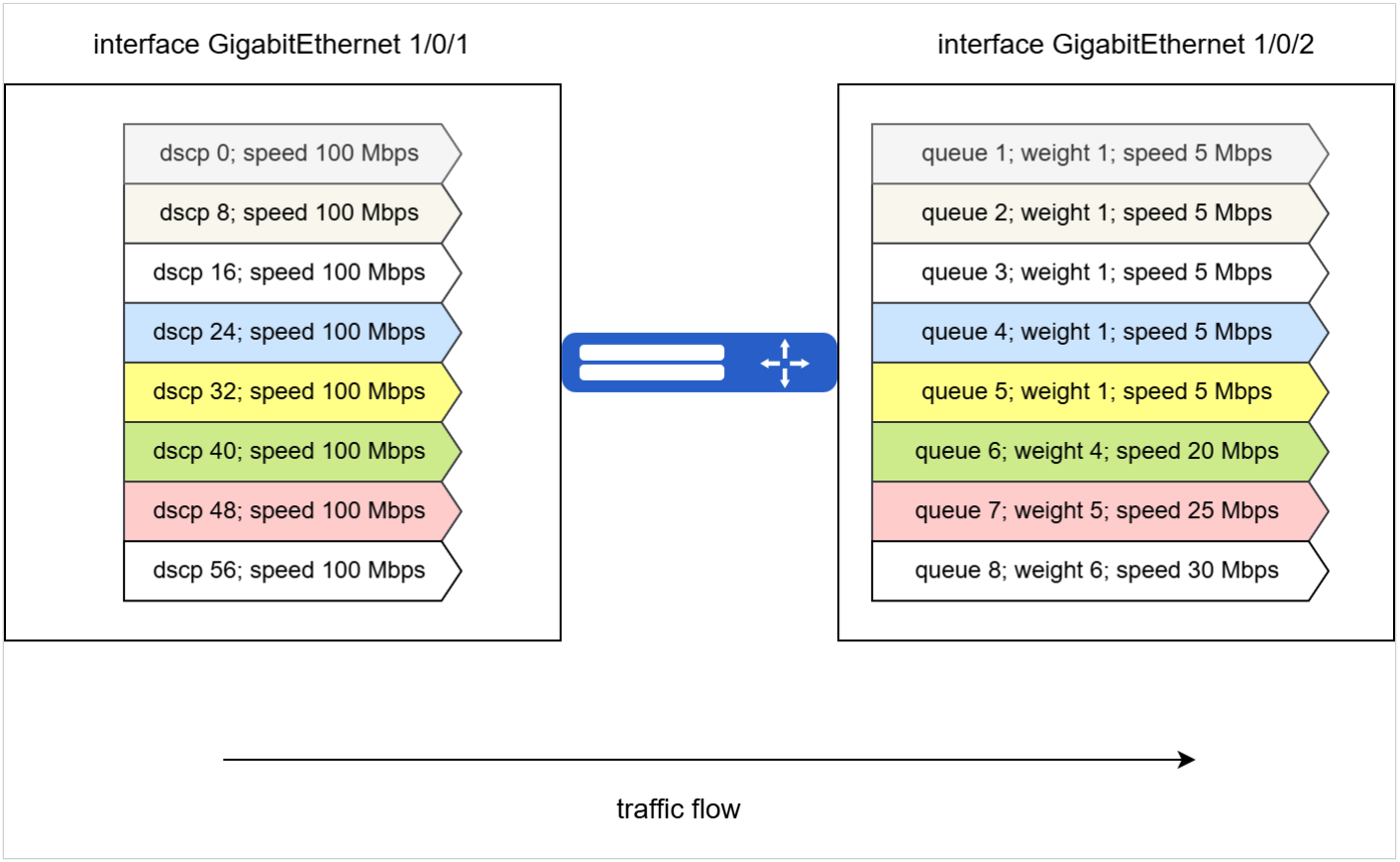
Установим ограничение по скорости в 60 Мбит/с для седьмой очереди:

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

Просмотреть статистику по QoS можно командой:

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

10.1.3 Пример расчета пропускной способности для взвешенных очередей



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

Пример конфигурации:

Конфигурация ESR

```
hostname ESR

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

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

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

В приведенном примере настроены взвешенные очереди с соответствующими весами.

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

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

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

Map DSCP to queue

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

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

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

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

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

10.2 Расширенный QoS

10.2.1 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 (необязательно).	**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 для классификации по полю DSCP в заголовке IP-пакета для конфигурируемого класса.	**esr(config-class-map)# match dscp <DSCP>**	<DSCP> – значение кода DSCP, принимает значения [0..63].
6	Задать значение для классификации по полю EXP в MPLS заголовке для конфигурируемого класса.	**esr(config-class-map)# match mpls experimental topmost <EXP>**	<EXP> – значение поля EXP, принимает значения [0..7].

Шаг	Описание	Команда	Ключи
7	Определить трафик протокола NHRP в туннеле GRE к конфигурируемому классу.	**esr(config-class-map)# match protocol nhrp**	
8	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].
9	Задать значение 802.1p приоритета, которое будет установлено в пакетах, соответствующих конфигурируемому классу (невозможно назначать одновременно с полями DSCP и IP Precedence) (при необходимости перемаркировки).	**esr(config-class-map)# set cos <COS>**	<COS> – значение 802.1p приоритета, принимает значения [0..7].
10	Задать значение кода DSCP, которое будет установлено в IP-пакетах, соответствующих конфигурируемому классу (невозможно назначать одновременно с полями IP Precedence и CoS) (при необходимости перемаркировки).	**esr(config-class-map)# set dscp <DSCP>**	<DSCP> – значение кода DSCP, принимает значения [0..63].
11	Создать политику QoS и осуществить переход в режим настройки параметров политики.	**esr(config)# policy-map <NAME>** **esr(config-policy-map)#**	<NAME> – имя создаваемой политики, задается строкой до 31 символа.
12	Задать описание политики QoS (необязательно).	**esr(config-policy-map)# description <description>**	<description> – до 255 символов.

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

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

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

Шаг	Описание	Команда	Ключи
19	Установить разделяемую полосу пропускания исходящего трафика для определенного класса. Данную полосу класс может занять, если менее приоритетный класс не занял свою гарантированную полосу (при необходимости).	**esr(config-class-policy-map)# shape peak { <BANDWIDTH> | percent <BANDWIDTH_PERCENT> } [BURST]**	<BANDWIDTH> – общая для priority class полоса трафика в Кбит/с, конкуренция происходит на основании приоритета класса, принимает значение [64..10000000]; <BANDWIDTH_PERCENT> – общая для priority class полоса трафика в %, конкуренция происходит на основании приоритета класса, рассчитывается от (в порядке от более приоритетного к менее приоритетному значению): • значения **shape average** корневой политики; • значения **traffic-shape** на сетевом интерфейсе, bridge, туннеле; • значения **speed** сетевого интерфейса. Принимает значение [1..100]. <BURST> – размер сдерживающего порога в Кбайт, принимает значение [4..16000]. По умолчанию 128 Кбайт.
20	Установить параметр, позволяющий вручную скорректировать расчетные значения пакетов при формировании исходящего трафика для класса в рамках политики (при необходимости).	**esr(config-class-policy-map)# shape account user-defined <OFFSET>**	<OFFSET> – корректирующее значение размера пакетов в байтах; Принимает значение [-128..128]. Параметр user-defined устанавливается либо на родительском, либо на дочерних элементах в рамках HQos. Значения user-defined в разных классах могут отличаться друг от друга, и для каждого class-map будет производится свой пересчет.

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

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

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

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

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

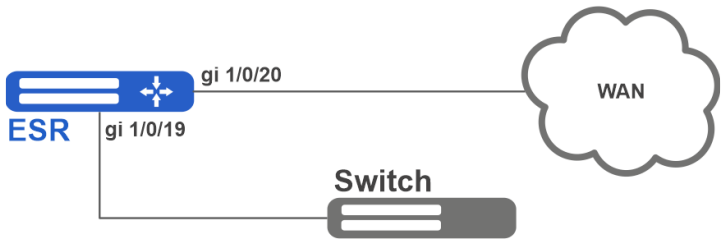
Шаг	Описание	Команда	Ключи
32	Определить очередь по умолчанию для механизма GRED.	**esr(config-class-policy-map)# random-detect queue default <QUEUE-NUM>**	Данной командой определяется очередь по умолчанию для механизма GRED. Для применения данной команды предварительно необходимо настроить команду **random-detect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

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

10.2.2 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 разграничение по подсетям (40 Мбит/с и 60 Мбит/с), ограничить общую полосу до 250 Мбит/с, остальной трафик обрабатывать через механизм SFQ.



Решение:

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

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

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

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

Создаём политику и определяем ограничение общей полосы пропускания:

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

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

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

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

Для другого трафика настраиваем класс с режимом SFQ:

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

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

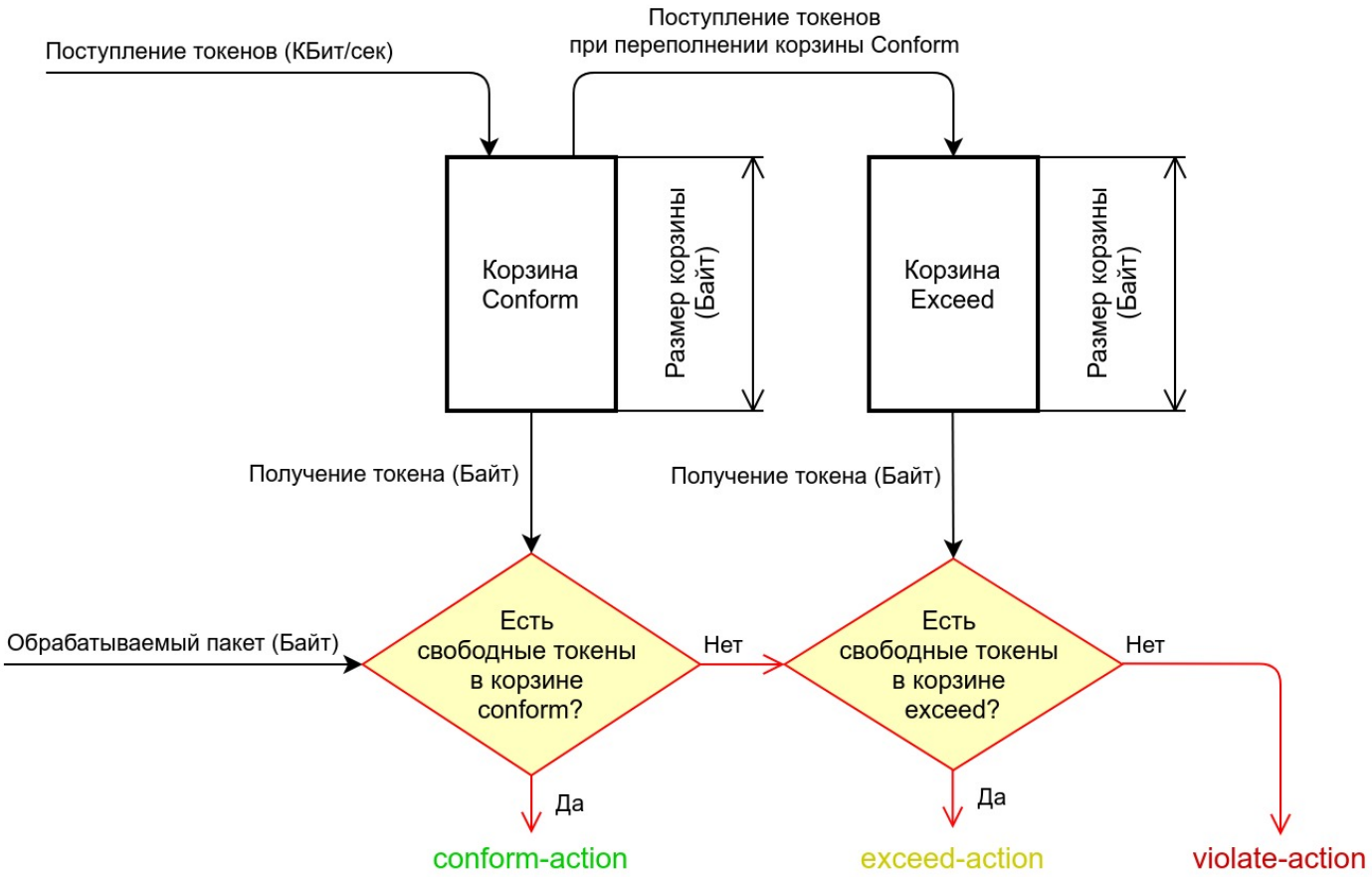
```
esr(config)# interface gigabitethernet 1/0/19
esr(config-if-gi)# qos enable
esr(config-if-gi)# service-policy input fl
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/20
esr(config-if-gi)# qos enable
esr(config-if-gi)# service-policy output fl
esr(config-if-gi)# exit
```

Для просмотра статистики используется команда:

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

10.2.3 Механизм работы полисера

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



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

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

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

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

10.3 MPLS QoS

QoS в MPLS позволяет реализовать управление приоритетами трафика внутри MPLS-домена путём использования EXP-поля в заголовке MPLS. Это даёт возможность классифицировать, маркировать и обрабатывать трафик в соответствии с политиками DiffServ, обеспечивая нужный уровень сервиса для критически важных приложений в L3VPN и других сценариях. Рассмотрим поведение маршрутизатора по умолчанию с полями DSCP и EXP в различных сценариях:

Если ESR выступает в роли PE-маршрутизатора:

- При инкапсуляции IP в MPLS происходит наследование старших трех битов DSCP исходного IP-заголовка в поле EXP сервисной и транспортной меток;
- При инкапсуляции IP в MPLS, а затем в GRE, наследуются старшие три бита исходного IP-заголовка в поле EXP сервисной и транспортной меток. Значение DSCP исходного IP-заголовка наследуется в поле DSCP внешнего IP-заголовка;
- При декапсуляции MPLS значение поля DSCP исходного IP-пакета не изменяется.

Если ESR выступает в роли P-маршрутизатора:

- При операции Swap label значение поля EXP будет унаследовано;
- При операции Explicit null значение поля EXP будет унаследовано;
- При инкапсуляции в GRE происходит наследование поля EXP в три старших бита поля DSCP внешнего IP-заголовка.

Если ESR выступает в роли ASBR-маршрутизатора:

- При операции push label (добавление новых меток) значение поля EXP будет наследовано в поле EXP всех новых меток;
- При операции pop label значение поля EXP не будет унаследовано в стек нижестоящих MPLS меток.

11 Управление маршрутизацией

- Политика фильтрации маршрутной информации
  - Протокол RIP
  - Протокол OSPF
  - Протокол IS-IS
  - Протокол iBGP
  - Протокол eBGP
- Конфигурирование статических маршрутов
  - Алгоритм настройки
  - Пример настройки
- Конфигурирование статических multipath-маршрутов
  - Алгоритм настройки
  - Пример настройки
- Настройка RIP
  - Алгоритм настройки
  - Пример настройки
- Настройка RIPng
  - Алгоритм настройки
  - Пример настройки
- Настройка OSPF
  - Алгоритм настройки
  - Пример настройки
  - Пример настройки OSPF stub area
  - Пример настройки Virtual link
- Настройка BGP
  - Алгоритм настройки
  - Пример настройки
  - Политика выбора лучшего маршрута в протоколе BGP
  - Условное анонсирование маршрутной информации (Conditional Advertisement)
    - Алгоритм настройки
    - Пример настройки
  - Быстрая деактивация пиринговых сессий
    - Метод на основе протокола BFD
      - Алгоритм настройки
      - Пример настройки
    - Метод на основе Fast Peer Deactivation (Fall-over)
      - Алгоритм настройки
      - Пример настройки
  - Настройка политик маршрутизации Route-map
    - Алгоритм настройки
    - Пример настройки 1
    - Пример настройки 2
    - Использование регулярных выражений
      - Алгоритм настройки
      - Пример настройки
  - Конфедерация
    - Алгоритм настройки
    - Пример настройки
- Настройка Policy-Based Routing
  - Алгоритм настройки
  - Пример настройки
- Настройка BFD
  - Настройка таймеров
  - Алгоритм настройки

    - Пример настройки
- Настройка VRF
    - Алгоритм настройки
    - Пример настройки
- Настройка MultiWAN
    - Алгоритм настройки
    - Пример настройки
- Настройка IS-IS
    - Алгоритм настройки
    - Пример настройки

11.1 Политика фильтрации маршрутной информации

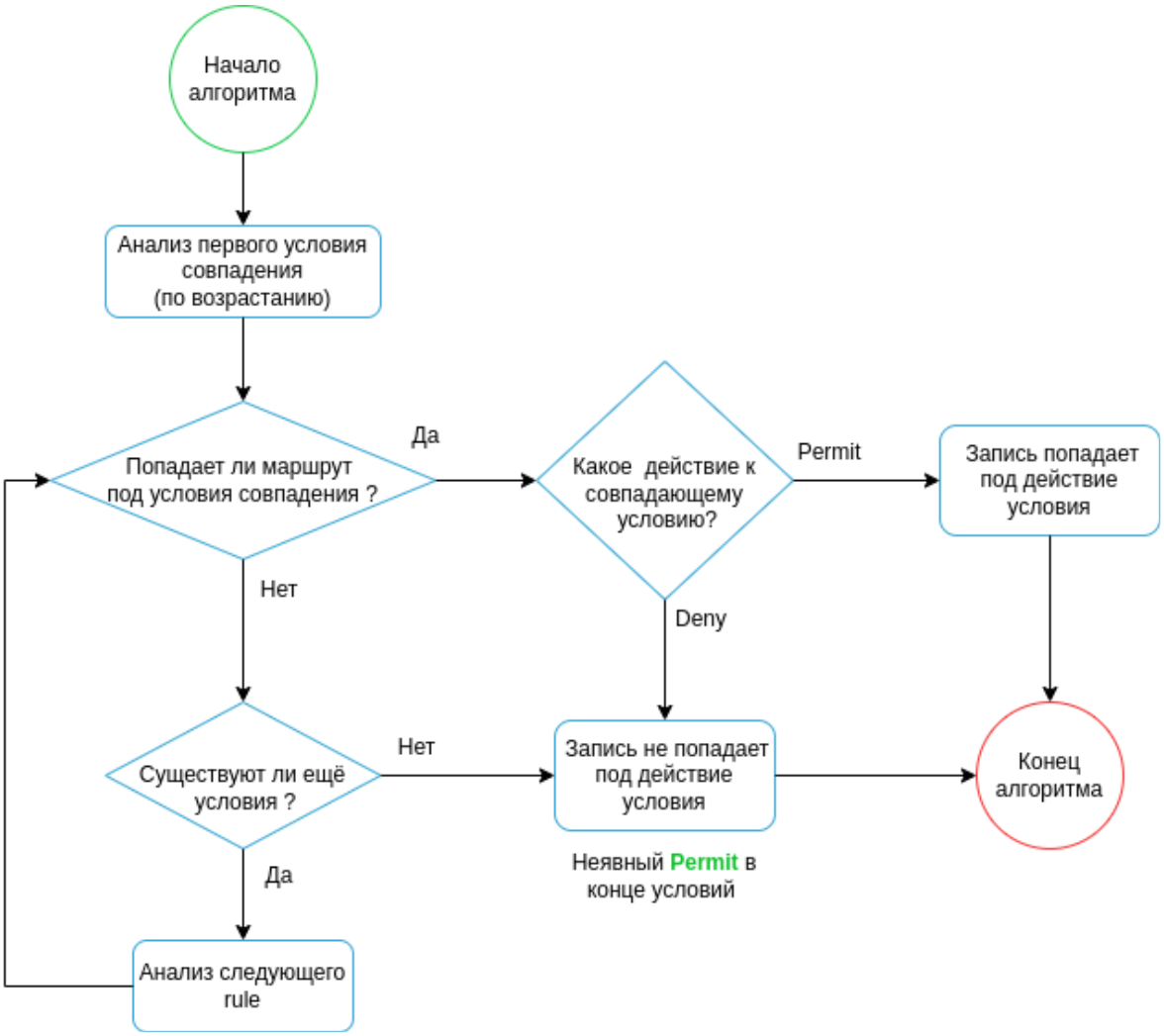
Фильтрация маршрутной информации в динамических протоколах маршрутизации осуществляется с помощью prefix-list и route-map. Структурно они состоят из последовательных условий, совпадений (match) и действий, применяемых для заданных условий – permit/deny. В зависимости от политики обработки маршрутов (импорт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

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

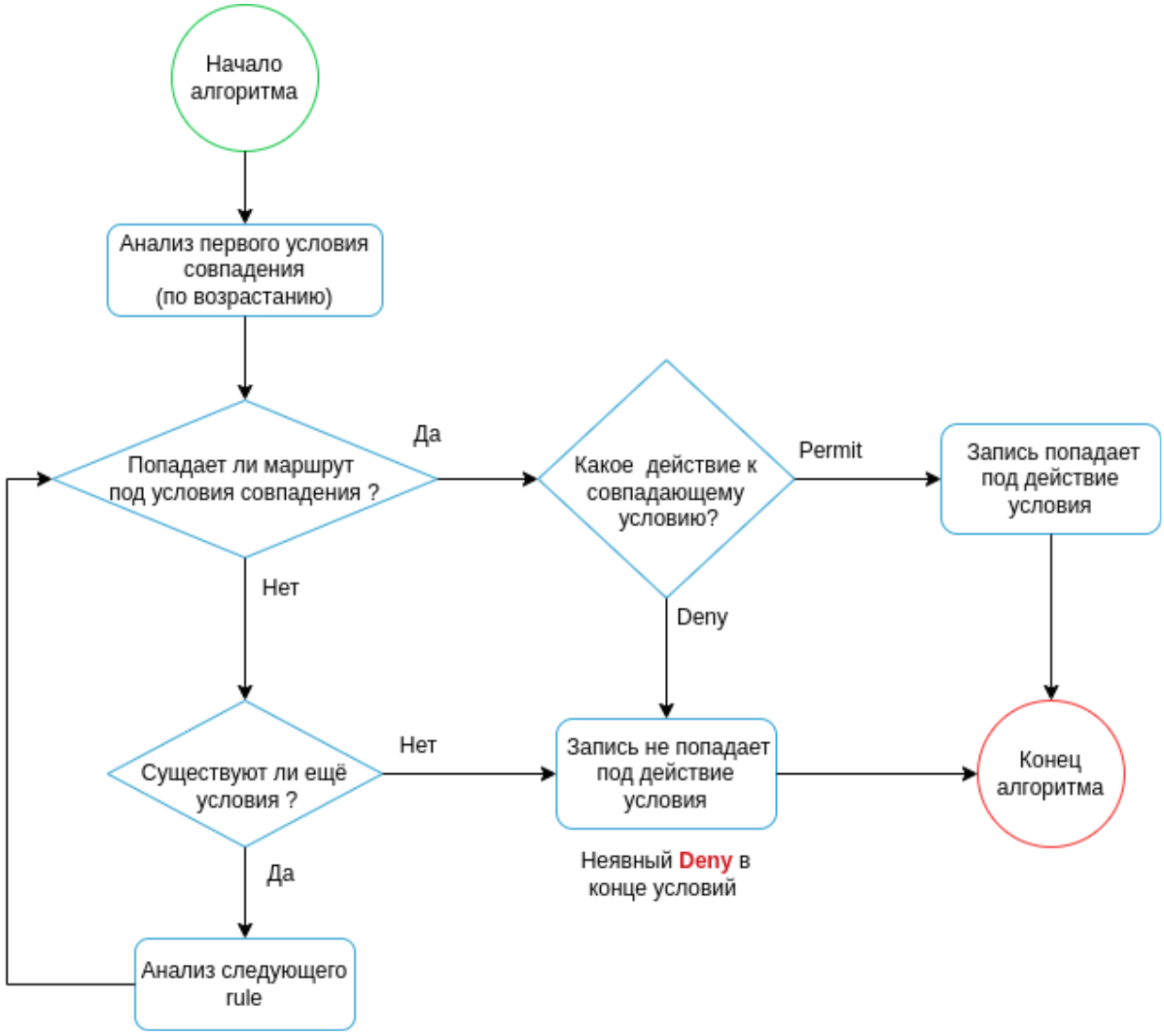
- В route-map: маршруты сопоставляются с IP-префиксами по очереди в списке правил в соответствии с их нумераций – от самого младшего до самого старшего.
- В prefix-list: маршруты сопоставляются с IP-префиксами по очереди в списке IP-префиксов, указанных в prefix-list в том порядке, котором они были заданы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

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

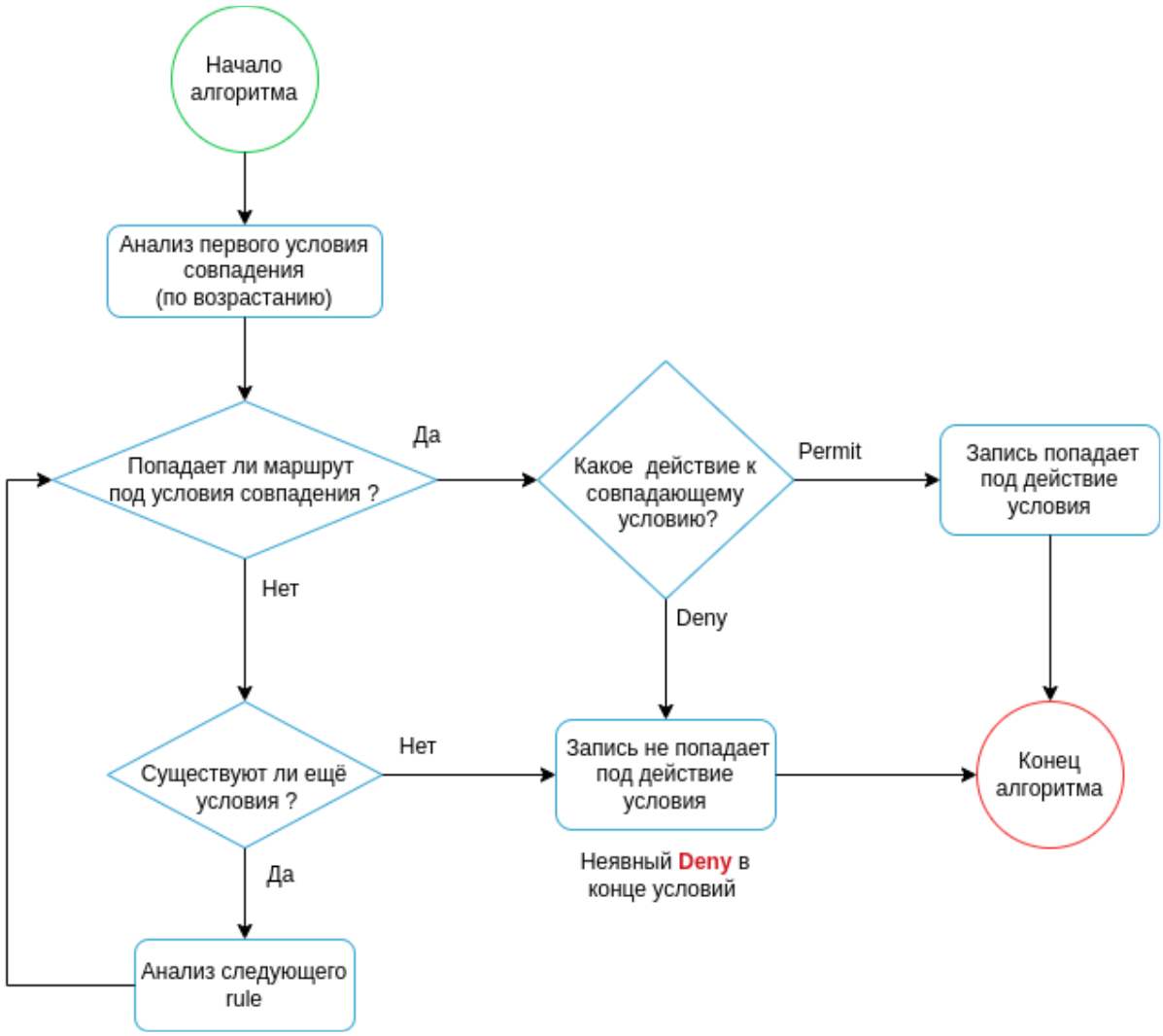
Обработка правил фильтрации маршрутной информации политики export для протоколов RIP, OSPF, IS-IS, iBGP:



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



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



Ниже приведены обобщенные таблицы по протоколам:

11.1.1 Протокол RIP

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

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

11.1.2 Протокол OSPF

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

11.1.3 Протокол IS-IS

in/ out	Политика по умолчанию	Способы анонсирования	Способы фильтрации	Уровни применения политик фильтрации
Import	Получение маршрутной информации не ограничено.	Network, Redistribute	Route-map — последнее (неявное) правило запрещает все, что явно не разрешено предыдущими правилами. Prefix-list — последнее (неявное) правило запрещает все, что явно не разрешено предыдущими правилами.	Процесс IS-IS
Export	Анонсируется информация о интерфейсах, на которых включен протокол IS-IS.		Route-map — последнее (неявное) правило разрешает все, что явно не запрещено предыдущими правилами. Prefix-list — последнее (неявное) правило разрешает все, что явно не запрещено предыдущими правилами.	

11.1.4 Протокол iBGP

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

11.1.5 Протокол eBGP

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

11.2 Конфигурирование статических маршрутов

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

11.2.1 Алгоритм настройки

Добавить статический маршрут возможно командой в режиме глобальной конфигурации:

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

- <VRF> – имя экземпляра VRF, задается строкой до 31 символа;
- <SUBNET> – адрес назначения, может быть задан в следующих видах:
  - AAA.BBB.CCC.DDD – IP-адрес хоста, где каждая часть принимает значения [0..255];
  - AAA.BBB.CCC.DDD/NN – IP-адрес подсети с маской в виде префикса, где AAA-DDD принимают значения [0..255] и NN принимает значения [1..32].
- <NEXTHOP> – IP-адрес шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];
- resolve – при указании данного параметра IP-адрес шлюза будет рекурсивно вычислен через таблицу маршрутизации. Если при рекурсивном вычислении не удастся найти шлюз из напрямую подключенной подсети, то данный маршрут не будет установлен в систему;
- <ID> – номер юнита, принимает значения [1..4];
- <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);
- <METRIC> – метрика маршрута, принимает значения [0..255];
- <TRACK-ID> – идентификатор Tracking-объекта. Если маршрут привязан к Tracking-объекту, то он появится в системе только при выполнении всех условий, заданных в объекте;
- <NAME> – имя (описание) маршрута, текстовая переменная длиной до 31 символа;
- bfd – при указании данного ключа активируется удаление статического маршрута в случае недоступности next-hop. Для работы данного механизма должен быть запущен механизм BFD с IP-адресом next-hop (см. раздел ip bfd neighbor).
  Проверка next-hop при помощи протокола BFD. В случае недоступности next-hop маршрут удаляется.

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

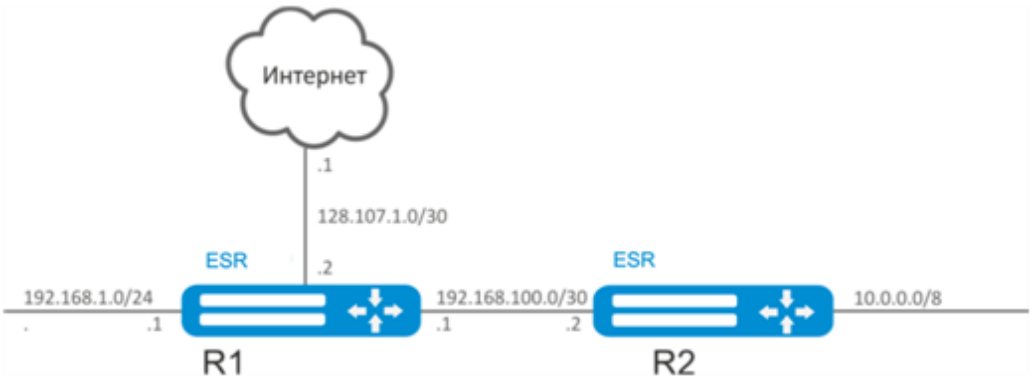
```
esr(config)# ipv6 route [ vrf <VRF> ] <SUBNET> { { <NEXTHOP> [ resolve ] [bfd] [ unit <ID> ] |
interface <IF> | blackhole | unreachable | prohibit [ <METRIC> ] [ name <NAME>] } | wan load-
balance rule <RULE> [ <METRIC> ] }
no ipv6 route [ vrf <VRF> ] <SUBNET> [ <METRIC> ] [ unit <ID> ]
```

- <VRF> – имя экземпляра VRF, задается строкой до 31 символа;
- <SUBNET> – адрес назначения, может быть задан в следующих видах:
  - X:X:X:X::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;
- <ID> – номер юнита, принимает значения [1..4];
- <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];
- <NAME> – имя (описание) маршрута, текстовая переменная длиной до 31 символа;
- bfd – при указании данного ключа активируется проверка next-hop при помощи протокола BFD. В случае недоступности next-hop маршрут удаляется.

11.2.2 Пример настройки

Задача:

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



Решение:

Зададим имя устройства для маршрутизатора R1:

```
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
```

11.3 Конфигурирование статических multipath-маршрутов

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

11.3.1 Алгоритм настройки

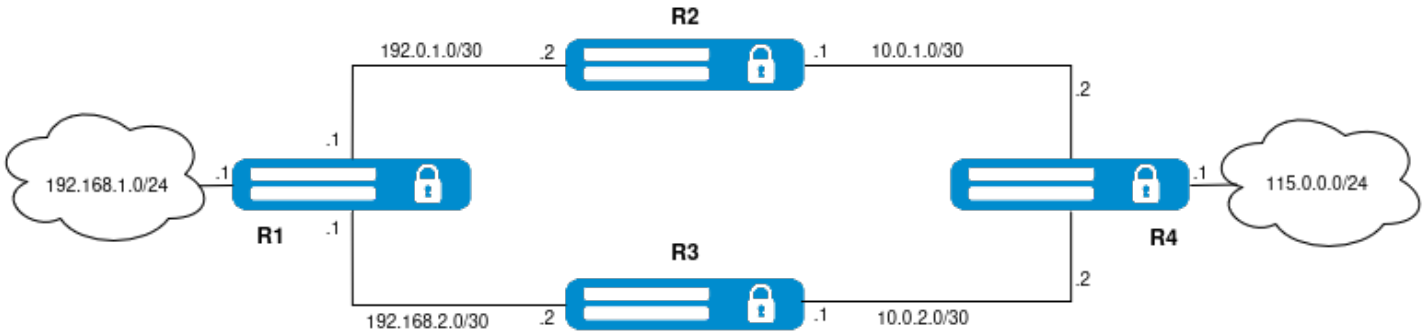
Шаг	Описание	Команда	Ключи
1	Создать статический multipath ipv4 маршрут.	**esr(config)# ip route multipath [vrf <VRF>] <SUBNET> [track <TRACK-ID>] [name <NAME>] [<METRIC>]**	<VRF> – имя экземпляра VRF, задается строкой до 31 символа; <SUBNET> – адрес назначения, может быть задан в следующих видах: •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

Шаг	Описание	Команда	Ключи
2	Создать статический multipath ipv6 маршрут.	**esr(config)# ipv6 route multipath [vrf <VRF>] <SUBNET> [name <NAME>] [<METRIC>]**	<VRF> – имя экземпляра VRF, задается строкой до 31 символа; <SUBNET> – адрес назначения, может быть задан в следующих видах: • X:X:X:X::X – IPv6-адрес хоста, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; • X:X:X:X::X/EE – IPv6-адрес подсети с маской в виде префикса, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128]. <NAME> – имя (описание) маршрута, текстовая переменная длиной до 31 символа; <METRIC> – метрика маршрута, принимает значения [0..255].
3	Настроить шлюзы для маршрута.	**esr(config)# gateway { <NEXTHOP> [<WEIGHT>] [bfd] [unit <ID>] [track <TRACK-ID>] | <IF> [<WEIGHT>] | <TUN> [<WEIGHT>] }**	<NEXTHOP> – адрес шлюза, может быть задан в следующих видах: • AAA.BBB.CCC.DDD – IP-адрес шлюза, где каждая часть принимает значения [0..255]; • X:X:X:X::X – IPv6-адрес шлюза, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <WEIGHT> – метрика шлюза, принимает значения [0..255]. <ID> – номер юнита, принимает значения [1..4]; <IF> – имя IP-интерфейса, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора; <TUN> – имя туннеля, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора; <TRACK-ID> – идентификатор Tracking-объекта. Если шлюз привязан к Tracking-объекту, то он появится в системе только при выполнении всех условий, заданных в объекте. Доступно только для ipv4; bfd – при указании данного ключа активируется проверка доступности шлюза при помощи протокола BFD. В случае недоступности шлюз удаляется из таблицы маршрутизации.

11.3.2 Пример настройки

Задача:

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



Решение:

Конфигурация R1:

R1

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

Конфигурация R2:

R2

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

Конфигурация R3:

R3

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

Конфигурация R4:

R4

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

Проверить таблицу маршрутов можно командой:

```
esr# show ip route
```

11.4 Настройка RIP

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

11.4.1 Алгоритм настройки

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

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

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

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

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

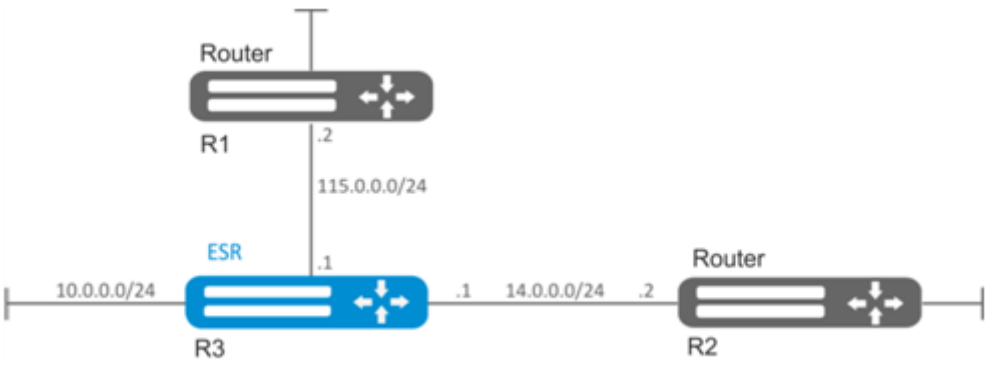
Шаг	Описание	Команда	Ключи
		esr(config-rip)# redistribute isis <ID><ROUTE-TYPE> [route-map <NAME>]	<ID> – номер процесса, может принимать значение [1..65535]; <ROUTE-TYPE> – тип маршрута: • **level-1** – анонсирование маршрутов ISIS-процесса уровня 1; • **level-2** – анонсирование маршрутов ISIS-процесса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

Шаг	Описание	Команда	Ключи
19	Установить режим анонсирования маршрутов по протоколу RIP (необязательно).	**esr(config-if-gi)# ip rip mode <MODE>**	<MODE> – режим анонсирования маршрутов: • **multicast** – маршруты анонсируются в многоадресном режиме; • **broadcast** – маршруты анонсируются в широковещательном режиме; • **unicast** – маршруты анонсируются в unicast-режиме соседям. Значение по умолчанию: multicast.
20	Задать IP-адрес соседа для установления отношения в unicast-режиме анонсирования маршрутов (необязательно).	**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 (необязательно).	**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].
22	Включить протокол BFD для протокола RIP (необязательно).	**esr(config-if-gi)# ip rip bfd-enable**	

11.4.2 Пример настройки

Задача:

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



Решение:

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

Перейдём в режим конфигурирования протокола RIP:

```
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 включим 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.

11.5 Настройка RIPng

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

11.5.1 Алгоритм настройки

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

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

Шаг	Описание	Команда	Ключи
9	Установить временной интервал корректности маршрутной записи без обновления (необязательно).	**esr(config-ripng)# timers invalid <TIME>**	<TIME> – время в секундах, принимает значения [12..65535]. Значение по умолчанию: 180 секунд.
10	Установить временной интервал, по истечении которого производиться удаление маршрута (необязательно).	**esr(config-ripng)# timers flush <TIME>**	<TIME> – время в секундах, принимает значения [12..65535]. При установке значения нужно учитывать следующее правило: «timersinvalid + 60» Значение по умолчанию: 240 секунд.
11	Включить анонсирование подсетей.	**esr(config-ripng)# network <IPV6-ADDR/LEN>**	<IPV6-ADDR/LEN> – IPv6-адрес и маска подсети, задаётся в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128].
12	Добавить фильтрацию подсетей во входящих или исходящих обновлениях (необязательно).	**esr(config-ripng)# prefix-list <PREFIX-LIST-NAME> { in | out }**	<PREFIX-LIST-NAME> – имя сконфигурированного списка подсетей, задаётся строкой до 31 символа. • **in** – фильтрация входящих маршрутов; • **out** – фильтрация анонсируемых маршрутов.
13	Включить анонсирование маршрутов, полученных альтернативным способом (необязательно).	**esr(config-ripng)# redistribute static [route-map <NAME>]**	<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых статических маршрутов, задаётся строкой до 31 символа.

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

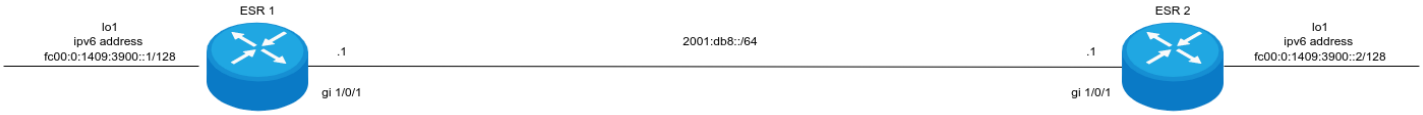
Шаг	Описание	Команда	Ключи
		esr(config-ripng)# redistribute isis <ID><ROUTE-TYPE> [route-map <NAME>]	<ID> – номер процесса, может принимать значение [1..65535]; <ROUTE-TYPE> – тип маршрута: • **level-1** – анонсирование маршрутов ISIS-процесса уровня 1; • **level-2** – анонсирование маршрутов ISIS-процесса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

Шаг	Описание	Команда	Ключи
16	Включить суммаризацию подсетей (необязательно).	**esr(config-if-gi)# ipv6 rip summary-address <IPV6-ADDR/LEN>**	<IPV6-ADDR/LEN> – IPv6-адрес и маска подсети, задаётся в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128].
17	Включить протокол BFD для протокола RIP (необязательно).	**esr(config-if-gi)# ipv6 rip bfd-enable**	

11.5.2 Пример настройки

Задача:

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



Решение:

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

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

```
ESR1(config)# ipv6 router rip
ESR1(config-ripng)# network c00:0:1409:3900::1/128
```

На втором маршрутизаторе произведем аналогичные действия:

```
ESR2(config)# ipv6 router rip
ESR2(config-ripng)# network c00:0:1409:3900::2/128
```

Активируем протокол RIPng на обоих маршрутизаторах:

```
ESR1(config-ripng)# enable

ESR2(config-ripng)# enable
```

Проверяем распространение маршрутной информации:

```
ESR1# sh ipv6 route rip
R     * fc00:0:1409:3900::2/128 [100/2]           via fe80::aaf9:4bff:fead:fed2 on gi1/0/1 [rip
06:01:33]

ESR2# sh ipv6 route rip
R     * fc00:0:1409:3900::2/128 [100/2]           via fe80::aaf9:4bff:fead:fed1 on gi1/0/1 [rip
06:01:33]
```

На этом базовая настройка протокола RIPng закончена.

11.6 Настройка OSPF

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

11.6.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Настроить приоритетность протокола OSPF-маршрутизации для основной таблицы маршрутизации (необязательно).	**esr(config)# ip protocols ospf preference <VALUE>**	<VALUE> – приоритетность протокола, принимает значения в диапазоне [1..255]. Значение по умолчанию: 150.
		esr(config-vrf)# ip protocols ospf preference <VALUE>	

Шаг	Описание	Команда	Ключи
2	Настроить емкость таблиц маршрутизации протокола OSPF (необязательно).	**esr(config)# ip protocols ospf max-routes <VALUE>**	<VALUE> – количество маршрутов протокола OSPF в маршрутной таблице, принимает значения в диапазоне: • для ESR-1000/1200/1500/1511/1700/3100/3150/3200/3200L/3250/3300/3350 – [1..500000]; • для ESR-20/21/30/31/100/200 – [1..300000]; • для ESR-10/12V(F)/15/15R/15VF – [1..30000]. Значение по умолчанию для глобального режима: • для ESR-1000/1200/1500/1511/1700/3100/3150/3200/3200L/3250/3300/3350 – (500000); • для ESR-20/21/30/31/100/200 – (300000); • для ESR-10/12V(F)/15/15R/15VF – (30000). 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 (необязательно).	**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 (необязательно).	**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 (необязательно).	**esr(config-pl)# permit [{ object-group <OBJ-GROUP-NETWORK-NAME> | <ADDR/LEN> | <IPV6-ADDR/LEN> }] [{ eq <LEN> | le <LEN> | ge <LEN> [le <LEN>] }]** **esr(config-pl)# deny [{ object-group <OBJ-GROUP-NETWORK-NAME> | <ADDR/LEN > | <IPV6-ADDR/LEN> }] [{ eq <LEN> | le <LEN> | ge <LEN> [le <LEN>] }]**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IPv4/IPv6-адресов, задаётся строкой до 31 символа; <ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <LEN> – длина префикса, принимает значения [1..32] в IP-списках префиксов; • **eq** – при указании команды длина префикса должна соответствовать указанной; • **le** – при указании команды длина префикса должна быть меньше либо соответствовать указанной; • **ge** – при указании команды длина префикса должна быть больше либо соответствовать указанной.
6	Добавить OSPF-процесс в систему и осуществить переход в режим настройки параметров OSPF-процесса.	**esr(config)# router ospf <ID> [vrf <VRF>]** **esr(config)# ipv6 router ospf <ID> [vrf <VRF>]**	<ID> – номер автономной системы процесса, принимает значения [1..65535] <VRF> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет работать протокол маршрутизации.

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

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

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

Шаг	Описание	Команда	Ключи
		esr(config-ospf)# redistribute bgp <AS> [metric <TYPE> <METRIC>] [route-map <NAME>]	<TYPE> – тип атрибута OSPF Metric, принимает значение type-1 и type-2; <METRIC> – значение атрибута OSPF Metric, принимает значения [0..65535]. <AS> – номер автономной системы, может принимать значения [1..4294967295]; <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых BGP-маршрутов, задаётся строкой до 31 символа.
14	Включить анонсирование подсетей (необязательно).	**esr(config-ospf)# network <ADDR/LEN>**	<ADDR/LEN> – адрес подсети, указывается в следующем формате: AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32].
		esr(config-ipv6-ospf)# 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].
15	Включить наследование внутренней метрики протокола маршрутизации BGP (MED) в метрику протокола маршрутизации OSPF(Cost) при редистрибуции маршрутов.	**esr(config-ospf)# inherit-metric bgp**	
		esr(config-ipv6-ospf)# inherit-metric bgp	
16	Активировать OSPF-процесс.	**esr(config-ospf)# enable**	
		esr(config-ipv6-ospf)# enable	

Шаг	Описание	Команда	Ключи
17	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>	
18	Определить тип области (необязательно).	**esr(config-ospf-area)# area-type <TYPE> [no-summary]**	<TYPE> – тип области: • **stub** – устанавливает значение stub (тупиковая область); no-summary – команда в связке с параметром «stub» образует область «totallystubby» (для передачи информации за пределы области используется только маршрут по умолчанию). • **nssa** – устанавливает значение nssa (область NSSA); no-summary – в связке с параметром nssa образует область totallynssa (автоматически генерирует маршрут по умолчанию как межобластной).
		esr(config-ipv6-ospf-area)# area-type <TYPE> [no-summary]	
19	Включить генерацию маршрута по умолчанию для NSSA или stub-области и анонсирование его в качестве Type-7 или Type-3 LSA соответственно (необязательно).	**esr(config-ospf-area)# default-information-originate**	
		esr(config-ipv6-ospf-area)# default-information-originate	
20	Определить тип метрики маршрута по умолчанию для NSSA-области (необязательно).	**esr(config-ospf-area)# default-metric-type <TYPE>**	• **type-1** – устанавливает тип метрики **E1** для маршрута по умолчанию в NSSA-области; • **type-2** – устанавливает тип метрики **E2** для маршрута по умолчанию в NSSA-области.
		esr(config-ipv6-ospf-area)# default-metric-type <TYPE>	
21	Активировать OSPF-область.	**esr(config-ospf-area)# enable**	
		esr(config-ipv6-ospf-area)# enable	

Шаг	Описание	Команда	Ключи
22	Установить виртуальное соединение между основной и удаленными областями, имеющими между ними несколько областей (необязательно).	**esr(config-ospf-area)# virtual-link <ID>** **esr(config-ipv6-ospf-area)# virtual-link <ID>**	<ID> – идентификатор маршрутизатора, с которым устанавливается виртуальное соединение, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
23	Установить интервал времени в секундах, по истечении которого маршрутизатор повторно отправит пакет, который не получил подтверждения о получении (необязательно).	**esr(config-ospf- vlink)# restransmit-interval <TIME>** **esr(config-ipv6-ospf- vlink)# restransmit-interval <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 5 секунд.
24	Установить интервал времени в секундах, по истечении которого маршрутизатор отправляет следующий hello-пакет (необязательно).	**esr(config-ospf- vlink)# hello-interval <TIME>esr(config-bgp-neighbor)# fall-over bfd** **esr(config-ipv6-ospf- vlink)# hello-interval <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 10 секунд.
25	Установить интервал времени в секундах, по истечении которого сосед будет считаться неактивным (необязательно). Этот интервал должен быть кратным значению «hello-interval».	**esr(config-ospf- vlink)# dead-interval <TIME>** **esr(config-ipv6-ospf-vlink)# dead-interval <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Для **(config-(ipv6)-ospf- vlink**) - [2..65535] Значение по умолчанию: 40 секунд.
26	Определяется интервал времени в секундах, по истечении которого маршрутизатор выберет DR в сети (необязательно).	**esr(config-ospf- vlink)# wait-interval <TIME>** **esr(config-ipv6-ospf- vlink)# wait-interval <TIME>**	<TIME> – время в секундах, принимает значения [2..65535]. Значение по умолчанию: 40 секунд.
27	Определить алгоритм аутентификации (необязательно).	**esr(config-ospf- vlink)# authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм аутентификации: • **cleartext** – пароль, передается открытым текстом (доступно только для RIP и OSPF-VLINK); • **md 5** – пароль, хешируется по алгоритму md5.

Шаг	Описание	Команда	Ключи
28	Установить пароль для аутентификации с соседом (необязательно).	**esr(config-ospf- vlink)# authentication key ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов. <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).
29	Определить список паролей для аутентификации через алгоритм хеширования md5 (необязательно).	**esr(config-ospf- vlink)# authentication key chain <KEYCHAIN>**	<KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов.
30	Активировать виртуальное соединение (необязательно).	**esr(config-ospf- vlink)# enable**	
31	Перейти в режим конфигурирования интерфейса/туннеля/сетевого моста.	**esr(config)# interface <IF-TYPE><IF-NUM>**	<IF-TYPE> – тип интерфейса; <IF-NUM> – F/S/P – F-фрейм (1), S – слот (0), P – порт.
		esr(config)# tunnel <TUN-TYPE><TUN-NUM>	<TUN-TYPE> – тип туннеля; <TUN-NUM> – номер туннеля.
		esr(config)# bridge <BR-NUM>	<BR-NUM> – номер bridge.
32	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>	
33	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>	
34	Включить маршрутизацию по протоколу OSPF на интерфейсе.	**esr(config-if-gi)# ip ospf**	
		esr(config-if-gi)# ipv6 ospf	
35	Включить режим, в котором OSPF-процесс будет игнорировать значение MTU интерфейса во входящих Database Description-пакетах (необязательно).	**esr(config-if-gi)# ip ospf mtu-ignore**	
		esr(config-if-gi)# ipv6 ospf mtu-ignore	

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

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

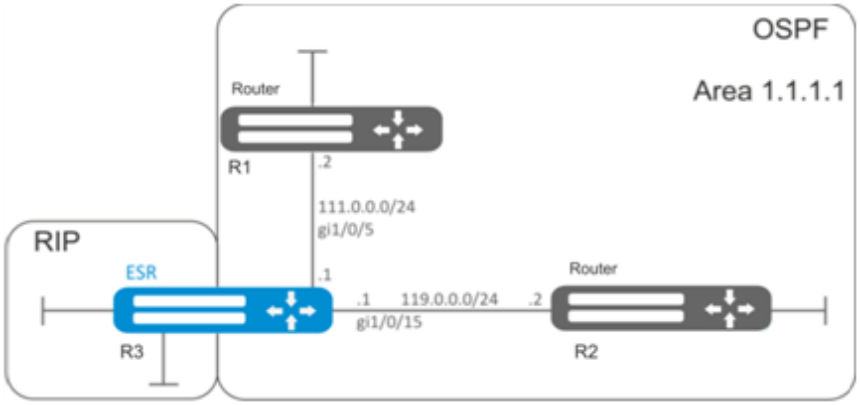
Шаг	Описание	Команда	Ключи
46	Определить тип сети для установления OSPF-соседства (необязательно).	**esr(config-if-gi)# ip ospf network <TYPE>** **esr(config-if-gi)# ipv6 ospf network <TYPE>**	<TYPE> – тип сети: • **broadcast** – тип соединения широковещательный; • **non - broadcast** – тип соединения NBMA; • **point - to - multipoint** – тип соединения точка-многоточие; • **point-to-multipoint non-broadcast** – тип соединения NBMA точка-многоточие; • **point - to - point** – тип соединения точка-точка. Значение по умолчанию: broadcast.
47	Перевести интерфейс в пассивный режим работы. В этом режиме не рассылаются hello-пакеты, не устанавливаются отношения соседства, но подключенная сеть анонсируется соседям (необязательно).	**esr(config-if-gi)# ip ospf passive-interface** **esr(config-if-gi)# ipv6 ospf passive-interface**	
48	Установить приоритет маршрутизатора, который используется для выбора DR и BDR (необязательно).	**esr(config-if-gi)# ip ospf priority <VALUE>** **esr(config-if-gi)# ipv6 ospf priority <VALUE>**	<VALUE> – приоритет интерфейса, принимает значения [1..65535]. Значение по умолчанию: 128.
49	Установить величину метрики на интерфейсе или туннеле (необязательно).	**esr(config-if-gi)# ip ospf cost <VALUE> [track <TRACK-ID>]** **esr(config-if-gi)# ipv6 ospf cost <VALUE> [track <TRACK-ID>]**	<VALUE> – величина метрики, задаётся в размере [0..32767]. Значение по умолчанию: 10. <TRACK-ID> – идентификатор объекта отслеживания, при выполнении всех условий которого будет исполняться указанное действие. Изменяется в диапазоне [1..100].
50	Включить протокол BFD для протокола OSPF (необязательно).	**esr(config-if-gi)# ip ospf bfd-enable**	

Шаг	Описание	Команда	Ключи
		esr(config-if-gi)# ipv6 ospf bfd-enable	
51	Включить механизм ttl-security hops (необязательно).	**esr(config-if-gi)# ip ospf ttl-security-hops <VALUE>**	<VALUE> – значение ttl, задаётся в размере [1..255]. Значение по умолчанию: 0.
		esr(config-if-gi)# ipv6 ospf ttl-security-hops <VALUE>	

11.6.2 Пример настройки

Задача:

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



Решение:

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

Создадим OSPF-процесс с идентификатором 10 и 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:

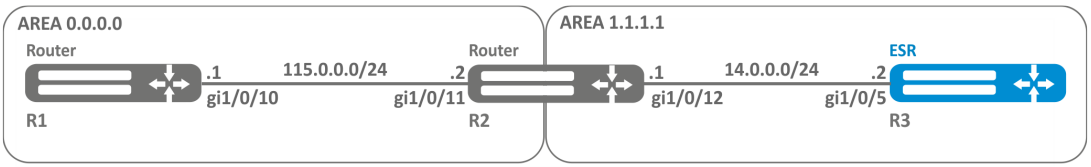
```
esr(config)# interface gigabitethernet 1/0/5
esr(config-if-gi)# ip ospf instance 10
esr(config-if-gi)# ip ospf area 1.1.1.1
esr(config-if-gi)# ip ospf
esr(config-if-gi)# exit
```

```
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
```

11.6.3 Пример настройки OSPF stub area

Задача:

Изменить тип области 1.1.1.1, область должна быть тупиковой.



Решение:

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

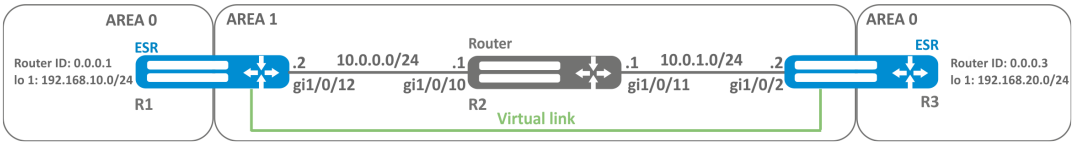
Изменим тип области на тупиковый. На каждом маршрутизаторе из области 1.1.1.1 в режиме конфигурирования области выполним команду:

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

11.6.4 Пример настройки Virtual link

Задача:

Объединить две магистральные области в одну с помощью virtual link.



Решение:

> ⚠ В firewall необходимо разрешить протокол OSPF (89).

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

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

На маршрутизаторе R1 перейдем в режим конфигурирования области 1.1.1.1:

```
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
```

11.7 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.

11.7.1 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 (необязательно).	**esr(config)# ip protocols bgp preference <VALUE>**	<VALUE> – приоритетность протокола, принимает значения в диапазоне [1..255]. Значение по умолчанию: BGP (170).

Шаг	Описание	Команда	Ключи
2	Настроить емкость таблиц маршрутизации протокола BGP (необязательно при использовании глобальной таблицы маршрутизации).	**esr(config)# ip protocols bgp max-routes <VALUE>**	<VALUE> – количество маршрутов протокола BGP в маршрутной таблице, принимает значения в диапазоне: • для ESR-1000/1200/1500/1511/1700/3100/3150/3200/3200L/3250/3300/3350 – [1..5000000]; • для ESR-20/21/30/31/100/200 – [1..2500000]; • для ESR-10/12V(F)/15/15R/15VF – [1..1000000]. Значение по умолчанию для глобальной таблицы маршрутизации: • для ESR-1000/1200/1500/1511/1700/3100/3150/3200/3200L/3250/3300/3350 – [5000000]; • для ESR-20/21/30/31/100/200 – [2500000]; • для ESR-10/12V/12VF/15/15R/15VF – [1000000]. Значение по умолчанию для VRF: 0.
		esr(config)# ipv6 protocols bgp max-routes <VALUE>	
		esr(config-vrf)# ip protocols bgp max-routes <VALUE>	
		esr(config-vrf)# ipv6 protocols bgp max-routes <VALUE>	
3	Включить вывод информации о состоянии отношений с соседями для протокола маршрутизации BGP (необязательно).	**esr(config)# router bgp log-neighbor-changes**	
		esr(config)# ipv6 router bgp log-neighbor-changes	
4	Включить ECMP и определяется максимальное количество равноценных маршрутов до цели.	**esr(config)# router bgp maximum-paths <VALUE>**	<VALUE> – количество допустимых равноценных маршрутов до цели, принимает значения [1..16].
5	Выбрать метод фильтрации для передаваемой информации между роутерами (обязательно при конфигурировании eBGP для анонсирования подсетей).		

Шаг	Описание	Команда	Ключи
5.1.1	При выборе метода фильтрации на основе route-map создать список правил, который в дальнейшем будет использоваться для фильтрации анонсируемых и получаемых IP-маршрутов.	**esr(config)# route-map <NAME>**	<NAME> – имя конфигурируемых правил маршрутизации, задаётся строкой до 31 символа.
5.1.2	Создать правило.	**(config-route-map)# rule <ORDER>**	<ORDER> – номер правила, принимает значения [1 .. 10000].

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

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

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

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

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

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

Шаг	Описание	Команда	Ключи
18	Включить анонсирование подсетей.	**esr(config-bgp-af)# network <ADDR/LEN> [route-map <NAME>]**	<ADDR/LEN> – адрес подсети, указывается в одном из следующих формате: • AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32]; • X:X:X:X::X/EE – IPv6-адрес и маска подсети, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128]. <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых BGP-маршрутов, задаётся строкой до 31 символа.
19	Осуществить выход из режима глобального конфигурирования анонсов маршрутной информации процесса BGP	**esr(config-bgp-af)# exit**	
20	Добавить BGP-соседа и осуществить переход в режим настройки параметров BGP-соседа.	**esr(config-bgp)# neighbor <ADDR>|<IPV6-ADDR>**	<ADDR> – IP-адрес соседа, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> – IPv6-адрес клиента, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
21	Задать описание соседа (необязательно).	**esr(config-bgp-neighbor)# description <DESCRIPTION>**	<DESCRIPTION> – описание соседа, задаётся строкой до 255 символов.

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

Шаг	Описание	Команда	Ключи
28	Задать IP/IPv6-адрес маршрутизатора, который будет использоваться в качестве IP/IPv6-адреса источника в отправляемых обновлениях маршрутной информации BGP (необязательно).	**esr(config-bgp-neighbor)# update-source { <ADDR> | <IPV6-ADDR> | <IF> | <TUN> }**	<ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> – IPv6-адрес источника, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. <IF> – интерфейс, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора. <TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора.
29	Включить режим, в котором разрешен приём маршрутов в BGP-атрибуте, AS Path которых содержит номера автономной системы процесса (необязательно).	**esr(config-bgp-neighbor)# allow-local-as <NUMBER>**	<NUMBER> – пороговое число вхождений номера автономной системы процесса в атрибуте AS Path, при которых маршрут будет принят, диапазон допустимых значений [1..10].
30	Включить BFD-протокол на конфигурируемом BGP-соседе (необязательно, используется совместно с параметром update-source).	**esr(config-bgp-neighbor)# fall-over bfd**	
31	Включить режим, при котором соседство BGP разрывается, как только указанный маршрут к соседу удаляется из таблицы маршрутизации.	**esr(config-bgp-neighbor)# fall-over route-map [route-map <NAME>]**	<NAME> – имя маршрутной карты, которая будет использоваться для отслеживания наличия маршрута, задаётся строкой до 31 символа.
32	Определить алгоритм аутентификации с соседом (необязательно).	**esr(config-bgp-neighbor)# authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм шифрования: md5 – пароль шифруется по алгоритму md5.

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

Шаг	Описание	Команда	Ключи
40	Определить приоритетность маршрутов, получаемых от соседа (необязательно).	**esr(config-bgp-neighbor-af)# preference <VALUE>**	<VALUE> – приоритетность маршрутов соседа, принимает значения в диапазоне [1..255]. Значение по умолчанию: 170.
41	Задать режим, в котором перед отправлением обновления из BGP-атрибута AS Path маршрутов удаляются приватные номера автономных систем (в соответствии с RFC 6996) (необязательно, отсутствует для vpnv4).	**esr(config-bgp-neighbor-af)# remove-private-as [{ all | nearest | replace }]**	**all** – удалить все частные номера AS из AS-path; **nearest** – заменить ближайшие частные AS в AS-path на рядом стоящую публичную AS; **replace** – заменить все частные номера AS номером текущего процесса BGP. Значение по умолчанию: all.
42	Включить обмен маршрутной информацией.	**esr(config-bgp-neighbor-af)# enable**	
43	Задать режим, в котором маршрутизатор будет представляться указанным номером автономной системы вместо реального номера автономной системы (необязательно).	**esr(config-bgp-neighbor)# local-as <AS>**	<AS> – номер автономной системы, принимает значения [1..4294967295].
44	Не добавлять указанный в local-as номер автономной системы в AS-Path при приёме маршрута (необязательно).	**esr(config-bgp-local-as)# no-prepend**	
45	Добавлять в AS-Path только номер автономной системы, указанный в local-as (необязательно).	**esr(config-bgp-local-as)# replace-as**	

Шаг	Описание	Команда	Ключи
46	Включить агрегирование маршрутной информации (необязательно).	**esr(config-bgp)# aggregate-address { <ADDR/LEN> | <IPV6-ADDR/LEN } **	<ADDR/LEN> – IP-адрес и маска подсети, задается в виде: • AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32]; <IPV6-ADDR/LEN> – IPv6-адрес и маска подсети, задается в виде: • X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128];
47	Задать route-map для установки дополнительных условий агрегирования маршрутов (необязательно).	**esr(config-bgp-aggregate)# advertise-map [route-map <NAME>]**	<NAME> – имя маршрутной карты, которая будет использоваться для задания условий агрегирования BGP-маршрутов, задаётся строкой до 31 символа.
48	Добавлять в AS-Path агрегированного маршрута номера автономных систем из AS-Path его компонентов (необязательно).	**esr(config-bgp-aggregate)# as-set**	
49	Задать route-map для установки дополнительных атрибутов агрегированного маршрута (необязательно).	**esr(config-bgp-aggregate)# attribute-map [route-map <NAME>]**	<NAME> – имя маршрутной карты, которая будет использоваться для задания атрибутов агрегированного BGP-маршрута, задаётся строкой до 31 символа.
50	Подавлять все компоненты агрегированного маршрута (необязательно).	**esr(config-bgp-aggregate)# summary-only**	
51	Задать route-map для подавления компонентов агрегированного маршрута (необязательно).	**esr(config-bgp-aggregate)# suppress-map [route-map <NAME>]**	<NAME> – имя маршрутной карты, которая будет использоваться для задания подавляемых компонентов агрегированного BGP-маршрута, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
52	Задать возможность динамически устанавливать BGP-сессию без указания конкретного адреса соседа. Соседство может быть установлено с любым адресом, попадающим в указанную подсеть (необязательно).	**esr(config-bgp-aggregate)# listen-range { <ADDR/LEN> | <IPV6-ADDR/LEN }**	<ADDR/LEN> – IP-адрес и маска подсети, задается в виде: • AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32]; <IPV6-ADDR/LEN> – IPv6-адрес и маска подсети, задается в виде: • X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128].
53	Разрешить возможность динамической установки BGP-сессии только с соседями, которые имеют определённые номера AS.	**esr(config-bgp-listen)# as-range <AS-PATH>**	<AS-PATH> – список номеров автономных систем, задается в виде AS-AS,AS,AS-AS, принимает значения [1..4294967295].

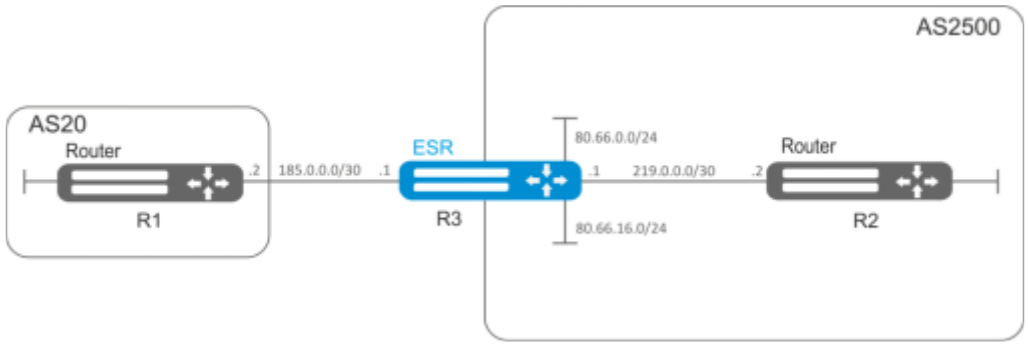
Часто бывает, особенно при конфигурировании iBGP, что в одном bgp-процессе необходимо настроить несколько bgp neighbor с одинаковыми параметрами. Во избежание избыточности конфигурации рекомендуется использовать bgp peer-group, в которой возможно описать общие параметры, а в конфигурации bgp neighbor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

11.7.2 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, AS20.



Решение:

Сконфигурируем необходимые сетевые интерфейсы:

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

Сконфигурируем firewall для приема маршрутизатором 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 object-group og_bgp
esr-R3(config-zone-pair-rule)# action permit
esr-R3(config-zone-pair-rule)# enable
esr-R3(config-zone-pair-rule)# exit
esr-R3(config-zone-pair)# exit
```

И укажем принадлежность интерфейсов к зоне безопасности:

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

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

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

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

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

Сконфигурируем анонсирование подсетей, подключенных напрямую:

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

Создадим соседство с роутером R2 по iBGP:

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

И включим обмен IPv4-маршрутами:

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

Создадим соседство с роутером R1 по eBGP:

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

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

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

Включим работу протокола:

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

Информацию о BGP-пирах можно посмотреть командой:

```
esr# show bgp neighbors
```

Таблицу маршрутов протокола BGP можно просмотреть с помощью команды:

```
esr# show bgp ipv4 unicast
```

11.7.3 Политика выбора лучшего маршрута в протоколе BGP

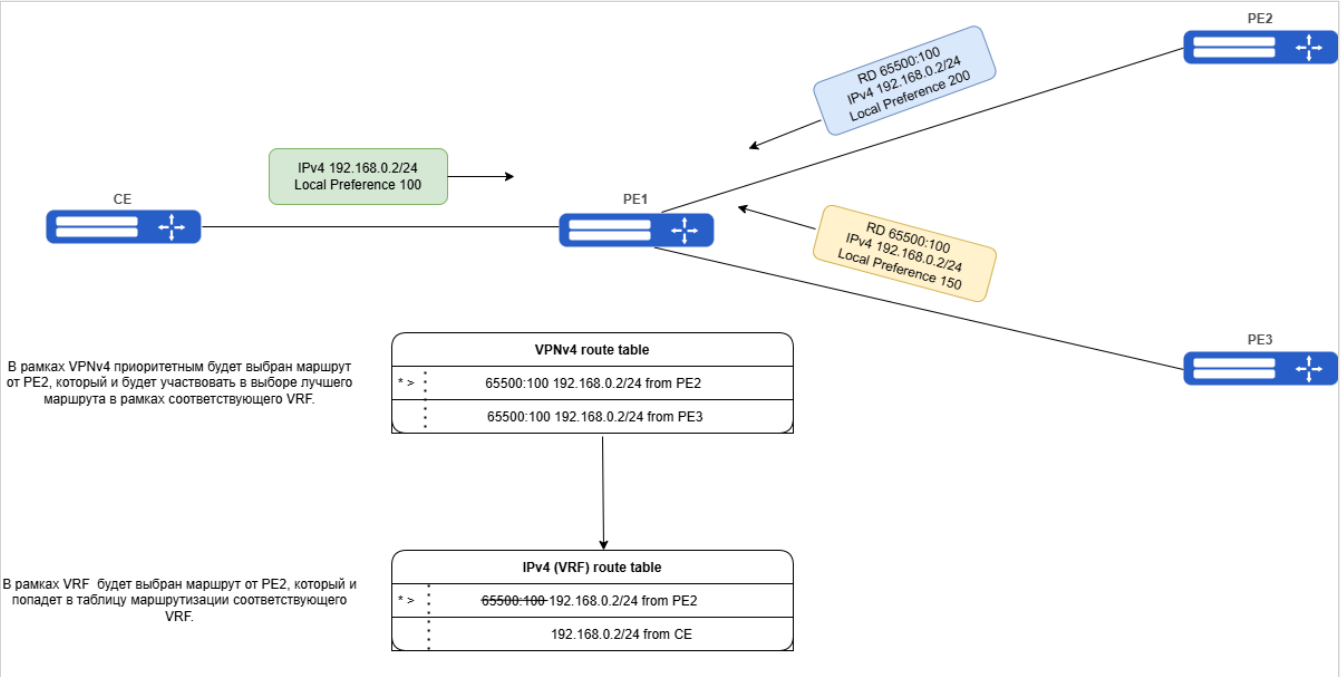
В процессе работы BGP обычно вычисляет один лучший маршрут до каждой полученной подсети. Если нет более приоритетного маршрута, полученного при помощи другого протокола маршрутизации до этой подсети, то маршрут устанавливается в таблицу маршрутизации.

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

Ниже приведен алгоритм выбора лучшего маршрута в протоколе BGP:

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

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



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

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

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

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

```
ESR# show bgp ipv4 unicast 192.0.2.0/24
192.0.2.0/24 via 100.64.28.1 on gi1/0/1.2800   [bgp65514 2022-05-22] (65041i)
    Administrative Distance: 170
    Type:                    unicast
    Origin:                  IGP
    AS PATH:                 65054 65055 65056 65077 65098 65059
    Next Hop:                100.64.28.1
    Local Preference:        100
    Community:               (3356:2) (3356:22) (3356:86) (3356:501) (3356:666) (3356:903)
(3356:2065)
                             (12389:6) (65000:64990)
    Weight:                  0
    Valid
192.0.2.0/24 via 101.7.0.1 on gi1/0/1.2800   [bgp65514 2022-05-22] (65041i)
    Administrative Distance: 170
    Type:                    unicast
    Origin:                  IGP
    AS PATH:                 65020 65030
    Next Hop:                101.7.0.1
    Local Preference:        200
    Community:               (3356:2) (3356:22) (3356:86) (3356:501) (3356:666) (3356:903)
(3356:2065)
                             (12389:6) (65000:64990)
    Weight:                  0
    Valid,Best
```

11.7.4 Условное анонсирование маршрутной информации (Conditional Advertisement)

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

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

Для работы Conditional advertisement необходимо выполнить следующие шаги:

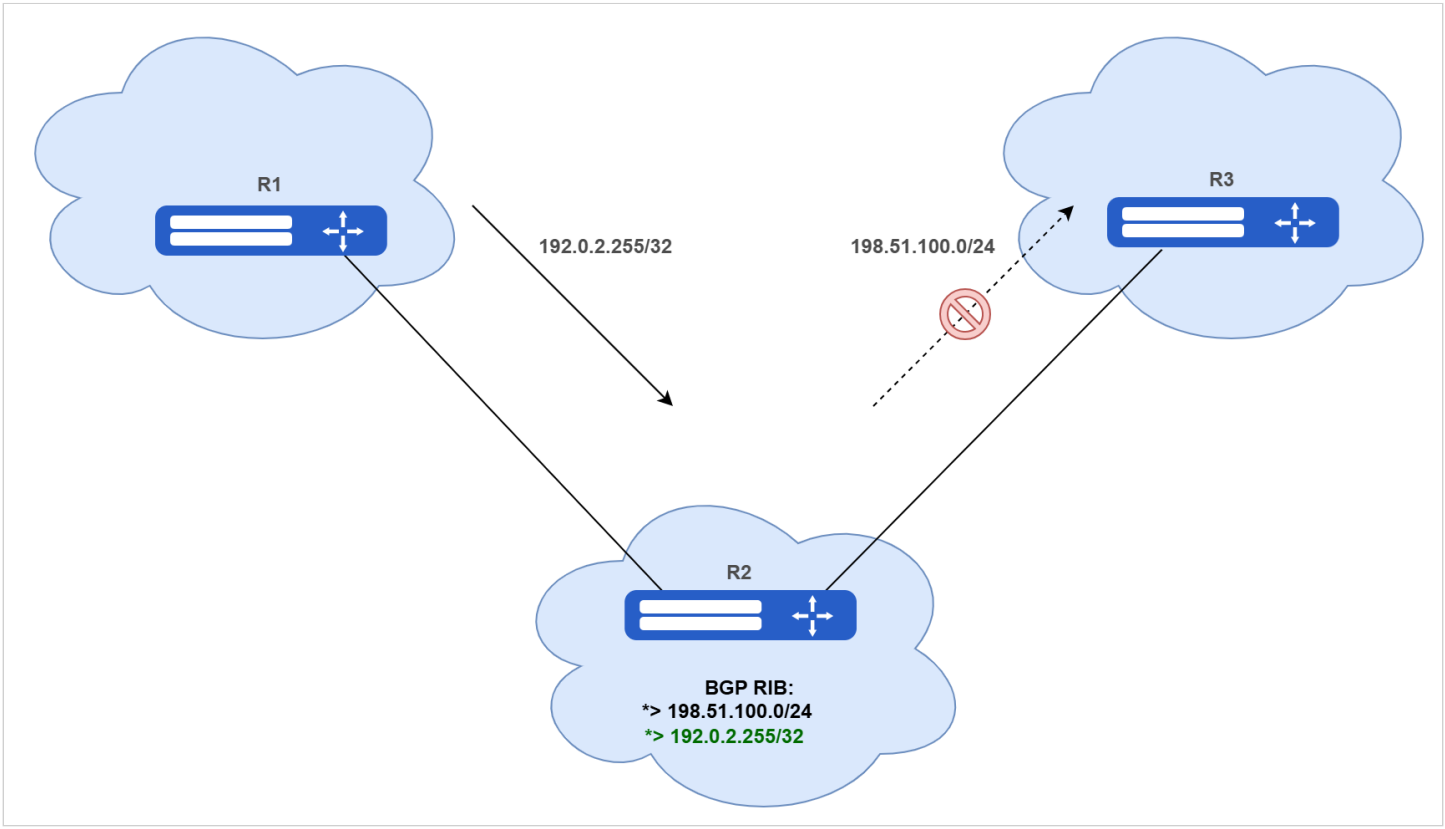
1. Описать маршрутные карты condition-map и advertise-map:

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

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

Условие EXIST-MAP:

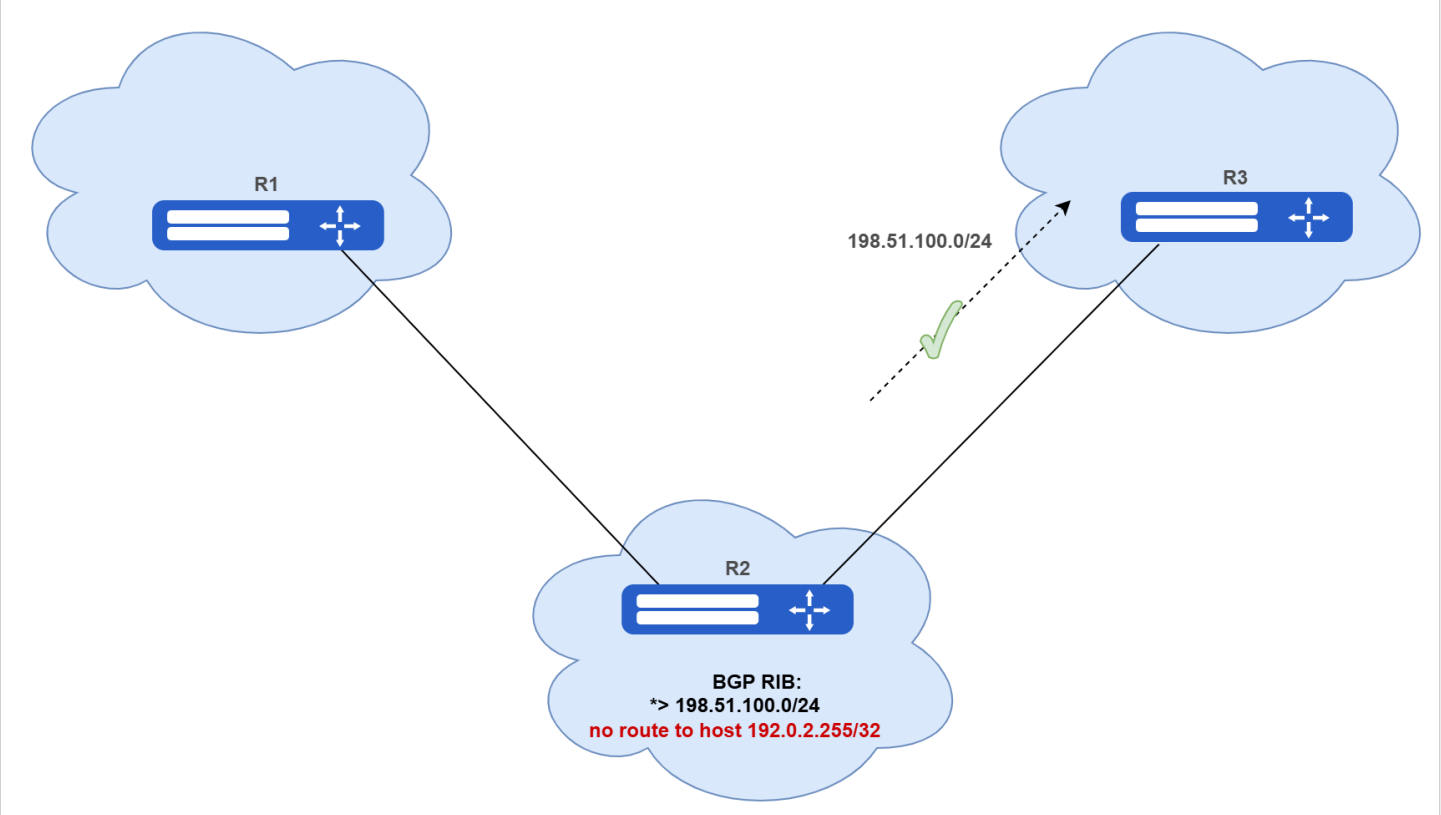
- Если R2 содержит в BGP RIB маршрут 192.0.2.255/32, то R2 анонсирует в сторону R3 маршрут 198.51.100.0/24 (пример на рисунке ниже);
- Если R2 не содержит в BGP RIB маршрут 192.0.2.255/32, то анонсирование маршрута 198.51.100.0/24 соседу R3 не происходит.



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

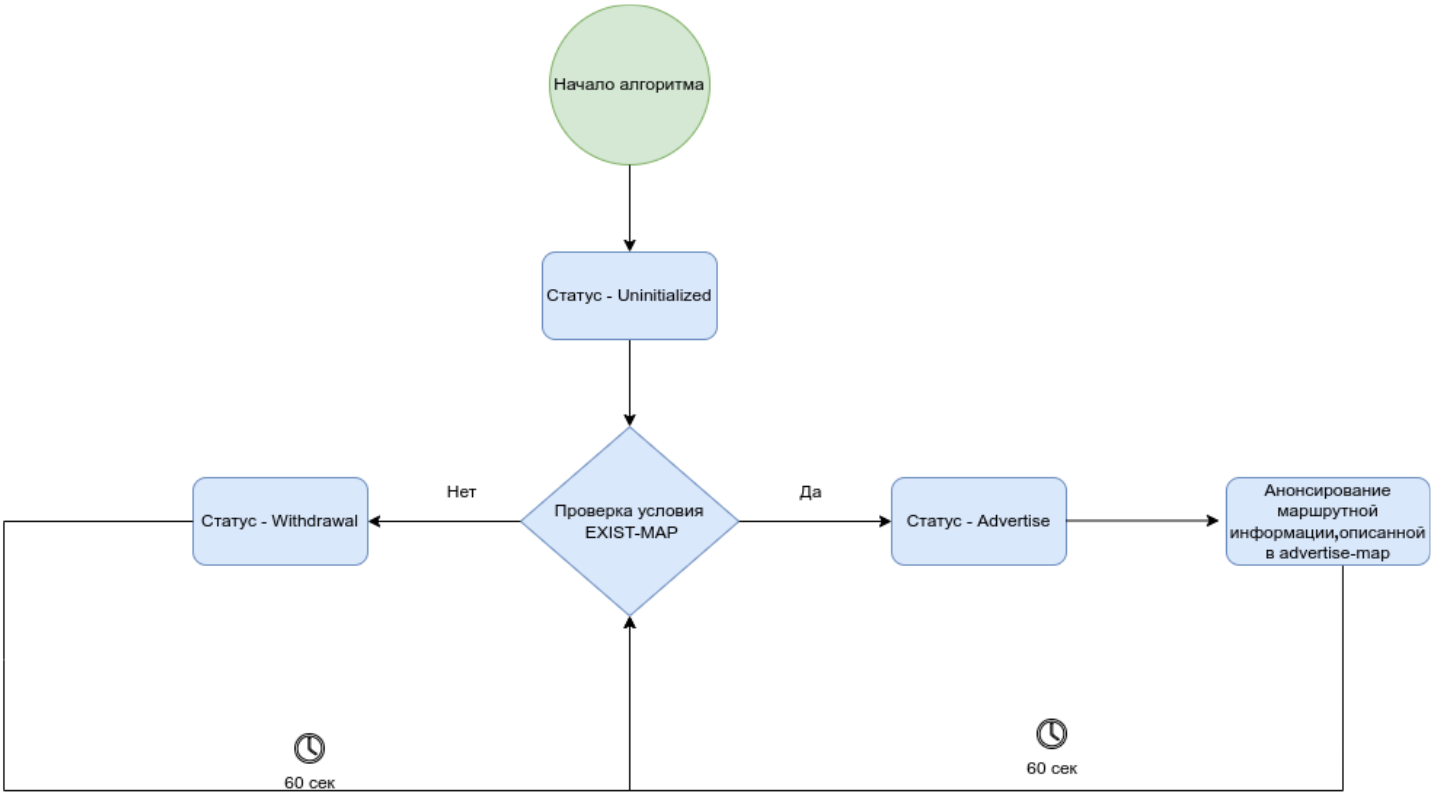
Условие not EXIST-MAP:

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



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

Ниже приведена диаграмма состояний для условия EXIST-MAP:



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

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

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

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

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

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

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

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

// Вывод атрибутов BGP маршрута после прохождения всех политик:
show bgp ipv4 unicast 10.100.0.255/32
Administrative Distance: 170
Type: unicast
Origin: Incomplete
AS path: --
Next Hop: 192.168.1.1
Output Label: --
Input Label: imp-null
Local Preference: 200
MED: 78
Cluster List: --
Community: 65:65
EXT Community: --
Weight: --
```

Алгоритм настройки

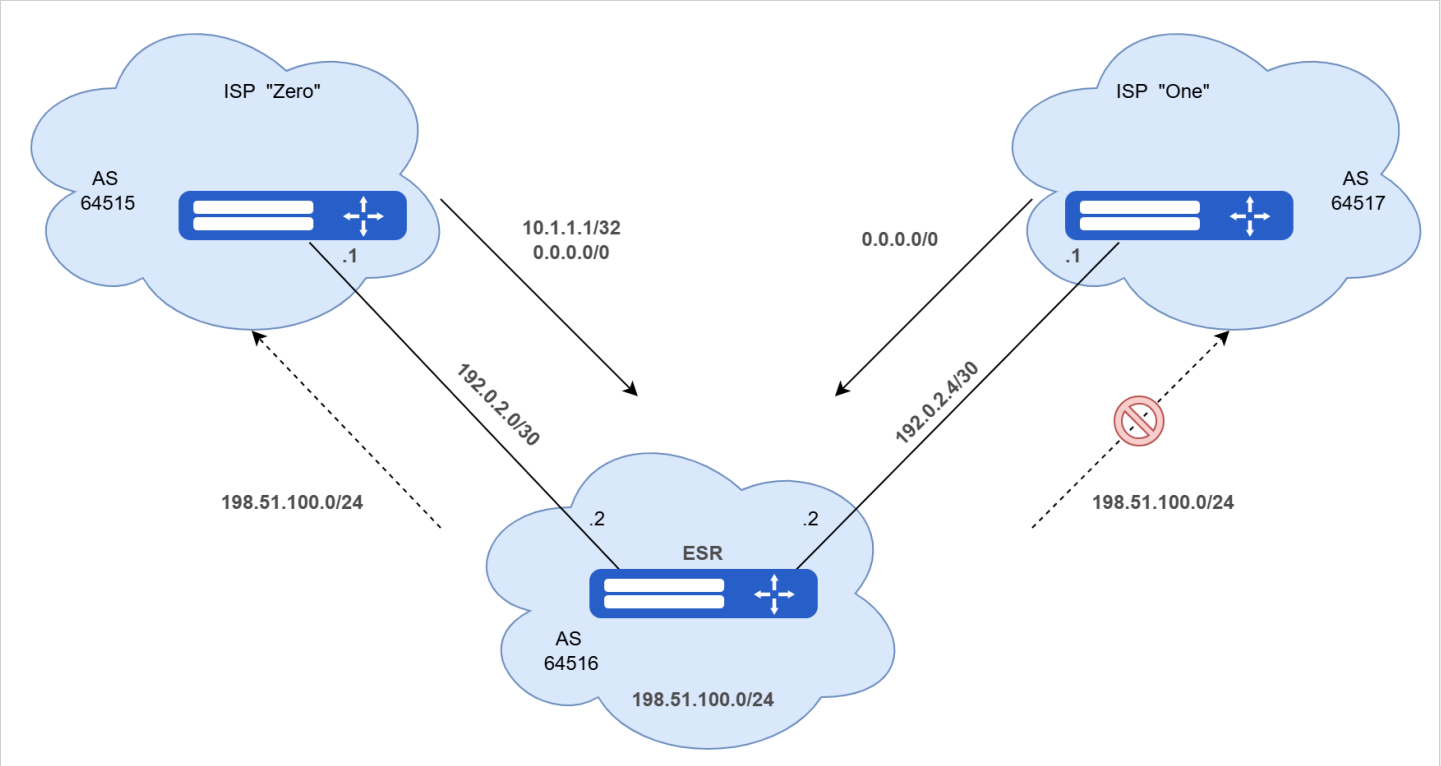
Шаг	Описание	Команда	Ключ
1	Настроить протокол BGP (см. раздел Настройка BGP).		
2	Создать advertise-map, описав в нем список подсетей для дальнейшего анонсирования.	**esr(config)# route-map <ADVERTISE>**	<ADVERTISE> – имя конфигурируемых правил маршрутизации, задаётся строкой до 31 символа.
3	Создать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

Пример настройки

Задача:

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

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



Решение:

Сконфигурируем необходимые сетевые интерфейсы на каждом устройстве в сети:

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

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

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

Произведем настройку BGP:

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

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

```
ISP-ONE(config)# ip route 0.0.0.0/0 blackhole
ISP-ONE(config)# route-map OUT
ISP-ONE(config-route-map)# rule 1
ISP-ONE(config-route-map-rule)# exit
ISP-ONE(config-route-map)# exit
ISP-ONE(config)# router bgp 64517
ISP-ONE(config-bgp)# neighbor 192.0.2.5
ISP-ONE(config-bgp-neighbor)# address-family ipv4 unicast
ISP-ONE(config-bgp-neighbor-af)# route-map OUT out
ISP-ONE(config-bgp-neighbor-af)# enable
ISP-ONE(config-bgp-neighbor-af)# exit
ISP-ONE(config-bgp-neighbor)# remote-as 64516
ISP-ONE(config-bgp-neighbor)# enable
ISP-ONE(config-bgp-neighbor)# exit
ISP-ONE(config-bgp)# enable
ISP-ONE(config-bgp)# address-family ipv4 unicast
ISP-ONE(config-bgp-af)# redistribute static
ISP-ONE(config-bgp-af)# do commit
ISP-ONE(config-bgp-af)# do confirm
```

Опишем advertise и condition maps на ESR:

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

Активируем функцию Conditional advertisement, применив ранее созданные маршрутные карты:

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

Проверим корректность настройки:

```
//Проверяем наличие маршрута 10.1.1.1/32 в BGP RIB

ESR# sh bgp ipv4 unicast 10.1.1.1/32
10.1.1.1/32        via 192.0.2.1 on gi1/0/1          [bgp64516 07:07:59] (64515?)
    Administrative Distance: 170
    Type:                    unicast
    Origin:                  Incomplete
    AS path:                 64515
    Next Hop:                192.0.2.1
    Output Label:            --
    Input Label:             --
    Local Preference:        100
    MED:                     --
    Cluster List:            --
    Community:               --
    EXT Community:           --
    Weight:                  0
    Valid, Best
// Проверяем статус conditional advertisement и отсутствие анонса 198.51.100.0/24 провайдеру
 ISP "One"
ESR# sh bgp ipv4 unicast neighbor 192.0.2.6 advertise-routes

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

Настройка завершена.

11.7.5 Быстрая деактивация пиринговых сессий

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

Метод на основе протокола BFD

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

По умолчанию BFD-сессия устанавливается в следующем режиме:

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

Алгоритм настройки

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

Пример настройки

Задача:

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



Решение:

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

```
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
```

Следующим шагом на R1 настроим eBGP и включим BFD:

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

На 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
```

Далее на R2 настроим eBGP и включим BFD:

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

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

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

esrv#  sh bfd neighbors 10.0.0.2
Neighbor address:                   10.0.0.2
Local address:                      10.0.0.1
Interface:                          gi1/0/1
Remote discriminator:               889907056
Local discriminator:                924658435
State:                              Up
Session type:                       Control
Session mode:                       Single-hop
Local diagnostic code:              No Diagnostic
Remote diagnostic code:             No Diagnostic
Minimal Tx Interval:                300 ms
Minimal Rx Interval:                300 ms
Multiplier:                         5
Actual Tx Interval:                 300 ms
Actual Detection Interval:          1500 ms
Number of transmitted packets:      257
Number of received packets:         156
Uptime (d,h:m:s):                   00,00:00:38
Client:                             BGP
Last received packet:
    Desired Min Tx Interval:        200 ms
    Required Min Rx Interval:       200 ms
    Multiplier:                     5
```

Метод на основе Fast Peer Deactivation (Fall-over)

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

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

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

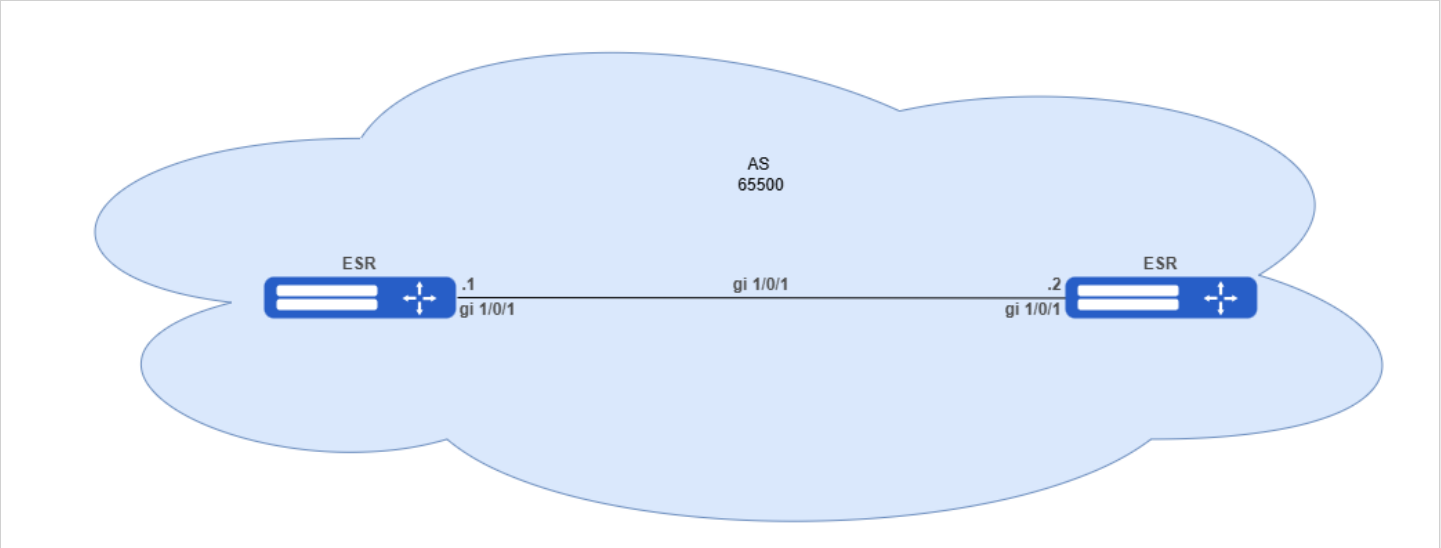
Алгоритм настройки

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

Пример настройки

Задача:

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



Решение:

Предварительно настроим связность между маршрутизаторами в схеме:

R1

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

R2

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

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

R1

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

R2

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

Настроим протокол BGP на обоих маршрутизаторах:

R1

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

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

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

R1

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

R2

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

Привяжем созданные маршрутные карты в контексте настройки BGP-пира:

R1

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

R2

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

Для просмотра оперативного состояния можно воспользоваться следующей командой:

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

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

Настройка завершена.

11.7.6 Настройка политик маршрутизации Route-map

Route-map – это механизм, позволяющий применять условия (условные фильтры) и действия к маршрутам и ,соответственно, к трафику. Он используется для фильтрации, изменения и управления атрибутами протокола BGP, обеспечивая расширенные возможности по сравнению с Prefix-list. Подробная логика работы описана в разделе Политика фильтрации маршрутной информации.

Функциональные возможности Route-map позволяют работать со следующими атрибутами:

Название	Семейство адресов (AF)	Манипуляции		Поддержка регулярных выражений в классификации
		Тип действия	Поддержка трекинга	
As-path	IPv4, IPv6, VPNv4, L2VPN, Flowspec	Prepend, Replace	⊕	⊕
Community	Pv4, IPv6, VPNv4, L2VPN, Flowspec	no-advertise, no-export, добавление в атрибута (add), создание списка (set)	⊕	⊕
Extended community	VPNv4, L2VPN	Добавление в список (add), создание списка (set)	⊕	⊕

Название	Семейство адресов (AF)	Манипуляции		Поддержка регулярных выражений в классификации
		Тип действия	Поддержка трекинга	
Local preference	IPv4, IPv6, VPNv4, L2VPN, Flowspec	Установка атрибута, увеличение, уменьшение	⊕	⊕
MED (metric)	IPv4, IPv6, VPNv4, L2VPN, Flowspec	Установка атрибута, увеличение, уменьшение	⊕	⊕
Next-hop	IPv4, IPv6, VPNv4, L2VPN, Flowspec	Установка атрибута	⊖	⊖
Origin	IPv4, IPv6, VPNv4, L2VPN, Flowspec	Установка атрибута	⊕	⊖
Weight	IPv4, IPv6, VPNv4, L2VPN, Flowspec	Установка атрибута, увеличение, уменьшение	⊖	⊕

Алгоритм настройки

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

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

Шаг	Описание	Команда	Ключи
6	Задать значение атрибута BGP Extended Community, для которого должно срабатывать правило (необязательно).	**esr(config-route-map-rule)# match extcommunity { <EXTCOMMUNITY-LIST> | regex <REGEX> }**	<EXTCOMMUNITY-LIST> – список extcommunity, задается в виде KIND:AS:N, KIND:AS:N, где KIND – тип extcommunity: • **rt** (Route Target); • **ro** (Route Origin). N – номер extcommunity, принимает значения [1..65535]. • **regex** – значение атрибута соответствует регулярному выражению. <REGEX> – регулярное выражение, задаётся по стандарту POSIX-Extended Regular Expressions.
7	Задать профиль IP-адресов, содержащий значения подсетей назначения в маршруте (необязательно).	**esr(config-route-map-rule)# match ip address object-group <OBJ-GROUP-NETWORK-NAME>**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, содержащего префиксы подсетей назначения, задаётся строкой до 31 символа.
		esr(config-route-map-rule)# match ipv6 address object-group <OBJ-GROUP-NETWORK-NAME>	
8	Задать профиль IP-адресов, содержащий значения атрибута BGP Next-Hop в маршруте для которого должно срабатывать правило (необязательно).	**esr(config-route-map-rule)# match ip bgp next-hop object-group <OBJ-GROUP-NETWORK-NAME>**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, содержащего префиксы подсетей назначения, задается строкой до 31 символа.
		esr(config-route-map-rule)# match ipv6 bgp next-hop object-group <OBJ-GROUP-NETWORK-NAME>	
9	Задать профиль, содержащий IP-адреса маршрутизатора, анонсировавшего маршрут, для которого должно срабатывать правило (необязательно).	**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 (необязательно).	**esr(config-route-map-rule)# match access-group <NAME>**	<NAME> – имя списка контроля доступа, задается строкой до 31 символа.

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

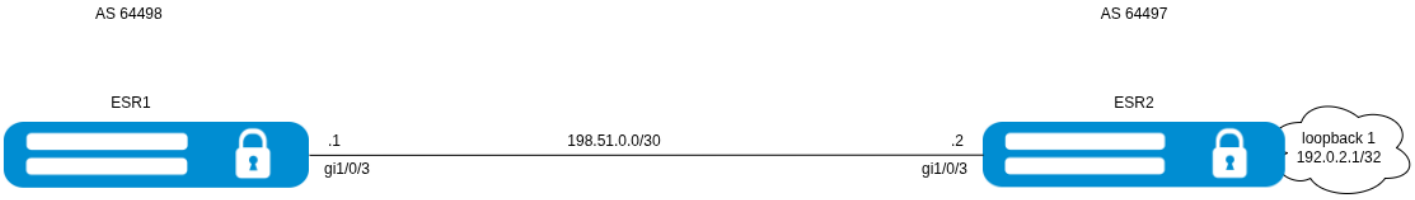
Шаг	Описание	Команда	Ключи
16	Задать атрибут BGP Next-Hop, который будет установлен в маршруте при анонсировании (необязательно).	**esr(config-route-map-rule)# action set ip bgp-next-hop <ADDR>**	<ADDR> – IP-адрес шлюза, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
		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].
17	Задать значение атрибута BGP Local Preference, который будет установлен в маршруте (необязательно).	**esr(config-route-map-rule)# action set local-preference <PREFERENCE>**	<PREFERENCE> – значение атрибута BGP Local Preference, принимает значения [0..255].
18	Задать значение атрибута BGP Origin, которое будет установлено в маршруте (необязательно).	**esr(config-route-map-rule)# action set origin <ORIGIN>**	<ORIGIN> – значение атрибута BGP Origin: • **egp** – маршрут выучен по протоколу EGP; • **igp** – маршрут получен внутри исходной AS; • **incomplete** – маршрут выучен другим образом.
19	Задать значение BGP MED, которое будет установлено в маршруте (необязательно).	**esr(config-route-map-rule)# action set metric bgp <METRIC>**	<METRIC> – значение атрибута BGP MED, принимает значения [0..4294967295].
20	Добавить фильтрацию и модификацию маршрутов во входящих или исходящих направлениях.	**esr(config-bgp-neighbor)# route-map <NAME><DIRECTION>**	<NAME> – имя сконфигурированной маршрутной карты; <DIRECTION> – направление: • **in** – фильтрация и модификация получаемых маршрутов; • **out** – фильтрация и модификация анонсируемых маршрутов.
		esr(config-ipv6-bgp-neighbor)# route-map <NAME><DIRECTION>	

Пример настройки 1

Задача:

Назначить community для маршрутной информации, приходящей из AS 64498.

Схема:



Базовая конфигурация:

ESR1

```
security zone Untrusted
exit
router bgp 64498
  neighbor 198.51.100.2
    remote-as 64497
    address-family ipv4 unicast
      enable
    exit
    enable
  exit
  enable
exit

interface gigabitethernet 1/0/3
  security-zone Untrusted
  ip address 198.51.100.1/30
exit

security zone-pair Untrusted self
  rule 1
    action permit
    match protocol tcp
    match destination-port port-range 179
    enable
  exit
  rule 2
    action deny
    enable
  exit
exit
```

ESR2

```
security zone Untrusted
exit

route-map BGP
  rule 1
    match ip address 192.0.2.1/32
  exit
exit

router bgp 64497
  neighbor 198.51.100.1
    remote-as 64498
    address-family ipv4 unicast
      route-map BGP out
      enable
    exit
    enable
  exit
  address-family ipv4 unicast
    network 192.0.2.1/32
  exit
  enable
exit

interface gigabitethernet 1/0/3
  security-zone Untrusted
  ip address 198.51.100.2/30
exit
interface loopback 1
  ip address 192.0.2.1/32
exit

security zone-pair Untrusted self
  rule 1
    action permit
    match protocol tcp
    match destination-port port-range 179
    enable
  exit
  rule 2
    action deny
    enable
  exit
exit
```

Решение:

Создаем политику на ESR1:

```
ESR1# config
ESR1(config)# route-map set_community
```

Создаем правило 1:

```
ESR1(config-route-map)# rule 1
```

Если AS PATH содержит AS 64497, то назначаем ему community 64497:100, выходим и применяем конфигурацию:

```
ESR1(config-route-map-rule)# match as-path contain 64497
ESR1(config-route-map-rule)# action set community 64497:100
ESR1(config-route-map-rule)# exit
ESR1(config-route-map)# exit
ESR1(config)# do com
Configuration has been successfully applied and saved to flash. Commit timer started, changes
will be reverted in 600 seconds.
ESR1(config)# do conf
Configuration has been confirmed. Commit timer canceled.
```

Проверяем, что политика была создана:

ESR1

```
ESR1# sh ip route-map set_community
Order:                                  1
Description:                            --
Matching pattern:
    Access group                            --
    AS path                                 contains 64497
    Community                               --
    Extcommunity                            --
    BGP local-preference:                   --
    BGP metric (MED):                       --
    BGP weight:                             --
    Address (object-group):                 --
    Next hop (object-group):                --
    Route source (object-group):            --
    RIP metric                              --
    RIP tag                                 --
    OSPF metric type                        --
    OSPF metric                             --
    OSPF tag                                --
Actions:
    Decision:                               Permit
    Route next hop:                         --
    Route IPv6 next hop:                    --
    IP address:                             --
    IPv6 address:                           --
    AS path (prepand):                      --
    Community:                              64497:100
    Extcommunity:                           --
    Local preference:                       --
    BGP next hop address:                   --
    BGP IPv6 next hop address:              --
    BGP metric (MED):                       --
    BGP weight:                             --
    Origin:                                 --
    RIP metric                              --
    RIP tag                                 --
    OSPF metric type                        --
    OSPF metric                             --
    OSPF tag                                --
------------------------------------------------------------------------------
```

В контексте настройки BGP-инстанса заходим в настройки параметров соседа:

```
ESR1(config)# router bgp 64498
ESR1(config-bgp)# neighbor 198.51.100.2
ESR1(config-bgp-neighbor)# address-family ipv4 unicast
```

Привязываем политику к принимаемой маршрутной информации:

```
ESR1(config-bgp-neighbor-af)# route-map set_community in
ESR1(config-bgp-neighbor-af)# do com
ESR1(config-bgp-neighbor-af)# do conf
```

Проверяем, что для полученного префикса установлена необходимая community:

ESR1

```
ESR1# show bgp ipv4 unicast 192.0.2.1/32
192.0.2.1/32       via 198.51.100.2 on gi1/0/3       [bgp64498 08:44:32] (64497i)
    Administrative Distance: 170
    Type:                    unicast
    Origin:                  IGP
    AS path:                 64497
    Next Hop:                198.51.100.2
    Output Label:            --
    Input Label:             --
    Local Preference:        100
    MED:                     --
    Cluster List:            --
    Community:               64497:100
    EXT Community:           --
    Weight:                  0
    Valid, Best
```

Настройка завершена.

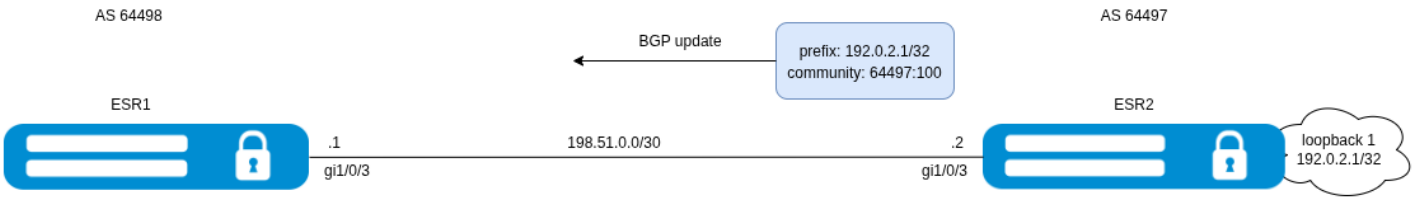
Пример настройки 2

Задача:

Для всей полученной маршрутной информации (с community 64497:100) от ESR2 установить следующие BGP-атрибуты:

- MED – 240;
- Origin – EGP.

Схема:



Базовая конфигурация:

ESR1

ESR1

```
security zone Untrusted
exit

route-map set_community
  rule 1
    match as-path contain 64497
    action set community 64497:100
  exit
exit

router bgp 64498
  neighbor 198.51.100.2
    remote-as 64497
    address-family ipv4 unicast
      enable
    exit
    enable
  exit
  enable
exit

interface gigabitethernet 1/0/3
  security-zone Untrusted
  ip address 198.51.100.1/30
exit

security zone-pair Untrusted self
  rule 1
    action permit
    match protocol tcp
    match destination-port port-range 179
    enable
  exit
  rule 2
    action deny
    enable
  exit
exit
```

ESR2

ESR2

```
security zone Untrusted
exit

route-map BGP
  rule 1
    match ip address 192.0.2.1/32
    action set community 64497:100
  exit
exit

router bgp 64497
  neighbor 198.51.100.1
    remote-as 64498
    address-family ipv4 unicast
      route-map BGP out
      enable
    exit
    enable
  exit
  address-family ipv4 unicast
    network 192.0.2.1/32
  exit
  enable
exit

interface gigabitethernet 1/0/3
  security-zone Untrusted
  ip address 198.51.100.2/30
exit
interface loopback 1
  ip address 192.0.2.1/32
exit

security zone-pair Untrusted self
  rule 1
    action permit
    match protocol tcp
    match destination-port port-range 179
    enable
  exit
  rule 2
    action deny
    enable
  exit
exit
```

Решение:

Для решения задачи настройка будет производиться на ESR1. Первым шагом создаем политику:

```
ESR1(config)# route-map community_in
```

Далее правило:

```
ESR1(config-route-map)# rule 1
```

Если community содержит 64497:100, то назначаем ему MED 240 и Origin EGP:

```
ESR1(config)# route-map community_in
ESR1(config-route-map)# rule 1
ESR1(config-route-map-rule)#
ESR1(config-route-map-rule)# match community 64497:100
ESR1(config-route-map-rule)# action set metric bgp 240
ESR1(config-route-map-rule)# action set origin egp
ESR1(config-route-map-rule)# do com
Configuration has been successfully applied and saved to flash. Commit timer started, changes
will be reverted in 600 seconds.
ESR1(config-route-map-rule)# do conf
```

Проверим, что политика создана корректно:

ESR1

```
ESR1# sh ip route-map community_in
Order:                                  1
Description:                            --
Matching pattern:
    Access group                            --
    AS path                                 --
    Community                               64497:100
    Extcommunity                            --
    BGP local-preference:                   --
    BGP metric (MED):                       --
    BGP weight:                             --
    Address (object-group):                 --
    Next hop (object-group):                --
    Route source (object-group):            --
    RIP metric                              --
    RIP tag                                 --
    OSPF metric type                        --
    OSPF metric                             --
    OSPF tag                                --
Actions:
    Decision:                               Permit
    Route next hop:                         --
    Route IPv6 next hop:                    --
    IP address:                             --
    IPv6 address:                           --
    AS path (prepand):                      --
    Community:                              --
    Extcommunity:                           --
    Local preference:                       --
    BGP next hop address:                   --
    BGP IPv6 next hop address:              --
    BGP metric (MED):                       set 240
    BGP weight:                             --
    Origin:                                 EGP
    RIP metric                              --
    RIP tag                                 --
    OSPF metric type                        --
    OSPF metric                             --
    OSPF tag                                --
------------------------------------------------------------------------------
```

В контексте настройки BGP-инстанса заходим в настройки параметров соседа:

```
ESR1(config)# router bgp 64498
ESR1(config-bgp)# neighbor 198.51.100.2
ESR1(config-bgp-neighbor)# address-family ipv4 unicast
```

Привязываем политику для получаемой маршрутной информации:

```
ESR1(config-bgp-neighbor-af)# route-map community_in in
ESR1(config-bgp-neighbor-af)# do com
ESR1(config-bgp-neighbor-af)# do conf
```

Проверим, что соответствующие атрибуты были изменены:

ESR1

```
ESR1# sh bgp ipv4 unicast 192.0.2.1/32
192.0.2.1/32       via 198.51.100.2 on gi1/0/3       [bgp64498 09:19:24] (64497e)
    Administrative Distance: 170
    Type:                    unicast
    Origin:                  EGP
    AS path:                 64497
    Next Hop:                198.51.100.2
    Output Label:            --
    Input Label:             --
    Local Preference:        100
    MED:                     240
    Cluster List:            --
    Community:               64497:100
    EXT Community:           --
    Weight:                  0
    Valid, Best
```

Настройка завершена.

Использование регулярных выражений

Начиная с версии 1.23 доступно использование регулярных выражений в Route-map для контроля распространения маршрутной информации по протоколу BGP. Контроль можно производить по шести атрибутам BGP: AS-path, community, extcommunity, local-preference, metric, weight. Синтаксис регулярных выражений соответствует стандарту POSIX ERE. В таблице ниже представлены некоторые примеры регулярных выражений.

Условие совпадения	Регулярное выражение
Маршруты с любым содержимым AS-path	.*
Маршруты с пустым AS-path	^$
Маршруты с одной любой AS в AS-path	^[0-9]+$
Маршруты с двумя любыми AS в AS-path	^[0-9]+ [0-9]+$
Маршруты, зарождённые в AS 15	(^|.*)15$
Маршруты, полученные из AS 20	^20(.*|$)
Маршруты, проходящие через AS 22	.* 22 .*

Условие совпадения	Регулярное выражение
Маршруты, проходящие через AS 30, а затем через AS 22	.* 22 30 .*
Маршруты, проходящие через AS 30 или AS 43	.* (30|43) .*
Маршруты, зарождённые в AS 66 и проходящие через AS 60	.* 60 (.*)*66$
Маршруты, зарождённые в AS 70 или проходящие через неё	.* 70(.*|$)
Маршруты, содержащие приватные AS в AS-path	(^|.*)((6451[2-9])|(645[2-9][0-9])|(64[6-9][0-9]{2})|(65[0-4][0-9]{2})|(655[0-2][0-9])|(6553[0-4]))(.*|$)
Номер AS 100, номер community 200	^100:200$
Номера AS 112 или 232, любой номер community	^(112|232):[0-9]*$
Номер AS 277, номер community начинается с 3	^277:3[0-9]*$
Любой номер AS, номер community в диапазоне 150-1230	^([0-9]*):((1[5-9][0-9])|([2-9][0-9]{2})|(1[0-2][0-2][0-9])|(1230))$
Тип route target, IP-адрес 10.10.10.1, номер extcommunity 653 и 654	^rt:10\.10\.10\.1:65[34]$

Алгоритм настройки

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

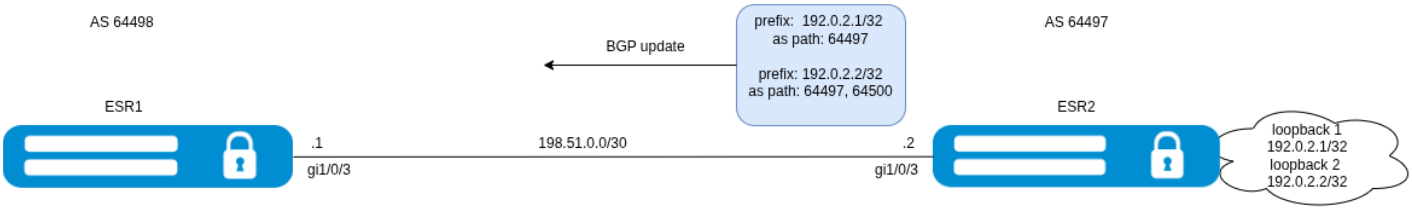
Шаг	Описание	Команда	Ключи
4	Задать значение BGP AS-Path, Community,Extended Community, Local-preference, Metric, Weight в маршруте, для которого должно срабатывать правило (необязательно).	**esr(config-route-map-rule)# match as-path { [begin | contain | end] <AS-PATH> | empty | regex <REGEX> }**	**regex** – значение атрибута соответствует регулярному выражению. <REGEX> – регулярное выражение, задаётся по стандарту POSIX-Extended Regular Expressions.
		esr(config-route-map-rule)# match community { <COMMUNITY-LIST> | regex <REGEX> }	
		esr(config-route-map-rule)# match extcommunity { <EXTCOMMUNITY-LIST> | regex <REGEX> }	
		esr(config-route-map-rule)# match local-preference { <VALUE> | regex <REGEX> }	
		esr(config-route-map-rule)# match metric bgp { <VALUE> | regex <REGEX> }	
		esr(config-route-map-rule)# match weight bgp { <VALUE> | regex <REGEX> }	
5	Описать дополнительные условия для выбора и действие (см. раздел Настройка политик маршрутизации Route-map).		
6	Применить созданный Route-map в контексте настройки BGP peer, peer-group, address-family.	**esr(config-bgp-neighbor)# route-map <NAME><DIRECTION>**	<NAME> – имя сконфигурированной маршрутной карты; • **in** – фильтрация и модификация получаемых маршрутов; • **out** – фильтрация и модификация анонсируемых маршрутов.
		esr(config-ipv6-bgp-neighbor)# route-map <NAME><DIRECTION>	

Пример настройки

Задача:

Запретить прием маршрутной информации по BGP, содержащей в атрибуте AS-path номер AS 64500.

Схема:



Базовая конфигурация:

ESR1

```
security zone Untrusted
exit

interface gigabitethernet 1/0/1
  security-zone Untrusted
  ip address 198.51.100.1/30
exit
interface loopback 1
  ip address 192.0.2.1/32
exit

security zone-pair Untrusted self
  rule 1
    action permit
    match protocol tcp
    match destination-port port-range 179
    enable
  exit
  rule 2
    action deny
    enable
  exit
exit
```

ESR2

```
security zone Untrusted
exit
security zone Trusted
exit

interface gigabitethernet 1/0/1
  security-zone Untrusted
  ip address 198.51.100.2/30
exit
interface gigabitethernet 1/0/2
  security-zone Trusted
  ip address 203.0.113.1/30
exit

security zone-pair Untrusted self
  rule 1
    action permit
    match protocol tcp
    match destination-port port-range 179
    enable
  exit
  rule 2
    action deny
    enable
  exit
exit
security zone-pair Trusted self
  rule 1
    action permit
    match protocol tcp
    match destination-port port-range 179
    enable
  exit
  rule 2
    action deny
    enable
  exit
exit
```

ESR3

```
security zone Trusted
exit

interface gigabitethernet 1/0/2
  security-zone Trusted
  ip address 203.0.113.2/30
exit
interface loopback 1
  ip address 192.0.2.2/32
exit

security zone-pair Trusted self
  rule 1
    action permit
    match protocol tcp
    match destination-port port-range 179
    enable
  exit
  rule 2
    action deny
    enable
  exit
exit
```

Решение:

Первым шагом необходимо создать Route-map на ESR1, в котором с помощью регулярных выражений опишем интересующий AS-path. В случае совпадения укажем – запретить:

ESR1

```
route-map AS
  rule 1
    match as-path regex '(64500)'
    action deny
  exit
  rule 2
  exit
exit
```

Проверим корректность ранее созданного Route-map:

ESR1

```
ESR1# sh ip route-map AS
Order:                                  1
Description:                            --
Matching pattern:
    Access group                            --
    AS path                                 regex "(64500)"
    Community                               --
    Extcommunity                            --
    BGP local-preference:                   --
    BGP metric (MED):                       --
    BGP weight:                             --
    Address (object-group):                 --
    Next hop (object-group):                --
    Route source (object-group):            --
    RIP metric                              --
    RIP tag                                 --
    OSPF metric type                        --
    OSPF metric                             --
    OSPF tag                                --
Actions:
    Decision:                               Deny
    Route next hop:                         --
    Route IPv6 next hop:                    --
    IP address:                             --
    IPv6 address:                           --
    AS path (prepand):                      --
    Community:                              --
    Extcommunity:                           --
    Local preference:                       --
    BGP next hop address:                   --
    BGP IPv6 next hop address:              --
    BGP metric (MED):                       --
    BGP weight:                             --
    Origin:                                 --
    RIP metric                              --
    RIP tag                                 --
    OSPF metric type                        --
    OSPF metric                             --
    OSPF tag                                --
------------------------------------------------------------------------------
Order:                                  2
Description:                            --
Matching pattern:
    Access group                            --
    AS path                                 --
    Community                               --
    Extcommunity                            --
    BGP local-preference:                   --
    BGP metric (MED):                       --
    BGP weight:                             --
    Address (object-group):                 --
    Next hop (object-group):                --
    Route source (object-group):            --
    RIP metric                              --
    RIP tag                                 --
    OSPF metric type                        --
    OSPF metric                             --
```

```
    OSPF tag                                --
Actions:
    Decision:                               Permit
    Route next hop:                         --
    Route IPv6 next hop:                    --
    IP address:                             --
    IPv6 address:                           --
    AS path (prepand):                      --
    Community:                              --
    Extcommunity:                           --
    Local preference:                       --
    BGP next hop address:                   --
    BGP IPv6 next hop address:              --
    BGP metric (MED):                       --
    BGP weight:                             --
    Origin:                                 --
    RIP metric                              --
    RIP tag                                 --
    OSPF metric type                        --
    OSPF metric                             --
    OSPF tag                                --
------------------------------------------------------------------------------
```

В контексте настройки пира применим созданный Route-map для фильтрации входящих маршрутов:

ESR1

```
ESR1(config)# router bgp 64498
ESR1(config-bgp)# neighbor 198.51.100.2
ESR1(config-bgp-neighbor)# address-family ipv4 unicast
ESR1(config-bgp-neighbor-af)# route-map AS in
ESR1(config-bgp-neighbor-af)# do com
ESR1(config-bgp-neighbor-af)# do conf
```

Проверим, что BGP RIB не содержит маршрут, в котором AS-path 64500:

ESR1

```
ESR1# sh bgp ipv4 unicast
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 192.0.2.1/32         198.51.100.2         --      100         0      64497 i
```

Настройка завершена.

11.7.7 Конфедерация

Механизм позволяет разделить одну автономную систему на множество под-AS, фIS-IS — протокол динамической маршрутизации, стандартизированный ISO, ункционирующих как отдельные административные единицы, но представляющих единую AS для внешних автономных систем. Взаимодействие между под-AS осуществляется посредством межконфедерационных BGP-сессий, использующих расширенную семантику AS_PATH. Для реализации механизма в рамках RFC 5065 введены атрибуты AS_CONFED_SEQUENCE и AS_CONFED_SET, которые применяются исключительно внутри конфедерации и подлежат удалению перед передачей маршрутов за её пределы.

Ограничения

1. При работе с атрибутом AS-PATH в route-map будет использован AS_SEQUENCE/AS_SET;
2. Для корректной работы с динамическими соседями (listen-range) необходимо, чтобы все AS, описанные в as-range, входили в диапазон confederation peers.

Стандарт и реализация включают в себя следующие изменения в поведении:

- Значение атрибута MED распространяется между eBGP-пирами;
- Значение атрибута next-hop не изменяется при eBGP-пиринге (поведение можно переопределить с помощью команды **next-hop-self**);
- Внутри конфедерации политика анонсирования маршрутной информации аналогична политика анонсирования для iBGP-пиринга;
- Длина списка AS_CONFED_SEQUENCE или AS_CONFED_SET не участвует в политике выбора лучшего маршрута.

Алгоритм настройки

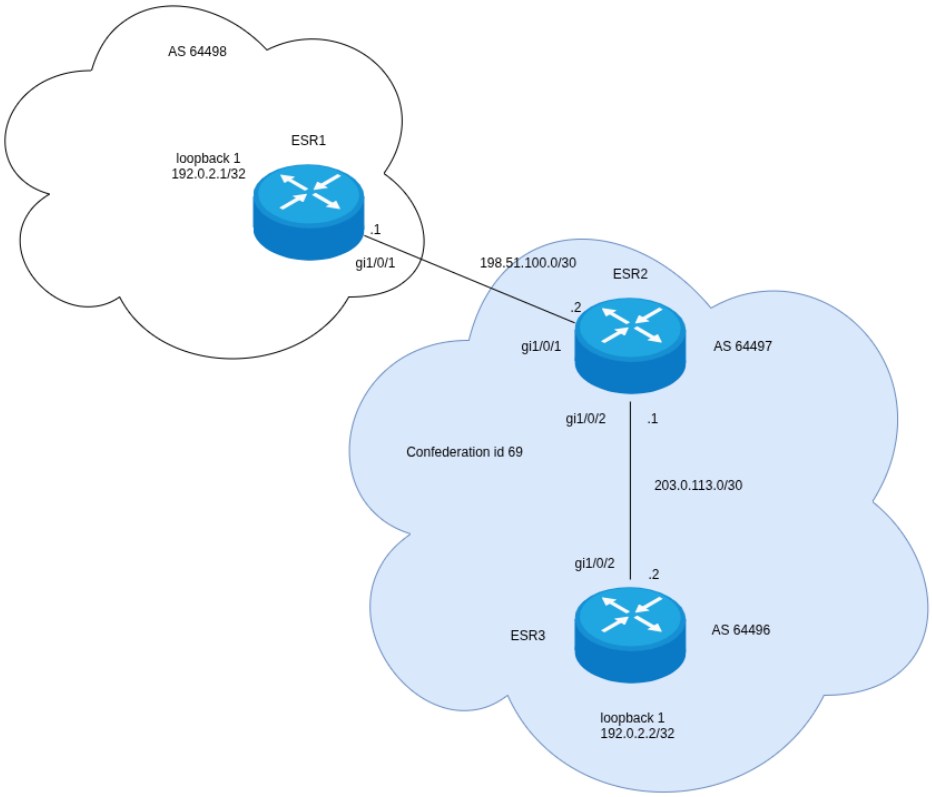
Шаг	Описание	Команда	Ключи
1	В контексте настройки BGP указать идентификатор конфедерации	**esr(config-bgp)# confederation identifier <ID>**	<ID> – идентификатор конфедерации, принимает значение [1..4294967295].
2	Сконфигурировать члены конфедерации	**esr(config-bgp)# confederation peer <AS>**	<AS> – список номеров автономных систем, задается в виде AS-AS,AS,AS-AS, принимает значения [1..4294967295].

Пример настройки

Задача:

Необходимо настроить конфедерацию между ESR2 и ESR3. На ESR2 настроить eBGP-пиринг с ESR1, проанонсировать подсети в соответствии со схемой.

Схема:



Базовая конфигурация:

ESR1

```
security zone Untrusted
exit

interface gigabitethernet 1/0/1
  security-zone Untrusted
  ip address 198.51.100.1/30
exit
interface loopback 1
  ip address 192.0.2.1/32
exit

security zone-pair Untrusted self
  rule 1
    action permit
    match protocol tcp
    match destination-port port-range 179
    enable
  exit
  rule 2
    action deny
    enable
  exit
exit
```

ESR2

```
security zone Untrusted
exit
security zone Trusted
exit

interface gigabitethernet 1/0/1
  security-zone Untrusted
  ip address 198.51.100.2/30
exit
interface gigabitethernet 1/0/2
  security-zone Trusted
  ip address 203.0.113.1/30
exit

security zone-pair Untrusted self
  rule 1
    action permit
    match protocol tcp
    match destination-port port-range 179
    enable
  exit
  rule 2
    action deny
    enable
  exit
exit
security zone-pair Trusted self
  rule 1
    action permit
    match protocol tcp
    match destination-port port-range 179
    enable
  exit
  rule 2
    action deny
    enable
  exit
exit
```

ESR3

```
security zone Trusted
exit

interface gigabitethernet 1/0/2
  security-zone Trusted
  ip address 203.0.113.2/30
exit
interface loopback 1
  ip address 192.0.2.2/32
exit

security zone-pair Trusted self
  rule 1
    action permit
    match protocol tcp
    match destination-port port-range 179
    enable
  exit
  rule 2
    action deny
    enable
  exit
exit
```

Решение:

Первым шагом настроим BGP внутри конфедерации: установим пиринг, зададим идентификатор, определим члены конфедерации. На ESR3 проанонсируем соответствующий loopback.

ESR2

```
ESR2(config)# router bgp 64497
ESR2(config-bgp)#   confederation id 69            <--- Назначение идентификатора конфедерации
ESR2(config-bgp)#   confederation peer 64496       <--- AS с номер 64496 является членом
конфедерации
ESR2(config-bgp)#   neighbor 203.0.113.2
ESR2(config-bgp-neighbor)#     remote-as 64496
ESR2(config-bgp-neighbor)#     address-family ipv4 unicast
ESR2(config-bgp-neighbor-af)#       enable
ESR2(config-bgp-neighbor-af)#     exit
ESR2(config-bgp-neighbor)#     enable
ESR2(config-bgp-neighbor)#   exit
ESR2(config-bgp)#   enable
ESR2(config-bgp)# exit
ESR2(config)#
ESR2(config)# do com
ESR2(config)# do conf
```

ESR3

```
ESR3(config)# router bgp 64496
ESR3(config-bgp)#   confederation id 69
ESR3(config-bgp)#   confederation peer 64497
ESR3(config-bgp)#   neighbor 203.0.113.1
ESR3(config-bgp-neighbor)#     remote-as 64497
ESR3(config-bgp-neighbor)#     address-family ipv4 unicast
ESR3(config-bgp-neighbor-af)#       enable
ESR3(config-bgp-neighbor-af)#     exit
ESR3(config-bgp-neighbor)#     enable
ESR3(config-bgp-neighbor)#   exit
ESR3(config-bgp)#   address-family ipv4 unicast
ESR3(config-bgp-af)#     network 192.0.2.2/32
ESR3(config-bgp-af)#   exit
ESR3(config-bgp)#   enable
ESR3(config-bgp)# exit
ESR3(config)# do com
ESR3(config)# do conf
```

Проверяем, что конфедерация успешно сконфигурирована с обеих сторон:

```
ESR2# sh bgp summary
2025-11-26 06:37:55
  BGP router identifier 198.51.100.2, local AS number 64497, AS confederation identifier
69   <----
  BGP activity 1/0 prefixes
  Neighbor                 AS              MsgRcvd      MsgSent      Up/Down      St/PfxRcd
                                                                    (d,h:m:s)
  -----------------------  -------------   ----------   ----------   ----------   ------------
  203.0.113.2              64496           9            10           00,00:03:07   1

ESR3# sh bgp summary
2025-11-26 06:38:52
  BGP router identifier 192.0.2.2, local AS number 64496, AS confederation identifier
69      <---
  BGP activity 0/1 prefixes
  Neighbor                 AS              MsgRcvd      MsgSent      Up/Down      St/PfxRcd
                                                                    (d,h:m:s)
  -----------------------  -------------   ----------   ----------   ----------   ------------
  203.0.113.1              64497           7            10           00,00:04:03   0
```

BGP-сессия перешла в состояние "Established". Необходимо убедиться, что тип сессии соответствует "confed-external". Для eBGP-сессии автоматически увеличится multi-hop до 255:

```
ESR3# sh bgp neighbors
BGP neighbor is 203.0.113.1
    BGP state:                          Established
    Type:                               Static neighbor
    Neighbor address:                   203.0.113.1
    Neighbor AS:                        64497
    Neighbor ID:                        198.51.100.2
    Neighbor caps:                      refresh enhanced-refresh restart-aware AS4
    Session:                            confed-external multihop AS4           <-----
    Source address:                     203.0.113.2
    Weight:                             0
    Hold timer:                         120/180
    Keepalive timer:                    18/60
    EBGP multi-hop:                     255   <-----
    RR client:                          No
    Address family ipv4 unicast:
      Send-label:                       No
      Default originate:                No
      Default information originate:    No
      Preference:                       170
      Remove private AS:                No
      Next-hop self:                    No
      Next-hop unchanged:               No
    Uptime (d,h:m:s):                   00,00:02:09

ESR2# sh bgp neighbors
BGP neighbor is 203.0.113.2
    BGP state:                          Established
    Type:                               Static neighbor
    Neighbor address:                   203.0.113.2
    Neighbor AS:                        64496
    Neighbor ID:                        192.0.2.2
    Neighbor caps:                      refresh enhanced-refresh restart-aware AS4
    Session:                            confed-external multihop AS4           <-----
    Source address:                     203.0.113.1
    Weight:                             0
    Hold timer:                         140/180
    Keepalive timer:                    38/60
    EBGP multi-hop:                     255   <----
    RR client:                          No
    Address family ipv4 unicast:
      Send-label:                       No
      Default originate:                No
      Default information originate:    No
      Preference:                       170
      Remove private AS:                No
      Next-hop self:                    No
      Next-hop unchanged:               No
    Uptime (d,h:m:s):                   00,00:08:05
```

Проверим, что ESR2 принимает анонсируемый ESR3 маршрут 192.0.2.2/32:

⚠ Для обозначения использования AS_CONFED_SEQUENCE AS Path указывается в круглых скобках.

ESR2

```
ESR2# sh bgp ipv4 unicast 192.0.2.2/32
192.0.2.2/32       via 203.0.113.2 on gi1/0/2        [bgp64497 06:34:48] (64496i)
    Administrative Distance: 170
    Type:                    unicast
    Origin:                  IGP
    Aggregator:              --
    AS path:                 (64496)   <----
    Next Hop:                203.0.113.2
    Output Label:            --
    Input Label:             --
    Local Preference:        100
    MED:                     --
    Cluster List:            --
    Community:               --
    EXT Community:           --
    Weight:                  0
    Valid, best, confed-external
```

Следующим шагом настроим взаимодействие конфедерации с внешней автономной системой. При настройке пиринга необходимо помнить, что в качестве внешней AS будет использоваться идентификатор конфедерации.

ESR1

```
ESR1(config)#  route-map OUT
ESR1(config-route-map)#   rule 1
ESR1(config-route-map-rule)#     match ip address 192.0.2.1/32
ESR1(config-route-map-rule)#   exit
ESR1(config-route-map)#   rule 2
ESR1(config-route-map-rule)#     action deny
ESR1(config-route-map-rule)#   exit
ESR1(config-route-map)# exit
ESR1(config)#  router bgp 64498
ESR1(config-bgp)#   neighbor 198.51.100.2
ESR1(config-bgp-neighbor)#     remote-as 69
ESR1(config-bgp-neighbor)#     address-family ipv4 unicast
ESR1(config-bgp-neighbor-af)#       route-map OUT out
ESR1(config-bgp-neighbor-af)#       enable
ESR1(config-bgp-neighbor-af)#     exit
ESR1(config-bgp-neighbor)#     enable
ESR1(config-bgp-neighbor)#   exit
ESR1(config-bgp)#   address-family ipv4 unicast
ESR1(config-bgp-af)#     network 192.0.2.1/32
ESR1(config-bgp-af)#   exit
ESR1(config-bgp)#   enable
ESR1(config-bgp)# exit
ESR1(config)#
ESR1(config)# do com
ESR1(config)# do conf
```

ESR2

```
ESR2(config)#  route-map OUT
ESR2(config-route-map)#   rule 1
ESR2(config-route-map-rule)#     match ip address 192.0.2.2/32
ESR2(config-route-map-rule)#   exit
ESR2(config-route-map)#   rule 2
ESR2(config-route-map-rule)#     action deny
ESR2(config-route-map-rule)#   exit
ESR2(config-route-map)# exit
ESR2(config)#
ESR2(config)#  router bgp 64497
ESR2(config-bgp)#    neighbor 198.51.100.1
ESR2(config-bgp-neighbor)#     remote-as 64498
ESR2(config-bgp-neighbor)#     address-family ipv4 unicast
ESR2(config-bgp-neighbor-af)#       route-map OUT out
ESR2(config-bgp-neighbor-af)#       enable
ESR2(config-bgp-neighbor-af)#     exit
ESR2(config-bgp-neighbor)#     enable
ESR2(config-bgp-neighbor)#   exit
ESR2(config-bgp)# neighbor 203.0.113.2
ESR2(config-bgp-neighbor)# address-family ipv4 unicast
ESR2(config-bgp-neighbor-af)# next-hop-self
ESR2(config-bgp-neighbor-af)# exit
ESR2(config-bgp-neighbor)# do com
ESR2(config-bgp)# do com
ESR2(config-bgp)# do conf
```

Проверяем, что пиринг поднялся:

```
ESR2# sh bgp neighbors 198.51.100.1
BGP neighbor is 198.51.100.1
    BGP state:                          Established
    Type:                               Static neighbor
    Neighbor address:                   198.51.100.1
    Neighbor AS:                        64498
    Neighbor ID:                        192.0.2.1
    Neighbor caps:                      refresh enhanced-refresh restart-aware AS4
    Session:                            external AS4
    Source address:                     198.51.100.2
    Weight:                             0
    Hold timer:                         136/180
    Keepalive timer:                    36/60
    RR client:                          No
    Address family ipv4 unicast:
      Send-label:                       No
      Default originate:                No
      Default information originate:    No
      Outgoing route-map:               OUT
      Preference:                       170
      Remove private AS:                No
      Next-hop self:                    No
      Next-hop unchanged:               No
    Uptime (d,h:m:s):                   00,00:16:04

ESR1# sh bgp neighbors 198.51.100.2
BGP neighbor is 198.51.100.2
    BGP state:                          Established
    Type:                               Static neighbor
    Neighbor address:                   198.51.100.2
    Neighbor AS:                        69
    Neighbor ID:                        198.51.100.2
    Neighbor caps:                      refresh enhanced-refresh restart-aware AS4
    Session:                            external AS4
    Source address:                     198.51.100.1
    Weight:                             0
    Hold timer:                         135/180
    Keepalive timer:                    39/60
    RR client:                          No
    Address family ipv4 unicast:
      Send-label:                       No
      Default originate:                No
      Default information originate:    No
      Outgoing route-map:               OUT
      Preference:                       170
      Remove private AS:                No
      Next-hop self:                    No
      Next-hop unchanged:               No
    Uptime (d,h:m:s):                   00,00:34:20
```

Проверяем корректность анонсируемой информации:

ESR1

```
ESR1# sh bgp ipv4 unicast  192.0.2.2/32
192.0.2.2/32       via 198.51.100.2 on gi1/0/1       [bgp64498 07:49:49] (69i)
    Administrative Distance: 170
    Type:                    unicast
    Origin:                  IGP
    Aggregator:              --
    AS path:                 69
    Next Hop:                198.51.100.2
    Output Label:            --
    Input Label:             --
    Local Preference:        100
    MED:                     --
    Cluster List:            --
    Community:               --
    EXT Community:           --
    Weight:                  0
    Valid, best, external
```

ESR2

```
ESR3# sh bgp ipv4 unicast  192.0.2.1/32
192.0.2.1/32       via 203.0.113.1 on gi1/0/2        [bgp64496 07:49:51] (64498i)
    Administrative Distance: 170
    Type:                    unicast
    Origin:                  IGP
    Aggregator:              --
    AS path:                 (64497) 64498
    Next Hop:                203.0.113.1
    Output Label:            --
    Input Label:             --
    Local Preference:        100
    MED:                     --
    Cluster List:            --
    Community:               --
    EXT Community:           --
    Weight:                  0
    Valid, best, confed-external
```

Настройка завершена.

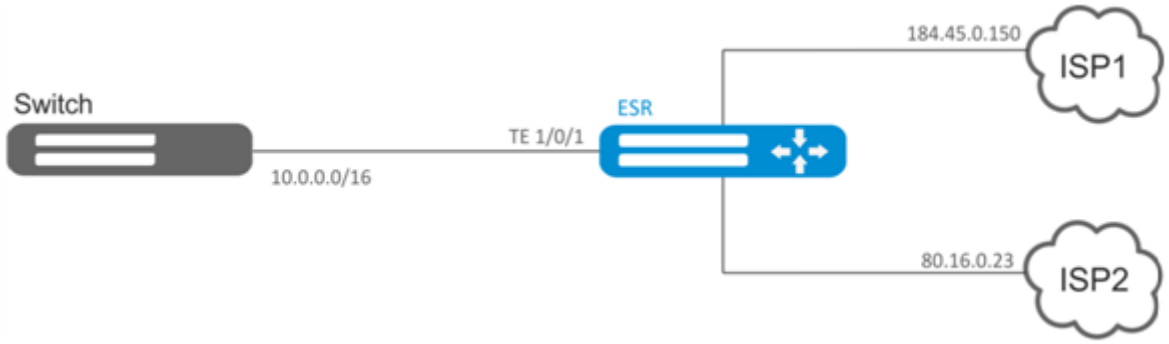
11.8 Настройка Policy-Based Routing

Policy-Based Routing (PBR) – это механизм маршрутизации, который позволяет принимать решения о форвардинге трафика на основе заданных политик, а не основываясь на таблице маршрутизации. В отличие от традиционной маршрутизации, которая опирается исключительно на наилучший путь по метрике (например, кратчайший маршрут), PBR предоставляет администраторам гибкий инструмент для управления трафиком с учётом дополнительных параметров: источника трафика, типа протокола, VLAN, уровня приоритета и других.

11.8.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать маршрутную карту для фильтрации и модификации IP-маршрутов.	**esr(config)# route-map <NAME>**	<NAME> – имя маршрутной карты, задаётся строкой до 31 символа.
2	Создать правило маршрутной карты.	**esr(config-route-map)# rule <ORDER>**	<ORDER> – номер правила, принимает значения [1..10000].
3	Указать действие, которое должно быть применено для маршрутной информации.	**esr(config-route-map-rule)# action <ACT>**	<ACT> – назначаемое действие: • **permit** – прием или анонсирование маршрутной информации разрешено; • **deny** – запрещено.
4	Задать ACL, для которого должно срабатывать правило (необязательно).	**esr(config-route-map-rule)# match ip access-group <NAME>**	<NAME> – имя списка контроля доступа, задаётся строкой до 31 символа.
5	Задать Next-Hop для пакетов, которые попадают под критерии в указанном списке доступа (ACL) (необязательно).	**esr(config-route-map-rule)# action set ip next-hop verify-availability <NEXTHOP><METRIC>**	<NEXTHOP> – IP-адрес шлюза задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <METRIC> – метрика маршрута, принимает значения [0..255].
6	Назначить политику маршрутизации на основе списков доступа (ACL).	**esr(config-if-gi)# ip policy route-map <NAME>**	<NAME> – имя сконфигурированной политики маршрутизации, строка до 31 символа.
7	Разрешить фильтрацию и модификацию локального трафика на основе политики маршрутизации.	**esr(config)# ip local policy [vrf <VRF>] route-map <NAME>**	<NAME> – имя сконфигурированной политики маршрутизации, строка до 31 символа.

11.8.2 Пример настройки



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
```

11.9 Настройка BFD

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

По умолчанию сессия устанавливается в следующем режиме:

Протокол	Режим
iBGP	multi-hop
eBGP	single-hop
eBGP multi-hop	multi-hop
OSPF	single-hop
IS-IS	single-hop
Static route	single-hop
RIP	single-hop
LDP interface	single-hop
LDP target	multi-hop

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

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

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

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

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

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

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

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

11.9.1 Настройка таймеров

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

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

```
ESR(config)# ip bfd min-tx-interval 1000
ESR(config)# ip bfd min-rx-interval 1000
ESR(config)# do commmit

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

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

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

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

11.9.2 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Активировать BFD для протокола OSPF на интерфейсе.	**esr(config-if-gi)# ip ospf bfd-enable**	
2	Активировать BFD для neighbor протокола BGP.	**esr(config-bgp-neighbor)# fall-over bfd**	
3	Активировать BFD для протокола RIP на интерфейсе.	**esr(config-if-gi)# ip rip bfd-enable**	

Шаг	Описание	Команда	Ключи
4	Задать интервал, по истечении которого происходит отправка BFD-сообщения соседу. Глобально (необязательно).	**esr(config)# ip bfd idle-tx-interval <TIMEOUT>**	<TIMEOUT> – интервал, по истечении которого происходит отправка BFD-пакета, принимает значение в миллисекундах в диапазоне: • для ESR-1000/1200/1500/1511 (rev.B)/1700/3100/3150/3200/3200L/3250/3300/3350 – [200..65535]; • для ESR-10/12V(F)/15/15R/1VF/20/21/30/31/100/200 – [300..65535]. По умолчанию: 1 секунда.
5	Включить логирование изменений состояния BFD-протокола (необязательно).	**esr(config)# ip bfd log-adjacency-changes**	
6	Задать минимальный интервал, по истечении которого сосед должен сгенерировать BFD-сообщение. Глобально (необязательно).	**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: • для ESR-1000/1200/1500/1511 (rev.B)/1700/3100/3150/3200/3200L/3250/3300/3350 – [200..65535]; • для ESR-10/12V(F)/15/15R/15VF/20/21/30/31/100/200 – [300..65535]. По умолчанию: • на ESR-1000/1200/1500/1511 (rev.B)/1700/3100/3150/3200/3200L/3250/3300/3350: 200 миллисекунд; • на ESR-10/12V(F)/15/15R/15/VF/20/21/30/31/100/200: 300 миллисекунд.

Шаг	Описание	Команда	Ключи
7	Задать минимальный интервал, по истечении которого происходит отправка BFD-сообщения соседу. Глобально (необязательно).	**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: • для ESR-1000/1200/1500/1511 (rev.B)/1700/3100/3150/3200/3200L/3250/3300/3350 – [200..65535]; • для ESR-10/12V(F)/15/15R/15VF/20/21/30/31/100/200 – [300..65535]. По умолчанию: • на ESR-1000/1200/1500/1511 (rev.B)/1700/3100/3150/3200/3200L/3250/3300/3350 – 200 миллисекунд; • на ESR-10/12V(F)/15/15R/15VF/20/21/30/31/100/200 – 300 миллисекунд.
8	Задать число пропущенных пакетов, после достижения которого BFD-сосед считается недоступным. Глобально.	**esr(config)# ip bfd multiplier <COUNT>**	<COUNT> – число пропущенных пакетов, после достижения которого сосед считается недоступным, принимает значение в диапазоне [1..100]. По умолчанию: 5.

Шаг	Описание	Команда	Ключи
9	Запустить работу механизма BFD с определенным IP-адресом.	**esr(config)# ip bfd neighbor <ADDR> [{ interface <IF> | tunnel <TUN> }] [local-address <ADDR> [multihop]] [vrf <VRF>]**	<ADDR> – IP-адрес шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IF> – интерфейс или группы интерфейсов; <TUN> – тип и номер туннеля; <VRF> – имя экземпляра VRF, задается строкой до 31 символа; multihop – ключ для установки TTL=255, для работы механизма BFD через маршрутизируемую сеть.
10	Перевести BFD-сессию в пассивный режим, то есть BFD-сообщения не будут отправляться до тех пор, пока не будут получены сообщения от BFD-соседа. Глобально (необязательно).	**esr(config)# ip bfd passive**	
11	Задать интервал, по истечении которого происходит отправка BFD-сообщения соседу. На интерфейсе (необязательно).	**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: • для ESR-1000/1200/1500/1511 (rev.B)/1700/3100/3150/3200/3200L/3250/3300/3350 – [200..65535]; • для ESR-10/12V(F)/15/15R/15VF/20/21/30/31/100/200 – [300..65535]. По умолчанию: 1 секунда.

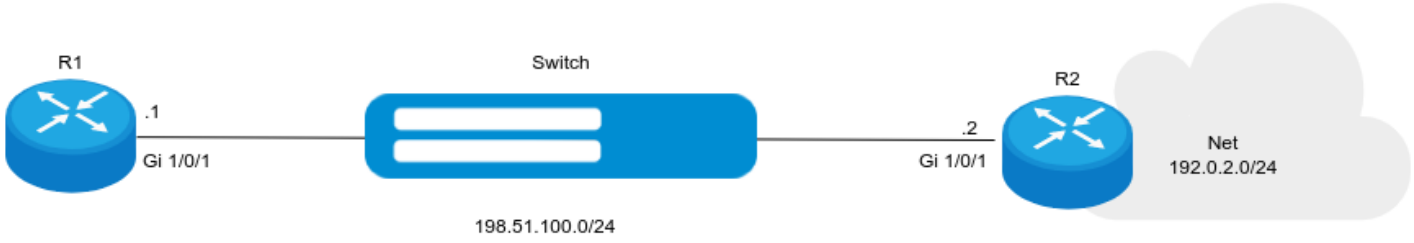
Шаг	Описание	Команда	Ключи
12	Задать минимальный интервал, по истечении которого сосед должен сгенерировать BFD-сообщение. На интерфейсе (необязательно).	**esr(config-if-gi)# ip bfd min-rx-interval <TIMEOUT>**	<TIMEOUT> – интервал, по истечении которого должна происходить отправка BFD-сообщения соседом, принимает значение в миллисекундах в диапазоне: • для ESR-1000/1200/1500/1511 (rev.B)/1700/3100/3150/3200.3200L/3250/3300/3350 – [200..65535]; • для ESR-10/12V(F)/15/15R/15VF/20/21/30/31/100/200 – [300..65535]. По умолчанию: • на ESR-1000/1200/1500/1511 (rev.B)/1700/3100/3150/3200/3200L/3250/3300/3350 – 200 миллисекунд; • на ESR-10/12V(F)/15/15R/15VF/20/21/30/31/100/200 – 300 миллисекунд.

Шаг	Описание	Команда	Ключи
13	Задать минимальный интервал, по истечении которого происходит отправка BFD-сообщения соседу. На интерфейсе (необязательно).	**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: • для ESR-1000/1200/1500/1511 (rev.B)/1700/3100/3150/3200/3200L/3250/3300/3350 – [200..65535]; • для ESR-10/12V(F)/15/15R/15VF/20/21/30/31/100/200 – [300..65535]. По умолчанию: • на ESR-1000/1200/1500/1511 (rev.B)/1700/3100/3150/3200/3200L/3250/3300/3350 – 200 миллисекунд; • на ESR-10/12V(F)/15/15R/15VF/20/21/30/31/100/200 – 300 миллисекунд.
14	Задать число пропущенных пакетов, после достижения которого BFD-сосед считается недоступным. На интерфейсе (необязательно).	**esr(config-if-gi)# ip bfd multiplier <COUNT>**	<COUNT> – число пропущенных пакетов, после достижения которого сосед считается недоступным, принимает значение в диапазоне [1..100]. По умолчанию: 5.
15	Перевести BFD-сессию в пассивный режим, то есть BFD-сообщения не будут отправляться до тех пор, пока не будут получены сообщения от BFD-соседа. На интерфейсе (необязательно).	**esr(config-if-gi)# ip bfd passive**	
16	При активизации работы протока BFD на интерфейсе с включенным firewall, необходимо разрешить работу протокола UDP порт назначения – 3784 из зоны сконфигурированной на интерфейсе в зону self. Как создать необходимое правило описано в разделе Конфигурирование Firewall.		

11.9.3 Пример настройки

Задача:

Необходимо настроить протокол BFD для статического маршрута на маршрутизаторе R1.



Решение:

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

R1

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

R2

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

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

R1

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

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

R2

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

Для вывода оперативной информации возможно использование следующих команд:

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

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

S     * 192.0.2.0/24       [1/0]             via 198.51.100.2 on gi1/0/1       [static
16:22:27]
R1# sh bfd neighbors
Neighbor                                Discriminator State     Interface
--------------------------------------- ------------- --------- ----------------
198.51.100.2                            2907010617    Up        gi1/0/1
R1# sh ip route 192.0.2.0/24
 Codes: C - connected, S - static, R - RIP derived,
        O - OSPF derived, IA - OSPF inter area route,
        E1 - OSPF external type 1 route, E2 - OSPF external type 2 route
        B - BGP derived, D - DHCP derived, K - kernel route, V - VRRP route
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        H - NHRP, * - FIB route

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

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

R1# sh bfd neighbors
Neighbor                                Discriminator State     Interface
--------------------------------------- ------------- --------- ----------------
198.51.100.2                            2907010617     Down      gi1/0/1

R1# sh ip route 192.0.2.0/24
```

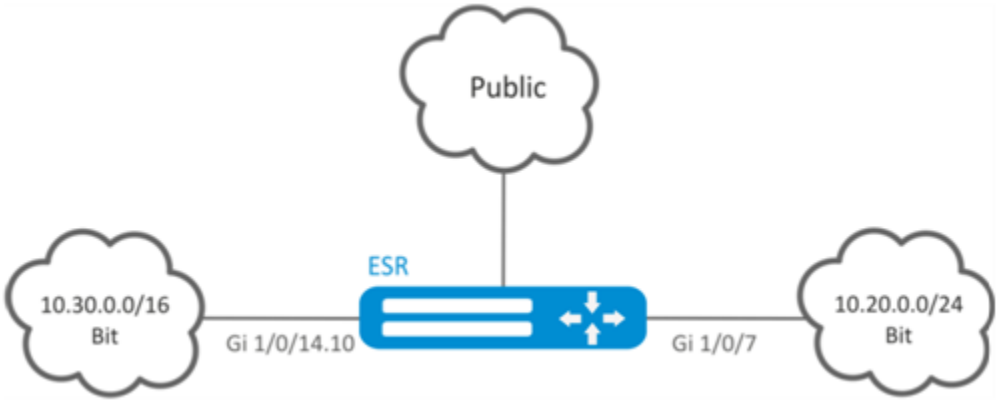
```
Codes: C - connected, S - static, R - RIP derived,
       O - OSPF derived, IA - OSPF inter area route,
       E1 - OSPF external type 1 route, E2 - OSPF external type 2 route
       B - BGP derived, D - DHCP derived, K - kernel route, V - VRRP route
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS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

R1#
```

Настройка завершена.

11.10 Настройка VRF

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



11.10.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать экземпляр VRF и перейти в режим настройки параметров экземпляра VRF.	**esr(config)# ip vrf <VRF>**	<VRF> – имя экземпляра VRF, задается строкой до 31 символа.
2	Назначить описание конфигурируемого экземпляра VRF.	**esr(config-vrf)# description <DESCRIPTION>**	<DESCRIPTION> – описание экземпляра VRF, задаётся строкой до 255 символов.

Шаг	Описание	Команда	Ключи
3	Настроить емкость таблиц маршрутизации в конфигурируемом VRF для IPv4/IPv6 протоколов маршрутизации (необязательно).	**esr(config-vrf)# ip protocols <PROTOCOL> max-routes <VALUE>** **esr(config-vrf)#ipv6 protocols <PROTOCOL> max-routes <VALUE>**	<PROTOCOL> – вид протокола, принимает значения: ospf, bgp; <VALUE> – количество маршрутов в маршрутной таблице, принимает значения в диапазоне: • OSPF ESR-1000/1200/1500/1511 (rev.B)/1700/3100/3150/3200/3200L/3250/3300/3350 – [1..500000], ESR-20/21/30/31/100/200 – [1..300000], ESR-10/12V(F)/15/15R/15VF – [1..30000] • BGP ESR-1000/1200/1500/1511 (rev.B)/1700/3100/3150/3200/3200L/3250/3300/3350 – [1..5000000], ESR-20/21/30/31/100/200 – [1..2500000], ESR-10/12V(F)/15/15VF/15R – [1..1000000]. Значение по умолчанию: 0.
4	Включить и настроить протоколы динамической маршрутизации трафика (Static/OSPF/BGP/IS-IS) в экземпляре VRF (необязательно). 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.

11.10.2 Пример настройки

Задача:

К маршрутизатору 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 protocol udp
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 protocol tcp
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-if-sub)# ip vrf forwarding bit
esr(config-if-sub)# ip address 10.30.0.1/16
esr(config-if-sub)# security-zone vrf-sec
esr(config-if-sub)# 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
```

11.11 Настройка MultiWAN

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

11.11.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Сконфигурировать интерфейсы, по которым будет работать MultiWAN: установить IP-адреса и указать security-zone.		
2	Прописать статические маршруты через WAN (если необходимо).	**esr(config)# ip route <SUBNET> wan load-balance rule <ID> [<METRIC>]**	<ID> – идентификатор создаваемого правила из п.2. [METRIC] – метрика маршрута, принимает значения [0..255].
3	Создать правило WAN и перейти в режим настройки параметров правила.	**esr(config)# wan load-balance rule <ID>**	<ID> – идентификатор создаваемого правила, принимает значения [1..50].
4	Задать интерфейсы или туннели, которые являются шлюзами в маршруте, создаваемом службой MultiWAN.	**esr(config-wan-rule)# outbound { interface <IF> | tunnel <TUN> } [WEIGHT]**	<IF>– имя интерфейса; <TUN> – имя туннеля; [WEIGHT] – вес туннеля или интерфейса, определяется в диапазоне [1..255]. Если установить значение 2, то по данному интерфейсу будет передаваться в 2 раза больше трафика, чем по интерфейсу со значением по умолчанию. В режиме резервирования активным будет маршрут с наибольшим весом. Значение по умолчанию 1.
5	Описать правила (необязательно).	**esr(config-wan-rule)# description <DESCRIPTION>**	<DESCRIPTION> – описание правила wan, задаётся строкой до 255 символов.

Шаг	Описание	Команда	Ключи
6	Данной командой осуществляется переключение из режима балансировки в режим резервирования (если необходимо).	**esr(config-wan-rule)# failover**	
7	Данной командой включается отправка ответных пакетов сессии через тот же интерфейс, через который получены входящие пакеты сессии (если необходимо).	**esr(config-wan-rule)# stickiness**	
8	Включить wan-правило.	**esr(config-wan-rule)# enable**	
9	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.
10	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.
11	Описать target (необязательно).	**esr(config-wan-target)# description <DESCRIPTION>**	<DESCRIPTION> – описание target, задаётся строкой до 255 символов.
12	Указать время ожидания ответа на запрос по протоколу ICMP (необязательно).	**esr(config-wan-target)# resp-time <TIME>**	<TIME> – время ожидания, определяется в секундах [1..30].
13	Указать IP-адрес проверки.	**esr(config-wan-target)# ip address <ADDR>**	<ADDR> – IP-адрес назначения, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
		esr(config-wan-target)# ipv6 address <IPV6-ADDR>	<IPV6-ADDR> – IPv6-адрес назначения, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
14	Включить проверку цели.	**esr(config-wan-target)# enable**	
Команды для пунктов 14–17 необходимо применить на интерфейсах/туннелях в MultiWAN.			

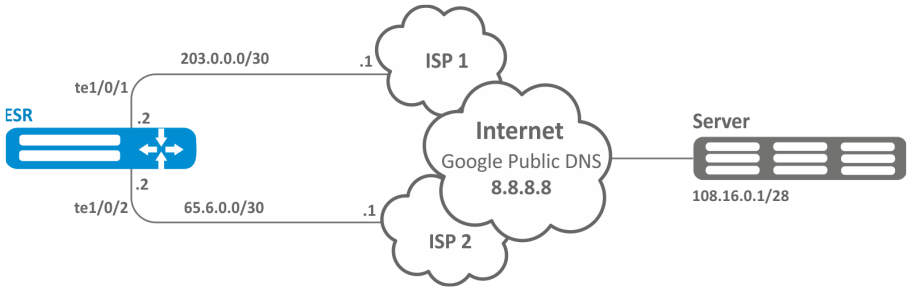
Шаг	Описание	Команда	Ключи
15	Включить WAN-режим на интерфейсе для IPv4/IPv6-стека.	**esr(config-if-gi)# wan load-balance enable**	
		esr(config-if-gi)# ipv6 wan load-balance enable	
16	Задать количество неудачных попыток проверки соединения, после которых, при отсутствии ответа от встречной стороны, соединение будет считается неактивным (необязательно).	**esr(config-if-gi)# wan load-balance failure-count <VALUE>**	<VALUE> – количество попыток, определяется в диапазоне [1..10]. Значение по умолчанию: 1.
		esr(config-if-gi)# ipv6 wan load-balance failure-count <VALUE>	
17	Задать количество успешных попыток проверки соединения, после которых, в случае успеха, соединение считается вновь активным (необязательно).	**esr(config-if-gi)# wan load-balance success-count <VALUE>**	<VALUE> – количество попыток, определяется в диапазоне [1..10]. Значение по умолчанию: 1.
		esr(config-if-gi)# ipv6 wan load-balance success-count <VALUE>	
18	Задать IP-адрес соседа, который будет указан в качестве одного из шлюзов в статическом маршруте, создаваемом службой MultiWAN.	**esr(config-if-gi)# wan load-balance nexthop { <IP> | dhcp enable | tunnel enable }**	<IP> – IP-адрес назначения (шлюз), задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. dhcp enable – если на интерфейсе IP-адрес получен через DHCP-клиента, используется шлюз с DHCP-сервера. tunnel enable – использовать в качестве nexthop – p-t-p адрес назначения. Применимо для подключаемых интерфейсов, работающих через ppp.
		esr(config-if-gi)# ipv6 wan load-balance nexthop { <IPV6> }	<IPV6> – IPv6-адрес назначения (шлюз), задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
19	Данной командой будут проверяться IP-адреса из списка проверки целостности. В случае недоступности всех (по умолчанию)/хотя бы одной (с использованием ключа chack-all) из проверяемых узлов, шлюз будет считаться недоступным.	**esr(config-if-gi)# wan load-balance target-list { check-all | <NAME> }**	<NAME> – проверку производить на основании конкретного target листа (заданного в п.7). check-all – проверку производить на основании всех target листа.
		esr(config-if-gi)# ipv6 wan load-balance target-list { check-all | <NAME> }	

Шаг	Описание	Команда	Ключи
20	Прописать статические маршруты через WAN.	**esr(config)# ip route <SUBNET> wan load-balance rule <ID> [<METRIC>]**	<ID> – идентификатор создаваемого правила из п.2. [METRIC] – метрика маршрута, принимает значения [0..255].
		esr(config)# ipv6 route <SUBNET> wan load-balance rule <ID [<METRIC>]	

11.11.2 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
```

11.12 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.

11.12.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать IS-IS процесс и перейти в режим настройки параметров этого процесса.	**esr(config)# router isis <ID> [vrf <VRF>]**	<ID> – номер процесса, принимает значения [1..65535]; <VRF> – имя экземпляра VRF, задается строкой до 31 символа.
2	Установить NET-адрес.	**esr(config-isis)# net {<NET>}**	<NET> – NET-адрес, формат: ff[.ffff.ffff.ffff.ffff.ffff].ffff.ffff.ffff.00.
3	Включить IS-IS процесс.	**esr(config-isis)# enable**	
4	Установить алгоритм аутентификации для L2-уровня (необязательно).	**esr(config-isis)# authentication domain algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм аутентификации: • cleartext – пароль, передается открытым текстом; • md5 – пароль, хешируется по алгоритму md5.
5	Установить пароль аутентификации для L2-уровня (необязательно).	**esr(config-isis)# authentication domain key ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<CLEAR-TEXT> – пароль, задаётся строкой 8 символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером 8 байт (16 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).
6	Установить список ключей для аутентификации (необязательно).	**esr(config-isis)# authentication domain key chain <KEYCHAIN>**	<KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов.

Шаг	Описание	Команда	Ключи
7	Выбрать алгоритм аутентификации для L1-уровня (необязательно).	**esr(config-isis)# authentication area algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм аутентификации: • cleartext – пароль, передается открытым текстом; • md5 – пароль, хешируется по алгоритму md5.
8	Установить пароль аутентификации для L1-уровня (необязательно).	**esr(config-isis)# authentication area key ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<CLEAR-TEXT> – пароль, задаётся строкой 8 символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером 8 байт (16 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).
9	Установить список ключей для аутентификации (необязательно).	**esr(config-isis)# authentication area key chain <KEYCHAIN>**	<KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов.
10	Включить передачу имени маршрутизатора в LSP (необязательно).	**esr(config-isis)# hostname dynamic**	
11	Установить уровень работы IS-IS процесса (необязательно).	**esr(config-isis)# is-type {<LEVEL>}**	<LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-1-2 – работа производится и на 1, и на 2 уровне; • level-2 – работа производится только на 2 уровне.
12	Установить тип метрики, который будет использоваться в работе IS-IS процесса (необязательно).	**esr(config-isis)# metric-style { narrow | wide | transition } [<LEVEL>]**	narrow – принимает и генерирует TLV (о достижимости сетей) старого типа; wide – принимает и генерирует TLV (о достижимости сетей) нового типа; transition – принимает и генерирует TLV (о достижимости сетей) нового и старого типа; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.

Шаг	Описание	Команда	Ключи
13	Установить приоритетность маршрутов для данного IS-IS процесса (необязательно).	**esr(config-isis)# preference {<VALUE>}**	<VALUE> – принимает значения [1..255].
14	Включить работу IS-IS с IPv4 и/или IPv6 адресами (необязательно).	**esr(config-isis)# address-family { ipv4 | ipv6 }**	ipv4 – семейство адресов IPv4; ipv6 – семейство адресов IPv6.
15	Установить интервал обновления собственных LSP (необязательно).	**esr(config-isis)# lsp-refresh-interval { min | max } <TIME> [<LEVEL>]**	min – минимальный интервал обновления/генерации; max – максимальный интервал обновления/генерации; <TIME> – время в секундах, принимает значения [1..65535]; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
16	Установить время жизни собственных LSP (необязательно).	**esr(config-isis)# max-lsp-lifetime <TIME> [<LEVEL>]**	<TIME> – время в секундах, принимает значения [1..65535]; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
17	Установить таймаут перед следующим расчётом SPF (необязательно).	**esr(config-isis)# spf-timeout <TIME> [<LEVEL>]**	<TIME> – время в миллисекундах, принимает значения [1..10000]; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.

<table>
<tr><th>Шаг</th><th>Описание</th><th>Команда</th><th>Ключи</th></tr>
<tr><td rowspan="3">18</td><td rowspan="3">Включить анонсирование маршрутов, полученных альтернативным способом (необязательно).</td><td>esr(config-isis)# redistribute bgp <AS> [route-map <NAME>] [is-type <LEVEL>]</td><td rowspan="2"><AS> – номер автономной системы, может принимать значения [1..4294967295];
<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых маршрутов, задаётся строкой до 31 символа;
<LEVEL> – уровень работы протокола IS-IS:
level-1 – работа производится только на 1 уровне;
level-2 – работа производится только на 2 уровне.</td></tr>
<tr><td>esr(config-isis)# redistribute ipv6 bgp <AS> [route-map <NAME>] [is-type <LEVEL>]</td></tr>
<tr><td>esr(config-isis)# redistribute ospf <ID> <ROUTE-TYPE> [route-map <NAME>] [is-type <LEVEL>]</td><td rowspan="2"><ID> – номер процесса, может принимать значение [1..65535];
<ROUTE-TYPE> – тип маршрута:
intra-area – анонсирование маршрутов OSPF-процесса в пределах зоны;
inter-area – анонсирование маршрутов OSPF-процесса между зонами;
external1 – анонсирование внешних маршрутов OSPF-формата 1;
external2 – анонсирование внешних маршрутов OSPF-формата 2;
<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых OSPF-маршрутов, задаётся строкой до 31 символа;
<LEVEL> – уровень работы протокола IS-IS:
level-1 – работа производится только на 1 уровне;
level-2 – работа производится только на 2 уровне.</td></tr>
<tr><td>esr(config-isis)# redistribute ipv6 ospf <ID> <ROUTE-TYPE> [route-map <NAME>] [is-type <LEVEL>]</td></tr>
</table>

Шаг	Описание	Команда	Ключи
		esr(config-isis)# redistribute isis <ID> <ROUTE-TYPE> [route-map <NAME>] [is-type <LEVEL>]	<ID> – номер процесса, может принимать значение [1..65535]; <ROUTE-TYPE> – тип маршрута: • level-1 – анонсирование маршрутов 1 уровня; • level-2 – анонсирование маршрутов 1 уровня; • inter-area – анонсирование маршрутов IS-IS-процесса между зонами; <NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых IS-IS-маршрутов, задаётся строкой до 31 символа; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
		esr(config-isis)# redistribute rip [route-map <NAME>] [is-type <LEVEL>]	<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых RIP-маршрутов, задаётся строкой до 31 символа; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
		esr(config-isis)# redistribute ipv6 rip [route-map <NAME>] [is-type <LEVEL>]	
		esr(config-isis)# redistribute static [route-map <NAME>] [is-type <LEVEL>]	<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых статических маршрутов, задаётся строкой до 31 символа; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.

Шаг	Описание	Команда	Ключи
		esr(config-isis)# redistribute connected [route-map <NAME>] [is-type <LEVEL>]	<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых подключённых маршрутов, задаётся строкой до 31 символа; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
19	Добавить фильтрацию подсетей во входящих или исходящих обновлениях (необязательно).	**esr(config-isis)# prefix-list { ipv6 <LIST_NAME> | <LIST_NAME> } {in|out}**	<LIST-NAME> – имя сконфигурированного списка подсетей, задаётся строкой до 31 символа. in – фильтрация входящих маршрутов; out – фильтрация анонсируемых маршрутов.
20	Добавить фильтрацию подсетей во входящих или исходящих обновлениях (необязательно).	**esr(config-isis)# route-map <NAME> {in|out}**	<NAME> – имя маршрутной карты, которая будет использоваться для фильтрации и модификации анонсируемых маршрутов, задаётся строкой до 31 символа.
21	Установить принадлежность интерфейса к определенному IS-IS процессу.	**esr(config-if-gi)# isis instance <ID>**	<ID> – номер процесса, принимает значения [1..65535].
22	Включить работу протокола IS-IS на интерфейсе.	**esr(config-if-gi)# isis enable**	
23			
24	Включить использование TLV#8 в hello-пакетах (необязательно).	**esr(config-if-gi)# isis hello-padding**	
25	Установить приоритет при выборе DIS (необязательно).	**esr(config-if-gi)# isis priority <VALUE> [<LEVEL>]**	<VALUE> – число, принимающее значения [0..127]; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.

Шаг	Описание	Команда	Ключи
26	Установить значение метрики для интерфейса (необязательно).	**esr(config-if-gi)# isis metric <VALUE> [<LEVEL>]**	<VALUE> – число, принимающее значения [1..16777215]; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
27	Установить на каком уровне маршрутизации будет работать текущий процесс IS-IS на конкретном интерфейсе (необязательно).	**esr(config-if-gi)# isis circuit-type {<LEVEL>}**	<LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-1-2 – работа производится и на 1, и на 2 уровне; • level-2 – работа производится только на 2 уровне.
28	Установить интервал отправки hello-пакетов (необязательно).	**esr(config-if-gi)# isis hello-interval <TIME> [<LEVEL>]**	<TIME> – время в секундах, принимает значения [1..65535]; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
29	Установить множитель для вычисления и отправки Hold Time (необязательно).	**esr(config-if-gi)# isis hello-multiplier <VALUE> [<LEVEL>]**	<VALUE> – число, принимающее значения [3..1000]; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
30	Перевести интерфейс в режим работы point-to-point протокола IS-IS (необязательно).	**esr(config-if-gi)# isis network point-to-point**	

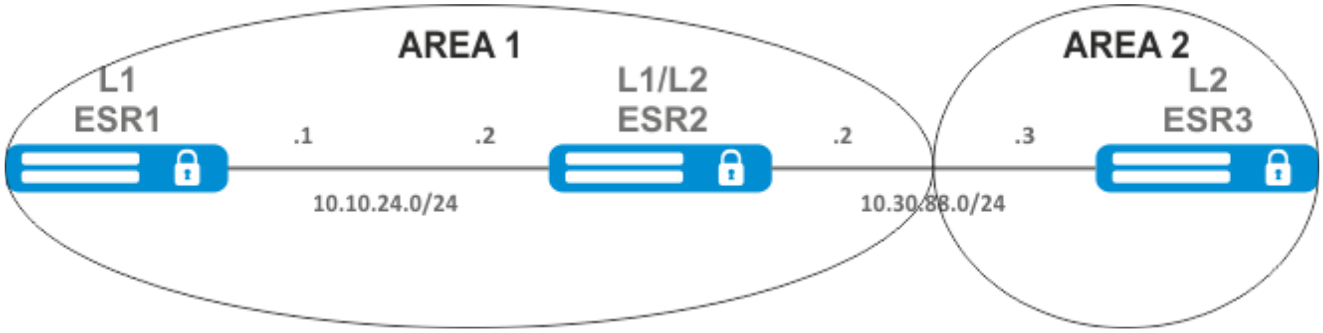
Шаг	Описание	Команда	Ключи
31	Установить интервал генерации и отправки CSNP (необязательно).	**esr(config-if-gi)# isis csnp-interval <TIME> [<LEVEL>]**	<TIME> – время в секундах, принимает значения [1..65535]; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
32	Установить интервал генерации и отправки PSNP (необязательно).	**esr(config-if-gi)# isis psnp-interval <TIME> [<LEVEL>]**	<TIME> – время в секундах, принимает значения [1..65535]; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
33	Установить интервал между передачами LSP в Broadcast-сети (необязательно).	**esr(config-if-gi)# isis lsp-interval <TIME> [<LEVEL>]**	<TIME> – время в миллисекундах, принимает значения [1-10000]; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
34	Установить интервал повторного распространения LSP в PtP-сети (необязательно).	**esr(config-if-gi)# isis lsp-retransmit-interval <TIME> [<LEVEL>]**	<TIME> – время в секундах, принимает значения [1..65535]; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.

Шаг	Описание	Команда	Ключи
35	Установить алгоритм аутентификации для hello-пакетов (необязательно).	**esr(config-if-gi)# isis authentication algorithm <ALGORITHM> [<LEVEL>]**	<ALGORITHM> – алгоритм аутентификации: • cleartext – пароль, передается открытым текстом; • md5 – пароль, хешируется по алгоритму md5; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
36	Установить пароль для аутентификации hello-пакетов (необязательно).	**esr(config-if-gi)# isis authentication key ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> } [<LEVEL>]**	<CLEAR-TEXT> – пароль, задаётся строкой 8 символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером 8 байт (16 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...); <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
37	Установить список ключей для аутентификации hello-пакетов (необязательно).	**esr(config-if-gi)# isis authentication key chain <KEYCHAIN> [<LEVEL>]**	<KEYCHAIN> – идентификатор списка ключей, задаётся строкой до 16 символов; <LEVEL> – уровень работы протокола IS-IS: • level-1 – работа производится только на 1 уровне; • level-2 – работа производится только на 2 уровне.
38	Включить протокол BFD для протокола IS-IS (необязательно).	**esr(config-if-gi)# isis bfd-enable** **esr(config-if-gi)# isis ipv6-bfd-enable**	

11.12.2 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 маршрутизатор и его системный идентификатор:

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

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

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

Зададим работу маршрутизатора с узкой метрикой на первом уровне:

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

Включим работу процесса IS-IS на маршрутизаторе:

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

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

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

Перейдём к настройке маршрутизатора ESR2:

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

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

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

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

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

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

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

Перейдём к настройке маршрутизатора ESR3:

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

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

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

12 Управление технологией MPLS

- Настройка протокола LDP
  - Алгоритм настройки
  - Пример настройки
- Конфигурирование параметров сессии в протоколе LDP
  - Алгоритм настройки параметров Hello holdtime и Hello interval в глобальной конфигурации LDP
  - Алгоритм настройки параметров Hello holdtime и Hello interval для address family
  - Алгоритм настройки параметра Keepalive holdtime в глобальной конфигурации LDP
  - Алгоритм настройки параметра Keepalive holdtime для определенного соседа
  - Пример настройки
- Конфигурирование параметров сессии в протоколе targeted-LDP
  - Алгоритм настройки параметров Hello holdtime, Hello interval и Keepalive holdtime для процесса LDP
  - Алгоритм настройки параметров Hello holdtime, Hello interval и Keepalive holdtime для определенного соседа
  - Пример настройки
- Настройка фильтрации LDP-меток
  - Метод на основе Advertise-labels
    - Алгоритм настройки
    - Пример настройки
  - Метод на основе Prefix-list
    - Алгоритм настройки
    - Пример настройки
- Настройка сервиса L2VPN Martini mode
  - Алгоритм настройки L2VPN VPWS
  - Пример настройки L2VPN VPWS
  - Алгоритм настройки L2VPN VPLS
  - Пример настройки L2VPN VPLS
- Настройка сервиса L2VPN Kompella mode (BGP Autodiscovery and Signaling)
  - Алгоритм настройки L2VPN VPLS
  - Пример настройки L2VPN VPLS
- Настройка сервиса L3VPN
  - Алгоритм настройки
  - Пример настройки
- Балансировка трафика MPLS
  - Пример настройки
- Работа с бридж-доменом в рамках MPLS
- Назначение MTU при работе с MPLS
- Inter-AS Option A
  - L2VPN
  - L3VPN
- Inter-AS Option B
  - L3VPN
- Inter-AS Option C
  - L3VPN
- MPLS over GRE
  - L2VPN
  - L3VPN

12.1 Настройка протокола LDP

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

В маршрутизаторах ESR поддержаны следующие режимы работы LDP:

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

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

В текущей реализации протокол LDP работает только с IPv4-адресами.

12.1.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	В контексте настройки параметров MPLS указать интерфейсы, участвующие в процессе MPLS-коммутации.	**esr(config-mpls)# forwarding interface { <IF> | <TUN> }**	<IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора; <TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора.
2	Задать router-id для LDP (необязательно, если указан transport-address).	**esr(config-ldp)# router-id { <ID> | <IF> | <TUN> }**	<ID> – идентификатор маршрутизатора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. <IF> – интерфейс, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора. <TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора.

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

В рамках настройки протокола LDP также доступен следующий функционал:

- Настройка фильтрации LDP-меток (см. Настройка фильтрации LDP-меток);
- Настройка параметров LDP-сессии (см. Конфигурирование параметров сессии в протоколе LDP);
- Настройка параметров tLDP-сессии (см. Конфигурирование параметров сессии в протоколе targeted-LDP).

⚠ Если изменить значение router-id, то новое значение будет применено только после рестарта данного протокола. Для рестарта mpls ldp используется команда clear mpls ldp.

12.1.2 Пример настройки

Задача:

Настроить взаимодействие по протоколу LDP между пирами.



Решение:

Предварительная конфигурация маршрутизаторов:

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

Предварительная конфигурация ESR:

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


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


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

Предварительная конфигурация ESR1:

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


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


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

Настройка на ESR:

ESR

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

Настройка на ESR1:

ESR1

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

Проверка:

На одном из пиров ввести следующие команды:

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

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

Сессия LDP должна находиться в статусе «Operational».

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

12.2 Конфигурирование параметров сессии в протоколе LDP



По умолчанию в рассылаемых hello-сообщениях установлены следующие значения:

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

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

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

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

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

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

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

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

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

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

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

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

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

12.2.1 Алгоритм настройки параметров Hello holdtime и Hello interval в глобальной конфигурации LDP

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

12.2.2 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]. 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]. Значение по умолчанию: 5.

12.2.3 Алгоритм настройки параметра Keepalive holdtime в глобальной конфигурации LDP

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

12.2.4 Алгоритм настройки параметра Keepalive holdtime для определенного соседа

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

12.2.5 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

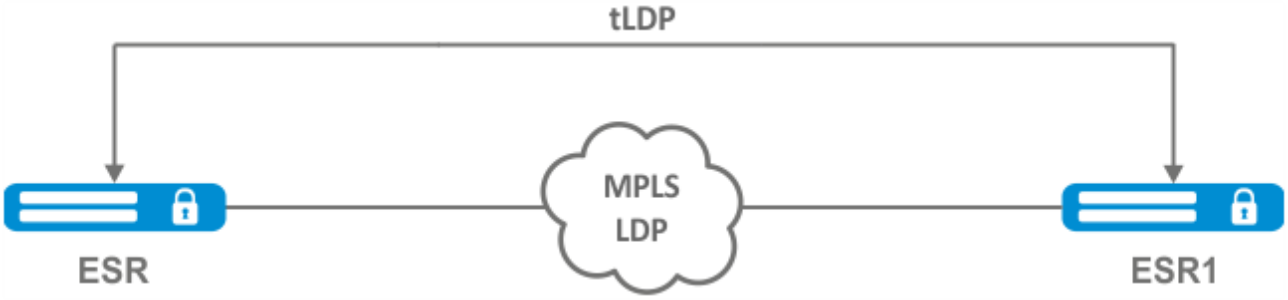
```
ESR# sh mpls ldp discovery detailed
Local LDP ID: 4.4.4.4
Discovery sources:
    Interfaces:
        gigabitethernet 1/0/4:
            Hello interval:       10 seconds
            Transport IP address: 4.4.4.4
            LDP ID:               1.1.1.1
                Source IP address:    10.10.10.1
                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:
```

12.3 Конфигурирование параметров сессии в протоколе targeted-LDP



По умолчанию для targeted LDP-сессии установлены следующие значения:

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

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

```
ESR1# sh mpls ldp discovery detailed

...
Targeted hellos:
1.1.1.1 -> 4.4.4.4:
Hello interval: 2 seconds
Transport IP address: 1.1.1.1
LDP ID: 4.4.4.4
Source IP address: 4.4.4.4
Transport IP address: 4.4.4.4
Hold time: 30 seconds
Proposed hold time: 30/45 (local/peer) seconds
```

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

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

Пример вывода для процесса LDP:

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

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

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

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

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

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


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

12.3.1 Алгоритм настройки параметров Hello holdtime, Hello interval и Keepalive holdtime для процесса 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 targeted-hello holdtime <TIME>**	<TIME> – время в секундах в интервале [3..65535]. Значение по умолчанию: 45.
3	В режиме конфигурации протокола LDP задать Hello interval.	**esr(config-ldp)# discovery targeted- hello interval <TIME>**	<TIME> – время в секундах в интервале [1..65535]. Значение по умолчанию: 5.
4	В режиме конфигурации протокола LDP задать Keepalive holdtime.	**esr(config-ldp)# keepalive <TIME>**	<TIME> – время в секундах в интервале [3..65535]. Значение по умолчанию: 180.

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

Шаг	Описание	Команда	Ключи
1	Настроить протокол LDP (см. раздел Конфигурирование протокола LDP).		
2	В режиме конфигурации LDP-соседа задать Hello holdtime.	**esr(config-ldp-neig)# discovery targeted-hello holdtime <TIME>**	<TIME> – время в секундах в интервале [3..65535]. Значение по умолчанию: 45.
3	В режиме конфигурации LDP-соседа задать Hello interval.	**esr(config-ldp-neig)# discovery targeted- hello interval <TIME>**	<TIME> – время в секундах в интервале [1..65535]. Значение по умолчанию: 5.
4	В режиме конфигурации LDP-соседа задать Keepalive holdtime.	**esr(config-ldp-neig)# keepalive <TIME>**	<TIME> – время в секундах в интервале [3..65535]. Значение по умолчанию: 180.

12.3.3 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
  ...
```

12.4 Настройка фильтрации LDP-меток

По умолчанию маршрутизаторы выделяют на каждый FEC отдельную метку. Существуют сценарии, когда необходимо выделять MPLS-метки только для определенных FEC. Ниже рассмотрены существующие возможности для реализации фильтрации LDP-меток.

12.4.1 Метод на основе Advertise-labels

Данный метод позволяет аллоцировать метки протоколом LDP только на префиксы, описанные в соответствующей object-group. Отличительной особенностью данного метода является то, что префиксы должны иметь точное совпадение с маршрутом из FIB.

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 префиксы, для которых будут назначаться метки.	**esr(config-object-group-network)# ip prefix <ADDR/LEN> [unit <ID>]**	<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]. <ID> – номер юнита, принимает значения [1..4].
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.).

ℹ Данный функционал поддержан для протокола IPv4.

Пример настройки



Задача:

Назначить MPLS-метки только FEC 10.10.0.2/32 и 10.10.0.1/32.

Решение:

На ESR_A и ESR_B создадим object-group ADV_LABELS типа network и добавим в нее префиксы 10.10.0.1/32 и 10.10.0.2/32 соответственно:

ESR_A

```
esr(config)# object-group network ADV_LABELS
esr(config-object-group-network)# ip prefix 10.10.0.1/32
esr(config-object-group-network)# ip prefix 10.10.0.2/32
```

ESR_B

```
esr(config)# object-group network ADV_LABELS
esr(config-object-group-network)# ip prefix 10.10.0.1/32
esr(config-object-group-network)# ip prefix 10.10.0.2/32
```

Применим созданную object-group на обоих маршрутизаторах:

ESR_A и ESR_B

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

Проверка:

На ESR_B убедимся, что метка назначена для соответствующих префиксов:

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

И не назначена для 192.168.2.0/24:

```
esr# sh mpls ldp bindings 192.168.2.0/24
esr#
```

12.4.2 Метод на основе Prefix-list

Данный метод позволяет управлять выделением меток для протокола LDP на основе подсетей, описанный в соответствующем Prefix-list. В отличие от метода на основе Advertise-labels, гибкость функционала Prefix-list позволяет задать диапазон (префикс), для подсетей которого будет аллоцирована метка. Данный вариант настройки является более гибким и масштабируемым.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Настроить протокол LDP (см. раздел Конфигурирование протокола LDP).		
2	Создать prefix-list.	**esr(config)# ip prefix-list <NAME>**	<NAME> – имя конфигурируемого списка подсетей, задаётся строкой до 31 символа.
3	Описать подсеть, для адресов которой будут выделяться метки.	**esr(config-object-group-network)# ip prefix <ADDR/LEN> [{ eq <LEN> | le <LEN> | ge <LEN> [le <LEN>] }**	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <LEN> – длина префикса, принимает значения [1..32]; eq – при указании команды длина префикса должна соответствовать указанной; le – при указании команды длина префикса должна быть меньше либо соответствовать указанной; ge – при указании команды длина префикса должна быть больше либо соответствовать указанной.
4	В контексте настройки LDP применить prefix-list для соответствующей address-family.	**esr(config-ldp-af-ipv4)# prefix-list <NAME>**	<NAME> – имя конфигурируемого списка, задаётся строкой до 31 символа.

Пример настройки



Задача:

Для организации сервисов L2VPN и L3VPN выделена подсеть 10.10.0.0/24. Необходимо средствами протокола LDP назначить транспортные MPLS-метки для всех адресов (подсетей/32), входящих в выделенный диапазон.

Решение:

На ESR_A и ESR_B создадим prefix-list и опишем необходимый для сервисов диапазон адресов:

ESR_A

```
esr(config)# ip prefix-list LDP_ALLOCATE
esr(config-pl)# permit 10.10.0.0/24 eq 32
```

ESR_B

```
esr(config)# ip prefix-list LDP_ALLOCATE
esr(config-pl)# permit 10.10.0.0/24 eq 32
```

Применим созданный prefix-list на обоих маршрутизаторах:

ESR_A и ESR_B

```
esr(config)# mpls
esr(config-ldp)# ldp
esr(config-ldp)# address-family ipv4
esr(config-ldp-af-ipv4)# prefix-list LDP_ALLOCATE
esr(config-ldp-af-ipv4)# do commit
esr(config-ldp-af-ipv4)# do confirm
```

Проверка:

На примере ESR_B убедимся, что метка назначена для соответствующих префиксов:

```
esr# sh mpls ldp bindings 10.10.0.1/32
10.10.0.1/32
local label: exp-null
remote label: 45 lsr: 172.16.0.1
```

И не назначена для 192.168.2.0/24:

```
esr# sh mpls ldp bindings 192.168.2.0/24
esr#
```

12.5 Настройка сервиса L2VPN Martini mode

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

1. P2P – туннель, создаваемый по схеме «точка-точка».
2. VPLS – туннель, создаваемый по схеме «точка-многоточка».

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

12.5.1 Алгоритм настройки L2VPN VPWS

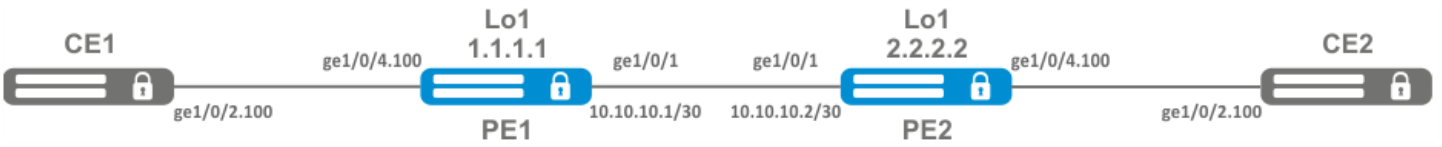
Шаг	Описание	Команда	Ключи
1	Настроить протокол LDP (см. раздел Конфигурирование протокола LDP).		
2	Создать pw-class в системе и осуществить переход в режим настройки параметров pw-class.	**esr(config-l2vpn)# pw-class <WORD>**	<WORD> – имя pw-class длиной [1..31] символов.
3	Добавить описание для pw-class (необязательно).	**esr(config-l2vpn-pw-class)# description <LINE>**	<LINE> – описание. Задается в виде строки длиной [1..255] символов.
4	Установить значение MTU для pseudo-wire входящих в pw-class (необязательно).	**esr(config-l2vpn-pw-class)# encapsulation mpls mtu <MTU>**	<MTU> – значение MTU, принимает значение в диапазоне [552..10000] Значение по умолчанию: 1500.
5	Отключить обмен status-tlv сообщениями (необязательно).	**esr(config-l2vpn-pw-class)# encapsulation mpls status-tlv disable**	Значение по умолчанию: status-tlv enable.
6	Создать p2p-туннель в системе и осуществить переход в режим настройки параметров p2p-туннеля.	**esr(config-l2vpn)# p2p <NAME>**	<NAME> – имя p2p-сервиса, задается строкой до 31 символа.
7	Задать Attached Circuit интерфейс.	**esr(config-l2vpn-p2p)# interface { <IF> | <TUN> }**	<IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора; <TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора.
8	Включить p2p-туннель.	**esr(config-l2vpn-p2p)# enable**	

Шаг	Описание	Команда	Ключи
9	Задать транспортный режим (необязательно).	**esr(config-l2vpn-p2p)# transport-mode { ethenet | vlan }**	<ethernet> – режим, при котором при входе в pseudo-wire из заголовка удаляется 802.1Q тег; <vlan> – режим, при котором 802.1Q тег может быть сохранен при передаче через pseudo-wire. Значение по умолчанию: ethernet.
10	Создать pseudo-wire и осуществить переход в режим настройки его параметров.	**esr(config-l2vpn-p2p)# pw <PW_ID> <LSR_ID>**	<PW_ID> – идентификатор psewdowire, задается в виде числа в диапазоне [1..4294967295] <LSR_ID> – идентификатор LSR, до которого строится pseudo-wire, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]
11	Добавить описание для pseudo-wire (необязательно).	**esr(config-l2vpn-pw)# description <LINE>**	<LINE> – описание. Задается в виде строки длиной [1..255] символов.
12	Задать pw-class для pseudo-wire.	**esr(config-l2vpn-pw)# pw-class <WORD>**	<WORD> – имя pw-class длиной [1..31] символов.
13	Задать адрес LSR до которого устанавливается pseudo-wire (не обязательно, если neighbor address совпадает с LSR_ID).	**esr(config-l2vpn-pw)# neighbor-address <ADDR>**	<ADDR> – IP-адрес маршрутизатора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
14	Включить pseudo-wire.	**esr(config-l2vpn-pw)# enable**	
В случае если необходимо изменить параметры по умолчанию для targeted LDP-сессии, обратитесь к разделу Конфигурирование параметров сессии в протоколе targeted-LDP.			

12.5.2 Пример настройки L2VPN VPWS

Задача:

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



Решение:

Предварительно нужно:

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

На маршрутизаторе PE1 создадим саб-интерфейс, на который будем принимать трафик от CE1:

```
PE1# configure
PE1(config)# interface gigabitethernet 1/0/4.100
PE1(config-if-sub)# 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 PE2, идентификатор pw для удобства возьмем равным VID (в данном случае равным 100):

```
PE1(config-l2vpn)# p2p to_PE2_VLAN100
PE1(config-l2vpn-p2p)# interface gigabitethernet 1/0/4.100
PE1(config-l2vpn-p2p)# pw 100 2.2.2.2
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-if-sub)# 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.

12.5.3 Алгоритм настройки L2VPN VPLS

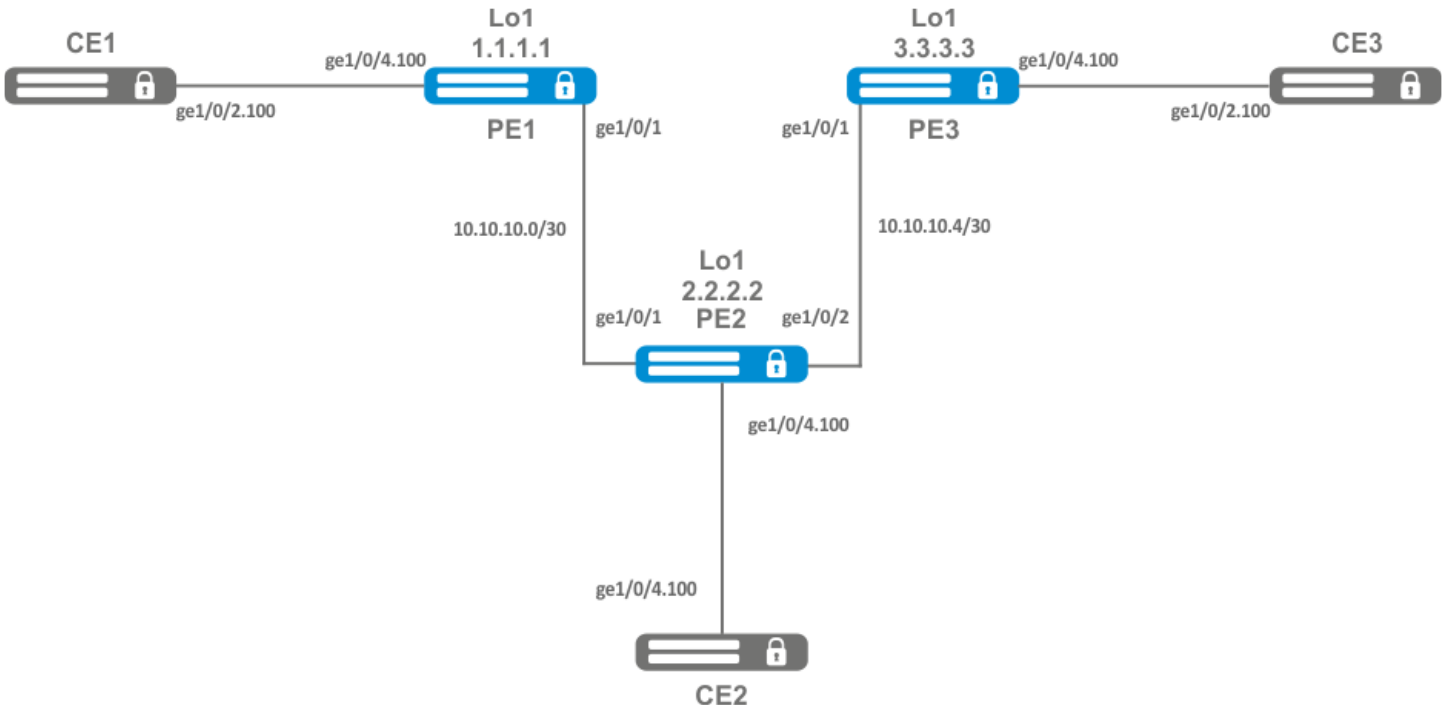
Шаг	Описание	Команда	Ключи
1	Настроить протокол LDP (см. раздел Конфигурирование протокола LDP).		
2	Создать сетевой мост в системе без указания IP-адреса (см. раздел Настройка Bridge).		
3	Создать pw-class в системе и осуществить переход в режим настройки параметров pw-class.	**esr(config-l2vpn)# pw-class <WORD>**	<WORD> – имя pw-class длиной [1..31] символов.
4	Добавить описание для pw-class (необязательно).	**esr(config-l2vpn-pw-class)# description <LINE>**	<LINE> – описание. Задается в виде строки длиной [1..255] символов.
5	Установить значение MTU для pseudo-wire входящих в pw-class (необязательно).	**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 (необязательно).	**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**	

Шаг	Описание	Команда	Ключи
9	Добавить бридж-домен.	**esr (config-l2vpn-vpls)# bridge-group <ID>**	<ID> – идентификатор бридж-домена, задается в виде числа в диапазоне [1..250].
10	Задать транспортный режим (необязательно).	**esr(config-l2vpn-vpls)# transport-mode { ethenet | vlan }**	<ethernet> – режим, при котором при входе в pseudo-wire из заголовка удаляется 802.1Q тег; <vlan> – режим, при котором 802.1Q тег может быть сохранен при передаче через pseudo-wire. Значение по умолчанию: ethernet.
11	Создать pseudo-wire и осуществить переход в режим настройки его параметров.	**esr(config-l2vpn-vpls)# pw <PW_ID> <LSR_ID>**	<PW_ID> – идентификатор psewdowire, задается в виде числа в диапазоне [1..4294967295] <LSR_ID> – идентификатор LSR до которого строится pseudo-wire, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
12	Добавить описание для pseudo-wire (необязательно).	**esr(config-l2vpn-pw)# description <LINE>**	<LINE> – описание. Задается в виде строки длиной [1..255] символов.
13	Задать pw-class для pseudo-wire.	**esr(config-l2vpn-pw)# pw-class <WORD>**	<WORD> – имя pw-class длиной [1..31] символов.
14	Задать адрес LSR до которого устанавливается pseudo-wire (необязательно, если neighbor address совпадает с LSR_ID).	**esr(config-l2vpn-pw)# neighbor-address <ADDR>**	<ADDR> – IP-адрес маршрутизатора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
15	Включить pseudo-wire.	**esr(config-l2vpn-pw)# enable**	
16	В случае если топология создаваемого VPLS-домена требует установить более одного pseudo-wire, повторить шаги с 10 по 14.		
17	В случае если необходимо изменить параметры по умолчанию для targeted LDP-сессии, обратитесь к разделу Конфигурирование параметров сессии в протоколе targeted-LDP.		

12.5.4 Пример настройки L2VPN VPLS

Задача:

Настроить l2vpn таким образом, чтобы маршрутизаторы CE1, CE2, CE3 имели L2-связность через интерфейсы gi1/0/2.100 и gi1/0/4 (CE2).



Решение:

Предварительно необходимо:

- Включить поддержку Jumbo-фреймов с помощью команды **system jumbo-frames** (для вступления изменений в силу требуется перезагрузка устройства);
- Настроить IP-адреса на интерфейсах согласно схеме сети, приведенной на рисунке выше;
- Организовать обмен маршрутами между PE1, PE2 и PE3 при помощи IGP протокола (OSPF, IS-IS).

На маршрутизаторе PE1 создадим бридж-группу и включим ее:

```
PE1# configure
PE1(config)# bridge 10
PE1(config-bridge)# enable
PE1(config-bridge)# exit
```

Интерфейсе в сторону CE1 включим в созданную бридж-группу:

```
PE1(config)# interface gigabitethernet 1/0/4.100
PE1(config-if-sub)# bridge-group 10
PE1(config-if-sub)# exit
```

Выставим на интерфейсе в сторону PE2 значение MTU равным 9600, для того чтобы избежать ситуации с превышением MTU после инкапсуляции MPLS-заголовка, а также отключим межсетевой экран:

```
PE1#(config)# interface gigabitethernet 1/0/1
PE1(config-if-gi)# mtu 9600
PE1(config-if-gi)# ip firewall disable
PE1(config-if-gi)# exit
```

Разрешим прием пакетов с MPLS-заголовком на интерфейсе в сторону MPLS-сети (в данном примере интерфейс в сторону PE2):

```
PE1(config)# mpls
PE1(config-mpls)# forwarding interface gigabitethernet 1/0/1
```

Настроим протокол LDP и включим обнаружение соседей на интерфейсе в сторону PE2:

```
PE1(config-mpls)# ldp
PE1(config-ldp)# router-id 1.1.1.1
PE1(config-ldp)# address-family ipv4
PE1(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1
PE1(config-ldp-af-ipv4-if)# exit
PE1(config-ldp-af-ipv4)# transport-address 1.1.1.1
PE1(config-ldp-af-ipv4)# exit
PE1(config-ldp)# enable
PE1(config-ldp)# exit
```

Создадим pw-class, на основе которого в дальнейшем будет созданы виртуальные каналы (pw). Так как в данном примере на pw будут применяться параметры по умолчанию, достаточно будет указать имя класса:

```
PE1(config-mpls)# l2vpn
PE1(config-l2vpn)# pw-class for_vpls1
PE1(config-l2vpn-pw-class)# exit
```

Создадим новый l2vpn типа vpls и добавим pw до маршрутизаторов PE2 и PE3, идентификатор pw для удобства возьмем равным VID (в данном случае равным 100):

```
PE1(config-l2vpn)# vpls vpls1
PE1(config-l2vpn-vpls)# bridge-group 10
PE1(config-l2vpn-vpls)# pw 100 2.2.2.2
PE1(config-l2vpn-pw)# pw-class for_vpls1
PE1(config-l2vpn-pw)# enable
PE1(config-l2vpn-pw)# exit
PE1(config-l2vpn-vpls)# pw 100 3.3.3.3
PE1(config-l2vpn-pw)# pw-class for_vpls1
PE1(config-l2vpn-pw)# enable
PE1(config-l2vpn-pw)# exit
PE1(config-l2vpn-vpls)# enable
PE1(config-l2vpn-vpls)# end
```

Применим созданную конфигурацию:

```
PE1# commit
PE1# confirm
```

Проведем настройку маршрутизатора PE2 и PE3 по аналогии с PE1:

```
PE2# configure
PE2(config)# bridge 10
PE2(config-bridge)# enable
PE2(config-bridge)# exit
PE2(config)# interface gigabitethernet 1/0/4.100
PE2(config-if-sub)# bridge-group 10
PE2(config-if-sub)# 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-if-sub)# bridge-group 10
PE3(config-if-sub)# exit
PE3(config)# interface gigabitethernet 1/0/1
PE3(config-if-gi)# mtu 9600
PE3(config-if-gi)# ip firewall disable
PE3(config-if-gi)# exit
PE3(config)# mpls
PE3(config-mpls)# forwarding interface gigabitethernet 1/0/1
PE3(config-mpls)# exit
PE3(config)# mpls
PE3(config-mpls)# ldp
```

```
PE3(config-ldp)# enable
PE3(config-ldp)# router-id 3.3.3.3
PE3(config-ldp)# address-family ipv4
PE3(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1
PE3(config-ldp-af-ipv4-if)# exit
PE3(config-ldp-af-ipv4)# transport-address 3.3.3.3
PE3(config-ldp-af-ipv4)# exit
PE3(config-ldp)# exit
PE3(config-mpls)# l2vpn
PE3(config-l2vpn)# pw-class for_vpls
PE3(config-l2vpn-pw-class)# exit
PE3(config-l2vpn)# vpls vpls1
PE3(config-l2vpn-vpls)# enable
PE3(config-l2vpn-vpls)# bridge-group 10
PE3(config-l2vpn-vpls)# pw 100 2.2.2.2
PE3(config-l2vpn-pw)# pw-class for_vpls
PE3(config-l2vpn-pw)# enable
PE3(config-l2vpn-pw)# exit
PE3(config-l2vpn-vpls)# pw 100 1.1.1.1
PE3(config-l2vpn-pw)# pw-class for_vpls
PE3(config-l2vpn-pw)# enable
PE3(config-l2vpn-pw)# end
PE3# commit
PE3# confirm
```

Убедимся в установлении соседства по протоколу LDP и выведем информацию по статусу виртуального канала (pseudowire) между PE1, PE2 и PE3:

```
PE3# show mpls ldp neighbor
Peer LDP ID: 1.1.1.1; Local LDP ID 3.3.3.3
    State: Operational
    TCP connection: 1.1.1.1:646 - 3.3.3.3:45979
    Messages sent/received: 22/22
    Uptime: 00:13:16
    LDP discovery sources:
        3.3.3.3 -> 1.1.1.1
Peer LDP ID: 2.2.2.2; Local LDP ID 3.3.3.3
    State: Operational
    TCP connection: 2.2.2.2:646 - 3.3.3.3:59627
    Messages sent/received: 22/22
    Uptime: 00:13:20
    LDP discovery sources:
        3.3.3.3 -> 2.2.2.2
        gigabitethernet 1/0/1
```

```
PE3# show mpls l2vpn pseudowire
Neighbor                                    PW ID    Type          Status
------------------------------------- ----------      ----------       ------
1.1.1.1                                       100        Ethernet     Up
2.2.2.2                                       100        Ethernet     Up
```

Соседство по протоколу LDP установлено, pseudowire перешел в статус 'UP'. Настройка l2vpn завершена.

12.6 Настройка сервиса L2VPN Kompella mode (BGP Autodiscovery and Signaling)

В отличии от Martini mode, где вся работа ложится на LDP, в данном режиме LDP отводится только работа с транспортными метками. Автообнаружение и построение псевдо-провода возложено на протокол BGP. Регламент описан в rfc 4761.

12.6.1 Алгоритм настройки L2VPN VPLS

Шаг	Описание	Команда	Ключи
1	Настроить протокол LDP (см. раздел Конфигурирование протокола LDP).		
2	Создать сетевой мост в системе без указания IP-адреса (см. раздел Настройка Bridge).		
3	Создать VPLS-домен в системе и осуществить переход в режим настройки параметров VPLS-домена.	**esr(config-l2vpn)# vpls <NAME>**	<NAME> – имя p2p-сервиса, задается строкой до 31 символа.
4	Включить VPLS-туннель.	**esr(config-l2vpn-vpls)# enable**	
5	Добавить бридж-домен.	**esr(config-l2vpn-vpls)# bridge-group <ID>**	<ID> – идентификатор бридж-домена, задается в виде числа в диапазоне [1..250].
6	Перейти в контекст настройки autodiscovery bgp.	**esr(config-l2vpn-vpls)# autodiscovery bgp**	
7	Указать route distinguisher для данного экземпляра VPLS.	**esr(config-bgp)# rd <RD>**	<RD> – значение Route distinguisher, задается в одном из следующих видов: • <ASN>:<nn> – где <ASN> – принимает значение [1..65535], nn – принимает значение [1..65535]; • <ADDR>:<nn> – где <ADDR> имеет вид – AAA.BBB.CCC.DDD/EE и AAA-DDD принимают значения [0..255], а nn – принимает значение [1..65535]; • <4ASN>:<nn> – где <4ASN> – принимает значение [1..4294967295], nn – принимает значение [1..65535].

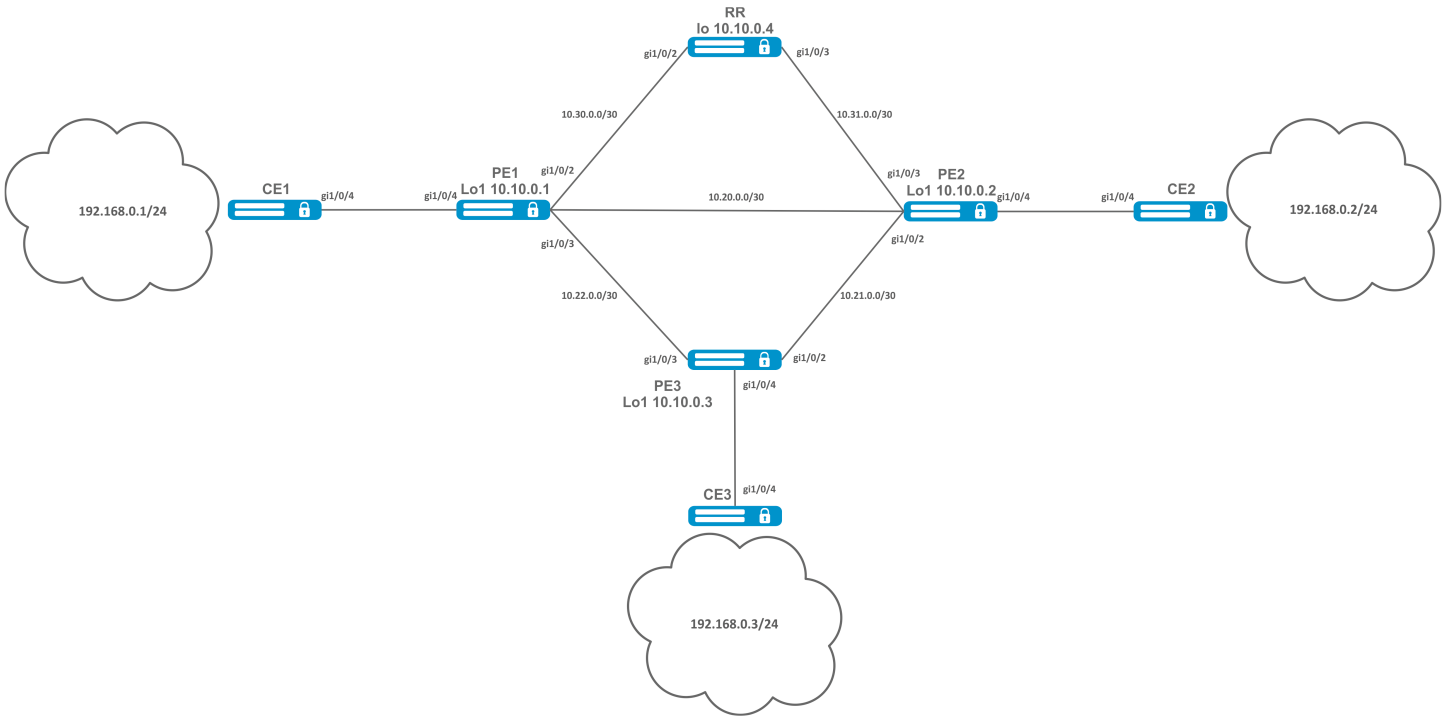
Шаг	Описание	Команда	Ключи
8	Указать route target import для данного экземпляра VPLS.	**esr(config-bgp)# route-target import <RT>**	<RT> – значение route-target, задается в одном из следующих видов: • <ASN>:<nn> – где <ASN> – принимает значение [1..65535], nn – принимает значение [1..65535]; • <ADDR>:<nn> – где <ADDR> имеет вид – AAA.BBB.CCC.DDD/EE и AAA-DDD принимают значения [0..255], а nn – принимает значение [1..65535]; • <4BASN>:<nn> – где <4ASN> – принимает значение [1..4294967295], nn – принимает значение [1..65535].
9	Указать route target export для данного экземпляра VPLS.	**esr(config-bgp)# route-target export <RT>**	<RT> – значение route-target, задается в одном из следующих видов: • <ASN>:<nn> – где <ASN> – принимает значение [1..65535], nn – принимает значение [1..65535]; • <ADDR>:<nn> – где <ADDR> имеет вид – AAA.BBB.CCC.DDD/EE и AAA-DDD принимают значения [0..255], а nn – принимает значение [1..65535]; • <4BASN>:<nn> – где <4ASN> – принимает значение [1..4294967295], nn – принимает значение [1..65535].
10	Указать ve id.	**esr(config-bgp)# ve id <ID>**	<ID> – идентификатор экземпляра VPLS, задается в виде числа в диапазоне [1..16384].
11	Указать vpn id.	**esr (config-bgp)# vpn id <ID>**	<ID> – идентификатор VPN, задается в виде числа в диапазоне [1..4294967295].
12	Указать ve range (необязательно).	**esr (config-bgp)# ve range <RANGE>**	<RANGE> – диапазон идентификаторов пограничных устройств VPLS [8..100].

Шаг	Описание	Команда	Ключи
13	Указать mtu (необязательно).	**esr (config-bgp)# mtu <VALUE>**	<VALUE> – значение MTU [552..10000].
14	Включить игнорирование типа инкапсуляции (необязательно).	**esr(config-bgp)# ignore encapsulation-mismatch**	
15	Включить игнорирование значений MTU (необязательно).	**esr(config-bgp)# ignore mtu-mismatch**	
16	В контексте настройки address-family l2vpn vpls протокола BGP включить передачу расширенных атрибутов.	**esr(config-bgp-neighbor-af)# send-community extended**	

12.6.2 Пример настройки L2VPN VPLS

Задача:

Настроить L2VPN-сервис: все CE-устройства должны работать в рамках одного широковещательного домена.



Решение:

Предварительно необходимо:

- Включить поддержку Jumbo-фреймов с помощью команды **system jumbo-frames** (для вступления изменений в силу требуется перезагрузка устройства);
- Настроить IP-адреса на интерфейсах согласно схеме сети, приведенной на рисунке выше;
- Организовать обмен маршрутами между PE1, PE2, PE3 и RR при помощи IGP-протокола (OSPF, IS-IS).

Настроим маршрутизатор RR:

```
hostname RR

system jumbo-frames

router ospf 1
area 0.0.0.0
enable
exit
enable
exit

interface gigabitethernet 1/0/2
mtu 9500
ip firewall disable
ip address 10.30.0.2/30
ip ospf instance 1
ip ospf
exit
interface gigabitethernet 1/0/3
mtu 9500
ip firewall disable
ip address 10.31.0.2/30
ip ospf instance 1
ip ospf
exit
interface loopback 1
ip address 10.10.0.4/32
ip ospf instance 1
ip ospf
exit
mpls
ldp
router-id 10.10.0.4
address-family ipv4
interface gigabitethernet 1/0/2
exit
interface gigabitethernet 1/0/3
exit
exit
enable
exit
forwarding interface gigabitethernet 1/0/2
forwarding interface gigabitethernet 1/0/3
exit
```

```
RR(config)# router bgp 65500
RR(config-bgp)#   router-id 10.10.0.4
RR(config-bgp)#   neighbor 10.10.0.1
RR(config-bgp-neighbor)#     remote-as 65500
RR(config-bgp-neighbor)#     route-reflector-client
RR(config-bgp-neighbor)#     update-source 10.10.0.4
RR(config-bgp-neighbor)#     address-family l2vpn vpls
RR(config-bgp-neighbor-af)#       send-community extended
RR(config-bgp-neighbor-af)#       enable
RR(config-bgp-neighbor-af)#     exit
RR(config-bgp-neighbor)#     enable
RR(config-bgp-neighbor)#   exit
RR(config-bgp)#   neighbor 10.10.0.2
RR(config-bgp-neighbor)#     remote-as 65500
RR(config-bgp-neighbor)#     route-reflector-client
RR(config-bgp-neighbor)#     update-source 10.10.0.4
RR(config-bgp-neighbor)#     address-family l2vpn vpls
RR(config-bgp-neighbor-af)#       send-community extended
RR(config-bgp-neighbor-af)#       enable
RR(config-bgp-neighbor-af)#     exit
RR(config-bgp-neighbor)#     enable
RR(config-bgp-neighbor)#   exit
RR(config-bgp)#   neighbor 10.10.0.3
RR(config-bgp-neighbor)#     remote-as 65500
RR(config-bgp-neighbor)#     route-reflector-client
RR(config-bgp-neighbor)#     update-source 10.10.0.4
RR(config-bgp-neighbor)#     address-family l2vpn vpls
RR(config-bgp-neighbor-af)#       send-community extended
RR(config-bgp-neighbor-af)#       enable
RR(config-bgp-neighbor-af)#     exit
RR(config-bgp-neighbor)#     enable
RR(config-bgp-neighbor)#   exit
RR(config-bgp)#   enable
```

Настройка протокола BGP на PE-маршрутизаторах:

Предварительная конфигурация

```
hostname PE1

system jumbo-frames

router ospf 1
area 0.0.0.0
enable
exit
enable
exit

interface gigabitethernet 1/0/1
mtu 9500
```

Предварительная конфигурация

```
ip firewall disable
ip address 10.20.0.1/30
ip ospf instance 1
ip ospfexit
interface gigabitethernet 1/0/2
mtu 9500
ip firewall disable
ip address 10.30.0.1/30
ip ospf instance 1
ip ospf
exitinterface gigabitethernet 1/0/3
mtu 9500
ip firewall disable
ip address 10.22.0.1/30
ip ospf instance 1
ip ospf
exit
interface loopback 1
ip address 10.10.0.1/32
ip ospf instance 1
ip ospf
exit
mpls
ldp
router-id 10.10.0.1
address-family ipv4
interface gigabitethernet 1/0/1
exit
interface gigabitethernet 1/0/2
exit
interface gigabitethernet 1/0/3
exit

exit

enable

exit
forwarding interface gigabitethernet 1/0/1
forwarding interface gigabitethernet 1/0/2
forwarding interface gigabitethernet 1/0/3
exit
```

Настройка протокола BGP:

```
PE1(config)# router bgp 65500
PE1(config-bgp)#   neighbor 10.10.0.4
PE2(config-bgp)#   router-id 10.10.0.1
PE1(config-bgp-neighbor)#     remote-as 65500
PE1(config-bgp-neighbor)#     update-source 10.10.0.1
PE1(config-bgp-neighbor)#     address-family l2vpn vpls
PE1(config-bgp-neighbor-af)#       send-community extended
PE1(config-bgp-neighbor-af)#       enable
PE1(config-bgp-neighbor-af)#     exit
PE1(config-bgp-neighbor)#     enable
PE1(config-bgp-neighbor)#   exit
PE1(config-bgp)#   enable
PE1(config-bgp)# exit
```

Проверим, что BGP-сессия успешно установлена с RR:

```
    `   PE1# show bgp neighbors
BGP neighbor is 10.10.0.4
BGP state: Established
Neighbor address: 10.10.0.4
Neighbor AS: 65500
Neighbor ID: 10.10.0.4
Neighbor caps: refresh enhanced-refresh restart-aware AS4
Session: internal multihop AS4
Source address: 10.10.0.1
Weight: 0
Hold timer: 110/180
Keepalive timer: 21/60
Uptime: 7375 s
```

Настройка BGP на PE2:

Предварительная конфигурация

```
hostname PE2

system jumbo-frames

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

Предварительная конфигурация

```
interface gigabitethernet 1/0/1
mtu 9500
ip firewall disable
ip address 10.20.0.2/30
ip ospf instance 1
ip ospf
exit
interface gigabitethernet 1/0/2
mtu 9500
ip firewall disable
ip address 10.21.0.1/30
ip ospf instance 1
ip ospf
exit
interface gigabitethernet 1/0/3
mtu 9500
ip firewall disable
ip address 10.31.0.1/30
ip ospf instance 1
ip ospf
exit
interface loopback 1
ip address 10.10.0.2/32
ip ospf instance 1
ip ospf
exit
mpls
ldp
router-id 10.10.0.2
address-family ipv4
interface gigabitethernet 1/0/1
exit
interface gigabitethernet 1/0/2
exit
interface gigabitethernet 1/0/3
exit
exit

enable

exit
forwarding interface gigabitethernet 1/0/1
forwarding interface gigabitethernet 1/0/2
forwarding interface gigabitethernet 1/0/3
exit
```

```
PE2(config)# router bgp 65500
PE2(config-bgp)#   router-id 10.10.0.2
PE2(config-bgp)#   neighbor 10.10.0.4
PE2(config-bgp-neighbor)#     remote-as 65500
PE2(config-bgp-neighbor)#     update-source 10.10.0.2
PE2(config-bgp-neighbor)#     address-family l2vpn vpls
PE2(config-bgp-neighbor-af)#       send-community extended
PE2(config-bgp-neighbor-af)#       enable
PE2(config-bgp-neighbor-af)#     exit
PE2(config-bgp-neighbor)#     enable
PE2(config-bgp-neighbor)#   exit
PE2(config-bgp)#   enable
PE2(config-bgp)# exit
```

Убедимся, что сессия с RR поднялась успешно:

```
PE2# show bgp neighbors
BGP neighbor is 10.10.0.4
BGP state: Established
Neighbor address: 10.10.0.4
Neighbor AS: 65500
Neighbor ID: 10.10.0.4
Neighbor caps: refresh enhanced-refresh restart-aware AS4
Session: internal multihop AS4
Source address: 10.10.0.2
Weight: 0
Hold timer: 113/180
Keepalive timer: 56/60
Uptime: 47 s
```

Настройка BGP на PE3:

Предварительная конфигурация

```
hostname PE3

system jumbo-frames

router ospf 1
area 0.0.0.0
enable
exit
enable
exit

interface gigabitethernet 1/0/2
mtu 9500
ip firewall disable
ip address 10.21.0.2/30
ip ospf instance 1
ip ospf
exit
interface gigabitethernet 1/0/3
mtu 9500
ip firewall disable
ip address 10.22.0.2/30
ip ospf instance 1
ip ospf
exit
interface loopback 1
ip address 10.10.0.3/24
ip ospf instance 1
ip ospf
exit
mpls
ldp
router-id 10.10.0.3
address-family ipv4
interface gigabitethernet 1/0/2
exit
interface gigabitethernet 1/0/3
exit
exit
enable
exit
forwarding interface gigabitethernet 1/0/2
forwarding interface gigabitethernet 1/0/3
exit
```

```
PE3(config)# router bgp 65500
PE3(config-bgp)#   router-id 10.10.0.3
PE3(config-bgp)#   neighbor 10.10.0.4
PE3(config-bgp-neighbor)#     remote-as 65500
PE3(config-bgp-neighbor)#     update-source 10.10.0.3
PE3(config-bgp-neighbor)#     address-family l2vpn vpls
PE3(config-bgp-neighbor-af)#       send-community extended
PE3(config-bgp-neighbor-af)#       enable
PE3(config-bgp-neighbor-af)#     exit
PE3(config-bgp-neighbor)#     enable
PE3(config-bgp-neighbor)#   exit
PE3(config-bgp)#   enable
PE3(config-bgp)# exit
```

Проверим, что сессия BGP установлена успешно:

```
PE3# show bgp neighbors
BGP neighbor is 10.10.0.4
BGP state: Established
Neighbor address: 10.10.0.4
Neighbor AS: 65500
Neighbor ID: 10.10.0.4
Neighbor caps: refresh enhanced-refresh restart-aware AS4
Session: internal multihop AS4
Source address: 10.10.0.3
Weight: 0
Hold timer: 141/180
Keepalive timer: 27/60
Uptime: 77 s
```

Следующим этапом на каждом PE-маршрутизаторе создадим бридж-домен и включим в него интерфейс (Attachment circuit, AC), смотрящий в сторону CE:

PE1:

```
PE1(config)# bridge 1
PE1(config-bridge)# enable
PE1(config-bridge)# exit
PE1(config)# interface gigabitethernet 1/0/4
PE1(config-if-gi)# mode switchport
PE1(config-if-gi)# bridge-group 1
```

Проверим, что интерфейс включен в бридж-домен:

```
PE1# show interfaces bridge
Bridges      Interfaces
----------   ------------------------------------------------------------
bridge 1     gi1/0/4

PE1# sh interfaces status bridge 1
Interface 'bridge 1' status information:
 Description:          --
 Operational state:    Up
 Administrative state: Up
 Supports broadcast:   Yes
 Supports multicast:   Yes
 MTU:                  1500
 MAC address:          a8:f9:4b:ac:4d:15
 Last change:          4 minutes and 22 seconds
 Mode:                 Routerport
```

PE2:

```
PE2(config)# bridge 1
PE2(config-bridge)# enable
PE2(config-bridge)# exit
PE2(config)# interface gigabitethernet 1/0/4
PE2(config-if-gi)# mode switchport
PE2(config-if-gi)# bridge-group 1
```

```
PE2# show interfaces bridge 1
Bridges      Interfaces
----------   ------------------------------------------------------------
bridge 1     gi1/0/4

PE2# sh interfaces status bridge 1
Interface 'bridge 1' status information:
 Description:          --
 Operational state:    Up
 Administrative state: Up
 Supports broadcast:   Yes
 Supports multicast:   Yes
 MTU:                  1500
 MAC address:          a8:f9:4b:ad:f2:45
 Last change:          10 seconds
 Mode:                 routerport
```

PE3:

```
PE3(config)# bridge 1
PE3(config-bridge)# enable
PE3(config-bridge)# exit
PE3(config)# interface gigabitethernet 1/0/4
PE3(config-if-gi)# mode switchport
PE3(config-if-gi)# bridge-group 1
```

```
PE3# show interfaces bridge
Bridges      Interfaces
----------   ------------------------------------------------------------
bridge 1     gi1/0/4
PE3# sh interfaces status bridge
Interface            Admin   Link    MTU      MAC address          Last change
Mode
                     state   state
------------------   -----   -----   ------   ------------------   -------------------------
----------
bridge 1             Up      Up      1500     a8:f9:4b:ac:df:f0    1 minute and 21 seconds
Routerport

PE3# sh interfaces status bridge 1
Interface 'bridge 1' status information:
 Description:          --
 Operational state:    Up
 Administrative state: Up
 Supports broadcast:   Yes
 Supports multicast:   Yes
 MTU:                  1500
 MAC address:          a8:f9:4b:ac:df:f0
 Last change:          1 minute and 24 seconds
 Mode:                 Routerport
```

Далее выполним настройку VPLS:

PE1:

Переходим в контекст настройки L2VPN и включим в него заранее созданный бридж-домен.

```
PE1(config)# mpls
PE1(config-mpls)# l2vpn
PE1(config-l2vpn)# vpls l2vpn
PE1(config-l2vpn-vpls)# bridge-group 1
```

Укажем RD, RT, VE-ID, VPN ID согласно схеме сети и активируем сервис:

В некоторых случаях можно отказаться от ввода таких параметров, как RD и RT: если указать только VPN ID, то они будут сформированы следующим образом: <номер AS> : <vpn-id>. Например, есть номер автономной системы AS 65550, vpn-id указан 10, тогда сгенерируются следующие параметры:
RD - 65550: 10.
RT import/export - 65550:10.

```
PE1(config-l2vpn-vpls)# autodiscovery bgp
PE1(config-bgp)# rd 65500:100
PE1(config-bgp)# route-target import 65500:100
PE1(config-bgp)# route-target export 65500:100
PE1(config-bgp)# ve id 1
PE1(config-bgp)# vpn id 1
PE1(config-bgp)# exit
PE1(config-l2vpn-vpls)# enable
```

После активации сервиса проверим, что в таблице l2vpn появилась маршрутная информация и она анонсируется на RR:

```
PE1# show bgp l2vpn vpls all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes Route Distinguisher   VID   VBO   VBS   Next hop        Metric     LocPrf     Weight Path
----- --------------------- ----- ----- ----- --------------- ---------- ---------- ------
-------------------
*>    65500:100             1     1     10    --              --         --         --


PE1# show bgp l2vpn vpls all neighbor 10.10.0.4 advertise-routes
Origin codes: i - IGP, e - EGP, ? - incomplete

Route Distinguisher   VID   VBO   VBS   Next hop        Metric     LocPrf     Path
--------------------- ----- ----- ----- --------------- ---------- ----------
----------------------
65500:100             1     1     10    10.10.0.1       --         100        i


* Подробный вывод анонсированного маршрута *

PE1# show bgp l2vpn vpls all neighbor 10.10.0.4 advertise-routes  ve-id 1 block
-offset 1
BGP routing table entry for 65500:100 VE ID 1 VE Block Offset 1
    VE Block Size:      10
    Label Base:         86
    Next hop:           10.10.0.1
    AS path:            --
    Origin:             IGP
    Local preference:   100
    Extended Community: RT:65500:100
    Layer2-info:        encaps (VPLS), control flags(0x00), MTU (1500)
```

Переходим к настройке PE2:

```
PE2(config-mpls)# l2vpn
PE2(config-l2vpn)# vpls l2vpn
PE2(config-l2vpn-vpls)# bridge-group 1
PE2(config-l2vpn-vpls)# autodiscovery bgp
PE2(config-bgp)# rd 65500:100
```

```
PE2(config-bgp)# route-target export 65500:100
PE2(config-bgp)# route-target import  65500:100
PE2(config-bgp)# vpn id 2
PE2(config-bgp)# ve id 2
PE2(config-bgp)# exit
PE2(config-l2vpn-vpls)# enable
```

Проверим, что PE2 анонсирует маршрутную информацию на RR:

```
PE2# show bgp l2vpn vpls all  neighbor 10.10.0.4 advertise-routes
Origin codes: i - IGP, e - EGP, ? - incomplete

Route Distinguisher   VID   VBO   VBS   Next hop        Metric     LocPrf     Path
--------------------- ----- ----- ----- --------------- ---------- ----------
----------------------
65500:100             2     1     10    10.10.0.2       --         100        i
```

В таблице l2vpn видны как и свои маршруты, так и от PE1:

```
PE2# show bgp l2vpn vpls all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes Route Distinguisher   VID   VBO   VBS   Next hop        Metric     LocPrf     Weight Path
----- --------------------- ----- ----- ----- --------------- ---------- ---------- ------
-------------------
*>    65500:100             2     1     10    --              --         --         --
*>i   65500:100             1     1     10    10.10.0.1       --         100        0      i
```

Просмотреть вычисленные сервисные метки можно следующим образом:

1)

```
PE2# show mpls l2vpn bindings
Neighbor: 10.10.0.1, PW ID: 2, VE ID: 1
Local label: 45
Encasulation Type: VPLS
Control flags: 0x00
MTU: 1500
Remote label: 87
Encasulation Type: VPLS
Control flags: 0x00
MTU: 1500
```

2)

```
PE2# show mpls forwarding-table
Local       Outgoing          Prefix              Outgoing                Next Hop
label       label             or tunnel ID        Interface
--------    --------          ------------------  -----------------
-----------------------------------

45          87                PW ID 2                   --                10.10.0.1
```

Проверим состояние сервиса:

```
PE2# show mpls l2vpn vpls l2vpn
VPLS: l2vpn
    bridge 1:
        MTU:    1500
        Status: Up
    ACs:
      gigabitethernet 1/0/4:
        MTU:    1500
        Status: Up
    PWs:
      PW ID 2, Neighbor 10.10.0.1:
        MTU:         1500
        Last change: 00:21:33
        Status:      Up
```

Перейдем к настройке PE3:

```
PE3#    config
PE3(config)# mpls
PE3(config-mpls)# l2vpn
PE3(config-l2vpn)# vpls l2vpn
PE3(config-l2vpn-vpls)# bridge-group 1
PE3(config-l2vpn-vpls)# autodiscovery bgp
PE3(config-bgp)# rd 65500:100
PE3(config-bgp)# route-target export 65500:100
PE3(config-bgp)# route-target import  65500:100
PE3(config-bgp)# ve id 3
PE3(config-bgp)# vpn id 3
PE3(config-bgp)# exit
PE3(config-l2vpn-vpls)# enable
```

Проверим маршрутную информацию на PE3:

```
PE3# show bgp l2vpn vpls all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes Route Distinguisher   VID   VBO   VBS   Next hop        Metric     LocPrf     Weight Path
----- --------------------- ----- ----- ----- --------------- ---------- ---------- ------
-------------------
*>    65500:100             3     1     10    --              --         --         --
*>i   65500:100             2     1     10    10.10.0.2       --         100        0      i
*>i   65500:100             1     1     10    10.10.0.1       --         100        0      i
```

Убедимся, что PE3 анонсирует маршрутную информацию на RR:

```
PE3# show bgp l2vpn vpls all neighbor 10.10.0.4 advertise-routes
Origin codes: i - IGP, e - EGP, ? - incomplete

Route Distinguisher   VID   VBO   VBS   Next hop        Metric     LocPrf     Path
--------------------- ----- ----- ----- --------------- ---------- ----------
----------------------
65500:100             3     1     10    10.10.0.3       --         100        i
```

Проверим, что псевдо-провод построен до обеих PE и находится в статусе 'UP':

```
PE3# show mpls l2vpn vpls l2vpn
VPLS: l2vpn
    bridge 1:
        MTU:    1500
        Status: Up
    ACs:
      gigabitethernet 1/0/4:
        MTU:    1500
        Status: Up
    PWs:
      PW ID 3, Neighbor 10.10.0.2:
        MTU:         1500
        Last change: 00:06:08
        Status:      Up
      PW ID 3, Neighbor 10.10.0.1:
        MTU:         1500
        Last change: 00:06:08
        Status:      Up
```

Проверим сетевую доступность клиентских устройств (CE):

```
CE3# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
!!!!!
--- 192.168.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 0.173/0.208/0.290/0.045 ms
CE3# ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
!!!!!
--- 192.168.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 0.158/0.204/0.255/0.032 ms

PE3# sh mac address-table bridge 1
VID     MAC Address          Interface                       Type
-----   ------------------   -----------------------------   -------
--      a8:f9:4b:aa:11:08    gigabitethernet 1/0/4           Dynamic
--      a8:f9:4b:aa:11:06    dypseudowire 3_10.10.0.1        Dynamic
--      a8:f9:4b:aa:11:07    dypseudowire 3_10.10.0.2        Dynamic
3 valid mac entries
```

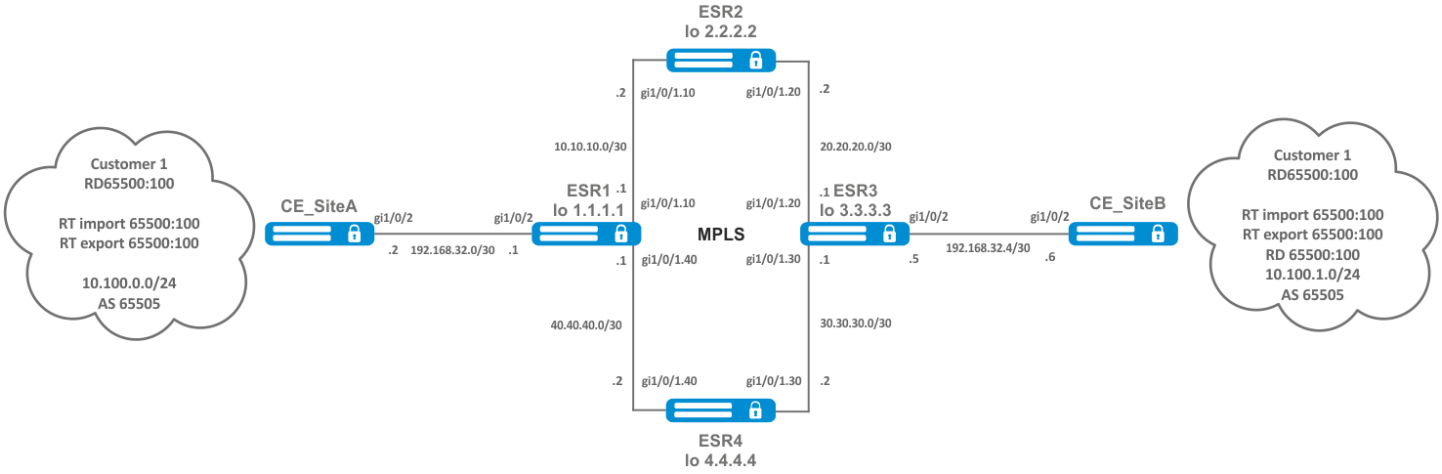
Настройка L2VPN-сервиса завершена.

Настроим BGP Route Reflector для address family l2vpn:

12.7 Настройка сервиса L3VPN

Сервис L3VPN позволяет объединить распределенные клиентские IP-сети и обеспечить передачу трафика между ними с рамках единой VRF.

⚠ В текущей реализации протокола MP-BGP поддержана передача только VPN-IPv4 маршрутов (AFI = 1, SAFI = 128).



12.7.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Настроить адресацию и один из протоколов IGP на всех P и PE-маршрутизаторах.		
2	Настроить распространение транспортных меток по протоколу LDP.		
3	Создать VRF.	**esr(config)# ip vrf <VRF>**	<VRF> – имя экземпляра VRF, задается строкой до 31 символа.
4	Указать route distinguisher для данного VRF.	**esr(config-vrf)# rd <RD>**	<RD> – значение Route distinguisher, задается в одном из следующих видов: • <ASN>:<nn> – где <ASN> – принимает значение [1..65535], nn – принимает значение [1..65535]; • <ADDR>:<nn> – где <ADDR> имеет вид – AAA.BBB.CCC.DDD/EE и AAA-DDD принимают значения [0..255], а nn – принимает значение [1..65535]; • <4ASN>:<nn> – где <4ASN> – принимает значение [1..4294967295], nn – принимает значение [1..65535].

Шаг	Описание	Команда	Ключи
5	Указать route target import для данного VRF.	**esr(config-vrf)# route-target import <RT>**	<RT> – значение route-target, задается в одном из следующих видов: • <ASN>:<nn> – где <ASN> – принимает значение [1..65535], nn – принимает значение [1..65535]; • <ADDR>:<nn> – где <ADDR> имеет вид – AAA.BBB.CCC.DDD/EE и AAA-DDD принимают значения [0..255], а nn – принимает значение [1..65535]; • <4BASN>:<nn> – где <4ASN> – принимает значение [1..4294967295], nn – принимает значение [1..65535].
6	Указать route target export для данного VRF.	**esr(config-vrf)# route-target export <RT>**	<RT> – значение route-target, задается в одном из следующих видов: • <ASN>:<nn> – где <ASN> – принимает значение [1..65535], nn – принимает значение [1..65535]; • <ADDR>:<nn> – где <ADDR> имеет вид – AAA.BBB.CCC.DDD/EE и AAA-DDD принимают значения [0..255], а nn – принимает значение [1..65535]; • <4BASN>:<nn> – где <4ASN> – принимает значение [1..4294967295], nn – принимает значение [1..65535].

Шаг	Описание	Команда	Ключи
7	Указать разрешенное количество маршрутов для данного VRF.	**esr(config-vrf)# ip protocols <PROTOCOLS> max-routes <VALUE>**	<PROTOCOL> – вид протокола, принимает значения: rip (только в глобальном режиме), ospf, isis, bgp; <VALUE> – количество маршрутов в маршрутной таблице, принимает значения в диапазоне: • BGP: ESR-1000/1200/1500/1511 (rev.B)/1700/3100/3150/3200/3200L/3250/3300/3350/ – [1..5000000]; ESR-20/21/30/31/100/200 – [1..2500000]; ESR-10/12V/12VF/15/15R/15VF – [1.. 1000000]. • OSPF и IS-IS: ESR-1000/1200/1500/1511 (rev.B)/1700/3100/3150/3200/3200L/3250/3300/3350 – [1..500000]; ESR-20/21/30/31/100/200 – [1..300000]; ESR-10/12V/12VF/15/15VF/15R – [1..30000].
8	В рамках настройки address-family VPNv4 протокола BGP включить передачу расширенных атрибутов.	**esr(config-bgp-neighbor-af)# send-community extended**	

12.7.2 Пример настройки

Задача:

Настроить L3VPN на базе технологии MPLS между ESR1 и ESR3. Конечным результатом настройки является появление связности между узлами, подключенными к VRF на различных маршрутизаторах сети (то есть объединение VRF на разных маршрутизаторах через MPLS-транспорт). При этом должна быть обеспечена передача сервисных MPLS-меток для сервиса L3VPN посредством MP-BGP и передача транспортных меток для достижения nexthop-адресов полученных BGP-маршрутов.

Решение:

Настройка адресации и включение IGP на P/PE-маршрутизаторах

ESR1

```
ESR1(config)# router ospf log-adjacency-changes
ESR1(config)# router ospf 1
ESR1(config-ospf)# router-id 1.1.1.1
ESR1(config-ospf)# area 0.0.0.0
ESR1(config-ospf-area)# enable
ESR1(config-ospf-area)# exit
ESR1(config-ospf)# enable
ESR1(config-ospf)# exit
ESR1(config)#
ESR1(config)# interface loopback 1
ESR1(config-loopback)# ip address 1.1.1.1/32
ESR1(config-loopback)# ip ospf instance 1
ESR1(config-loopback)# ip ospf
ESR1(config-loopback)# exit
ESR1(config)#
ESR1(config)# interface gigabitethernet 1/0/1.10
ESR1(config-if-sub)# ip firewall disable
ESR1(config-if-sub)# ip address 10.10.10.1/30
ESR1(config-if-sub)# ip ospf instance 1
ESR1(config-if-sub)# ip ospf
ESR1(config-if-sub)# exit
ESR1(config)#
ESR1(config)# interface gigabitethernet 1/0/1.40
ESR1(config-if-sub)# ip firewall disable
ESR1(config-if-sub)# ip address 40.40.40.1/30
ESR1(config-if-sub)# ip ospf instance 1
ESR1(config-if-sub)# ip ospf
ESR1(config-if-sub)# exit
ESR1(config)#
ESR1(config)# system jumbo-frames
ESR1(config)# do commit
ESR1(config)# do confirm
```

ESR2

```
ESR2(config)# router ospf log-adjacency-changes
ESR2(config)# router ospf 1
ESR2(config-ospf)# router-id 2.2.2.2
ESR2(config-ospf)# area 0.0.0.0
ESR2(config-ospf-area)# enable
ESR2(config-ospf-area)# exit
ESR2(config-ospf)# enable
ESR2(config-ospf)# exit
ESR2(config)#
ESR2(config)# interface loopback 1
ESR2(config-loopback)# ip address 2.2.2.2/32
ESR2(config-loopback)# ip ospf instance 1
ESR2(config-loopback)# ip ospf
ESR2(config-loopback)# exit
ESR2(config)#
ESR2(config)# interface gigabitethernet 1/0/1.10
ESR2(config-if-sub)# ip firewall disable
ESR2(config-if-sub)# ip address 10.10.10.2/30
ESR2(config-if-sub)# ip ospf instance 1
ESR2(config-if-sub)# ip ospf
ESR2(config-if-sub)# exit
ESR2(config)#
ESR2(config)# interface gigabitethernet 1/0/1.20
ESR2(config-if-sub)# ip firewall disable
ESR2(config-if-sub)# ip address 20.20.20.2/30
ESR2(config-if-sub)# ip ospf instance 1
ESR2(config-if-sub)# ip ospf
ESR2(config-if-sub)# exit
ESR2(config)#
ESR2(config)# system jumbo-frames
ESR2(config)# do commit
ESR2(config)# do confirm
```

ESR3

```
ESR3(config)# router ospf log-adjacency-changes
ESR3(config)# router ospf 1
ESR3(config-ospf)# router-id 3.3.3.3
ESR3(config-ospf)# area 0.0.0.0
ESR3(config-ospf-area)# enable
ESR3(config-ospf-area)# exit
ESR3(config-ospf)# enable
ESR3(config-ospf)# exit
ESR3(config)#
ESR3(config)# interface loopback 1
ESR3(config-loopback)# ip address 3.3.3.3/32
ESR3(config-loopback)# ip ospf instance 1
ESR3(config-loopback)# ip ospf
ESR3(config-loopback)# exit
ESR3(config)#
ESR3(config)# interface gigabitethernet 1/0/1.20
ESR3(config-if-sub)# ip firewall disable
ESR3(config-if-sub)# ip address 20.20.20.1/30
ESR3(config-if-sub)# ip ospf instance 1
ESR3(config-if-sub)# ip ospf
ESR3(config-if-sub)# exit
ESR3(config)#
ESR3(config)# interface gigabitethernet 1/0/1.30
ESR3(config-if-sub)# ip firewall disable
ESR3(config-if-sub)# ip address 30.30.30.1/30
ESR3(config-if-sub)# ip ospf instance 1
ESR3(config-if-sub)# ip ospf
ESR3(config-if-sub)# exit
ESR3(config)#
ESR3(config)# system jumbo-frames
ESR3(config)# do commit
ESR3(config)# do confirm
```

ESR4

```
ESR4(config)# router ospf log-adjacency-changes
ESR4(config)# router ospf 1
ESR4(config-ospf)# router-id 4.4.4.4
ESR4(config-ospf)# area 0.0.0.0
ESR4(config-ospf-area)# enable
ESR4(config-ospf-area)# exit
ESR4(config-ospf)# enable
ESR4(config-ospf)# exit
ESR4(config)#
ESR4(config)# interface loopback 1
ESR4(config-loopback)# ip address 4.4.4.4/32
ESR4(config-loopback)# ip ospf instance 1
ESR4(config-loopback)# ip ospf
ESR4(config-loopback)# exit
ESR4(config)#
ESR4(config)# interface gigabitethernet 1/0/1.40
ESR4(config-if-sub)# ip firewall disable
ESR4(config-if-sub)# ip address 40.40.40.2/30
ESR4(config-if-sub)# ip ospf instance 1
ESR4(config-if-sub)# ip ospf
ESR4(config-if-sub)# exit
ESR4(config)#
ESR4(config)# interface gigabitethernet 1/0/1.30
ESR4(config-if-sub)# ip firewall disable
ESR4(config-if-sub)# ip address 30.30.30.2/30
ESR4(config-if-sub)# ip ospf instance 1
ESR4(config-if-sub)# ip ospf
ESR4(config-if-sub)# exit
ESR4(config)#
ESR4(config)# system jumbo-frames
ESR4(config)# do commit
ESR4(config)# do confirm
```

Необходимо убедиться, что протокол OSPF запущен на каждом маршрутизаторе:

```
ESR1# show ip ospf neighbors


Router ID        Pri  State          DTime  Interface      Router IP
---------        ---  -----          -----  -------------  ---------
2.2.2.2          128  Full/BDR       00:39  gi1/0/1.10     10.10.10.2
4.4.4.4          128  Full/BDR       00:32  gi1/0/1.40     40.40.40.2


ESR1# show ip ospf
O       40.40.40.0/30       [150/10]          dev gi1/0/1.40                    [ospf1
1970-01-08]  (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)
```

Настройка LDP на P/PE-маршрутизаторах

ESR1

```
ESR1# config
ESR1(config)# mpls
ESR1(config-mpls)# ldp
ESR1(config-ldp)# address-family ipv4
ESR1(config-ldp-af-ipv4)# transport-address 1.1.1.1
ESR1(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1.10
ESR1(config-ldp-af-ipv4-if)# exit
ESR1(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1.40
ESR1(config-ldp-af-ipv4-if)# exit
ESR1(config-ldp-af-ipv4)# exit
ESR1(config-ldp)# enable
ESR1(config-ldp)# exit
ESR1(config-mpls)# forwarding interface gigabitethernet 1/0/1.10
ESR1(config-mpls)# forwarding interface gigabitethernet 1/0/1.40
ESR1(config-mpls)# exit
ESR1(config)# do commit
ESR1(config)# do confirm
```

ESR2

```
ESR2# config
ESR2(config)# mpls
ESR2(config-mpls)# ldp
ESR2(config-ldp)# address-family ipv4
ESR2(config-ldp-af-ipv4)# transport-address 2.2.2.2
ESR2(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1.10
ESR2(config-ldp-af-ipv4-if)# exit
ESR2(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1.20
ESR2(config-ldp-af-ipv4-if)# exit
ESR2(config-ldp-af-ipv4)# exit
ESR2(config-ldp)# enable
ESR2(config-ldp)# exit
ESR2(config-mpls)# forwarding interface gigabitethernet 1/0/1.10
ESR2(config-mpls)# forwarding interface gigabitethernet 1/0/1.20
ESR2(config-mpls)# exit
ESR2(config)# do commit
ESR2(config)# do confirm
```

ESR3

```
ESR3# config
ESR3(config)# mpls
ESR3(config-mpls)# ldp
ESR3(config-ldp)# address-family ipv4
ESR3(config-ldp-af-ipv4)# transport-address 3.3.3.3
ESR3(config-ldp-af-ipv4)#  interface gigabitethernet 1/0/1.20
ESR3(config-ldp-af-ipv4-if)# exit
ESR3(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1.30
ESR3(config-ldp-af-ipv4-if)# exit
ESR3(config-ldp-af-ipv4)# exit
ESR3(config-ldp)# enable
ESR3(config-ldp)# exit
ESR3(config-mpls)# forwarding interface gigabitethernet 1/0/1.20
ESR3(config-mpls)# forwarding interface gigabitethernet 1/0/1.30
ESR3(config-mpls)# exit
ESR3(config)# do commit
ESR3(config)# do confirm
```

ESR4

```
ESR4# config
ESR4(config)# mpls
ESR4(config-mpls)# ldp
ESR4(config-ldp)# address-family ipv4
ESR4(config-ldp-af-ipv4)# transport-address 4.4.4.4
ESR4(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1.30
ESR4(config-ldp-af-ipv4-if)# exit
ESR4(config-ldp-af-ipv4)# interface gigabitethernet 1/0/1.40
ESR4(config-ldp-af-ipv4-if)# exit
ESR4(config-ldp-af-ipv4)# exit
ESR4(config-ldp)# enable
ESR4(config-ldp)# exit
ESR4(config-mpls)# forwarding interface gigabitethernet 1/0/1.30
ESR4(config-mpls)# forwarding interface gigabitethernet 1/0/1.40
ESR4(config-mpls)# exit
ESR4(config)# do commit
ESR4(config)# do confirm
```

Для проверки сходимости LDP можно воспользоваться одной из следующих команд:

```
ESR1# show mpls ldp neighbor
Peer LDP ID: 2.2.2.2; Local LDP ID 1.1.1.1
    State: Operational
    TCP connection: 2.2.2.2:33933 - 1.1.1.1:646
    Messages sent/received: 1059/1070
    Uptime: 17:32:07
    LDP discovery sources:
        gigabitethernet 1/0/1.10
Peer LDP ID: 4.4.4.4; Local LDP ID 1.1.1.1
    State: Operational
    TCP connection: 4.4.4.4:40894 - 1.1.1.1:646
    Messages sent/received: 1376/1386
    Uptime: 22:38:38
    LDP discovery sources:
        gigabitethernet 1/0/1.40
```

Настройка MP-BGP

Создадим VRF на ESR1 и ESR3 соответственно. Укажем RD, rt-export/import в соответствии со схемой, настроим интерфейс для взаимодействия с CE (CE-SiteA и CE-SiteB). Дополнительно создадим route-map для разрешения анонсирования маршрутов по протоколу BGP:

⚠ Без указания атрибутов RD и RT маршрутная информация не попадет в таблицу VPNv4.

ESR1

```
ESR1(config)# ip vrf Customer1
ESR1(config-vrf)# ip protocols bgp max-routes 1000
ESR1(config-vrf)# rd 65500:100
ESR1(config-vrf)# route-target import 65500:100
ESR1(config-vrf)# route-target export 65500:100
ESR1(config-vrf)# exit
ESR1(config)# interface gigabitethernet 1/0/2
ESR1(config-if-gi)# ip vrf forwarding Customer1
ESR1(config-if-gi)# description "Customer1"
ESR1(config-if-gi)# ip firewall disable
ESR1(config-if-gi)# ip address 192.168.32.1/30
ESR1(config-if-gi)# exit
ESR1(config)# route-map OUTPUT
ESR1(config-route-map)# rule 1
ESR1(config-route-map-rule)# action permit
ESR1(config-route-map-rule)# exit
ESR1(config-route-map)# exit
ESR1(config)# do commit
ESR1(config)# do confirm
```

ESR3

```
ESR3(config)# ip vrf Customer1
ESR3(config-vrf)# ip protocols bgp max-routes 1000
ESR3(config-vrf)# rd 65500:100
ESR3(config-vrf)# route-target export 65500:100
ESR3(config-vrf)# route-target import 65500:100
ESR3(config-vrf)# exit
ESR3(config)# interface gigabitethernet 1/0/2
ESR3(config-if-gi)# ip vrf forwarding Customer1
ESR3(config-if-gi)# description "Customer1"
ESR3(config-if-gi)# ip firewall disable
ESR3(config-if-gi)# ip address 192.168.32.5/30
ESR3(config-if-gi)# exit
ESR3(config)# route-map OUTPUT
ESR3(config-route-map)# rule 1
ESR3(config-route-map-rule)# action permit
ESR3(config-route-map-rule)# exit
ESR3(config-route-map)# exit
ESR3(config)# do commit
ESR3(config)# do confirm
```

Настроим iBGP между ESR1 и ESR3. Включим отправку extended community на обоих устройствах:

ESR1

```
ESR1(config)# router bgp log-neighbor-changes
ESR1(config)# router bgp 65500
ESR1(config-bgp)# router-id 1.1.1.1
ESR1(config-bgp)# enable
ESR1(config-bgp)# neighbor 3.3.3.3
ESR1(config-bgp-neighbor)# remote-as 65500
ESR1(config-bgp-neighbor)# update-source 1.1.1.1
ESR1(config-bgp-neighbor)# enable
ESR1(config-bgp-neighbor)# address-family vpnv4 unicast
ESR1(config-bgp-neighbor-af)# send-community extended
ESR1(config-bgp-neighbor-af)# enable
ESR1(config-bgp-neighbor-af)# exit
ESR1(config-bgp-neighbor)# exit
ESR1(config-bgp)# exit
ESR1(config)# do commit
ESR1(config)# do confirm
```

ESR3

```
ESR3(config)# router bgp log-neighbor-changes
ESR3(config)# router bgp 65500
ESR3(config-bgp)# router-id 3.3.3.3
ESR3(config-bgp)# enable
ESR3(config-bgp)# neighbor 1.1.1.1
ESR3(config-bgp-neighbor)# remote-as 65500
ESR3(config-bgp-neighbor)# update-source 3.3.3.3
ESR3(config-bgp-neighbor)# enable
ESR3(config-bgp-neighbor)# address-family vpnv4 unicast
ESR3(config-bgp-neighbor-af)# send-community extended
ESR3(config-bgp-neighbor-af)# enable
ESR3(config-bgp-neighbor-af)# exit
ESR3(config-bgp-neighbor)# exit
ESR3(config-bgp)# exit
ESR3(config)# do commit
ESR3(config)# do confirm
```

Необходимо убедиться, что BGP-сессия успешно установлена:

```
ESR1# show bgp neighbors
BGP neighbor is 3.3.3.3
    BGP state: Established
    Neighbor address: 3.3.3.3
    Neighbor AS: 65500
    Neighbor ID: 3.3.3.3
    Neighbor caps: refresh enhanced-refresh restart-aware AS4
    Session: internal multihop AS4
    Source address: 1.1.1.1
    Weight: 0
    Hold timer: 126/180
    Keepalive timer: 40/60
    Address family ipv4 unicast:
    Default originate: No
    Default information originate: No
    Uptime: 88495 s
```

Настройка маршрутизации PE-CE

Согласно топологии, Customer1 анонсирует по BGP (AS65505) подсеть 10.100.0.0/24. Необходимо настроить соответствующие интерфейсы, eBGP между ESR1 и CE_SiteA. Также необходимо разрешить анонсирование маршрутов в сторону PE.

По умолчанию для eBGP анонсирование маршрутов запрещено, необходимо настроить разрешающее правило. Для iBGP анонсирование маршрутов разрешено.

Необходимая конфигурация на маршрутизаторе CE-SiteA:

CE _SiteA

```
CE-SiteA(config)# interface gigabitethernet 1/0/2
CE-SiteA(config-if-gi)# ip firewall disable
CE-SiteA(config-if-gi)# ip address 192.168.32.2/30
CE-SiteA(config-if-gi)# exit
CE-SiteA(config)# interface loopback 1
CE-SiteA(config-loopback)# ip address 10.100.0.1/24
CE-SiteA(config-loopback)# exit
CE-SiteA(config)# route-map OUTPUT
CE-SiteA(config-route-map)# rule 1
CE-SiteA(config-route-map-rule)# match ip address 10.100.0.0/24
CE-SiteA(config-route-map-rule)# action permit
CE-SiteA(config-route-map-rule)# exit
CE-SiteA(config-route-map)# exit
CE-SiteA(config)# router bgp log-neighbor-changes
CE-SiteA(config)# router bgp 65505
CE-SiteA(config-bgp)# router-id 192.168.32.1
CE-SiteA(config-bgp)# neighbor 192.168.32.1
CE-SiteA(config-bgp-neighbor)# remote-as 65500
CE-SiteA(config-bgp-neighbor)# allow-local-as 1
CE-SiteA(config-bgp-neighbor)# update-source 192.168.32.2
CE-SiteA(config-bgp-neighbor)# address-family ipv4 unicast
CE-SiteA(config-bgp-neighbor-af)# route-map OUTPUT out
CE-SiteA(config-bgp-neighbor-af)# enable
CE-SiteA(config-bgp-neighbor-af)# exit
CE-SiteA(config-bgp-neighbor)# enable
CE-SiteA(config-bgp-neighbor)# exit
CE-SiteA(config-bgp)# address-family ipv4 unicast
CE-SiteA(config-bgp-af)# network 10.100.0.0/24
CE-SiteA(config-bgp-af)# exit
CE-SiteA(config-bgp)# enable
CE-SiteA(config-bgp)# exit
CE-SiteA(config)# do commit
CE-SiteA(config)# do confirm
```

Переходим к настройке eBGP на маршрутизаторе ESR1.

Создадим eBGP-сессию с CE_SiteA и разрешим передачу маршрутов BGP-пиру:

ESR1

```
ESR1(config)# router bgp 65500
ESR1(config-bgp)# vrf Customer1
ESR1(config-bgp-vrf)# router-id 192.168.32.1
ESR1(config-bgp-vrf)# neighbor 192.168.32.2
ESR1(config-bgp-vrf-neighbor)# remote-as 65505
ESR1(config-bgp-vrf-neighbor)# update-source 192.168.32.1
ESR1(config-bgp-vrf-neighbor)# address-family ipv4 unicast
ESR1(config-bgp-neighbor-af-vrf)# route-map OUTPUT out
ESR1(config-bgp-neighbor-af-vrf)# enable
ESR1(config-bgp-neighbor-af-vrf)# exit
ESR1(config-bgp-vrf-neighbor)# enable
ESR1(config-bgp-vrf-neighbor)# exit
ESR1(config-bgp-vrf)# address-family ipv4 unicast
ESR1(config-bgp-vrf-af)# redistribute connected
ESR1(config-bgp-vrf-af)# redistribute bgp 65500
ESR1(config-bgp-vrf-af)# exit
ESR1(config-bgp-vrf)# enable
ESR1(config-bgp-vrf)# exit
ESR1(config-bgp)# exit
ESR1(config)# do commit
ESR1(config)# do confirm
```

⚠ При передаче маршрутов из VRF в таблицу VPNv4 достаточно настроить передачу (redistribute) маршрутов в этом VRF.
Пример конфигурации передачи в VPNv4 таблицу connected- и static-сетей:

```
ESR1(config)# router bgp 65500
ESR1(config-bgp)# router-id 1.1.1.1
ESR1(config-bgp)# neighbor 3.3.3.3
ESR1(config-bgp-neighbor)# remote-as 65500
ESR1(config-bgp-neighbor)# update-source 1.1.1.1
ESR1(config-bgp-neighbor)# enable
ESR1(config-bgp-neighbor)# address-family vpnv4 unicast
ESR1(config-bgp-neighbor-af)# send-community extended
ESR1(config-bgp-neighbor-af)# enable
ESR1(config-bgp-neighbor-af)# exit
ESR1(config-bgp-neighbor)# exit
ESR1(config-bgp)# enable
EESR1(config-bgp)# vrf Customer1
ESR1(config-bgp-vrf)# address-family ipv4 unicast
ESR1(config-bgp-vrf-af)# redistribute connected
ESR1(config-bgp-vrf-af)# redistribute static
ESR1(config-bgp-vrf-af)# exit
ESR1(config-bgp-vrf)# exit
ESR1(config-bgp)# exit
ESR1(config)# do commit
ESR1(config)# do confirm
```

Для проверки принятых и анонсированных маршрутов можно воспользоваться следующими командами:

```
ESR1# show bgp vpnv4 unicast vrf Customer1 neighbors 192.168.32.2 advertise-routes
Status codes: u - unicast, b - broadcast, m - multicast, a - anycast
              * - valid, > - best
Origin codes: i - IGP, e - EGP, ? - incomplete


     Network              Next Hop            Metric  LocPrf      Weight Path
*> u 10.100.1.0/24        192.168.32.1                100                 65500 i
*> u 192.168.32.4/30      192.168.32.1                100                 65500 i
```

Вывод анонсируемых маршрутов для определенного пира. Маршрутная информация отображается после применения фильтрации:

```
ESR1# show bgp vpnv4 unicast vrf Customer1 neighbors 192.168.32.2 routes
Status codes: u - unicast, b - broadcast, m - multicast, a - anycast
              * - valid, > - best
Origin codes: i - IGP, e - EGP, ? - incomplete


     Network              Next Hop            Metric  LocPrf      Weight Path
*> u 10.100.0.0/24        192.168.32.2                100         0      65505
```

Вывод принятой маршрутной информации от определенного пира. Маршрутная информация отображается после применения фильтрации.

CE-SiteB

Необходимо проделать схожие операции между маршрутизаторами ESR3 и CE_SiteB.

Произвести настройку соответствующих интерфейсов и создать eBGP-сессию между ESR3 и CE_SiteB:

CE-SiteB

```
CE-SiteB(config)# interface gigabitethernet 1/0/2
CE-SiteB(config-if-gi)# ip firewall disable
CE-SiteB(config-if-gi)# ip address 192.168.32.6/30
CE-SiteB(config-if-gi)# exit
CE-SiteB(config)#
CE-SiteB(config)# interface loopback 1
CE-SiteB(config-loopback)# ip address 10.100.1.1/24
CE-SiteB(config-loopback)# exit
CE-SiteB(config)#
CE-SiteB(config)# route-map OUTPUT
CE-SiteB(config-route-map)# rule 1
CE-SiteB(config-route-map-rule)# match ip address 10.100.1.0/24
CE-SiteB(config-route-map-rule)# action permit
CE-SiteB(config-route-map-rule)# exit
CE-SiteB(config-route-map)# exit
CE-SiteB(config)#
CE-SiteB(config)# router bgp 65505
CE-SiteB(config-bgp)# router-id 192.168.32.6
CE-SiteB(config-bgp)# neighbor 192.168.32.5
CE-SiteB(config-bgp-neighbor)# remote-as 65500
CE-SiteB(config-bgp-neighbor)# allow-local-as 1
CE-SiteB(config-bgp-neighbor)# update-source 192.168.32.6
CE-SiteB(config-bgp-neighbor)# address-family ipv4 unicast
CE-SiteB(config-bgp-neighbor-af)# route-map OUTPUT out
CE-SiteB(config-bgp-neighbor-af)# enable
CE-SiteB(config-bgp-neighbor-af)# exit
CE-SiteB(config-bgp-neighbor)# enable
CE-SiteB(config-bgp-neighbor)# exit
CE-SiteB(config-bgp)# address-family ipv4 unicast
CE-SiteB(config-bgp-af)# network 10.100.1.0/24
CE-SiteB(config-bgp-af)# exit
CE-SiteB(config-bgp)# enable
CE-SiteB(config-bgp)# exit
CE-SiteB(config)# do commit
CE-SiteB(config)# do confirm
```

Со стороны ESR3 также настроить eBGP и разрешить передачу маршрутной информации из VRF в таблицу VPNv4:

ESR3

```
router bgp 65500
ESR3(config)# router bgp 65500
ESR3(config-bgp)# vrf Customer1
ESR3(config-bgp-vrf)# router-id 192.168.32.5
ESR3(config-bgp-vrf)# neighbor 192.168.32.6
ESR3(config-bgp-vrf-neighbor)# remote-as 65505
ESR3(config-bgp-vrf-neighbor)# update-source 192.168.32.5
ESR3(config-bgp-vrf-neighbor)# address-family ipv4 unicast
ESR3(config-bgp-neighbor-af-vrf)# route-map OUTPUT out
ESR3(config-bgp-neighbor-af-vrf)# enable
ESR3(config-bgp-neighbor-af-vrf)# exit
ESR3(config-bgp-vrf-neighbor)# enable
ESR3(config-bgp-vrf-neighbor)# exit
ESR3(config-bgp-vrf)# address-family ipv4 unicast
ESR3(config-bgp-vrf-af)# redistribute connected
ESR3(config-bgp-vrf-af)# redistribute bgp 65500
ESR3(config-bgp-vrf-af)# exit
ESR3(config-bgp-vrf)# enable
ESR3(config-bgp-vrf)# exit
ESR3(config-bgp)# exit
ESR3(config)# do commit
ESR3(config)# do confirm
```

Для просмотра VPNv4-таблицы воспользоваться командой:

```
ESR1# show bgp vpnv4 unicast all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

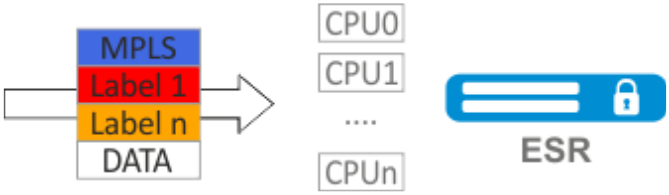

Codes Route Distinguisher   IP Prefix          Next hop        Metric     Label   LocPrf
    Weight Path
----- --------------------- ------------------ --------------- ---------- ------- ----------
------ ----------------
*>    65500:100             10.100.0.0/24      --              --         23      --         --
    ?
*>i   65500:100             192.168.32.4/30    3.3.3.3         --         84      100        0
      i
*>i   65500:100             10.100.1.0/24      3.3.3.3         --         84      100        0
      i
```

Данная команда выводит все принятые VPNv4-маршруты после применения фильтрации.

12.8 Балансировка трафика MPLS

Маршрутизаторы ESR имеют многоядерную архитектуру. Одним из первых звеньев обработки поступающего трафика является load balancer daemon (lbd), который выполняет две основных функции:

1. Равномерно распределяет нагрузку между всеми CPU маршрутизатора.
2. Выявляет аномальные ситуации с высокой нагрузкой на отдельные CPU и перераспределяет обработку с этих CPU на менее загруженные.



По умолчанию lbd использует только MPLS-метки для вычисления хеша и дальнейшего распределения нагрузки на различные CPU. Данное поведение не всегда дает преимущество, особенно когда существуют «большие» однородные потоки MPLS-трафика. Для добавления энтропии в хеш можно включить дополнительную функцию:

cpu load-balance mpls passenger ip
Включает возможность «заглядывать» дальше MPLS-заголовка для поиска IP-заголовка и добавления ip-src и ip-dst в расчет хеша:
Для L3VPN: идет поиск пары ip-src и ip-dst в ip-заголовке, находящимся за MPLS-заголовком.



Для L2VPN: ESR попытается «заглянуть» в ethernet-фрейм (который находится за mpls-заголовком) и получить ip-src и ip-dst в ip-заголовке для добавления в расчет хеша.



cpu load-balance mpls passenger ip-over-ethernet-pseudowire-with-cw
cpu load-balance mpls passenger ip-over-ethernet-pseudowire-without-cw
Позволяет явно указать, используется ли при построении L2VPN поле Control Word. Это позволяет исключить возникновение ошибки, когда при анализе IP-пакет может быть ошибочно распознан как Ethernet-фрейм.

При хешировании MPLS-меток действуют следующие ограничения:

- В расчет не добавляются метки 0-15 (Special-Purpose Labels) – см. RFC 7274;
- В расчет не добавляется метка, если непосредственно перед ней следует метка 15 (Extension Label) – см. RFC 7274;
- В расчет хеша добавляется не более трёх меток.

Во избежание падения LDP-сессии при большой нагрузке на CPU маршрутизатора на моделях ESR-200, ESR-1000, ESR-1200, ESR-1500, ESR-1700 после включения функции все пакеты протокола LDP будут обрабатываться управляющими CPU (Management CPU), которые не участвуют в обработке трафика. Для ESR-200, ESR-1000, ESR-1200, ESR-1500 – это CPU 0, ESR-1700 – CPU 0-1.

12.8.1 Пример настройки

Задача:

Включить балансировку L2VPN-трафика без использования функционала Control Word.

Решение:

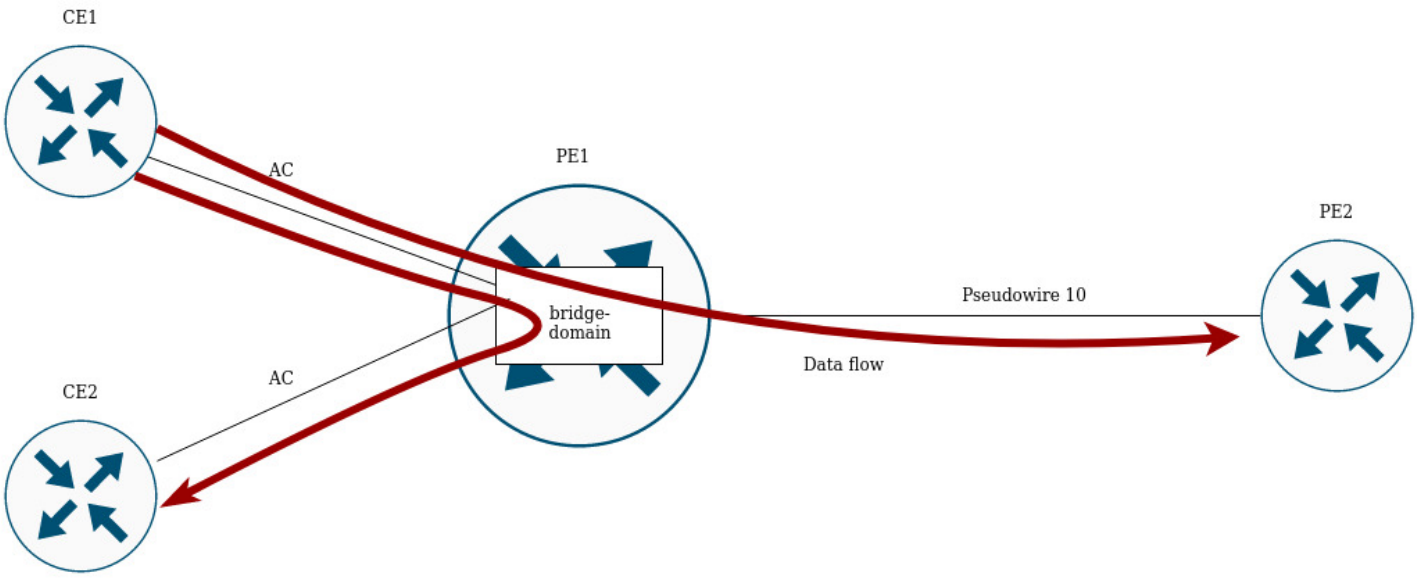
ESR

```
ESR(config)# system cpu load-balance mpls passenger ip
ESR(config)# system cpu load-balance mpls passenger ipoe-pw-without-cw
```

12.9 Работа с бридж-доменом в рамках MPLS

Для организации L2VPN-сервиса необходимо настроить на устройстве бридж-домен, создать требуемые AC, PW (LDP-signaling) и связать все данные элементы с бридж-доменом.

Для point-to-point бридж-домен создается автоматически.



Между элементами бридж-домена осуществляется коммутация трафика на основании перечисленных правил:

1. Для каждого бридж-домена автоматически создается таблица MAC-адресов по аналогии с Ethernet-коммутаторами. Ethernet-кадры коммутируются на основании анализа MAC-адреса получателя (DST MAC).
2. Кадры с известным DST MAC будут отправляться в соответствующие AC/PW.
3. Кадры с неизвестным DST MAC, broadcast- и multicast-кадры (т. н. BUM-трафик, Broadcast, Unknown unicast и Multicast) будут отправляться во все элементы бридж-домена, за исключением того элемента (AC либо PW), с которого вошли в бридж-домен.
4. При коммутации учитываются DST MAC в кадрах, но не учитываются VLAN-теги, имеющиеся на кадрах – таким образом, коммутация внутри бридж-домена не является «VLAN-aware».

Бридж-домен может работать в двух транспортных режимах: ethernet или vlan. Транспортный режим задает правила обработки трафика на входе и выходе с бридж-домена.

В LDP signaling по умолчанию используется ethernet mode (Raw mode, type 5). Для каждого отдельного экземпляра VPLS можно задать транспортный режим.

В BGP signaling бридж-домен работает только в ethernet mode.

```
PE1# config
PE1(config)# mpls
PE1(config-mpls)# l2vpn
PE1(config-l2vpn)# vpls MARTINI_br
PE1(config-l2vpn-vpls)# transport-mode vlan

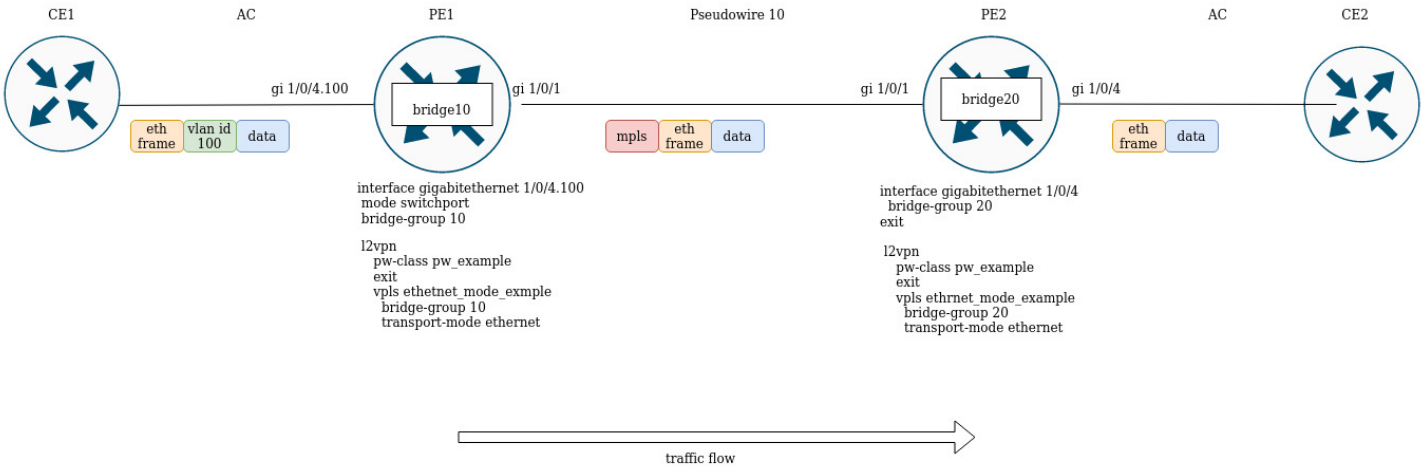
PE1# sh mpls l2vpn pseudowire
Neighbor                                PW ID      Sig Type       Status
--------------------------------------- ---------- --- ---------- ------
10.10.0.2                               200        LDP Eth Tagged Up
```

⚠ В LDP signaling транспортный режим согласуется между PE в процессе создания псевдо-провода, поэтому он должен совпадать на обоих PE.

Рассмотрим правила обработки трафика:

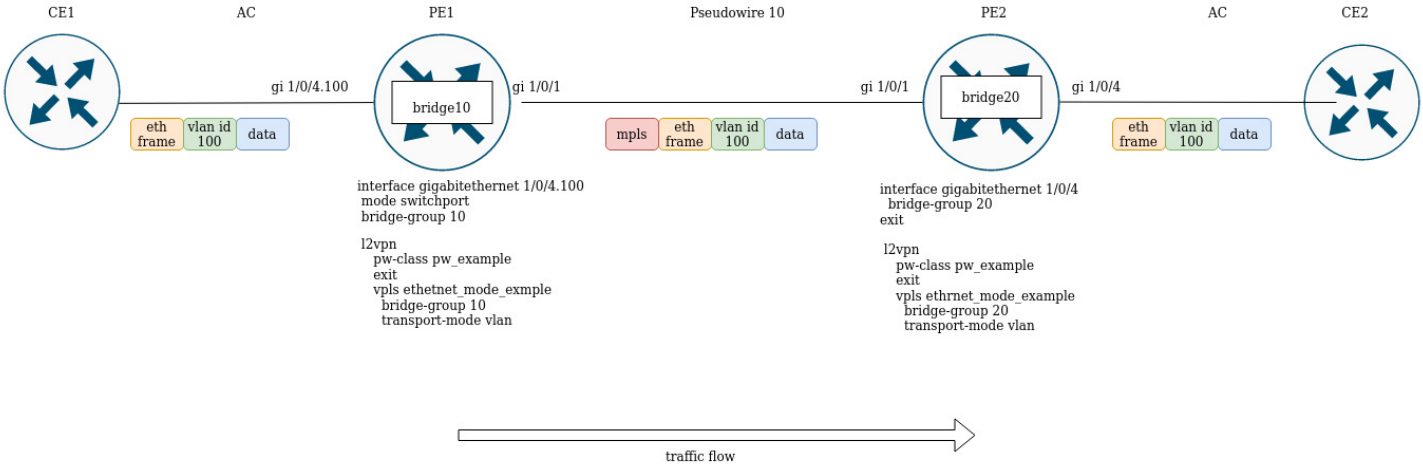
1. Ethernet (Raw) mode:

- Если AC является саб-интерфейсом, то vlan-тег перед помещение в бридж снимается. При выходе из бриджа vlan-тег восстанавливается.
- Если AC является интерфейсом, то тегированный и нетегированный трафики проходят в обоих направлениях без модификаций.



Предположим, PE1 и PE2 сконфигурированы в ethernet mode. Со стороны PE1 в бридж-домен включен саб-интерфейс gigabitethernet 1/0/4.100, поэтому vlan-тег (vlan id 100) с входящего трафика будет удален перед помещением в Pseudowire 10 (соответственно, восстановлен при трафике в сторону AC). С другой стороны, AC на PE2 является интерфейсом, значит трафик будет проходить без модификаций в обоих направлениях.

- Если AC является саб-интерфейсом, то vlan-тег перед помещением в бридж сохраняется. При выходе из бриджа vlan-тег может быть сохранен или перезаписан в зависимости от конфигурации.
- Если AC является интерфейсом, то модификация тегов не происходит в обоих направлениях.



2. Vlan (Tagged) mode:

12.10 Назначение MTU при работе с MPLS

Важно правильно настроить MTU на интерфейсах, участвующих в передаче трафика. Существует два ключевых момента:

1. Размер Ethernet-заголовка (18 байт), inner tag (4 байта), outer tag (4 байта) не учитываются на AC-интерфейсах;
2. На интерфейсах, принимающих участие в пересылке MPLS-трафика, необходимо увеличить MTU на количество меток (каждая метка равна 4 байтам).

Значение MTU также участвует в сигнализации при построении псевдо-провода как в LDP-signaling, так и в BGP-signaling. Ниже рассмотрены примеры настройки для обоих случаев:

Для сигнализации (LDP, BGP) значение MTU по умолчанию – 1500.

Значения MTU, участвующие в сигнализации, не влияют на фактический размер пакета, проходящего по псевдо-проводу.

В LDP-signaling MTU задается в рамках настройки pw – class:

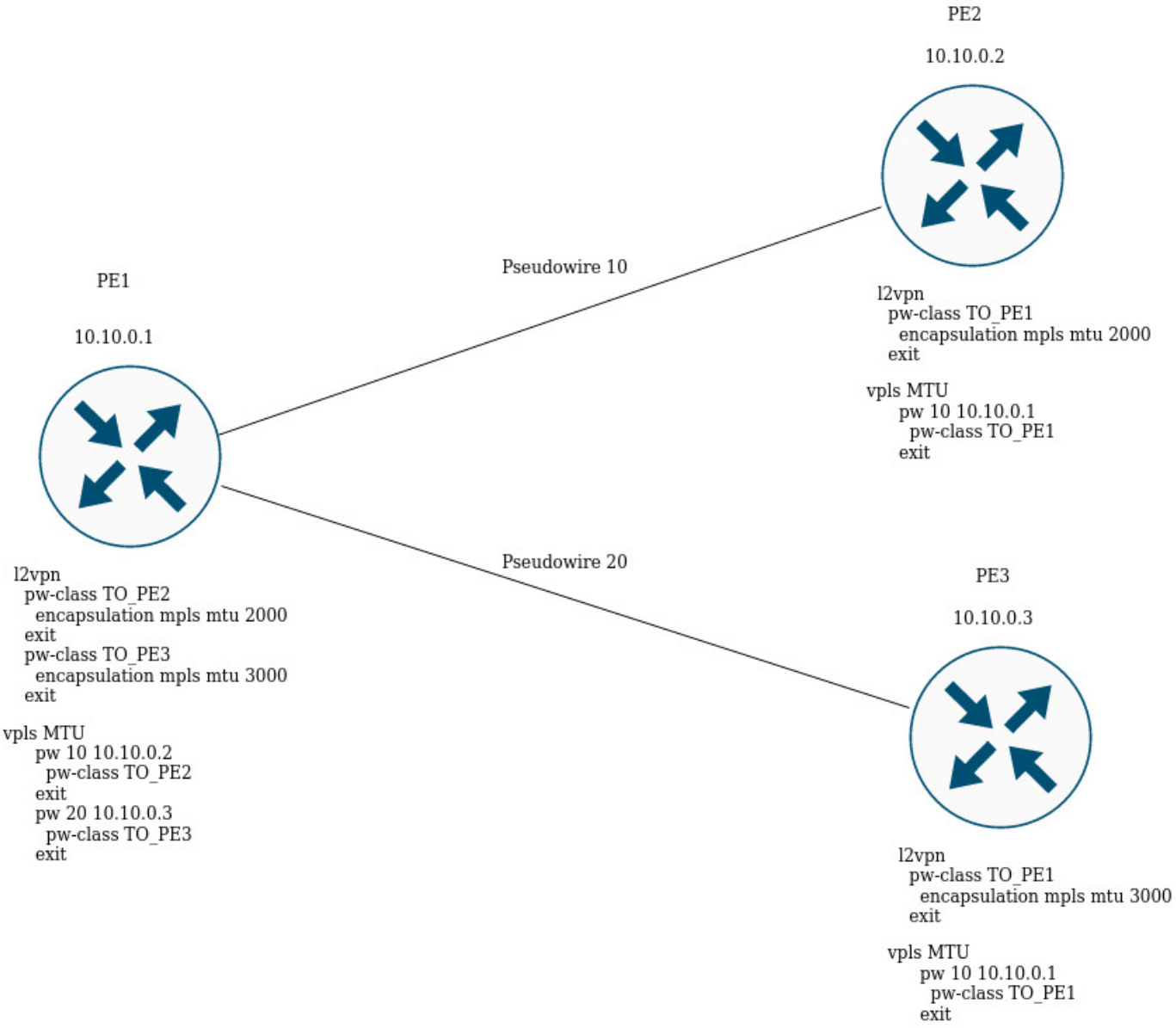
LDP-signaling. Настройка MTU для согласования

```
PE2(config)# mpls
PE2(config-mpls)# l2vpn
PE2(config-l2vpn)# pw-class MTU_example
PE2(config-l2vpn-pw-class)# encapsulation mpls mtu 9000
PE2(config-l2vpn-pw-class)# exit
PE2(config-mpls)# l2vpn
PE2(config-l2vpn)# vpls MTU_Example_PW
PE2(config-l2vpn-vpls)# pw 200 10.10.0.1
PE2(config-l2vpn-pw)# pw-class
PE2(config-l2vpn-pw)# pw-class MTU_example

*Просмотр созданных pw-class'ов*
PE2#  sh mpls l2vpn pw-class
PW-class                        Neighbor   PW ID      Status Status-tlv MTU
------------------------------- ---------- ---------- ------ ---------- ------
MTU_example                      10.10.0.1  200         Up     Enable     9000


PE2# sh mpls l2vpn vpls  MTU_Example_PW
VPLS:  MTU_Example_PW
...
    PWs:
      PW ID 2, Neighbor 10.10.0.1:
        MTU:         9000
        Last change: 01:27:42
        Status:      Up

* Для сигнализации PW 2 данного VPLS выбрано MTU 9000*
```



На рисунке выше PE1 поднимает два псевдо-провода: pseudowire 10 до PE2, и pseudowire 20 до PE3 соответственно. Для сигнализации с PE2 MTU будет равным 2000 (pw-class TO_PE2), для PE3 – MTU будет равным 3000 (pw-class TO_PE3).

Для BGP-signaling MTU указывается в рамках конфигурации l2vpn-сервиса:

BGP -signaling. Настройка MTU для согласования

```
PE1(config)# mpls
PE1(config-mpls)# l2vpn
PE1(config-l2vpn)# vpls l2vpn_MTU
PE1(config-l2vpn-vpls)# autodiscovery bgp
PE1(config-bgp)# mtu 1500

PE2# sh mpls l2vpn vpls  l2vpn_MTU
VPLS: l2vpn_MTU
...
    PWs:
      PW ID 2, Neighbor 10.10.0.1:
        MTU:          1500
        Last change: 01:27:42
        Status:       Up

* Для сигнализации всех псевдо-проводов данного VPLS будет выбрано MTU 1500 *
```

Если при согласовании значение MTU не совпадает, то статус псевдо-провода будет – 'DOWN', 'Reason: MTU mismatch':

```
PE1(config-l2vpn)# vpls l2vpn_MTU
PE1(config-l2vpn-vpls)# autodiscovery bgp
PE1(config-bgp)# mtu 2000

PE2# sh mpls l2vpn vpls l2vpn_MTU
...
    PWs:
      PW ID 2, Neighbor 10.10.0.1:
        MTU:          2000
        Last change: 00:00:10
        Status:       Down
        Reason:       MTU mismatch
```

⚠ В BGP-signaling можно отключить проверку MTU для сервиса:

```
PE1(config)# mpls
PE1(config-mpls)# l2vpn
PE1(config-l2vpn)# vpls l2vpn _MTU
PE1(config-l2vpn-vpls)# autodiscovery bgp
PE1(config-bgp)# ignore mtu-mismatch
```

Теперь при согласовании значение MTU будет игнорироваться.

По умолчанию бридж-домен имеет MTU равным 1500 байт. Стоит отметить, что бридж-домен автоматически выбирает наименьшее значение MTU, исходя из собственного MTU и MTU интерфейсов, включенных в бридж-домен.

```
* Например, имеем бридж-домен 100, в который включены интерфейсы gi1/0/1 со значением MTU 2000,
и gi1/0/2 со значением MTU 3000 *
CE3(config)# bridge 100
CE3(config-bridge)# enable
CE3(config-bridge)# exit
CE3(config)# interface gigabitethernet 1/0/1
CE3(config-if-gi)# mtu 2000
CE3(config-if-gi)# bridge-group 100
CE3(config-if-gi)# exit
CE3(config)# interface gigabitethernet 1/0/2
CE3(config-if-gi)# mtu 3000
CE3(config-if-gi)# bridge-group 100
CE3(config-if-gi)# do com

* MTU бридж-домена будет равным 1500, так как по умолчанию сам бридж имеет MTU 1500 (значение
по умолчанию), которое и стало наименьшим:
 MTU bridge 100 = 1500  <-- Наименьшее значение MTU
 MTU gi1/0/1  = 2000
 MTU gi1/0/2 = 3000
*


CE3# sh interfaces bridge
Bridges      Interfaces
----------   ------------------------------------------------------------
bridge 100   gi1/0/1-2

CE3# sh interfaces status bridge 100
Interface 'bridge 100' status information:
 Description:          --
 Operational state:    UP
 Administrative state: Up
 Supports broadcast:   Yes
 Supports multicast:   Yes
 MTU:                  1500
 MAC address:          a8:f9:4b:aa:11:00
 Last change:          1 minute and 46 seconds
 Mode:                 Routerport

* Изменим MTU на самом бридж-домене:  *

CE3(config)# bridge 100
CE3(config-bridge)# mtu 6000
CE3(config-bridge)# do com

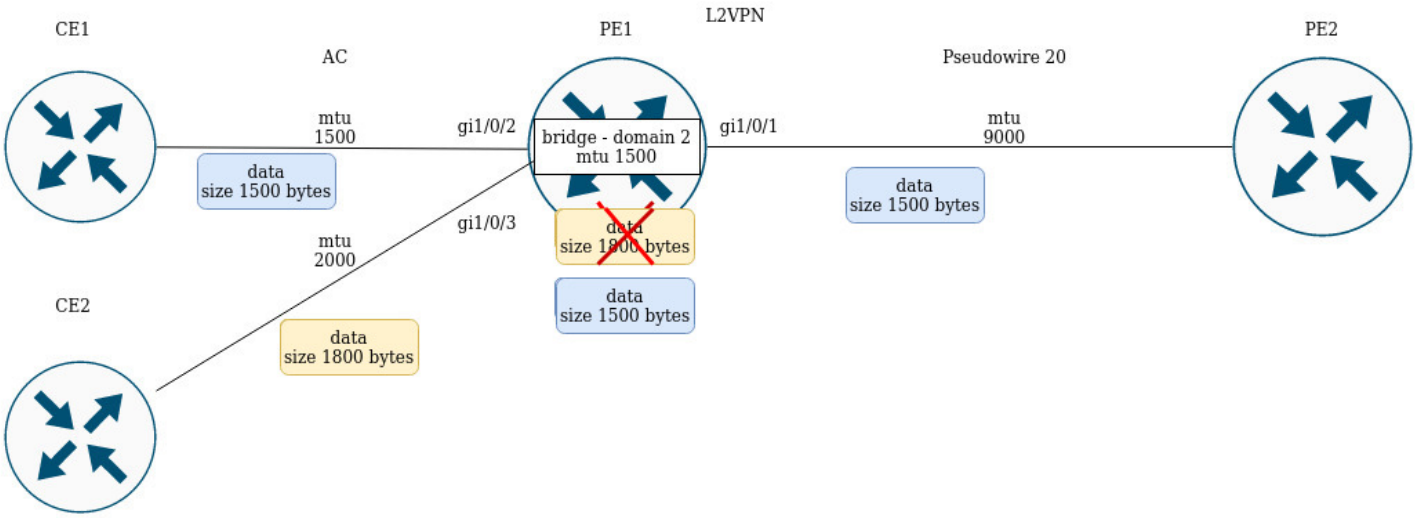
* MTU бридж-домена стало равным 2000 байт, так как gi1/0/2 имеет наименьшее MTU:
 MTU bridge 100 = 6000
 MTU gi1/0/1 = 2000 <-- Наименьшее значение MTU
 MTU gi1/0/2 = 3000
*

CE3# sh interfaces bridge
Bridges      Interfaces
----------   ------------------------------------------------------------
bridge 100   gi1/0/1-2

CE3# sh interfaces status bridge 100
Interface 'bridge 100' status information:
 Description:          --
```

```
Operational state:    Up
Administrative state: Up
Supports broadcast:   Yes
Supports multicast:   Yes
MTU:                  2000
MAC address:          a8:f9:4b:aa:11:00
Last change:          6 minutes and 42 seconds
Mode:                 Routerport
```

Рассмотрим пример прохождения трафика в L2VPN-сервисе:



PE1 имеет следующие значения MTU на интерфейсах:

```
PE1# sh interfaces status
Interface            Admin    Link     MTU      MAC address          Last change
Mode
                     state    state
-------------------  -----    -----    ------   -------------------  --------------------------
----------
gi1/0/1              Up       Up       9000     a8:f9:4b:ac:4d:16    5 hours, 25 minutes and
2   Routerport                                                       seconds

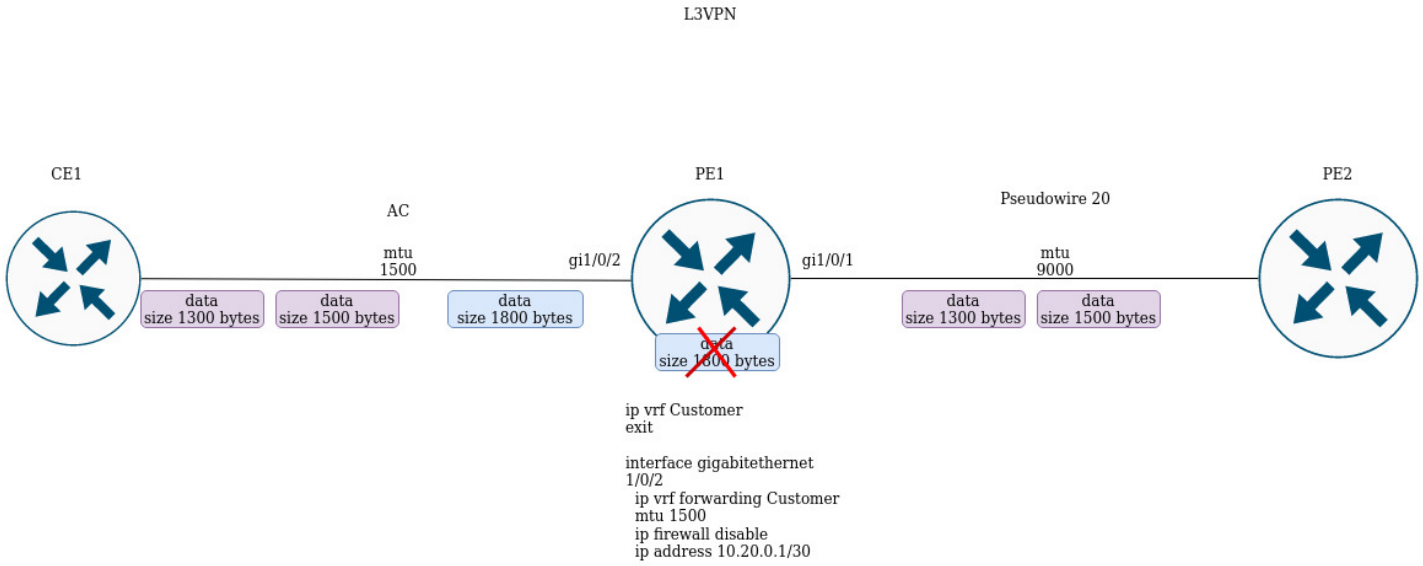
gi1/0/2              Up       Up       1500     a8:f9:4b:ac:4d:17    4 days, 4 hours,
49         Switchport                                                minutes and 40 seconds

gi1/0/3              Up       Up       1800     a8:f9:4b:ac:4d:18    4 days, 1 hour,
49          Switchport                                               minutes and 38 seconds

bridge 2             Up       Up       1500     a8:f9:4b:ac:4d:15    1 day, 1 hour, 27 minutes
Routerport                                                           and 28 seconds
```

CE1 посылает пакеты размером 1500 байт, CE2 – 1800 байт соответственно. Так как MTU бридж-домена меньше, чем MTU пакета от CE2, то пакет от CE2 будет отброшен перед попаданием в бридж-домен. Аналогичные действия будут, если MTU интерфейса, смотрящего в сторону mpls-core (gi1/0/1), меньше чем MTU, приходящих от CE-пакетов (с учетом MPLS-заголовка).

Схожее поведение и при прохождении трафика в L3VPN-сервисе:

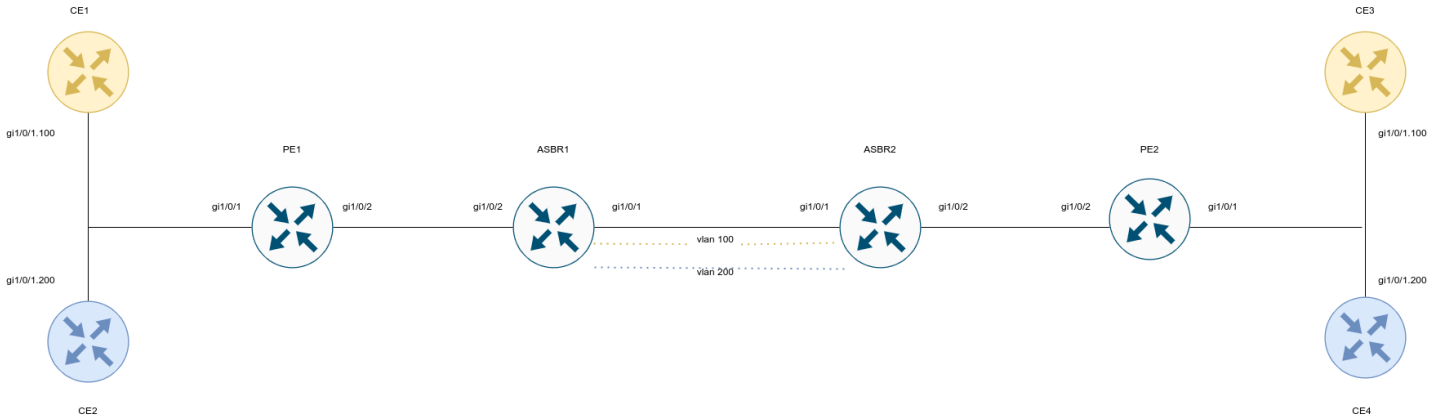


Если CE1 пошлет пакет с большим MTU, чем на интерфейсе, смотрящим в сторону клиента (gi1/0/2) или в сторону mpls-core (gi1/0/1), то пакет будет отброшен.

12.11 Inter-AS Option A

Рассмотрим примеры настройки на базе построения сервисов l3vpn и l2vpn. Главная особенность inter-AS Option A – отсутствие mpls-меток в трафике при передаче между ASBR. Для разделения трафика клиентских сервисов между ASBR обычно используют VRF для l3vpn или тегирование (dot1q, q-in-q) для сервисов l2vpn.

12.11.1 L2VPN



Настроим CE:

CE1

```
ESR# config
ESR(config)# hostname CE1
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-if-gi)# ip firewall disable
ESR(config-if-gi)# ip address 192.168.1.1/24
ESR(config-if-gi)# do com
ESR(config-if-gi)# do conf
```

CE2

```
ESR# config
ESR(config)# hostname CE2
ESR(config)# interface gigabitethernet 1/0/1.200
ESR(config-if-gi)# ip firewall disable
ESR(config-if-gi)# ip address 192.168.2.1/24
ESR(config-if-gi)# do com
ESR(config-if-gi)# do conf
```

CE3

```
ESR# config
ESR(config)# hostname CE3
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-if-gi)# ip firewall disable
ESR(config-if-gi)# ip address 192.168.1.2/24
ESR(config-if-gi)# do com
ESR(config-if-gi)# do conf
```

CE4

```
ESR# config
ESR(config)# hostname CE4
ESR(config)# interface gigabitethernet 1/0/1.200
ESR(config-if-gi)# ip firewall disable
ESR(config-if-gi)# ip address 192.168.2.2/24
ESR(config-if-gi)# do com
ESR(config-if-gi)# do conf
```

Произведем настройку PE1 и PE2. Анонсирование сервисных меток возложим на протокол BGP (Kompella mode):

PE1

```
ESR(config)# hostname PE1
ESR(config)# system jumbo-frames
ESR(config)# router bgp log-neighbor-changes
ESR(config)# router bgp 65500
ESR(config-bgp)#   neighbor 10.10.1.2
ESR(config-bgp-neighbor)#     remote-as 65500
ESR(config-bgp-neighbor)#     update-source 10.10.1.1
ESR(config-bgp-neighbor)#     address-family l2vpn vpls
ESR(config-bgp-neighbor-af)#       send-community extended
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     enable
ESR(config-bgp-neighbor)#   exit
ESR(config-bgp)#   enable
ESR(config-bgp)# exit
ESR(config)#
ESR(config)# router ospf 1
ESR(config-ospf)#   area 0.0.0.0
ESR(config-ospf-area)#     enable
ESR(config-ospf-area)#   exit
ESR(config-ospf)#   enable
ESR(config-ospf)# exit
ESR(config)#
ESR(config)# bridge 100
ESR(config-bridge)#   enable
ESR(config-bridge)# exit
ESR(config)# bridge 200
ESR(config-bridge)#   enable
ESR(config-bridge)# exit
ESR(config)#
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-if-sub)#   description "to CE1"
ESR(config-if-sub)#   bridge-group 100
ESR(config-if-sub)# exit
ESR(config)# interface gigabitethernet 1/0/1.200
ESR(config-if-sub)#   description "to CE2"
ESR(config-if-sub)#   bridge-group 200
ESR(config-if-sub)# exit
ESR(config)# interface gigabitethernet 1/0/2
ESR(config-if-gi)#   mtu 1522
ESR(config-if-gi)#   ip firewall disable
ESR(config-if-gi)#   ip address 10.100.0.1/30
ESR(config-if-gi)#   ip ospf instance 1
ESR(config-if-gi)#   ip ospf
ESR(config-if-gi)# exit
ESR(config)# interface loopback 1
ESR(config-loopback)#   ip address 10.10.1.1/32
ESR(config-loopback)#   ip ospf instance 1
ESR(config-loopback)#   ip ospf
ESR(config-loopback)# exit
ESR(config)# mpls
ESR(config-mpls)#   ldp
ESR(config-ldp)#     router-id 10.10.1.1
ESR(config-ldp)#     address-family ipv4
ESR(config-ldp-af-ipv4)#       interface gigabitethernet 1/0/2
ESR(config-ldp-af-ipv4-if)#       exit
ESR(config-ldp-af-ipv4)#     exit
```

```
ESR(config-ldp)#     enable
ESR(config-ldp)#   exit
ESR(config-mpls)#   l2vpn
ESR(config-l2vpn)#     vpls CE1
ESR(config-l2vpn-vpls)#       bridge-group 100
ESR(config-l2vpn-vpls)#       autodiscovery bgp
ESR(config-bgp)#         vpn id 1
ESR(config-bgp)#         ve id 2
ESR(config-bgp)#         rd 65500:1
ESR(config-bgp)#         route-target export 65500:1
ESR(config-bgp)#         route-target import 65500:1
ESR(config-bgp)#       exit
ESR(config-l2vpn-vpls)#       enable
ESR(config-l2vpn-vpls)#     exit
ESR(config-l2vpn)#     vpls CE2
ESR(config-l2vpn-vpls)#       bridge-group 200
ESR(config-l2vpn-vpls)#       autodiscovery bgp
ESR(config-bgp)#         vpn id 2
ESR(config-bgp)#         ve id 2
ESR(config-bgp)#         rd 65500:2
ESR(config-bgp)#         route-target export 65500:2
ESR(config-bgp)#         route-target import 65500:2
ESR(config-bgp)#       exit
ESR(config-l2vpn-vpls)#       enable
ESR(config-l2vpn-vpls)#     exit
ESR(config-l2vpn)#   exit
ESR(config-mpls)#   forwarding interface gigabitethernet 1/0/2
ESR(config-mpls)# exit
ESR(config)# do com
ESR(config)# do conf
```

PE2

```
ESR(config)# hostname ESR
ESR(config)# system jumbo-frames
ESR(config)#
ESR(config)# router bgp log-neighbor-changes
ESR(config)# router bgp 65500
ESR(config-bgp)#   router-id 10.11.1.1
ESR(config-bgp)#   neighbor 10.11.1.2
ESR(config-bgp-neighbor)#     remote-as 65500
ESR(config-bgp-neighbor)#     update-source 10.11.1.1
ESR(config-bgp-neighbor)#     address-family l2vpn vpls
ESR(config-bgp-neighbor-af)#       send-community extended
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     enable
ESR(config-bgp-neighbor)#   exit
ESR(config-bgp)#   enable
ESR(config-bgp)# exit
ESR(config)#
ESR(config)# router ospf 1
ESR(config-ospf)#   area 0.0.0.0
ESR(config-ospf-area)#     enable
ESR(config-ospf-area)#   exit
ESR(config-ospf)#   enable
ESR(config-ospf)# exit
ESR(config)#
ESR(config)# bridge 100
ESR(config-bridge)#   enable
ESR(config-bridge)# exit
ESR(config)# bridge 200
ESR(config-bridge)#   enable
ESR(config-bridge)# exit
ESR(config)#
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-if-sub)#   description "to CE3"
ESR(config-if-sub)#   bridge-group 100
ESR(config-if-sub)# exit
ESR(config)# interface gigabitethernet 1/0/1.200
ESR(config-if-sub)#   description "to CE4"
ESR(config-if-sub)#   bridge-group 200
ESR(config-if-sub)# exit
ESR(config)# interface gigabitethernet 1/0/2
ESR(config-if-gi)#   mtu 1522
ESR(config-if-gi)#   ip firewall disable
ESR(config-if-gi)#   ip address 10.101.0.1/30
ESR(config-if-gi)#   ip ospf instance 1
ESR(config-if-gi)#   ip ospf
ESR(config-if-gi)# exit
ESR(config)# interface loopback 1
ESR(config-loopback)#   ip address 10.11.1.1/32
ESR(config-loopback)#   ip ospf instance 1
ESR(config-loopback)#   ip ospf
ESR(config-loopback)# exit
ESR(config)# mpls
ESR(config-mpls)#   ldp
ESR(config-ldp)#     router-id 10.11.1.1
ESR(config-ldp)#     address-family ipv4
ESR(config-ldp-af-ipv4)#       interface gigabitethernet 1/0/2
```

```
ESR(config-ldp-af-ipv4-if)#       exit
ESR(config-ldp-af-ipv4)#     exit
ESR(config-ldp)#     enable
ESR(config-ldp)#   exit
ESR(config-mpls)#   l2vpn
ESR(config-l2vpn)#     vpls CE1
ESR(config-l2vpn-vpls)#       bridge-group 100
ESR(config-l2vpn-vpls)#       autodiscovery bgp
ESR(config-bgp)#         vpn id 1
ESR(config-bgp)#         ve id 2
ESR(config-bgp)#         rd 65500:1
ESR(config-bgp)#         route-target export 65500:1
ESR(config-bgp)#         route-target import 65500:1
ESR(config-bgp)#       exit
ESR(config-l2vpn-vpls)#       enable
ESR(config-l2vpn-vpls)#     exit
ESR(config-l2vpn)#     vpls CE2
ESR(config-l2vpn-vpls)#       bridge-group 200
ESR(config-l2vpn-vpls)#       autodiscovery bgp
ESR(config-bgp)#         vpn id 2
ESR(config-bgp)#         ve id 2
ESR(config-bgp)#         rd 65500:2
ESR(config-bgp)#         route-target export 65500:2
ESR(config-bgp)#         route-target import 65500:2
ESR(config-bgp)#       exit
ESR(config-l2vpn-vpls)#       enable
ESR(config-l2vpn-vpls)#     exit
ESR(config-l2vpn)#   exit
ESR(config-mpls)#   forwarding interface gigabitethernet 1/0/2
ESR(config-mpls)# exit
ESR(config)# do com
ESR(config)# do conf
```

Настроим ASBR1 и ASBR2. Для разделения трафика от CE1 и CE2 в сторону ASBR2 сделаем интерфейс gi1/0/1 транковым. Vlan 100 и 200 будут предназначены для трафика от CE1 и CE2 соответственно:

ASBR1

```
ESR(config)#  hostname ASBR1
ESR(config)#
ESR(config)# system jumbo-frames
ESR(config)#
ESR(config)# vlan 100,200
ESR(config-vlan)# exit
ESR(config)#
ESR(config)# router bgp 65500
ESR(config-bgp)#   router-id 10.10.1.2
ESR(config-bgp)#   neighbor 10.10.1.1
ESR(config-bgp-neighbor)#     remote-as 65500
ESR(config-bgp-neighbor)#     update-source 10.10.1.2
ESR(config-bgp-neighbor)#     address-family l2vpn vpls
ESR(config-bgp-neighbor-af)#       send-community extended
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     enable
ESR(config-bgp-neighbor)#   exit
ESR(config-bgp)#   enable
ESR(config-bgp)# exit
ESR(config)#
ESR(config)# router ospf 1
ESR(config-ospf)#   area 0.0.0.0
ESR(config-ospf-area)#     enable
ESR(config-ospf-area)#   exit
ESR(config-ospf)#   enable
ESR(config-ospf)# exit
ESR(config)#
ESR(config)# bridge 10
ESR(config-bridge)#   vlan 100
ESR(config-bridge)#   enable
ESR(config-bridge)# exit
ESR(config)# bridge 20
ESR(config-bridge)#   vlan 200
ESR(config-bridge)#   enable
ESR(config-bridge)# exit
ESR(config)#
ESR(config)# interface gigabitethernet 1/0/1
ESR(config-if-gi)#   description "to ASBR2"
ESR(config-if-gi)#   mode switchport
ESR(config-if-gi)#   spanning-tree disable
ESR(config-if-gi)#   switchport forbidden default-vlan
ESR(config-if-gi)#   switchport mode trunk
ESR(config-if-gi)#   switchport trunk allowed vlan add 100,200
ESR(config-if-gi)# exit
ESR(config)# interface gigabitethernet 1/0/2
ESR(config-if-gi)#   description "to PE1"
ESR(config-if-gi)#   mtu 1522
ESR(config-if-gi)#   ip firewall disable
ESR(config-if-gi)#   ip address 10.100.0.2/30
ESR(config-if-gi)#   ip ospf instance 1
ESR(config-if-gi)#   ip ospf
ESR(config-if-gi)# exit
ESR(config)# interface loopback 1
ESR(config-loopback)#   ip address 10.10.1.2/32
ESR(config-loopback)#   ip ospf instance 1
ESR(config-loopback)#   ip ospf
```

```
ESR(config-loopback)# exit
ESR(config)# mpls
ESR(config-mpls)#   ldp
ESR(config-ldp)#     router-id 10.10.1.2
ESR(config-ldp)#     address-family ipv4
ESR(config-ldp-af-ipv4)#       interface gigabitethernet 1/0/2
ESR(config-ldp-af-ipv4-if)#       exit
ESR(config-ldp-af-ipv4)#     exit
ESR(config-ldp)#     enable
ESR(config-ldp)#   exit
ESR(config-mpls)#   l2vpn
ESR(config-l2vpn)#     vpls CE1
ESR(config-l2vpn-vpls)#       bridge-group 10
ESR(config-l2vpn-vpls)#       autodiscovery bgp
ESR(config-bgp)#         vpn id 1
ESR(config-bgp)#         ve id 1
ESR(config-bgp)#         rd 65500:1
ESR(config-bgp)#         route-target export 65500:1
ESR(config-bgp)#         route-target import 65500:1
ESR(config-bgp)#       exit
ESR(config-l2vpn-vpls)#       enable
ESR(config-l2vpn-vpls)#     exit
ESR(config-l2vpn)#     vpls CE2
ESR(config-l2vpn-vpls)#       bridge-group 20
ESR(config-l2vpn-vpls)#       autodiscovery bgp
ESR(config-bgp)#         vpn id 2
ESR(config-bgp)#         ve id 1
ESR(config-bgp)#         rd 65500:2
ESR(config-bgp)#         route-target export 65500:2
ESR(config-bgp)#         route-target import 65500:2
ESR(config-bgp)#       exit
ESR(config-l2vpn-vpls)#       enable
ESR(config-l2vpn-vpls)#     exit
ESR(config-l2vpn)#   exit
ESR(config-mpls)#   forwarding interface gigabitethernet 1/0/2
ESR(config-mpls)# exit
ESR(config)# do com
ESR(config)# do conf
```

ASBR2

```
ESR(config)#  hostname ASBR2
ESR(config)#
ESR(config)# system jumbo-frames
ESR(config)#
ESR(config)# vlan 100,200
ESR(config-vlan)# exit
ESR(config)#
ESR(config)# router bgp 65500
ESR(config-bgp)#   router-id 10.10.1.2
ESR(config-bgp)#   neighbor 10.10.1.1
ESR(config-bgp-neighbor)#     remote-as 65500
ESR(config-bgp-neighbor)#     update-source 10.10.1.2
ESR(config-bgp-neighbor)#     address-family l2vpn vpls
ESR(config-bgp-neighbor-af)#       send-community extended
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     enable
ESR(config-bgp-neighbor)#   exit
ESR(config-bgp)#   enable
ESR(config-bgp)# exit
ESR(config)#
ESR(config)# router ospf 1
ESR(config-ospf)#   area 0.0.0.0
ESR(config-ospf-area)#     enable
ESR(config-ospf-area)#   exit
ESR(config-ospf)#   enable
ESR(config-ospf)# exit
ESR(config)#
ESR(config)# bridge 10
ESR(config-bridge)#   vlan 100
ESR(config-bridge)#   enable
ESR(config-bridge)# exit
ESR(config)# bridge 20
ESR(config-bridge)#   vlan 200
ESR(config-bridge)#   enable
ESR(config-bridge)# exit
ESR(config)#
ESR(config)# interface gigabitethernet 1/0/1
ESR(config-if-gi)#   description "to ASBR1"
ESR(config-if-gi)#   mode switchport
ESR(config-if-gi)#   spanning-tree disable
ESR(config-if-gi)#   switchport forbidden default-vlan
ESR(config-if-gi)#   switchport mode trunk
ESR(config-if-gi)#   switchport trunk allowed vlan add 100,200
ESR(config-if-gi)# exit
ESR(config)# interface gigabitethernet 1/0/2
ESR(config-if-gi)#   description "to PE1"
ESR(config-if-gi)#   mtu 1522
ESR(config-if-gi)#   ip firewall disable
ESR(config-if-gi)#   ip address 10.100.0.2/30
ESR(config-if-gi)#   ip ospf instance 1
ESR(config-if-gi)#   ip ospf
ESR(config-if-gi)# exit
ESR(config)# interface loopback 1
ESR(config-loopback)#   ip address 10.10.1.2/32
ESR(config-loopback)#   ip ospf instance 1
ESR(config-loopback)#   ip ospf
```

```
ESR(config-loopback)# exit
ESR(config)# mpls
ESR(config-mpls)#   ldp
ESR(config-ldp)#     router-id 10.10.1.2
ESR(config-ldp)#     address-family ipv4
ESR(config-ldp-af-ipv4)#       interface gigabitethernet 1/0/2
ESR(config-ldp-af-ipv4-if)#       exit
ESR(config-ldp-af-ipv4)#     exit
ESR(config-ldp)#     enable
ESR(config-ldp)#   exit
ESR(config-mpls)#   l2vpn
ESR(config-l2vpn)#     vpls CE1
ESR(config-l2vpn-vpls)#       bridge-group 10
ESR(config-l2vpn-vpls)#       autodiscovery bgp
ESR(config-bgp)#         vpn id 1
ESR(config-bgp)#         ve id 1
ESR(config-bgp)#         rd 65500:1
ESR(config-bgp)#         route-target export 65500:1
ESR(config-bgp)#         route-target import 65500:1
ESR(config-bgp)#       exit
ESR(config-l2vpn-vpls)#       enable
ESR(config-l2vpn-vpls)#     exit
ESR(config-l2vpn)#     vpls CE2
ESR(config-l2vpn-vpls)#       bridge-group 20
ESR(config-l2vpn-vpls)#       autodiscovery bgp
ESR(config-bgp)#         vpn id 2
ESR(config-bgp)#         ve id 1
ESR(config-bgp)#         rd 65500:2
ESR(config-bgp)#         route-target export 65500:2
ESR(config-bgp)#         route-target import 65500:2
ESR(config-bgp)#       exit
ESR(config-l2vpn-vpls)#       enable
ESR(config-l2vpn-vpls)#     exit
ESR(config-l2vpn)#   exit
ESR(config-mpls)#   forwarding interface gigabitethernet 1/0/2
ESR(config-mpls)# exit
ESR(config)# do com
ESR(config)# do conf
```

Проверим назначение меток, статус сервисов, а также сетевую доступность между CE:

Информация о метках

```
ASBR2# sh bgp l2vpn vpls all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes Route Distinguisher   VID   VBO   VBS   Next hop        Metric     LocPrf     Weight Path
----- --------------------- ----- ----- ----- --------------- ---------- ---------- ------
-------------------
*>i   65500:1               2     1     10    10.11.1.1       --         100        0      i
*>i   65500:2               2     1     10    10.11.1.1       --         100        0      i
*>    65500:1               1     1     10    --              --         --         --
*>    65500:2               1     1     10    --              --         --         --

ASBR2# sh mpls forwarding-table
Local    Outgoing Prefix                                    Outgoing         Next Hop
label    label    or tunnel ID                              Interface
-------- -------- ----------------------------------------- ----------------
--------------------------------------
56       imp-null 10.11.1.1/32                              gi1/0/2          10.101.0.1
47       37       PW ID 1                                   --               10.11.1.1
37       47       PW ID 2                                   --               10.11.1.1
```

Статус сервисов

```
ASBR2# sh mpls l2vpn vpls
VPLS: CE1
    bridge 10:
        MTU:    1500
        Status: Up
    PWs:
      PW ID 1, Neighbor 10.11.1.1:
        MTU:         1500
        Last change: 00:16:59
        Status:      Up
VPLS: CE2
    bridge 20:
        MTU:    1500
        Status: Up
    PWs:
      PW ID 2, Neighbor 10.11.1.1:
        MTU:         1500
        Last change: 00:16:59
        Status:      Up
```

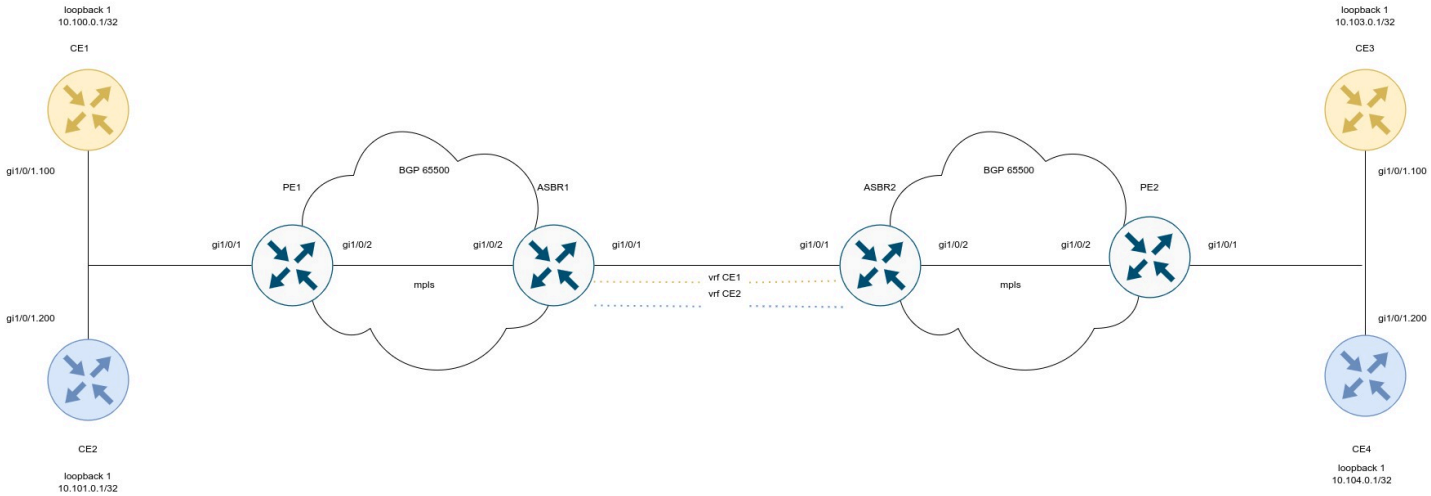
Проверка сетевой доступности

```
CE1# ping 192.168.1.2 detailed
PING 192.168.1.2 (192.168.1.2) 56 bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=0 time=1.08 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=0 time=1.06 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=0 time=1.01 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=0 time=0.971 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=0 time=0.972 ms

CE2# ping 192.168.2.2 detailed  packets
PING 192.168.2.2 (192.168.2.2) 56 bytes of data.
64 bytes from 192.168.2.2: icmp_seq=1 ttl=0 time=1.17 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=0 time=0.972 ms
64 bytes from 192.168.2.2: icmp_seq=3 ttl=0 time=0.960 ms
64 bytes from 192.168.2.2: icmp_seq=4 ttl=0 time=1.04 ms
64 bytes from 192.168.2.2: icmp_seq=5 ttl=0 time=0.976 ms

ASBR2# sh mac address-table bridge 10
VID     MAC Address          Interface                       Type
-----   ------------------   -----------------------------   -------
--      e4:5a:d4:01:b9:73    vlan 100                        Dynamic
--      e4:5a:d4:a1:34:61    dypseudowire 1_10.11.1.1        Dynamic
2 valid mac entries
ASBR2# sh mac address-table bridge 20
VID     MAC Address          Interface                       Type
-----   ------------------   -----------------------------   -------
--      e4:5a:d4:01:c1:80    vlan 200                        Dynamic
--      e4:5a:d4:a1:34:61    dypseudowire 2_10.11.1.1        Dynamic
2 valid mac entries
```

12.11.2 L3VPN



Настроим CE:

CE1

```
ESR(config)# hostname CE1
ESR(config)#
ESR(config)# route-map BGP
ESR(config-route-map)#   rule 1
ESR(config-route-map-rule)#   exit
ESR(config-route-map)# exit
ESR(config)# router bgp 65501
ESR(config-bgp)#   neighbor 192.168.1.2
ESR(config-bgp-neighbor)#     remote-as 65500
ESR(config-bgp-neighbor)#     address-family ipv4 unicast
ESR(config-bgp-neighbor-af)#       route-map BGP out
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     enable
ESR(config-bgp-neighbor)#   exit
ESR(config-bgp)#   address-family ipv4 unicast
ESR(config-bgp-af)#     network 10.110.0.1/32
ESR(config-bgp-af)#   exit
ESR(config-bgp)#   enable
ESR(config-bgp)# exit
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-if-sub)#   ip firewall disable
ESR(config-if-sub)#   ip address 192.168.1.1/30
ESR(config-if-sub)# exit
ESR(config)# interface loopback 1
ESR(config-loopback)#   ip address 10.110.0.1/32
ESR(config-loopback)# exit
ESR(config)# do com
ESR(config)# do conf
```

CE2

```
ESR(config)# hostname CE2
ESR(config)#
ESR(config)# route-map BGP
ESR(config-route-map)#   rule 1
ESR(config-route-map-rule)#   exit
ESR(config-route-map)# exit
ESR(config)# router bgp 65501
ESR(config-bgp)#   neighbor 192.168.2.2
ESR(config-bgp-neighbor)#     remote-as 65500
ESR(config-bgp-neighbor)#     address-family ipv4 unicast
ESR(config-bgp-neighbor-af)#       route-map BGP out
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     enable
ESR(config-bgp-neighbor)#   exit
ESR(config-bgp)#   address-family ipv4 unicast
ESR(config-bgp-af)#     network 10.112.0.1/32
ESR(config-bgp-af)#   exit
ESR(config-bgp)#   enable
ESR(config-bgp)# exit
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-if-sub)#   ip firewall disable
ESR(config-if-sub)#   ip address 192.168.2.1/30
ESR(config-if-sub)# exit
ESR(config)#
ESR(config)# interface loopback 1
ESR(config-loopback)#   ip address 10.112.0.1/32
ESR(config-loopback)# exit
ESR(config)# do com
ESR(config)# do conf
```

CE3

```
ESR(config)# hostname CE3
ESR(config)#
ESR(config)# route-map BGP
ESR(config-route-map)#   rule 1
ESR(config-route-map-rule)#   exit
ESR(config-route-map)# exit
ESR(config)# router bgp 65501
ESR(config-bgp)#   neighbor 192.168.3.2
ESR(config-bgp-neighbor)#     remote-as 65500
ESR(config-bgp-neighbor)#     address-family ipv4 unicast
ESR(config-bgp-neighbor-af)#       route-map BGP out
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     enable
ESR(config-bgp-neighbor)#   exit
ESR(config-bgp)#   address-family ipv4 unicast
ESR(config-bgp-af)#     network 10.113.0.1/32
ESR(config-bgp-af)#   exit
ESR(config-bgp)#   enable
ESR(config-bgp)# exit
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-if-sub)#   ip firewall disable
ESR(config-if-sub)#   ip address 192.168.3.1/30
ESR(config-if-sub)# exit
ESR(config)#
ESR(config)# interface loopback 1
ESR(config-loopback)#   ip address 10.113.0.1/32
ESR(config-loopback)# exit
ESR(config)# do com
ESR(config)# do conf
```

CE4

```
ESR(config)# hostname CE4
ESR(config)#
ESR(config)# route-map BGP
ESR(config-route-map)#   rule 1
ESR(config-route-map-rule)#   exit
ESR(config-route-map)# exit
ESR(config)# router bgp 65501
ESR(config-bgp)#   neighbor 192.168.4.2
ESR(config-bgp-neighbor)#     remote-as 65500
ESR(config-bgp-neighbor)#     address-family ipv4 unicast
ESR(config-bgp-neighbor-af)#       route-map BGP out
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     enable
ESR(config-bgp-neighbor)#   exit
ESR(config-bgp)#   address-family ipv4 unicast
ESR(config-bgp-af)#     network 10.114.0.1/32
ESR(config-bgp-af)#   exit
ESR(config-bgp)#   enable
ESR(config-bgp)# exit
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-if-sub)#   ip firewall disable
ESR(config-if-sub)#   ip address 192.168.4.1/30
ESR(config-if-sub)# exit
ESR(config)#
ESR(config)# interface loopback 1
ESR(config-loopback)#   ip address 10.114.0.1/32
ESR(config-loopback)# exit
ESR(config)# do com
ESR(config)# do conf
```

Произведем настройку PE1 и PE2:

PE1

```
ESR(config)# hostname PE1
ESR(config)#
ESR(config)# ip vrf CE1
ESR(config-vrf)#   ip protocols bgp max-routes 100
ESR(config-vrf)#   rd 65500:1
ESR(config-vrf)#   route-target export 65500:1
ESR(config-vrf)#   route-target import 65500:1
ESR(config-vrf)# exit
ESR(config)# ip vrf CE2
ESR(config-vrf)#   ip protocols bgp max-routes 100
ESR(config-vrf)#   rd 65500:2
ESR(config-vrf)#   route-target export 65500:2
ESR(config-vrf)#   route-target import 65500:2
ESR(config-vrf)# exit
ESR(config)#
ESR(config)# system jumbo-frames
ESR(config)#
ESR(config)# route-map BGP
ESR(config-route-map)#   rule 1
ESR(config-route-map-rule)#   exit
ESR(config-route-map)# exit
ESR(config)# router bgp log-neighbor-changes
ESR(config)# router bgp 65500
ESR(config-bgp)#   neighbor 10.10.1.2
ESR(config-bgp-neighbor)#     remote-as 65500
ESR(config-bgp-neighbor)#     update-source 10.10.1.1
ESR(config-bgp-neighbor)#     address-family vpnv4 unicast
ESR(config-bgp-neighbor-af)#       send-community extended
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     enable
ESR(config-bgp-neighbor)#   exit
ESR(config-bgp)#   enable
ESR(config-bgp)#   vrf CE1
ESR(config-bgp-vrf)#     neighbor 192.168.1.1
ESR(config-bgp-vrf-neighbor)#       remote-as 65501
ESR(config-bgp-vrf-neighbor)#       address-family ipv4 unicast
ESR(config-bgp-neighbor-af-vrf)#         route-map BGP out
ESR(config-bgp-neighbor-af-vrf)#         enable
ESR(config-bgp-neighbor-af-vrf)#       exit
ESR(config-bgp-vrf-neighbor)#       enable
ESR(config-bgp-vrf-neighbor)#     exit
ESR(config-bgp-vrf)#     address-family ipv4 unicast
ESR(config-bgp-vrf-af)#       redistribute bgp 65500 route-map BGP
ESR(config-bgp-vrf-af)#     exit
ESR(config-bgp-vrf)#     enable
ESR(config-bgp-vrf)#   exit
ESR(config-bgp)#   vrf CE2
ESR(config-bgp-vrf)#     neighbor 192.168.2.1
ESR(config-bgp-vrf-neighbor)#       remote-as 65501
ESR(config-bgp-vrf-neighbor)#       address-family ipv4 unicast
ESR(config-bgp-neighbor-af-vrf)#         route-map BGP out
ESR(config-bgp-neighbor-af-vrf)#         enable
ESR(config-bgp-neighbor-af-vrf)#       exit
ESR(config-bgp-vrf-neighbor)#       enable
ESR(config-bgp-vrf-neighbor)#     exit
ESR(config-bgp-vrf)#     address-family ipv4 unicast
```

```
ESR(config-bgp-vrf-af)#       redistribute bgp 65500 route-map BGP
ESR(config-bgp-vrf-af)#     exit
ESR(config-bgp-vrf)#     enable
ESR(config-bgp-vrf)#   exit
ESR(config-bgp)# exit
ESR(config)#
ESR(config)# router ospf 1
ESR(config-ospf)#   area 0.0.0.0
ESR(config-ospf-area)#     enable
ESR(config-ospf-area)#   exit
ESR(config-ospf)#   enable
ESR(config-ospf)# exit
ESR(config)#
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-if-sub)#   ip vrf forwarding CE1
ESR(config-if-sub)#   description "to CE1"
ESR(config-if-sub)#   ip firewall disable
ESR(config-if-sub)#   ip address 192.168.1.2/30
ESR(config-if-sub)# exit
ESR(config)# interface gigabitethernet 1/0/1.200
ESR(config-if-sub)#   ip vrf forwarding CE2
ESR(config-if-sub)#   description "to CE2"
ESR(config-if-sub)#   ip firewall disable
ESR(config-if-sub)#   ip address 192.168.2.2/30
ESR(config-if-sub)# exit
ESR(config)# interface gigabitethernet 1/0/2
ESR(config-if-gi)#   mtu 1522
ESR(config-if-gi)#   ip firewall disable
ESR(config-if-gi)#   ip address 10.100.0.1/30
ESR(config-if-gi)#   ip ospf instance 1
ESR(config-if-gi)#   ip ospf
ESR(config-if-gi)# exit
ESR(config)# interface loopback 1
ESR(config-loopback)#   ip address 10.10.1.1/32
ESR(config-loopback)#   ip ospf instance 1
ESR(config-loopback)#   ip ospf
ESR(config-loopback)# exit
ESR(config)# mpls
ESR(config-mpls)#   ldp
ESR(config-ldp)#     router-id 10.10.1.1
ESR(config-ldp)#     address-family ipv4
ESR(config-ldp-af-ipv4)#       interface gigabitethernet 1/0/2
ESR(config-ldp-af-ipv4-if)#       exit
ESR(config-ldp-af-ipv4)#     exit
ESR(config-ldp)#     enable
ESR(config-ldp)#   exit
ESR(config-mpls)#   forwarding interface gigabitethernet 1/0/2
ESR(config-mpls)# exit
ESR(config)# do com
ESR(config)# do conf
```

PE2

```
ESR(config)# hostname PE2
ESR(config)#
ESR(config)# ip vrf CE1
ESR(config-vrf)#   ip protocols bgp max-routes 100
ESR(config-vrf)#   rd 65500:1
ESR(config-vrf)#   route-target export 65500:1
ESR(config-vrf)#   route-target import 65500:1
ESR(config-vrf)# exit
ESR(config)# ip vrf CE2
ESR(config-vrf)#   ip protocols bgp max-routes 100
ESR(config-vrf)#   rd 65500:2
ESR(config-vrf)#   route-target export 65500:2
ESR(config-vrf)#   route-target import 65500:2
ESR(config-vrf)# exit
ESR(config)#
ESR(config)# system jumbo-frames
ESR(config)#
ESR(config)# route-map BGP
ESR(config-route-map)#   rule 1
ESR(config-route-map-rule)#   exit
ESR(config-route-map)# exit
ESR(config)# router bgp log-neighbor-changes
ESR(config)# router bgp 65500
ESR(config-bgp)#   router-id 10.11.1.1
ESR(config-bgp)#   neighbor 10.11.1.2
ESR(config-bgp-neighbor)#     remote-as 65500
ESR(config-bgp-neighbor)#     update-source 10.11.1.1
ESR(config-bgp-neighbor)#     address-family vpnv4 unicast
ESR(config-bgp-neighbor-af)#       send-community extended
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     enable
ESR(config-bgp-neighbor)#   exit
ESR(config-bgp)#   enable
ESR(config-bgp)#   vrf CE1
ESR(config-bgp-vrf)#     neighbor 192.168.3.1
ESR(config-bgp-vrf-neighbor)#       remote-as 65501
ESR(config-bgp-vrf-neighbor)#       address-family ipv4 unicast
ESR(config-bgp-neighbor-af-vrf)#         route-map BGP out
ESR(config-bgp-neighbor-af-vrf)#         enable
ESR(config-bgp-neighbor-af-vrf)#       exit
ESR(config-bgp-vrf-neighbor)#       enable
ESR(config-bgp-vrf-neighbor)#     exit
ESR(config-bgp-vrf)#     address-family ipv4 unicast
ESR(config-bgp-vrf-af)#       redistribute bgp 65500 route-map BGP
ESR(config-bgp-vrf-af)#     exit
ESR(config-bgp-vrf)#     enable
ESR(config-bgp-vrf)#   exit
ESR(config-bgp)#   vrf CE2
ESR(config-bgp-vrf)#     neighbor 192.168.4.1
ESR(config-bgp-vrf-neighbor)#       remote-as 65501
ESR(config-bgp-vrf-neighbor)#       address-family ipv4 unicast
ESR(config-bgp-neighbor-af-vrf)#         route-map BGP out
ESR(config-bgp-neighbor-af-vrf)#         enable
ESR(config-bgp-neighbor-af-vrf)#       exit
ESR(config-bgp-vrf-neighbor)#       enable
ESR(config-bgp-vrf-neighbor)#     exit
```

```
ESR(config-bgp-vrf)#     address-family ipv4 unicast
ESR(config-bgp-vrf-af)#       redistribute bgp 65500 route-map BGP
ESR(config-bgp-vrf-af)#     exit
ESR(config-bgp-vrf)#     enable
ESR(config-bgp-vrf)#   exit
ESR(config-bgp)# exit
ESR(config)#
ESR(config)# router ospf 1
ESR(config-ospf)#   area 0.0.0.0
ESR(config-ospf-area)#     enable
ESR(config-ospf-area)#   exit
ESR(config-ospf)#   enable
ESR(config-ospf)# exit
ESR(config)#
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-if-sub)#   ip vrf forwarding CE1
ESR(config-if-sub)#   description "to CE3"
ESR(config-if-sub)#   ip firewall disable
ESR(config-if-sub)#   ip address 192.168.3.2/30
ESR(config-if-sub)# exit
ESR(config)# interface gigabitethernet 1/0/1.200
ESR(config-if-sub)#   ip vrf forwarding CE2
ESR(config-if-sub)#   description "to CE4"
ESR(config-if-sub)#   ip firewall disable
ESR(config-if-sub)#   ip address 192.168.4.2/30
ESR(config-if-sub)# exit
ESR(config)# interface gigabitethernet 1/0/2
ESR(config-if-gi)#   mtu 1522
ESR(config-if-gi)#   ip firewall disable
ESR(config-if-gi)#   ip address 10.101.0.1/30
ESR(config-if-gi)#   ip ospf instance 1
ESR(config-if-gi)#   ip ospf
ESR(config-if-gi)# exit
ESR(config)# interface loopback 1
ESR(config-loopback)#   ip address 10.11.1.1/32
ESR(config-loopback)#   ip ospf instance 1
ESR(config-loopback)#   ip ospf
ESR(config-loopback)# exit
ESR(config)# mpls
ESR(config-mpls)#   ldp
ESR(config-ldp)#     router-id 10.11.1.1
ESR(config-ldp)#     address-family ipv4
ESR(config-ldp-af-ipv4)#       interface gigabitethernet 1/0/2
ESR(config-ldp-af-ipv4-if)#       exit
ESR(config-ldp-af-ipv4)#     exit
ESR(config-ldp)#     enable
ESR(config-ldp)#   exit
ESR(config-mpls)#   forwarding interface gigabitethernet 1/0/2
ESR(config-mpls)# exit
ESR(config)# do com
ESR(config)# do conf
```

Настроим ASBR1 и ASBR2. Для передачи маршрутной информации между ними воспользуемся протоколом OSPF в соответствующих VRF:

ASBR1

```
ESR(config)# hostname ASBR1
ESR(config)#
ESR(config)# ip vrf CE1
ESR(config-vrf)#   ip protocols ospf max-routes 100
ESR(config-vrf)#   rd 65500:1
ESR(config-vrf)#   route-target export 65500:1
ESR(config-vrf)#   route-target import 65500:1
ESR(config-vrf)# exit
ESR(config)# ip vrf CE2
ESR(config-vrf)#   ip protocols ospf max-routes 100
ESR(config-vrf)#   rd 65500:2
ESR(config-vrf)#   route-target export 65500:2
ESR(config-vrf)#   route-target import 65500:2
ESR(config-vrf)# exit
ESR(config)#
ESR(config)# system jumbo-frames
ESR(config)#
ESR(config)# vlan 100,200
ESR(config-vlan)# exit
ESR(config)#
ESR(config)# router bgp 65500
ESR(config-bgp)#   router-id 10.10.1.2
ESR(config-bgp)#   neighbor 10.10.1.1
ESR(config-bgp-neighbor)#     remote-as 65500
ESR(config-bgp-neighbor)#     update-source 10.10.1.2
ESR(config-bgp-neighbor)#     address-family vpnv4 unicast
ESR(config-bgp-neighbor-af)#       send-community extended
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     enable
ESR(config-bgp-neighbor)#   exit
ESR(config-bgp)#   enable
ESR(config-bgp)#   vrf CE1
ESR(config-bgp-vrf)#     address-family ipv4 unicast
ESR(config-bgp-vrf-af)#       redistribute ospf 1 intra-area inter-area external1 external2
ESR(config-bgp-vrf-af)#     exit
ESR(config-bgp-vrf)#   exit
ESR(config-bgp)#   vrf CE2
ESR(config-bgp-vrf)#     address-family ipv4 unicast
ESR(config-bgp-vrf-af)#       redistribute ospf 1 intra-area inter-area external1 external2
ESR(config-bgp-vrf-af)#     exit
ESR(config-bgp-vrf)#   exit
ESR(config-bgp)# exit
ESR(config)#
ESR(config)# router ospf log-adjacency-changes
ESR(config)# router ospf 1
ESR(config-ospf)#   area 0.0.0.0
ESR(config-ospf-area)#     enable
ESR(config-ospf-area)#   exit
ESR(config-ospf)#   enable
ESR(config-ospf)# exit
ESR(config)# router ospf 1 vrf CE1
ESR(config-ospf)#   redistribute bgp 65500
ESR(config-ospf)#   area 0.0.0.0
ESR(config-ospf-area)#     enable
ESR(config-ospf-area)#   exit
ESR(config-ospf)#   enable
```

```
ESR(config-ospf)# exit
ESR(config)# router ospf 1 vrf CE2
ESR(config-ospf)#   area 0.0.0.0
ESR(config-ospf-area)#     enable
ESR(config-ospf-area)#   exit
ESR(config-ospf)#   enable
ESR(config-ospf)# exit
ESR(config)#
ESR(config)# bridge 10
ESR(config-bridge)#   ip vrf forwarding CE1
ESR(config-bridge)#   vlan 100
ESR(config-bridge)#   ip firewall disable
ESR(config-bridge)#   ip address 172.16.32.1/30
ESR(config-bridge)#   ip ospf instance 1
ESR(config-bridge)#   ip ospf
ESR(config-bridge)#   enable
ESR(config-bridge)# exit
ESR(config)# bridge 20
ESR(config-bridge)#   ip vrf forwarding CE2
ESR(config-bridge)#   vlan 200
ESR(config-bridge)#   ip firewall disable
ESR(config-bridge)#   ip address 172.16.32.5/30
ESR(config-bridge)#   ip ospf instance 1
ESR(config-bridge)#   ip ospf
ESR(config-bridge)#   enable
ESR(config-bridge)# exit
ESR(config)#
ESR(config)# interface gigabitethernet 1/0/1
ESR(config-if-gi)#   description "to ASBR2"
ESR(config-if-gi)#   mode switchport
ESR(config-if-gi)#   mtu 1522
ESR(config-if-gi)#   spanning-tree disable
ESR(config-if-gi)#   switchport forbidden default-vlan
ESR(config-if-gi)#   switchport mode trunk
ESR(config-if-gi)#   switchport trunk allowed vlan add 100,200
ESR(config-if-gi)# exit
ESR(config)# interface gigabitethernet 1/0/2
ESR(config-if-gi)#   description "to PE1"
ESR(config-if-gi)#   mtu 1522
ESR(config-if-gi)#   ip firewall disable
ESR(config-if-gi)#   ip address 10.100.0.2/30
ESR(config-if-gi)#   ip ospf instance 1
ESR(config-if-gi)#   ip ospf
ESR(config-if-gi)# exit
ESR(config)# interface loopback 1
ESR(config-loopback)#   ip address 10.10.1.2/32
ESR(config-loopback)#   ip ospf instance 1
ESR(config-loopback)#   ip ospf
ESR(config-loopback)# exit
ESR(config)# mpls
ESR(config-mpls)#   ldp
ESR(config-ldp)#     router-id 10.10.1.2
ESR(config-ldp)#     address-family ipv4
ESR(config-ldp-af-ipv4)#       interface gigabitethernet 1/0/2
ESR(config-ldp-af-ipv4-if)#       exit
ESR(config-ldp-af-ipv4)#     exit
ESR(config-ldp)#     enable
ESR(config-ldp)#   exit
ESR(config-mpls)#   forwarding interface gigabitethernet 1/0/2
ESR(config-mpls)# exit
```

```
ESR(config)# do com
ESR(config)# do conf
```

ASBR2

```
ESR(config)# hostname ASBR2
ESR(config)#
ESR(config)# ip vrf CE1
ESR(config-vrf)#   ip protocols ospf max-routes 100
ESR(config-vrf)#   rd 65500:1
ESR(config-vrf)#   route-target export 65500:1
ESR(config-vrf)#   route-target import 65500:1
ESR(config-vrf)# exit
ESR(config)# ip vrf CE2
ESR(config-vrf)#   ip protocols ospf max-routes 100
ESR(config-vrf)#   rd 65500:2
ESR(config-vrf)#   route-target export 65500:2
ESR(config-vrf)#   route-target import 65500:2
ESR(config-vrf)# exit
ESR(config)#
ESR(config)# system jumbo-frames
ESR(config)#
ESR(config)# vlan 100,200
ESR(config-vlan)# exit
ESR(config)#
ESR(config)# router bgp 65500
ESR(config-bgp)#   router-id 10.11.1.2
ESR(config-bgp)#   neighbor 10.11.1.1
ESR(config-bgp-neighbor)#     remote-as 65500
ESR(config-bgp-neighbor)#     update-source 10.11.1.2
ESR(config-bgp-neighbor)#     address-family vpnv4 unicast
ESR(config-bgp-neighbor-af)#       send-community extended
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     enable
ESR(config-bgp-neighbor)#   exit
ESR(config-bgp)#   enable
ESR(config-bgp)#   vrf CE1
ESR(config-bgp-vrf)#     address-family ipv4 unicast
ESR(config-bgp-vrf-af)#       redistribute ospf 1 intra-area inter-area external1 external2
ESR(config-bgp-vrf-af)#     exit
ESR(config-bgp-vrf)#   exit
ESR(config-bgp)#   vrf CE2
ESR(config-bgp-vrf)#     address-family ipv4 unicast
ESR(config-bgp-vrf-af)#       redistribute ospf 1 intra-area inter-area external1 external2
ESR(config-bgp-vrf-af)#     exit
ESR(config-bgp-vrf)#   exit
ESR(config-bgp)# exit
ESR(config)#
ESR(config)# router ospf log-adjacency-changes
ESR(config)# router ospf 1
ESR(config-ospf)#   area 0.0.0.0
ESR(config-ospf-area)#     enable
ESR(config-ospf-area)#   exit
ESR(config-ospf)#   enable
ESR(config-ospf)# exit
ESR(config)# router ospf 1 vrf CE1
ESR(config-ospf)#   redistribute bgp 65500
ESR(config-ospf)#   area 0.0.0.0
ESR(config-ospf-area)#     enable
ESR(config-ospf-area)#   exit
ESR(config-ospf)#   enable
```

```
ESR(config-ospf)# exit
ESR(config)# router ospf 1 vrf CE2
ESR(config-ospf)#   redistribute bgp 65500
ESR(config-ospf)#   area 0.0.0.0
ESR(config-ospf-area)#     enable
ESR(config-ospf-area)#   exit
ESR(config-ospf)#   enable
ESR(config-ospf)# exit
ESR(config)#
ESR(config)# bridge 10
ESR(config-bridge)#   ip vrf forwarding CE1
ESR(config-bridge)#   vlan 100
ESR(config-bridge)#   ip firewall disable
ESR(config-bridge)#   ip address 172.16.32.2/30
ESR(config-bridge)#   ip ospf instance 1
ESR(config-bridge)#   ip ospf
ESR(config-bridge)#   enable
ESR(config-bridge)# exit
ESR(config)# bridge 20
ESR(config-bridge)#   ip vrf forwarding CE2
ESR(config-bridge)#   vlan 200
ESR(config-bridge)#   ip firewall disable
ESR(config-bridge)#   ip address 172.16.32.6/30
ESR(config-bridge)#   ip ospf instance 1
ESR(config-bridge)#   ip ospf
ESR(config-bridge)#   enable
ESR(config-bridge)# exit
ESR(config)#
ESR(config)# interface gigabitethernet 1/0/1
ESR(config-if-gi)#   description "to ASBR1"
ESR(config-if-gi)#   mode switchport
ESR(config-if-gi)#   mtu 1522
ESR(config-if-gi)#   spanning-tree disable
ESR(config-if-gi)#   switchport forbidden default-vlan
ESR(config-if-gi)#   switchport mode trunk
ESR(config-if-gi)#   switchport trunk allowed vlan add 100,200
ESR(config-if-gi)# exit
ESR(config)# interface gigabitethernet 1/0/2
ESR(config-if-gi)#   description "to PE2"
ESR(config-if-gi)#   mtu 1522
ESR(config-if-gi)#   ip firewall disable
ESR(config-if-gi)#   ip address 10.101.0.2/30
ESR(config-if-gi)#   ip ospf instance 1
ESR(config-if-gi)#   ip ospf
ESR(config-if-gi)# exit
ESR(config)# interface loopback 1
ESR(config-loopback)#   ip address 10.11.1.2/32
ESR(config-loopback)#   ip ospf instance 1
ESR(config-loopback)#   ip ospf
ESR(config-loopback)# exit
ESR(config)# mpls
ESR(config-mpls)#   ldp
ESR(config-ldp)#     router-id 10.11.1.2
ESR(config-ldp)#     address-family ipv4
ESR(config-ldp-af-ipv4)#       interface gigabitethernet 1/0/2
ESR(config-ldp-af-ipv4-if)#       exit
ESR(config-ldp-af-ipv4)#     exit
ESR(config-ldp)#     enable
ESR(config-ldp)#   exit
ESR(config-mpls)#   forwarding interface gigabitethernet 1/0/2
```

```
ESR(config-mpls)# exit
ESR(config)# do com
ESR(config)# do conf
```

Проверим распространение маршрутной информации и сетевую доступность узлов:

```
PE1# sh bgp vpnv4 unicast all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes Route Distinguisher   IP Prefix          Next hop        Metric     Label   LocPrf
Weight Path
----- --------------------- ------------------ --------------- ---------- ------- ----------
------ ----------------
*>    65500:1               10.110.0.1/32      --              --         37      100        --
65501 i
*>    65500:1               10.111.0.1/32      --              --         35      100        --
65501 i
*>i   65500:1               10.113.0.1/32      10.10.1.2       --         43      100
0      ?
*>i   65500:1               10.114.0.1/32      10.10.1.2       --         48      100
0      ?

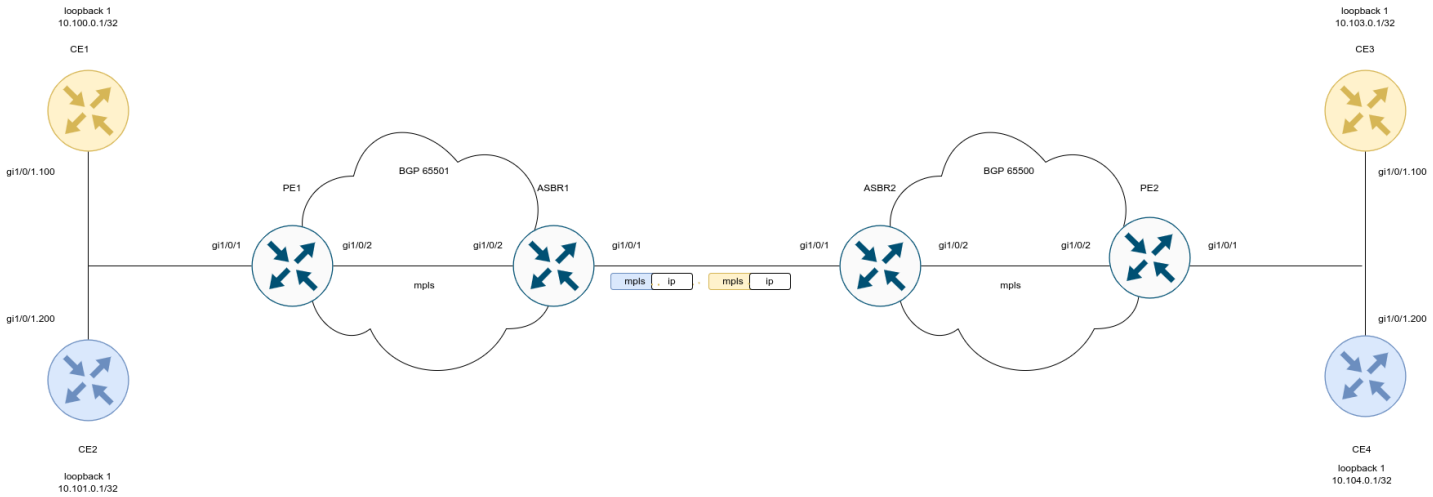
CE1# ping 10.113.0.1 source ip 10.110.0.1 detailed
PING 10.113.0.1 (10.113.0.1) from 10.110.0.1 : 56 bytes of data.
64 bytes from 10.113.0.1: icmp_seq=1 ttl=0 time=1.31 ms
64 bytes from 10.113.0.1: icmp_seq=2 ttl=0 time=1.14 ms
64 bytes from 10.113.0.1: icmp_seq=3 ttl=0 time=1.08 ms
64 bytes from 10.113.0.1: icmp_seq=4 ttl=0 time=1.06 ms
64 bytes from 10.113.0.1: icmp_seq=5 ttl=0 time=1.16 ms
```

12.12 Inter-AS Option B

В отличие от Option A, между ASBR нет необходимости использовать VRF: при передаче трафика между ASBR будет навешиваться mpls-метка. Данная схема имеет лучшую масштабируемость.

> ⚠ В текущей реализации Option B поддержана только для VPN-IPv4 маршрутов (AFI = 1, SAFI = 128).

12.12.1 L3VPN



Настроим CE:

CE1

```
ESR(config)# hostname CE1
ESR(config)#
ESR(config)# route-map BGP
ESR(config-route-map)#   rule 1
ESR(config-route-map-rule)#   exit
ESR(config-route-map)# exit
ESR(config)# router bgp 65510
ESR(config-bgp)#   neighbor 192.168.1.2
ESR(config-bgp-neighbor)#     remote-as 65500
ESR(config-bgp-neighbor)#     address-family ipv4 unicast
ESR(config-bgp-neighbor-af)#       route-map BGP out
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     enable
ESR(config-bgp-neighbor)#   exit
ESR(config-bgp)#   address-family ipv4 unicast
ESR(config-bgp-af)#     network 10.100.0.1/32
ESR(config-bgp-af)#   exit
ESR(config-bgp)#   enable
ESR(config-bgp)# exit
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-if-sub)#   ip firewall disable
ESR(config-if-sub)#   ip address 192.168.1.1/30
ESR(config-if-sub)# exit
ESR(config)# interface loopback 1
ESR(config-loopback)#   ip address 10.100.0.1/32
ESR(config-loopback)# exit
ESR(config)# do com
ESR(config)# do conf
```

CE2

```
ESR(config)# hostname CE2
ESR(config)#
ESR(config)# route-map BGP
ESR(config-route-map)#   rule 1
ESR(config-route-map-rule)#   exit
ESR(config-route-map)# exit
ESR(config)# router bgp 65511
ESR(config-bgp)#   neighbor 192.168.2.2
ESR(config-bgp-neighbor)#     remote-as 65500
ESR(config-bgp-neighbor)#     address-family ipv4 unicast
ESR(config-bgp-neighbor-af)#       route-map BGP out
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     enable
ESR(config-bgp-neighbor)#   exit
ESR(config-bgp)#   address-family ipv4 unicast
ESR(config-bgp-af)#     network 10.101.0.1/32
ESR(config-bgp-af)#   exit
ESR(config-bgp)#   enable
ESR(config-bgp)# exit
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-if-sub)#   ip firewall disable
ESR(config-if-sub)#   ip address 192.168.2.1/30
ESR(config-if-sub)# exit
ESR(config)#
ESR(config)# interface loopback 1
ESR(config-loopback)#   ip address 10.101.0.1/32
ESR(config-loopback)# exit
ESR(config)# do com
ESR(config)# do conf
```

CE3

```
ESR(config)# hostname CE3
ESR(config)#
ESR(config)# route-map BGP
ESR(config-route-map)#   rule 1
ESR(config-route-map-rule)#   exit
ESR(config-route-map)# exit
ESR(config)# router bgp 65512
ESR(config-bgp)#   neighbor 192.168.3.2
ESR(config-bgp-neighbor)#     remote-as 65500
ESR(config-bgp-neighbor)#     address-family ipv4 unicast
ESR(config-bgp-neighbor-af)#       route-map BGP out
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     enable
ESR(config-bgp-neighbor)#   exit
ESR(config-bgp)#   address-family ipv4 unicast
ESR(config-bgp-af)#     network 10.103.0.1/32
ESR(config-bgp-af)#   exit
ESR(config-bgp)#   enable
ESR(config-bgp)# exit
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-if-sub)#   ip firewall disable
ESR(config-if-sub)#   ip address 192.168.3.1/30
ESR(config-if-sub)# exit
ESR(config)#
ESR(config)# interface loopback 1
ESR(config-loopback)#   ip address 10.103.0.1/32
ESR(config-loopback)# exit
ESR(config)# do com
ESR(config)# do conf
```

CE4

```
ESR(config)# hostname CE4
ESR(config)#
ESR(config)# route-map BGP
ESR(config-route-map)#   rule 1
ESR(config-route-map-rule)#   exit
ESR(config-route-map)# exit
ESR(config)# router bgp 65513
ESR(config-bgp)#   neighbor 192.168.4.2
ESR(config-bgp-neighbor)#     remote-as 65500
ESR(config-bgp-neighbor)#     address-family ipv4 unicast
ESR(config-bgp-neighbor-af)#       route-map BGP out
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     enable
ESR(config-bgp-neighbor)#   exit
ESR(config-bgp)#   address-family ipv4 unicast
ESR(config-bgp-af)#     network 10.104.0.1/32
ESR(config-bgp-af)#   exit
ESR(config-bgp)#   enable
ESR(config-bgp)# exit
ESR(config)# interface gigabitethernet 1/0/1.100
ESR(config-if-sub)#   ip firewall disable
ESR(config-if-sub)#   ip address 192.168.4.1/30
ESR(config-if-sub)# exit
ESR(config)#
ESR(config)# interface loopback 1
ESR(config-loopback)#   ip address 10.104.0.1/32
ESR(config-loopback)# exit
ESR(config)# do com
ESR(config)# do conf
```

Произведем настройку PE1 и PE2:

PE1

```
PE1(config)# hostname PE1
PE1(config)#
PE1(config)# ip vrf CE1
PE1(config-vrf)# ip protocols bgp max-routes 100
PE1(config-vrf)# rd 65501:1
PE1(config-vrf)# route-target export 65501:1
PE1(config-vrf)# route-target import 65501:1
PE1(config-vrf)# exit
PE1(config)# ip vrf CE2
PE1(config-vrf)# ip protocols bgp max-routes 100
PE1(config-vrf)# rd 65501:2
PE1(config-vrf)# route-target export 65501:2
PE1(config-vrf)# route-target import 65501:2
PE1(config-vrf)# exit
PE1(config)#
PE1(config)# system jumbo-frames
PE1(config)#
PE1(config)# route-map BGP_OUT
PE1(config-route-map)# rule 1
PE1(config-route-map-rule)# exit
PE1(config-route-map)# exit
PE1(config)# router bgp 65501
PE1(config-bgp)# neighbor 10.10.1.2
PE1(config-bgp-neighbor)# remote-as 65501
PE1(config-bgp-neighbor)# update-source 10.10.1.1
PE1(config-bgp-neighbor)# address-family vpnv4 unicast
PE1(config-bgp-neighbor-af)# send-community extended
PE1(config-bgp-neighbor-af)# enable
PE1(config-bgp-neighbor-af)# exit
PE1(config-bgp-neighbor)# enable
PE1(config-bgp-neighbor)# exit
PE1(config-bgp)# enable
PE1(config-bgp)# vrf CE1
PE1(config-bgp-vrf)# neighbor 192.168.1.1
PE1(config-bgp-vrf-neighbor)# remote-as 65510
PE1(config-bgp-vrf-neighbor)# address-family ipv4 unicast
PE1(config-bgp-neighbor-af-vrf)# route-map BGP_OUT out
PE1(config-bgp-neighbor-af-vrf)# enable
PE1(config-bgp-neighbor-af-vrf)# exit
PE1(config-bgp-vrf-neighbor)# enable
PE1(config-bgp-vrf-neighbor)# exit
PE1(config-bgp-vrf)# address-family ipv4 unicast
PE1(config-bgp-vrf-af)# redistribute bgp 65501 route-map BGP_OUT
PE1(config-bgp-vrf-af)# exit
PE1(config-bgp-vrf)# enable
PE1(config-bgp-vrf)# exit
PE1(config-bgp)# vrf CE2
PE1(config-bgp-vrf)# neighbor 192.168.2.1
PE1(config-bgp-vrf-neighbor)# remote-as 65511
PE1(config-bgp-vrf-neighbor)# address-family ipv4 unicast
PE1(config-bgp-neighbor-af-vrf)# route-map BGP_OUT out
PE1(config-bgp-neighbor-af-vrf)# enable
PE1(config-bgp-neighbor-af-vrf)# exit
PE1(config-bgp-vrf-neighbor)# enable
PE1(config-bgp-vrf-neighbor)# exit
PE1(config-bgp-vrf)# address-family ipv4 unicast
PE1(config-bgp-vrf-af)# redistribute bgp 65501 route-map BGP_OUT
```

```
PE1(config-bgp-vrf-af)# exit
PE1(config-bgp-vrf)# enable
PE1(config-bgp-vrf)# exit
PE1(config-bgp)# exit
PE1(config)#
PE1(config)# router ospf 1
PE1(config-ospf)# area 0.0.0.0
PE1(config-ospf-area)# enable
PE1(config-ospf-area)# exit
PE1(config-ospf)# enable
PE1(config-ospf)# exit
PE1(config)#
PE1(config)# interface gigabitethernet 1/0/1.100
PE1(config-if-sub)# ip vrf forwarding CE1
PE1(config-if-sub)# description "to CE1"
PE1(config-if-sub)# ip firewall disable
PE1(config-if-sub)# ip address 192.168.1.2/30
PE1(config-if-sub)# exit
PE1(config)# interface gigabitethernet 1/0/1.200
PE1(config-if-sub)# ip vrf forwarding CE2
PE1(config-if-sub)# description "to CE2"
PE1(config-if-sub)# ip firewall disable
PE1(config-if-sub)# ip address 192.168.2.2/30
PE1(config-if-sub)# exit
PE1(config)# interface gigabitethernet 1/0/2
PE1(config-if-gi)# description "to ASBR1"
PE1(config-if-gi)# mtu 1522
PE1(config-if-gi)# ip firewall disable
PE1(config-if-gi)# ip address 10.100.0.1/30
PE1(config-if-gi)# ip ospf instance 1
PE1(config-if-gi)# ip ospf
PE1(config-if-gi)# exit
PE1(config)# interface loopback 1
PE1(config-loopback)# ip address 10.10.1.1/32
PE1(config-loopback)# ip ospf instance 1
PE1(config-loopback)# ip ospf
PE1(config-loopback)# exit
PE1(config)# mpls
PE1(config-mpls)# ldp
PE1(config-ldp)# router-id 10.10.1.1
PE1(config-ldp)# address-family ipv4
PE1(config-ldp-af-ipv4)# interface gigabitethernet 1/0/2
PE1(config-ldp-af-ipv4-if)# exit
PE1(config-ldp-af-ipv4)# exit
PE1(config-ldp)# enable
PE1(config-ldp)# exit
PE1(config-mpls)# forwarding interface gigabitethernet 1/0/2
PE1(config-mpls)# exit
PE1(config)# do com
PE1(config)# do conf
```

PE2

```
PE2(config)# hostname PE2
PE2(config)#
PE2(config)# ip vrf CE3
PE2(config-vrf)#   ip protocols bgp max-routes 100
PE2(config-vrf)#   rd 65501:1
PE2(config-vrf)#   route-target export 65501:1
PE2(config-vrf)#   route-target import 65501:1
PE2(config-vrf)# exit
PE2(config)# ip vrf CE4
PE2(config-vrf)#   ip protocols bgp max-routes 100
PE2(config-vrf)#   rd 65501:2
PE2(config-vrf)#   route-target export 65501:2
PE2(config-vrf)#   route-target import 65501:2
PE2(config-vrf)# exit
PE2(config)#
PE2(config)# system jumbo-frames
PE2(config)#
PE2(config)# route-map BGP_OUT
PE2(config-route-map)#   rule 1
PE2(config-route-map-rule)#   exit
PE2(config-route-map)# exit
PE2(config)# router bgp 65500
PE2(config-bgp)#   neighbor 10.11.1.2
PE2(config-bgp-neighbor)#     remote-as 65500
PE2(config-bgp-neighbor)#     update-source 10.11.1.1
PE2(config-bgp-neighbor)#     address-family vpnv4 unicast
PE2(config-bgp-neighbor-af)#       send-community extended
PE2(config-bgp-neighbor-af)#       enable
PE2(config-bgp-neighbor-af)#     exit
PE2(config-bgp-neighbor)#     enable
PE2(config-bgp-neighbor)#   exit
PE2(config-bgp)#   enable
PE2(config-bgp)#   vrf CE3
PE2(config-bgp-vrf)#     neighbor 192.168.3.1
PE2(config-bgp-vrf-neighbor)#       remote-as 65512
PE2(config-bgp-vrf-neighbor)#       address-family ipv4 unicast
PE2(config-bgp-neighbor-af-vrf)#         route-map BGP_OUT out
PE2(config-bgp-neighbor-af-vrf)#         enable
PE2(config-bgp-neighbor-af-vrf)#       exit
PE2(config-bgp-vrf-neighbor)#       enable
PE2(config-bgp-vrf-neighbor)#     exit
PE2(config-bgp-vrf)#     address-family ipv4 unicast
PE2(config-bgp-vrf-af)#       redistribute bgp 65500 route-map BGP_OUT
PE2(config-bgp-vrf-af)#     exit
PE2(config-bgp-vrf)#     enable
PE2(config-bgp-vrf)#   exit
PE2(config-bgp)#   vrf CE4
PE2(config-bgp-vrf)#     neighbor 192.168.4.1
PE2(config-bgp-vrf-neighbor)#       remote-as 65513
PE2(config-bgp-vrf-neighbor)#       address-family ipv4 unicast
PE2(config-bgp-neighbor-af-vrf)#         route-map BGP_OUT out
PE2(config-bgp-neighbor-af-vrf)#         enable
PE2(config-bgp-neighbor-af-vrf)#       exit
PE2(config-bgp-vrf-neighbor)#       enable
PE2(config-bgp-vrf-neighbor)#     exit
PE2(config-bgp-vrf)#     address-family ipv4 unicast
PE2(config-bgp-vrf-af)#       redistribute bgp 65500 route-map BGP_OUT
```

```
PE2(config-bgp-vrf-af)#     exit
PE2(config-bgp-vrf)#     enable
PE2(config-bgp-vrf)#   exit
PE2(config-bgp)# exit
PE2(config)#
PE2(config)# router ospf 1
PE2(config-ospf)#   router-id 10.11.1.1
PE2(config-ospf)#   area 0.0.0.0
PE2(config-ospf-area)#     enable
PE2(config-ospf-area)#   exit
PE2(config-ospf)#   enable
PE2(config-ospf)# exit
PE2(config)#
PE2(config)# interface gigabitethernet 1/0/1.100
PE2(config-if-sub)#   ip vrf forwarding CE3
PE2(config-if-sub)#   description "to CE3"
PE2(config-if-sub)#   ip firewall disable
PE2(config-if-sub)#   ip address 192.168.3.2/30
PE2(config-if-sub)# exit
PE2(config)# interface gigabitethernet 1/0/1.200
PE2(config-if-sub)#   ip vrf forwarding CE4
PE2(config-if-sub)#   description "CE4"
PE2(config-if-sub)#   ip firewall disable
PE2(config-if-sub)#   ip address 192.168.4.2/30
PE2(config-if-sub)# exit
PE2(config)# interface gigabitethernet 1/0/2
PE2(config-if-gi)#   description "to ASBR2"
PE2(config-if-gi)#   mtu 1522
PE2(config-if-gi)#   ip firewall disable
PE2(config-if-gi)#   ip address 10.102.0.1/30
PE2(config-if-gi)#   ip ospf instance 1
PE2(config-if-gi)#   ip ospf
PE2(config-if-gi)# exit
PE2(config)# interface loopback 1
PE2(config-loopback)#   ip address 10.11.1.1/32
PE2(config-loopback)#   ip ospf instance 1
PE2(config-loopback)#   ip ospf
PE2(config-loopback)# exit
PE2(config)# mpls
PE2(config-mpls)#   ldp
PE2(config-ldp)#     router-id 10.11.1.1
PE2(config-ldp)#     address-family ipv4
PE2(config-ldp-af-ipv4)#       interface gigabitethernet 1/0/2
PE2(config-ldp-af-ipv4-if)#       exit
PE2(config-ldp-af-ipv4)#     exit
PE2(config-ldp)#     enable
PE2(config-ldp)#   exit
PE2(config-mpls)#   forwarding interface gigabitethernet 1/0/2
PE2(config-mpls)# exit
PE2(config)# do com
PE2(config)# do conf
```

Настроим ASBR1 и ASBR2:

ASBR1

```
ASBR1(config)# hostname ASBR1
ASBR1(config)#
ASBR1(config)# system jumbo-frames
ASBR1(config)#
ASBR1(config)# route-map VPNv4
ASBR1(config-route-map)#   rule 1
ASBR1(config-route-map-rule)#   exit
ASBR1(config-route-map)# exit
ASBR1(config)# router bgp 65501
ASBR1(config-bgp)#   router-id 10.10.1.2
ASBR1(config-bgp)#   neighbor 10.10.1.1
ASBR1(config-bgp-neighbor)#     remote-as 65501
ASBR1(config-bgp-neighbor)#     update-source 10.10.1.2
ASBR1(config-bgp-neighbor)#     address-family vpnv4 unicast
ASBR1(config-bgp-neighbor-af)#       next-hop-self
ASBR1(config-bgp-neighbor-af)#       send-community extended
ASBR1(config-bgp-neighbor-af)#       enable
ASBR1(config-bgp-neighbor-af)#     exit
ASBR1(config-bgp-neighbor)#     enable
ASBR1(config-bgp-neighbor)#   exit
ASBR1(config-bgp)#   neighbor 10.101.0.1
ASBR1(config-bgp-neighbor)#     remote-as 65500
ASBR1(config-bgp-neighbor)#     address-family vpnv4 unicast
ASBR1(config-bgp-neighbor-af)#       route-map VPNv4 out
ASBR1(config-bgp-neighbor-af)#       send-community extended
ASBR1(config-bgp-neighbor-af)#       enable
ASBR1(config-bgp-neighbor-af)#     exit
ASBR1(config-bgp-neighbor)#     enable
ASBR1(config-bgp-neighbor)#   exit
ASBR1(config-bgp)#   enable
ASBR1(config-bgp)# exit
ASBR1(config)#
ASBR1(config)# router ospf 1
ASBR1(config-ospf)#   area 0.0.0.0
ASBR1(config-ospf-area)#     enable
ASBR1(config-ospf-area)#   exit
ASBR1(config-ospf)#   enable
ASBR1(config-ospf)# exit
ASBR1(config)#
ASBR1(config)# interface gigabitethernet 1/0/1
ASBR1(config-if-gi)#   description "to ASBR2"
ASBR1(config-if-gi)#   ip firewall disable
ASBR1(config-if-gi)#   ip address 10.101.0.2/30
ASBR1(config-if-gi)# exit
ASBR1(config)# interface gigabitethernet 1/0/2
ASBR1(config-if-gi)#   description "to PE1"
ASBR1(config-if-gi)#   mtu 1522
ASBR1(config-if-gi)#   ip firewall disable
ASBR1(config-if-gi)#   ip address 10.100.0.2/30
ASBR1(config-if-gi)#   ip ospf instance 1
ASBR1(config-if-gi)#   ip ospf
ASBR1(config-if-gi)# exit
ASBR1(config)# interface loopback 1
ASBR1(config-loopback)#   ip address 10.10.1.2/32
ASBR1(config-loopback)#   ip ospf instance 1
ASBR1(config-loopback)#   ip ospf
ASBR1(config-loopback)# exit
```

```
ASBR1(config)# mpls
ASBR1(config-mpls)#   ldp
ASBR1(config-ldp)#     router-id 10.10.1.2
ASBR1(config-ldp)#     address-family ipv4
ASBR1(config-ldp-af-ipv4)#       interface gigabitethernet 1/0/2
ASBR1(config-ldp-af-ipv4-if)#       exit
ASBR1(config-ldp-af-ipv4)#     exit
ASBR1(config-ldp)#     enable
ASBR1(config-ldp)#   exit
ASBR1(config-mpls)#   forwarding interface gigabitethernet 1/0/1
ASBR1(config-mpls)#   forwarding interface gigabitethernet 1/0/2
ASBR1(config-mpls)# exit
ASBR1(config)# do com
ASBR1(config)# do conf
```

ASBR2

```
ASBR2(config)# hostname ASBR2
ASBR2(config)#
ASBR2(config)# system jumbo-frames
ASBR2(config)#
ASBR2(config)# route-map VPNv4
ASBR2(config-route-map)#   rule 1
ASBR2(config-route-map-rule)#   exit
ASBR2(config-route-map)# exit
ASBR2(config)# router bgp 65500
ASBR2(config-bgp)#   router-id 10.11.1.2
ASBR2(config-bgp)#   neighbor 10.101.0.2
ASBR2(config-bgp-neighbor)#     remote-as 65501
ASBR2(config-bgp-neighbor)#     address-family vpnv4 unicast
ASBR2(config-bgp-neighbor-af)#       route-map VPNv4 out
ASBR2(config-bgp-neighbor-af)#       send-community extended
ASBR2(config-bgp-neighbor-af)#       enable
ASBR2(config-bgp-neighbor-af)#     exit
ASBR2(config-bgp-neighbor)#     enable
ASBR2(config-bgp-neighbor)#   exit
ASBR2(config-bgp)#   neighbor 10.11.1.1
ASBR2(config-bgp-neighbor)#     remote-as 65500
ASBR2(config-bgp-neighbor)#     update-source 10.11.1.2
ASBR2(config-bgp-neighbor)#     address-family vpnv4 unicast
ASBR2(config-bgp-neighbor-af)#       next-hop-self
ASBR2(config-bgp-neighbor-af)#       send-community extended
ASBR2(config-bgp-neighbor-af)#       enable
ASBR2(config-bgp-neighbor-af)#     exit
ASBR2(config-bgp-neighbor)#     enable
ASBR2(config-bgp-neighbor)#   exit
ASBR2(config-bgp)#   enable
ASBR2(config-bgp)# exit
ASBR2(config)#
ASBR2(config)# router ospf 1
ASBR2(config-ospf)#   router-id 10.11.1.2
ASBR2(config-ospf)#   area 0.0.0.0
ASBR2(config-ospf-area)#     enable
ASBR2(config-ospf-area)#   exit
ASBR2(config-ospf)#   enable
ASBR2(config-ospf)# exit
ASBR2(config)#
ASBR2(config)# interface gigabitethernet 1/0/1
ASBR2(config-if-gi)#   description "to ASBR1"
ASBR2(config-if-gi)#   ip firewall disable
ASBR2(config-if-gi)#   ip address 10.101.0.1/30
ASBR2(config-if-gi)# exit
ASBR2(config)# interface gigabitethernet 1/0/2
ASBR2(config-if-gi)#   description "to PE2"
ASBR2(config-if-gi)#   mtu 1522
ASBR2(config-if-gi)#   ip firewall disable
ASBR2(config-if-gi)#   ip address 10.102.0.2/30
ASBR2(config-if-gi)#   ip ospf instance 1
ASBR2(config-if-gi)#   ip ospf
ASBR2(config-if-gi)# exit
ASBR2(config)# interface loopback 1
ASBR2(config-loopback)#   ip address 10.11.1.2/32
ASBR2(config-loopback)#   ip ospf instance 1
ASBR2(config-loopback)#   ip ospf
```

```
ASBR2(config-loopback)# exit
ASBR2(config)# mpls
ASBR2(config-mpls)#   ldp
ASBR2(config-ldp)#     router-id 10.11.1.2
ASBR2(config-ldp)#     address-family ipv4
ASBR2(config-ldp-af-ipv4)#       interface gigabitethernet 1/0/2
ASBR2(config-ldp-af-ipv4-if)#       exit
ASBR2(config-ldp-af-ipv4)#     exit
ASBR2(config-ldp)#     enable
ASBR2(config-ldp)#   exit
ASBR2(config-mpls)#   forwarding interface gigabitethernet 1/0/1
ASBR2(config-mpls)#   forwarding interface gigabitethernet 1/0/2
ASBR2(config-mpls)# exit
ASBR2(config)# do com
ASBR2(config)# do conf
```

После завершения настройки проверим распространение маршрутной информации и сетевую доступность узлов:

```
PE1# sh bgp vpnv4 unicast all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes Route Distinguisher   IP Prefix          Next hop        Metric     Label   LocPrf
Weight Path
----- --------------------- ------------------ --------------- ---------- ------- ----------
------ ----------------
*>i   65501:2               10.104.0.1/32      10.10.1.2       --         23      100        0
65500 65513 i
*>i   65501:1               10.103.0.1/32      10.10.1.2       --         19      100        0
65500 65512 i
*>    65501:2               10.101.0.1/32      --              --         29      100        --
65511 i
*>    65501:1               10.100.0.1/32      --              --         28      100        --
65510 i
ASBR1#    sh bgp vpnv4 unicast all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes Route Distinguisher   IP Prefix          Next hop        Metric     Label   LocPrf
Weight Path
----- --------------------- ------------------ --------------- ---------- ------- ----------
------ ----------------
*>    65501:2               10.104.0.1/32      10.101.0.1      --         24      100        0
65500 65513 i
*>    65501:1               10.103.0.1/32      10.101.0.1      --         20      100        0
65500 65512 i
*>i   65501:2               10.101.0.1/32      10.10.1.1       --         29      100        0
65511 i
*>i   65501:1               10.100.0.1/32      10.10.1.1       --         28      100        0
65510 i

ASBR2# sh bgp vpnv4 unicast all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes Route Distinguisher   IP Prefix          Next hop        Metric     Label   LocPrf
Weight Path
----- --------------------- ------------------ --------------- ---------- ------- ----------
------ ----------------
*>i   65501:2               10.104.0.1/32      10.11.1.1       --         19      100        0
65513 i
*>i   65501:1               10.103.0.1/32      10.11.1.1       --         18      100        0
65512 i
*>    65501:2               10.101.0.1/32      10.101.0.2      --         30      100        0
65501 65511 i
*>    65501:1               10.100.0.1/32      10.101.0.2      --         31      100        0
65501 65510 i

PE2# sh bgp vpnv4 unicast all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes Route Distinguisher   IP Prefix          Next hop        Metric     Label   LocPrf
Weight Path
----- --------------------- ------------------ --------------- ---------- ------- ----------
------ ----------------
```

```
*>    65501:2              10.104.0.1/32      --              --          19      100         --
65513 i
*>    65501:1              10.103.0.1/32      --              --          18      100         --
65512 i
*>i   65501:2              10.101.0.1/32      10.11.1.2       --          29      100         0
65501 65511 i
*>i   65501:1              10.100.0.1/32      10.11.1.2       --          30      100         0
65501 65510 i

CE4# ping 10.104.0.1 source ip 10.101.0.1  detailed
PING 10.104.0.1 (10.104.0.1) from 10.101.0.1 : 56 bytes of data.
64 bytes from 10.104.0.1: icmp_seq=1 ttl=0 time=2.25 ms
64 bytes from 10.104.0.1: icmp_seq=2 ttl=0 time=2.08 ms
64 bytes from 10.104.0.1: icmp_seq=3 ttl=0 time=2.15 ms
64 bytes from 10.104.0.1: icmp_seq=4 ttl=0 time=2.12 ms
64 bytes from 10.104.0.1: icmp_seq=5 ttl=0 time=2.09 ms

CE1# ping 10.103.0.1 source ip 10.100.0.1 detailed
PING 10.103.0.1 (10.103.0.1) from 10.100.0.1 : 56 bytes of data.
64 bytes from 10.103.0.1: icmp_seq=1 ttl=0 time=2.22 ms
```

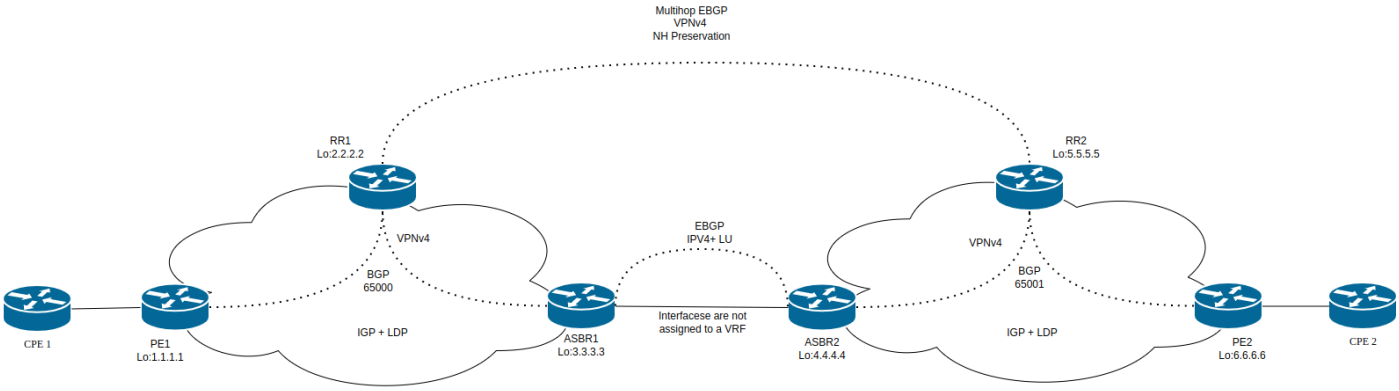
12.13 Inter-AS Option C

Inter-AS Option C является третьим сценарием для настройки связности различных автономных систем, описанным в RFC 4364. Данный сценарий является наиболее масштабируемым из описанных ранее, однако он имеет свои особенности, которые необходимо учитывать при построении сети.

В данной схеме ASBR-ы не хранят клиентские VPNv4-префиксы, а только распространяют маршрутную информацию и метки для PE-устройств в своей автономной системе.

Для распространения клиентских VPNv4-префиксов между различными автономными системами используется MP-EBGP-сессия между устройствами, выполняющими роль RR (route reflector), либо между PE-устройствами. В случае, если VPNv4-сессия настраивается между RR, то в передаваемых BGP update сообщениях не должен меняться атрибут next-hop.

В рамках EBGP-сессии между ASBR производится обмен маршрутной информацией о транспортных префиксах PE различных автономных систем. Эти маршруты отвечают за доступность next-hop для клиентских VPNv4-префиксов, передаваемых в рамках MP-EBGP-сессии между RR или PE. Данные префиксы также используются для установления MP-EBGP-сессии между устройствами, выполняющими роль RR либо роль PE в разных автономных системах.



Из плюсов данного решения можно отметить хорошую масштабируемость. ASBR-устройства не хранят данные клиентских префиксов, вся информация хранится на RR, что положительно сказывается на производительности.

Из недостатков можно отметить следующее:

- Безопасность. Передача транспортных префиксов PE из локальной AS во вне несет в себе потенциальные риски. Межу AS должен быть установлен высокий уровень доверия.
- QoS. VPN-контексты отсутствует на ASBR, соответственно нет возможности применить shaping/policing per VPN.

Для организации сквозных настроек QoS требуется согласование настроек на стыке ASBR↔ASBR.

12.13.1 L3VPN

Предварительная конфигурация:

- Внутри AS должен быть настроен IGP для распространения маршрутной информации для связности PE.
- Внутри AS должен быть настроен протокол LDP для распространения меток.
- На PE, к которым подключены абонентские CPE, должны быть настроены соответствующие VRF. Интерфейсы, к которым подключены CPE, должны быть помещены в соответствующий VRF.

Для настройки сервиса VPN приведем пример конфигурации устройств одной из AS (настройки в другой AS будут полностью зеркальные):

PE-1

```
ESR(config)# hostname PE1
ESR(config)#
ESR(config)# ip vrf vrf1
ESR(config-vrf)#  rd 1.1.1.1:1
ESR(config-vrf)#   route-target export 100:1
ESR(config-vrf)#   route-target import 100:1
ESR(config-vrf)# exit
ESR(config)#
ESR(config)# router bgp 65000
ESR(config-bgp)#   neighbor 2.2.2.2
ESR(config-bgp-neighbor)#     remote-as 65000
ESR(config-bgp-neighbor)#     update-source loopback 1
ESR(config-bgp-neighbor)#     address-family ipv4 unicast
ESR(config-bgp-neighbor-af)#       send-label
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     address-family vpnv4 unicast
ESR(config-bgp-neighbor-af)#       next-hop-self
ESR(config-bgp-neighbor-af)#       send-community extended
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     enable
ESR(config-bgp-neighbor)#   exit
ESR(config-bgp)#   enable
ESR(config-bgp)#   vrf vrf1
ESR(config-bgp-vrf)#     address-family ipv4 unicast
ESR(config-bgp-vrf-af)#       network 100.100.100.1/32
ESR(config-bgp-vrf-af)#     exit
ESR(config-bgp-vrf)#   exit
ESR(config-bgp)# exit
```

В примере конфигурации PE устройства префикс 100.100.100.1 является примером абонентской подсети.

RR-1

```
ESR(config)# hostname RR1
ESR(config)#
ESR(config)# route-map VPNv4_RM1
ESR(config-route-map)#   rule 1
ESR(config-route-map-rule)#   exit
ESR(config-route-map)# exit
ESR(config)# router bgp 65000
ESR(config-bgp)#   neighbor 3.3.3.3
ESR(config-bgp-neighbor)#     remote-as 65000
ESR(config-bgp-neighbor)#     route-reflector-client
ESR(config-bgp-neighbor)#     update-source loopback 1
ESR(config-bgp-neighbor)#     address-family ipv4 unicast
ESR(config-bgp-neighbor-af)#         send-label
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     enable
ESR(config-bgp-neighbor)#   exit
ESR(config-bgp)#   neighbor 1.1.1.1
ESR(config-bgp-neighbor)#     remote-as 65000
ESR(config-bgp-neighbor)#     route-reflector-client
ESR(config-bgp-neighbor)#     update-source loopback 1
ESR(config-bgp-neighbor)#     address-family ipv4 unicast
ESR(config-bgp-neighbor-af)#       send-label
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     address-family vpnv4 unicast
ESR(config-bgp-neighbor-af)#       send-community extended
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     enable
ESR(config-bgp-neighbor)#   exit
ESR(config-bgp)#   neighbor 5.5.5.5
ESR(config-bgp-neighbor)#     remote-as 65001
ESR(config-bgp-neighbor)#     ebgp-multihop 10
ESR(config-bgp-neighbor)#     update-source loopback 1
ESR(config-bgp-neighbor)#     address-family vpnv4 unicast
ESR(config-bgp-neighbor-af)#       route-map VPNv4_RM1 out
ESR(config-bgp-neighbor-af)#       next-hop-unchanged
ESR(config-bgp-neighbor-af)#       send-community extended
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     enable
ESR(config-bgp-neighbor)#   exit
ESR(config-bgp)#   enable
ESR(config-bgp)# exit
```

ASBR-1

```
ESR(config)# hostname ASBR1
ESR(config)#
ESR(config)# route-map RM1
ESR(config-route-map)#   rule 1
ESR(config-route-map-rule)#   exit
ESR(config-route-map)#exit
ESR(config)# router bgp 65000
ESR(config-bgp)#   neighbor 2.2.2.2
ESR(config-bgp-neighbor)#     remote-as 65000
ESR(config-bgp-neighbor)#     update-source loopback 1
ESR(config-bgp-neighbor)#     address-family ipv4 unicast
ESR(config-bgp-neighbor-af)#       next-hop-self
ESR(config-bgp-neighbor-af)#       send-label
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     enable
ESR(config-bgp-neighbor)#   exit
ESR(config-bgp)#   neighbor 192.168.100.1
ESR(config-bgp-neighbor)#     remote-as 65001
ESR(config-bgp-neighbor)#     address-family ipv4 unicast
ESR(config-bgp-neighbor-af)#       route-map RM1 out
ESR(config-bgp-neighbor-af)#       send-label
ESR(config-bgp-neighbor-af)#       enable
ESR(config-bgp-neighbor-af)#     exit
ESR(config-bgp-neighbor)#     enable
ESR(config-bgp-neighbor)#   exit
ESR(config-bgp)#   address-family ipv4 unicast
ESR(config-bgp-af)#     network 1.1.1.1/32
ESR(config-bgp-af)#     network 2.2.2.2/32
ESR(config-bgp-af)#     network 3.3.3.3/32
ESR(config-bgp-af)#   exit
ESR(config-bgp)#   enable
ESR(config-bgp)# exit
```

12.14 MPLS over GRE

В этом разделе приведен пример настройки VPN сервисов, построенных через GRE-туннель.

12.14.1 L2VPN

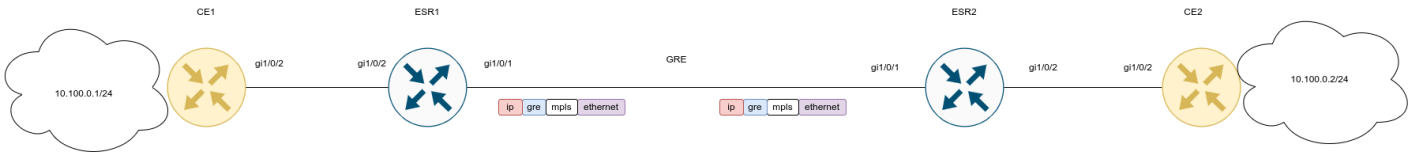
В качестве сервиса l2vpn произведем настройку EoMPLS over GRE. Также возможно построение VPLS over GRE (BGP или LDP signaling).

⚠ При настройке MTU на туннеле необходимо учитывать следующее:

- По крайней мере одна mpls-метка будет присутствовать при передаче через туннель. В учет стоит включать все метки в стеке, например, explicit null или entropy label;
- Необходимо учитывать vlan, q-in-q заголовки (если они имеются);
- При превышении MTU исходящего интерфейса пакет будет отброшен (если не включена безусловная фрагментация GRE-трафика);
- Control world не поддержан;
- DF-бит будет выставлен в единицу.

Ниже представлена примерная структура пакета:





Настройки CE1 и CE2:

CE1

```
hostname CE1

interface gigabitethernet 1/0/2
  ip firewall disable
  ip address 10.100.0.1/24
exit
```

CE2

```
hostname CE2

interface gigabitethernet 1/0/2
  ip firewall disable
  ip address 10.100.0.2/24
exit
```

Конфигурация ESR1 и ESR2:

ESR1

```
ESR1(config)# hostname ESR1
ESR1(config)#
ESR1(config)# system cpu load-balance mpls passenger ip
ESR1(config)# system cpu load-balance mpls passenger ipoe-pw-without-cw
ESR1(config)# security zone trusted
ESR1(config-zone)# exit
ESR1(config)# security zone untrusted
ESR1(config-zone)# exit
ESR1(config)#
ESR1(config)# router ospf 1
ESR1(config-ospf)#   area 0.0.0.0
ESR1(config-ospf-area)#     enable
ESR1(config-ospf-area)#   exit
ESR1(config-ospf)#   enable
ESR1(config-ospf)# exit
ESR1(config)#
ESR1(config)# interface gigabitethernet 1/0/1
ESR1(config-if-gi)#   security-zone untrusted
ESR1(config-if-gi)#   ip address 192.0.2.1/30
ESR1(config-if-gi)# exit
ESR1(config)# interface gigabitethernet 1/0/2
ESR1(config-if-gi)#   description "From CE1"
ESR1(config-if-gi)#   mode switchport
ESR1(config-if-gi)# exit
ESR1(config)# interface loopback 1
ESR1(config-loopback)#   ip address 10.100.0.1/32
ESR1(config-loopback)#   ip ospf instance 1
ESR1(config-loopback)#   ip ospf
ESR1(config-loopback)# exit
ESR1(config)# tunnel gre 1
ESR1(config-gre)#   key 60
ESR1(config-gre)#   ttl 64
ESR1(config-gre)#   mtu 1458
ESR1(config-gre)#   ip firewall disable
ESR1(config-gre)#   local address 192.0.2.1
ESR1(config-gre)#   remote address 192.0.2.2
ESR1(config-gre)#   ip address 10.0.0.1/30
ESR1(config-gre)#   ip ospf instance 1
ESR1(config-gre)#   ip ospf network point-to-point
ESR1(config-gre)#   ip ospf
ESR1(config-gre)#   enable
ESR1(config-gre)# exit
ESR1(config)#
ESR1(config)# mpls
ESR1(config-mpls)#   ldp
ESR1(config-ldp)#     router-id 10.100.0.1
ESR1(config-ldp)#     address-family ipv4
ESR1(config-ldp-af-ipv4)#       interface gre 1
ESR1(config-ldp-af-ipv4-if)#       exit
ESR1(config-ldp-af-ipv4)#     exit
ESR1(config-ldp)#     enable
ESR1(config-ldp)#   exit
ESR1(config-mpls)#   l2vpn
ESR1(config-l2vpn)#     pw-class VPWS
ESR1(config-l2vpn-pw-class)#     exit
ESR1(config-l2vpn)#     p2p EoMPLS
ESR1(config-l2vpn-p2p)#       interface gigabitethernet 1/0/2
```

```
ESR1(config-l2vpn-p2p)#       pw 100 10.100.0.2
ESR1(config-l2vpn-pw)#         pw-class VPWS
ESR1(config-l2vpn-pw)#         enable
ESR1(config-l2vpn-pw)#       exit
ESR1(config-l2vpn-p2p)#       enable
ESR1(config-l2vpn-p2p)#     exit
ESR1(config-l2vpn)#   exit
ESR1(config-mpls)#   forwarding interface gre 1
ESR1(config-mpls)# exit
ESR1(config)# security zone-pair untrusted self
ESR1(config-zone-pair)#   rule 1
ESR1(config-zone-pair-rule)#     action permit
ESR1(config-zone-pair-rule)#     match protocol gre
ESR1(config-zone-pair-rule)#     enable
ESR1(config-zone-pair-rule)#   exit
ESR1(config-zone-pair)# exit
ESR1(config)# do com
ESR1(config)# do conf
```

ESR2

```
ESR2(config)# hostname ESR2
ESR2(config)#
ESR2(config)# system cpu load-balance mpls passenger ip
ESR2(config)# system cpu load-balance mpls passenger ipoe-pw-without-cw
ESR2(config)# security zone trusted
ESR2(config-zone)# exit
ESR2(config)# security zone untrusted
ESR2(config-zone)# exit
ESR2(config)#
ESR2(config)# router ospf 1
ESR2(config-ospf)#   area 0.0.0.0
ESR2(config-ospf-area)#     enable
ESR2(config-ospf-area)#   exit
ESR2(config-ospf)#   enable
ESR2(config-ospf)# exit
ESR2(config)#
ESR2(config)# interface gigabitethernet 1/0/1
ESR2(config-if-gi)#   security-zone untrusted
ESR2(config-if-gi)#   ip address 192.0.2.2/30
ESR2(config-if-gi)# exit
ESR2(config)# interface gigabitethernet 1/0/2
ESR2(config-if-gi)#   description "From CE2"
ESR2(config-if-gi)#   mode switchport
ESR2(config-if-gi)# exit
ESR2(config)# interface loopback 1
ESR2(config-loopback)#   ip address 10.100.0.2/32
ESR2(config-loopback)#   ip ospf instance 1
ESR2(config-loopback)#   ip ospf
ESR2(config-loopback)# exit
ESR2(config)# tunnel gre 1
ESR2(config-gre)#   key 60
ESR2(config-gre)#   ttl 64
ESR2(config-gre)#   mtu 1458
ESR2(config-gre)#   ip firewall disable
ESR2(config-gre)#   local address 192.0.2.2
ESR2(config-gre)#   remote address 192.0.2.1
ESR2(config-gre)#   ip address 10.0.0.2/30
ESR2(config-gre)#   ip ospf instance 1
ESR2(config-gre)#   ip ospf network point-to-point
ESR2(config-gre)#   ip ospf
ESR2(config-gre)#   enable
ESR2(config-gre)# exit
ESR2(config)#
ESR2(config)# mpls
ESR2(config-mpls)#   ldp
ESR2(config-ldp)#     router-id 10.100.0.2
ESR2(config-ldp)#     address-family ipv4
ESR2(config-ldp-af-ipv4)#       interface gre 1
ESR2(config-ldp-af-ipv4-if)#       exit
ESR2(config-ldp-af-ipv4)#     exit
ESR2(config-ldp)#     enable
ESR2(config-ldp)#   exit
ESR2(config-mpls)#   l2vpn
ESR2(config-l2vpn)#     pw-class VPWS
ESR2(config-l2vpn-pw-class)#     exit
ESR2(config-l2vpn)#     p2p EoMPLS
ESR2(config-l2vpn-p2p)#       interface gigabitethernet 1/0/2
```

```
ESR2(config-l2vpn-p2p)#       pw 100 10.100.0.1
ESR2(config-l2vpn-pw)#         pw-class VPWS
ESR2(config-l2vpn-pw)#         enable
ESR2(config-l2vpn-pw)#       exit
ESR2(config-l2vpn-p2p)#       enable
ESR2(config-l2vpn-p2p)#     exit
ESR2(config-l2vpn)#   exit
ESR2(config-mpls)#   forwarding interface gre 1
ESR2(config-mpls)# exit
ESR2(config)# security zone-pair untrusted self
ESR2(config-zone-pair)#   rule 1
ESR2(config-zone-pair-rule)#     action deny
ESR2(config-zone-pair-rule)#     match protocol gre
ESR2(config-zone-pair-rule)#     enable
ESR2(config-zone-pair-rule)#   exit
ESR2(config-zone-pair)# exit
ESR2(config)# do com
ESR2(config)# do conf
```

Проверим состояние сервиса и доступность узлов:

```
* Конфигурация туннеля*
ESR2# sh tunnels configuration gre 1
State:                                                Enabled
Description:                                          --
Mode:                                                 ip
Bridge group:                                         --
VRF:                                                  --
Local address:                                        192.0.2.2
Remote address:                                       192.0.2.1
Calculates checksums for outgoing GRE packets:        No
Requires that all input GRE packets were checksum:    No
key:                                                  60
TTL:                                                  64
DSCP:                                                 Inherit
MTU:                                                  1458
Path MTU discovery:                                   Enabled
Don't fragment bit suppression:                       Disabled
Security zone:                                        --
Multipoint mode:                                      Disabled
Keepalive:
    State:                                                Disabled
    Timeout:                                              10
    Retries:                                              6
    Destination address:                                  --

*Статус сервиса и выделенные метки*
sh mpls l2vpn p2p
P2P: EoMPLS
    gigabitethernet 1/0/2:
        MTU:    1500
        Status: Up
    PW ID 100, Neighbor 10.100.0.1:
        MTU:         1500
        Status TLV:  Enable
        Last change: 00:14:27
        Status:      Up

ESR2# sh mpls forwarding-table
Local    Outgoing Prefix                                    Outgoing         Next Hop
label    label    or tunnel ID                              Interface
-------- -------- ------------------------------------------ ----------------
----------------------------------------
17       imp-null 10.100.0.1/32                              gre 1            10.0.0.1
16       16       PW ID 100                                  --               10.100.0.1

*Доступность*CE1# ping 10.100.0.2 detailed
PING 10.100.0.2 (10.100.0.2) 56 bytes of data.
64 bytes from 10.100.0.2: icmp_seq=1 ttl=0 time=1.38 ms
64 bytes from 10.100.0.2: icmp_seq=2 ttl=0 time=1.22 ms
64 bytes from 10.100.0.2: icmp_seq=3 ttl=0 time=1.33 ms
64 bytes from 10.100.0.2: icmp_seq=4 ttl=0 time=1.26 ms
64 bytes from 10.100.0.2: icmp_seq=5 ttl=0 time=1.17 ms
```

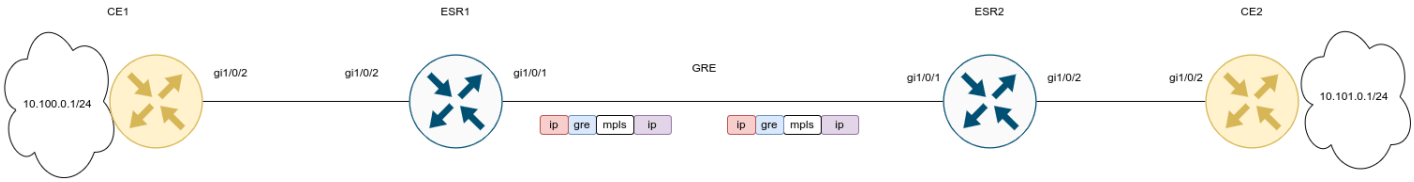
12.14.2 L3VPN

При настройке MTU на туннеле необходимо учитывать следующее:

- По крайне мере одна mpls-метка будет присутствовать при передаче через туннель. В учет стоит включать все метки в стеке, например, explicit null и/или entropy label;
- При превышении MTU исходящего интерфейса пакет будет отброшен (если не включена безусловная фрагментация GRE-трафика);
- Control world не поддержан;
- DF-бит будет выставлен в единицу.

Ниже представлена примерная структура пакета:





Настройки CE1 и CE2:

CE1

```
CE1(config)# hostname CE1
CE1(config)#
CE1(config)# route-map BGP_OUT
CE1(config-route-map)#   rule 1
CE1(config-route-map-rule)#   exit
CE1(config-route-map)# exit
CE1(config)# router bgp 65501
CE1(config-bgp)#   neighbor 10.10.0.2
CE1(config-bgp-neighbor)#     remote-as 65500
CE1(config-bgp-neighbor)#     address-family ipv4 unicast
CE1(config-bgp-neighbor-af)#       route-map BGP_OUT out
CE1(config-bgp-neighbor-af)#       enable
CE1(config-bgp-neighbor-af)#     exit
CE1(config-bgp-neighbor)#     enable
CE1(config-bgp-neighbor)#   exit
CE1(config-bgp)#   address-family ipv4 unicast
CE1(config-bgp-af)#     network 10.100.0.0/24
CE1(config-bgp-af)#   exit
CE1(config-bgp)#   enable
CE1(config-bgp)# exit
CE1(config)#
CE1(config)#
CE1(config)# interface gigabitethernet 1/0/2
CE1(config-if-gi)#   description "to ESR1"
CE1(config-if-gi)#   ip firewall disable
CE1(config-if-gi)#   ip address 10.10.0.1/30
CE1(config-if-gi)# exit
CE1(config)# interface loopback 1
CE1(config-loopback)#   ip address 10.100.0.1/24
CE1(config-loopback)# exit
```

CE2

```
CE2(config)# hostname CE2
CE2(config)#
CE2(config)# route-map BGP_OUT
CE2(config-route-map)#   rule 1
CE2(config-route-map-rule)#   exit
CE2(config-route-map)# exit
CE2(config)# router bgp 65502
CE2(config-bgp)#   neighbor 10.10.0.5
CE2(config-bgp-neighbor)#     remote-as 65500
CE2(config-bgp-neighbor)#     address-family ipv4 unicast
CE2(config-bgp-neighbor-af)#       route-map BGP_OUT out
CE2(config-bgp-neighbor-af)#       enable
CE2(config-bgp-neighbor-af)#     exit
CE2(config-bgp-neighbor)#     enable
CE2(config-bgp-neighbor)#   exit
CE2(config-bgp)#   address-family ipv4 unicast
CE2(config-bgp-af)#     network 10.101.0.0/24
CE2(config-bgp-af)#   exit
CE2(config-bgp)#   enable
CE2(config-bgp)# exit
CE2(config)#
CE2(config)#
CE2(config)# interface gigabitethernet 1/0/2
CE2(config-if-gi)#   description "to ESR2"
CE2(config-if-gi)#   ip firewall disable
CE2(config-if-gi)#   ip address 10.10.0.6/30
CE2(config-if-gi)# exit
CE2(config)# interface loopback 1
CE2(config-loopback)#   ip address 10.101.0.1/24
CE2(config-loopback)# exit
```

Конфигурация ESR1 и ESR2:

ESR1

```
ESR1(config)# hostname ESR1
ESR1(config)#
ESR1(config)# ip vrf l3vpn_service
ESR1(config-vrf)#   ip protocols bgp max-routes 100
ESR1(config-vrf)#   rd 65500:1
ESR1(config-vrf)#   route-target export 65500:1
ESR1(config-vrf)#   route-target import 65500:1
ESR1(config-vrf)# exit
ESR1(config)#
ESR1(config)#
ESR1(config)# system cpu load-balance mpls passenger ip
ESR1(config)# security zone untrusted
ESR1(config-zone)# exit
ESR1(config)# security zone trusted
ESR1(config-zone)# exit
ESR1(config)#
ESR1(config)# route-map BGP_OUT
ESR1(config-route-map)#   rule 1
ESR1(config-route-map-rule)#   exit
ESR1(config-route-map)# exit
ESR1(config)# router bgp 65500
ESR1(config-bgp)#   router-id 10.12.0.1
ESR1(config-bgp)#   neighbor 10.12.0.2
ESR1(config-bgp-neighbor)#     remote-as 65500
ESR1(config-bgp-neighbor)#     update-source 10.12.0.1
ESR1(config-bgp-neighbor)#     address-family vpnv4 unicast
ESR1(config-bgp-neighbor-af)#       send-community extended
ESR1(config-bgp-neighbor-af)#       enable
ESR1(config-bgp-neighbor-af)#     exit
ESR1(config-bgp-neighbor)#     enable
ESR1(config-bgp-neighbor)#   exit
ESR1(config-bgp)#   enable
ESR1(config-bgp)#   vrf l3vpn_service
ESR1(config-bgp-vrf)#     neighbor 10.10.0.1
ESR1(config-bgp-vrf-neighbor)#       remote-as 65501
ESR1(config-bgp-vrf-neighbor)#       address-family ipv4 unicast
ESR1(config-bgp-neighbor-af-vrf)#         route-map BGP_OUT out
ESR1(config-bgp-neighbor-af-vrf)#         enable
ESR1(config-bgp-neighbor-af-vrf)#       exit
ESR1(config-bgp-vrf-neighbor)#       enable
ESR1(config-bgp-vrf-neighbor)#     exit
ESR1(config-bgp-vrf)#     address-family ipv4 unicast
ESR1(config-bgp-vrf-af)#       redistribute bgp 65500 route-map BGP_OUT
ESR1(config-bgp-vrf-af)#     exit
ESR1(config-bgp-vrf)#     enable
ESR1(config-bgp-vrf)#   exit
ESR1(config-bgp)# exit
ESR1(config)#
ESR1(config)# router ospf 1
ESR1(config-ospf)#   router-id 10.12.0.1
ESR1(config-ospf)#   area 0.0.0.0
ESR1(config-ospf-area)#     enable
ESR1(config-ospf-area)#   exit
ESR1(config-ospf)#   enable
ESR1(config-ospf)# exit
ESR1(config)#
ESR1(config)# interface gigabitethernet 1/0/1
```

```
ESR1(config-if-gi)#   security-zone untrusted
ESR1(config-if-gi)#   ip address 192.0.2.1/30
ESR1(config-if-gi)# exit
ESR1(config)# interface gigabitethernet 1/0/2
ESR1(config-if-gi)#   ip vrf forwarding l3vpn_service
ESR1(config-if-gi)#   description "from CE1"
ESR1(config-if-gi)#   ip firewall disable
ESR1(config-if-gi)#   ip address 10.10.0.2/30
ESR1(config-if-gi)# exit
ESR1(config)# interface loopback 1
ESR1(config-loopback)#   ip address 10.12.0.1/32
ESR1(config-loopback)#   ip ospf instance 1
ESR1(config-loopback)#   ip ospf
ESR1(config-loopback)# exit
ESR1(config)# tunnel gre 1
ESR1(config-gre)#   key 60
ESR1(config-gre)#   ttl 64
ESR1(config-gre)#   mtu 1472
ESR1(config-gre)#   ip firewall disable
ESR1(config-gre)#   local address 192.0.2.1
ESR1(config-gre)#   remote address 192.0.2.2
ESR1(config-gre)#   ip address 10.11.0.1/30
ESR1(config-gre)#   ip ospf instance 1
ESR1(config-gre)#   ip ospf
ESR1(config-gre)#   enable
ESR1(config-gre)# exit
ESR1(config)#
ESR1(config)# mpls
ESR1(config-mpls)#   ldp
ESR1(config-ldp)#    router-id 10.12.0.1
ESR1(config-ldp)#    address-family ipv4
ESR1(config-ldp-af-ipv4)#       interface gre 1
ESR1(config-ldp-af-ipv4-if)#       exit
ESR1(config-ldp-af-ipv4)#    exit
ESR1(config-ldp)#    enable
ESR1(config-ldp)#   exit
ESR1(config-mpls)#   forwarding interface gre 1
ESR1(config-mpls)# exit
ESR1(config)# security zone-pair untrusted self
ESR1(config-zone-pair)#   rule 1
ESR1(config-zone-pair-rule)#    action permit
ESR1(config-zone-pair-rule)#    match protocol gre
ESR1(config-zone-pair-rule)#    enable
ESR1(config-zone-pair-rule)#   exit
ESR1(config-zone-pair)# exit
```

```
ESR2(config)# hostname ESR2
ESR2(config)#
ESR2(config)# ip vrf l3vpn_service
ESR2(config-vrf)#   ip protocols bgp max-routes 100
ESR2(config-vrf)#   rd 65500:1
ESR2(config-vrf)#   route-target export 65500:1
ESR2(config-vrf)#   route-target import 65500:1
ESR2(config-vrf)# exit
ESR2(config)#
ESR2(config)#
ESR2(config)# system cpu load-balance mpls passenger ip
ESR2(config)# security zone untrusted
ESR2(config-zone)# exit
ESR2(config)# security zone trusted
ESR2(config-zone)# exit
ESR2(config)#
ESR2(config)# route-map BGP_OUT
ESR2(config-route-map)#   rule 1
ESR2(config-route-map-rule)#   exit
ESR2(config-route-map)# exit
ESR2(config)# router bgp 65500
ESR2(config-bgp)#   router-id 10.12.0.2
ESR2(config-bgp)#   neighbor 10.12.0.1
ESR2(config-bgp-neighbor)#     remote-as 65500
ESR2(config-bgp-neighbor)#     update-source 10.12.0.2
ESR2(config-bgp-neighbor)#     address-family vpnv4 unicast
ESR2(config-bgp-neighbor-af)#       send-community extended
ESR2(config-bgp-neighbor-af)#       enable
ESR2(config-bgp-neighbor-af)#     exit
ESR2(config-bgp-neighbor)#     enable
ESR2(config-bgp-neighbor)#   exit
ESR2(config-bgp)#   enable
ESR2(config-bgp)#   vrf l3vpn_service
ESR2(config-bgp-vrf)#     neighbor 10.10.0.6
ESR2(config-bgp-vrf-neighbor)#       remote-as 65502
ESR2(config-bgp-vrf-neighbor)#       address-family ipv4 unicast
ESR2(config-bgp-neighbor-af-vrf)#         route-map BGP_OUT out
ESR2(config-bgp-neighbor-af-vrf)#         enable
ESR2(config-bgp-neighbor-af-vrf)#       exit
ESR2(config-bgp-vrf-neighbor)#       enable
ESR2(config-bgp-vrf-neighbor)#     exit
ESR2(config-bgp-vrf)#     address-family ipv4 unicast
ESR2(config-bgp-vrf-af)#       redistribute bgp 65500 route-map BGP_OUT
ESR2(config-bgp-vrf-af)#     exit
ESR2(config-bgp-vrf)#     enable
ESR2(config-bgp-vrf)#   exit
ESR2(config-bgp)# exit
ESR2(config)#
ESR2(config)# router ospf 1
ESR2(config-ospf)#   router-id 10.12.0.2
ESR2(config-ospf)#   area 0.0.0.0
ESR2(config-ospf-area)#     enable
ESR2(config-ospf-area)#   exit
ESR2(config-ospf)#   enable
ESR2(config-ospf)# exit
ESR2(config)#
ESR2(config)# interface gigabitethernet 1/0/1
ESR2(config-if-gi)#   security-zone untrusted
ESR2(config-if-gi)#   ip address 192.0.2.2/30
```

```
ESR2(config-if-gi)# exit
ESR2(config)# interface gigabitethernet 1/0/2
ESR2(config-if-gi)#   ip vrf forwarding l3vpn_service
ESR2(config-if-gi)#   description "from CE2"
ESR2(config-if-gi)#   ip firewall disable
ESR2(config-if-gi)#   ip address 10.10.0.5/30
ESR2(config-if-gi)# exit
ESR2(config)# interface loopback 1
ESR2(config-loopback)#   ip address 10.12.0.2/32
ESR2(config-loopback)#   ip ospf instance 1
ESR2(config-loopback)#   ip ospf
ESR2(config-loopback)# exit
ESR2(config)# tunnel gre 1
ESR2(config-gre)#   key 60
ESR2(config-gre)#   ttl 64
ESR2(config-gre)#   mtu 1472
ESR2(config-gre)#   ip firewall disable
ESR2(config-gre)#   local address 192.0.2.2
ESR2(config-gre)#   remote address 192.0.2.1
ESR2(config-gre)#   ip address 10.11.0.2/30
ESR2(config-gre)#   ip ospf instance 1
ESR2(config-gre)#   ip ospf
ESR2(config-gre)#   enable
ESR2(config-gre)# exit
ESR2(config)#
ESR2(config)# mpls
ESR2(config-mpls)#   ldp
ESR2(config-ldp)#     router-id 10.12.0.2
ESR2(config-ldp)#     address-family ipv4
ESR2(config-ldp-af-ipv4)#       interface gre 1
ESR2(config-ldp-af-ipv4-if)#       exit
ESR2(config-ldp-af-ipv4)#     exit
ESR2(config-ldp)#     enable
ESR2(config-ldp)#   exit
ESR2(config-mpls)#   forwarding interface gre 1
ESR2(config-mpls)# exit
ESR2(config)# security zone-pair untrusted self
ESR2(config-zone-pair)#   rule 1
ESR2(config-zone-pair-rule)#     action permit
ESR2(config-zone-pair-rule)#     match protocol gre
ESR2(config-zone-pair-rule)#     enable
ESR2(config-zone-pair-rule)#   exit
ESR2(config-zone-pair)# exit
```

После завершения настройки проверим статус сервиса и доступность узлов в сети:

```
*Конфигурация туннеля GRE*
ESR2# sh tunnels configuration
Tunnel             State      Description
----------------   --------   ------------------------------
gre 1              Enabled    --

ESR2# sh tunnels configuration gre 1
State:                                              Enabled
Description:                                        --
Mode:                                               ip
Bridge group:                                       --
VRF:                                                --
Local address:                                      192.0.2.2
Remote address:                                     192.0.2.1
Calculates checksums for outgoing GRE packets:      No
Requires that all input GRE packets were checksum: No
key:                                                60
TTL:                                                64
DSCP:                                               Inherit
MTU:                                                1472
Path MTU discovery:                                 Enabled
Don't fragment bit suppression:                     Disabled
Security zone:                                      --
Multipoint mode:                                    Disabled
Keepalive:
    State:                                              Disabled
    Timeout:                                            10
    Retries:                                            6
    Destination address:                                --

*Наличие vpnv4-маршрутов*
SR2# sh bgp vpnv4 unicast all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes Route Distinguisher   IP Prefix          Next hop        Metric     Label   LocPrf
Weight Path
----- --------------------- ------------------ --------------- ---------- ------- ----------
------ ----------------
*>    65500:1               10.101.0.0/24      --              --         34      100        --
65502 i
*>i   65500:1               10.100.0.0/24      10.12.0.1       --         16      100        0
65501 i

*Состояние протокола LDP*
ESR2# sh mpls ldp neighbor
Peer LDP ID: 10.12.0.1; Local LDP ID 10.12.0.2
    State:                  Operational
    TCP connection:         10.12.0.1:646 - 10.12.0.2:46444
    Messages sent/received: 60/60
    Uptime:                 00:53:59
    LDP discovery sources:
        gre 1
ESR2# sh mpls forwarding-table
Local    Outgoing Prefix                                    Outgoing         Next Hop
label    label    or tunnel ID                              Interface
-------- -------- ------------------------------------------ ----------------
---------------------------------------
35       imp-null 10.12.0.1/32                               gre 1            10.11.0.1
```

```
*Доступность узлов в сети*
CE2# ping 10.100.0.1 source ip 10.101.0.1 detailed
PING 10.100.0.1 (10.100.0.1) from 10.101.0.1 : 56 bytes of data.
64 bytes from 10.100.0.1: icmp_seq=1 ttl=0 time=1.32 ms
64 bytes from 10.100.0.1: icmp_seq=2 ttl=0 time=1.12 ms
64 bytes from 10.100.0.1: icmp_seq=3 ttl=0 time=1.14 ms
64 bytes from 10.100.0.1: icmp_seq=4 ttl=0 time=1.09 ms
64 bytes from 10.100.0.1: icmp_seq=5 ttl=0 time=1.15 ms
```

13 Управление безопасностью

- Настройка AAA
  - Алгоритм настройки локальной аутентификации
  - Алгоритм настройки AAA по протоколу RADIUS
  - Алгоритм настройки AAA по протоколу TACACS
  - Алгоритм настройки AAA по протоколу LDAP
  - Пример настройки аутентификации по Telnet через RADIUS-сервер
- Настройка привилегий команд
  - Алгоритм настройки
  - Пример настройки привилегий команд
- Настройка логирования и защиты от ARP-spoofing атак
  - Алгоритм настройки
  - Пример настройки защиты от ARP-spoofing атак
- Настройка логирования и защиты от сетевых атак
  - Алгоритм настройки
  - Описание механизмов защиты от атак
  - Пример настройки логирования и защиты от сетевых атак
- Конфигурирование Firewall
  - Алгоритм настройки
  - Пример настройки Firewall
  - Пример настройки Firewall по доменным именам
  - Пример настройки фильтрации приложений (DPI)
  - Пример настройки Firewall по расписанию
- Настройка списков доступа (IP ACL)
  - Алгоритм настройки
  - Пример настройки списка доступа
- Настройка списков доступа (MAC ACL)
  - Алгоритм настройки
  - Пример настройки списка доступа
- Проксирование HTTP/HTTPS-трафика
  - Алгоритм настройки
  - Пример настройки HTTP-прокси
- Настройка IPS/IDS
  - Алгоритм базовой настройки
  - Алгоритм настройки автообновления правил IPS/IDS из внешних источников
  - Рекомендуемые открытые источники обновления правил
    - SSL Blacklist
    - Feodo Tracker
    - Travis Green
    - Etnetera Core
  - Пример настройки IPS/IDS с автообновлением правил
  - Алгоритм настройки базовых пользовательских правил
  - Пример настройки базовых пользовательских правил
  - Алгоритм настройки расширенных пользовательских правил
  - Пример настройки расширенных пользовательских правил
- Настройка взаимодействия с Eltex Distribution Manager
  - Алгоритм базовой настройки
  - Пример настройки
- Настройка сервиса контентной фильтрации
  - Алгоритм базовой настройки
  - Пример настройки правил контентной фильтрации

13.1 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.

13.1.1 Алгоритм настройки локальной аутентификации

Шаг	Описание	Команда	Ключи
1	Задать список методов аутентификации по умолчанию (default)/с именем <NAME> и указать local.	**esr(config)# aaa authentication login { default | <NAME> } <METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]**	<NAME> – имя списка, задаётся строкой до 31 символа. Способы аутентификации: • local – аутентификация с помощью локальной базы пользователей; • tacacs – аутентификация по списку TACACS-серверов; • radius – аутентификация по списку RADIUS-серверов; • ldap – аутентификация по списку LDAP-серверов.
2	Задать список методов аутентификации повышения привилегий пользователей по умолчанию (default)/с именем <NAME> и указать enable.	**esr(config)# aaa authentication enable <NAME><METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]**	<NAME> – имя списка, задаётся строкой до 31 символа. Способы аутентификации: • local – аутентификация с помощью локальной базы пользователей; • tacacs – аутентификация по списку TACACS-серверов; • radius – аутентификация по списку RADIUS-серверов; • ldap – аутентификация по списку LDAP-серверов.

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

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

Шаг	Описание	Команда	Ключи
14	Установить минимальное количество специальных символов в пароле локального пользователя и ENABLE-пароле (необязательно).	**esr(config)# security passwords special-case <COUNT>**	<COUNT> – минимальное количество специальных символов в пароле. Принимает значение в диапазоне [0..128]. Значение по умолчанию: 0.
15	Добавить пользователя в локальную базу и перейти в режим настройки параметров пользователя.	**esr(config)# username <NAME>**	<NAME> – имя пользователя, задаётся строкой до 31 символа.
16	Установить пароль пользователя.	**esr(config-user)# password { <CLEAR-TEXT> | encrypted <HASH_SHA512> }**	<CLEAR-TEXT> – пароль, задаётся строкой [8 .. 32] символов, принимает значения [0-9a-fA-F]; <HASH_SHA512> – хеш пароля по алгоритму sha512, задаётся строкой из 110 символов.
17	Установить уровень привилегий пользователя.	**esr(config-user)# privilege <PRIV>**	<PRIV> – необходимый уровень привилегий. Принимает значение [1..15].

Шаг	Описание	Команда	Ключи
18	Установить режим работы учетной записи пользователя (необязательно).	**esr(config-user)# mode <MODE>**	<MODE> – режим работы учетной записи пользователя. Может принимать значения: • cli – режим работы по умолчанию, пользователь получает доступ к интерфейсу командной строки, предназначенному для управления, просмотра состояния и мониторинга устройства; • techsupport – пользователь получает доступ к командной оболочке, в которой выполняется процедура отладки устройства совместно с специалистами технической поддержки; • sftp – пользователь используется для организации доступа к встроенному SFTP-серверу, возможность работы в какой-либо командой оболочке при этом у пользователя отсутствует.

Шаг	Описание	Команда	Ключи
19	Указать метод аутентификации SSH-сессий для пользователя (необязательно).	**esr(config-user)# ssh authentication method <METHOD>**	<METHOD> – метод аутентификации SSH-сессий. Может принимать значения: • password – аутентификация пользователя при открытии SSH-сессий может быть произведена только по паролю; • pubkey – аутентификация пользователя при открытии SSH-сессий может быть произведена только по публичному ключу; • both – аутентификация пользователя при открытии SSH-сессий может быть произведена как по паролю, так и по публичному ключу.
20	Указать имя файла публичного ключа, который будет использован при аутентификации SSH-сессии пользователя (необязательно).	**esr(config-user)# ssh pubkey <NAME>**	<NAME> – имя файла публичного ключа, расположенного в разделе crypto:public-key, задаётся строкой до 31 символа.
21	Отключить авторизацию для предустановленного пользователя admin (необязательно).	**esr(config)# no admin login enable**	
22	Перейти в режим конфигурирования соответствующего терминала.	**esr(config)# line <TYPE>**	<TYPE> – тип консоли: • console – локальная консоль; • telnet – удаленная консоль; • ssh – защищенная удаленная консоль.
23	Активировать список аутентификации входа пользователей в систему.	**esr(config-line-console)# login authentication <NAME>**	<NAME> – имя списка, задаётся строкой до 31 символа. Создан на шаге 1.
24	Активировать список аутентификации повышения привилегий пользователей.	**esr(config-line-console)# enable authentication <NAME>**	<NAME> – имя списка, задаётся строкой до 31 символа. Создан на шаге 2.

Шаг	Описание	Команда	Ключи
25	Задать интервал, по истечении которого будет разрываться бездействующая сессия.	**esr(config-line-console)# exec-timeout <SEC>**	<SEC> – период времени в минутах, принимает значения [1..65535].

13.1.2 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 (необязательно).	**esr(config)# radius-server dscp <DSCP>**	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 63.
2	Задать глобальное значение количества перезапросов к последнему активному RADIUS-серверу (необязательно).	**esr(config)# radius-server retransmit <COUNT>**	<COUNT> – количество перезапросов к RADIUS-серверу, принимает значения [1..10]. Значение по умолчанию: 1.
3	Задать глобальное значение интервала, по истечении которого маршрутизатор считает, что RADIUS-сервер недоступен (необязательно).	**esr(config)# radius-server timeout <SEC>**	<SEC> – период времени в секундах, принимает значения [1..30]. Значение по умолчанию: 3 секунды.
4	Добавить RADIUS-сервер в список используемых серверов и перейти в режим его конфигурирования.	**esr(config)# radius-server host { <IP-ADDR> | <IPV6-ADDR> } [vrf <VRF>]**	<IP-ADDR> – IP-адрес RADIUS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> – IPv6-адрес RADIUS-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF] <VRF> – имя экземпляра VRF, задается строкой до 31 символа.
5	Задать описание конфигурируемого RADIUS-сервера (необязательно).	**esr(config-radius-server)# description <description>**	<description> – описание RADIUS-сервера, задается строкой до 255 символов.

Шаг	Описание	Команда	Ключи
6	Указать количество неудачных попыток аутентификации для блокировки логина пользователя и времени блокировки (необязательно).	**esr(config-radius-server)# aaa authentication attempts max-fail <COUNT> <TIME>**	<COUNT> – количество неудачных попыток аутентификации, после которых произойдет блокировка пользователя, принимает значения [1..65535]; <TIME> – интервал времени в секундах, на который будет заблокирован пользователь, принимает значения [1..65535]. Значение по умолчанию: <COUNT> – 5; <TIME> – 300.
7	Задать пароль для аутентификации на удаленном RADIUS-сервере.	**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.
8	Задать приоритет использования удаленного RADIUS-сервера (необязательно).	**esr(config-radius-server)# priority <PRIORITY>**	<PRIORITY> – приоритет использования удаленного сервера, принимает значения [1..65535]. Чем ниже значение, тем приоритетнее сервер. Значение по умолчанию: 1.
9	Задать интервал, по истечении которого маршрутизатор считает, что данный RADIUS-сервер недоступен (необязательно).	**esr(config-radius-server)# timeout <SEC>**	<SEC> – период времени в секундах, принимает значения [1..30]. Значение по умолчанию: используется значение глобального таймера.
10	Задать IPv4/IPv6-адрес, который будет использоваться в качестве IPv4/IPv6-адреса источника в отправляемых RADIUS-пакетах.	**esr(config-radius-server)# source-address { <ADDR> | object-group <NETWORK_OBJ_GROUP_NAME> }**	<ADDR> – IP-адрес источника, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве source address.

Шаг	Описание	Команда	Ключи
11	Задать интерфейс или туннель маршрутизатора, IPv4/IPv6-адрес которого будет использоваться в качестве IPv4/IPv6-адреса источника в отправляемых RADIUS-пакетах.	**esr(config-radius-server)# source-interface { <IF> | <TUN> }**	<IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора; <TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора.
12	Задать список методов аутентификации по умолчанию (default)/с именем <NAME> и указать radius.	**esr(config)# aaa authentication login { default | <NAME> } <METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]**	<NAME> – имя списка, задаётся строкой до 31 символа. Способы аутентификации: • local – аутентификация с помощью локальной базы пользователей; • tacacs – аутентификация по списку TACACS-серверов; • radius – аутентификация по списку RADIUS-серверов; • ldap – аутентификация по списку LDAP-серверов.
13	Задать список методов аутентификации повышения привилегий пользователей по умолчанию (default)/с именем <NAME> и указать radius.	**esr(config)# aaa authentication enable <NAME><METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]**	<NAME> – имя списка строка до 31 символа; • default – имя списка по умолчанию. <METHOD> – способы аутентификации: • enable – аутентификация с помощью enable-паролей; • tacacs – аутентификация по протоколу TACACS; • radius – аутентификация по протоколу RADIUS; • ldap – аутентификация по протоколу LDAP.

Шаг	Описание	Команда	Ключи
14	Указать способ перебора методов аутентификации в случае отказа (необязательно).	**esr(config)# aaa authentication mode <MODE>**	<MODE> – способы перебора методов: • chain – если сервер вернул FAIL, переход к следующему в цепочке методу аутентификации; • break – если сервер вернул FAIL, прекратить попытки аутентификации. Если сервер недоступен, продолжить попытки аутентификации следующими в цепочке методами. Значение по умолчанию: chain.
15	Сконфигурировать RADIUS в списке способов учета сессий пользователей (необязательно).	**esr(config)# aaa accounting login start-stop <METHOD 1> [<METHOD 2>]**	<METHOD> – способы учета: • tacacs – учет сессий по протоколу TACACS; • radius – учет сессий по протоколу RADIUS.
16	Перейти в режим конфигурирования соответствующего терминала.	**esr(config)# line <TYPE>**	<TYPE> – тип консоли: • console – локальная консоль; • telnet – удаленная консоль; • ssh – защищенная удаленная консоль.
17	Активировать список аутентификации входа пользователей в систему.	**esr(config-line-console)# login authentication <NAME>**	<NAME> – имя списка, задаётся строкой до 31 символа. Создан на шаге 12.
18	Активировать список аутентификации повышения привилегий пользователей.	**esr(config-line-console)# enable authentication <NAME>**	<NAME> – имя списка, задаётся строкой до 31 символа. Создан на шаге 13.

13.1.3 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 (необязательно).	**esr(config)# tacacs-server dscp <DSCP>**	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 63.

Шаг	Описание	Команда	Ключи
2	Задать глобальное значение интервала, по истечении которого маршрутизатор считает, что TACACS-сервер недоступен (необязательно).	**esr(config)# tacacs-server timeout <SEC>**	<SEC> – период времени в секундах, принимает значения [1..30]. Значение по умолчанию: 3 секунды.
3	Добавить TACACS-сервер в список используемых серверов и перейти в режим его конфигурирования.	**esr(config)# tacacs -server host { <IP-ADDR> | <IPV6-ADDR> } [vrf <VRF>]**	<IP-ADDR> – IP-адрес TACACS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255] <IPV6-ADDR> – IPv6-адрес TACACS -сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF] <VRF> – имя экземпляра VRF, задается строкой до 31 символа.
4	Задать описание конфигурируемого TACACS-сервера (необязательно).	**esr(config-tacacs-server)# description <description>**	<description> – описание TACACS-сервера, задается строкой до 255 символов.
5	Указать количество неудачных попыток аутентификации для блокировки логина пользователя и время блокировки (необязательно)	**esr(config-tacacs-server)# aaa authentication attempts max-fail <COUNT> <TIME>**	<COUNT> – количество неудачных попыток аутентификации, после которых произойдет блокировка пользователя, принимает значения [1..65535]; <TIME> – интервал времени в минутах, на который будет заблокирован пользователь, принимает значения [1..65535]. Значение по умолчанию: <COUNT> – 5; <TIME> – 300.
6	Задать пароль для аутентификации на удаленном TACACS-сервере	**esr(config-tacacs-server)# key ascii-text { <TEXT> | encrypted <ENCRYPTED-TEXT> }**	<TEXT> – строка [8..16] ASCII-символов; <ENCRYPTED-TEXT> – зашифрованный пароль, размером [8..16] байт, задаётся строкой [16..32] символов.

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

Шаг	Описание	Команда	Ключи
11	Задать список методов аутентификации по умолчанию (default)/с именем <NAME> и указать tacacs.	**esr(config)# aaa authentication login { default | <NAME> } <METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]**	<NAME> – имя списка, задаётся строкой до 31 символа. Способы аутентификации: • local – аутентификация с помощью локальной базы пользователей; • tacacs – аутентификация по списку TACACS-серверов; • radius – аутентификация по списку RADIUS-серверов; • ldap – аутентификация по списку LDAP-серверов.
12	Задать список методов аутентификации повышения привилегий пользователей по умолчанию (default)/с именем <NAME> и указать tacacs.	**esr(config)# aaa authentication enable <NAME><METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]**	<NAME> – имя списка строка до 31 символа; • default – имя списка по умолчанию. <METHOD> – способы аутентификации: • enable – аутентификация с помощью enable-паролей; • tacacs – аутентификация по протоколу TACACS; • radius – аутентификация по протоколу RADIUS; • ldap – аутентификация по протоколу LDAP.
13	Задать список методов авторизации команд, вводимых пользователем в систему по умолчанию (default)/с именем <NAME> и указать tacacs.	**esr(config)# aaa authorization commands { default | <NAME> } <METHOD 1>[<METHOD 2>]**	<NAME> – имя списка, задаётся строкой до 31 символа. Способы аутентификации: local – авторизация с помощью локальной базы пользователей; tacacs – авторизация по списку TACACS-серверов;

Шаг	Описание	Команда	Ключи
14	Указать способ перебора методов аутентификации в случае отказа (необязательно).	**esr(config)# aaa authentication mode <MODE>**	<MODE> – способы перебора методов: • chain – если сервер вернул FAIL, переход к следующему в цепочке методу аутентификации; • break – если сервер вернул FAIL, прекратить попытки аутентификации. Если сервер недоступен, продолжить попытки аутентификации следующими в цепочке методами. Значение по умолчанию: chain.
15	Сконфигурировать список способов учета команд, введённых в CLI (необязательно).	**esr(config)# aaa accounting commands stop-only <METHOD>**	<METHOD> – способы учета: tacacs – учет введенных команд по протоколу TACACS.
16	Сконфигурировать tacacs в списке способов учета сессий пользователей (необязательно).	**esr(config)# aaa accounting login start-stop <METHOD 1> [<METHOD 2>]**	<METHOD> – способы учета: • tacacs – учет сессий по протоколу TACACS; • radius – учет сессий по протоколу RADIUS.
17	Перейти в режим конфигурирования соответствующего терминала.	**esr(config)# line <TYPE>**	<TYPE> – тип консоли: • console – локальная консоль; • telnet – удаленная консоль; • ssh – защищенная удаленная консоль.
18	Активировать список аутентификации входа пользователей в систему.	**esr(config-line-console)# login authentication <NAME>**	<NAME> – имя списка, задаётся строкой до 31 символа. Создан на шаге 11.
19	Активировать список аутентификации повышения привилегий пользователей.	**esr(config-line-console)# enable authentication <NAME>**	<NAME> – имя списка, задаётся строкой до 31 символа. Создан на шаге 12.
20	Активировать список авторизации команд вводимых пользователем в систему.	**esr(config-line-console)# commands authorization <NAME>**	<NAME> – имя списка, задаётся строкой до 31 символа. Создан на шаге 13.

13.1.4 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 (необязательно).	**esr(config)# ldap-server bind timeout <SEC>**	<SEC> – период времени в секундах, принимает значения [1..30]. Значение по умолчанию: 3 секунды.
3	Задать DN (Distinguished name) пользователя с правами администратора, под которым будет происходить авторизация на LDAP-сервере при поиске пользователей.	**esr(config)# ldap-server bind authenticate root-dn <NAME>**	<NAME> – DN пользователя с правами администратора, задается строкой до 255 символов.
4	Задать пароль пользователя с правами администратора, под которым будет происходить авторизация на LDAP-сервере при поиске пользователей.	**esr(config)# ldap-server bind authenticate root-password ascii-text { <TEXT> | encrypted <ENCRYPTED-TEXT> }**	<TEXT> – строка [8..16] ASCII-символов; <ENCRYPTED-TEXT> – зашифрованный пароль, размером [8..16] байт, задаётся строкой [16..32] символов.
5	Задать имя класса объектов, среди которых необходимо выполнять поиск пользователей на LDAP-сервере (необязательно).	**esr(config)# ldap-server search filter user-object-class <NAME>**	<NAME> – имя класса объектов, задаётся строкой до 127 символов. Значение по умолчанию: posixAccount.
6	Задать область поиска пользователей в дереве LDAP-сервера (необязательно).	**esr(config)# ldap-server search scope <SCOPE>**	<SCOPE> – область поиска пользователей на LDAP-сервере, принимает следующие значения: • onelevel – выполнять поиск в объектах на следующем уровне после базового DN в дереве LDAP-сервера; • subtree – выполнять поиск во всех объектах поддерева базового DN в дереве LDAP-сервера. Значение по умолчанию: subtree.

Шаг	Описание	Команда	Ключи
7	Задать интервал, по истечении которого устройство считает, что LDAP-сервер не нашел записей пользователей, подходящих под условие поиска (необязательно).	**esr(config)# ldap-server search timeout <SEC>**	<SEC> – период времени в секундах, принимает значения [0..30] Значение по умолчанию: 0 – устройство ожидает завершения поиска и получения ответа от LDAP-сервера.
8	Задать имя атрибута объекта, со значением которого идет сравнение имени искомого пользователя на LDAP-сервере (необязательно).	**esr(config)# ldap-server naming-attribute <NAME>**	<NAME> – имя атрибута объекта, задаётся строкой до 127 символов. Значение по умолчанию: uid.
9	Задать имя атрибута объекта, значение которого будет определять начальные привилегии пользователя на устройстве (необязательно).	**esr(config)# ldap-server privilege-level-attribute <NAME>**	<NAME> – имя атрибута объекта, задаётся строкой до 127 символов. Значение по умолчанию: priv-lvl.
10	Задать глобальное значение кода DSCP для использования в IP-заголовках исходящих пакетов LDAP-сервера (необязательно).	**esr(config)# ldap-server dscp <DSCP>**	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 63.
11	Добавить LDAP-сервер в список используемых серверов и перейти в режим его конфигурирования.	**esr(config)# ldap-server host { <IP-ADDR> | <IPV6-ADDR> } [vrf <VRF>]**	<IP-ADDR> – IP-адрес LDAP-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255] <IPV6-ADDR> – IPv6-адрес LDAP-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF] <VRF> – имя экземпляра VRF, задается строкой до 31 символа.
12	Задать описание конфигурируемого LDAP-сервера (необязательно).	**esr(config-ldap-server)# description <description>**	<description> – описание LDAP-сервера, задается строкой до 255 символов.

Шаг	Описание	Команда	Ключи
13	Указать количество неудачных попыток аутентификации для блокировки логина пользователя и время блокировки (необязательно).	**esr(config-ldap-server)# aaa authentication attempts max-fail <COUNT> <TIME>**	<COUNT> – количество неудачных попыток аутентификации, после которых произойдет блокировка пользователя, принимает значения [1..65535]; <TIME> – интервал времени в минутах, на который будет заблокирован пользователь, принимает значения [1..65535]. Значение по умолчанию: <COUNT> – 5; <TIME> – 300.
14	Задать номер порта для обмена данными с удаленным LDAP-сервером (необязательно).	**esr(config-ldap-server)# port <PORT>**	<PORT> – номер TCP-порта для обмена данными с удаленным сервером, принимает значения [1..65535]. Значение по умолчанию: 389 для LDAP-сервера.
15	Задать приоритет использования удаленного LDAP-сервера (необязательно).	**esr(config-ldap-server)# priority <PRIORITY>**	<PRIORITY> – приоритет использования удаленного сервера, принимает значения [1..65535]. Чем ниже значение, тем приоритетнее сервер. Значение по умолчанию: 1.
16	Задать IPv4/IPv6-адрес, который будет использоваться в качестве IP/IPv6-адреса источника в отправляемых LDAP-пакетах.	**esr(config-ldap-server)# source-address { <ADDR> | object-group <NETWORK_OBJ_GROUP_NAME> }**	<ADDR> – IP-адрес источника, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве source address.

Шаг	Описание	Команда	Ключи
17	Задать интерфейс или туннель маршрутизатора, IPv4/IPv6-адрес которого будет использоваться в качестве IPv4/IPv6-адреса источника в отправляемых LDAP-пакетах.	**esr(config-ldap-server)# source-interface { <IF> | <TUN> }**	<IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора; <TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора.
18	Задать список методов аутентификации по умолчанию (default)/с именем <NAME> и указать ldap.	**esr(config)# aaa authentication login { default | <NAME> } <METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]**	<NAME> – имя списка, задаётся строкой до 31 символа. Способы аутентификации: • local – аутентификация с помощью локальной базы пользователей; • tacacs – аутентификация по списку TACACS-серверов; • radius – аутентификация по списку RADIUS-серверов; • ldap – аутентификация по списку LDAP-серверов.
19	Задать список методов аутентификации повышения привилегий пользователей по умолчанию (default)/с именем <NAME> и указать ldap.	**esr(config)# aaa authentication enable <NAME> <METHOD 1> [<METHOD 2>] [<METHOD 3>] [<METHOD 4>]**	<NAME> – имя списка строка до 31 символа; • default – имя списка по умолчанию. <METHOD> – способы аутентификации: • enable – аутентификация с помощью enable-паролей; • tacacs – аутентификация по протоколу TACACS; • radius – аутентификация по протоколу RADIUS; • ldap – аутентификация по протоколу LDAP.

Шаг	Описание	Команда	Ключи
20	Указать способ перебора методов аутентификации в случае отказа.	**esr(config)# aaa authentication mode <MODE>**	<MODE> – способы перебора методов: • chain – если сервер вернул FAIL, переход к следующему в цепочке методу аутентификации; • break – если сервер вернул FAIL, прекратить попытки аутентификации. Если сервер недоступен, продолжить попытки аутентификации следующими в цепочке методами. Значение по умолчанию: chain.
21	Перейти в режим конфигурирования соответствующего терминала.	**esr(config)# line <TYPE>**	<TYPE> – тип консоли: • console – локальная консоль; • telnet – удаленная консоль; • ssh – защищенная удаленная консоль.
22	Активировать список аутентификации входа пользователей в систему.	**esr(config-line-console)# login authentication <NAME>**	<NAME> – имя списка, задаётся строкой до 31 символа. Создан на шаге 17.
23	Активировать список аутентификации повышения привилегий пользователей.	**esr(config-line-console)# enable authentication <NAME>**	<NAME> – имя списка, задаётся строкой до 31 символа. Создан на шаге 18.

13.1.5 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
```

13.2 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.

13.2.1 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.

13.2.2 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"
```

13.3 Настройка логирования и защиты от ARP-spoofing атак

13.3.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Включить защиту от ARP-spoofing атак на сетевом интерфейсе/сетевом мосту.	**esr(config-if-gi)# ip arp inspection**	
2	Включить логирование отброшенных ARP-ответов (необязательно).	**esr(config)# logging firewall arp-inspection**	

13.3.2 Пример настройки защиты от ARP-spoofing атак

Задача:

Необходимо защитить LAN-сеть и маршрутизатор ESR от ARP-spoofing атак и настроить логирование об атаках на удаленный syslog-сервер.



Решение:

Настраиваем интерфейсы и включем на них защиту от ARP-spoofing атак:

```
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# ip address 10.0.0.1/24
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 192.168.0.1/24
esr(config-if-gi)# ip arp inspection
esr(config-if-gi)# exit
```

Настраиваем параметры удаленного syslog-сервера:

```
esr(config)# syslog host SYSLOG_SERVER
esr(config-syslog-host)# remote-address 192.168.0.10
esr(config-syslog-host)# severity info
esr(config-syslog-host)# exit
```

Включаем логирование об ARP-spoofing атаках:

```
esr(config)# logging firewall arp-inspection
```

Просмотреть счетчики заблокированных ARP-ответов:

```
esr# show ip firewall arp-inspections
Interface              Count
--------------------   --------------------
gi1/0/1                9
```

Сбросить счетчики заблокированных ARP-ответов:

```
esr# clear ip firewall arp-inspections counters
```

Уведомление об ARP-spoofing атаке на удаленном syslog-сервере:

```
2025-11-24T12:29:01+07:00 esr firewalld %FIREWALL-W-EVENT_WARN: arp-inspection
a8:f9:4b:ac:4d:3e(192.168.0.12) -> 50:75:bd:04:fd:00(192.168.0.1) denied (gi1/0/1
 a8:f9:4b:ac:4d:3e)
```

13.4 Настройка логирования и защиты от сетевых атак

13.4.1 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].

Шаг	Описание	Команда	Ключи
2	Включить защиту от land-атак.	**esr(config)# firewall screen dos-defense land**	
3	Включить ограничение числа пакетов, отправляемых за одну секунду на один адрес назначения	**esr(config)# ip firewall screen dos-defense limit-session-destination { <NUM> }**	<NUM> – ограничение числа IP-пакетов в секунду, задается в диапазоне [1..10000].
4	Включить ограничение числа пакетов, отправляемых за одну секунду с единого адреса источника	**esr(config)# ip firewall screen dos-defense limit-session-source { <NUM> }**	<NUM> – ограничение числа IP-пакетов в секунду, задается в диапазоне [1..10000].
5	Включить защиту от SYN flood-атак.	**esr(config)# ip firewall screen dos-defense syn-flood { <NUM> } [src-dsr]**	<NUM> – максимальное количество TCP-пакетов с установленным флагом SYN в секунду, задается в диапазоне [1..10000]. src-dst – ограничение количества TCP-пакетов с установленным флагом SYN на основании адреса источника и адреса назначения.
6	Включить защиту от UDP flood-атак.	**esr(config)# ip firewall screen dos-defense udp-threshold { <NUM> }**	<NUM> – максимальное количество UDP-пакетов в секунду, задается в диапазоне [1..10000].
7	Включить защиту от winnuke-атак.	**esr(config)# ip firewall screen dos-defense winnuke**	
8	Включить защиту от zero-port-атак	**esr(config)# ip firewall screen dos-defense zero-port**	
9	Включить блокировку TCP-пакетов с установленным флагом FIN и не установленным флагом ACK.	**esr(config)# ip firewall screen spy-blocking fin-no-ack**	
10	Включить блокировку ICMP-пакетов различных типов.	**esr(config)# ip firewall screen spy-blocking icmp-type**	<TYPE> – тип ICMP, может принимать значения: • destination-unreachable • echo-request • reserved • source-quench • time-exceeded

Шаг	Описание	Команда	Ключи
11	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].
12	Включить защиту от port scan-атак.	**esr(config)# ip firewall screen spy-blocking port-scan { <threshold> } [<TIME>]**	<threshold> – интервал в секундах, в течение которого будет фиксироваться port scan-атака [1..10000]. <TIME> – время блокировки в миллисекундах [1..1000000].
13	Включить защиту от IP spoofing-атак.	**esr(config)# ip firewall screen spy-blocking spoofing**	
14	Исключить из защиты от IP-spoofing атак указанную Object Group.	**esr(config)# ip firewall screen spy-blocking spoofing exclude <object-group>**	<object-group> – список разрешённых для spoofing подсетей.
15	Включить блокировку TCP-пакетов, с установленными флагами SYN и FIN.	**esr(config)# ip firewall screen spy-blocking syn-fin**	
16	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**	
17	Включить блокировку TCP-пакетов, с нулевым полем flags.	**esr(config)# ip firewall screen spy-blocking tcp-no-flag**	
18	Включить блокировку фрагментированных ICMP-пакетов.	**esr(config)# ip firewall screen suspicious-packets icmp-fragment**	
19	Включить блокировку фрагментированных IP-пакетов.	**esr(config)# ip firewall screen suspicious-packets ip-fragment**	
20	Включить блокировку ICMP-пакетов длиной более 1024 байт.	**esr(config)# ip firewall screen suspicious-packets icmp-fragment**	
21	Включить блокировку фрагментированных TCP-пакетов, с флагом SYN.	**esr(config)# ip firewall screen suspicious-packets syn-fragment**	
22	Включить блокировку фрагментированных UDP-пакетов.	**esr(config)# ip firewall screen suspicious-packets udp-fragment**	

Шаг	Описание	Команда	Ключи
23	Включить блокировку пакетов, с ID протокола в заголовке IP равном 137 и более.	**esr(config)# ip firewall screen suspicious-packets unknown-protocols**	
24	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].
25	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.
26	Включить механизм обнаружения и логирования шпионской активности через CLI, Syslog и по SNMP.	**esr(config)# logging firewall screen spy-blocking { <ATACK_TYPE> | icmp-type <ICMP_TYPE> }**	<ATACK_TYPE> – тип шпионской активности, принимает значения: fin-no-ack, ip-sweep, port-scan, spoofing, syn-fin, tcp-all-flag, tcp-no-flag. <ICMP_TYPE> – тип ICMP, принимает значения: destination-unreachable, echo-request, reserved, source-quench, time-exceeded.
27	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.

13.4.2 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 source-адреса. 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 DoS-атаках: SYN flood, UDP flood, ICMP flood, и т.д.). Команда включает ограничение числа пакетов, передаваемых за секунду на один адреса назначения, которое смягчает DoS-атаки.
ip firewall screen dos-defense limit-session-source	Когда таблица IP-сессий хоста переполняется, он больше не в состоянии организовывать новые сессии и отбрасывает запросы (такое может происходить при различных DoS-атаках: SYN flood, UDP flood, ICMP flood, и т.д.). Команда включает ограничение числа пакетов, передаваемых за секунду с одного адреса источника, которое смягчает DoS-атаки.
ip firewall screen dos-defense syn-flood	Данная команда включает защиту от SYN flood-атак. При включенной защите ограничивается количество TCP-пакетов с установленным флагом SYN в секунду для одного адреса назначения. Атака приводит к перегрузке хоста и выводу его из строя из-за необходимости обрабатывать каждый TCP SYN пакет и попыток установить TCP-сессии.
ip firewall screen dos-defense udp-threshold	Данная команда включает защиту от UDP flood-атак. При включенной защите ограничивается количество UDP-пакетов в секунду для одного адреса назначения. Атака приводит к перегрузке хоста и выводу его из строя из-за массивного UDP-трафика.
ip firewall screen dos-defense winnuke	Данная команда включает защиту от winnuke-атак. При включенной защите блокируются TCP-пакеты с установленным флагом URG и 139 портом назначения. Атака приводит к выходу из строя старых версий Windows (до 95 версии).
ip firewall screen dos-defense zero-port	Данная команда включает защиту от zero-port-атак. При включенной защите блокируются TCP/UDP-пакеты с установленным портом источника/назначения равным нулю.
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.

Команда	Описание
ip firewall screen spy-blocking icmp-type source-quench	Данная команда включает блокировку всех ICMP-пакетов 4 типа (source quench), включая пакеты, сгенерированные самим маршрутизатором. Защита не дает злоумышленнику узнать о топологии сети и доступности хостов.
ip firewall screen spy-blocking icmp-type time-exceeded	Данная команда включает блокировку всех ICMP-пакетов 11 типа (time exceeded), включая пакеты, сгенерированные самим маршрутизатором. Защита не дает злоумышленнику узнать о топологии сети и доступности хостов.
ip firewall screen spy-blocking ip-sweep	Данная команда включает защиту от IP sweep-атак. При включенной защите, если в течение заданного в параметрах интервала приходит более 10 ICMP-запросов от одного источника, первые 10 запросов пропускаются маршрутизатором, а 11 и последующие отбрасываются на оставшееся время интервала. Защита не дает злоумышленнику узнать о топологии сети и доступности хостов.
ip firewall screen spy-blocking port-scan	Данная команда включает защиту от port scan-атак. Если в течение первого заданного интервала времени (<threshold>) на один источник приходит более 10 TCP-пакетов с флагом SYN на разные TCP-порты или более 10 UDP-пакетов на разные UDP-порты, то такое поведение фиксируется как port scan-атака, и все последующие пакеты такого рода от источника блокируются на второй заданный интервал времени (<TIME>). Злоумышленник не сможет быстро просканировать открытые порты на устройстве.
ip firewall screen spy-blocking spoofing	Данная команда включает защиту от ip spoofing-атак. При включенной защите маршрутизатор проверяет пакеты на соответствие адреса источника и записей в таблице маршрутизации, и в случае несоответствия пакет отбрасывается. Например, если пакет с адресом источника 10.0.0.1/24 приходит на интерфейс Gi1/0/1, а в таблице маршрутизации данная подсеть располагается за интерфейсом Gi1/0/2, то считается, что адрес источника был подменен. Защищает от вторжений в сеть с подмененными source IP-адресами.
ip firewall screen spy-blocking spoofing exclude <object-group>	Данная команда исключает из защиты от IP-spoofing атак указанную Object Group. В Object Group помещается список из допустимых адресов, которые будут игнорироваться. Команда используется вместе с основной ip firewall screen spy-blocking spoofing, которая включает защиту, иначе она не будет иметь эффекта. В случае, если на маршрутизатор приходит spoofing от разрешённых подсетей (например, частый опрос устройств в сети), пакеты пропускаются.
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.

Команда	Описание
ip firewall screen spy-blocking tcp-no-flag	Данная команда включает блокировку TCP-пакетов с нулевым полем flags. Такие пакеты являются нестандартными, и по ответу можно определить операционную систему жертвы.
ip firewall screen suspicious-packets icmp-fragment	Данная команда включает блокировку фрагментированных ICMP-пакетов. ICMP-пакеты обычно небольшого размера и необходимости в их фрагментировании нет.
ip firewall screen suspicious-packets ip-fragment	Данная команда включает блокировку фрагментированных пакетов.
ip firewall screen suspicious-packets large-icmp	Данная команда включает блокировку ICMP-пакетов длиной более 1024 байт.
ip firewall screen suspicious-packets syn-fragment	Данная команда включает блокировку фрагментированных TCP-пакетов с флагом SYN. TCP-пакеты с SYN-флагом обычно небольшого размера и необходимости в их фрагментировании нет. Защита предотвращает накопление фрагментированных пакетов в буфере.
ip firewall screen suspicious-packets udp-fragment	Данная команда включает блокировку фрагментированных UDP-пакетов.
ip firewall screen suspicious-packets unknown-protocols	Данная команда включает блокировку пакетов, с ID протокола в заголовке IP равном 137 и более.

13.4.3 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-security-zone)# exit
esr(config)# security zone WAN
esr(config-security-zone)# exit
esr(config)# security zone-pair LAN WAN
esr(config-security-zone-pair)# rule 100
esr(config-security-zone-pair-rule)# action permit
esr(config-security-zone-pair-rule)# enable
esr(config-security-zone-pair-rule)# exit
esr(config-security-zone-pair)# exit
esr(config)# security zone-pair WAN LAN
esr(config-security-zone-pair)# rule 100
esr(config-security-zone-pair-rule)# action permit
esr(config-security-zone-pair-rule)# enable
esr(config-security-zone-pair-rule)# exit
esr(config-security-zone-pair)# exit
esr(config)# exit
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# security-zone LAN
esr(config-if-gi)# ip address 192.168.0.1/24
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# security-zone WAN
esr(config-if-gi)# ip address 10.0.0.1/24
esr(config-if-gi)# exit
```

Настроим защиту от land, syn-flood, ICMP flood-атак:

```
esr(config)# ip firewall screen dos-defense land
esr(config)# ip firewall screen dos-defense syn-flood 100 src-dst
esr(config)# ip firewall screen dos-defense icmp-threshold 100
```

Настроим логирование обнаруженных атак:

```
esr(config)# logging firewall screen dos-defense land
esr(config)# logging firewall screen dos-defense syn-flood
esr(config)# logging firewall screen dos-defense icmp-threshold
```

Настроим SNMP-сервер, на который будут отправляться трапы:

```
esr(config)# snmp-server
esr(config)# snmp-server host 192.168.0.10
esr(config)# snmp-server enable traps screen land
esr(config)# snmp-server enable traps screen syn-flood
esr(config)# snmp-server enable traps screen icmp-threshold
```

Посмотреть статистику по зафиксированным сетевым атакам можно командой:

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

Очистить статистику по зафиксированным сетевым атакам можно командой:

```
esr# clear ip firewall screen counters
```

13.5 Конфигурирование Firewall

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

13.5.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать зоны безопасности.	**esr(config)# security zone <zone-name1>** **esr(config)# security zone <zone-name2>**	<zone-name> – до 12 символов. Имена all, any и self зарезервированы.
2	Задать описание зоны безопасности.	**esr(config-security-zone)# description <description>**	<description> – до 255 символов.
3	Указать экземпляр VRF, в котором будет работать данная зона безопасности (необязательно).	**esr(config- security-zone)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.
4	Включить счетчики сессий для NAT и Firewall (необязательно, снижает производительность).	**esr(config)# ip firewall sessions counters**	
5	Отключить фильтрацию пакетов, для которых не удалось определить принадлежность к какому-либо известному соединению и которые не являются началом нового соединения (необязательно, снижает производительность).	**esr(config)# ip firewall sessions unknown <ACTION>**	<ACTION> – правило обработки неизвестных сессий для межсетевого экрана: permit – разрешить неизвестные сессии; deny – отбрасывать неизвестные сессии; reject – отбрасывать неизвестные сессии и отправлять обратно пакет с ошибкой.

Шаг	Описание	Команда	Ключи
6	Выбрать режим работы межсетевого экрана (необязательно). В режиме stateful проверяется только первый пакет сессии, и если «прямой» трафик разрешён, «ответный» трафик разрешается автоматически. В режиме stateless происходит проверка каждого пакета. «Прямой» и «ответный» трафики требуется разрешать в соответствующих zone-pair (см. шаг 29). Работа межсетевого экрана по списку приложений возможна только в режиме stateless.	**esr(config)# ip firewall mode <MODE>**	<MODE> – режим работы межсетевого экрана, может принимать значения: stateful, stateless. Значение по умолчанию: stateful.
7	Определить время жизни сессии для неподдерживаемых протоколов (необязательно).	**esr(config)# ip firewall sessions generic-timeout <TIME>**	<TIME> – время жизни сессии для неподдерживаемых протоколов, принимает значения в секундах [1..8553600]. По умолчанию: 60 секунд.
8	Определить время жизни ICMP-сессии, по истечении которого она считается устаревшей (необязательно).	**esr(config)# ip firewall sessions icmp-timeout <TIME>**	<TIME> – время жизни ICMP-сессии, принимает значения в секундах [1..8553600]. По умолчанию: 30 секунд.
9	Определить время жизни ICMPv6-сессии, по истечении которого она считается устаревшей (необязательно).	**esr(config)# ip firewall sessions icmpv6-timeout <TIME>**	<TIME> – время жизни ICMP-сессии, принимает значения в секундах [1..8553600]. По умолчанию: 30 секунд.
10	Определить размер таблицы сессий, ожидающих обработки (необязательно).	**esr(config)# ip firewall sessions max-expect <COUNT>**	<COUNT> – размер таблицы, принимает значения [1..8553600]. По умолчанию: 256.
11	Определить размер таблицы отслеживаемых сессий (необязательно).	**esr(config)# ip firewall sessions max-tracking <COUNT>**	<COUNT> – размер таблицы, принимает значения [1..8553600]. По умолчанию: 512000.

Шаг	Описание	Команда	Ключи
12	Определить время жизни TCP-сессии в состоянии «соединение устанавливается», по истечении которого она считается устаревшей (необязательно).	**esr(config)# ip firewall sessions tcp-connect-timeout <TIME>**	<TIME> – время жизни TCP-сессии в состоянии «соединение устанавливается», принимает значения в секундах [1..8553600]. По умолчанию: 60 секунд.
13	Определить время жизни TCP-сессии в состоянии «соединение закрывается», по истечении которого она считается устаревшей (необязательно).	**esr(config)# ip firewall sessions tcp-disconnect-timeout <TIME>**	<TIME> – время жизни TCP-сессии в состоянии «соединение закрывается» принимает значения в секундах [1..8553600]. По умолчанию: 30 секунд.
14	Определить время жизни TCP-сессии в состоянии «соединение установлено», по истечении которого она считается устаревшей (необязательно).	**esr(config)# ip firewall sessions tcp-established-timeout <TIME>**	<TIME> – время жизни TCP-сессии в состоянии «соединение установлено», принимает значения в секундах [1..8553600]. По умолчанию: 120 секунд.
15	Определить время ожидания, по истечении которого происходит фактическое удаление закрытой TCP-сессии из таблицы отслеживаемых сессий (необязательно).	**esr(config)# ip firewall sessions tcp-latecome-timeout <TIME>**	<TIME> – время ожидания, принимает значения в секундах [1..8553600]. По умолчанию: 120 секунд.

Шаг	Описание	Команда	Ключи
16	Включить функцию отслеживания сессий уровня приложений для отдельных протоколов (необязательно).	**esr(config)# ip firewall sessions tracking**	<PROTOCOL> – протокол уровня приложений [ftp, h323, pptp, netbios-ns, tftp], сессии которого должны отслеживаться. <OBJECT-GROUP-SERVICE> – имя профиля TCP/UDP-портов sip-сессии, задаётся строкой до 31 символа. Если группа не указана, то отслеживание сессий sip будет осуществляться для порта 5060. Вместо имени отдельного протокола можно использовать ключ «all», который включает функцию отслеживания сессий уровня приложений для всех доступных протоколов. По умолчанию – отключено для всех протоколов.
17	Определить время жизни UDP-сессии в состоянии «соединение подтверждено», по истечении которого она считается устаревшей (необязательно).	**esr(config)# ip firewall sessions udp-assured-timeout <TIME>**	<TIME> – время жизни UDP-сессии в состоянии «соединение подтверждено», принимает значения в секундах [1..8553600]. По умолчанию: 180 секунд.
18	Определить время жизни UDP-сессии в состоянии «соединение не подтверждено», по истечении которого она считается устаревшей.	**esr(config)# ip firewall sessions udp-wait-timeout <TIME>**	<TIME> – время жизни UDP-сессии в состоянии «соединение не подтверждено», принимает значения в секундах [1..8553600]. По умолчанию: 30 секунд.
19	Создать списки MAC-адресов, которые будут использоваться при фильтрации.	**esr(config)# object-group mac <obj-group-name>**	<obj-group-name> – до 31 символа.
20	Задать описание списка MAC-адресов (необязательно).	**esr(config-object-group-mac)# description <description>**	<description> – описание профиля, задается строкой до 255 символов.

Шаг	Описание	Команда	Ключи
21	Внести необходимые MAC-адреса в список.	**esr(config-object-group-mac)# mac address <ADDR> <WILDCARD>**	<ADDR> – MAC-адрес, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]. <WILDCARD> – маска MAC-адреса, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]. Биты маски, установленные в 0, задают биты MAC-адреса, исключаемые из сравнения при поиске.
22	Создать списки IP-адресов, которые будут использоваться при фильтрации.	**esr(config)# object-group network <obj-group-name>**	<obj-group-name> – до 31 символа.
23	Задать описание списка IP-адресов (необязательно).	**esr(config-object-group-network)# description <description>**	<description> – описание профиля, задается строкой до 255 символов.
24	Внести необходимые IPv4/IPv6-адреса в список.	**esr(config-object-group-network)# ip prefix <ADDR/LEN> [unit <ID>]**	<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]. <ID> – номер юнита, принимает значения [1..4].
		esr(config-object-group-network)# ip address-range <FROM-ADDR>-<TO-ADDR> [unit <ID>]	<FROM-ADDR> – начальный IP-адрес диапазона адресов; <TO-ADDR> – конечный IP-адрес диапазона адресов, опциональный параметр. Если параметр не указан, то командой задаётся одиночный IP-адрес. Адреса задаются в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. <ID> – номер юнита, принимает значения [1..4].

Шаг	Описание	Команда	Ключи
		esr(config-object-group-network)# ipv6 prefix <IPV6-ADDR/LEN> [unit <ID>]	<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]. <ID> – номер юнита, принимает значения [1..4].
		esr(config-object-group-network)# ipv6 address-range <FROM-ADDR>-<TO-ADDR> [unit <ID>]	<FROM-ADDR> – начальный IPv6-адрес диапазона адресов; <TO-ADDR> – конечный IPv6-адрес диапазона адресов, опциональный параметр. Если параметр не указан, то командой задаётся одиночный IPv6-адрес. Адреса задаются в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. <ID> – номер юнита, принимает значения [1..4].
25	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.
26	Задать описание списка сервисов (необязательно).	**esr(config-object-group-service)# description <description>**	<description> – описание профиля, задается строкой до 255 символов.
27	Внести необходимые сервисы (tcp/udp-порты) в список.	**esr(config-object-group-service)# port-range <port>**	<port> – принимает значение [1..65535]. Можно указать несколько портов перечислением через запятую «,» либо указать диапазон портов через «-».
28	Создать списки приложений, которые будут использоваться в механизме DPI.	**esr(config)# object-group application <NAME>**	<NAME> – имя профиля приложений, задается строкой до 31 символа.
29	Задать описание списка приложений (необязательно).	**esr(config-object-group-application)# description <description>**	<description> – описание профиля, задается строкой до 255 символов.

Шаг	Описание	Команда	Ключи
30	Внести необходимые приложения в списки.	**esr(config-object-group-application)# application < APPLICATION >**	<APPLICATION> – указывает приложение, попадающее под действие данного профиля.
31	Создать список доменных имен, которые будут использоваться при фильтрации.	**esr(config)# object-group domain-name <NAME>**	<NAME> – имя профиля доменных имен, задается строкой до 31 символа.
32	Задать описание списка доменных имен (необязательно).	**esr(config-object-group-domain-name)# description <description>**	<description> – описание профиля, задается строкой до 255 символов.
33	Внести необходимые доменные имена в списки.	**esr(config-object-group-domain-name)# domain <DOMAIN>**	<DOMAIN> – доменное имя, строка длинной от 1 до 253 символов.
34	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**	
	Отключить функции Firewall глобально на всех сетевых сущностях (если необходимо).	**esr(config)# ip firewall disable**	
35	Создать набор правил межзонового взаимодействия. На маршрутизаторе всегда существует зона безопасности с именем «self». Если в качестве получателя трафика выступает сам маршрутизатор, то есть трафик не является транзитным, то в качестве параметра указывается зона «self». Очерёдность обработки трафика для разных zone-pair описана в примечании.	**esr(config)# security zone-pair <src-zone-name1> <dst-zone-name2>**	<src-zone-name> – до 12 символов. <dst-zone-name> – до 12 символов.

Шаг	Описание	Команда	Ключи
36	Создать правило межзонового взаимодействия.	**esr(config-security-zone-pair)# rule <rule-number>**	<rule-number> – 1..10000.
37	Задать описание правила (необязательно).	**esr(config-security-zone-pair)# description <description>**	<description> – до 255 символов.
38	Указать действие данного правила.	**esr(config-security-zone-pair-rule)# action <action> [log]**	<action> – permit/deny/reject/ netflow-sample/sflow-sample/ rate-limit/session-limit ⚠ Ключ session-limit применим только на моделях ESR-30/ESR-31/ ESR-3100/ESR-3150/ ESR-3200/ESR-3200L/ ESR-3250/ ESR-3300/ ESR-3350. log – ключ для активации логирования сессий, устанавливающимися согласно данному правилу.
39	Установить имя или номер IP-протокола, для которого должно срабатывать правило (необязательно).	**esr(config-security-zone-pair-rule)# match [not] protocol <protocol-type>**	<protocol-type> – тип протокола, принимает значения: esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre. При указании значения «any» правило будет срабатывать для любых протоколов.
		esr(config-security-zone-pair-rule)# match [not] protocol-id <protocol-id>	<protocol-id> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF].

Шаг	Описание	Команда	Ключи
40	Установить IP-адрес отправителя, для которых должно срабатывать правило (необязательно).	**esr(config-security-zone-pair-rule)# match [not] source-address { address-range { <ADDR>[-<ADDR>] | <IPV6-ADDR>[-<IPV6-ADDR>] } | prefix { <ADDR/LEN> | <IPv6-ADDR/LEN> } | object-group { network <OBJ-GROUP-NETWORK-NAME> | domain-name <OBJ-GROUP-DOMAIN-NAME> } | any }**	**address-range** <ADDR>[-<ADDR>] – диапазон IP-адресов для правил firewall. Если не указывать IP-адрес конца диапазона, то в качестве IP-адреса для срабатывания правила используется только IP-адрес начала диапазона. Параметр задаётся в виде A.B.C.D, где каждая часть принимает значения [0..255]; <IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; **prefix** <ADDR/LEN> – IP-подсеть, используемая для срабатывания правила фильтрации firewall. Параметр задаётся в виде A.B.C.D/E, где каждая часть A – D принимает значения [0..255] и E принимает значения [1..32]; <IPv6-ADDR/LEN> – IPv6-адрес, задаётся в виде X:X:X:X::X/E, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и E принимает значения [1..128]; **object-group network** <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа; **object-group domain-name** <OBJ-GROUP-DOMAIN-NAME> – имя профиля доменных имен, задаётся строкой до 31 символа. При указании значения **any** правило будет срабатывать для любого IP-адреса получателя.
41	Установить IP-адрес получателя, для которых должно срабатывать правило (необязательно).	**esr(config-security-zone-pair-rule)# match [not] destination-address { address-range { <ADDR>[-<ADDR>] | <IPV6-ADDR>[-<IPV6-ADDR>] } | prefix { <ADDR/LEN> | <IPv6-ADDR/LEN> } | object-group { network <OBJ-GROUP-NETWORK-NAME> | domain-name <OBJ-GROUP-DOMAIN-NAME> } | any }**	

Шаг	Описание	Команда	Ключи
42	Установить MAC-адрес отправителя, для которого должно срабатывать правило (необязательно).	**esr(config-security-zone-pair-rule)# match [not] source-mac {<mac-addr> | <OBJ-GROUP-NAME>}**	<mac-addr> – задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]. <OBJ-GROUP-NAME> – имя профиля MAC-адресов, задаётся строкой до 31 символа.
43	Установить MAC-адрес получателя, для которого должно срабатывать правило (необязательно).	**esr(config-security-zone-pair-rule)# match [not] destination-mac {<mac-addr> | <OBJ-GROUP-NAME>}**	
44	Установить TCP/UDP-порт отправителя, для которого должно срабатывать правило (если указан протокол).	**esr(config-security-zone-pair-rule)# match [not] source-port <TYPE> {<PORT-SET-NAME> | <FROM-PORT> - <TO-PORT>}**	<TYPE> – тип аргумента, устанавливаемый в качестве порта: • **object-group** – указать имя профиля; • **port-range** – указать диапазон портов; • **any** – установить в качестве порта любой порт. <PORT-SET-NAME> – задаётся строкой до 31 символа; <FROM-PORT> – начальный порт диапазона; <TO-PORT> – конечный порт диапазона.
45	Установить TCP/UDP-порт получателя, для которого должно срабатывать правило (если указан протокол).	**esr(config-security-zone-pair-rule)# match [not] destination-port <TYPE> {<PORT-SET-NAME> | <FROM-PORT> - <TO-PORT>}**	
46	Установить профиль приложений, который будет использоваться в механизме DPI.	**esr(config-security-zone-pair-rule)# match [not] application <OBJ-GROUP-NAME>**	<OBJ-GROUP-NAME> – имя профиля приложений, задаётся строкой до 31 символа.
47	Установить тип и код сообщений протокола ICMP, для которых должно срабатывать правило (если в качестве протокола выбран ICMP) (необязательно).	**esr(config-security-zone-pair-rule)# match [not] icmp <ICMP_TYPE> <ICMP_CODE>**	<ICMP_TYPE> – тип сообщения протокола ICMP, принимает значения [0..255]; <ICMP_CODE> – код сообщения протокола ICMP, принимает значения [0..255]. При указании значения «any» правило будет срабатывать для любого кода сообщения протокола ICMP.

Шаг	Описание	Команда	Ключи
48	Установить тип и код сообщений протокола ICMPv6, для которых должно срабатывать правило (если в качестве протокола выбран ICMP) (необязательно).	**esr(config-security-zone-pair-rule)# match [not] icmpv6 <ICMP_TYPE> <ICMP_CODE>**	<ICMP_TYPE> – тип сообщения протокола ICMPv6, принимает значения [0..255]; <ICMP_CODE> – код сообщения протокола ICMPv6, принимает значения [0..255]. При указании значения «any» правило будет срабатывать для любого кода сообщения протокола ICMP.
49	Установить ограничение, при котором правило будет срабатывать только для трафика, измененного сервисом трансляции IP-адресов и портов получателя.	**esr(config-security-zone-pair-rule)# match [not] destination-nat**	
50	Установить фильтрацию только для фрагментированных IP-пакетов (необязательно, доступно только для zone-pair any self и zone-pair <zone-name> any).	**esr(config-security-zone-pair-rule)# match [not] fragment**	
51	Установить фильтрацию для IP-пакетов, содержащих ip-option (необязательно, доступно только для zone-pair any self и zone-pair <zone-name> any).	**esr(config-security-zone-pair-rule)# match [not] ip-option**	
52	Включить правило межзонового взаимодействия.	**esr(config-security-zone-pair-rule)# enable**	
53	Активировать фильтрацию и режим отслеживания сессий при прохождении пакетов между участниками одной Bridge-группы (необязательно).	**esr(config-bridge)# ports firewall enable**	
54	Добавить работу правила безопасности по расписанию.	**esr(config-security-zone-pair-rule)# scheduler <SCHEDULER>**	<SCHEDULER> – название существующего в конфигурации расписания.

Порядок обработки транзитного трафика правилами firewall

1. Трафик проверяется правилами zone-pair user-zone any.
   Если трафик не попал ни под одно из правил текущей zone-pair, переходим к следующему шагу.
   Разрешение трафика правилом в этой zone-pair не пропускает проверки следующих zone-pair.

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

Порядок обработки трафика, терминируемого на маршрутизаторе

1. Трафик проверяется правилами zone-pair any self.
   Если трафик не попал ни под одно из правил текущей zone-pair, переходим к следующему шагу.
   Разрешение трафика правилом в этой zone-pair не пропускает проверки следующих zone-pair.
2. Трафик проверяется правилами zone-pair user-zone self.
   Если трафик не попал ни под одно из правил текущей zone-pair, переходим к следующему шагу.
3. Трафик проверяется правилами zone-pair any any.
   Если трафик не попал ни под одно из правил текущей zone-pair, он отбрасывается.

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

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

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

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

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

На маршрутизаторе всегда существует зона безопасности с именем «self». Если в качестве получателя трафика выступает сам маршрутизатор, то есть трафик не является транзитным, то в качестве

параметра указывается зона «self». Создадим пару зон для трафика, идущего из зоны «WAN» в зону «self». Добавим правило, разрешающее проходить ICMP-трафику между R2 и маршрутизатором ESR, для того чтобы маршрутизатор начал отвечать на ICMP-запросы из зоны «WAN»:

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

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

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

13.5.3 Пример настройки Firewall по доменным именам

Задача:

Фиксировать обращения на ресурсы компании Yandex из локальной сети в Syslog:



Решение:

Создадим зоны безопасности для локальной сети и uplink-интерфейса в сторону интернет-провайдера:

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

Настроим маршрут по умолчанию в сторону интернет-провайдера:

```
esr(config)# ip route 0.0.0.0/0 10.0.0.254
```

Настроим систему разрешения доменных имен, её настройка необходима для работы Firewall по доменным именам:

```
esr(config)# domain lookup enable
esr(config)# domain nameserver 10.0.0.254
```

Настроим простую конфигурацию Source-NAT для любого транзитного через ESR трафика:

```
esr(config)# nat source
esr(config-snat)# ruleset SNAT
esr(config-snat-ruleset)# to zone WAN
esr(config-snat-ruleset)# rule 1
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
```

Создадим профиль доменных имен, включающий в себя популярные домены компании "Яндекс":

ESR также позволяет работать с интернационализованными доменными именами (домены, использующие символы национальных алфавитов). Для использования интернационализованного доменного имени в конфигурации ESR его нужно преобразовать к виду ASCII-compatible encoding при помощи любого Punycode-преобразователя. Т. е. получим:
яндекс.рф → xn--d1acpjx3f.xn--p1ai
президент.рф → xn--d1abbgf6aiiy.xn--p1ai
И уже ASCII-compatible encoding вариант доменного имени можно указывать в конфигурации ESR.

```
esr(config)# object-group domain-name YANDEX
esr(config-object-group-domain-name)# domain ya.ru
esr(config-object-group-domain-name)# domain yandex.ru
esr(config-object-group-domain-name)# domain dzen.ru
esr(config-object-group-domain-name)# domain xn--d1acpjx3f.xn--p1ai
esr(config-object-group-domain-name)# exit
```

Разрешим прохождение трафика из зоны «LAN» в зону «WAN» и отдельно создадим правило, которое будет фиксировать в Syslog обращения на домены компании "Яндекс":

```
esr(config)# security zone-pair LAN WAN
esr(config-security-zone-pair)# rule 1
esr(config-security-zone-pair-rule)# action permit log
esr(config-security-zone-pair-rule)# match destination-address object-group domain-name YANDEX
esr(config-security-zone-pair-rule)# enable
esr(config-security-zone-pair-rule)# exit
esr(config-security-zone-pair)# rule 2
esr(config-security-zone-pair-rule)# action permit
esr(config-security-zone-pair-rule)# enable
esr(config-security-zone-pair-rule)# exit
esr(config-security-zone-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
```

Посмотреть кэш DNS можно с помощью команд:

```
esr# show dns records
esr# show dns records negative
```

Пример сообщения Syslog при срабатывании правила:

```
<190>1 2025-07-07T17:40:10+07:00 esr firewalld - - - %FIREWALL-I-LOG: zone-pair 'LAN WAN' rule
1 permitted tcp 192.168.0.21:45574 (gi1/0/2) -> 77.88.44.55:443 dscp 48
```

13.5.4 Пример настройки фильтрации приложений (DPI)

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

Задача:

Блокировать доступ пользователей в локальной сети к Telegram, Facebook Messenger и Skype.



Решение:

Для каждой сети ESR создадим свою зону безопасности:

```
esr# configure
esr(config)# security zone LAN
esr(config-security-zone)# exit
esr(config)# security zone WAN
esr(config-security-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 BLACKLIST
esr(config-object-group-application)# application telegram
esr(config-object-group-application)# application facebook-messenger
esr(config-object-group-application)# application skype-teams
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-security-zone-pair)# rule 1
esr(config-security-zone-pair-rule)# action deny
esr(config-security-zone-pair-rule)# match application BLACKLIST
esr(config-security-zone-pair-rule)# enable
esr(config-security-zone-pair-rule)# exit
esr(config-security-zone-pair)# rule 2
esr(config-security-zone-pair-rule)# action permit
esr(config-security-zone-pair-rule)# enable
esr(config-security-zone-pair-rule)# exit
esr(config-security-zone-pair)# exit
```

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

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

13.5.5 Пример настройки Firewall по расписанию

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

Задача:

Блокировать доступ пользователей из локальной сети к YouTube в рабочее время, начиная с 1 января 2026 года.



Решение:

Создадим зоны безопасности для локальной сети и uplink-интерфейса в сторону интернет-провайдера:

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

Настроим маршрут по умолчанию в сторону интернет-провайдера:

```
esr(config)# ip route 0.0.0.0/0 10.0.0.254
```

Создадим расписание, по которому будет активироваться правило.

```
esr(config)# scheduler WORK_HOURS
esr(config-scheduler)# periodic weekdays
esr(config-scheduler-weekdays)# start-time 08:00:00 stop-time 12:00:00
esr(config-scheduler-weekdays)# start-time 13:00:00 stop-time 17:00:00
esr(config-scheduler-weekdays)# exit
esr(config-scheduler)# start-date 00:00:00 01 January 2026
esr(config-scheduler)# exit
```

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

```
esr(config)# object-group application BLACKLIST
esr(config-object-group-application)# application youtube
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-security-zone-pair)# rule 1
esr(config-security-zone-pair-rule)# action deny
esr(config-security-zone-pair-rule)# match application BLACKLIST
esr(config-security-zone-pair-rule)# scheduler WORK_HOURS
esr(config-security-zone-pair-rule)# enable
esr(config-security-zone-pair-rule)# exit
esr(config-security-zone-pair)# rule 2
esr(config-security-zone-pair-rule)# action permit
esr(config-security-zone-pair-rule)# enable
esr(config-security-zone-pair-rule)# exit
esr(config-security-zone-pair)# exit
```

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

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

13.6 Настройка списков доступа (IP ACL)

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

13.6.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать список контроля доступа и перейти в режим его конфигурирования.	**esr(config)# ip access-list extended <NAME>**	<NAME> – имя создаваемого списка контроля доступа, задаётся строкой до 31 символа.
2	Указать описание конфигурируемого списка контроля доступа (необязательно).	**esr(config-acl-ip)# description <DESCRIPTION>**	<DESCRIPTION> – описание списка контроля доступа, задаётся строкой до 255 символов.
3	Создать правило и перейти в режим его конфигурирования. Правила обрабатываются маршрутизатором в порядке возрастания их номеров.	**esr(config-acl-ip)# rule <ORDER>**	<ORDER> – номер правила, принимает значения [1...4094].

Шаг	Описание	Команда	Ключи
4	Указать действие, которое должно быть применено для трафика, удовлетворяющего заданным критериям.	**esr(config-acl-ip-rule)# action <ACT>**	<ACT> – назначаемое действие: • permit – прохождение трафика разрешается; • deny – прохождение трафика запрещается.
5	Установить имя/номер протокола, для которого должно срабатывать правило (необязательно).	**esr(config-acl-ip-rule)# match protocol <TYPE>**	<TYPE> – тип протокола, принимает значения: esp, icmp, icmp6, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rsvp, l2tp, gre. При указании значения «any» правило будет срабатывать для любых протоколов.
		esr(config-acl-ip-rule)# match protocol-id <ID>	<ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF].
6	Установить IP-адреса отправителя, для которых должно срабатывать правило (необязательно).	**esr(config-acl-ip-rule)# match source-address { <ADDR> <MASK> | any }**	<ADDR> – IP-адрес отправителя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <MASK> – маска IP-адреса, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Биты маски, установленные в 0, задают биты IP-адреса, исключаемые из сравнения при поиске. При указании значения «any» правило будет срабатывать для любого IP-адреса отправителя/получателя.
7	Установить IP-адреса получателя, для которых должно срабатывать правило (необязательно).	**esr(config-acl-ip-rule)# match destination-address { <ADDR> <MASK> | any }**	

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

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

Также списки доступа могут использоваться для организации политик QoS.

13.6.2 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-ip)# rule 1
esr(config-acl-ip-rule)# action permit
esr(config-acl-ip-rule)# match source-address 192.168.20.0 255.255.255.0
esr(config-acl-ip-rule)# enable
esr(config-acl-ip-rule)# exit
esr(config-acl-ip)# 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 ip input white
```

Просмотреть детальную информацию о списке доступа возможно через команду:

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

13.7 Настройка списков доступа (MAC ACL)

MAC Access Control List или MAC ACL — список контроля доступа, содержит правила на основе L2 заголовка, определяющие прохождение трафика через интерфейс.

13.7.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать список контроля доступа и перейти в режим его конфигурирования.	**esr(config)# mac access-list extended <NAME>**	<NAME> – имя создаваемого списка контроля доступа, задаётся строкой до 31 символа.
2	Указать описание конфигурируемого списка контроля доступа (необязательно).	**esr(config-acl-mac)# description <DESCRIPTION>**	<DESCRIPTION> – описание списка контроля доступа, задаётся строкой до 255 символов.
3	Создать правило и перейти в режим его конфигурирования. Правила обрабатываются маршрутизатором в порядке возрастания их номеров.	**esr(config-acl-mac)# rule <ORDER>**	<ORDER> – номер правила, принимает значения [1...4094].
4	Указать действие, которое должно быть применено для трафика, удовлетворяющего заданным критериям.	**esr(config-acl-mac-rule)# action <ACT>**	<ACT> – назначаемое действие: • permit – прохождение трафика разрешается; • deny – прохождение трафика запрещается.
5	Установить имя/номер протокола, для которого должно срабатывать правило (необязательно).	**esr(config-acl-mac-rule)# match protocol <TYPE>**	<TYPE> – тип протокола, принимает значения: arp, ip, ipv6, lacp, lldp, cdp, stp, vtp. При указании значения «any» правило будет срабатывать для любых протоколов.
		esr(config-acl-mac-rule)# match ethertype <ID>	<ID> – идентификационный номер инкапсулированного протокола, принимает значения [0x0600-0xFFFF].

Шаг	Описание	Команда	Ключи
8	Установить MAC-адреса отправителя, для которых должно срабатывать правило (необязательно).	**esr(config-acl-mac-rule)# match source-mac <ADDR><WILDCARD>**	<ADDR> – MAC-адрес отправителя, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]; <WILDCARD> – маска MAC-адреса, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]. Биты маски, установленные в 0, задают биты MAC-адреса, исключаемые из сравнения при поиске.
9	Установить MAC-адреса получателя, для которых должно срабатывать правило (необязательно).	**esr(config-acl-mac-rule)# match destination-mac <ADDR><WILDCARD>**	
12	Установить значение 802.1p приоритета, для которого должно срабатывать правило (необязательно).	**esr(config-acl-mac-rule)# match cos <COS>**	<COS> – значение 802.1p приоритета, принимает значения [0..7].
15	Установить значение идентификационного номера VLAN, для которого должно срабатывать правило (необязательно).	**esr(config-acl-mac-rule)# match vlan <VID>**	<VID> – идентификационный номер VLAN, принимает значения [1..4094].
16	Активировать правило.	**esr(config-acl-mac-rule)# enable**	
17	Указать список контроля доступа к конфигурируемому интерфейсу для фильтрации входящего трафика.	**esr(config-if-gi)# service-acl mac input <NAME>**	<NAME> – имя списка контроля доступа, задаётся строкой до 31 символа.
18	Указать список контроля доступа к конфигурируемому интерфейсу для фильтрации исходящего трафика.	**esr(config-if-gi)# service-acl mac output <NAME>**	<NAME> – имя списка контроля доступа, задаётся строкой до 31 символа.

13.7.2 Пример настройки списка доступа

Задача:

Разрешить прохождение ARP запросов только с VLAN 343.

Решение:

Настроим список доступа для фильтрации по протоколу и vlan:

```
esr# configure
esr(config)# mac access-list extended white
esr(config-acl-mac)# rule 1
esr(config-acl-mac-rule)# action permit
esr(config-acl-mac-rule)# match protocol arp
esr(config-acl-mac-rule)# match vlan 343
esr(config-acl-mac-rule)# enable
esr(config-acl-mac-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 mac input white
```

Просмотреть детальную информацию о списке доступа возможно через команду:

```
esr# show mac access-list white
```

13.8 Проксирование HTTP/HTTPS-трафика

13.8.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать объект с URL.	**esr(config)# object-group url <NAME>**	
2	Указать набор.	**esr(config-object-group-url)# url <URL>**	<URL> – адрес веб-страницы, сайта.
3	Создать профиль проксирования.	**esr(config)# ip http profile <NAME>**	<NAME> – название профиля.
4	Выбрать действие по умолчанию.	**esr(config-profile)# default action { deny | permit | redirect } [redirect-url <URL>]**	<URL> – адрес хоста, на который будут передаваться запросы.
5	Указать описание (необязательно).	**esr(config-profile)# description <description>**	<description> – до 255 символов.

Шаг	Описание	Команда	Ключи
6	Указать режим фильтрации данных (необязательно).	**esr(config-profile)# filter <DATA-TYPE>**	<DATA-TYPE> – тип данных, подлежащих фильтрации. Может принимать значения (как одно, так и несколько): • **activex** – заблокировать все приложения ActiveX; • **cookie** – запретить веб-сайтам размещать cookie на пользовательских компьютерах; • **js** – заблокировать все страницы или приложения на основе Javascript.
7	Указать удаленный или локальный список URL и тип операции (блокировка/пропуск трафика/ перенаправление) (необязательно).	**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.
8	Указать удаленный сервер, где лежат необходимые списки URL (необязательно).	**esr(config)# ip http proxy server-url <URL>**	<URL> – адрес сервера, откуда будут брать удалённые списки url.
9	Указать прослушиваемый порт для проксирования http (необязательно).	**esr(config)# ip http proxy listen-ports <OBJ_GROUP_NAME>**	<OBJ_GROUP_NAME> – имя профиля порта, задаётся строкой до 31 символа. По умолчанию прослушиваются порты 80 и 8080
10	Указать прослушиваемый порт для проксирования (необязательно).	**esr(config)# ip https proxy listen-ports <OBJ_GROUP_NAME>**	<OBJ_GROUP_NAME> – имя профиля порта, задаётся строкой до 31 символа. По умолчанию прослушивается порт 443
11	Указать базовый порт для проксирования http (необязательно).	**esr(config)# ip http proxy redirect-port <PORT>**	<PORT> – номер порта, указывается в диапазоне [1..65535]. Значение по умолчанию 3128.
12	Указать базовый порт для проксирования https (необязательно).	**esr(config)# ip http proxy redirect-port <PORT>**	<PORT> – номер порта, указывается в диапазоне [1..65535]. Значение по умолчанию 3128.

Шаг	Описание	Команда	Ключи
13	Включить проксирование на интерфейсе на основе выбранного HTTP-профиля.	**esr(config-if)# ip http proxy <PROFILE_NAME>**	<PROFILE_NAME> – название профиля.
14	Включить проксирование на интерфейсе на основе выбранного HTTPS-профиля.	**esr(config-if)# ip https proxy <PROFILE_NAME>**	<PROFILE_NAME> – название профиля.
15	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.
16	Задать описание списка сервисов (необязательно).	**esr(config-object-group-service)# description <description>**	<description> – описание профиля, задается строкой до 255 символов.
17	Внести необходимые сервисы (TCP/UDP-порты) в список.	**esr(config-object-group-service)# port-range 3128-3135**	Прокси-сервер ESR использует для своей работы порты, начиная с базового порта, определённого на 10 шаге. Для http proxy используются порты, начиная с базового порта по базовый порт + количество cpu данной модели ESR - 1. Для https proxy используются порты, начиная с базового порта + количество cpu данной модели ESR по базовый порт + количество cpu данной модели ESR * 2 - 1. Количество CPU можно посмотреть с помощью команды **show cpu utilization**.
18	Создать набор правил межзонового взаимодействия.	**esr(config)# security zone-pair <src-zone-name> self**	<src-zone-name> – зона безопасности, в которой находятся интерфейсы с функцией ip http proxy или ip https proxy. self – предопределенная зона безопасности для трафика, поступающего на сам ESR.
19	Создать правило межзонового взаимодействия.	**esr(config-zone-pair)# rule <rule-number>**	<rule-number> – 1..10000.

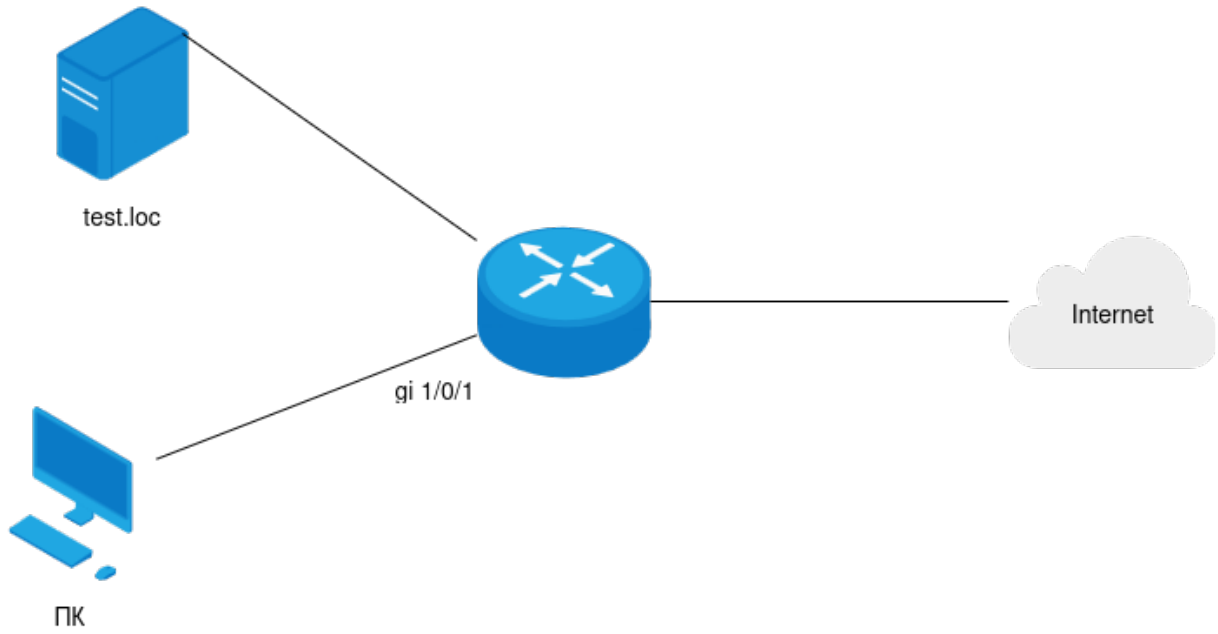
Шаг	Описание	Команда	Ключи
20	Задать описание правила (необязательно).	**esr(config-zone-rule)# description <description>**	<description> – до 255 символов.
21	Указать действие данного правила.	**esr(config-zone-rule)# action <action> [log]**	<action> – permit. log – ключ для активации логирования сессий, которые устанавливаются согласно данному правилу.
22	Установить имя IP-протокола, для которого должно срабатывать правило.	**esr(config-zone-rule)# match protocol <protocol-type>**	<protocol-type> – tcp. Прокси-сервер ESR работает по протоколу ESR.
23	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.
24	Включить правило межзонового взаимодействия.	**esr(config-zone-rule)# enable**	

⚠ Если функция Firewall на ESR принудительно не отключена, необходимо создать разрешающее правило для зоны Self.

13.8.2 Пример настройки HTTP-прокси

Задача №1:

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 FILTER_OG
esr(config-object-group-url)# regexp *speedtest.net/
esr(config-object-group-url)# url http://ya.ru/
esr(config-object-group-url)# url https://ya.ru/
esr(config-object-group-url)# exit
```

Создаем профиль, где указываем действие для всех URL и действие для созданной группы URL:

```
esr(config)# ip http profile PROXY_LIST
esr(config-profile)# default action permit
esr(config-profile)# urls local FILTER_OG action redirect redirect-url http://test.loc
esr(config-profile)# exit
```

Включим проксирование на интерфейсе по профилю 'PROXY_LIST':

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

Если используется Firewall, создадим для него разрешающие правила. Для этого:

Определим число CPU, доступных для данной модели:

```
esr(config)# do show cpu utilization
CPU    Last      Last      Last
       5 sec     1 min     5 min
----   -------   -------   -------
0      3.79%     1.61%     1.55%
1      0.00%     0.00%     0.01%
2      0.00%     0.00%     0.01%
3      0.00%     0.02%     0.01%
```

В примере используется модель ESR-20, у которой 4 CPU.

Соответственно по формуле, описанной на 17 шаге алгоритма настройки http/https-прокси, получаем:

Для http proxy необходимо открыть порты с 3128 по 3131 (3128+4-1=3131).

Для https proxy необходимо открыть порты с 3132 по 3135 (3128+4=3132, 3128+2*4-1=3135).

Создаем профиль портов прокси-сервера:

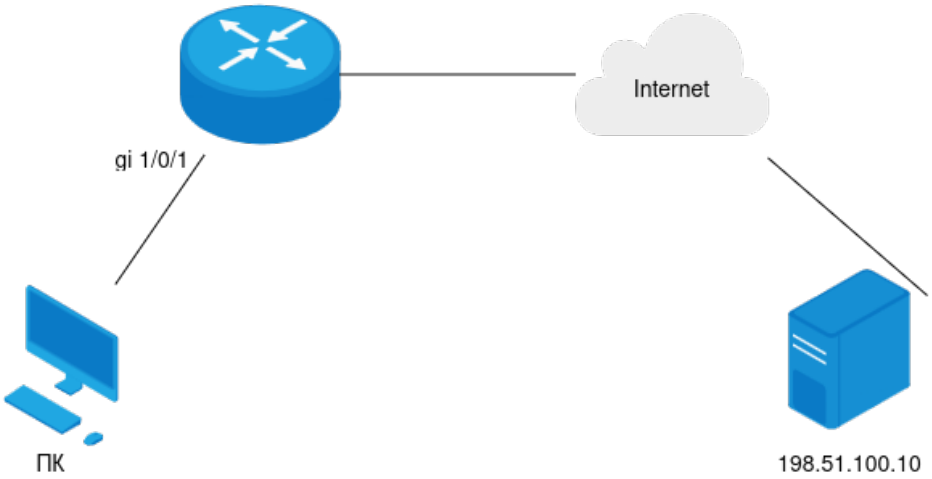
```
esr(config)# object-group service PROXY_PORTS
esr(config-object-group-service)# port-range 3128-3135
esr(config-object-group-service)# exit
```

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 object-group PROXY_PORTS
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
```

Задача №2:

Изменить локальный список с URL для фильтрации proxy-сервером из задачи №1 на список, получаемый с удалённого сервера.



Решение:

Для использования remote-списка необходимо в конфигурации прописать адрес сервера, а в `ip http profile` изменить `urls local` на `urls remote <list>` – название списка, лежащего на сервере:

```
esr(config)# ip http proxy server-url http://198.51.100.10
esr(config)# ip http profile PROXY_LIST
esr(config-profile)# default action permit
esr(config-profile)# urls remote URLS_PROXY action deny
esr(config-profile)# exit
```

Задача №3:

Организовать фильтрацию по веб-скриптам ActiveX URL для ряда адресов посредством прокси и настроить логирование событий в консоль.

Решение:

Вы можете настроить Proxy-сервер для фильтрации определённых веб-скриптов. Для фильтрации доступны ActiveX, cookie, JavaScript.

Для блокировки сайтов, использующих ActiveX, настроим фильтрацию и включим логирование событий proxy:

```
esr(config)# ip http profile PROXY_LIST
esr(config-profile)# default action permit
esr(config-profile)# urls local FILTER_OG action redirect redirect-url http://test.loc
esr(config-profile)# filter activex
esr(config-profile)# log enable
esr(config-profile)# exit
```

Теперь при срабатывании фильтрации, а также указанных действий для URL, в консоль будут попадать логи вида:

```
%FIREWALL-I-LOG: http proxy 'Filter' (QQ) denied (ActiveX)
%FIREWALL-I-LOG: http proxy 'PROXY_LIST' permitted
```

13.9 Настройка IPS/IDS

⚠ Данная функция активируется только при наличии лицензии.

IPS/IDS (Intrusion Prevention System/Intrusion Detection System) – система предотвращения вторжений – программная система сетевой и компьютерной безопасности, обнаруживающая вторжения или нарушения безопасности и автоматически защищающая от них.

Работа системы основана на сигнатурном анализе трафика. Сигнатуры для систем IPS/IDS принято называть правилами. Устройства ESR позволяют скачивать актуальные правила с открытых источников в сети Интернет или с корпоративного сервера. Также с помощью CLI можно создавать свои специфические правила.

13.9.1 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 (необязательно).	**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 (необязательно).	**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 (необязательно).	**esr(config-ips)# perfomance max**	По умолчанию для IPS/IDS отдается половина доступных ядер процессора.

Шаг	Описание	Команда	Ключи
8	Задать параметры удаленного сервера для отправки статистики работы сервиса IPS/IDS в формате EVE (elasticsearch) (необязательно).	**esr(config-ips)# logging remote-server { <ADDR> | <IPV6-ADDR> } [<TRANSPORT>] [<PORT>] [source-address { <SRC-ADDR> | <IPV6-SRC-ADDR> | object-group <NETWORK_OBJ_GROUP_NAME> }]**	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <TRANSPORT> – протокол передачи данных, по умолчанию – UDP, принимает значения: • TCP – передача данных осуществляется по протоколу TCP; • UDP – передача данных осуществляется по протоколу UDP. <PORT> – номер TCP/UDP-порта, опциональный параметр, принимает значения [1..65535], по умолчанию 514; <SRC-ADDR> – IPv4-адрес маршрутизатора, который будет использоваться в качестве IP-адреса источника в отправляемых syslog-пакетах, по умолчанию – IPv4-адрес интерфейса, с которого отправляются пакеты; <IPV6-SRC-ADDR> – IPv6-адрес маршрутизатора, который будет использоваться в качестве IPv6-адреса источника в отправляемых syslog-пакетах, по умолчанию – IPv6-адрес интерфейса, с которого отправляются пакеты; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве source address.

Шаг	Описание	Команда	Ключи
9	Установить интервал отправки статистики работы сервиса IPS/IDS в формате EVE (elasticsearch) (необязательно).	**esr(config-ips)# logging update-interval <INTERVAL>**	<INTERVAL> – интервал отправки статистики работы сервиса IPS/IDS, задаётся в минутах.
10	Заблокировать передачу трафика при начальной загрузке до запуска сервиса IPS/IDS и загрузки хотя бы одного настроенного или существующего правила (необязательно).	**esr(config-ips)# fail-close enable**	
11	Установить размер виртуальных очередей (необязательно).	**esr(config-ips)# queue-limit <QUEUE-LIMIT>**	<QUEUE-LIMIT> – предельное количество пакетов в виртуальной очереди, принимает значения в диапазоне [32..4096] Размер очереди по умолчанию 1024
12	Активировать сервис IPS.	**esr(config-ips)# enable**	
13	Активировать IPS/IDS на интерфейсе.	**esr(config-if-gi)# service-ips { inline | monitor }**	inline – этот режим устанавливается, когда ESR с сервисом IPS/IDS ставится в разрыв сети. monitor – этот режим устанавливается, когда ESR с сервисом IPS/IDS мониторит зеркалируемый трафик.

13.9.2 Алгоритм настройки автообновления правил IPS/IDS из внешних источников

Шаг	Описание	Команда	Ключи
1	Задать имя внешнего хранилища скачиваемых правил (необязательно).	**esr(config-ips)# storage-path { usb://<USB-NAME>:/ | mmc://<MMC-NAME>:/ }**	<USB-NAME> – имя подключенного USB-носителя. Имя можно узнать в выводе команды show storage-devices usb; <MMC-NAME> – имя подключенного MMC-носителя. Имя можно узнать в выводе команды show storage-devices mmc. Для использования с системой IPS/IDS на внешнем носителе должен быть создан раздел файловой системы в формате exFAT.
2	Перейти в режим конфигурирования автообновлений.	**esr(config-ips)# auto-upgrade**	
3	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.
4	Задать описание пользовательского сервера обновлений (необязательно).	**esr(config-ips-upgrade-user-server)# description <DESCRIPTION>**	<DESCRIPTION> – описание задаётся строкой до 255 символов.
5	Задать URL.	**esr(config-ips-upgrade-user-server)# url <URL>**	<URL> – текстовое поле, содержащее URL-ссылку длиной от 8 до 255 символов. В качестве URL-ссылки может быть указан: • файл правил с расширение .rule; • файл классификатора правил с именем classification.config; • каталог на сервере содержащий файлы правил и/или файл классификатора правил.

Шаг	Описание	Команда	Ключи
6	Задать частоту проверки обновлений (необязательно).	**esr(config-ips-upgrade-user-server)# upgrade interval <HOURS>**	<HOURS> – интервал обновлений в часах, от 1 до 240. Значение по умолчанию: 24 часа.
7	Активизировать пользовательский сервер обновлений.	**esr(config-ips-upgrade-user-server)# enable**	

Для правил IPS/IDS, загружаемых из внешних источников, на маршрутизаторах ESR выделена отдельная область энергозависимой памяти.
Размер этой области зависит от модели ESR:

- ESR-1X – 25 МБ;
- ESR-2X – 50 МБ;

Для всех остальных моделей – 100 МБ.
Если настроить слишком много источников правил или загружать правила, превышающие указанные лимиты, то маршрутизатор будет выдавать сообщения об ошибке %STORAGE_IPS_MGR-I-ERR: There no free space in rules directory.
В этом случае стоит уменьшить объем запрашиваемых правил или использовать внешнее хранилище.

13.9.3 Рекомендуемые открытые источники обновления правил

SSL Blacklist

Чёрный список SSL (SSLBL) – это проект abuse.ch, целью которого является обнаружение вредоносных SSL-соединений путём идентификации и внесения в чёрный список SSL-сертификатов, используемых серверами управления ботнетами.

https://sslbl.abuse.ch/blacklist/sslblacklist_tls_cert.rules – набор правил SSL-сертификатов от SSLBL используется для обнаружения и/или блокировки вредоносных SSL-соединений в вашей сети на основе отпечатка SSL-сертификата. Набор правил SSL-сертификатов генерируется каждые 5 минут. Рекомендуется запрашивать его не чаще, чем раз в 5 минут.

https://sslbl.abuse.ch/blacklist/ja3_fingerprints.rules – набор правил JA3 FingerprintRuleset от SSLBL используется для обнаружения и/или блокировки вредоносных SSL-соединений в вашей сети на основе отпечатка JA3. Набор правил для отпечатков пальцев Suricata JA3 генерируется каждые 5 минут. Рекомендуется запрашивать его не чаще, чем раз в 5 минут.

Отпечатки JA3, внесённые в чёрный список SSLBL, были собраны путём анализа более 25 000 000 PCAP-файлов с образцами вредоносного ПО. Эти отпечатки ещё не были протестированы на известном безопасном трафике и могут привести к значительному количеству ложных срабатываний.

Feodo Tracker

Feodo Tracker – это проект abuse.ch, целью которого является обмен информацией о серверах управления ботнетами, связанными с Dridex, Emotet (также известным как Heodo), TrickBot, QakBot (также известным как QuakBot/Qbot) и BazarLoader (также известным как BazarBackdoor).

https://feodotracker.abuse.ch/downloads/feodotracker.rules – набор правил используется для обнаружения и/или блокировки сетевых подключений к хост-серверам (комбинация IP-адреса и порта). Набор правил генерируется каждые 5 минут. Рекомендуется обновлять набор правил IDS каждые 5–15 минут, чтобы обеспечить лучшую защиту от Dridex, Emotet, TrickBot, QakBot и BazarLoader.

⚠ Поскольку IP-адреса перерабатываются и используются повторно, в этот список блокировки входят только C2-серверы ботнетов, которые либо активны, либо в последний раз использовались в течение последних 30 дней. Таким образом, процент ложных срабатываний в этом списке блокировки должен быть низким.

https://feodotracker.abuse.ch/downloads/feodotracker_aggressive.rules – набор правил IDS с полным списком всех C2-серверов ботнетов. Однако, поскольку IP-адреса используются повторно, количество ложных срабатываний в этом наборе правил намного выше.

⛔ Не рекомендуется использовать агрессивную версию индикаторов компрометации ботнета C2 (IOC), так как она определённо вызовет ложные срабатывания.

Travis Green

Travis Green – набор правил для поиска угроз от специалиста по кибербезопасности Тревиса Грина.

https://raw.githubusercontent.com/travisbgreen/hunting-rules/master/hunting.rules

Etnetera Core

Набор правил с «агрессивными» IP-адресами от центра кибербезопасности компании Etnetera Core.

https://security.etnetera.cz/feeds/etn_aggressive.rules

13.9.4 Пример настройки IPS/IDS с автообновлением правил

Задача:

Организовать защиту локальной сети с автообновлением правил из открытых источников.

192.168.1.0/24 – локальная сеть.

Решение:

Создадим профиль адресов защищаемой локальной сети:

```
esr(config)# object-group network LAN
esr(config-object-group-network)# ip prefix 192.168.1.0/24
esr(config-object-group-network)# exit
```

Настроим на ESR DNS-клиента для разрешения имен источников обновления правил IPS/IDS:

```
esr(config)# domain lookup enable
esr(config)# domain nameserver 8.8.8.8
```

Создадим политику безопасности IPS/IDS:

```
esr(config)# security ips policy OFFICE
esr(config-ips-policy)# description "My Policy"
esr(config-ips-policy)# protect network-group LAN
```

Разрешим работу IPS/IDS на интерфейсе локальной сети bridge 1:

```
esr(config)# bridge 1
esr(config-bridge)# service-ips inline
```

Настроим параметры IPS/IDS:

```
esr(config)# security ips
esr(config-ips)# logging remote-server 192.168.10.1
esr(config-ips)# logging update-interval 15
esr(config-ips)# policy OFFICE
esr(config-ips)# enable
```

Устройство будет использоваться только как шлюз безопасности, по этому отдадим сервису IPS/IDS все доступные ресурсы:

```
esr(config-ips)# perfomance max
```

Настроим автообновление правил с сайтов etnetera.cz и Abuse.ch:

```
esr(config-ips)# auto-upgrade
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)# enable
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_tls_cert.rules
esr(config-ips-upgrade-user-server)# upgrade interval 4
esr(config-ips-upgrade-user-server)# enable
esr(config-ips-upgrade-user-server)# exit
```

13.9.5 Алгоритм настройки базовых пользовательских правил

Шаг	Описание	Команда	Ключи
1	Задать имя и перейти в режим конфигурирования набора пользовательских правил.	**esr(config)# security ips-category user-defined <WORD>**	<WORD> – имя набора пользовательских правил, задаётся строкой до 32 символов.
2	Задать описание набора пользовательских правил (не обязательно).	**esr(config-ips-category)# description <DESCRIPTION>**	<DESCRIPTION> – описание задаётся строкой до 255 символов.
3	Создать правило и перейти в режим конфигурирования правила.	**esr(config-ips-category)# rule <ORDER>**	<ORDER> – номер правила, принимает значения [1..512].
4	Задать описание правила (необязательно).	**esr(config-ips-category-rule)# description <DESCRIPTION>**	<DESCRIPTION> – описание задаётся строкой до 255 символов.

Шаг	Описание	Команда	Ключи
5	Указать действие данного правила.	**esr(config-ips-category-rule)# action { alert | reject | pass | drop }**	• alert – прохождение трафика разрешается, и сервис IPS/IDS генерирует сообщение; • reject – прохождение трафика запрещается. Если это TCP-трафик, отправителю и получателю посылается пакет TCP-RESET, для остального типа трафика посылается пакет ICMP-ERROR. Сервис IPS/IDS генерирует сообщение; • pass – прохождение трафика разрешается; • drop – прохождение трафика запрещается, и сервис IPS/IDS генерирует сообщение.
6	Установить имя IP-протокола, для которого должно срабатывать правило.	**esr(config-ips-category-rule)# protocol <PROTOCOL>**	<PROTOCOL> – принимает значения any/ip/icmp/http/ tcp/udp. При указании значения «any» правило будет срабатывать для любых протоколов.

Шаг	Описание	Команда	Ключи
7	Установить IP-адреса отправителя, для которых должно срабатывать правило.	**esr(config-ips-category-rule)# source-address {ip <ADDR> | ip-prefix <ADDR/LEN> | object-group <OBJ_GR_NAME> | policy-object-group { protect | external } | any }**	<ADDR> – IP-адрес отправителя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <ADDR/LEN> – IP-подсеть отправителя, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и LEN принимает значения [1..32]. < OBJ_GR_NAME> – имя профиля IP-адресов, который содержит IP-адреса отправителя, задаётся строкой до 31 символа. • protect – устанавливает в качестве адресов отправителя и protect-адреса определенные адреса в политике IPS/IDS; • external – устанавливает в качестве адресов отправителя и external-адреса определенные адреса в политике IPS/IDS. При указании значения «any» правило будет срабатывать для любого IP-адреса отправителя.
8	Установить номера TCP/UDP-портов отправителя, для которых должно срабатывать правило. Для значения protocol icmp, значение source-port может быть только any.	**esr(config-ips-category-rule)# source-port {any | <PORT> | object-group <OBJ-GR-NAME> }**	<PORT> – номер TCP/UDP-порта отправителя, принимает значения [1..65535]. <OBJ_GR_NAME> – имя профиля TCP/UDP-портов отправителя, задаётся строкой до 31 символа. При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта отправителя.

Шаг	Описание	Команда	Ключи
9	Установить IP-адреса получателя, для которых должно срабатывать правило.	**esr(config-ips-category-rule)# destination-address {ip <ADDR> | ip-prefix <ADDR/LEN> | object-group <OBJ_GR_NAME> | policy-object-group { protect | external } | any }**	<ADDR> – IP-адрес получателя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <ADDR/LEN> – IP-подсеть получателя, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и LEN принимает значения [1..32]; <OBJ_GR_NAME> – имя профиля IP-адресов, который содержит IP-адреса получателя, задаётся строкой до 31 символа. • protect – устанавливает в качестве адресов получателя protect-адреса, определенные в политике IPS/IDS; • external – устанавливает в качестве адресов получателя external-адреса, определенные в политике IPS/IDS. При указании значения «any» правило будет срабатывать для любого IP-адреса получателя.
10	Установить номера TCP/UDP-портов получателя, для которых должно срабатывать правило. Для значения protocol icmp, значение destination-port может быть только any.	**esr(config-ips-category-rule)# destination-port {any | <PORT> | object-group <OBJ-GR-NAME> }**	<PORT> – номер TCP/UDP-порта получателя, принимает значения [1..65535]; <OBJ_GR_NAME> – имя профиля TCP/UDP-портов получателя, задаётся строкой до 31 символа. При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта получателя.

Шаг	Описание	Команда	Ключи
11	Установить направление потока трафика, для которого должно срабатывать правило.	**esr(config-ips-category-rule)# direction { one-way | round-trip }**	• one-way – трафик передаётся в одну сторону. • round-trip – трафик передаётся в обе стороны.
12	Определить сообщение, которое IPS/IDS будет записывать в лог при срабатывании этого правила.	**esr(config-ips-category-rule)# meta log-message <MESSAGE>**	<MESSAGE> – текстовое сообщение, задаётся строкой до 129 символов.

Шаг	Описание	Команда	Ключи
13	Определить классификацию трафика, которая будет записывать в лог при срабатывании этого правила (необязательно).	**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 – неподозрительный трафик. • unknown – неизвестный трафик. • bad-unknown – потенциально плохой трафик. • attempted-recon – попытка утечки информации. • successful-recon-limited – утечка информации. • successful-recon-largescale – масштабная утечка информации. • attempted-dos – попытка отказа в обслуживании. • successful-dos – отказ в обслуживании. • attempted-user – попытка получения привилегий пользователя. • unsuccessful-user – безуспешная попытка получения привилегий пользователя. • successful-user – успешная попытка получения привилегий пользователя. • attempted-admin – попытка получения привилегий администратора. • successful-admin – успешная попытка получения привилегий администратора. • rpc-portmap-decode – декодирование запроса RPC. • shellcode-detect – обнару жен исполняемый код. • string-detect – обнаружена подозрительная строка. • suspicious-filename-detect – было обнаружено подозрительное имя-файла.

Шаг	Описание	Команда	Ключи
			• suspicious-login – была обнаружена попытка входа с использованием подозрительного имени пользователя. • system-call-detect – обнаружен системный вызов. • tcp-connection – обнаружено TCP-соединение. • trojan-activity – был обнаружен сетевой троян. • unusual-client-port-connection – клиент использовал необычный порт. • network-scan – обнаружение сетевого сканирования. • denial-of-service – обнаружение атаки отказа в обслуживании. • non-standard-protocol – обнаружение нестандартного протокола или события. • protocol-command-decode – обнаружена попытка шифрования. • web-application-activity – доступ к потенциально уязвимому веб-приложению. • web-application-attack – атака на веб-приложение. • misc-activity – прочая активность. • misc-attack – прочие атаки. • icmp-event – общее событие ICMP. • inappropriate-content – обнаружено неприемлемое содержание. • policy-violation – потенциальное нарушение корпоративной конфиденциальности.

Шаг	Описание	Команда	Ключи
			• default-login-attempt – попытка входа с помощью стандартного логина/пароля.
14	Установить значение кода DSCP, для которого должно срабатывать правило (необязательно).	**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 (необязательно).	**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 (необязательно). Применимо только для значения protocol any.	**esr(config-ips-category-rule)# ip protocol-id <ID>**	<ID> – идентификационный номер IP-протокола, принимает значения [1..255].
17	Установить значения ICMP CODE, для которого должно срабатывать правило (необязательно). Применимо только для значения protocol icmp.	**esr(config-ips-category-rule)# ip icmp code <CODE>**	<CODE> – значение CODE протокола ICMP, принимает значение в диапазоне [0..255].
		esr(config-ips-category-rule)# ip icmp code comparison-operator { greater-than | less-than }	Оператор сравнения для значения ip icmp code: • greater-than – больше чем.. • less-than – меньше чем..
18	Установить значения ICMP ID, для которого должно срабатывать правило (необязательно). Применимо только для значения protocol icmp.	**esr(config-ips-category-rule)# ip icmp id <ID>**	<ID> – значение ID протокола ICMP, принимает значение в диапазоне [0.. 65535].
19	Установить значения ICMP Sequence-ID, для которого должно срабатывать правило (необязательно). Применимо только для значения protocol icmp.	**esr(config-ips-category-rule)# ip icmp sequence-id <SEQ-ID>**	<SEQ-ID> – значение Sequence-ID протокола ICMP, принимает значение в диапазоне [0.. 4294967295].
20	Установить значения ICMP TYPE, для которого должно срабатывать правило (необязательно). Применимо только для значения protocol icmp.	**esr(config-ips-category-rule)# ip icmp type <TYPE>**	<TYPE> – значение TYPE протокола ICMP, принимает значение в диапазоне [0..255].

Шаг	Описание	Команда	Ключи
		esr(config-ips-category-rule)# ip icmp type comparison-operator { greater-than | less-than }	Оператор сравнения для значения ip icmp type: • greater-than – больше чем.. • less-than – меньше чем..
21	Установить значения TCP Acknowledgment-Number, для которого должно срабатывать правило (необязательно). Применимо только для значения protocol tcp.	**esr(config-ips-category-rule)# ip tcp acknowledgment-number <ACK-NUM>**	<ACK-NUM> – значение Acknowledgment-Number протокола TCP, принимает значение в диапазоне [0.. 4294967295].
22	Установить значения TCP Sequence-ID, для которого должно срабатывать правило (необязательно). Применимо только для значения protocol tcp.	**esr(config-ips-category-rule)# ip tcp sequence-id <SEQ-ID>**	<SEQ-ID> – значение Sequence-ID протокола TCP, принимает значение в диапазоне [0.. 4294967295].
23	Установить значения TCP Window-Size, для которого должно срабатывать правило (необязательно). Применимо только для значения protocol tcp.	**esr(config-ips-category-rule)# ip tcp window-size <SIZE>**	<SIZE> – значение Window-Size протокола TCP, принимает значение в диапазоне [0.. 65535].
24	Установить ключевые слова протокола HTTP, для которых должно срабатывать правило (необязательно). Применимо только для значения protocol http.	**esr(config-ips-category-rule)# ip http { accept | accept-enc | accept-lang | client-body | connection | content-type | cookie | file-data | header | header-names | host | method | protocol | referer | request-line | response-line | server-body | start | start-code | start-msg | uri | user-agent }**	Значение ключевых слов см. в документации Suricata 4.X. https://suricata.readthedocs.io/en/suricata-4.1.4/rules/http-keywords.html
25	Установить значение ключевого слова URI LEN протокола HTTP, для которых должно срабатывать правило (необязательно). Применимо только для значения protocol http.	**esr(config-ips-category-rule)# ip http urilen <LEN>**	<LEN> – принимает значение в диапазоне [0.. 65535].
		esr(config-ips-category-rule)# ip http urilen comparison-operator { greater-than | less-than }	Оператор сравнения для значения ip http urilen: • greater-than – больше чем.. • less-than – меньше чем..

Шаг	Описание	Команда	Ключи
26	Установить значение содержимого пакетов (Payload content), для которых должно срабатывать правило (необязательно).	**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 (необязательно). Применимо только совместно с командой payload content.	**esr(config-ips-category-rule)# payload no-case**	
28	Установить, сколько байтов с начала содержимого пакета будет проверено (необязательно). Применимо только совместно с командой payload content.	**esr(config-ips-category-rule)# payload depth <DEPTH>**	<DEPTH> – число байт с начала содержимого пакета, принимает значение в диапазоне [1.. 65535]. По умолчанию проверяется все содержимое пакета.
29	Установить число байт смещения от начала содержимого пакета для проверки (необязательно). Применимо только совместно с командой payload content.	**esr(config-ips-category-rule)# payload offset <OFFSET>**	<OFFSET> – число байт смещения от начала содержимого пакета, принимает значение в диапазоне [1.. 65535]. По умолчанию проверяется с начала содержимого.
30	Установить размер содержимого пакетов, для которых должно срабатывать правило (необязательно).	**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: • greater-than – больше чем.. • less-than – меньше чем.
31	Указать пороговое значение количества пакетов, при котором сработает правило (необязательно).	**esr(config-ips-category-rule)# threshold count <COUNT>**	<COUNT> – число пакетов, принимает значение в диапазоне [1.. 65535].
32	Указать интервал времени, для которого считается пороговое количество пакетов. (Обязательно, если включен threshold count).	**esr(config-ips-category-rule)# threshold second <SECOND>**	<SECOND> – интервал времени в секундах, принимает значение в диапазоне [1.. 65535].

Шаг	Описание	Команда	Ключи
33	Указать по адресу отправителя или получателя будут считаться пороги. (Обязательно, если включен threshold count).	**esr(config-ips-category-rule)# threshold track { by-src | by-dst }**	• by-src – считать пороговое значение для пакетов с одинаковым IP-отправителя. • by-dst – считать пороговое значение для пакетов с одинаковым IP-получателя.
34	Указать метод обработки пороговых значений.	**esr(config-ips-category-rule)# threshold type {threshold | limit | both }**	• threshold – выдавать сообщение каждый раз по достижении порога. • limit – выдавать сообщение не чаще <COUNT> раз за интервал времени <SECOND>. • both – комбинация threshold и limit. Сообщение будет генерироваться, если в течении интервала времени <SECOND> было <COUNT> или более пакетов подходящих под условия правила, и сообщение будет отправлено только один раз в течении интервала времени <SECOND>.
35	Активировать правило.	**esr(config-ips-category-rule)# enable**	

13.9.6 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"
```

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 был указан 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 используемый сервер:

```
esr(config-ips-category-rule)# destination-address ip 192.168.1.10
```

Атакующий может отправлять пакеты с любого адреса:

```
esr(config-ips-category-rule)# source-address any
```

Зададим направление трафика:

```
esr(config-ips-category-rule)# direction one-way
```

Правило будет срабатывать на пакеты размером больше 1024 байт:

```
esr(config-ips-category-rule)# payload data-size 1024
esr(config-ips-category-rule)# payload data-size comparison-operator greate r-than
```

Правило будет срабатывать, если нагрузка на сервер будет превышать 3 Мбит/с, при этом сообщение об атаке будет генерироваться не чаще одного раза в минуту:

```
3 Мб/с = 3145728 бит в сек
Пакет размером 1Кбайт = 8192 бита
3145728 / 8192 = 384 пакета в сек
384 * 60 = 23040 пакетов в минуту
```

```
esr(config-ips-category-rule)# threshold count 23040
esr(config-ips-category-rule)# threshold second 60
esr(config-ips-category-rule)# threshold track by-dst
esr(config-ips-category-rule)# threshold type both
```

Активизируем правило:

```
esr(config-ips-category-rule)# enable
```

13.9.7 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 (необязательно).	**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 (необязательно).	**esr(config-ips-category-rule-advanced)# description <DESCRIPTION>**	<DESCRIPTION> – описание задаётся строкой до 255 символов.
5	Указать действие данного правила.	**esr(config-ips-category-rule-advanced)# rule-text <LINE>**	<CONTENT> – текстовое сообщение в формате SNORT 2.X / Suricata 4.X, задаётся строкой до 1024 символов. ⚠ При написании правил в тексте правила необходимо использовать только двойные кавычки (символ "), а само правило необходимо заключать в одинарные кавычки (символ ').
6	Активировать правило.	**esr(config-ips-category-rule-advanced)# enable**	

13.9.8 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;)'
esr(config-ips-category-rule-advanced)# enable
esr(config-ips-category-rule-advanced)# exit
```

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; )'
esr(config-ips-category-rule-advanced)#
```

13.10 Настройка взаимодействия с Eltex Distribution Manager

EDM (Eltex Distribution Manager) — сервис распространения лицензируемого контента на устройства по коммерческой подписке.

Благодаря использованию инфраструктуры безопасности «Лаборатории Касперского», в том числе облачного «коллективного разума» Kaspersky Security Network с поддержкой Kaspersky SafeStream II, сервисный маршрутизатор ESR способен обнаруживать вредоносное ПО во всех типах трафика (web, email, P2P, сервисы мгновенного обмена сообщениями и т.п.). В результате обеспечивается защита пользователей от самых опасных киберугроз, в том числе угроз нулевого дня, программ-шифровальщиков, заражённых сайтов и иных типов.

Система IPS на устройствах ESR может использовать следующие наборы правил, предоставляемых Kaspersky SafeStream II:

- Данные о репутации IP-адресов — набор IP-адресов с контекстной информацией, сообщающей о подозрительных и вредоносных узлах;
- URL-адреса вредоносных ссылок — набор URL-адресов, соответствующих опасным ссылкам и веб-сайтам;

- URL-адреса фишинговых ссылок — набор URL-адресов, распознаваемых «Лабораторией Касперского» как фишинговые. Доступны записи с масками и без масок;
- URL-адреса командных серверов ботнетов — набор URL-адресов командных серверов ботнетов и связанных с ними вредоносных объектов;
- URL-адреса шифровальщиков — набор URL-адресов шифровальщиков;
- Хэши вредоносных объектов — набор файловых хэшей, охватывающий наиболее опасные и распространенные, а также самые новые вредоносные программы;
- Хэши вредоносных объектов для мобильных устройств — набор файловых хэшей для обнаружения вредоносных объектов, заражающих мобильные устройства;
- URL-адреса командных серверов ботнетов для мобильных устройств — набор URL-адресов с контекстной информацией для выявления командных серверов ботнетов, использующих мобильные устройства;
- URL-адреса веб-сайтов, используемых для размещения вредоносных программ, заражающих устройства Internet of Things (IoT).

13.10.1 Алгоритм базовой настройки

Шаг	Описание	Команда	Ключи
1	Перейти в конфигурирование контент-провайдера.	**esr (config)# content-provider**	
2	Задать IP-адрес edm-сервера.	**esr (config-content-provider)# host address <A.B.C.D | WORD | X:X:X:X::X>**	<IP-ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. WORD(1-31) – DNS-имя сервера.
3	Задать порт для подключения к edm-серверу.	**esr (config-content-provider)# host port <PORT>**	<PORT> – номер TCP/UDP-порта отправителя, принимает значения [1..65535].
4	Задать тип и раздел внешнего устройства для создания крипто-хранилища.	**esr (config-content-provider)# storage-path <DEVICE>**	<DEVICE> – лейбл и имя раздела на внешнем носителе информации в формате usb://Partion_name:/ mmc://Partion_name:/. На внешнем носителе должна быть создана файловая система в формате exFAT.

Шаг	Описание	Команда	Ключи
5	Установить время перезагрузки устройства после получения сертификата.	**esr (config-content-provider)# reboot immediately | [time <HH:MM:SS> | <WEEK_DAY>]**	Перезагрузить устройство после получения сертификата. time <HH:MM:SS> – время, в которое ESR перезагрузится <Часы:минуты:секунды>. <WEEK_DAY> - день недели, принимает значения: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday.
6	Включить контент провайдер.	**enable**	
7	Установить интервал обращения к edm-серверу в часах.	**esr (config-content-provider)# upgrade interval <1-240>**	
8	Установить описание (необязательно).	**esr (config-content-provider)# description < LINE >**	LINE (1-255) String describing server
9	Задать текстовое имя устройства, которое передаётся на сервер EDM (необязательно).	**esr (config-content-provider)# system-name < WORD >**	<WORD> – имя, задаётся строкой до 255 символов.
10	Задать текстовое описание, которое передаётся на сервер EDM (необязательно).	**esr (config-content-provider)# location < WORD >**	<WORD> – описание, задаётся строкой до 255 символов.
11	Задать значение DSCP, которое будет использоваться для маркировки трафика при обращениях к EDM-серверу (необязательно).	**esr (config-content-provider)# dscp <DSCP>**	<DSCP> – значение DSCP, принимает значения [0..63], по умолчанию 48.

Шаг	Описание	Команда	Ключи
12	Создать списки IP-адресов, которые будут использоваться при фильтрации.	**esr (config)# object-group network <WORD>** **esr (config-object-group-network)# ip prefix <ADDR/LEN> [unit <ID>]**	<WORD> – имя сервера, задаётся строкой до 32 символов. <ADDR/LEN> – подсеть, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. <ID> – номер юнита, принимает значения [1..4].
13	На интерфейсе включить service-ips.	**esr (config)# interface gigabitethernet 1/0/Xesr (config-if-gi)# service-ips enable**	
14	Создать политику безопасности IPS/IDS.	**esr (config)# security ips policy WORD(1-31)**	WORD(1-31)
15	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.
16	Войти в раздел конфигурирования вендора.	**esr (config-ips-policy)# vendor kaspersky**	
17	Подключить необходимую категорию.	**esr (config-ips-vendor)# category WORD(1-64)**	Категории, доступные по текущей подписке, можно посмотреть в контекстной подсказке или командой: `show security ips content-provider rules-info`

Шаг	Описание	Команда	Ключи
18	Задать тип правил.	**esr (config-ips-vendor-category)# rules action <ACTION>**	<ACTION> - drop | reject | alert | pass – действия, которые будут применяться к пакетам. • alert – прохождение трафика разрешается, и сервис IPS/IDS генерирует сообщение; • reject – прохождение трафика запрещается. Если это TCP-трафик, отправителю и получателю посылается пакет TCP-RESET, для остального типа трафика посылается пакет ICMP-ERROR. Сервис IPS/IDS генерирует сообщение; • pass – прохождение трафика разрешается; • drop – прохождение трафика запрещается, и сервис IPS/IDS генерирует сообщение.

Шаг	Описание	Команда	Ключи

19	Задать количество скачиваемых правил.	**esr (config-ips-vendor-category)# rules { all | count <COUNT> | percent <PERCENT> | recomended }**	• all – данной командой указывается, что система IPS/IDS будет работать с полным набором правил данной категории;
			• count <COUNT> – данной командой указывается действующее число правил данной категории, с которым будет работать система IPS/IDS:
			  • <COUNT> – число правил. Минимальное значение 1, максимальное значение зависит от категории правил.
			• percent <PERCENT> – данной командой указывается процентное соотношение от общего числа правил данной категории, с которым будет работать система IPS/IDS:
			  • <PERCENT> – процент от общего числа правил.
			• recomended – данной командой указывается, что система IPS/IDS будет использовать рекомендованное количество правил в данной категории. Рекомендованное количество составляет 42% от общего числа правил.
			
			Максимальное число правил по категориям можно посмотреть в контекстной подсказке или командой:
			
			`show security ips content-provider rules-info`

20	Включить категорию.	**enable**	
21	Перейти в режим конфигурирования IPS/IDS.	**esr (config)# security ips**	
22	Назначить политику безопасности IPS/IDS.	**esr(config-ips)# policy <NAME>**	<NAME> – имя политики безопасности, задаётся строкой до 32 символов.
23	Использовать все ресурсы ESR для IPS/IDS (необязательно).	**esr(config-ips)# perfomance max**	

Шаг	Описание	Команда	Ключи
24	Задать параметры удаленного сервера для отправки статистики работы сервиса IPS/IDS в формате EVE (elasticsearch) (необязательно).	**esr(config-ips)# logging remote-server { <ADDR> | <IPV6-ADDR> } [<TRANSPORT>] [<PORT>] [source-address { <SRC-ADDR> | <IPV6-SRC-ADDR> }]**	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <TRANSPORT> – протокол передачи данных, по умолчанию – UDP, принимает значения: • TCP – передача данных осуществляется по протоколу TCP; • UDP – передача данных осуществляется по протоколу UDP. <PORT> – номер TCP/UDP-порта, опциональный параметр, принимает значения [1..65535], по умолчанию 514; <SRC-ADDR> – IPv4-адрес маршрутизатора, который будет использоваться в качестве IP-адреса источника в отправляемых syslog-пакетах, по умолчанию – IPv4-адрес интерфейса, с которого отправляются пакеты; <IPV6-SRC-ADDR> – IPv6-адрес маршрутизатора, который будет использоваться в качестве IPv6-адреса источника в отправляемых syslog-пакетах, по умолчанию – IPv6-адрес интерфейса, с которого отправляются пакеты.
25	Установить интервал отправки статистики работы сервиса IPS/IDS в формате EVE (elasticsearch) (необязательно).	**esr(config-ips)# logging update-interval <INTERVAL>**	<INTERVAL> – интервал отправки статистики работы сервиса IPS/IDS, задаётся в минутах.
26	Активировать IPS/IDS.	**esr(config- ips)# enable**	

13.10.2 Пример настройки

Задать параметры content-provider — это адрес сервера ELTEX. Между сервером content-provider и маршрутизатором должна быть сетевая доступность.

```
content-provider
  host address edm.eltex-co.ru
  host port 8098
  upgrade interval 1
  storage-path mmc://TEST:/
  reboot immediately
  enable
exit
```

После перезагрузки устройства можно начинать настраивать сервис IPS.

Задать профиль IP-адресов, которые будет защищать IPS/IDS:

```
object-group network objectgroup0
  ip prefix 192.168.30.0/24
exit
```

На интерфейсе включить IPS:

```
interface gigabitethernet 1/0/1
  service-ips enable
exit
```

Настроить политику безопасности:

```
security ips policy policy0
  protect network-group objectgroup0
  vendor kaspersky
    category MaliciousURLsDF
      rules action alert
      rules all
      enable
    exit
    category MobileBotnetCAndCDF
      rules action alert
      rules recomended
      enable
    exit
    category BotnetCAndCURLsDF
      rules action alert
      rules percent 50
      enable
    exit
    category IPReputationDF
      rules action alert
      rules recomended
      enable
    exit
    category IoTURLsDF
      rules action alert
      rules percent 15
      enable
    exit
    category MaliciousHashDF
      rules action alert
      rules count 1
      enable
    exit
    category MobileMaliciousHashDF
      rules action alert
      rules count 1
      enable
    exit
    category PSMSTrojanDF
      rules action alert
      rules count 1
      enable
    exit
    category PhishingURLsDF
      rules action alert
      rules count 1000
      enable
    exit
    category RansomwareURLsDF
      rules action alert
      rules count 1000
      enable
    exit
  exit
exit
```

Назначить сервису IPS-политику для работы и включить его:

```
security ips
  performance max
  policy policy0
  enable
exit
```

Для просмотра информации о загруженном контенте для IPS/IDS можно использовать две следующие команды:

show security ips content-provider:

```
esr-20# show security ips content-provider
 Server: content-provider
               Last MD5 of received files:        c60bd0f10716d3f48e18f24828337135
               Next update: 30 October 2020 00:37:06
```

С помощью этой команды можно узнать, скачивал ли контент-провайдер правила с сервера EDM (по признаку присутствия контрольной суммы md5) и когда по времени устройства планируется следующее обновление.

show security ips counters:

```
esr-20# show security ips counters
-----------------------------------------------
IPS general counters
-----------------------------------------------
Packets decoded by ips engine:               83971
Invalid packets decoded by ips engine:       0
Packets accepted by ips engine:              83977
Packets blocked by ips engine:               0
Packets replaced by ips engine:              0
Alerts generated:                            8
-----------------------------------------------
IPS Decoder engine
-----------------------------------------------
Packets decoded by ips engine:               83971
Bytes decoded by ips engine:                 125677543
Invalid packets decoded by ips engine:       0
IPv4 packets decoded by ips engine:          83971
IPv6 packets decoded by ips engine:          0
TCP packets decoded by ips engine:           75
UDP packets decoded by ips engine:           83891
SCTP packets decoded by ips engine:          0
ICMPv4 packets decoded by ips engine:        5
ICMPv6 packets decoded by ips engine:        0
PPP packets decoded by ips engine:           0
PPPoE packets decoded by ips engine:         0
GRE packets decoded by ips engine:           0
Teredo packets decoded by ips engine:        0
Average packets size decoded by ips engine:  1496
Maximum packets size decoded by ips engine:  1500
-----------------------------------------------
IPS Application Layer
-----------------------------------------------
HTTP Flow decoded by ips engine:             0
FTP Flow decoded by ips engine:              0
FTP-DATA Flow decoded by ips engine:         0
SMTP Flow decoded by ips engine:             0
TLS Flow decoded by ips engine:              0
SSH Flow decoded by ips engine:              0
IMAP Flow decoded by ips engine:             0
SMB Flow decoded by ips engine:              0
DCE/RPC flow over TCP decoded by ips engine: 0
DCE/RPC flow over UDP decoded by ips engine: 0
DNS flow over TCP decoded by ips engine:     0
DNS flow over UDP decoded by ips engine:     0
ENIP flow over TCP decoded by ips engine:    0
ENIP flow over UDP decoded by ips engine:    0
-----------------------------------------------
IPS Flow engine
-----------------------------------------------
TCP Flow decoded by ips engine:              1
UDP Flow decoded by ips engine:              1
ICMPv4 Flow decoded by ips engine:           1
ICMPv6 Flow decoded by ips engine:           0
Failed TCP Flow decoded by ips engine:       0
Failed UDP Flow decoded by ips engine:       1
-----------------------------------------------
IPS TCP engine
-----------------------------------------------
TCP sessions decoded by ips engine:          1
```

```
TCP SYN packets decoded by ips engine:       1
TCP SYN-ACK packets decoded by ips engine:   0
TCP RST packets decoded by ips engine:       0
TCP packets with invalid checksum:           0
TCP packets with wrong thread:               0
Packets with TCP header length too small:    0
TCP packets with invalid options:            0
```

Показывает прошедший трафик через IPS/IDS и действия, которые применялись к трафику, а также число срабатываний правил IPS/IDS.

13.11 Настройка сервиса контентной фильтрации

⚠ Данная функция активируется только при наличии лицензии.

Сервис контентной фильтрации предназначен для ограничения доступа к HTTP/HTTPS-сайтам на основании их содержимого. Для каждого сайта определяется принадлежность его к той или иной категории. В качестве базы категорий сайтов используется база Лаборатории Касперского. Для определения категории сайтов ESR отправляет HTTPS-запросы на сервер Лаборатории Касперского по адресу https://ksn-vt.kaspersky-labs.com.

Работа сервиса контентной фильтрации основана на системе предотвращения вторжений (IPS) и настраивается как пользовательские правила IPS.

13.11.1 Алгоритм базовой настройки

Шаг	Описание	Команда	Ключи
1	Определить IP-адрес DNS-сервера, используемого для разрешения DNS-имен.	**esr(config)# domain nameserver <IP>**	<IP> – IP-адрес используемого DNS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
2	Включить разрешение DNS-имен на устройстве.	**esr(config)# domain lookup enable**	
3	Создать политику безопасности IPS/IDS.	**esr(config)# security ips policy <NAME>**	<NAME> – имя политики безопасности, задаётся строкой до 31 символа.
4	Задать описание политики (необязательно).	**esr(config-ips-policy)# description <DESCRIPTION>**	<DESCRIPTION> – описание задаётся строкой до 255 символов.

Шаг	Описание	Команда	Ключи
5	Создать списки IP-адресов, которые будут использоваться при фильтрации.	**esr (config)# object-group network <WORD>** **esr (config-object-group-network)# ip prefix <ADDR/LEN> [unit <ID>]**	<WORD> – имя сервера, задаётся строкой до 31 символов. <ADDR/LEN> – подсеть, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. <ID> – номер юнита, принимает значения [1..4].
6	Задать профиль IP-адресов, которые будет защищать IPS/IDS.	**esr(config-ips-policy)# protect network-group <OBJ-GROUP-NETWORK_NAME>**	<OBJ-GROUP-NETWORK-NAME> – имя профиля защищаемых IP-адресов, задается строкой до 31 символов.
7	Задать профиль IP-адресов, внешних для IPS/IDS (необязательно).	**esr(config-ips-policy)# external network-group <OBJ-GROUP-NETWORK_NAME>**	<OBJ-GROUP-NETWORK-NAME> – имя профиля внешних IP-адресов, задается строкой до 31 символов.
8	Создать профиль категорий контентной фильтрации.	**esr(config)# object-group content-filter <NAME>**	<NAME> – имя профиля контентной фильтрации, задается строкой до 31 символа.
9	Задать описание профиля категорий контентной фильтрации (необязательно).	**esr(config-object-group-content-filter)# description <DESCRIPTION>**	<DESCRIPTION> – описание задаётся строкой до 255 символов.
10	Задать поставщика категорий контентной фильтрации.	**esr(config-object-group-content-filter)# vendor <CONTENT-FILTER-VENDOR>**	<CONTENT-FILTER-VENDOR> – название поставщика категорий контентной фильтрации. В текущей версии ПО в качестве поставщика категорий контентной фильтрации может выступать только Лаборатория Касперского.
11	Задать необходимые категории контентной фильтрации.	**esr(config-object-group-cf-kaspersky)# category <CATEGORY>**	<CATEGORY> – имя категории. Описание доступных категорий приведено в справочнике команд.

Шаг	Описание	Команда	Ключи
12	Перейти в режим конфигурирования IPS/IDS.	**esr(config)# security ips**	
13	Назначить политику безопасности IPS/IDS.	**esr(config-ips)# policy <NAME>**	<NAME> – имя политики безопасности, задаётся строкой до 32 символов.
14	Использовать все ресурсы ESR для IPS/IDS (необязательно).	**esr(config-ips)# perfomance max**	По умолчанию для IPS/IDS отдается половина доступных ядер процессора.

Шаг	Описание	Команда	Ключи
15	Задать параметры удаленного сервера для отправки статистики работы сервиса IPS/IDS в формате EVE (elasticsearch) (необязательно).	**esr(config-ips)# logging remote-server { <ADDR> | <IPV6-ADDR> } [<TRANSPORT>] [<PORT>] [source-address { <SRC-ADDR> | <IPV6-SRC-ADDR> }]**	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <TRANSPORT> – протокол передачи данных, по умолчанию – UDP, принимает значения: • TCP – передача данных осуществляется по протоколу TCP; • UDP – передача данных осуществляется по протоколу UDP; <PORT> – номер TCP/UDP-порта, опциональный параметр, принимает значения [1..65535], по умолчанию 514; <SRC-ADDR> – IPv4-адрес маршрутизатора, который будет использоваться в качестве IP-адреса источника в отправляемых syslog-пакетах, по умолчанию – IPv4-адрес интерфейса, с которого отправляются пакеты; <IPV6-SRC-ADDR> – IPv6-адрес маршрутизатора, который будет использоваться в качестве IPv6-адреса источника в отправляемых syslog-пакетах, по умолчанию – IPv6-адрес интерфейса, с которого отправляются пакеты.
16	Установить интервал отправки статистики работы сервиса IPS/IDS в формате EVE (elasticsearch) (необязательно).	**esr(config-ips)# logging update-interval <INTERVAL>**	<INTERVAL> – интервал отправки статистики работы сервиса IPS/IDS, задаётся в минутах.

Шаг	Описание	Команда	Ключи
17	Настроить параметры кэширования сервиса контентной фильтрации.	**esr(config-ips)# content-filter**	
18	Установить количество хранящихся в кэше записей.	**esr(config-ips-content-filter)# uri cache-size <NUMBER>**	<NUMBER> – количество записей, хранящихся в кэше, принимает значения [1..32768].
19	Установить среднее время, в течение которого запись URI будет действительной в кэше.	**esr(config-ips-content-filter)# uri reachable-interval <DAYS>**	<DAYS> – количество дней, в течение которых запись будет действительной, принимает значения [1..365].
20	Активировать IPS/IDS.	**esr(config-ips)# enable**	
21	Активировать IPS/IDS на интерфейсе.	**esr(config-if-gi)# service-ips enable**	
22	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 31 символов.
23	Задать описание набора пользовательских правил (необязательно).	**esr(config-ips-category)# description <DESCRIPTION>**	<DESCRIPTION> – описание задаётся строкой до 255 символов.
24	Создать правило и перейти в режим конфигурирования правила.	**esr(config-ips-category)# rule <ORDER>**	<ORDER> – номер правила, принимает значения [1..512].
25	Задать описание правила (необязательно).	**esr(config-ips-category-rule)# description <DESCRIPTION>**	<DESCRIPTION> – описание задаётся строкой до 255 символов.

Шаг	Описание	Команда	Ключи
26	Указать действие данного правила.	**esr(config-ips-category-rule)# action { alert | reject | pass | drop }**	• alert – прохождение трафика разрешается, и сервис IPS/IDS генерирует сообщение; • reject – прохождение трафика запрещается. Если это TCP-трафик, отправителю и получателю посылается пакет TCP-RESET, для остального типа трафика посылается пакет ICMP-ERROR. Сервис IPS/IDS генерирует сообщение; • pass – прохождение трафика разрешается; • drop – прохождение трафика запрещается, и сервис IPS/IDS генерирует сообщение.
27	Установить в качестве протокола HTTP/HTTPS.	**esr(config-ips-category-rule)# protocol { http | tls }**	• http – анализируется HTTP-трафик. • tls – анализируется HTTP-трафик, защищенный TLS-шифрованием.

Шаг	Описание	Команда	Ключи
28	Установить IP-адреса отправителя, для которых должно срабатывать правило.	**esr(config-ips-category-rule)# source-address {ip <ADDR> | ip-prefix <ADDR/LEN> | object-group <OBJ_GR_NAME> | policy-object-group { protect | external } | any }**	<ADDR> – IP-адрес отправителя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <ADDR/LEN> – IP-подсеть отправителя, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и LEN принимает значения [1..32]. <OBJ_GR_NAME> – имя профиля IP-адресов, который содержит IP-адреса отправителя, задаётся строкой до 31 символа. • protect – устанавливает в качестве адресов отправителя protect-адреса, определенные в политике IPS/IDS; • external – устанавливает в качестве адресов отправителя external-адреса. определенные в политике IPS/IDS. При указании значения «any» правило будет срабатывать для любого IP-адреса отправителя.
29	Установить номера TCP/UDP-портов отправителя, для которых должно срабатывать правило.	**esr(config-ips-category-rule)# source-port {any | <PORT> | object-group <OBJ-GR-NAME> }**	<PORT> – номер TCP/UDP-порта отправителя, принимает значения [1..65535]. <OBJ_GR_NAME> – имя профиля TCP/UDP портов отправителя, задаётся строкой до 31 символа. При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта отправителя.

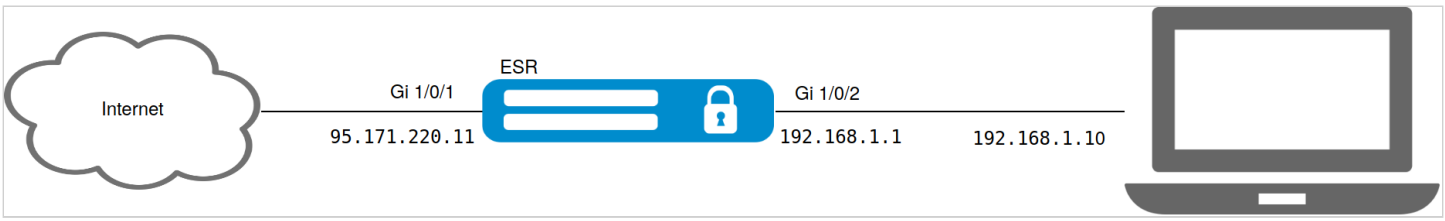
Шаг	Описание	Команда	Ключи
30	Установить IP-адреса получателя, для которых должно срабатывать правило.	**esr(config-ips-category-rule)# destination-address {ip <ADDR> | ip-prefix <ADDR/LEN> | object-group <OBJ_GR_NAME> | policy-object-group { protect | external } | any }**	<<ADDR> – IP-адрес получателя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <ADDR/LEN> – IP-подсеть получателя, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и LEN принимает значения [1..32]. < OBJ_GR_NAME> – имя профиля IP-адресов, который содержит IP-адреса получателя, задаётся строкой до 31 символа. • protect – устанавливает в качестве адресов получателя protect-адреса, определенные в политике IPS/IDS; • external – устанавливает в качестве адресов получателя external-адреса, определенные в политике IPS/IDS. При указании значения «any» правило будет срабатывать для любого IP-адреса получателя.
32	Установить номера TCP/UDP-портов получателя, для которых должно срабатывать правило. Обычно для протокола http используется значение TCP-порт 80. В случаях когда когда используются web-сервера на нестандартных портах надо пописывать эти порты тоже.	**esr(config-ips-category-rule)# destination-port {any | <PORT> | object-group <OBJ-GR-NAME> }**	<PORT> – номер TCP/UDP-порта получателя, принимает значения [1..65535]. <OBJ_GR_NAME> – имя профиля TCP/UDP портов получателя, задаётся строкой до 31 символа. При указании значения «any» правило будет срабатывать для любого TCP/UDP-порта получателя.

Шаг	Описание	Команда	Ключи
33	Установить направление потока трафика, для которого должно срабатывать правило.	**esr(config-ips-category-rule)# direction { one-way | round-trip }**	• one-way – трафик передаётся в одну сторону. • round-trip – трафик передаётся в обе стороны.
34	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 128 символов.
35	Назначить профиль категорий контентной фильтрации.	**esr(config-ips-category-rule)# ip { http | tls } content-filter <NAME>**	• http – анализируется HTTP-трафик. • tls – анализируется трафик, защищенный TLS-шифрованием. <NAME> – имя профиля контентной фильтрации задаётся строкой до 31 символа. any – правило будет срабатывать для HTTP/HTTPS-сайтов любой категории.
36	Активировать правило.	**esr(config-ips-category-rule)# enable**	

13.11.2 Пример настройки правил контентной фильтрации

Задача:

Запретить доступ к https-сайтам, относящимся к категориям addictive-substances, addictive-substances narcotics, scam, gambling casino из локальной сети 192.168.1.0/24.



Решение:

На устройстве предварительно должны быть настроены интерфейсы и правила firewall.

Создадим профиль адресов защищаемой локальной сети:

```
esr(config)# object-group network LAN
esr(config-object-group-network)# ip prefix 192.168.1.0/24
esr(config-object-group-network)# exit
```

Настроим на ESR DNS-клиента для разрешения имен источников обновления правил IPS/IDS:

```
esr(config)# domain lookup enable
esr(config)# domain nameserver 8.8.8.8
```

Создадим политику безопасности IPS/IDS:

```
esr(config)# security ips policy OFFICE
esr(config-ips-policy)# description "My Policy"
esr(config-ips-policy)# protect network-group LAN
```

Разрешим работу IPS/IDS на интерфейсе локальной сети gigabitethernet 1/0/2:

```
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# service-ips inline
```

Настроим параметры IPS/IDS и параметры кэширования ответов с облака:

```
esr(config)# security ips
esr(config-ips)# policy OFFICE
esr(config-ips)# enable
esr(config-ips)# content-filter
esr(config-ips-content-filter)# uri cache-size 500
esr(config-ips-content-filter)# uri reachable-interval 3
```

Устройство будет использоваться только как шлюз безопасности, поэтому отдадим сервису IPS/IDS все доступные ресурсы:

```
esr(config-ips)# perfomance max
```

Создадим профиль контентной фильтрации для выбранных категорий:

```
esr(config)# object-group content-filter Black
esr(config-object-group-content-filter)# vendor kaspersky-lab
esr(config-object-group-cf-kaspersky)# category addictive-substances
esr(config-object-group-cf-kaspersky)# category addictive-substances narcotics
esr(config-object-group-cf-kaspersky)# category scam
esr(config-object-group-cf-kaspersky)# category gambling casino
```

Создадим набор пользовательских правил:

```
esr(config)# security ips-category user-defined USER
```

Создадим правило:

```
esr(config-ips-category)# rule 10
esr(config-ips-category-rule)# description "Content-Filter Block"
```

Будем отбрасывать пакеты:

```
esr(config-ips-category-rule)# action drop
```

Настроим сообщение об атаке:

```
esr(config-ips-category-rule)# meta log-message "Corporate policy violation"
```

Укажем тип протокола для правила:

```
esr(config-ips-category-rule)# protocol tls
```

При https-запросах в качестве TCP/UDP-порта отправителя операционная система использует случайное значение, поэтому требуется указать any:

```
esr(config-ips-category-rule)# source-port any
```

В качестве TCP/UDP-порта назначения для протокола http обычно используется 80 порт, но интернет-сайты могут работать и на нестандартных портах, поэтому укажем any:

```
esr(config-ips-category-rule)# destination-port any
```

В качестве адреса получателя может быть любой сайт в интернете:

```
esr(config-ips-category-rule)# destination-address any
```

Запросы к сайтам отправляются из нашей локальной сети:

```
esr(config-ips-category-rule)# source-address policy-object-group protect
```

Зададим направление трафика:

```
esr(config-ips-category-rule)# direction one-way
```

Правило будет срабатывать на категории сайтов, перечисленные в профиле Black:

```
esr(config-ips-category-rule)# ip tls content-filter Black
```

Активируем правило:

```
esr(config-ips-category-rule)# enable
esr(config-ips-category-rule)# exit
esr(config-ips-category-rule)# threshold type both
```

Выведем записи, которые хранятся в кэше:

```
esr# show content-filter cache
URI                                Vendor             Categories                  Time to live
                                                                                  (d,h:m:s)
---------------------------------  -----------------  --------------------------  ------------
rutube.ru                          kaspersky-lab      downloadable-content,       06,23:28:32
                                                      hobbies-recreation,
                                                      media-content
ya.ru                              kaspersky-lab      it-services, searchers      06,23:29:04
vtb.ru                             kaspersky-lab      finance, human-life,        06,23:46:01
                                                      online-banks, payments,
                                                      transactions
```

Команда для очистки кэша:

```
esr# clear content-filter cache
```

14 Управление сертификатами и ключами

- Автоматическое распространение ключей и сертификатов X.509
  - Общее описание инфраструктуры открытых ключей
  - Планирование инфраструктуры открытых ключей
  - Настройка PKI-сервера в роли корневого удостоверяющего центра
    - Алгоритм настройки
    - Пример настройки
  - Настройка PKI-клиента
    - Алгоритм настройки
    - Пример настройки PKI-клиента для подключения к корневому удостоверяющему центру
  - Процесс автоматического перевыпуска сертификата PKI-клиента
  - Процесс автоматического перевыпуска сертификата PKI-сервера
- Ручная генерация и распространение ключей и сертификатов X.509
  - Алгоритм генерации ключей и запросов на сертификацию
  - Пример ручного выпуска сертификата через внешний удостоверяющий центр

14.1 Автоматическое распространение ключей и сертификатов X.509

14.1.1 Общее описание инфраструктуры открытых ключей

Инфраструктура открытых ключей (Public Key Infrastructure, PKI) – комплекс средств, мер и политик, обеспечивающих работу систем на базе алгоритмов шифрования с открытым ключом.

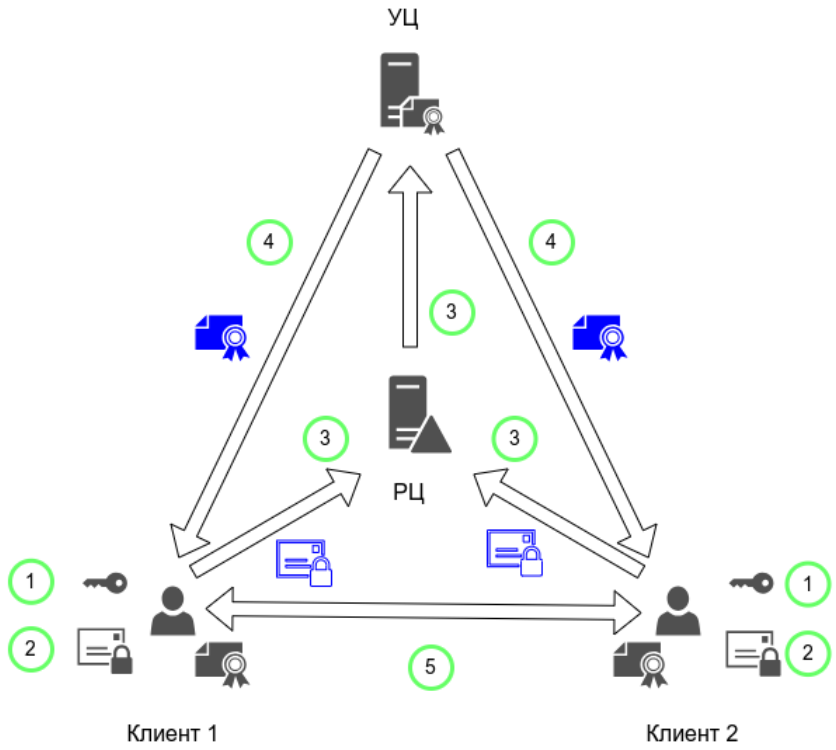
К участникам PKI обычно относятся:

- Удостоверяющий центр (УЦ),
- Регистрационный центр (РЦ),
- Клиент.

В процессе взаимодействия участников PKI появляются и используются следующие объекты:

- Приватный ключ,
- Публичный ключ,
- Запрос на сертификацию,
- Сертификат,
- Список отозванных сертификатов.

Схематично основные процедуры в инфраструктуре открытых ключей можно описать следующим образом:



1. Клиент генерирует у себя приватный ключ.
2. Клиент формирует запрос на сертификацию, включающий в себя публичный ключ, парный к раннее сгенерированному приватному ключу, информацию о владельце приватного ключа и запрашиваемые опции, которые затем могут быть добавлены в выпускаемый сертификат.
3. Клиент доставляет запрос на сертификацию в удостоверяющий центр. При наличии в структуре PKI регистрационного центра запрос от клиента будет приходить на него и после валидации будет уходить в удостоверяющий центр.
4. Удостоверяющий центр на основании клиентского запроса на сертификацию выпишет сертификат, содержащий всю клиентскую информацию и информацию о самом УЦ. Сам сертификат будет подписан приватным ключом УЦ, тем самым данные в клиентском сертификате не смогут быть изменены третьей стороной. От УЦ сертификат передается клиенту.
5. Теперь клиенты могут, используя свой приватный ключ, подписывать данные в рамках используемых процессов (в нашем случае – сетевых протоколов) при отправке и валидировать данные при помощи публичного сертификата на приёме.

14.1.2 Планирование инфраструктуры открытых ключей

Сервисные маршрутизаторы ESR могут принимать участие в структуре PKI в качестве корневого удостоверяющего центра и клиента PKI. Перед развертыванием инфраструктуры PKI крайне важно её спланировать для обеспечения безопасности и стабильной работы.

Основные рекомендации по планированию инфраструктуры открытых ключей:

1. Определите роли устройств в структуре PKI.
2. Определите схему именования сертификатов.
3. Определите политику доступа к центру сертификации и механизмы ограничения доступа к нему от недоверенных клиентов.
4. Обеспечьте актуальность времени на всех хостах, используемых в структуре PKI.

14.1.3 Настройка PKI-сервера в роли корневого удостоверяющего центра

Базовый вариант настройки PKI-сервера – корневой удостоверяющий центр, работающий на самоподписанных сертификатах, который напрямую обслуживает запросы конечных клиентов.

Изменение отличительного имени сертификата удостоверяющего центра приводит к перегенерации приватного ключа и сертификата PKI-сервера и очистке базы выписанных сертификатов. Требуется заранее, на этапе планирования структуры PKI, определиться с идентификацией владельца удостоверяющего центра и после ввода удостоверяющего центра в эксплуатацию не менять эти настройки.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Настроить NTP-клиент согласно разделу Алгоритм настойки NTP. Маршрутизатор должен получать точное время от NTP-сервера или NTP-пира, либо доверять локально настроенному времени с включенным режимом NTP Master.		
2	Перейти в режим настройки PKI-клиента, который будет использоваться в настройках PKI-сервера как источник самоподписанных сертификатов.	**esr(config)# crypto pki trustpoint <TRUSTPOINT>**	<TRUSTPOINT> – имя PKI-клиента, задаётся строкой от 1 до 31 символа.
3	Перейти в режим настройки отличительного имени сертификата – набора атрибутов, уникально описывающих удостоверяющий центр.	**esr(config-trustpoint)# subject-name**	
4	Указать код страны (необязательно).	**esr(config-trustpoint-subject-name)# country <COUNTRY>**	<COUNTRY> – код страны, задаётся строкой длиной 2 символа. Рекомендуется использовать двухбуквенные обозначения стран "alpha-2" из стандарта ISO 3166-1.
5	Указать название штата, области или провинции (необязательно).	**esr(config-trustpoint-subject-name)# state <STATE>**	<STATE> – название штата, области или провинции, задаётся строкой от 1 до 128 символов.

Шаг	Описание	Команда	Ключи
6	Указать название населенного пункта или его территориальной единицы (необязательно).	**esr(config-trustpoint-subject-name)# locality <LOCATION>**	<LOCATION> – название населенного пункта или его территориальной единицы, задаётся строкой от 1 до 128 символов.
7	Указать название организации (необязательно).	**esr(config-trustpoint-subject-name)# organization <ORGANIZATION>**	<ORGANIZATION> – название организации, задаётся строкой от 1 до 64 символов.
8	Указать подразделение организации (необязательно).	**esr(config-trustpoint-subject-name)# organization-unit <ORGANIZATION-UNIT>**	<ORGANIZATION-UNIT> – название подразделения организации, задаётся строкой от 1 до 64 символов.
9	Указать общее имя сертификата.	**esr(config-trustpoint-subject-name)# common-name <COMMON-NAME>**	<COMMON-NAME> – общее имя, задаётся строкой от 1 до 64 символов. Как правило в качестве общего имени сертификата удостоверяющего центра используется имя домена, который обслуживает удостоверяющий центр или юридическое название удостоверяющего центра.
10	Перейти в режим настройки альтернативных имен сертификата (необязательно).	**esr(config-trustpoint)# subject-alt-name**	
11	Указать IP-адрес в качестве альтернативного имени сертификата (необязательно).	**esr(config-trustpoint-san)# ipv4 <ADDR>**	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
		esr(config-trustpoint-san)# ipv6 <IPV6-ADDR>	<IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
12	Указать полное доменное имя хоста в качестве альтернативного имени сертификата (необязательно).	**esr(config-trustpoint-san)# dns <NAME>**	<NAME> – полное доменное имя хоста (FQDN), задается строкой от 1 до 235 символов. Пример записи доменного имени – router.example.loc.

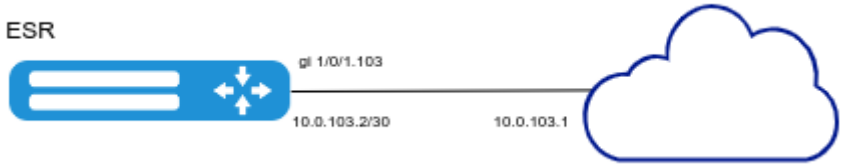
Шаг	Описание	Команда	Ключи
13	Указать адрес электронной почты в качестве альтернативного имени сертификата (необязательно).	**esr(config-trustpoint-san)# email <EMAIL>**	<EMAIL> – адрес электронной почты, задается строкой от 6 до 254 символов. Пример записи электронной почты – router@example.loc.
14	Перейти в режим настройки механизма выпуска сертификата. Для PKI-клиента, выпускающего самоподписанные сертификаты укажем тип "selfsigned".	**esr(config-trustpoint)# enrollment selfsigned**	
15	Указать время жизни самоподписанных сертификатов (необязательно).	**esr(config-trustpoint-enrollment-selfsigned)# lifetime <DAYS>**	<DAYS> – количество дней, принимает значения в диапазоне [1..3650]. Значение по умолчанию: 3650.
16	Указать назначение генерируемых сертификатов. Для PKI-клиента, используемого в настройках PKI-сервера в качестве источника самоподписанных сертификатов необходимо указать значение "root-ca".	**esr(config-trustpoint)# usage root-ca**	
17	Указать экземпляр VRF, в котором будет работать PKI-клиент (необязательно). Если планируется работа PKI-сервера в определенном VRF, PKI-клиент с самоподписанными сертификатами также требуется вынести в этот VRF.	**esr(config-trustpoint)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.
18	Включить PKI-клиент.	**esr(config-trustpoint)# enable**	
19	Перейти в режим настройки PKI-сервера.	**esr(config)# crypto pki server**	
20	Указать имя раннее настроенного PKI-клиента, который будет использоваться в настройках PKI-сервера как источник самоподписанных сертификатов.	**esr(config-pki-server)# trustpoint <TRUSTPOINT>**	<TRUSTPOINT> – имя PKI-клиента, задаётся строкой от 1 до 31 символа.
21	Указать экземпляр VRF, в котором будет работать PKI-сервер (необязательно).	**esr(config-pki-server)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.

Шаг	Описание	Команда	Ключи
22	Указать IP-адрес или сетевой интерфейс, который будет будет прослушиваться PKI-сервером для обработки входящих запросов (необязательно). В случае, если настройка не будет указана PKI-сервер будет принимать запросы на всех настроенных IP-интерфейсах маршрутизатора.	**esr(config-pki-server)# source-address <ADDR>**	<ADDR> – IP-адрес, назначенный на локальном сетевом интерфейсе маршрутизатора, на котором PKI-сервер будет слушать входящие подключения, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
		esr(config-pki-server)# source-interface <IF>	<IF> – интерфейс или туннель, на котором PKI-сервер будет слушать входящие подключения.
23	Указать challenge-password, который будет использован для аутентификации PKI-клиентов (необязательно).	**esr(config-pki-server)# challenge-password { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<CLEAR-TEXT> – пароль, задаётся строкой от 8 до 32 символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 32 байт (от 16 до 64 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).
24	Указать время жизни выписываемых клиентам сертификатов в днях (необязательно).	**esr(config-pki-server)# lifetime <DAYS>**	<DAYS> – количество дней, принимает значения в диапазоне [1..3650]. Значение по умолчанию: 365.
25	Включить PKI-сервер.	**esr(config-pki-server)# enable**	

Пример настройки

Задача:

Настроить на маршрутизаторе PKI-сервер в роли корневого удостоверяющего центра. Время жизни сертификата удостоверяющего центра должно быть ограничено одним годом, а время жизни клиентских сертификатов должно быть ограничено двумя неделями.



В качестве начальной конфигурации на маршрутизаторе уже настроен сетевой интерфейс в сторону Интернет-провайдера, прописан шлюз по умолчанию и настроена зона безопасности. Шлюз Интернет-провайдера также может служить источником синхронизации времени по протоколу NTP.

```
hostname ESR.CA

security zone WAN
exit

interface gigabitethernet 1/0/1.103
  security-zone WAN
  ip address 10.0.103.2/30
exit

ip route 0.0.0.0/0 10.0.103.1
```

Решение:

Настроим NTP-клиент на получение точного времени от шлюза Интернет-провайдера:

```
ESR.CA(config)# ntp enable
ESR.CA(config)# ntp server 10.0.103.1
ESR.CA(config-ntp-server)# exit
ESR.CA(config)#
```

Применим конфигурацию на маршрутизаторе и дождемся успешной синхронизации времени по протоколу NTP:

> ⚠ Если произвести настройку подключения к NTP-серверу одновременно с настройкой PKI-сервера, сгенерированные на этапе запуска PKI-сервера служебные файлы и сертификаты могут содержать некорректные дату и время, что приведет к ошибкам в дальнейшей работе инфраструктуры PKI.

```
ESR.CA(config)# end
Warning: you have uncommitted configuration changes.
ESR.CA# commit
Configuration has been successfully applied and saved to flash. Commit timer started, changes
will be reverted in 600 seconds.
ESR.CA# confirm
Configuration has been confirmed. Commit timer canceled.
ESR.CA#
ESR.CA# sh ntp peers
Clock is synchronized, stratum 6, reference is 10.0.103.1
    remote                                          vrf          refid             st   t
when   poll   reach   delay      offset     jitter
-   ---------------------------------------------   ----------   ---------------   --   -
----   ----   -----   --------   --------   --------
*   10.0.103.1                                                   127.127.1.0       5    u
16     64     37      0.601      8.533      0.019
ESR.CA#
```

Перейдем к настройке PKI-клиента, который будет использоваться в качестве источника самоподписанных сертификатов для PKI-сервера:

```
ESR.CA(config)# crypto pki trustpoint ROOT_CA
ESR.CA(config-trustpoint)#
```

Перейдем в раздел настройки отличительного имени сертификата удостоверяющего центра. Настроим те атрибуты, которые позволят однозначно идентифицировать удостоверяющий центр:

```
ESR.CA(config-trustpoint)# subject-name
ESR.CA(config-trustpoint-subject-name)# country RU
ESR.CA(config-trustpoint-subject-name)# state Moscow
ESR.CA(config-trustpoint-subject-name)# locality Moscow
ESR.CA(config-trustpoint-subject-name)# organization Company
ESR.CA(config-trustpoint-subject-name)# common-name ca.company.loc
ESR.CA(config-trustpoint-subject-name)# exit
ESR.CA(config-trustpoint)#
```

Перейдем в раздел настройки альтернативных имен сертификата. Укажем в качестве альтернативных имен IP-адрес и полное доменное имя:

```
ESR.CA(config-trustpoint)# subject-alt-name
ESR.CA(config-trustpoint-san)# ipv4 10.0.103.2
ESR.CA(config-trustpoint-san)# dns ca.company.loc
ESR.CA(config-trustpoint-san)# exit
ESR.CA(config-trustpoint)#
```

Перейдем в режим настройки механизма выпуска сертификата. Для PKI-клиента, выпускающего самоподписанные сертификаты, укажем тип "selfsigned". В нем настроим время жизни самоподписанных сертификатов:

```
ESR.CA(config-trustpoint)# enrollment selfsigned
ESR.CA(config-trustpoint-enrollment-selfsigned)# lifetime 365
ESR.CA(config-trustpoint-enrollment-selfsigned)# exit
ESR.CA(config-trustpoint)#
```

Укажем назначение генерируемых сертификатов. Для PKI-клиента, используемого в настройках PKI-сервера, в качестве источника самоподписанных сертификатов необходимо указать значение "root-ca":

```
ESR.CA(config-trustpoint)# usage root-ca
ESR.CA(config-trustpoint)#
```

Включим PKI-клиент:

```
ESR.CA(config-trustpoint)# enable
ESR.CA(config-trustpoint)# exit
ESR.CA(config)#
```

Перейдем к настройке PKI-сервера:

```
ESR.CA(config)# crypto pki server
ESR.CA(config-pki-server)#
```

Укажем имя ранее настроенного PKI-клиента, который будет использоваться в настройках PKI-сервера как источник самоподписанных сертификатов:

```
ESR.CA(config-pki-server)# trustpoint ROOT_CA
ESR.CA(config-pki-server)#
```

Привяжем PKI-сервер к адресу сетевого интерфейса, смотрящего в сторону Интернет-провайдера:

```
ESR.CA(config-pki-server)# source-interface gi 1/0/1.103
ESR.CA(config-pki-server)#
```

Зададим challenge-password, для корректного обращения к удостоверяющему центру PKI-клиенты должны использовать правильный challenge-password.

```
ESR.CA(config-pki-server)# challenge-password StR0nnGP+ss
ESR.CA(config-pki-server)#
```

Включим PKI-сервер:

```
ESR.CA(config-pki-server)# enable
ESR.CA(config-pki-server)# exit
ESR.CA(config)#
```

Добавим пару зон безопасности и правило, разрешающее прохождение входящего на PKI-сервер трафика:

```
ESR.CA(config)# security zone-pair WAN self
ESR.CA(config-security-zone-pair)# rule 10
ESR.CA(config-security-zone-pair-rule)# description "Allow access to PKI-server from WAN"
ESR.CA(config-security-zone-pair-rule)# match protocol tcp
ESR.CA(config-security-zone-pair-rule)# match destination-port port-range 80
ESR.CA(config-security-zone-pair-rule)# match destination-address address-range 10.0.103.2
ESR.CA(config-security-zone-pair-rule)# action permit
ESR.CA(config-security-zone-pair-rule)# enable
ESR.CA(config-security-zone-pair-rule)# exit
ESR.CA(config-security-zone-pair)# exit
ESR.CA(config)#
```

Применим конфигурацию на маршрутизаторе:

```
ESR.CA(config)# end
Warning: you have uncommitted configuration changes.
ESR.CA# commit
Configuration has been successfully applied and saved to flash. Commit timer started, changes
will be reverted in 600 seconds.
ESR.CA# confirm
Configuration has been confirmed. Commit timer canceled.
ESR.CA#
```

В результате получим запущенный корневой удостоверяющий центр, готовый к обслуживанию клиентских запросов.

В команде **show crypto pki trustpoints** можно увидеть PKI-клиент ROOT_CA, готовый к работе, а добавив его имя в конце команды, можно более подробно рассмотреть его текущий статус:

```
ESR.CA# show crypto pki trustpoints
Name              Enrollment   Usage     Subject name                      Status
Next action
---------------   ----------   -------   -------------------------------   ------------------
--------------------
ROOT_CA           selfsigned   root-ca   CN=ca.company.loc/O=Company/L=   Ready
2026-12-17 08:59:16
                                         Moscow/ST=Moscow/C=RU

ESR.CA# show crypto pki trustpoints ROOT_CA
Name:               ROOT_CA
Usage:              root-ca
Subject name:       CN=ca.company.loc/O=Company/L=Moscow/ST=Moscow/C=RU
Enrollment:         selfsigned
Status:             Ready
Renew date:         2026-12-17 08:59:16
CRL:                Inactive
ESR.CA#
```

В команде **show crypto pki server** можно увидеть fingerprint сертификата удостоверяющего центра, который необходимо использовать в клиентах PKI совместно с установленным challenge-password для корректной авторизации:

```
ESR.CA# show crypto pki server
Status:                     Enabled
Associated trustpoint:      ROOT_CA
Lifetime days:              14
Certificate fingerprint:    A2:0C:10:C7:0E:06:3A:2F:EE:5F:C2:72:39:36:31:0A
Source:                     10.0.103.2
Last issued serial number: --
Challenge password:         Active
Shadow:                     Inactive
ESR.CA#
```

14.1.4 Настройка PKI-клиента

⚠ Изменение отличительного имени клиентского сертификата или URL подключения к PKI-серверу приводит к немедленному перезапросу нового сертификата у удостоверяющего центра.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим настройки PKI-клиента.	**esr(config)# crypto pki trustpoint <TRUSTPOINT>**	<TRUSTPOINT> – имя PKI-клиента, задаётся строкой от 1 до 31 символа.
2	Перейти в режим настройки отличительного имени сертификата – набора атрибутов, уникально описывающих владельца сертификата.	**esr(config-trustpoint)# subject-name**	
3	Указать код страны (необязательно).	**esr(config-trustpoint-subject-name)# country <COUNTRY>**	<COUNTRY> – код страны, задаётся строкой длиной 2 символа. Рекомендуется использовать двухбуквенные обозначения стран "alpha-2" из стандарта ISO 3166-1.
4	Указать название штата, области или провинции (необязательно).	**esr(config-trustpoint-subject-name)# state <STATE>**	<STATE> – название штата, области или провинции, задаётся строкой от 1 до 128 символов.
5	Указать название населенного пункта или его территориальной единицы (необязательно).	**esr(config-trustpoint-subject-name)# locality <LOCATION>**	<LOCATION> – название населенного пункта или его территориальной единицы, задаётся строкой от 1 до 128 символов.
6	Указать название организации (необязательно).	**esr(config-server-subject-name)# organization <ORGANIZATION>**	<ORGANIZATION> – название организации, задаётся строкой от 1 до 64 символов.
7	Указать подразделение организации (необязательно).	**esr(config-trustpoint-subject-name)# organization-unit <ORGANIZATION-UNIT>**	<ORGANIZATION-UNIT> – название подразделения организации, задаётся строкой от 1 до 64 символов.

Шаг	Описание	Команда	Ключи
8	Указать общее имя сертификата.	**esr(config-trustpoint-subject-name)# common-name <COMMON-NAME>**	<COMMON-NAME> – общее имя, задаётся строкой от 1 до 64 символов. Как правило в качестве общего имени клиентского сертификата используется полное доменное имя хоста, который использует данный клиентский сертификат или ФИО пользователя, использующего клиентский сертификат.
11	Перейти в режим настройки альтернативных имен сертификата (необязательно).	**esr(config-trustpoint)# subject-alt-name**	
12	Указать IP-адрес в качестве альтернативного имени сертификата (необязательно).	**esr(config-trustpoint-san)# ipv4 <ADDR>**	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
		esr(config-trustpoint-san)# ipv6 <IPV6-ADDR>	<IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
13	Указать полное доменное имя хоста в качестве альтернативного имени сертификата (необязательно).	**esr(config-trustpoint-san)# dns <NAME>**	<NAME> – полное доменное имя хоста (FQDN), задается строкой от 1 до 235 символов. Пример записи доменного имени – router.example.loc.
14	Указать адрес электронной почты в качестве альтернативного имени сертификата (необязательно).	**esr(config-trustpoint-san)# email <EMAIL>**	<EMAIL> – адрес электронной почты, задается строкой от 6 до 254 символов. Пример записи электронной почты – router@example.loc.
14	Перейти в режим настройки механизма выпуска сертификата. Для PKI-клиента, выпускающего сертификаты от вышестоящего удостоверяющего центра по протоколу SCEP необходимо указать значение "scep".	**esr(config-trustpoint)# enrollment scep**	

Шаг	Описание	Команда	Ключи
15	Указать URL для подключения к PKI-серверу.	**esr(config-trustpoint-enrollment-scep)# url <URL>**	<URL> – URL для подключения к PKI-серверу, задается в виде "http:// <ADDR>[:<PORT>]/", где: • <ADDR> – IP-адрес или доменное имя PKI-сервера; • <PORT> – порт, на котором запущен PKI-сервер, в случае если используется 80 порт по умолчанию, то настройку можно пропустить. В случае если PKI-сервер расположен на том же маршрутизаторе, на котором настраивается PKI-клиент необходимо указать в URL любой из IP-интерфейсов, которые слушает PKI-сервер.
16	Указать цифровой отпечаток сертификата PKI-сервера, к которому выполняется подключение.	**esr(config-trustpoint-enrollment-scep)# fingerprint <FINGERPRINT>**	<FINGERPRINT> – значение цифровой отпечаток сертификата, полученного при помощи алгоритма MD5. Имеет размер 16 байт и задается в виде HEX-строки длиной 32 символа без разделителей (YYYY...) или 47 символов с двоеточием в роли разделителя (YY:YY:YY...).
17	Указать challenge-password, который будет использован для аутентификации на PKI-сервере (необязательно).	**esr(config-trustpoint-enrollment-scep)# challenge-password { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<CLEAR-TEXT> – пароль, задаётся строкой от 8 до 32 символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 32 байт (от 16 до 64 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).

Шаг	Описание	Команда	Ключи
16	Указать назначение генерируемых сертификатов. Для PKI-клиента, используемого в качестве источника ключевой информации в IPsec-туннелях, необходимо указать значение "ipsec".	**esr(config-trustpoint)# usage ipsec**	
9	Указать экземпляр VRF, в котором будет работать PKI-клиент (необязательно).	**esr(config-trustpoint)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.
10	Указать IP-адрес или сетевой интерфейс, с которого PKI-клиент будет выполнять запросы к удостоверяющему центру (необязательно).	**esr(config-trustpoint)# source-address <ADDR>**	<ADDR> – IP-адрес, назначенный на локальном сетевом интерфейсе маршрутизатора, с которого PKI-клиент будет выполнять запросы, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
		esr(config-trustpoint)# source-interface <IF>	<IF> – интерфейс или туннель, с которого PKI-клиент будет выполнять запросы.
18	Включить PKI-клиент.	**esr(config-trustpoint)# enable**	

Пример настройки PKI-клиента для подключения к корневому удостоверяющему центру

Задача:

Настроить на маршрутизаторе PKI-клиент так, чтобы он успешно подключался к удостоверяющему центру. В качестве удостоверяющего центра рассмотрим полностью настроенный PKI-сервер из предыдущего примера. Помимо настройки отличительного имени сертификата, настроим в качестве альтернативного имени IP-адрес маршрутизатора и его полное доменное имя.



В качестве начальной конфигурации на маршрутизаторе уже настроен сетевой интерфейс в сторону Интернет-провайдера, прописан шлюз по умолчанию и настроена зона безопасности. Шлюз Интернет-провайдера также может служить источником синхронизации времени по протоколу NTP.

```
hostname ESR.CA

security zone WAN
exit

interface gigabitethernet 1/0/1.103
  security-zone WAN
  ip address 10.0.103.2/30
exit

security zone-pair WAN self
  rule 10
    description "Allow access to PKI-server from WAN"
    action permit
    match protocol tcp
    match destination-address address-range 10.0.103.2
    match destination-port port-range 80
    enable
  exit
exit

ip route 0.0.0.0/0 10.0.103.1

ntp enable
ntp server 10.0.103.1
exit

crypto pki server
  challenge-password StR0nnGPass
  subject-name
    common-name ca.company.loc
    organization Company
    locality Moscow
    state Moscow
    country RU
  exit
  lifetime 14
  source-interface gigabitethernet 1/0/1.103
  enable
exit
```

```
hostname ESR.R1

security zone WAN
exit

interface gigabitethernet 1/0/1.113
  security-zone WAN
  ip address 10.0.113.2/30
exit

ip route 0.0.0.0/0 10.0.113.1
```

Решение:

Настроим NTP-клиент на получение точного времени от шлюза Интернет-провайдера:

> Настройка NTP-клиента для работы PKI-клиента не является обязательной, в отличие от конфигурирования PKI-сервера. Но в связи с чувствительностью инфраструктуры открытых ключей к актуальности времени на узлах, использующих выписанные сертификаты, настройка NTP рекомендуется и на клиентской стороне.

```
ESR.R1(config)# ntp enable
ESR.R1(config)# ntp server 10.0.113.1
ESR.R1(config-ntp-server)# exit
ESR.R1(config)#
```

Применим конфигурацию на маршрутизаторе и дождемся успешной синхронизации времени по протоколу NTP:

> Если произвести настройку подключения к NTP серверу одновременно с настройкой PKI-клиента, сгенерированные на этапе запуска PKI-клиента служебные файлы и сертификаты могут содержать некорректные дату и время, что приведет к ошибкам в дальнейшей работе инфраструктуры PKI.

```
ESR.R1(config)# end
Warning: you have uncommitted configuration changes.
ESR.R1# commit
Configuration has been successfully applied and saved to flash. Commit timer started, changes
will be reverted in 600 seconds.
ESR.R1# confirm
Configuration has been confirmed. Commit timer canceled.
ESR.R1#
ESR.R1# sh ntp peers
Clock is synchronized, stratum 6, reference is 10.0.113.1
    remote                                          vrf          refid             st   t
when   poll   reach   delay      offset     jitter
-   ---------------------------------------------   ----------   ---------------   --   -
----   ----   -----   --------   --------   --------
*   10.0.113.1                                                   127.127.1.0       5    u
10     64     37      0.441      0.017      2.344
ESR.R1#
```

Перейдем к настройке PKI-клиента:

```
ESR.R1(config)# crypto pki trustpoint TP_R1
ESR.R1(config-trustpoint)#
```

Перейдем в раздел настройки отличительного имени клиентского сертификата. Настроим те атрибуты, которые позволят однозначно идентифицировать клиента:

```
ESR.R1(config-trustpoint)# subject-name
ESR.R1(config-trustpoint-subject-name)# country RU
ESR.R1(config-trustpoint-subject-name)# state Moscow
ESR.R1(config-trustpoint-subject-name)# locality Moscow
ESR.R1(config-trustpoint-subject-name)# organization Company
ESR.R1(config-trustpoint-subject-name)# common-name r1.company.loc
ESR.R1(config-trustpoint-subject-name)# exit
ESR.R1(config-trustpoint)#
```

Перейдем в раздел настройки альтернативных имен сертификата. Укажем в качестве альтернативных имен IP-адрес и полное доменное имя:

```
ESR.R1(config-trustpoint)# subject-alt-name
ESR.R1(config-trustpoint-san)# ipv4 10.0.113.2
ESR.R1(config-trustpoint-san)# dns r1.company.loc
ESR.R1(config-trustpoint-san)# exit
ESR.R1(config-trustpoint)#
```

Перейдем в режим настройки механизма выпуска сертификата. Для PKI-клиента, выпускающего сертификаты от вышестоящего удостоверяющего центра по протоколу SCEP необходимо указать значение "scep":

```
ESR.R1(config-trustpoint)# enrollment scep
ESR.R1(config-trustpoint-enrollment-scep)#
```

Укажем URL подключения к удостоверяющему центру:

```
ESR.R1(config-trustpoint-enrollment-scep)# url http://10.0.103.2/
ESR.R1(config-trustpoint-enrollment-scep)#
```

Укажем цифровой отпечаток сертификата удостоверяющего центра, при несовпадении настроенного в конфигурации PKI-клиента отпечатка с отпечатком сертификата, которым представится сам удостоверяющий центр процесс выпуска сертификата будет прерван. На сервисных маршрутизаторах ESR получить цифровой отпечаток сертификата удостоверяющего центра можно из вывода команды **show crypto pki server**:

```
ESR.R1(config-trustpoint-enrollment-scep)# fingerprint
A2:0C:10:C7:0E:06:3A:2F:EE:5F:C2:72:39:36:31:0A
ESR.R1(config-trustpoint-enrollment-scep)#
```

Зададим challenge-password для корректного обращения к удостоверяющему центру:

```
ESR.R1(config-trustpoint-enrollment-scep)# challenge-password StR0nnGP+ss
ESR.R1(config-trustpoint-enrollment-scep)# exit
ESR.R1(config-trustpoint)#
```

Укажем назначение генерируемых сертификатов. Для PKI-клиента, используемого в качестве источника ключевой информации в IPsec-туннелях, необходимо указать значение "ipsec".

```
ESR.R1(config-trustpoint)# usage ipsec
ESR.R1(config-trustpoint)#
```

Привяжем PKI-клиент к адресу сетевого интерфейса, смотрящего в сторону Интернет-провайдера:

```
ESR.R1(config-trustpoint)# source-interface gi 1/0/1.113
ESR.R1(config-trustpoint)#
```

Включим PKI-клиент:

```
ESR.R1(config-trustpoint)# enable
ESR.R1(config-trustpoint)# exit
ESR.R1(config)#
```

Поскольку трафик PKI-клиента исходящий, дополнительных правил фильтрации в Zone-Based Firewall добавлять не требуется.

Применим конфигурацию на маршрутизаторе:

```
ESR.R1(config)# end
Warning: you have uncommitted configuration changes.
ESR.R1# commit
Configuration has been successfully applied and saved to flash. Commit timer started, changes
will be reverted in 600 seconds.
ESR.R1# confirm
Configuration has been confirmed. Commit timer canceled.
ESR.R1#
```

В результате получим настроенный PKI-клиент, который сразу после запуска обратится к удостоверяющему центру за выпуском сертификата. Отследить состояние настроенных PKI-клиентов можно командой **show crypto pki trustpoints**:

```
ESR.R1# show crypto pki trustpoints
Name              Enrollment   Usage     Subject name                      Status
Next action
---------------   ----------   -------   -------------------------------   ------------------
--------------------
TP_R1             scep         ipsec     CN=r1.company.loc/O=Company/L=    Ready
2026-03-12 11:40:00
                                         Moscow/ST=Moscow/C=RU

ESR.R1#
```

Более подробную информацию о PKI-клиенте можно посмотреть, если выполнить команду **show crypto pki trustpoints** с указанием имени PKI-клиента:

```
ESR.R1# show crypto pki trustpoints TP_R1
Name:                TP_R1
Usage:               ipsec
Subject name:        CN=r1.company.loc/O=Company/L=Moscow/ST=Moscow/C=RU
Enrollment:          scep
Challenge password: Active
Status:              Ready
Renew date:          2026-03-12 11:40:00
CRL:                 Active
CRL status:          Exist
CRL renew date:      2026-03-01 08:59:16
ESR.R1#
```

14.1.5 Процесс автоматического перевыпуска сертификата PKI-клиента

При успешном получении сертификата от удостоверяющего центра PKI-клиент вычитывает период действия сертификата и за 20% времени до его истечения планирует процедуру перевыпуска нового сертификата (certificate auto-enroll). Дата запланированного перевыпуска сертификата соответствующего PKI-клиента присутствует в графе "Renew date" вывода команды **show crypto pki trustpoints** с указанием имени конкретного PKI-клиента:

```
ESR.R1# show crypto pki trustpoints TP_R1
Name:                TP_R1
Enrollment:          SCEP
Subject name:        CN=r1.company.loc/O=Company/L=Moscow/ST=Moscow/C=RU
Challenge password: Active
Status:              Ready
Renew date:          2025-11-02 11:35:39
ESR.R1#
```

При наступлении этого времени PKI-клиент запустит процедуру перевыпуска сертификата и в случае успеха заменит текущий сертификат на новый. На это укажет как факт смены запланированной даты перевыпуска сертификата, так и новый серийный номер сертификата:

```
ESR.R1# show crypto pki trustpoints TP_R1 cert | include "Serial"
Serial:
85:71:EC:28:6C:C8:4E:23:B2:03:03:2F:4D:DF:B8:63
ESR.R1# show crypto pki trustpoints TP_R1
Name:                TP_R1
Usage:               ipsec
Subject name:        CN=r1.company.loc/O=Company/L=Moscow/ST=Moscow/C=RU
Enrollment:          scep
Challenge password: Active
Status:              Ready
Renew date:          2026-03-12 11:40:00
CRL:                 Active
CRL status:          Exist
CRL renew date:      2026-03-01 08:59:16
ESR.R1#
```

```
ESR.R1# show date
"2025-11-02 11:35:46"
ESR.R1# show crypto pki trustpoints TP_R1
Name:                TP_R1
Usage:               ipsec
Subject name:        CN=r1.company.loc/O=Company/L=Moscow/ST=Moscow/C=RU
Enrollment:          scep
Challenge password: Active
Status:              Ready
Renew date:          2026-03-23 16:28:00
CRL:                 Active
CRL status:          Exist
CRL renew date:      2026-03-13 11:40:00
ESR.R1# show crypto pki trustpoints TP_R1 cert | include "Serial"
Serial:
D4:F1:0C:10:9B:59:4C:88:BF:95:03:D8:F4:E2:40:8B
ESR.R1#
```

В базе сертификатов удостоверяющего центра, в свою очередь, выписанный ранее клиентский сертификат будет отозван:

```
ESR.CA# show crypto pki server database
Serial                                          State       Issue date   Expiration
Revocation   Subject name
                                                                         date         date
------------------------------------------------   ---------   ----------   ----------
----------   ------------------------------
85:71:EC:28:6C:C8:4E:23:B2:03:03:2F:4D:DF:B8:63   Revoked     2026-03-01   2026-03-15
2026-03-12   CN=r1.company.loc/O=Company/L=
                                                                06:52:00     06:52:00
11:40:00     Moscow/ST=Moscow/C=RU

D4:F1:0C:10:9B:59:4C:88:BF:95:03:D8:F4:E2:40:8B   Valid       2026-03-12   2026-03-26   --
CN=r1.company.loc/O=Company/L=
                                                                11:40:00
11:40:00                  Moscow/ST=Moscow/C=RU

ESR.CA#
```

14.1.6 Процесс автоматического перевыпуска сертификата PKI-сервера

После завершения инициализации PKI-сервера обслуживающий его PKI-клиент вычитывает период действия сертификата и за 20% времени до его истечения планирует процедуру подготовки так называемого теневого сертификата (certificate auto-rollover). Данный сертификат предназначен для замены текущего сертификата удостоверяющего центра после его истечения. Наличие сгенерированного теневого сертификата отображается в графе "Shadow" вывода команды **show crypto pki server**. Дата запланированной генерации теневого сертификата присутствует в графе "Renew date" вывода команды **show crypto pki trustpoints** с указанием имени PKI-клиента, обслуживающего PKI-сервер:

```
ESR.CA# show crypto pki server
Status:                     Enabled
Associated trustpoint:      ROOT_CA
Lifetime days:              14
Certificate fingerprint:    A2:0C:10:C7:0E:06:3A:2F:EE:5F:C2:72:39:36:31:0A
Source:                     10.0.103.2
Last issued serial number: D4:F1:0C:10:9B:59:4C:88:BF:95:03:D8:F4:E2:40:8B
Challenge password:         Active
Shadow:                     Inactive
ESR.CA# show crypto pki trustpoints
Name               Enrollment   Usage     Subject name                      Status
Next action
---------------    ----------   -------   -------------------------------   ------------------
--------------------
ROOT_CA            selfsigned   root-ca   CN=ca.company.loc/O=Company/L=    Ready
2026-12-17 08:59:16
                                          Moscow/ST=Moscow/C=RU

ESR.CA# show crypto pki trustpoints ROOT_CA
Name:                ROOT_CA
Usage:               root-ca
Subject name:        CN=ca.company.loc/O=Company/L=Moscow/ST=Moscow/C=RU
Enrollment:          selfsigned
Status:              Ready
Renew date:          2026-12-17 08:59:16
CRL:                 Inactive
ESR.CA#
```

После успешной генерации теневого сертификата обновится графа "Shadow" вывода команды **show crypto pki server**, а также состояние соответствующего PKI-клиента в выводах команды **show crypto pki trustpoints**:

```
ESR.CA# show date
"2026-12-17 09:01:36"
ESR.CA#
ESR.CA# show crypto pki server
Status:                     Enabled
Associated trustpoint:      ROOT_CA
Lifetime days:              14
Certificate fingerprint:    A2:0C:10:C7:0E:06:3A:2F:EE:5F:C2:72:39:36:31:0A
Source:                     10.0.103.2
Last issued serial number: 0A:AF:EA:35:92:E6:48:08:B3:A3:7A:8B:29:85:3B:56
Challenge password:         Active
Shadow:                     Active
ESR.CA# show crypto pki trustpoints
Name               Enrollment   Usage     Subject name                      Status
Next action
---------------    ----------   -------   -------------------------------   ------------------
---------------------
ROOT_CA            selfsigned   root-ca   CN=ca.company.loc/O=Company/L=   Ready with shadow
2027-02-28 08:59:16
                                          Moscow/ST=Moscow/C=RU

ESR.CA# show crypto pki trustpoints ROOT_CA
Name:                ROOT_CA
Usage:               root-ca
Subject name:        CN=ca.company.loc/O=Company/L=Moscow/ST=Moscow/C=RU
Enrollment:          selfsigned
Status:              Ready with shadow
Renew date:          2027-02-28 08:59:16
CRL:                 Inactive
ESR.CA#
```

Любой PKI-клиент, обращающийся за выпуском сертификата в удостоверяющий центр и получивший клиентский сертификат со сроком завершения валидности, эквивалентным сроку завершения жизни сертификата удостоверяющего центра, зафиксирует событие истечения жизни сертификата удостоверяющего центра и отдельным запросом запросит теневой сертификат уже для себя:

```
ESR.R1# sh crypto pki trustpoints
Name              Enrollment   Usage     Subject name                      Status
Next action
---------------   ----------   -------   -------------------------------   ------------------
--------------------
TP_R1             scep         ipsec     CN=r1.company.loc/O=Company/L=   Ready with shadow
2027-02-28 08:59:16
                                         Moscow/ST=Moscow/C=RU

ESR.R1# sh crypto pki trustpoints TP_R1
Name:               TP_R1
Usage:              ipsec
Subject name:       CN=r1.company.loc/O=Company/L=Moscow/ST=Moscow/C=RU
Enrollment:         scep
Challenge password: Active
Status:             Ready with shadow
Renew date:         2027-02-28 08:59:16
CRL:                Active
CRL status:         Exist
CRL renew date:     2027-02-26 15:00:00
ESR.R1# sh crypto pki trustpoints TP_R1 ca | include " after"
    Valid after:                                2026-02-28 08:59:16
    Invalid after:                              2027-02-28 08:59:16
ESR.R1# sh crypto pki trustpoints TP_R1 cert | include " after"
    Valid after:                                2027-02-25 15:00:00
    Invalid after:                              2027-02-28 08:59:16
ESR.R1#
```

В момент, когда текущий сертификат удостоверяющего центра истечет, и PKI-клиент самого удостоверяющего центра, и PKI-клиенты, выписывающие клиентские сертификаты, произведут замену текущего сертификата на теневой и продолжат штатную работу:

```
ESR.CA# show crypto pki trustpoints
Name              Enrollment   Usage     Subject name                      Status
Next action
---------------   ----------   -------   -------------------------------   ------------------
--------------------
ROOT_CA           selfsigned   root-ca   CN=ca.company.loc/O=Company/L=   Ready with shadow
2027-02-28 08:59:16
                                         Moscow/ST=Moscow/C=RU

ESR.CA#
ESR.CA# show date
"2027-02-28 09:00:01"
ESR.CA# sh crypto pki server
Status:                     Enabled
Associated trustpoint:      ROOT_CA
Lifetime days:              14
Certificate fingerprint:    EA:13:09:02:46:6F:F3:91:46:F3:1F:AB:2F:90:CA:18
Source:                     10.0.103.2
Last issued serial number: F3:C4:74:88:E8:AC:44:4D:B9:DC:CD:E8:9E:95:0A:7E
Challenge password:         Active
Shadow:                     Inactive
ESR.CA# show crypto pki trustpoints
Name              Enrollment   Usage     Subject name                      Status
Next action
---------------   ----------   -------   -------------------------------   ------------------
--------------------
ROOT_CA           selfsigned   root-ca   CN=ca.company.loc/O=Company/L=   Ready
2027-12-17 08:59:16
                                         Moscow/ST=Moscow/C=RU

ESR.CA#
```

```
ESR.R1# show crypto pki trustpoints
Name              Enrollment   Usage     Subject name                      Status
Next action
---------------   ----------   -------   -------------------------------   ------------------
--------------------
TP_R1             scep         ipsec     CN=r1.company.loc/O=Company/L=    Ready with shadow
2027-02-28 08:59:16
                                         Moscow/ST=Moscow/C=RU

ESR.R1#
ESR.R1# show date
"2027-02-28 09:00:01"
ESR.R1# show crypto pki trustpoints
Name              Enrollment   Usage     Subject name                      Status
Next action
---------------   ----------   -------   -------------------------------   ------------------
--------------------
TP_R1             scep         ipsec     CN=r1.company.loc/O=Company/L=    Ready
2027-03-11 13:47:16
                                         Moscow/ST=Moscow/C=RU

ESR.R1#
```

14.2 Ручная генерация и распространение ключей и сертификатов X.509

Процесс выпуска сертификатов и ключей для маршрутизаторов ESR может быть и ручным. Небольшой набор команд позволяет администратору формировать приватный ключ, сгенерировать по нему запрос на сертификацию и отправить его на удаленный хост, откуда его уже можно будет доставить в УЦ для выпуска сертификата. Пользовательский сертификат, а также сопутствующие файлы могут быть загружены обратно на ESR для дальнейшего использования в сервисах маршрутизатора.

14.2.1 Алгоритм генерации ключей и запросов на сертификацию

Шаг	Описание	Команда	Ключи
1	Сгенерировать приватный ключ RSA.	**esr# crypto generate private-key rsa <KEY-SIZE> filename <NAME>**	<KEY-SIZE> – размер ключа в битах. Значение может находится в диапазоне от 1024 до 4096; <NAME> – имя файла приватного ключа, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
2	Сформировать запрос на сертификацию.	**esr# crypto generate csr private-key <PRIVATE-KEY> [[alternative-name <ALT-NAME>][common-name <COMMON-NAME>][country <COUNTRY>][email-address <E-MAIL>][locality <LOCATION>] [organization <ORGANIZATION>] [organizational-unit <ORGANIZATION-UNIT>][state <STATE>]] filename <NAME>**	<PRIVATE-KEY> – имя файла приватного ключа, задаётся строкой до 31 символа; <ALT-NAME> – альтернативное имя сертификата, задаётся строкой от 5 до 255 символов в формате <TYPE>:<VALUE>, где: • <TYPE> – спецификатор типа альтернативного имени, может принимать значения "IP" и "DNS".

Шаг	Описание	Команда	Ключи
			• <VALUE> – значение альтернативного имени сертификата, может принимать на сход корректно написанный IPv4-адрес или доменное имя. <COMMON-NAME> – общее имя, задаётся строкой от 1 до 64 символов. Чаще всего в качестве общего имени клиентского сертификата используется полное доменное имя хоста, который использует данный клиентский сертификат или ФИО пользователя, использующего клиентский сертификат; <COUNTRY> – код страны, задаётся строкой длиной 2 символа. Рекомендуется использовать двухбуквенные обозначения стран "alpha-2" из стандарта ISO 3166-1; <E-MAIL> – адрес электронной почты, задаётся строкой от 3 до 64 символов; <LOCATION> – название населенного пункта или его территориальной единицы, задаётся строкой от 1 до 128 символов; <ORGANIZATION> – название организации, задаётся строкой от 1 до 64 символов; <ORGANIZATION-UNIT> – название подразделения организации, задаётся строкой от 1 до 64 символов; <STATE> – название штата, области или провинции, задаётся строкой от 1 до 128 символов; <NAME> – имя файла запроса на сертификацию, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
3	Выгрузить запрос на сертификацию с устройства.	**esr# copy crypto:csr/<CERT-REQ> <DESTINATION>**	<CERT-REQ> – имя файла запроса на сертификацию, задаётся строкой до 31 символа; <DESTINATION> – локальное или удаленное файловое хранилище, куда будет выгружен запрос на сертификацию. Полный список возможных вариантов и синтаксис их описания подробно указан в описании команды **copy** в справочнике команд CLI.
4	Загрузить на устройство клиентский сертификат, выписанный удостоверяющим центром.	**esr# copy <SOURCE> crypto:cert/ <CERT>**	<SOURCE> – локальное или удаленное файловое хранилище, откуда будет загружен файл клиентского сертификата. Полный список возможных вариантов и синтаксис их описания подробно указан в описании команды **copy** в справочнике команд CLI; <CERT> – имя файла клиентского сертификата, задаётся строкой до 31 символа.
5	Загрузить на устройство сертификат удостоверяющего центра.	**esr# copy <SOURCE> crypto:cert/ <CA-CERT>**	<SOURCE> – локальное или удаленное файловое хранилище, откуда будет загружен файл сертификата удостоверяющего центра. Полный список возможных вариантов и синтаксис их описания подробно указан в описании команды **copy** в справочнике команд CLI; <CA-CERT> – имя файла сертификата удостоверяющего центра, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
6	Загрузить на устройство список отозванных сертификатов удостоверяющего центра.	**esr# copy <SOURCE> crypto:crl/ <CRL>**	<SOURCE> – локальное или удаленное файловое хранилище, откуда будет загружен файл со списком отозванных сертификатов. Полный список возможных вариантов и синтаксис их описания подробно указан в описании команды **copy** в справочнике команд CLI; <CRL> – имя файла со списком отозванных сертификатов, задаётся строкой до 31 символа.

14.2.2 Пример ручного выпуска сертификата через внешний удостоверяющий центр

Задача:

Сгенерировать на ESR приватный RSA-ключ и сформировать запрос на сертификацию. Помимо настройки отличительного имени сертификата настроим в качестве альтернативного имени его полное доменное имя.

Решение:

> Для удобства дальнейшей идентификации ключей и сертификатов рекомендуется использовать в качестве имен файлов доменное имя хоста, для которого формируется ключевая пара и префикс сервиса.

> Поскольку сертификаты (как клиентские, так и самого удостоверяющего центра) имеют ограниченный срок действия, то отслеживание истечения срока действия сертификатов и их своевременный перевыпуск полностью находится в зоне ответственности администратора маршрутизатора.

Сгенерируем приватный ключ RSA:

> При генерации ключей RSA рекомендуется использовать ключи длиной 2048 бит и более.

```
ESR.R1# crypto generate private-key rsa 2048 filename r1.company.loc.key
.....+.......+..+.........+...+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+*......+...+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*...+.........+..
+.+...+.........+..+...+......+....+...+........+
.......+........+.+......+.........+.........................+..+++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++
............++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.......+...++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+.+...+......+.....+......+.......
+......+......+.....+...+..............+.+.....
.+.....+.+.....+...+.......+.....+...+....+...+..+............+......+....+........+.+..
+............+.+...........+...................+...+....+...........+.........+....+..+.......
+......+......+........+............................+.....
........+...+.........+.....+.+...+............+..+..........+..+...+.+..+...+................
+.....+.+........+.+.....+....+...........+...+...+...+.......+........+..........+..+.........
+...+...+...+.+...+......+......+......+...+.....
.........+.+.....+.+...+..+...+.......+......+............+......+.........+.....+.
+............+.....+....+...+...+...................+...+.......+..+.+............+..+.+...+.....
+....+..............+...........+....+...+..................
+.+...........+...+.+.....+.+...+...........+..........+.....+.........+...+....+..............
+.+........+...+....+......+........+.+......+..+.+.....................+....+......+..+...
+................+...+........+.......+...........+.+
......+..+.+......+.....+...+......+.......+........+.+......+........+......+.+...
+............................+........+.+...+...........+.+.....+.+.........+...+.....+.......
+.....+......+...+......+.....................+..........+..+.
.....+......+.+..............+.+.....+....+...+...........+......+....+.....+....+...+...+..
+............+.+.................+...+.+.............+...........+.........+......+....
+......+...+.........+..+.+..+.+..+.....................
+........+.......+..+....+......+......+..+...+..........+.........................
+............+.....+...+.+.....+....+...+.....+....+...+...........+......+.+...+.....+++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++
ESR.R1#
```

Сформируем запрос на сертификацию:

```
ESR.R1# crypto generate csr private-key r1.company.loc.key country RU state Moscow locality
Moscow organization Company common-name r1.company.loc email-address netmaster@company.loc
alternative-name DNS:r1.company.loc filename r1.company.loc.csr
ESR.R1#
```

Выгрузим сформированный запрос на сертификацию на внешний TFTP-сервер для дальнейшей доставки в удостоверяющий центр:

```
ESR.R1# copy crypto:csr/r1.company.loc.csr tftp://10.0.113.1:/r1.company.loc.csr
|**************************************| 100% (1094B) Success!
ESR.R1#
```

Процесс доставки запроса на сертификацию в удостоверяющий центр и непосредственно сам выпуск сертификата индивидуален для каждого удостоверяющего центра и не рассматривается в данном разделе руководства.

После успешного выпуска сертификата удостоверяющим центром загрузим клиентский сертификат, сертификат удостоверяющего центра и список отозванных сертификатов на маршрутизатор:

```
ESR.R1# copy tftp://10.0.113.1:/ca.crt crypto:cert/ca.crt
|****************************************| 100% (2264B) Crypto file loaded successfully!
ESR.R1# copy tftp://10.0.113.1:/ca.crl crypto:crl/ca.crl
|****************************************| 100% (1064B) Crypto file loaded successfully!
ESR.R1# copy tftp://10.0.113.1:/r1.company.loc.crt crypto:cert/r1.company.loc.crt
|****************************************| 100% (1931B) Crypto file loaded successfully!
ESR.R1#
```

Посмотреть итоговое содержимое сертификата можно командой **show crypto certificates**:

```
ESR.R1# show crypto certificates cert r1.company.loc.crt
Version:                                        3
Serial:                                         4096
Subject name:
    C(countryName):                             RU
    ST(stateOrProvinceName):                    Moscow
    O(organizationName):                        Company
    CN(commonName):                             r1.company.loc
    emailAddress(emailAddress):                 netmaster@company.loc
Issuer name:
    C(countryName):                             RU
    ST(stateOrProvinceName):                    Moscow
    L(localityName):                            Moscow
    O(organizationName):                        Company
    CN(commonName):                             Company Root Certificate Authority
Validity period:
    Valid after:                                2025-10-28 03:26:41
    Invalid after:                              2025-11-27 03:26:41
Signature:
    Algorithm:                                  sha256WithRSAEncryption
    Value:
37:6D:30:DE:C3:EF:D8:06:D6:4B:AA:AC:6A:78:65:C2:7C:7B:

EA:E9:F6:C0:A7:0F:9B:01:D2:C6:05:95:43:A1:C6:7B:F7:43:

F7:BE:78:7F:BA:65:73:88:31:91:C5:4F:FA:BF:41:99:D6:28:

A5:29:72:85:20:52:2E:0C:1D:3E:37:78:10:B5:CC:AE:D5:A9:

A6:79:FE:07:F4:93:E2:E9:F4:48:17:E5:A6:EB:36:D9:3E:41:

2E:8D:E9:7A:D4:75:49:A5:98:8F:76:73:8A:A7:E6:1D:89:CA:

46:B2:FC:A6:E7:96:F3:79:EB:5A:B1:B0:63:E4:AC:7C:D9:29:

AE:2D:04:4E:45:B0:08:38:7F:C6:62:72:04:C6:A2:7C:BC:77:

AF:CE:92:2F:66:75:33:8B:81:AB:98:40:61:74:9C:6B:10:15:

78:A7:58:02:DA:D1:69:C2:C2:8B:DA:66:18:BD:13:FB:4F:7D:

35:35:C3:21:6F:0A:A0:53:ED:56:F8:B9:E9:0E:6F:6D:DD:E1:

A0:AD:4A:07:97:AE:79:3C:2F:7C:E6:76:DD:9F:37:50:EB:AD:

56:3D:BA:51:D0:C1:15:25:54:F6:E2:1D:12:39:46:5F:E3:33:

1E:49:26:04:E0:23:FB:C5:FA:A8:0D:B7:16:23:C5:C9:3E:0C:

85:E2:CE:72:B5:97:0D:3D:15:D6:5D:F7:12:78:9C:84:D2:21:

C8:EC:BE:45:90:A5:CB:38:87:AB:8C:04:4B:BA:42:2B:40:95:

94:BE:F9:82:80:44:76:79:ED:42:5A:ED:28:07:E4:16:6D:C8:

80:D4:33:87:97:39:20:E9:CC:EB:F3:74:CE:F2:3C:6E:4E:C8:

37:51:21:F8:CA:AD:C6:09:3B:19:07:B2:34:3C:17:31:B8:22:
```

```
CC:BA:73:5E:9F:CD:F4:8B:38:71:BB:2F:7A:A5:F5:43:A8:8E:

07:47:36:BA:8D:BA:DB:BB:8F:9C:EB:49:A4:6C:2E:30:30:C1:

AF:06:F1:0D:E6:C7:DA:7B:FD:94:68:FD:F0:B3:3F:30:45:8C:

ED:77:FE:09:64:0E:4D:02:03:82:3A:30:61:24:08:4A:AF:BD:

C2:32:6B:70:78:E6:C1:F2:6E:2A:3E:30:1A:7A:A2:BE:70:7F:

86:8A:9B:12:D0:92:7D:14:99:72:FA:30:29:BE:44:8F:3C:D8:

75:16:AE:BD:23:97:E0:04:B5:8A:B9:71:F0:F7:15:0A:A8:95:

CC:51:23:21:6E:3F:9B:64:B1:73:A7:2F:03:22:46:6F:DD:A2:

90:A1:E4:7F:94:92:7F:E7:C2:C5:B9:F9:9D:D3:19:CF:34:3D:
                                                    D0:C0:E0:30:F8:77:1A:E8
Public key info:
    Algorithm:                                      RSA
    Key size:                                       2048
    Exponent:                                       65537
    Modulus:
00:9D:41:BB:13:A8:99:9C:3E:E7:2C:0E:A5:B6:A8:CA:22:64:

BB:B9:77:E5:CE:DE:5E:71:83:9A:90:22:D1:32:E1:66:45:FC:

6C:53:DA:65:D5:FF:C7:35:2C:24:F6:BA:AD:72:DD:27:A5:09:

30:CC:AA:E3:F8:33:B5:10:1C:23:D9:EA:DA:30:6F:E4:2C:C4:

EC:08:E9:12:72:05:0C:C1:CF:6B:72:8F:B5:E8:5B:90:67:B1:

4C:59:D3:4D:CA:0C:73:94:47:F7:DB:BC:83:38:24:E2:AC:19:

DF:7D:8F:99:E0:B2:72:E3:A3:5B:7E:B8:EC:7B:6C:17:8C:48:

5A:F2:F5:A5:14:D3:07:E3:7E:5A:CD:70:6A:9E:38:2D:80:4F:

29:B3:60:F8:AC:7B:C5:09:09:B9:4B:92:D4:E0:44:5D:9E:1A:

AF:0E:25:FA:E5:73:C3:51:8F:DE:BB:F5:71:0C:2F:F3:AC:F5:

7D:79:8A:E6:87:0A:05:6A:D8:C8:6D:FE:BE:90:7D:B5:A2:3D:

3B:75:96:CF:25:98:5C:0B:F2:E3:C1:E7:B5:30:58:27:13:64:

DD:DB:77:A8:10:9C:A5:25:AC:85:DA:30:21:87:71:A8:D7:D8:

BC:60:40:C7:53:54:01:03:0E:60:5D:2B:43:99:97:F2:26:6E:
                                                    8F:F7:47:CF:9F
X509v3 Basic Constraints:
    CA:                                             No
    Critical:                                       Yes
X509v3 Subject key identifier:
    ID:
40:6D:58:0E:0A:4C:CD:89:71:CA:DB:D2:BC:AD:FA:27:C9:1E:
                                                    4D:D8
    Critical:                                       No
```

```
X509v3 Authority key identifier:
    ID:
7C:E6:3C:E3:FB:76:C5:18:B3:21:52:9D:8F:71:29:28:55:CA:
                                                    96:63
    Critical:                                       No
X509v3 Key Usage:
    Usage:                                          Digital Signature
                                                    Non Repudiation
    Critical:                                       Yes
X509v3 Subject Alternative Name:
    Names:                                          DNS:r1.company.loc
    Critical:                                       No
ESR.R1#
```

Как можно заметить, выписанный сертификат действует 30 дней и в нем было сохранено заданное альтернативное имя. Теперь данный сертификат можно использовать в сервисах маршрутизатора.

Для корректной работы сервисов, использующих сертификаты, рекомендуется настроить на маршрутизаторе синхронизацию времени по протоколу NTP.

15 Управление резервированием

- Настройка VRRP
  - Алгоритм настройки
  - Пример настройки 1
  - Пример настройки 2
- Настройка tracking
  - Алгоритм настройки
  - Пример настройки
- Настройка Firewall/NAT failover
  - Алгоритм настройки
  - Пример настройки
- Настройка DHCP failover
  - Алгоритм настройки
  - Пример настройки

15.1 Настройка VRRP

VRRP (англ. *Virtual Router Redundancy Protocol*) — сетевой протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию. Это достигается путём объединения группы маршрутизаторов в один виртуальный маршрутизатор и назначения им общего IP-адреса, который и будет использоваться как шлюз по умолчанию для хостов в сети.

15.1.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим конфигурирования интерфейса/сетевого моста, для которого необходимо настроить протокол VRRP.	**esr(config)# interface <IF-TYPE><IF-NUM>**	<IF-TYPE> – тип интерфейса; <IF-NUM> – F/S/P – F-фрейм (1), S – слот (0), P – порт.
		esr(config)# tunnel <TUN-TYPE><TUN-NUM>	<TUN-TYPE> – тип туннеля; <TUN-NUM> – номер туннеля.
		esr(config)# bridge <BR-NUM>	<BR-NUM> – номер сетевого моста.
2	Настроить необходимые параметры на интерфейсе/сетевом мосту, включая IP-адрес.		
3	Объявить номер экземпляра VRRP-процесса.	**esr(config-if-gi)# vrrp <VRRP-NUM>**	<VRRP-NUM> – номер экземпляра VRRP-процесса, принимает значения [1..255].
		esr(config-if-gi)# ipv6 vrrp <VRRP-NUM>	

Шаг	Описание	Команда	Ключи
4	Установить виртуальный IP-адрес VRRP-маршрутизатора.	**esr(config-vrrp)# ip address <ADDR/LEN> [secondary]**	<ADDR/LEN> – виртуальный IP-адрес и длина маски, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. Можно указать несколько IP-адресов перечислением через запятую. Может быть назначено до 8 IP-адресов на интерфейс. secondary – ключ для установки дополнительного IP-адреса.
		esr(config-vrrp)# ipv6 ip address <IPV6-ADDR>	<IPV6-ADDR> – виртуальный IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. Можно указать до 8 IPv6-адресов перечислением через запятую.
5	Включить VRRP-экземпляр на IP-интерфейсе.	**esr(config-vrrp)# enable**	
6	Установить описание VRRP-процесса (не обязательно).	**esr(config-vrrp)# description <DESCRIPTION>**	<DESCRIPTION> – описание VRRP-процесса, задаётся строкой до 255 символов.
7	Установить приоритет VRRP-маршрутизатора (не обязательно).	**esr(config-vrrp)# priority <PR>**	<PR> – приоритет VRRP-маршрутизатора, принимает значения [1..254]. Значение по умолчанию: 100.
		esr(config-vrrp)# ipv6 priority <PR>	
8	Установить принадлежность VRRP-маршрутизатора к группе. Группа предоставляет возможность синхронизировать несколько VRRP-процессов, так если в одном из процессов произойдет смена мастера, то в другом процессе также произойдёт смена ролей (не обязательно).	**esr(config-vrrp)# group <GRID>**	<GRID> – идентификатор группы VRRP-маршрутизатора, принимает значения [1..32].
		esr(config-vrrp)# ipv6 group <GRID>	

Шаг	Описание	Команда	Ключи
9	Установить наследование состояний VRRP. Статус интерфейса наследника будет следовать состояниям VRRP родителя, идентификатор которого был задан (не обязательно).	**esr(config-vrrp)# inherit-vrrp-id <VRID>**	<VRID> – идентификатора VRRP-маршрутизатора, принимает значения [1..255].
		esr(config-vrrp)# inherit-vrrp-id <VRID>	
10	Установить IP-адрес, который будет использоваться в качестве IP-адреса отправителя для VRRP-сообщений (не обязательно).	**esr(config-vrrp)# source-ip <IP>**	<IP> – IP-адрес отправителя, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
		esr(config-vrrp)# ipv6 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].
11	Установить интервал между отправкой VRRP-сообщений (не обязательно).	**esr(config-vrrp)# timers advertise <TIME>**	<TIME> – время в секундах, принимает значения [1..40]. Значение по умолчанию: 1 секунда.
		esr(config-vrrp)# ipv6 timers advertise <TIME>	
12	Установить интервал, по истечении которого происходит отправка GratuituousARP-сообщения(ий) при переходе маршрутизатора в состояние Master (не обязательно).	**esr(config-vrrp)# timers garp delay <TIME>**	<TIME> – время в секундах, принимает значения [1..60]. Значение по умолчанию: 5 секунд.
13	Установить количество GratuituousARP-сообщений, которые будут отправлены при переходе маршрутизатора в состояние Master (не обязательно).	**esr(config-vrrp)# timers garp repeat <COUNT>**	<COUNT> – количество сообщений, принимает значения [1..60]. Значение по умолчанию: 5.
14	Установить интервал, по истечении которого будет происходить периодическая отправка GratuituousARP-сообщения(ий), пока маршрутизатор находится в состоянии Master (не обязательно).	**esr(config-vrrp)# timers garp refresh <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: периодическая отправка отключена.

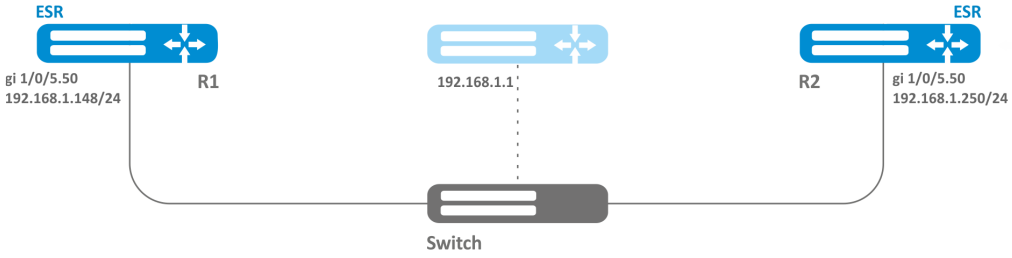
Шаг	Описание	Команда	Ключи
15	Установить количество GratuituousARP-сообщений, которые будут отправляться с периодом garprefresh, пока маршрутизатор находится в состоянии Master (не обязательно).	**esr(config-vrrp)# timers garp refresh-repeat <COUNT>**	<COUNT> – количество сообщений, принимает значения [1..60]. Значение по умолчанию: 1.
16	Определить, будет ли Backup-маршрутизатор с более высоким приоритетом пытаться перехватить на себя роль Master у текущего Master-маршрутизатора с более низким приоритетом (не обязательно).	**esr(config-vrrp)# preempt disable**	
		esr(config-vrrp)# ipv6 preempt disable	
17	Установить временной интервал, по истечении которого Backup-маршрутизатор с более высоким приоритетом будет пытаться перехватить на себя роль Master у текущего Master-маршрутизатора с более низким приоритетом (не обязательно).	**esr(config-vrrp)# preempt delay <TIME>**	<TIME> – время ожидания, определяется в секундах [1..1000]. Значение по умолчанию: 0.
		esr(config-vrrp)# ipv6 preempt delay <TIME>	
18	Установить пароль для аутентификации с соседом (не обязательно).	**esr(config-vrrp)# authentication key ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<CLEAR-TEXT> – ключ, задаётся строкой от 1 до 8 символов; <ENCRYPTED-TEXT> – зашифрованный ключ размером от 1 до 8 байт (от 2 до 16 символов). Задается в шестнадцатеричном формате (0xYYYY...) или (YYYY...).
19	Определить алгоритм аутентификации (не обязательно).	**esr(config-vrrp)# authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм аутентификации: • **cleartext** – пароль, передается открытым текстом; • **md 5** – пароль хешируется по алгоритму md5.
20	Задать версию VRRP-протокола (не обязательно).	**esr(config-vrrp)# version <VERSION>**	<VERSION> – версия VRRP-протокола: 2, 3.
21	Установить режим, когда vrrp IP-адрес остается в состоянии UP вне зависимости от состояния самого интерфейса (не обязательно).	**esr(config-vrrp)# force-up**	

Шаг	Описание	Команда	Ключи
22	Определить задержку между установлением ipv6 vrrp состояния MASTER и началом рассылки ND-сообщений (не обязательно).	**esr(config-vrrp)# ipv6 timers nd delay <TIME>**	<TIME> – время в секундах, принимает значения [1..60]. Значение по умолчанию: 5.
23	Определить период обновления информации протокола ND для ipv6 vrrp в состоянии MASTER (не обязательно).	**esr(config-vrrp)# ipv6 timers nd refresh <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 5.
24	Определить количество ND сообщений отправляемых за период обновления для ipv6 vrrp в состоянии MASTER (не обязательно).	**esr(config-vrrp)# ipv6 timers nd refresh-repeat <NUM>**	<NUM> – количество, принимает значения [1..60]. Значение по умолчанию: 0.
25	Определить количество отправок ND-пакетов после установки ipv6 vrrp в состоянии MASTER (не обязательно).	**esr(config-vrrp)# ipv6 timers nd repeat <NUM>**	<NUM> – количество, принимает значения [1..60]. Значение по умолчанию: 1.

15.1.2 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-if-sub)# vrrp 10
```

Укажем IP-адрес виртуального шлюза 192.168.1.1/24:

```
R1(config-vrrp)# ip address 192.168.1.1/24
```

Включим VRRP:

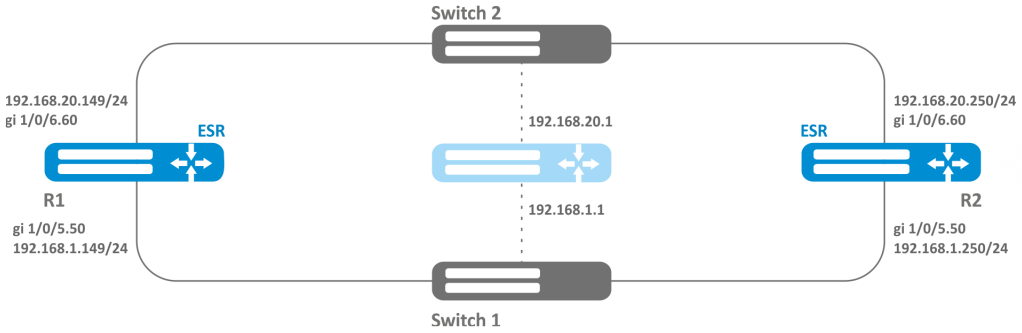
```
R1(config-vrrp)# enable
R1(config-vrrp)# exit
```

После чего необходимо произвести аналогичные настройки на R2.

15.1.3 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-if-sub)# vrrp 10
```

Укажем IP-адрес виртуального шлюза 192.168.1.1/24:

```
R1(config-vrrp)# ip address 192.168.1.1/24
```

Укажем идентификатор VRRP-группы:

```
R1(config-vrrp)# group 5
```

Включим VRRP:

```
R1(config-vrrp)# enable
R1(config-vrrp)# 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-if-sub)# vrrp 20
```

Укажем IP-адрес виртуального шлюза 192.168.20.1/24:

```
R1(config-vrrp)# ip address 192.168.20.1/24
```

Укажем идентификатор VRRP-группы:

```
R1(config-vrrp)# group 5
```

Включим VRRP:

```
R1(config-vrrp)# enable
R1(config-vrrp)# exit
```

Произвести аналогичные настройки на R2.

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

⚠ При использовании IPsec с VRRP рекомендуется настраивать DPD для ускорения перестроения IPsec-туннеля.

15.2 Настройка tracking

Tracking — механизм, позволяющий активировать сущности в зависимости от состояния VRRP/IP-SLA/туннеля/интерфейса.

15.2.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Настроить VRRP согласно разделу Алгоритм настройки VRRP, настроить SLA по инструкции Настройка SLA, или сконфигурировать туннель/интерфейс.		
2	Добавить в систему Tracking-объект и перейти в режим настройки параметров Tracking-объекта.	**esr(config)# track <ID>**	<ID> – номер Tracking-объекта, принимает значения [1..100].
3	Задать правило слежения, на основании которых Tracking-объект будет переходить в активное состояние.	**esr(config-track)# track vrrp id <VRID> state [not] { master | backup | fault } [vrf <VRF>]**	<VRID> – идентификатор отслеживаемого VRRP-маршрутизатора, принимает значения [1..255]; <VRF> – имя экземпляра VRF, задается строкой до 31 символа.
		esr(config-track)# track sla test <NUM> [mode <MODE>]	<NUM> – номер SLA-теста, задается в диапазоне [1..10000]; <MODE> – режим слежения за sla-тестом, может принимать значения: • state success – отслеживается успешное состояние sla-теста; • state fail – отслеживается провальное состояние sla-теста; • reachability – отслеживаются состояние канала связи, по которому осуществляется sla-тест. При указании команды без аргумента mode, по-умолчанию устанавливается значение mode state success.

Шаг	Описание	Команда	Ключи
		esr(config-track)# track { interface <IF> | tunnel <TUN> } [state <STATE>]	<IF> – имя IP-интерфейса, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора; <TUN> – имя туннеля, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора; <STATE> – режим слежения за sla-тестом, может принимать значения: • up – административное состояние "Up" ; • down – административное состояние "Down". При указании команды без аргумента state по умолчанию устанавливается значение mode state up.
4	Включить Tracking-объект.	**esr(config-track)# enable**	
5	Установить задержку смены состояния отслеживаемого объекта (не обязательно).	**esr(config-track)# delay { down | up } <TIME>**	<TIME> – время задержки в секундах, задается в диапазоне [1..300].
6	Задать режим работы track (не обязательно).	**esr(config-track)# mode <MODE>**	<MODE> – условие нахождения объекта отслеживания в активном состоянии, принимает значения: • and – объект будет находиться в активном состоянии, если выполняются все отслеживаемые условия; • or – объект будет находиться в активном состоянии, если выполняется хотя бы одно из отслеживаемых условий. По умолчанию используется устанавливается значение mode and.
7	Создать сущность на ESR, которая будет меняться в зависимости от состояния Tracking-объекта.		

Шаг	Описание	Команда	Ключи
7.1	Добавить возможность управления статическим IP-маршрутом к указанной подсети (не обязательно).	**esr(config)# ip route [vrf <VRF>] <SUBNET> { <NEXTHOP> [resolve] | interface <IF> | tunnel <TUN> | wan load-balance rule <RULE> | blackhole | unreachable | prohibit } [<METRIC>] [track <TRACK-ID>]**	<VRF> – имя экземпляра VRF, задается строкой до 31 символа; <SUBNET> – адрес назначения, может быть задан в следующих видах: AAA.BBB.CCC.DDD – IP-адрес хоста, где каждая часть принимает значения [0..255]; AAA.BBB.CCC.DDD/NN – IP-адрес подсети с маской в виде префикса, где AAA-DDD принимают значения [0..255] и NN принимает значения [1..32]. <NEXTHOP> – IP-адрес шлюза задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; • **resolve** – при указании данного параметра IP-адрес шлюза будет рекурсивно вычислен через таблицу маршрутизации. Если при рекурсивном вычислении не удастся найти шлюз из напрямую подключенной подсети, то данный маршрут не будет установлен в систему; <IF> – имя IP-интерфейса, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора; <TUN> – имя туннеля, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора; <RULE> – номер правила wan, задаётся в диапазоне [1..50]; • **blackhole** – при указании команды пакеты до данной подсети будут удаляться устройством без отправки уведомлений отправителю;

Шаг	Описание	Команда	Ключи
			• **unreachable** – при указании команды пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Host unreachable, code 1); • **prohibit** – при указании команды, пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Communication administratively prohibited, code 13); [METRIC] – метрика маршрута, принимает значения [0..255]; <TRACK-ID> – идентификатор Tracking-объекта. Если маршрут привязан к Tracking-объекту, то он появится в системе только при выполнении всех условий, заданных в объекте.
7.2	Добавить возможность управления логическим состоянием интерфейса (не обязательно).	**esr(config-if-gi)# shutdown track <ID>**	<ID> – номер Tracking-объекта, принимает значения [1..100].
7.3	Добавить возможность управления приоритетом VRRP-процесса (не обязательно).	**esr(config-if-gi)# vrrp priority track <ID> { <PRIO> | increment <INC> | decrement <DEC> }**	<ID> – номер Tracking-объекта, принимает значения в диапазоне [1..100]; <PRIO> – приоритет VRRP-процесса, который выставится, если Tracking-объект будет в активном состоянии, принимает значения в диапазоне [1..254]; <INC> – значение на которое увеличится приоритет VRRP-процесса, если Tracking-объект будет в активном состоянии, принимает значения в диапазоне [1..254]; <DEC> – значение на которое уменьшится приоритет VRRP-процесса, если Tracking-объект будет в активном состоянии, принимает значения в диапазоне [1..254].

Шаг	Описание	Команда	Ключи
7.4	Добавить возможность управления Next-Hop для пакетов, которые попадают под критерии в указанном списке доступа (ACL) (не обязательно).	**esr(config-route-map-rule)# action set ip next-hop verify-availability <NEXTHOP> <METRIC> track <ID>**	<NEXTHOP> – IP-адрес шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <METRIC> – метрика маршрута, принимает значения [0..255]; <ID> – номер Tracking-объекта, принимает значения [1..100].
7.5	Добавить возможность управления атрибутом BGP AS-Path, которое будет добавляться в начало списка AS-Path в маршруте (не обязательно).	**esr(config-route-map-rule)# action set as-path prepend <AS-PATH> track <ID> [default <AS-PATH>]**	<AS-PATH> – список номеров автономных систем, который будет добавлен к текущему значению в маршруте. Задаётся в виде AS,AS,AS, принимает значения [1..4294967295]; <ID> – номер Tracking-объекта, принимает значения [1..100].
7.6	Добавить возможность управления атрибутом BGP MED в маршруте, для которого должно срабатывать правило (не обязательно).	**esr(config-route-map-rule)# action set metric bgp { <METRIC> | increment <INC> | decrement <DEC> } track <ID> [default { <METRIC> | increment <INC> | decrement <DEC> }]**	<ID> – номер Tracking-объекта, принимает значения [1..100]; <METRIC> – значение атрибута BGP MED, принимает значения [0..4294967295]; <INC> – значение, на которое увеличится атрибут BGP MED, если Tracking-объект будет в активном состоянии. Принимает значения [0..4294967295]; <DEC> – значение, на которое уменьшится атрибут BGP MED, если Tracking-объект будет в активном состоянии. Принимает значения [0..4294967295];

Шаг	Описание	Команда	Ключи
7.7	Добавить возможность управления атрибутом BGP Community в маршруте, для которого должно срабатывать правило (не обязательно).	**esr(config-route-map-rule)# action { set | add | remove } community { no-advertise | no-export | <COMMUNITY-LIST> } track <TRACK-ID> [default <COMMUNITY-LIST>]**	<COMMUNITY-LIST> – список community, задаётся в виде AS:N,AS:N,AS:N, где AS-часть принимает значения [0..65535], N-часть принимает значения [0..65535]. Можно указать до 64 community; <TRACK-ID> – идентификатор объекта отслеживания, при выполнении всех условий которого будет исполняться указанное действие. Изменяется в диапазоне [1..100]; no-advertise – при указании команды маршруты, которые передаются с данным значением атрибута community, не должны анонсироваться другим BGP-соседям; no-export – при указании команды маршруты, которые передаются с таким значением атрибута community, не должны анонсироваться за пределы конфедерации (автономная система, которая не является частью конфедерации, считается конфедерацией). То есть, маршруты не анонсируются eBGP-соседям, но анонсируются внешним соседям в конфедерации.

Шаг	Описание	Команда	Ключи
7.8	Добавить возможность управления атрибутом BGP ExtCommunity в маршруте, для которого должно срабатывать правило (не обязательно).	**esr(config-route-map-rule)# action { set | add | remove } extcommunity <EXTCOMMUNITY-LIST> track <TRACK-ID> [default <EXTCOMMUNITY-LIST>]**	<TRACK-ID> – идентификатор объекта отслеживания, при выполнении всех условий которого будет исполняться указанное действие. Изменяется в диапазоне [1..100]; <EXTCOMMUNITY-LIST> – список community, задаётся в виде KIND:AS:N,KIND:AS:N,KIND:AS:N, где: • KIND – тип extcommunity, принимает значения rt (Route Target) и ro (Route Origin); • AS – номер автономной системы, принимает значения [1..4294967295]; • N – номер extcommunity, определяющий политику маршрутизации трафика, принимает значения [1..65535].
7.9	Добавить возможность управления атрибутом BGP Local Preference в маршруте, для которого должно срабатывать правило (не обязательно).	**esr(config-route-map-rule)# action set local-preference {<PREFERENCE> | increment < VALUE > | decrement < VALUE >} track <TRACK-ID> [default <PREFERENCE>] }**	<VALUE> – значение дельты изменения атрибута BGP Local Preference относительно исходного значения. Принимает значение [1..2147483647]. Если в результате применения операции increment/decrement значение метрики выйдет за допустимый диапазон, значение Local Preference принимается равным максимально или минимально допустимому значению соответственно; <PREFERENCE> – значение атрибута BGP Local Preference, принимает значения [1..2147483647]; <TRACK-ID> – идентификатор tracking-объекта, при выполнении всех условий которого будет исполняться указанное действие. Изменяется в диапазоне [1..100].

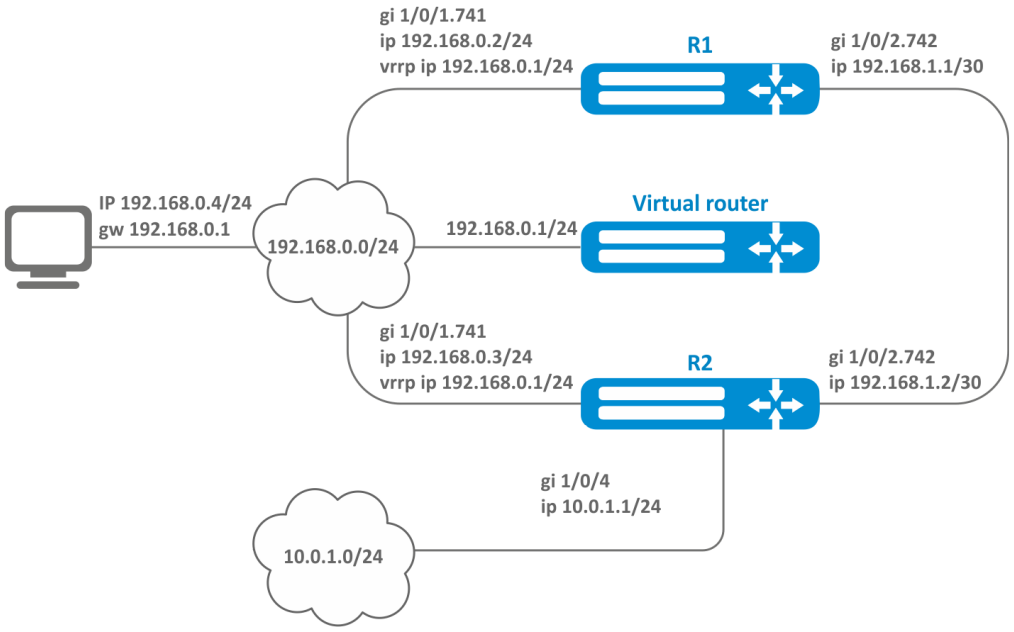
Шаг	Описание	Команда	Ключи
7.10	Добавить возможность управления атрибутом BGP Origin в маршруте, для которого должно срабатывать правило (не обязательно).	**esr(config-route-map-rule)# action set origin <ORIGIN> track <TRACK-ID> [default <ORIGIN>]**	<TRACK-ID> – идентификатор объекта отслеживания, при выполнении всех условий которого будет исполняться указанное действие. Изменяется в диапазоне [1..100]; <ORIGIN> – значение атрибута BGP Origin, принимает следующие значения: • egp – маршрут выучен по протоколу Exterior Gateway Protocol (EGP); • igp – маршрут получен внутри исходной автономной системы; • incomplete – маршрут выучен другим образом.
7.11	Добавить возможность управления атрибутом BGP Weight в маршруте, для которого должно срабатывать правило (не обязательно).	**esr(config-route-map-rule)# action set weight bgp {< WEIGHT > | increment < VALUE > | decrement < VALUE >} track <TRACK-ID> [default <WEIGHT>]**	<WEIGHT> – значение атрибута BGP weight, принимает значения [0..65535]; <TRACK-ID> – идентификатор объекта отслеживания, при выполнении всех условий которого будет исполняться указанное действие. Изменяется в диапазоне [1..100].
7.7	Добавить возможность управления активацией IPsec-туннеля.	**esr(config-ipsec-vpn)# enable track <ID>**	<ID> – номер tracking-объекта, принимает значения [1..100];

15.2.2 Пример настройки

Задача:

Для подсети 192.168.0.0/24 организован виртуальный шлюз 192.168.0.1/24 с использованием протокола VRRP на основе аппаратных маршрутизаторов R1 и R2. Также между маршрутизаторами R1 и R2 есть линк с вырожденной подсетью 192.168.1.0/30. Подсеть 10.0.1.0/24 терминируется только на маршрутизаторе R2. ПК имеет IP-адрес 192.168.0.4/24 и шлюз по умолчанию 192.168.0.1.

Когда маршрутизатор R1 находится в состоянии vrrp backup, трафик от ПК в подсеть 10.0.1.0/24 пойдет без дополнительных настроек. Когда маршрутизатор R1 находится в состоянии vrrp master, необходим дополнительный маршрут для подсети 10.0.1.0/24 через интерфейс 192.168.1.2.



Исходные конфигурации маршрутизаторов:

Маршрутизатор R1

```
hostname R1
interface gigabitethernet 1/0/1
  switchport forbidden default-vlan
exit
interface gigabitethernet 1/0/1.741
  ip firewall disable
  ip address 192.168.0.2/24
  vrrp 10
    ip address 192.168.0.1/24
    enable
  exit
interface gigabitethernet 1/0/2
  switchport forbidden default-vlan
exit
interface gigabitethernet 1/0/2.742
  ip firewall disable
  ip address 192.168.1.1/30
exit
```

Маршрутизатор R2

```
hostname R2
interface gigabitethernet 1/0/1
  switchport forbidden default-vlan
exit
interface gigabitethernet 1/0/1.741
  ip firewall disable
  ip address 192.168.0.3/24
  vrrp 10
    ip address 192.168.0.1/24
    enable
  exit
interface gigabitethernet 1/0/2
  switchport forbidden default-vlan
exit
interface gigabitethernet 1/0/2.742
  ip firewall disable
  ip address 192.168.1.2/30
exit
interface gigabitethernet 1/0/4
  ip firewall disable
  ip address 10.0.1.1/24
exit
```

Решение:

На маршрутизаторе R2 никаких изменений не требуется, так как подсеть 10.0.1.0/24 терминируется на нем, и в момент, когда R2 выступает в роли vrrp master, пакеты будут переданы в соответствующий интерфейс. На маршрутизаторе необходимо создать маршрут для пакетов с IP-адресом назначения из сети 10.0.1.0/24 в момент, когда R1 выступает в роли vrrp master.

Для этого создадим track-object с соответствующим условием:

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

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

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

15.3 Настройка Firewall/NAT failover

Firewall failover необходим для резервирования сессий firewall.

> ⚠ При включенном на устройстве firewall failover увеличивается потребление оперативной памяти на хранение firewall сессий.

15.3.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перед настройкой сервисов резервирования необходимо настроить общие параметры failover.		
2	Переход в конфигурационное меню общих настроек failover-сервисов.	**esr(config)# ip failover [vrf <VRF>]**	<VRF> – имя VRF, задается строкой до 31 символа.
3	Установка IP-адреса, на котором failover-сервисы принимают failover-сообщения при работе в режиме резервирования.	**esr(config-failover)# local-address { <ADDR> | object-group <NETWORK_OBJ_GROUP_NAME> }**	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве local address.
4	Установка многоадресного IP-адреса, который будет использоваться для обмена информацией при работе резервирования failover-сервисов в multicast-режиме.	**esr(config-failover)# multicast-address <ADDR>**	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];
5	Установка идентификатора multicast-группы для обмена информацией при работе резервирования failover-сервисов в multicast-режиме.	**esr(config-failover)# multicast-group <GROUP>**	<GROUP> – multicast-группа, указывается в диапазоне [1000..9999].
6	Установка IP-адреса, на который failover-сервисы отправляют failover-сообщения при работе в режиме резервирования.	**esr(config-failover)# remote-address { <ADDR> | object-group <NETWORK_OBJ_GROUP_NAME> }**	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве local address.
7	Выбор VRRP-группы, по состоянию которой будет определятся мастерство при работе failover-сервисов в режиме Active-Standby.	**esr(config-failover)# vrrp-group <GRID>**	<GRID> – идентификатор группы VRRP-маршрутизатора, принимает значения [1..32].
8	Переход в конфигурационное меню настроек Firewall failover.	**esr(config)# ip firewall failover [vrf <VRF>]**	<VRF> – имя VRF, задается строкой до 31 символа.
9	Выбор режима обмена информацией между маршрутизаторами.	**esr(config-firewall-failover)# sync-type <MODE>**	<MODE> – режим обмена информацией: • unicast – режим unicast; • multicast – режим multicast.

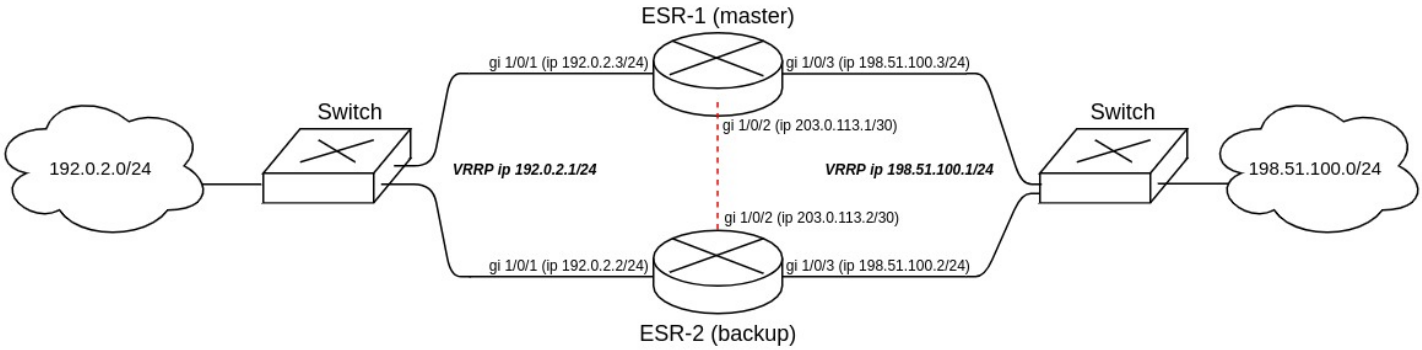
Шаг	Описание	Команда	Ключи
10	Настройка номера UDP-порта службы резервирования сессий Firewall, через который происходит обмен информацией при работе в unicast-режиме (не обязательно).	**esr(config-firewall-failover)# port <PORT>**	<PORT> – номер порта службы резервирования сессий Firewall, указывается в диапазоне [1..65535].
11	Включение резервирования сессий Firewall.	**esr(config-firewall-failover)# enable**	

⚠ При настройке firewall failover также будут синхронизироваться NAT-сессии между устройствами.

15.3.2 Пример настройки

Задача:

Настроить резервирование сессий firewall для VRRP-группы в unicast-режиме. Необходимо организовать резервирование для двух подсетей с помощью протокола VRRP, синхронизировать vrrp-процессы на маршрутизаторах.



Основные этапы решения задачи:

1) Необходимо настроить vrrp-процессы на маршрутизаторах. Для master будем использовать vrrp priority 20, для backup будем использовать vrrp priority 10.

2) Необходимо настроить firewall failover в режиме unicast с номером udp-порта 3333 для VRRP-группы.

3) Необходимо настроить зону безопасности для протокола vrrp и протокола udp.

Решение:

Настроим маршрутизатор ESR-1 (master).

Предварительно на интерфейсах настроим IP-адрес и определим принадлежность к зоне безопасности.

```
master(config)# interface gigabitethernet 1/0/1
master(config-if-gi)# security-zone trusted
master(config-if-gi)# ip address 192.0.2.3/24
master(config-if-gi)# exit
master(config)# interface gigabitethernet 1/0/2
master(config-if-gi)# security-zone trusted
master(config-if-gi)# ip address 203.0.113.1/30
master(config-if-gi)# exit
master(config)# interface gigabitethernet 1/0/3
master(config-if-gi)# security-zone trusted
master(config-if-gi)# ip address 198.51.100.3/24
master(config-if-gi)# exit
```

Настроим vrrp-процессы на интерфейсах. Необходимо настроить следующие параметры на интерфейсах маршрутизатора: идентификатор VRRP, IP-адрес VRRP, приоритет VRRP, принадлежность VRRP-маршрутизатора к группе.

Также дополнительно на backup необходимо настроить vrrp preempt delay, в результате чего появится время на установление синхронизации firewall перед тем, как backup-маршрутизатор попытается перехватить мастерство.

После чего необходимо включить vrrp-процесс с помощью команды **vrrp**.

⚠ Вместо настройки vrrp preempt delay есть возможность выбора режима работы vrrp preempt disable, в результате которого маршрутизатор с более высоким vrrp-приоритетом не будет забирать мастерство у маршрутизатора с более низким vrrp-приоритетом после возвращения в работу.

⚠ На маршрутизаторе необходимо установить принадлежность vrrp-процессов к одной группе для синхронизации состоянии vrrp-процессов (master, backup), а также для синхронизации сессий vrrp-процессов с помощью firewall failover.

```
master(config)# interface gigabitethernet 1/0/1
master(config-if-gi)# vrrp 1
master(config-vrrp)# ip address 192.0.2.1/24
master(config-vrrp)# priority 20
master(config-vrrp)# group 1
master(config-vrrp)# preempt delay 60
master(config-vrrp)# enable
master(config-vrrp)# exit
master(config)# interface gigabitethernet 1/0/3
master(config-if-gi)# vrrp 3
master(config-vrrp)# ip address 198.51.100.1/24
master(config-vrrp)# priority 20
master(config-vrrp)# group 1
master(config-vrrp)# preempt delay 60
master(config-vrrp)# enable
master(config-vrrp)# exit
```

Настроим общие параметры failover:

```
master(config)# ip failover
master(config-failover)# local-address 203.0.113.1
master(config-failover)# remote-address 203.0.113.2
master(config-failover)# vrrp-group 1
master(config-failover)# exit
```

Настроим firewall failover.

Выберем режим резервирование сессий unicast:

```
master(config)# ip firewall failover
master(config-firewall-failover)# sync-type unicast
```

Настроим номер UDP-порта службы резервирования сессий Firewall:

```
master(config-firewall-failover)# port 3333
```

Включим резервирования сессий Firewall:

```
master(config-firewall-failover)# enable
```

Для настройки правил зон безопасности потребуется создать профиль для порта firewall failover:

```
master(config)# object-group service failover
master(config-object-group-service)# port-range 3333
master(config-object-group-service)# exit
```

Дополнительно в security zone-pair trusted self необходимо разрешить следующие протоколы:

```
master(config)# security zone-pair trusted self
master(config-zone-pair)# rule 66
master(config-zone-pair-rule)# action permit
master(config-zone-pair-rule)# match protocol vrrp
master(config-zone-pair-rule)# enable
master(config-zone-pair-rule)# exit
master(config-zone-pair)# rule 67
master(config-zone-pair-rule)# action permit
master(config-zone-pair-rule)# match protocol udp
master(config-zone-pair-rule)# match destination-port object-group failover
master(config-zone-pair-rule)# enable
master(config-zone-pair-rule)# exit
master(config-zone-pair)# exit
```

Посмотреть статус vrrp-процессов есть возможность с помощью следующей команды:

```
master# show vrrp
Virtual router   Virtual IP                          Priority   Preemption   State    Inherit
Sync group ID
--------------   ---------------------------------   --------   ----------   ------   -------
-------------
1                192.0.2.1/24                       20         Enabled      Master   --
1
3                198.51.100.1/24                    20         Enabled      Master   --
1
```

Посмотреть состояние резервирования сессий Firewall есть возможность с помощью следующей команды:

```
master# show ip firewall failover
Communication interface:                    gigabitethernet 1/0/2
Status:                                     Running
Bytes sent:                                 2496
Bytes received:                             640
Packets sent:                               271
Packets received:                           40
Send errors:                                0
Receive errors:                             0
```

Посмотреть состояние систем резервирования устройства есть возможность с помощью следующей команды:

```
master# show high-availability state
AP Tunnels:
    State:                          Disabled
    Last state change:              --
DHCP server:
    State:                          Disabled
    Last state change:              --
Firewall sessions:
    State:                          successful synchronization
    Last synchronization:           09:38:00 05.08.2021
```

Настроим маршрутизатор ESR-2 (backup).

Настройка интерфейсов:

```
backup(config)# interface gigabitethernet 1/0/1
backup(config-if-gi)# security-zone trusted
backup(config-if-gi)# ip address 192.0.2.2/24
backup(config-if-gi)# vrrp 1
backup(config-vrrp)# ip address 192.0.2.1/24
backup(config-vrrp)# priority 10
backup(config-vrrp)# group 1
backup(config-vrrp)# enable
backup(config-vrrp)# exit
```

```
backup(config)# interface gigabitethernet 1/0/2
backup(config-if-gi)# security-zone trusted
backup(config-if-gi)# ip address 203.0.113.2/30
backup(config-if-gi)# exi
```

```
backup(config)# interface gigabitethernet 1/0/3
backup(config-if-gi)# security-zone trusted
backup(config-if-gi)# ip address 198.51.100.2/24
backup(config-if-gi)# vrrp 3
backup(config-vrrp)# ip address 198.51.100.1/24
backup(config-vrrp)# priority 10
backup(config-vrrp)# group 1
backup(config-vrrp)# enable
backup(config-vrrp)# exit
```

Настройка firewall failover:

```
backup(config)# ip failover
backup(config-failover)# local-address 203.0.113.2
backup(config-failover)# remote-address 203.0.113.1
backup(config-failover)# vrrp-group 1
backup(config-failover)# exit
backup(config)# ip firewall failover
backup(config-firewall-failover)# sync-type unicast
backup(config-firewall-failover)# port 3333
backup(config-firewall-failover)# enable
```

Настройка зоны безопасности аналогична настройки на маршрутизаторе ESR-1 (master).

15.4 Настройка DHCP failover

DHCP failover используется для резервирования базы IP-адресов, которые были динамически выданы в процессе работы DHCP-server.

15.4.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перед настройкой сервисов резервирования необходимо настроить общие параметры failover.		
2	Переход в конфигурационное меню общих настроек failover-сервисов.	**esr(config)# ip failover [vrf <VRF>]**	<VRF> – имя VRF, задается строкой до 31 символа;
3	Установка IP-адреса, на котором failover-сервисы принимают failover-сообщения при работе в режиме резервирования.	**esr(config-failover)# local-address { <ADDR> | object-group <NETWORK_OBJ_GROUP_NAME> }**	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве local address.
4	Установка IP-адреса, на который failover сервисы отправляют failover-сообщения при работе в режиме резервирования.	**esr(config-failover)# remote-address { <ADDR> | object-group <NETWORK_OBJ_GROUP_NAME> }**	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве local address.
5	Выбор VRRP-группы, по состоянию которой будет определятся мастерство при работе failover сервисов в режиме Active-Standby.	**esr(config-failover)# vrrp-group <GRID>**	<GRID> – идентификатор группы VRRP-маршрутизатора, принимает значения [1..32].
6	Переход в конфигурационное меню DHCP failover для его настройки.	**esr(config)# ip dhcp-server failover [vrf <VRF>]**	<VRF> – имя VRF, задается строкой до 31 символа;
7	Выбор режима работы DHCP failover.	**esr(config-dhcp-server-failover)# mode { active-active | active-standby }**	active-active – режим работы с двумя активными маршрутизаторами; active-standby – режим работы с одним активным маршрутизатором и одним резервным.

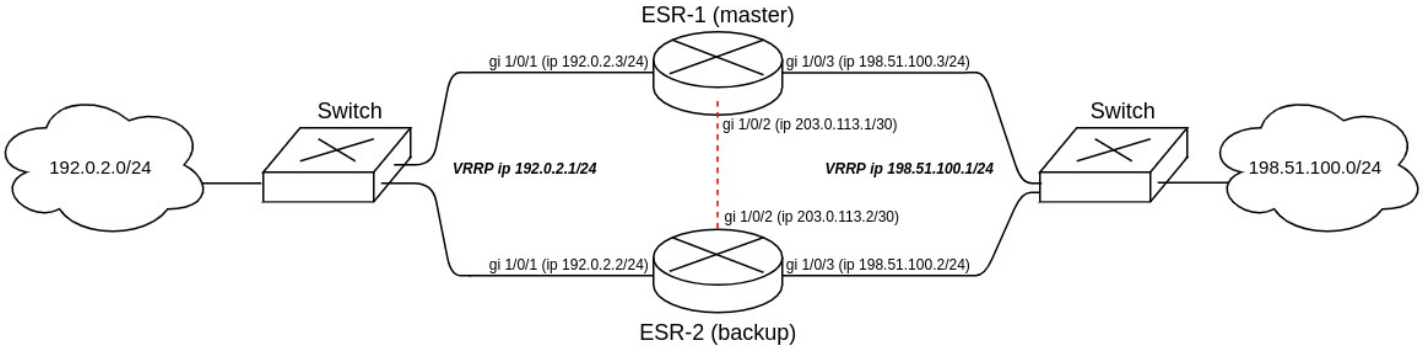
Шаг	Описание	Команда	Ключи
8	Настройка роли DHCP failover, при работе резервирования в режиме Active-Active.	**esr(config-dhcp-server-failover)# role <ROLE>**	<ROLE> – роль DHCP-сервера при работе в режиме резервирования: • primary – режим активного DHCP-сервера; • secondary – режим резервного DHCP-сервера.
9	Включение резервирования DHCP failover.	**esr(config-dhcp-server-failover)# enable**	

⚠ Режим active-standby не поддержан в VRF.

15.4.2 Пример настройки

Задача:

Настроить резервирование DHCP-сервера в режиме Active-Standby. Необходимо организовать резервирование для двух подсетей с помощью протокола VRRP, синхронизировать vrrp-процессы на маршрутизаторах.



Основные этапы решения задачи:

1) Необходимо настроить vrrp-процессы на маршрутизаторах. Для master будем использовать vrrp priority 20, для backup будем использовать vrrp priority 10.

2) Необходимо настроить DHCP failover в режиме Active-Standby.

3) Необходимо настроить зону безопасности для протоколов vrrp, udp и tcp.

Решение:

1. Настройка маршрутизатора ESR-1 (master).

Предварительно на интерфейсах настроим IP-адрес и определим принадлежность к зоне безопасности.

```
master(config)# interface gigabitethernet 1/0/1
master(config-if-gi)# security-zone trusted
master(config-if-gi)# ip address 192.0.2.3/24
master(config-if-gi)# exit
master(config)# interface gigabitethernet 1/0/2
master(config-if-gi)# security-zone trusted
master(config-if-gi)# ip address 203.0.113.1/30
master(config-if-gi)# exit
master(config)# interface gigabitethernet 1/0/3
master(config-if-gi)# security-zone trusted
master(config-if-gi)# ip address 198.51.100.3/24
master(config-if-gi)# exit
```

Настроим vrrp-процессы на интерфейсах. Необходимо настроить следующие параметры на интерфейсах маршрутизатора: идентификатор VRRP, IP-адрес VRRP, приоритет VRRP, принадлежность VRRP-маршрутизатора к группе.

После чего необходимо включить vrrp-процесс с помощью команды "vrrp".

⚠ Вместо настройки vrrp preempt delay есть возможность выбора режима работы vrrp preempt disable, в результате которого маршрутизатор с более высоким vrrp-приоритетом не будет забирать мастерство у маршрутизатора с более низким vrrp-приоритетом после возвращения в работу.

⚠ На маршрутизаторе необходимо установить принадлежность vrrp-процессов к одной группе для синхронизации состоянии vrrp-процессов (master, backup).

```
master(config)# interface gigabitethernet 1/0/1
master(config-if-gi)# vrrp 1
master(config-vrrp)# ip address 192.0.2.1/24
master(config-vrrp)# priority 20
master(config-vrrp)# group 1
master(config-vrrp)# enable
master(config-vrrp)# exit
master(config)# interface gigabitethernet 1/0/3
master(config-if-gi)# vrrp 3
master(config-vrrp)# ip address 198.51.100.1/24
master(config-vrrp)# priority 20
master(config-vrrp)# group 1
master(config-vrrp)# enable
master(config-vrrp)# exit
```

Настроим DHCP failover. Для DHCP failover необходимо настроить следующие параметры: mode, local-address, remote-address, принадлежность VRRP-маршрутизатора к группе.

```
master(config)# ip dhcp-server pool LAN
master(config-dhcp-server)# network 192.0.2.0/24
master(config-dhcp-server)# address-range 192.0.2.10-192.0.2.20
master(config-dhcp-server)# exit
master(config)# ip dhcp-server
master(config)# ip failover
master(config-failover)# local-address 203.0.113.1
master(config-failover)# remote-address 203.0.113.2
master(config-failover)# vrrp-group 1
master(config-failover)# exit
master(config)# ip dhcp-server failover
master(config-dhcp-server-failover)# mode active-standby
master(config-dhcp-server-failover)# enable
master(config-dhcp-server-failover)# exit
```

⚠ Для запуска DHCP failover необходимо предварительно настроить и включить DHCP-server, который будет резервироваться.

Для настройки правил зон безопасности потребуется создать профиль для порта DHCP failover:

```
master(config)# object-group service dhcp_failover
master(config-object-group-service)# port-range 873
master(config-object-group-service)# exit
```

⚠ DHCP failover для синхронизации использует TCP-порт 873, его необходимо разрешить при настройке firewall.

Дополнительно в security zone-pair trusted self необходимо разрешить следующие протоколы:

```
master(config)# security zone-pair trusted self
master(config-zone-pair)# rule 66
master(config-zone-pair-rule)# action permit
master(config-zone-pair-rule)# match protocol vrrp
master(config-zone-pair-rule)# enable
master(config-zone-pair-rule)# exit
master(config-zone-pair)# rule 67
master(config-zone-pair-rule)# action permit
master(config-zone-pair-rule)# match protocol tcp
master(config-zone-pair-rule)# match destination-port object-group dhcp_failover
master(config-zone-pair-rule)# enable
master(config-zone-pair-rule)# exit
master(config-zone-pair)# rule 68
master(config-zone-pair-rule)# action permit
master(config-zone-pair-rule)# match protocol udp
master(config-zone-pair-rule)# enable
master(config-zone-pair-rule)# exit
```

Посмотреть статус vrrp-процессов есть возможность с помощью следующей команды:

```
master# show vrrp
Virtual router   Virtual IP                          Priority   Preemption   State    Inherit
Sync group ID
--------------   ---------------------------------   --------   ----------   ------   -------
-------------
1                192.0.2.1/24                        20         Enabled      Master   --
1
3                198.51.100.1/24                     20         Enabled      Master   --
1
```

Посмотреть состояние резервирования сессий Firewall есть возможность с помощью следующей команды:

```
master# show ip dhcp server failover
VRF:       --
    State: Successful
```

Посмотреть состояние систем резервирования устройства есть возможность с помощью следующей команды:

```
master# show high-availability state
AP Tunnels:
    State:                          Disabled
    Last state change:              --
DHCP option 82 table:
    State:                          Disabled
    Last state change:              --
DHCP server:
VRF:                                --
    State:                          Successful synchronization
    State:                          Disabled
    Last synchronization:           --
```

⚠ Для успешной синхронизации сервиса DHCP failover на устройствах должно быть выставлено идентичное время.

2. Настройка маршрутизатора ESR-2 (backup).

Настройка интерфейсов:

```
backup(config)# interface gigabitethernet 1/0/1
backup(config-if-gi)#   security-zone trusted
backup(config-if-gi)#   ip address 192.0.2.2/24
backup(config-if-gi)# vrrp 1
backup(config-vrrp)# ip address 192.0.2.1/24
backup(config-vrrp)# priority 20
backup(config-vrrp)# group 1
backup(config-vrrp)# enable
backup(config-vrrp)# exit
backup(config)# interface gigabitethernet 1/0/2
backup(config-if-gi)#   security-zone trusted
backup(config-if-gi)#   ip address 203.0.113.2/30
backup(config-if-gi)# exit
backup(config)# interface gigabitethernet 1/0/3
backup(config-if-gi)#   security-zone trusted
backup(config-if-gi)#   ip address 198.51.100.2/24
backup(config-if-gi)# vrrp 3
backup(config-vrrp)# ip address 198.51.100.1/24
backup(config-vrrp)# priority 10
backup(config-vrrp)# group 1
backup(config-vrrp)# enable
backup(config-vrrp)# exit
```

Настройка DHCP failover:

```
backup(config)# ip dhcp-server pool LAN
backup(config-dhcp-server)#   network 192.0.2.0/24
backup(config-dhcp-server)#   address-range 192.0.2.10-192.0.2.20
backup(config-dhcp-server)# exit
backup(config)# ip dhcp-server
backup(config)# ip failover
backup(config-failover)# local-address 203.0.113.2
backup(config-failover)# remote-address 203.0.113.1
backup(config-failover)# vrrp-group 1
backup(config-failover)# exit
backup(config)# ip dhcp-server failover
backup(config-dhcp-server-failover)#   mode active-standby
backup(config-dhcp-server-failover)#   enable
backup(config-dhcp-server-failover)# exit
```

Настройка зоны безопасности аналогична настройке на маршрутизаторе ESR-1 (master).

16 Управление кластеризацией

16.1 Настройка кластера

Кластер используется для резервирования устройств в сети. Резервирование обеспечивается за счет синхронизации работы различных сервисов между устройствами, а также за счет организации единой конфигурации и единой точки управления устройствами.

16.1.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Сменить юнит у устройства, при необходимости. (смена юнита устройства вступает в силу после перезагрузки)	**esr# set unit id <ID>**	<ID> – номер юнита, принимает значения [1..4].
2	Создать VLAN, который будет использоваться в кластерном интерфейсе. Можно также использовать vlan 1, созданный по умолчанию.	**esr(config)# vlan <VID>**	<VID> – идентификатор VLAN, задаётся в диапазоне [2..4094].
3	Перейти в режим конфигурирования физических интерфейсов, которые будут использованы для работы кластерного интерфейса. Необходимо настроить интерфейсы всех юнитов, которые будут участвовать в кластере.	**esr(config)# interface gigabitethernet** **esr(config)# interface tengigabitethernet** **esr(config)# interface fourtygigabitethernet** **esr(config)# interface twentyfivegigabitethernet**	
4	Установить режим работы физических интерфейсов.	**esr(config-if-gi)# mode switchport**	Допустимо для всех ESR.
		esr(config-if-gi)# mode hybrid	Допустимо только для ESR-1000/1200/1500/1511(rev.B)/1700.
5	Задать режим работы L2-интерфейсов.	**esr(config-if-gi)# switchport mode access**	Только для ESR-10/12V(F)/15/15R/15VF/20/21/30/31/100/200/3100/3150/3200/3200L/3250/3300/3350. Данный режим является режимом по умолчанию и не отображается в конфигурации.
		esr(config-if-gi)# switchport mode trunk	Только для ESR-10/12V(F)/15/15R/15VF/20/21/30/31/100/200/3100/3150/3200/3200L/3250/3300/3350.

Шаг	Описание	Команда	Ключи
		esr(config-if-gi)# switchport mode general	Только для ESR-1000/1200/1500/ 1511 (rev.B)/1700. Данный режим является режимом по умолчанию и не отображается в конфигурации.
6	Настроить заранее созданный VLAN на интерфейсах.	**esr(config-if-gi)# switchport access vlan <VID>**	Только для ESR-10/12V(F)/ 15/15R/15VF/20/21/30/31/ 100/200/3100/3150/3200/ 3200L/3250/3300/3350. <VID> – идентификационный номер VLAN, задаётся в диапазоне [1…4094].
		esr(config-if-gi)# switchport trunk allowed vlan <ACT> <VID>	Для ESR-10/12V(F)/15/15R/ 15VF/20/21/30/31/100/200/ 3100/3150/3200/3200L/ 3250/3300/3350. <ACT> – назначаемое действие: **add** – включение интерфейса во VLAN; **remove** – исключение интерфейса из VLAN. <VID> – идентификационный номер VLAN, задаётся в диапазоне [2…4094]. Можно задать диапазоном через «-» или перечислением через «,».

Шаг	Описание	Команда	Ключи
		esr(config-if-gi)# switchport general allowed vlan <ACT> <VID> [<TYPE>]	Для ESR-1000/1200/1500/1511 (rev.B)/1700. <ACT> – назначаемое действие: **add** – включение интерфейса во VLAN; **remove** – исключение интерфейса из VLAN. <VID> – идентификационный номер VLAN, задаётся в диапазоне [2…4094]. Можно задать диапазоном через «-» или перечислением через «,»; <TYPE> – тип пакета: **tagged** – интерфейс будет передавать и принимать пакеты в указанных VLAN тегированными; **untagged** – интерфейс будет передавать пакеты в указанных VLAN нетегированными. VLAN, в который будут направлены входящие нетегированные пакеты, настраивается командой **switchport general pvid**.
7	Перейти в режим конфигурирования сетевого моста, который будет использован в качестве кластерного интерфейса.	**esr(config)# bridge <BR-NUM>**	<BR-NUM> – номер сетевого моста.
8	Настроить заранее созданный VLAN на кластерном интерфейсе.	**esr(config-bridge)# vlan <VID>**	<VID> – идентификационный номер VLAN, задаётся в диапазоне [1…4094].

Шаг	Описание	Команда	Ключи
9	Указать IPv4-адрес и маску подсети для кластерного интерфейса. Необходимо установить адреса для всех юнитов кластера. (для работы кластерного интерфейса поддерживается только IPv4-адресация)	**esr(config-bridge)# ip address <ADDR/LEN> [unit <ID>]**	<ADDR/LEN> – IP-адрес и длина маски подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. <ID> – номер юнита, принимает значения [1..4]. Дополнительные функции IPv4-адресации см. в разделе Настройка IP-адресации.
10	Установить номер экземпляра VRRP-процесса.	**esr(config-bridge)# vrrp <VRRP-NUM>**	<VRRP-NUM> – номер экземпляра VRRP-процесса, принимает значения [1..255]. Дополнительные функции VRRP-процесса см. в разделе Управление резервированием.
11	Установить виртуальный IP-адрес VRRP-маршрутизатора (адрес должен быть из той же подсети, что и ip address у юнитов).	**esr(config-vrrp)# ip address <ADDR/LEN> [secondary]**	<ADDR/LEN> – виртуальный IP-адрес и длина маски, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. Можно указать несколько IP-адресов перечислением через запятую. Может быть назначено до 8 IP-адресов на интерфейс. secondary – ключ для установки дополнительного IP-адреса.
12	Установить принадлежность VRRP-маршрутизатора к группе. Группа предоставляет возможность синхронизировать несколько VRRP-процессов, так если в одном из процессов произойдет смена мастера, то в другом процессе также произойдёт смена ролей.	**esr(config-vrrp)# group <GRID>**	<GRID> – идентификатор группы VRRP-маршрутизатора, принимает значения [1..32]

Шаг	Описание	Команда	Ключи
13	Включить VRRP-процесс на IP-интерфейсе.	**esr(config-vrrp)# enable**	
14	Активировать сетевой мост.	**esr(config-bridge)# enable**	
15	Перейти в режим конфигурирования кластера.	**esr(config)# cluster**	
16	Установить интерфейс, через который будет происходить обмен служебными сообщениями между юнитами в кластере.	**esr(config-cluster)# cluster-interface bridge [<BRIDGE-ID>]**	<BRIDGE-ID> – идентификационный номер моста, задается в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора.
17	Отключить синхронизацию конфигураций в кластере между юнитами (не обязательно).	**esr(config-cluster)# sync config disable**	
18	Перейти в режим конфигурирования юнита в кластере.	**esr(config-cluster)# unit <ID>**	<ID> – номер юнита, принимает значения [1..4].
19	Настроить для юнита соответствующий системный MAC-адрес устройства.	**esr(config-cluster-unit)# mac-address <ADDR>**	<ADDR> – MAC-адрес сетевого моста, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF].
20	Включить работу кластера.	**esr(config-cluster)# enable**	

⚠ Данные между юнитами кластера через канал синхронизации передаются в открытом виде. Также все вводимые команды конфигурирования, содержащие чувствительную информацию не в encrypted-виде, будут переданы в том же виде, в котором введены, после чего будут преобразованы в encrypted-вид.

16.1.2 Пример настройки кластера

В настоящем руководстве приведено описание настройки кластера для администратора сервисного маршрутизатора ESR (далее — маршрутизатор).



Схема реализации HA Cluster из 2 юнитов

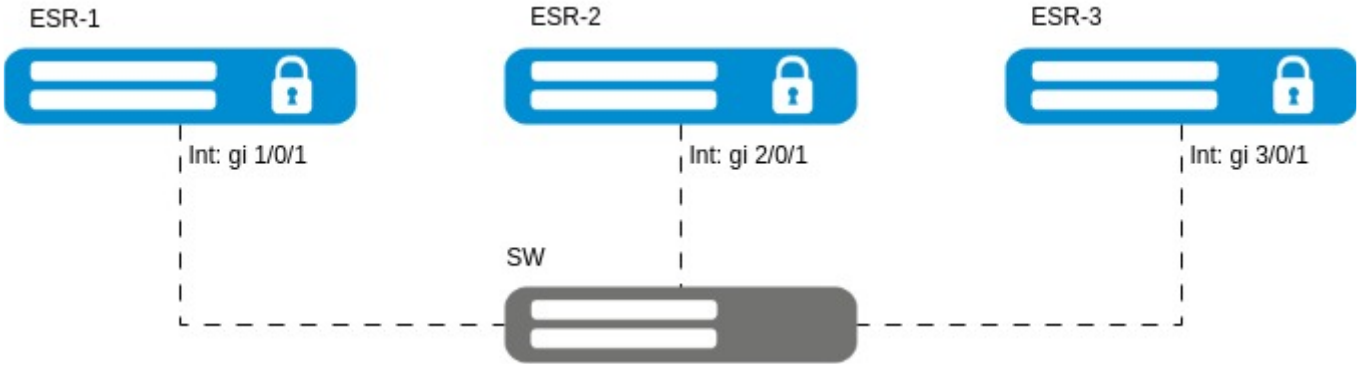


Схема реализации HA Cluster из 3 юнитов

⚠ В примере настройки кластера будет рассмотрен HA Cluster из 2 юнитов.
Для настройки более чем 2 юнитов в кластере необходимо дополнить конфигурацию юнитизированными командами по аналогии с указанным примером.

Первичная настройка кластера

Для начала работы необходимо полностью настроить одно устройство из кластера.

После включения устройства примените конфигурацию по умолчанию на устройствах, предназначенных для объединения в кластер:

ESR-1

```
esr# copy system:default-config system:candidate-config
Entire candidate configuration will be reset to default, all settings will be lost upon commit.
Do you really want to continue? (y/N): y
|****************************************| 100% (59B) Default configuration loaded
successfully.
```

Для более удобного и ясного восприятия рекомендуется переименовать устройства. В кластерной версии прошивки предусмотрена возможность указать имя устройства с привязкой к юниту. Устройство будет использовать только тот hostname, юнитом которого он является:

ESR-1

```
esr# configure
esr(config)# hostname ESR-1 unit 1
esr(config)# hostname ESR-2 unit 2
```

⚠ В конфигурации может одновременно находиться hostname с unit и hostname без unit.
Более приоритетным является **hostname**, указанный с привязкой к **unit**.

Чтобы изменить юнит устройства, выполните следующие команды:

ESR-1

```
ESR-1# set unit id 1
Unit ID will be 1 after reboot
ESR-1# reload system
Do you really want to reload system now? (y/N): y
```

⚠ Смена юнита устройства вступает в силу после перезагрузки.

⚠ При изменении номера юнита маршрутизатора не происходит автоматической конвертации конфигурации.
В случае если до маршрутизатора настроен удаленный доступ и у него меняется номер юнита, необходимо до перезагрузки настроить ip-интерфейсы для нового юнита аналогично текущим.

⚠ В заводской конфигурации присутствуют настройки интерфейсов только для юнита по умолчанию (unit = 1).
При копировании и применении заводской конфигурации настройка номера юнита не изменяется на значение по умолчанию.
Установить номер юнита по умолчанию возможно следующими способами:
1. используя консольное подключение;
2. зажав функциональную кнопку "F" на 15 секунд.

Убедитесь в том, что настройка юнита применилась успешно:

ESR-1

```
ESR-1# show unit id
Unit ID is 1
Unit ID will be 1 after reboot
```

⚠ Объединение устройств в кластер невозможно, если они относятся к одному и тому же юниту. Исключение — процесс ZTP, так как в процессе ZTP нужный unit у устройства выставится автоматически.

⚠ Для объединения в кластер vESR предварительно необходимо сделать разные системные MAC-адреса на устройствах путем смены серийного номера.

Настройка кластерного интерфейса

Для полноценной работы кластера требуется сконфигурировать кластерный интерфейс, который будет использоваться для передачи control plane трафика. В качестве кластерного интерфейса назначен bridge. В качестве механизма, отвечающего за определение ролей устройств, участвующих в резервировании, назначен протокол VRRP. Настройки cluster-интерфейса должны быть идентичны для всех участников кластера.

Так как кластер выполняет синхронизацию состояний между устройствами, необходимо создать зону безопасности SYNC (synchronization):

ESR-1

```
ESR-1(config)# security zone SYNC
ESR-1(config-security-zone)# exit
```

Далее перейдите к настройкам кластерного интерфейса:

ESR-1

```
ESR-1(config)# bridge 1
```

⚠ В текущей версии ПО в качестве cluster-интерфейса поддержан только bridge.

Укажите, к какому VLAN относится bridge, и зону безопасности:

ESR-1

```
ESR-1(config-bridge)# vlan 1
ESR-1(config-bridge)# security-zone SYNC
```

Далее укажите IP-адреса:

ESR-1

```
ESR-1(config-bridge)# ip address 198.51.100.254/24 unit 1
ESR-1(config-bridge)# ip address 198.51.100.253/24 unit 2
```

⚠ Для работы кластерного интерфейса поддерживается только IPv4-адресация.
На cluster-интерфейсе необходима настройка адресов с привязкой к unit. Количество настраиваемых адресов зависит от количества настраиваемых участников кластера.

Настройте идентификатор VRRP, принадлежность VRRP-маршрутизатора к группе, IP-адрес VRRP:

ESR-1

```
ESR-1(config-bridge)# vrrp 1
ESR-1(config-vrrp)# group 1
ESR-1(config-vrrp)# ip address 198.51.100.1/24
```

⚠ Адрес VRRP должен быть из той же подсети, что и адреса на интерфейсе.

Также на VRRP-интерфейсе можно назначить разные приоритеты для разных юнитов.

ESR-1

```
ESR-1(config-vrrp)# priority 254 unit 1
ESR-1(config-vrrp)# priority 253 unit 2
```

Включите протокол VRRP и bridge:

ESR-1

```
ESR-1(config-vrrp)# enable
ESR-1(config-vrrp)# exit
ESR-1(config-bridge)# enable
ESR-1(config-bridge)# exit
```

Настройте физические порты для выделенного линка синхронизации маршрутизаторов ESR-1 и ESR-2:

ESR-1

```
ESR-1(config)# interface gigabitethernet 1/0/1
ESR-1(config-if-gi)# description "Network: SYNC"
ESR-1(config-if-gi)# mode switchport
ESR-1(config-if-gi)# exit
ESR-1(config)# interface gigabitethernet 2/0/1
ESR-1(config-if-gi)# description "Network: SYNC"
ESR-1(config-if-gi)# mode switchport
ESR-1(config-if-gi)# exit
```

Для проверки работы протокола VRRP выполните следующую команду:

ESR-1

```
esr-30# show vrrp
Virtual router   Virtual IP                          Priority   Preemption   State    Inherit
Sync group ID
--------------   ---------------------------------   --------   ----------   ------   -------
-----------
1                198.51.100.1/24                     100        Disabled     Backup   --
1
```

Можно увидеть, что устройство приняло состояние Backup. Через 10 секунд устройство примет состояние Master.

Настройка кластера

Для запуска кластера необходимо указать заранее настроенный кластерный интерфейс и юниты, которые будут выполнять роли Active и Standby.

Перейдите в режим настройки кластера:

ESR-1

```
ESR-1(config)# cluster
```

Настройте юниты:

ESR-1

```
ESR-1(config-cluster)# unit 1
ESR-1(config-cluster-unit)# mac-address E4:5A:D4:A0:BE:35
ESR-1(config-cluster-unit)# exit
ESR-1(config-cluster)# unit 2
ESR-1(config-cluster-unit)# mac-address A8:F9:4B:AF:35:84
ESR-1(config-cluster-unit)# exit
```

⚠ В качестве mac-address указывается системный MAC-адрес устройства, его можно узнать с помощью команды **show system | include MAC**.

Укажите кластерный интерфейс, созданный ранее, и активируйте кластер:

ESR-1

```
ESR-1(config-cluster)# cluster-interface bridge 1
ESR-1(config-cluster)# enable
ESR-1(config-cluster)# exit
```

Первое устройство полностью настроено и готово к работе.
Аналогичные настройки необходимо произвести на втором устройстве, предварительно сменив у него юнит на требуемый. Также возможна настройка второго устройства средствами ZTP.

⚠ Для активации процесса ZTP необходимо на втором устройстве запустить dhcp-client на bridge-интерфейсе, логический или физический интерфейс которого будет включен в кластерный интерфейс первого устройства.
В качестве примера такой конфигурации подойдет factory-конфигурация (в factory-конфигурации для vESR нет настроенного dhcp-client).
В процессе ZTP устройство автоматически выставит себе:
1) Конфигурацию;
2) Юнит;
3) Версию ПО, на котором работает Active ESR;
4) Лицензию, если она предварительно загружена на Active ESR.

После выполнения этих шагов кластер будет успешно запущен. Текущее состояние кластера можно узнать, выполнив команду:

ESR-1

```
ESR-1# show cluster status
Unit   Hostname              Role         MAC address         State          IP address
----   --------------------  -----------  ------------------  -------------  ---------------
1*     ESR-1                 Active       e4:5a:d4:a0:be:35   Joined         198.51.100.254
2      ESR-2                 Standby      a8:f9:4b:af:35:84   Joined         198.51.100.253
```

После включения кластера и установления юнитов в состояние Joined дальнейшее конфигурирование устройств осуществляется настройкой Active-устройства.
Синхронизируются команды конфигурации, а также команды: **commit**, **confirm**, **rollback**, **restore**, **save, copy <source> system:candidate-config**.
В случае, если конфигурирование осуществляется на Standby, то внесенные изменения в конфигурацию засинхронизированы не будут. Все внесённые изменения в конфигурацию Standby будут потеряны при выполнении **commit** на Active-устройстве.
Есть возможность отключения синхронизации командой **sync config disable**.

Текущее состояние синхронизации подсистем кластера можно узнать, выполнив команду:

ESR-1

```
ESR-1# show cluster sync status
System part              Synced
-----------------------  ------
candidate-config         Yes
running-config           Yes
SW version               Yes
licence                  Yes
licence (After reboot)   Yes
date                     Yes
```

В текущей версии ПО не поддержано синхронное шифрование паролей, вводимых не в encryption-виде.
Такие пароли будут зашифрованы каждым из участников кластера самостоятельно.

Через минуту после включения кластера синхронизируется время, на Standby установится время Active-юнита.
Синхронизация времени проверяется раз в минуту, в случае расхождения время синхронизируется.

Работа с лицензиями в кластере описана в разделе Лицензирование в кластере.

16.2 Подключение сервисов

После успешной настройки кластера можно приступать к конфигурации различных сервисов.

16.2.1 Настройка System prompt

System prompt позволяет отобразить оперативное состояние кластера непосредственно в строке приглашения CLI устройства, что упрощает получение актуальной информации.

Варианты настройки system prompt, включая доступные параметры и синтаксис команды, приведены в разделе Настройка общесистемных параметров.

Пример настройки

Задача:

Настроить system prompt в кластере маршрутизаторов ESR-1 и ESR-2 со следующими параметрами:

- необходимо получать информацию о статусе полной синхронизации кластера;
- необходимо получать информацию о номере юнита администрируемого устройства;
- необходимо получать информацию о роли устройства в кластере;
- необходимо получать информацию о статусе кластерного VRRP;
- необходимо получать информацию о hostname устройства.

Исходная конфигурация кластера:

ESR-1

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address cc:9d:a2:71:83:78
  exit
  unit 2
    mac-address cc:9d:a2:71:82:38
  exit
  enable
exit

hostname ESR-1 unit 1
hostname ESR-2 unit 2

security zone SYNC
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  vrrp 1
    ip address 198.51.100.1/24
    priority 254 unit 1
    priority 253 unit 2
    group 1
    enable
  exit
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/1
  mode switchport
  spanning-tree disable
exit

security zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
exit
```

Решение:

Перейдем в режим конфигурирования устройства:

ESR-1

```
ESR-1# configure
ESR-1(config)#
```

Добавим в system prompt информацию о статусе полной синхронизации кластера:

ESR-1

```
ESR-1(config)# system prompt '(Cluster: %s%)'
```

Добавим в system prompt информацию о номере юнита администрируемого устройства:

ESR-1

```
ESR-1(config)# system prompt '(Cluster: %s% | Unit: %u%)'
```

Добавим в system prompt информацию о роли устройства в кластере:

ESR-1

```
ESR-1(config)# system prompt '(Cluster: %s% | Unit: %u% | State: %r%)'
```

Добавим в system prompt информацию о статусе кластерного VRRP:

ESR-1

```
ESR-1(config)# system prompt '(Cluster: %s% | Unit: %u% | State: %r% | VRRP id 1: %v1%)'
```

Добавим в system prompt информацию о hostname устройства:

ESR-1

```
ESR-1(config)# system prompt '(Cluster: %s% | Unit: %u% | State: %r% | VRRP id 1: %v1%)|%h%'
```

Применим конфигурацию и обновим пользовательскую сессию CLI:

ESR-1

```
ESR-1# commit
Configuration has been successfully applied and saved to flash. Commit timer started, changes
will be.
ESR-1# confirm
Configuration has been confirmed. Commit timer canceled.
ESR-1# exit

ESR-1 login: admin
Password:

****************************************
*            Welcome to ESR            *
****************************************

(Cluster: Yes | Unit: 1 | State: Active | VRRP id 1: Master)|ESR-1#
```

Обновим пользовательскую сессию CLI на втором устройстве:

ESR-2

```
ESR-2# 2024-12-27T15:25:04+00:00 %CLUSTER-I-SYNC_CONFIG_INFO: unit 1 'ESR-1' starts a
synchronous operation 'commit'
2024-12-27T15:25:09+00:00 %CLUSTER-I-SYNC_CONFIG_INFO: 'commit' successful performed
ESR-2# exit

ESR-2 login: admin
Password:

****************************************
*            Welcome to ESR            *
****************************************

(Cluster: Yes | Unit: 2 | State: Standby | VRRP id 1: Backup)|ESR-2#
```

⚠ Чтобы system prompt корректно работал, необходимо обновить пользовательскую сессию.

16.2.2 Настройка Port-channel U/N

Port-channel U/N позволяет объединять каналы в группы агрегации для конкретного устройства в составе группы (unit), обеспечивая единообразие конфигурации кластера и возможность индивидуальной настройки агрегации на каждом юните.

Варианты настройки port-channel, включая доступные параметры и синтаксис команды, приведены в разделе Типы и порядок именования интерфейсов маршрутизатора.

Пример настройки

Задача:

Настроить port-channel U/N в кластере маршрутизаторов ESR-1 и ESR-2 для передачи Control Plane-трафика кластера через агрегированный интерфейс.



Схема реализации port-channel U/N

Исходная конфигурация кластера:

ESR-1

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address cc:9d:a2:71:83:78
  exit
  unit 2
    mac-address cc:9d:a2:71:82:38
  exit
  enable
exit

hostname ESR-1 unit 1
hostname ESR-2 unit 2

security zone SYNC
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  vrrp 1
    ip address 198.51.100.1/24
    priority 254 unit 1
    priority 253 unit 2
    group 1
    enable
  exit
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/1
  mode switchport
  spanning-tree disable
exit

security zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
exit
```

Создадим для каждого юнита собственный агрегированный интерфейс:

ESR-2

```
ESR-1(config)# interface port-channel 1/1
ESR-1(config-if-port-channel)# mode switchport
ESR-1(config-if-port-channel)# description Control-Plane
ESR-1(config-if-port-channel)# exit
ESR-1(config)# interface port-channel 2/1
ESR-1(config-if-port-channel)# mode switchport
ESR-1(config-if-port-channel)# description Control-Plane
ESR-1(config-if-port-channel)# exit
```

Добавим каналы в агрегированные интерфейсы, которые отвечает за Control Plane кластера и применим конфигурацию:

ESR-2

```
ESR-1(config)# interface gigabitethernet 1/0/1
ESR-1(config-if-gi)# channel-group 1 mode auto
ESR-1(config-if-gi)# exit
ESR-1(config)# interface gigabitethernet 2/0/1
ESR-1(config-if-gi)# channel-group 1 mode auto
ESR-1(config-if-gi)# exit
ESR-1(config)# interface gigabitethernet 1/0/2
ESR-1(config-if-gi)# mode switchport
ESR-1(config-if-gi)# channel-group 1 mode auto
ESR-1(config-if-gi)# spanning-tree disable
ESR-1(config-if-gi)# exit
ESR-1(config)# interface gigabitethernet 2/0/2
ESR-1(config-if-gi)# mode switchport
ESR-1(config-if-gi)# channel-group 1 mode auto
ESR-1(config-if-gi)# spanning-tree disable
ESR-1(config-if-gi)# exit
ESR-1# commit
Configuration has been successfully applied and saved to flash. Commit timer started, changes
will be.
ESR-1# confirm
Configuration has been confirmed. Commit timer canceled.
```

Проверить состояние работы port-channel можно с помощью команды:

ESR-2

```
ESR-1# show interfaces status port-channel

Unit 1* 'ESR-1'
---------------
Interface               Admin        Link    MTU     MAC address         Last change     Mode
State        State                                  (d,h:m:s)
---------------------   ----------   -----   -----   -----------------   -------------
------------
po1/1                   Up           Up      1500    a8:f9:4b:ad:07:f9
00,00:26:29     switchport


Unit 2 'ESR-2'
--------------
Interface               Admin        Link    MTU     MAC address         Last change     Mode
State        State                                  (d,h:m:s)
---------------------   ----------   -----   -----   -----------------   -------------
------------
po2/1                   Up           Up      1500    a8:f9:4b:ac:e8:9d
00,00:26:29     switchport
```

⚠ Юнитизированный агрегированный интерфейс для Control Plane-трафика показан как пример. Можно использовать и для передачи Data Plane-трафика.

16.2.3 Настройка MultiWAN

Технология MultiWAN позволяет организовать отказоустойчивое соединение с резервированием линков от нескольких провайдеров.

Алгоритм настройки MultiWAN описан в разделе Алгоритм настройки MultiWAN.

Пример настройки

Задача:

Настроить MultiWAN в кластере маршрутизаторов ESR-1 и ESR-2 со следующими параметрами:

- обеспечить резервирование линков от нескольких провайдеров;
- обеспечить балансировку трафика в соотношении 70/30.

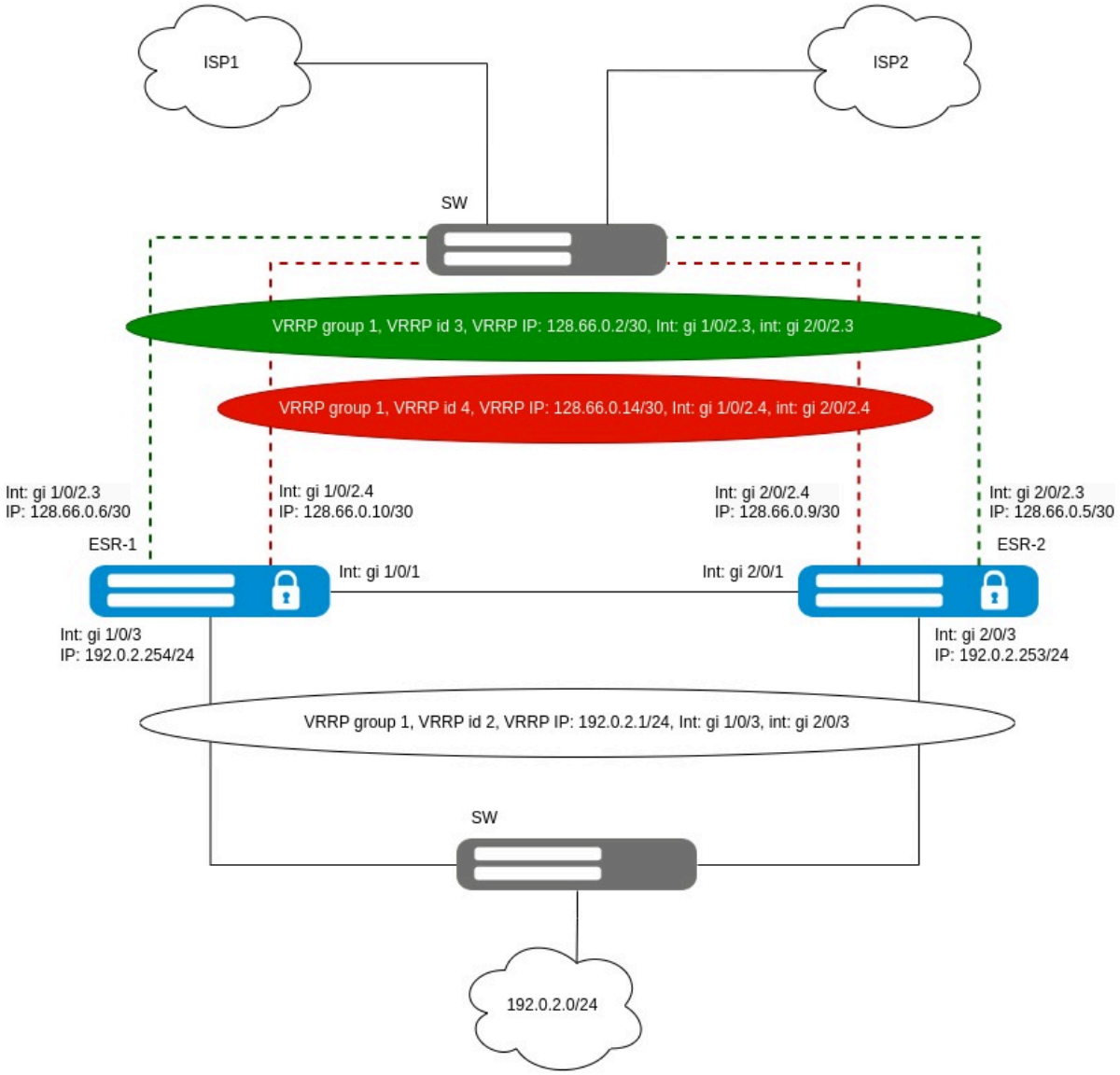


Схема реализации MultiWAN

Исходная конфигурация кластера:

ESR-1

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address cc:9d:a2:71:83:78
  exit
  unit 2
    mac-address cc:9d:a2:71:82:38
  exit
  enable
exit

hostname ESR-1 unit 1
hostname ESR-2 unit 2

security zone SYNC
exit
security zone LAN
exit
security zone WAN
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  vrrp 1
    ip address 198.51.100.1/24
    priority 254 unit 1
    priority 253 unit 2
    group 1
    enable
  exit
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 1/0/2.3
  security-zone WAN
  ip address 128.66.0.6/30
  vrrp 3
    ip address 128.66.0.2/30
    group 1
    enable
  exit
exit
interface gigabitethernet 1/0/2.4
  security-zone WAN
  ip address 128.66.0.10/30
  vrrp 4
    ip address 128.66.0.14/30
```

```
    group 1
    enable
  exit
exit
interface gigabitethernet 1/0/3
  security-zone LAN
  ip address 192.0.2.254/24
  vrrp 2
    ip address 192.0.2.1/24
    group 1
    enable
  exit
exit
interface gigabitethernet 2/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/2.3
  security-zone WAN
  ip address 128.66.0.5/30
  vrrp 3
    ip address 128.66.0.2/30
    group 1
    enable
  exit
exit
interface gigabitethernet 2/0/2.4
  security-zone WAN
  ip address 128.66.0.9/30
  vrrp 4
    ip address 128.66.0.14/30
    group 1
    enable
  exit
exit
interface gigabitethernet 2/0/3
  security-zone LAN
  ip address 192.0.2.253/24
  vrrp 2
    ip address 192.0.2.1/24
    group 1
    enable
  exit
exit

security zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
exit
security zone-pair WAN self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
exit
security zone-pair LAN self
```

```
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
exit
```

Создадим список IP-адресов для проверки целостности соединения:

ESR-1

```
ESR-1(config)# wan load-balance target-list WAN
ESR-1(config-wan-target-list)# target 1
ESR-1(config-wan-target)# ip address 128.66.0.17
ESR-1(config-wan-target)# enable
ESR-1(config-wan-target)# exit
ESR-1(config-wan-target-list)# exit
```

Настроим WAN на интерфейсе в сторону провайдера ISP1:

ESR-1

```
ESR-1(config)# interface gigabitethernet 1/0/2.3
ESR-1(config-if-sub)# wan load-balance nexthop 128.66.0.1
ESR-1(config-if-sub)# wan load-balance target-list WAN
ESR-1(config-if-sub)# wan load-balance enable
ESR-1(config-if-sub)# exit
ESR-1(config)# interface gigabitethernet 2/0/2.3
ESR-1(config-if-sub)# wan load-balance nexthop 128.66.0.1
ESR-1(config-if-sub)# wan load-balance target-list WAN
ESR-1(config-if-sub)# wan load-balance enable
ESR-1(config-if-sub)# exit
```

Настроим WAN на интерфейсе в сторону провайдера ISP2:

ESR-1

```
ESR-1(config)# interface gigabitethernet 1/0/2.4
ESR-1(config-if-sub)# wan load-balance nexthop 128.66.0.13
ESR-1(config-if-sub)# wan load-balance target-list WAN
ESR-1(config-if-sub)# wan load-balance enable
ESR-1(config-if-sub)# exit
ESR-1(config)# interface gigabitethernet 2/0/2.4
ESR-1(config-if-sub)# wan load-balance nexthop 128.66.0.13
ESR-1(config-if-sub)# wan load-balance target-list WAN
ESR-1(config-if-sub)# wan load-balance enable
ESR-1(config-if-sub)# exit
```

Укажем статический маршрут и создадим правило для балансировки трафика:

ESR-1

```
ESR-1(config)# ip route 0.0.0.0/0 wan load-balance rule 1 10
ESR-1(config)# wan load-balance rule 1
ESR-1(config-wan-rule)# outbound interface gigabitethernet 1/0/2.3 70
ESR-1(config-wan-rule)# outbound interface gigabitethernet 1/0/2.4 30
ESR-1(config-wan-rule)# outbound interface gigabitethernet 2/0/2.3 70
ESR-1(config-wan-rule)# outbound interface gigabitethernet 2/0/2.4 30
ESR-1(config-wan-rule)# enable
ESR-1(config-wan-rule)# exit
```

Проверить состояние работы MultiWAN можно с помощью команды:

ESR-1

```
ESR-1# show wan rules
Rule 1 detailed information:
    VRF:          default
    Failover:     Disabled
    Network: 0.0.0.0/0 Metric: 10
        gi1/0/2.3 Weight: 70 Nexthop: 128.66.0.1 [Active]
        gi1/0/2.4 Weight: 30 Nexthop: 128.66.0.13 [Active]
```

Также состояние работы MultiWAN можно проверить с помощью команды:

ESR-1

```
ESR-1# show wan interfaces status
Interface              Nexthop                  Status     Uptime/Downtime
                                                           (d,h:m:s)
--------------------   ----------------------   --------   --------------------
gi1/0/2.3              128.66.0.1               Active     00,00:00:44
gi1/0/2.4              128.66.0.13              Active     00,00:00:45
```

16.2.4 Настройка IPsec VPN

IPsec — это набор протоколов, обеспечивающих защиту данных, передаваемых по протоколу IP. 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.

Пример настройки Route-based IPsec VPN

Алгоритм настройки Route-based IPsec VPN описан в разделе Алгоритм настройки Route-based IPsec VPN.

Задача:

- Настроить IPsec туннель. Туннель необходимо поднять между адресами: кластер – 203.0.113.2 (VIP адрес), ответная сторона – 203.0.113.6;
- IKE:
    - группа Диффи-Хэллмана: 2;
    - алгоритм шифрования: AES 128 bit;
    - алгоритм аутентификации: MD5.
- IP sec:
    - алгоритм шифрования: AES 128 bit;
    - алгоритм аутентификации: MD5.

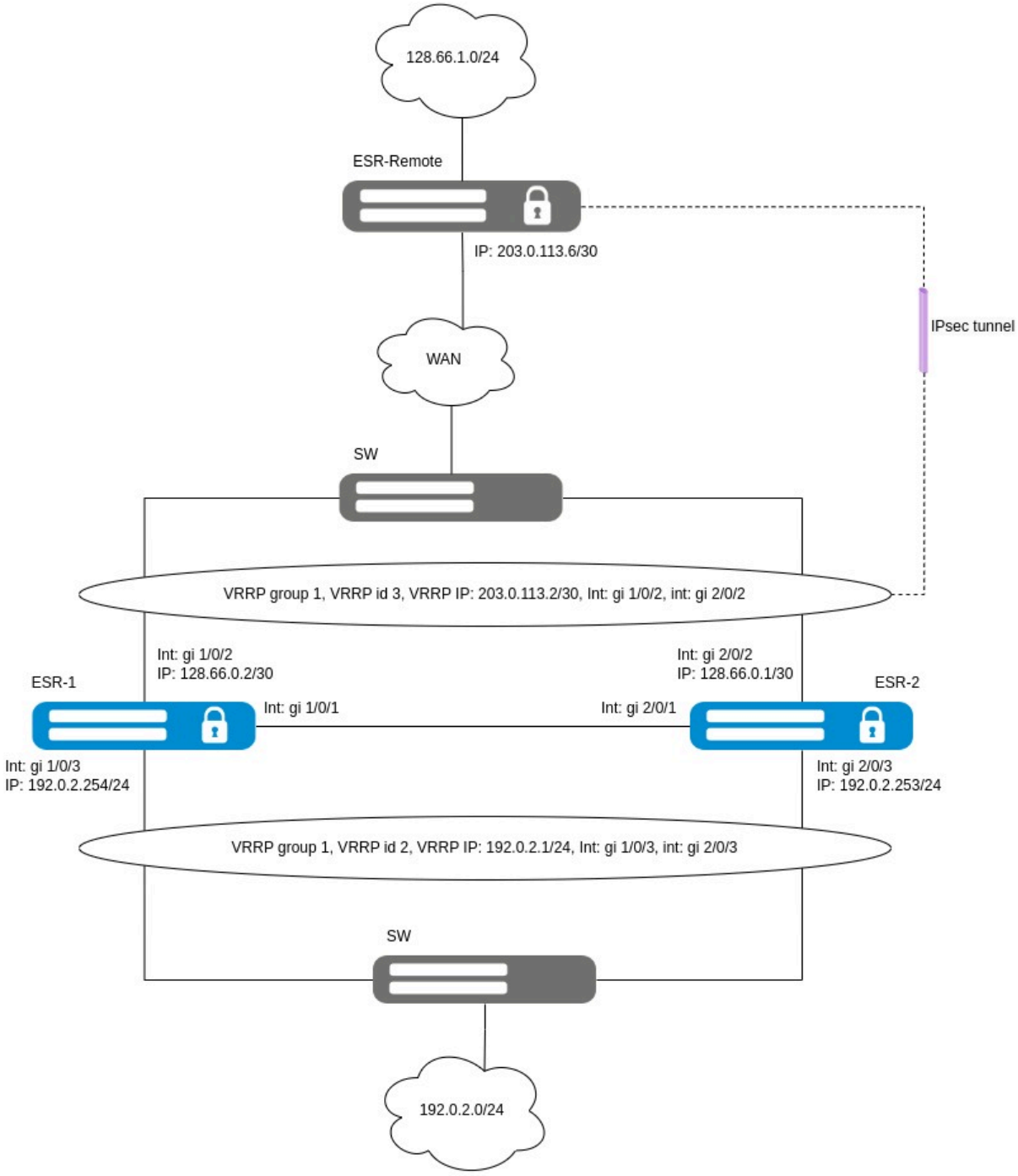


Схема реализации Route-based IPsec VPN

Исходная конфигурация кластера:

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address cc:9d:a2:71:83:78
  exit
  unit 2
    mac-address cc:9d:a2:71:82:38
  exit
  enable
exit

hostname ESR-1 unit 1
hostname ESR-2 unit 2

security zone SYNC
exit
security zone WAN
exit
security zone LAN
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  vrrp 1
    ip address 198.51.100.1/24
    priority 254 unit 1
    priority 253 unit 2
    group 1
    enable
  exit
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 1/0/2
  security-zone WAN
  ip address 128.66.0.2/30
  vrrp 3
    ip address 203.0.113.2/30
    group 1
    enable
  exit
exit
interface gigabitethernet 1/0/3
  security-zone LAN
  ip address 192.0.2.254/24
  vrrp 2
    ip address 192.0.2.1/24
    group 1
    enable
  exit
```

```
exit
interface gigabitethernet 2/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/2
  security-zone WAN
  ip address 128.66.0.1/30
  vrrp 3
    ip address 203.0.113.2/30
    group 1
    enable
  exit
exit
interface gigabitethernet 2/0/3
  security-zone LAN
  ip address 192.0.2.253/24
  vrrp 2
    ip address 192.0.2.1/24
    group 1
    enable
  exit
exit

security zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
exit
security zone-pair WAN self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
exit
security zone-pair LAN self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
exit
```

Решение:

Создадим профиль ISAKMP-портов, необходимых для работы протокола IPsec, включающий разрешение UDP-пакетов на порту 500 (а также на порту 4500 для поддержки NAT-T при необходимости):

ESR-1

```
ESR-1(config)# object-group service ISAKMP
ESR-1(config-object-group-service)# port-range 500
ESR-1(config-object-group-service)# port-range 4500
ESR-1(config-object-group-service)# exit
```

Добавим правила, разрешающее прохождение пакетов протоколов VRRP и ESP, а также UDP-пакетов с портами 500 и 4500, через IPsec-туннель:

ESR-1

```
ESR-1(config)# security zone-pair WAN self
ESR-1(config-security-zone-pair)# rule 2
ESR-1(config-security-zone-pair-rule)# action permit
ESR-1(config-security-zone-pair-rule)# match protocol udp
ESR-1(config-security-zone-pair-rule)# match destination-port object-group network ISAKMP
ESR-1(config-security-zone-pair-rule)# enable
ESR-1(config-security-zone-pair-rule)# exit
ESR-1(config-security-zone-pair)# rule 3
ESR-1(config-security-zone-pair-rule)# action permit
ESR-1(config-security-zone-pair-rule)# match protocol esp
ESR-1(config-security-zone-pair-rule)# enable
ESR-1(config-security-zone-pair-rule)# exit
ESR-1(config-security-zone-pair)# exit
```

Создадим зону безопасности IPsec и туннель VTI, через который будет перенаправляться трафик в IPsec-туннель. В качестве локального шлюза назначим VIP IP-адрес, настроенный на интерфейсах в сторону зоны WAN, а в качестве удалённого шлюза – IP-адрес соответствующего интерфейса:

ESR-1

```
ESR-1(config)# security zone IPSEC
ESR-1(config-security-zone)# exit
ESR-1(config)# tunnel vti 1
ESR-1(config-vti)# security-zone IPSEC
ESR-1(config-vti)# local address 203.0.113.2
ESR-1(config-vti)# remote address 203.0.113.6
ESR-1(config-vti)# ip address 128.66.0.6/30
ESR-1(config-vti)# enable
ESR-1(config-vti)# exit
```

Добавим правило, разрешающее прохождение трафика между зонами LAN и IPSEC:

ESR-1

```
ESR-1(config)# security zone-pair LAN IPSEC
ESR-1(config-security-zone-pair)# rule 1
ESR-1(config-security-zone-pair-rule)# action permit
ESR-1(config-security-zone-pair-rule)# enable
ESR-1(config-security-zone-pair-rule)# exit
ESR-1(config-security-zone-pair)# exit
ESR-1(config)# security zone-pair IPSEC LAN
ESR-1(config-security-zone-pair)# rule 1
ESR-1(config-security-zone-pair-rule)# action permit
ESR-1(config-security-zone-pair-rule)# enable
ESR-1(config-security-zone-pair-rule)# exit
ESR-1(config-security-zone-pair)# exit
```

Создадим профиль протокола IKE, в котором зададим следующие параметры безопасности: группу Диффи-Хэллмана 2, алгоритм шифрования AES 128 bit и алгоритм аутентификации MD5. Данные настройки обеспечивают надежную защиту IKE-соединения:

ESR-1

```
ESR-1(config)# security ike proposal ike_prop
ESR-1(config-ike-proposal)# dh-group 2
ESR-1(config-ike-proposal)# authentication algorithm md5
ESR-1(config-ike-proposal)# encryption algorithm aes128
ESR-1(config-ike-proposal)# exit
```

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

ESR-1

```
ESR-1(config)# security ike policy ike_pol
ESR-1(config-ike-policy)# pre-shared-key ascii-text password
ESR-1(config-ike-policy)# proposal ike_prop
ESR-1(config-ike-policy)# exit
```

Создадим шлюз протокола IKE с указанием VTI-туннеля, применимой политики, версии протокола и режима перенаправления трафика в туннель, а также отключим mobike:

ESR-1

```
ESR-1(config)# security ike gateway ike_gw
ESR-1(config-ike-gw)# version v2-only
ESR-1(config-ike-gw)# ike-policy ike_pol
ESR-1(config-ike-gw)# mode route-based
ESR-1(config-ike-gw)# mobike disable
ESR-1(config-ike-gw)# bind-interface vti 1
ESR-1(config-ike-gw)# exit
```

Создадим профиль параметров безопасности для IPsec-туннеля, в котором укажем алгоритм шифрования AES 128 bit и алгоритм аутентификации MD5, обеспечивая надежную защиту передаваемых данных:

ESR-1

```
ESR-1(config)# security ipsec proposal ipsec_prop
ESR-1(config-ipsec-proposal)# authentication algorithm md5
ESR-1(config-ipsec-proposal)# encryption algorithm aes128
ESR-1(config-ipsec-proposal)# exit
```

Создадим политику для IPsec-туннеля, в которой укажем перечень профилей IPsec-туннеля, используемых для согласования параметров безопасности между узлами:

ESR-1

```
ESR-1(config)# security ipsec policy ipsec_pol
ESR-1(config-ipsec-policy)# proposal ipsec_prop
ESR-1(config-ipsec-policy)# exit
```

Создадим IPsec VPN, в котором задаются следующие параметры: шлюз IKE-протокола, политика IPsec-туннеля, режим обмена ключами и способ установления соединения:

ESR-1

```
ESR-1(config)# security ipsec vpn ipsec
ESR-1(config-ipsec-vpn)# ike establish-tunnel route
ESR-1(config-ipsec-vpn)# ike gateway ike_gw
ESR-1(config-ipsec-vpn)# ike ipsec-policy ipsec_pol
ESR-1(config-ipsec-vpn)# enable
ESR-1(config-ipsec-vpn)# exit
```

Добавим статический маршрут до встречной клиентской подсети через VTI-туннель:

ESR-1

```
ESR-1(config)# ip route 128.66.1.0/24 128.66.0.5
```

⚠ Аналогичную настройку требуется выполнить на встречном устройстве.

Просмотреть состояние VTI-туннеля можно с помощью команды:

ESR-1

```
ESR-1# show tunnels status
Tunnel             Admin   Link    MTU      Local IP           Remote IP          Last change
                   state   state                                                  (d,h:m:s)
----------------   -----   -----   ------   ----------------   ----------------   -------------
vti 1              Up      Up      1500     203.0.113.2        203.0.113.6        00,00:05:59
```

Посмотреть состояние IPsec-туннеля можно с помощью команды:

ESR-1

```
ESR-1# show security ipsec vpn status
Name                              Local host        Remote host       Initiator spi
Responder spi        State
-------------------------------   ---------------   ---------------   ------------------
------------------   -----------
ipsec                             203.0.113.2       203.0.113.6       0x65212b7585c59b50
0x53028e1afc23a024   Established
```

Пример настройки Policy-based IPsec VPN

Алгоритм настройки Policy-based IPsec VPN описан в разделе Алгоритм настройки Policy-based IPsec VPN.

Задача:

- Настроить IPsec туннель. Туннель необходимо поднять между адресами: кластер – 203.0.113.2 (VIP адрес), ответная сторона – 203.0.113.6. Туннель необходим для организации доступа между клиентскими подсетями 192.0.2.0/24 и 128.66.1.0/24;
- IKE:
  - группа Диффи-Хэллмана: 2;
  - алгоритм шифрования: AES 128 bit;
  - алгоритм аутентификации: MD5.
- IP sec:
  - алгоритм шифрования: AES 128 bit;
  - алгоритм аутентификации: MD5.

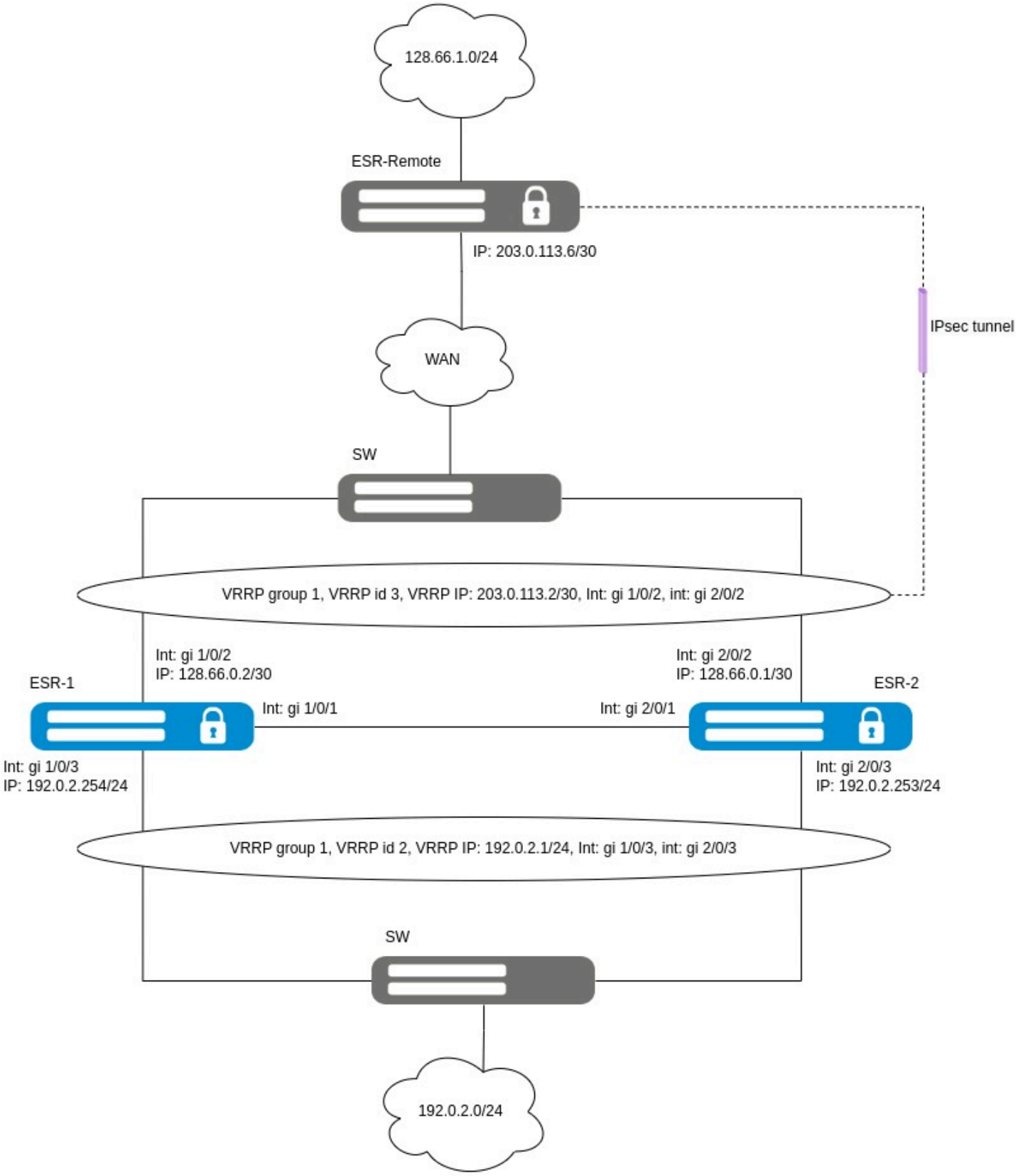


Схема реализации Policy-based IPsec VPN

Исходная конфигурация кластера:

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address cc:9d:a2:71:83:78
  exit
  unit 2
    mac-address cc:9d:a2:71:82:38
  exit
  enable
exit

hostname ESR-1 unit 1
hostname ESR-2 unit 2

security zone SYNC
exit
security zone WAN
exit
security zone LAN
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  vrrp 1
    ip address 198.51.100.1/24
    priority 254 unit 1
    priority 253 unit 2
    group 1
    enable
  exit
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 1/0/2
  security-zone WAN
  ip address 128.66.0.2/30
  vrrp 3
    ip address 203.0.113.2/30
    group 1
    enable
  exit
exit
interface gigabitethernet 1/0/3
  security-zone LAN
  ip address 192.0.2.254/24
  vrrp 2
    ip address 192.0.2.1/24
    group 1
    enable
  exit
```

```
exit
interface gigabitethernet 2/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/2
  security-zone WAN
  ip address 128.66.0.1/30
  vrrp 3
    ip address 203.0.113.2/30
    group 1
    enable
  exit
exit
interface gigabitethernet 2/0/3
  security-zone LAN
  ip address 192.0.2.253/24
  vrrp 2
    ip address 192.0.2.1/24
    group 1
    enable
  exit
exit

security zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
exit
security zone-pair WAN self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
exit
security zone-pair LAN self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
exit
```

Решение:

Создадим профиль ISAKMP-портов, необходимых для работы протокола IPsec, включающий разрешение UDP-пакетов на порту 500 (а также на порту 4500 для поддержки NAT-T при необходимости):

ESR-1

```
ESR-1(config)# object-group service ISAKMP
ESR-1(config-object-group-service)# port-range 500
ESR-1(config-object-group-service)# port-range 4500
ESR-1(config-object-group-service)# exit
```

Добавим правила, разрешающее прохождение пакетов протоколов VRRP и ESP, а также UDP-пакетов с портами 500 и 4500, через IPsec-туннель:

ESR-1

```
ESR-1(config)# security zone-pair WAN self
ESR-1(config-security-zone-pair)# rule 2
ESR-1(config-security-zone-pair-rule)# action permit
ESR-1(config-security-zone-pair-rule)# match protocol udp
ESR-1(config-security-zone-pair-rule)# match destination-port object-group ISAKMP
ESR-1(config-security-zone-pair-rule)# enable
ESR-1(config-security-zone-pair-rule)# exit
ESR-1(config-security-zone-pair)# rule 3
ESR-1(config-security-zone-pair-rule)# action permit
ESR-1(config-security-zone-pair-rule)# match protocol esp
ESR-1(config-security-zone-pair-rule)# enable
ESR-1(config-security-zone-pair-rule)# exit
ESR-1(config-security-zone-pair)# exit
```

Добавим правило, разрешающее прохождение трафика между зонами LAN и WAN для клиентских подсетей:

ESR-1

```
ESR-1(config)# object-group network LAN
ESR-1(config-object-group-network)# ip prefix 192.0.2.0/24
ESR-1(config-object-group-network)# exit
ESR-1(config)# object-group network IPSEC
ESR-1(config-object-group-network)# ip prefix 128.66.1.0/24
ESR-1(config-object-group-network)# exit
ESR-1(config)# security zone-pair LAN WAN
ESR-1(config-security-zone-pair)# rule 1
ESR-1(config-security-zone-pair-rule)# match source-address object-group network LAN
ESR-1(config-security-zone-pair-rule)# match destination-address object-group network IPSEC
ESR-1(config-security-zone-pair-rule)# action permit
ESR-1(config-security-zone-pair-rule)# enable
ESR-1(config-security-zone-pair-rule)# exit
ESR-1(config-security-zone-pair)# exit
ESR-1(config)# security zone-pair WAN LAN
ESR-1(config-security-zone-pair)# rule 1
ESR-1(config-security-zone-pair-rule)# match source-address object-group network IPSEC
ESR-1(config-security-zone-pair-rule)# match destination-address object-group network LAN
ESR-1(config-security-zone-pair-rule)# action permit
ESR-1(config-security-zone-pair-rule)# enable
ESR-1(config-security-zone-pair-rule)# exit
ESR-1(config-security-zone-pair)# exit
```

Создадим профиль протокола IKE, в котором зададим следующие параметры безопасности: группу Диффи-Хэллмана 2, алгоритм шифрования AES 128 bit и алгоритм аутентификации MD5. Данные настройки обеспечивают надежную защиту IKE-соединения:

ESR-1

```
ESR-1(config)# security ike proposal ike_prop
ESR-1(config-ike-proposal)# dh-group 2
ESR-1(config-ike-proposal)# authentication algorithm md5
ESR-1(config-ike-proposal)# encryption algorithm aes128
ESR-1(config-ike-proposal)# exit
```

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

ESR-1

```
ESR-1(config)# security ike policy ike_pol
ESR-1(config-ike-policy)# pre-shared-key ascii-text password
ESR-1(config-ike-policy)# proposal ike_prop
ESR-1(config-ike-policy)# exit
```

Создадим шлюз протокола IKE, определив применимую IKE-политику, локальные и удалённые параметры, а также режим перенаправления трафика в туннель. В качестве локального шлюза назначим VIP IP-адрес, настроенный на интерфейсах в сторону зоны WAN, с локальной подсетью 192.0.2.0/24, а удалённым – IP-адрес 203.0.113.1 с удаленной подсетью 128.66.1.0/24. Режим перенаправления трафика установлен как policy-based:

ESR-1

```
ESR-1(config)# security ike gateway ike_gw
ESR-1(config-ike-gw)# ike-policy ike_pol
ESR-1(config-ike-gw)# local address 203.0.113.2
ESR-1(config-ike-gw)# local network 192.0.2.0/24
ESR-1(config-ike-gw)# remote address 203.0.113.6
ESR-1(config-ike-gw)# remote network 128.66.1.0/24
ESR-1(config-ike-gw)# mode policy-based
ESR-1(config-ike-gw)# exit
```

Создадим профиль параметров безопасности для IPsec-туннеля, в котором укажем алгоритм шифрования AES 128 bit и алгоритм аутентификации MD5, обеспечивая надежную защиту передаваемых данных:

ESR-1

```
ESR-1(config)# security ipsec proposal ipsec_prop
ESR-1(config-ipsec-proposal)# authentication algorithm md5
ESR-1(config-ipsec-proposal)# encryption algorithm aes128
ESR-1(config-ipsec-proposal)# exit
```

Создадим политику для IPsec-туннеля, в которой укажем перечень профилей IPsec-туннеля, используемых для согласования параметров безопасности между узлами:

ESR-1

```
ESR-1(config)# security ipsec policy ipsec_pol
ESR-1(config-ipsec-policy)# proposal ipsec_prop
ESR-1(config-ipsec-policy)# exit
```

Создадим IPsec VPN, в котором задаются следующие параметры: шлюз IKE-протокола, политика IPsec-туннеля, режим обмена ключами и способ установления соединения:

ESR-1

```
ESR-1(config)# security ipsec vpn ipsec
ESR-1(config-ipsec-vpn)# ike establish-tunnel route
ESR-1(config-ipsec-vpn)# ike gateway ike_gw
ESR-1(config-ipsec-vpn)# ike ipsec-policy ipsec_pol
ESR-1(config-ipsec-vpn)# enable
ESR-1(config-ipsec-vpn)# exit
```

Добавим статический маршрут до встречной клиентской подсети через IPsec-туннель:

ESR-1

```
ESR-1(config)# ip route 128.66.1.0/24 203.0.113.1
```

⚠ Аналогичную настройку требуется выполнить на устройстве, находящемся на другой стороне туннеля.

Посмотреть состояние IPsec-туннеля можно с помощью команды:

ESR-1

```
ESR-1# show security ipsec vpn status
Name                              Local host        Remote host       Initiator spi
Responder spi        State
-------------------------------   ---------------   ---------------   ------------------
------------------   -----------
ipsec                             203.0.113.2       203.0.113.6       0x201602ebcafb809b
0x4556a21a7012d2c0   Established
```

16.2.5 Настройка firewall/NAT failover

Firewall failover необходим для резервирования сессий firewall.

Алгоритм настройки firewall/NAT failover описан в разделе Алгоритм настройки firewall failover.

Пример настройки firewall failover

Задача:

Настроить firewall failover в кластере маршрутизаторов ESR-1 и ESR-2 со следующими параметрами:

- режим резервирования сессий unicast;
- номер UDP-порта службы резервирования 9999;
- клиентская подсеть: 192.0.2.0/24.

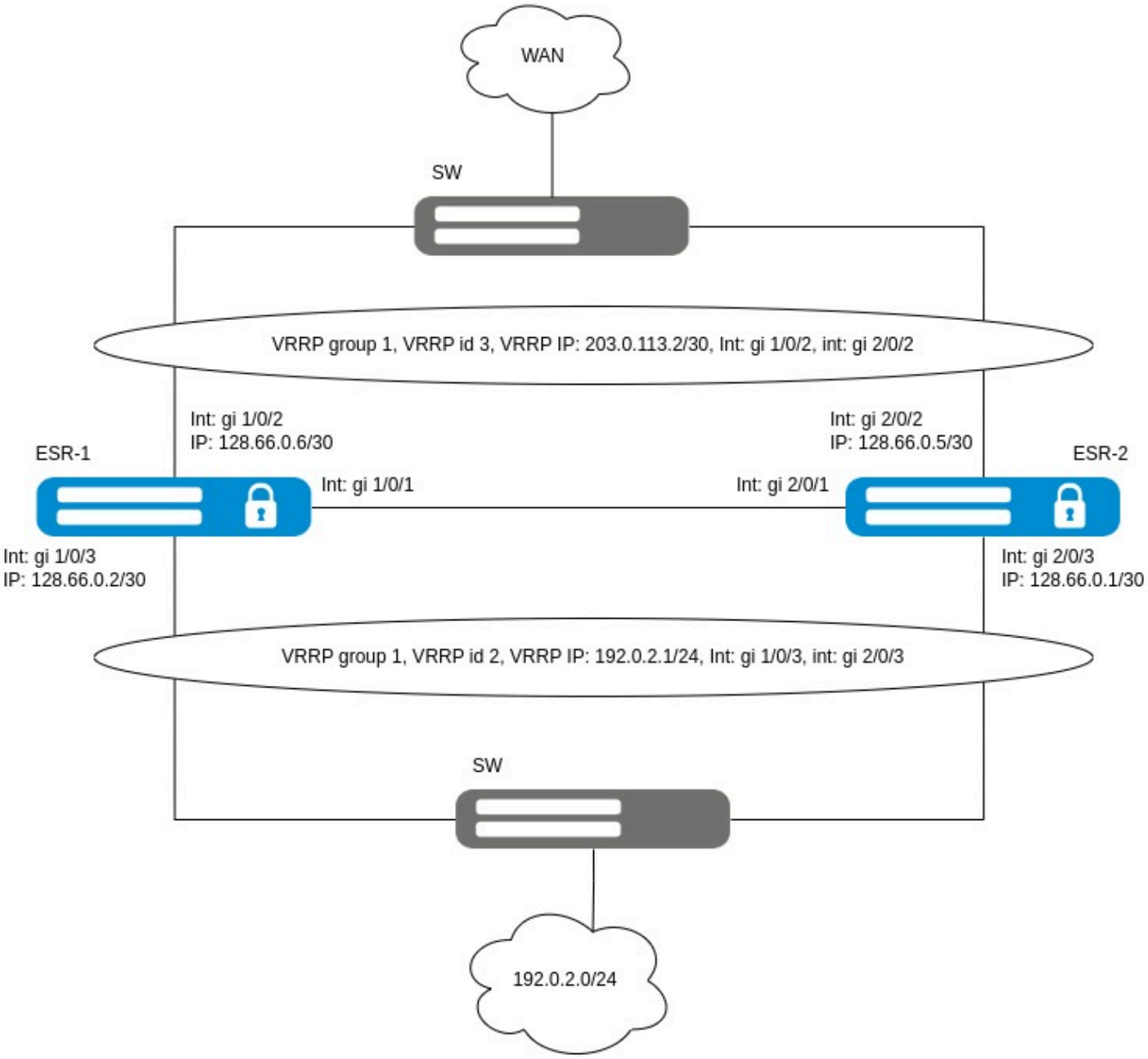


Схема реализации Firewall failover

Исходная конфигурация кластера:

ESR-1

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address cc:9d:a2:71:83:78
  exit
  unit 2
    mac-address cc:9d:a2:71:82:38
  exit
  enable
exit

hostname ESR-1 unit 1
hostname ESR-2 unit 2

security zone SYNC
exit
security zone WAN
exit
security zone LAN
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  vrrp 1
    ip address 198.51.100.1/24
    priority 254 unit 1
    priority 253 unit 2
    group 1
    enable
  exit
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 1/0/2
  security-zone WAN
  ip address 128.66.0.6/30
  vrrp 3
    ip address 203.0.113.2/30
    group 1
    enable
  exit
exit
interface gigabitethernet 1/0/3
  security-zone LAN
  ip address 128.66.0.2/30
  vrrp 2
    ip address 192.0.2.1/24
```

```
    group 1
    enable
  exit
exit
interface gigabitethernet 2/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/2
  security-zone WAN
  ip address 128.66.0.5/30
  vrrp 3
    ip address 203.0.113.2/30
    group 1
    enable
  exit
exit
interface gigabitethernet 2/0/3
  security-zone LAN
  ip address 128.66.0.1/30
  vrrp 2
    ip address 192.0.2.1/24
    group 1
    enable
  exit
exit

security zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
exit
security zone-pair LAN self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
exit
security zone-pair WAN self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
exit
security zone-pair LAN WAN
  rule 1
    action permit
    enable
  exit
exit

ip route 0.0.0.0/0 203.0.113.1
```

Решение:

Сконфигурируем object-group для настройки failover-сервисов:

ESR-1

```
ESR-1(config)# object-group network SYNC_SRC
ESR-1(config-object-group-network)# ip address-range 198.51.100.254 unit 1
ESR-1(config-object-group-network)# ip address-range 198.51.100.253 unit 2
ESR-1(config-object-group-network)# exit
ESR-1(config)# object-group network SYNC_DST
ESR-1(config-object-group-network)# ip address-range 198.51.100.253 unit 1
ESR-1(config-object-group-network)# ip address-range 198.51.100.254 unit 2
ESR-1(config-object-group-network)# exit
```

Перейдем к настройке общих параметров для failover-сервисов, а именно к выбору: IP-адреса, с которого будут отправляться сообщения для синхронизации, IP-адреса получателя сообщений для синхронизации и VRRP-группу, на основе которой определяется состояние (основной/резервный) маршрутизатора при работе failover-сервисов:

ESR-1

```
ESR-1(config)# ip failover
ESR-1(config-failover)# local-address object-group SYNC_SRC
ESR-1(config-failover)# remote-address object-group SYNC_DST
ESR-1(config-failover)# vrrp-group 1
ESR-1(config-failover)# exit
```

⚠ При включенном кластере использование object-group в настройке failover-сервисов для local-/remote-адресов обязательно.

Для настройки правил зон безопасности создадим профиль для порта firewall failover:

ESR-1

```
ESR-1(config)# object-group service FAILOVER
ESR-1(config-object-group-service)# port-range 9999
ESR-1(config-object-group-service)# exit
```

Создадим разрешающие правило для зоны безопасности SYNC, разрешив прохождение необходимого трафика для работы firewall failover:

ESR-1

```
ESR-1(config)# security zone-pair SYNC self
ESR-1(config-security-zone-pair)# rule 4
ESR-1(config-security-zone-pair-rule)# action permit
ESR-1(config-security-zone-pair-rule)# match protocol udp
ESR-1(config-security-zone-pair-rule)# match destination-port object-group FAILOVER
ESR-1(config-security-zone-pair-rule)# enable
ESR-1(config-security-zone-pair-rule)# exit
ESR-1(config-security-zone-pair)# exit
```

Выполним настройку firewall failover. Настроим режим резервирования сессий unicast, номер UDP-порта службы резервирования сессий firewall и включим firewall failover:

ESR-1

```
ESR-1(config)# ip firewall failover
ESR-1(config-firewall-failover)# sync-type unicast
ESR-1(config-firewall-failover)# port 9999
ESR-1(config-firewall-failover)# enable
ESR-1(config-firewall-failover)# exit
```

После успешного запуска firewall failover можно посмотреть информацию о сервисе с помощью команды:

ESR-1

```
ESR-1# show ip firewall failover
Communication interface:                    bridge 1
Status:                                     Running
Bytes sent:                                 3420
Bytes received:                             3320
Packets sent:                               209
Packets received:                           209
Send errors:                                0
Receive errors:                             0
Resend queue:
    Active entries:                         1
    Errors:
        No space left:                      0
Hold queue:
    Active entries:                         0
    Errors:
        No space left:                      0
```

Также возможно узнать текущее состояние firewall failover сервиса, выполнив команду:

ESR-1

```
ESR-1# show high-availability state
AP Tunnels:
    State:                          Disabled
    Last state change:              --
DHCP option 82 table:
    State:                          Disabled
    Last state change:              --
DHCP server:
    State:                          Disabled
    Last state change:              --
crypto-sync:
    State:                          Disabled
Firewall sessions and NAT translations:
VRF:                                --
    Tracking VRRP Group             1
    Tracking VRRP Group state:      Master
    State:                          Successful synchronization
    Fault Reason:                   --
    Last synchronization:           2025-02-12 07:05:47
```

Сгенерируем одну клиентскую сессии из LAN в WAN.

Посмотреть firewall-сессии, которые синхронизируются между устройствами, можно командами:

ESR-1

```
ESR-1# show ip firewall sessions failover internal
 Codes: E - expected, U - unreplied,
        A - assured, C - confirmed

Prot    Aging        Inside source           Inside destination      Outside source
Outside destination     Pkts         Bytes        Status
-----   ----------   --------------------   ---------------------   ---------------------
---------------------   ----------   ----------   ------
tcp     0            192.0.2.10:44812        128.66.1.1:22           128.66.1.1:22
192.0.2.10:44812        --           --           AC
```

ESR-2

```
ESR-1# show ip firewall sessions failover external
  Codes: E - expected, U - unreplied,
        A - assured, C - confirmed

Prot    Aging        Inside source           Inside destination      Outside source
Outside destination     Pkts         Bytes        Status
-----   ----------   --------------------   ---------------------   ---------------------
---------------------   ----------   ----------   ------
tcp     0            192.0.2.10:44812        128.66.1.1:22           128.66.1.1:22
192.0.2.10:44812        --           --           AC
```

Посмотреть счетчики для кэшей firewall failover можно командой:

ESR-1

```
ESR-1# show ip firewall failover cache
Internal sessions cache counters:
    Active entries:                         1
    Added:                                  5
    Deleted:                                4
    Updated:                                4
    Failed adding:                          0
        No memory left:                     0
        No space left:                      0
    Failed deleting:                        0
        No entry found:                     0
    Failed updating:                        0
        No entry found:                     0
External sessions cache counters:
    Active entries:                         0
    Added:                                  0
    Deleted:                                0
    Updated:                                0
    Installed to Kernel:                    0
    Failed adding:                          0
        No memory left:                     0
        No space left:                      0
    Failed deleting:                        0
        No entry found:                     0
    Failed updating:                        0
        No entry found:                     0
    Failed installing to Kernel:            0
```

Пример настройки нескольких экземпляров firewall failover, каждый – в своём VRF

Задача:

Настроить несколько экземпляров firewall failover в кластере маршрутизаторов ESR-1 и ESR-2, каждый в своем VRF, со следующими параметрами:

- режим резервирования сессий unicast;
- номер UDP-порта службы резервирования 9999;
- настроить приоритеты у разных firewall failover так, чтобы один из юнитов кластера был Master в одном VRF, а в другом был Backup;
- клиентская подсеть через первый VRF: 192.0.2.0/24;
- клиентская подсеть через второй VRF: 128.66.0.0/24.

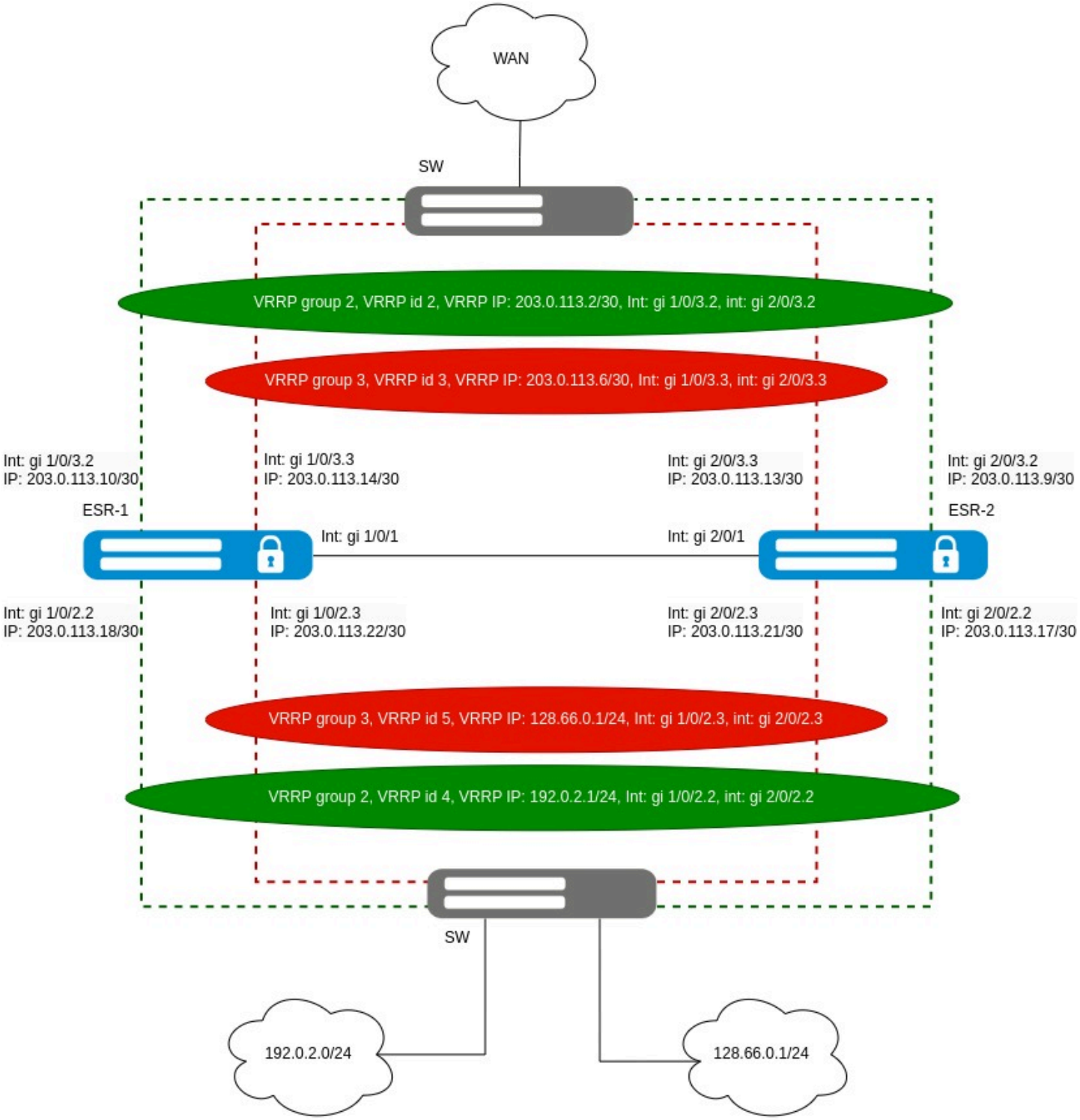


Схема реализации firewall failover в нескольких VRF

Исходная конфигурация кластера:

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address a2:00:00:10:c0:00
  exit
  unit 2
    mac-address a2:00:00:10:d0:00
  exit
  enable
exit

hostname ESR-1 unit 1
hostname ESR-2 unit 2

ip vrf PAIR_ONE
exit
ip vrf PAIR_TWO
exit

security zone SYNC
exit
security zone LAN_ONE
  ip vrf forwarding PAIR_ONE
exit
security zone LAN_TWO
  ip vrf forwarding PAIR_TWO
exit
security zone WAN_ONE
  ip vrf forwarding PAIR_ONE
exit
security zone WAN_TWO
  ip vrf forwarding PAIR_TWO
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  vrrp 1
    ip address 198.51.100.1/24
    priority 254 unit 1
    priority 253 unit 2
    group 1
    enable
  exit
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
exit
interface gigabitethernet 1/0/2.2
  ip vrf forwarding PAIR_ONE
  security-zone LAN_ONE
  ip address 203.0.113.18/30
  vrrp 4
```

```
    ip address 192.0.2.1/24
    priority 120
    group 2
    enable
  exit
exit
interface gigabitethernet 1/0/2.3
  ip vrf forwarding PAIR_TWO
  security-zone LAN_TWO
  ip address 203.0.113.22/30
  vrrp 5
    ip address 128.66.0.1/24
    priority 110
    group 3
    enable
  exit
exit
interface gigabitethernet 1/0/3.2
  ip vrf forwarding PAIR_ONE
  security-zone WAN_ONE
  ip address 203.0.113.10/30
  vrrp 2
    ip address 203.0.113.2/30
    group 2
    enable
  exit
exit
interface gigabitethernet 1/0/3.3
  ip vrf forwarding PAIR_TWO
  security-zone WAN_TWO
  ip address 203.0.113.14/30
  vrrp 3
    ip address 203.0.113.6/30
    group 3
    enable
  exit
exit
interface gigabitethernet 2/0/1
  mode switchport
exit
interface gigabitethernet 2/0/2.2
  ip vrf forwarding PAIR_ONE
  security-zone LAN_ONE
  ip address 203.0.113.17/30
  vrrp 4
    ip address 192.0.2.1/24
    priority 110
    group 2
    enable
  exit
exit
interface gigabitethernet 2/0/2.3
  ip vrf forwarding PAIR_TWO
  security-zone LAN_TWO
  ip address 203.0.113.21/30
  vrrp 5
    ip address 128.66.0.1/24
    priority 120
    group 3
    enable
```

```
  exit
exit
interface gigabitethernet 2/0/3.2
  ip vrf forwarding PAIR_ONE
  security-zone WAN_ONE
  ip address 203.0.113.9/30
  vrrp 2
    ip address 203.0.113.2/30
    group 2
    enable
  exit
exit
interface gigabitethernet 2/0/3.3
  ip vrf forwarding PAIR_TWO
  security-zone WAN_TWO
  ip address 203.0.113.13/30
  vrrp 3
    ip address 203.0.113.6/30
    group 3
    enable
  exit
exit

security zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
exit
security zone-pair LAN_ONE self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
exit
security zone-pair LAN_TWO self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
exit
security zone-pair WAN_ONE self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
exit
security zone-pair WAN_TWO self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
exit
security zone-pair LAN_ONE WAN_ONE
  rule 1
```

```
    action permit
    enable
  exit
exit
security zone-pair LAN_TWO WAN_TWO
  rule 1
    action permit
    enable
  exit
exit
```

Решение:

Сконфигурируем object-group для настройки failover-сервисов:

ESR-1

```
ESR-1(config)# object-group network DST_PAIR_ONE
ESR-1(config-object-group-network)# ip address-range 203.0.113.17 unit 1
ESR-1(config-object-group-network)# ip address-range 203.0.113.18 unit 2
ESR-1(config-object-group-network)# exit
ESR-1(config)# object-group network DST_PAIR_TWO
ESR-1(config-object-group-network)# ip address-range 203.0.113.21 unit 1
ESR-1(config-object-group-network)# ip address-range 203.0.113.22 unit 2
ESR-1(config-object-group-network)# exit
ESR-1(config)# object-group network SRC_PAIR_ONE
ESR-1(config-object-group-network)# ip address-range 203.0.113.18 unit 1
ESR-1(config-object-group-network)# ip address-range 203.0.113.17 unit 2
ESR-1(config-object-group-network)# exit
ESR-1(config)# object-group network SRC_PAIR_TWO
ESR-1(config-object-group-network)# ip address-range 203.0.113.22 unit 1
ESR-1(config-object-group-network)# ip address-range 203.0.113.21 unit 2
ESR-1(config-object-group-network)# exit
```

Перейдем к настойке ip failover для каждого VRF, настроим там local-address/remote-address и укажем привязки к соответствующим VRRP-group, на основе которых будет определяться, какой из маршрутизаторов будет синхронизировать сессии:

ESR-1

```
ESR-1(config)# ip failover vrf PAIR_ONE
ESR-1(config-failover)# local-address object-group SRC_PAIR_ONE
ESR-1(config-failover)# remote-address object-group DST_PAIR_ONE
ESR-1(config-failover)# vrrp-group 2
ESR-1(config-failover)# exit
ESR-1(config)# ip failover vrf PAIR_TWO
ESR-1(config-failover)# local-address object-group SRC_PAIR_TWO
ESR-1(config-failover)# remote-address object-group DST_PAIR_TWO
ESR-1(config-failover)# vrrp-group 3
ESR-1(config-failover)# exit
```

Перейдем к настройке firewall failover, каждый в своем VRF. Для каждого экземпляра необходимо указать режим синхронизирования unicast, настроить port 9999, а также включить его:

ESR-1

```
ESR-1(config)# ip firewall failover vrf PAIR_ONE
ESR-1(config-firewall-failover)# sync-type unicast
ESR-1(config-firewall-failover)# port 9999
ESR-1(config-firewall-failover)# enable
ESR-1(config-firewall-failover)# exit
ESR-1(config)# ip firewall failover vrf PAIR_TWO
ESR-1(config-firewall-failover)# sync-type unicast
ESR-1(config-firewall-failover)# port 9999
ESR-1(config-firewall-failover)# enable
ESR-1(config-firewall-failover)# exit
```

Разрешим в настройках firewall работу firewall failover в соответствующих зонах:

ESR-1

```
ESR-1(config)# object-group service FAILOVER
ESR-1(config-object-group-service)# port-range 9999
ESR-1(config-object-group-service)# exit
ESR-1(config)# security zone-pair LAN_ONE self
ESR-1(config-security-zone-pair)# rule 3
ESR-1(config-security-zone-pair-rule)# action permit
ESR-1(config-security-zone-pair-rule)# match protocol udp
ESR-1(config-security-zone-pair-rule)# match destination-port object-group FAILOVER
ESR-1(config-security-zone-pair-rule)# enable
ESR-1(config-security-zone-pair-rule)# exit
ESR-1(config-security-zone-pair)# exit
ESR-1(config)# security zone-pair LAN_TWO self
ESR-1(config-security-zone-pair)# rule 3
ESR-1(config-security-zone-pair-rule)# action permit
ESR-1(config-security-zone-pair-rule)# match protocol udp
ESR-1(config-security-zone-pair-rule)# match destination-port object-group FAILOVER
ESR-1(config-security-zone-pair-rule)# enable
ESR-1(config-security-zone-pair-rule)# exit
ESR-1(config-security-zone-pair)# exit
```

Просмотреть VRRP-статусы в разных VRF можно, используя команду **show vrrp**. Убедимся, что в одном VRF устройство находится в статусе Master, а в другом VRF – в статусе Backup:

ESR-1

```
ESR-1# show vrrp vrf PAIR_ONE

   Unit 1* 'ESR-1'
   ---------------
Virtual router   Virtual IP                          Priority   Preemption   State    Inherit
Sync group ID
--------------   ---------------------------------   --------   ----------   ------   -------
-------------
2                203.0.113.2/30                      100        Enabled      Master   --
2
4                192.0.2.1/24                        120        Enabled      Master   --
2


   Unit 2 'ESR-2'
   --------------
Virtual router   Virtual IP                          Priority   Preemption   State    Inherit
Sync group ID
--------------   ---------------------------------   --------   ----------   ------   -------
-------------
2                203.0.113.2/30                      100        Enabled      Backup   --
2
4                192.0.2.1/24                        110        Enabled      Backup   --
2

ESR-1# show vrrp vrf PAIR_TWO

   Unit 1* 'ESR-1'
   ---------------
Virtual router   Virtual IP                          Priority   Preemption   State    Inherit
Sync group ID
--------------   ---------------------------------   --------   ----------   ------   -------
-------------
3                203.0.113.6/30                      100        Enabled      Backup   --
3
5                128.66.0.1/24                       110        Enabled      Backup   --
3


   Unit 2 'ESR-2'
   --------------
Virtual router   Virtual IP                          Priority   Preemption   State    Inherit
Sync group ID
--------------   ---------------------------------   --------   ----------   ------   -------
-------------
3                203.0.113.6/30                      100        Enabled      Master   --
3
5                128.66.0.1/24                       120        Enabled      Master   --
3
```

Посмотреть информацию о сервисе firewall failover в каждом VRF можно с помощью следующей команды:

ESR-1

```
ESR-1# show ip firewall failover vrf PAIR_ONE
Communication interface:                    gigabitethernet 1/0/2.2
Status:                                     Running
Bytes sent:                                 7420
Bytes received:                             7200
Packets sent:                               465
Packets received:                           460
Send errors:                                0
Receive errors:                             0
Resend queue:
    Active entries:                         1
    Errors:
        No space left:                      0
Hold queue:
    Active entries:                         0
    Errors:
        No space left:                      0
ESR-1# show ip firewall failover vrf PAIR_TWO
Communication interface:                    gigabitethernet 1/0/2.3
Status:                                     Running
Bytes sent:                                 7320
Bytes received:                             7380
Packets sent:                               468
Packets received:                           464
Send errors:                                0
Receive errors:                             0
Resend queue:
    Active entries:                         1
    Errors:
        No space left:                      0
Hold queue:
    Active entries:                         0
    Errors:
        No space left:                      0
```

Также возможно узнать текущее состояние firewall failover сервисов во всех VRF, выполнив команду:

ESR-1

```
ESR-1# show high-availability state
DHCP server:
    State:                          Disabled
    Last state change:              --
crypto-sync:
    State:                          Disabled
Firewall sessions and NAT translations:
VRF:                                PAIR_ONE
    State:                          Successful synchronization
    Fault Reason:                   --
    Last synchronization:           2025-02-18 08:51:34
VRF:                                PAIR_TWO
    State:                          Successful synchronization
    Fault Reason:                   --
    Last synchronization:           2025-02-18 08:51:34
```

Сгенерируем по одной клиентской сессии из каждого LAN-пула.

Посмотреть вывод текущих сессий на устройстве можно с помощью команды **show ip firewall sessions**. Убедимся, что в выводе есть сессия только для того VRF, в котором устройство является в статусе Master:

ESR-1

```
ESR-1# show ip firewall sessions vrf PAIR_ONE protocol tcp
 Codes: E - expected, U - unreplied,
        A - assured, C - confirmed

Prot    Aging        Inside source           Inside destination      Outside source
Outside destination     Pkts         Bytes        Status
-----   ----------   ---------------------   ---------------------   ---------------------
---------------------   ----------   ----------   ------
tcp     110          192.0.2.10:47406        203.0.113.1:22          192.0.2.10:47406
203.0.113.1:22          --           --           AC
ESR-1# show ip firewall sessions vrf PAIR_TWO protocol tcp
```

ESR-2

```
ESR-2# show ip firewall sessions vrf PAIR_ONE protocol tcp
ESR-2# show ip firewall sessions vrf PAIR_TWO protocol tcp
 Codes: E - expected, U - unreplied,
        A - assured, C - confirmed

Prot    Aging        Inside source           Inside destination      Outside source
Outside destination     Pkts         Bytes        Status
-----   ----------   ---------------------   ---------------------   ---------------------
---------------------   ----------   ----------   ------
tcp     113          128.66.0.10:59108       203.0.113.5:22          128.66.0.10:59108
203.0.113.5:22          --           --           AC
```

Посмотреть вывод активных синхронизируемых сессий, используемых для работы firewal failover, на устройстве можно с помощью команды **show ip firewall session failover external/internal**. Убедимся, что для одного из VRF сессия находится в internal cash, а для второго VRF сессия находится в external cash:

ESR-1

```
ESR-1# show ip firewall sessions failover external vrf PAIR_ONE
ESR-1# show ip firewall sessions failover internal vrf PAIR_ONE
 Codes: E - expected, U - unreplied,
        A - assured, C - confirmed

Prot    Aging        Inside source           Inside destination      Outside source
Outside destination     Pkts         Bytes        Status
-----   ----------   ---------------------   ---------------------   ---------------------
---------------------   ----------   ----------   ------
tcp     0            192.0.2.10:47406        203.0.113.1:22          203.0.113.1:22
192.0.2.10:47406        --           --           AC
ESR-1# show ip firewall sessions failover external vrf PAIR_TWO
 Codes: E - expected, U - unreplied,
        A - assured, C - confirmed

Prot    Aging        Inside source           Inside destination      Outside source
Outside destination     Pkts         Bytes        Status
-----   ----------   ---------------------   ---------------------   ---------------------
---------------------   ----------   ----------   ------
tcp     0            128.66.0.10:59108       203.0.113.5:22          203.0.113.5:22
128.66.0.10:59108       --           --           AC
ESR-1# show ip firewall sessions failover internal vrf PAIR_TWO
```

ESR-2

```
ESR-2# show ip firewall sessions failover external vrf PAIR_ONE
 Codes: E - expected, U - unreplied,
        A - assured, C - confirmed

Prot    Aging        Inside source           Inside destination      Outside source
Outside destination     Pkts         Bytes        Status
-----   ----------   ---------------------   ---------------------   ---------------------
---------------------   ----------   ----------   ------
tcp     0            192.0.2.10:47406        203.0.113.1:22          203.0.113.1:22
192.0.2.10:47406        --           --           AC
ESR-2# show ip firewall sessions failover internal vrf PAIR_ONE
ESR-2# show ip firewall sessions failover external vrf PAIR_TWO
ESR-2# show ip firewall sessions failover internal vrf PAIR_TWO
 Codes: E - expected, U - unreplied,
        A - assured, C - confirmed

Prot    Aging        Inside source           Inside destination      Outside source
Outside destination     Pkts         Bytes        Status
-----   ----------   ---------------------   ---------------------   ---------------------
---------------------   ----------   ----------   ------
tcp     0            128.66.0.10:59108       203.0.113.5:22          203.0.113.5:22
128.66.0.10:59108       --           --           AC
```

Пример настройки firewall failover для кластера из 3 юнитов

Задача:

Настроить firewall failover в кластере маршрутизаторов ESR-1, ESR-2 и ESR-3 со следующими параметрами:

- режим резервирования сессий multicast;
- номер UDP-порта службы резервирования 2000;
- клиентская подсеть: 192.0.2.0/24.

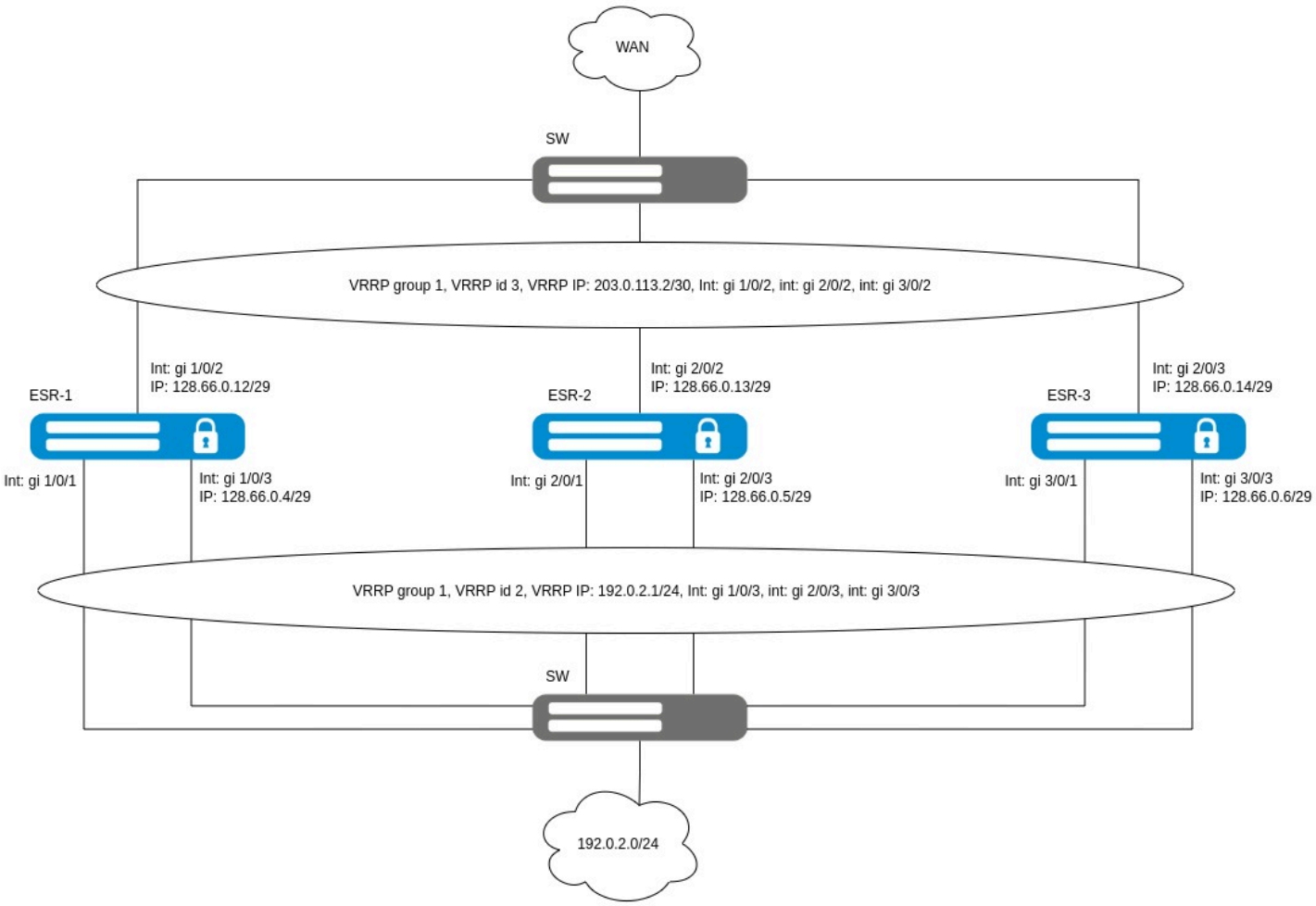


Схема реализации Firewall failover для кластера из 3-х юнитов

Исходная конфигурация кластера:

ESR-1

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address cc:9d:a2:71:83:78
  exit
  unit 2
    mac-address cc:9d:a2:71:82:38
  exit
  unit 3
    mac-address 68:13:e2:e2:05:28
  exit
  enable
exit

hostname ESR-1 unit 1
hostname ESR-2 unit 2
hostname ESR-3 unit 3

security zone SYNC
exit
security zone WAN
exit
security zone LAN
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  ip address 198.51.100.252/24 unit 3
  vrrp 1
    ip address 198.51.100.1/24
    priority 254 unit 1
    priority 253 unit 2
    priority 252 unit 3
    group 1
    enable
  exit
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 1/0/2
  security-zone WAN
  ip address 128.66.0.12/29
  vrrp 3
    ip address 203.0.113.2/30
    group 1
    enable
  exit
```

```
exit
interface gigabitethernet 1/0/3
  security-zone LAN
  ip address 128.66.0.4/29
  vrrp 2
    ip address 192.0.2.1/24
    group 1
    enable
  exit
exit
interface gigabitethernet 2/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/2
  security-zone WAN
  ip address 128.66.0.13/29
  vrrp 3
    ip address 203.0.113.2/30
    group 1
    enable
  exit
exit
interface gigabitethernet 2/0/3
  security-zone LAN
  ip address 128.66.0.5/29
  vrrp 2
    ip address 192.0.2.1/24
    group 1
    enable
  exit
exit
interface gigabitethernet 3/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 3/0/2
  security-zone WAN
  ip address 128.66.0.14/29
  vrrp 3
    ip address 203.0.113.2/30
    group 1
    enable
  exit
exit
interface gigabitethernet 3/0/3
  security-zone LAN
  ip address 128.66.0.6/29
  vrrp 2
    ip address 192.0.2.1/24
    group 1
    enable
  exit
exit

security zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
```

```
  exit
exit
security zone-pair LAN self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
exit
security zone-pair WAN self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
exit
security zone-pair LAN WAN
  rule 1
    action permit
    enable
  exit
exit

ip route 0.0.0.0/0 203.0.113.1
```

Решение:

Сконфигурируем object-group для настройки failover-сервисов:

ESR-1

```
ESR-1(config)# object-group network SYNC_SRC
ESR-1(config-object-group-network)# ip address-range 198.51.100.254 unit 1
ESR-1(config-object-group-network)# ip address-range 198.51.100.253 unit 2
ESR-1(config-object-group-network)# ip address-range 198.51.100.252 unit 3
ESR-1(config-object-group-network)# exit
```

Перейдем к настройке общих параметров для failover-сервисов, а именно к выбору: IP-адреса, с которого будут отправляться сообщения для синхронизации, multicast-группы, multicast IP-адреса, на который будут отправляться сообщения для синхронизации, и VRRP-группы, на основе которой определяется состояние (основной/резервный) маршрутизатора при работе failover-сервисов:

ESR-1

```
ESR-1(config)# ip failover
ESR-1(config-failover)# local-address object-group SYNC_SRC
ESR-1(config-failover)# multicast-address 224.0.0.1
ESR-1(config-failover)# multicast-group 2000
ESR-1(config-failover)# vrrp-group 1
ESR-1(config-failover)# exit
```

⚠ При включенном кластере использование object-group в настройке failover-сервисов для local-/remote-адресов обязательно.

Для настройки правил зон безопасности создадим профиль для порта firewall failover:

ESR-1

```
ESR-1(config)# object-group service FAILOVER
ESR-1(config-object-group-service)# port-range 2000
ESR-1(config-object-group-service)# exit
```

Создадим разрешающие правило для зоны безопасности SYNC, разрешив прохождение необходимого трафика для работы firewall failover:

ESR-1

```
ESR-1(config)# security zone-pair SYNC self
ESR-1(config-security-zone-pair)# rule 4
ESR-1(config-security-zone-pair-rule)# action permit
ESR-1(config-security-zone-pair-rule)# match protocol udp
ESR-1(config-security-zone-pair-rule)# match destination-port object-group FAILOVER
ESR-1(config-security-zone-pair-rule)# enable
ESR-1(config-security-zone-pair-rule)# exit
ESR-1(config-security-zone-pair)# exit
```

Выполним настройку firewall failover. Настроим режим резервирования сессий multicast и включим firewall failover:

ESR-1

```
ESR-1(config)# ip firewall failover
ESR-1(config-firewall-failover)# sync-type multicast
ESR-1(config-firewall-failover)# enable
ESR-1(config-firewall-failover)# exit
```

После успешного запуска firewall failover можно посмотреть информацию о сервисе с помощью команды:

ESR-1

```
ESR-1# show ip firewall failover
Communication interface:                    bridge 1
Status:                                     Running
Bytes sent:                                 8160
Bytes received:                             15520
Packets sent:                               1002
Packets received:                           1938
Send errors:                                0
Receive errors:                             0
```

Также возможно узнать текущее состояние firewall failover сервиса, выполнив команду:

ESR-1

```
ESR-1# show high-availability state
AP Tunnels:
    State:                          Disabled
    Last state change:              --
DHCP option 82 table:
    State:                          Disabled
    Last state change:              --
DHCP server:
    State:                          Disabled
    Last state change:              --
crypto-sync:
    State:                          Disabled
Firewall sessions and NAT translations:
VRF:                                --
    Tracking VRRP Group             1
    Tracking VRRP Group state:      Master
    State:                          Successful synchronization
    Fault Reason:                   --
    Last synchronization:           2025-10-02 16:53:30
```

Сгенерируем одну клиентскую сессии из LAN в WAN.

Посмотреть firewall-сессии, которые синхронизируются между устройствами, можно командами:

ESR-1

```
ESR-1# show ip firewall sessions failover internal
 Codes: E - expected, U - unreplied,
        A - assured, C - confirmed

Prot    Aging        Inside source           Inside destination      Outside source
Outside destination     Pkts         Bytes        Status
-----   ----------   --------------------   ---------------------   ---------------------
---------------------   ----------   ----------   ------
tcp     0            192.0.2.10:44812        128.66.1.1:22           128.66.1.1:22
192.0.2.10:44812        --           --           AC
```

ESR-2

```
ESR-2# show ip firewall sessions failover external
  Codes: E - expected, U - unreplied,
        A - assured, C - confirmed

Prot    Aging        Inside source           Inside destination      Outside source
Outside destination     Pkts         Bytes        Status
-----   ----------   --------------------   ---------------------   ---------------------
---------------------   ----------   ----------   ------
tcp     0            192.0.2.10:44812        128.66.1.1:22           128.66.1.1:22
192.0.2.10:44812        --           --           AC
```

ESR-3

```
ESR-3# show ip firewall sessions failover external
  Codes: E - expected, U - unreplied,
         A - assured, C - confirmed

Prot    Aging        Inside source           Inside destination      Outside source
Outside destination     Pkts         Bytes        Status
-----   ----------   ---------------------   ---------------------   ---------------------
---------------------   ----------   ----------   ------
tcp     0            192.0.2.10:44812        128.66.1.1:22           128.66.1.1:22
192.0.2.10:44812        --           --           AC
```

Посмотреть счетчики для кэшей firewall failover можно командой:

ESR-1

```
ESR-1# show ip firewall failover cache
Internal sessions cache counters:
    Active entries:                         1
    Added:                                  5
    Deleted:                                4
    Updated:                                4
    Failed adding:                          0
        No memory left:                     0
        No space left:                      0
    Failed deleting:                        0
        No entry found:                     0
    Failed updating:                        0
        No entry found:                     0
External sessions cache counters:
    Active entries:                         0
    Added:                                  0
    Deleted:                                0
    Updated:                                0
    Installed to Kernel:                    0
    Failed adding:                          0
        No memory left:                     0
        No space left:                      0
    Failed deleting:                        0
        No entry found:                     0
    Failed updating:                        0
        No entry found:                     0
    Failed installing to Kernel:            0
```

16.2.6 Настройка DHCP failover

DHCP-failover позволяет обеспечить высокую доступность службы DHCP.

Алгоритм настройки DHCP failover описан в разделе Алгоритм настройки DHCP failover.

Пример настройки

Задача:

Настроить DHCP failover в кластере маршрутизаторов ESR-1 и ESR-2 со следующими параметрами:

- в качестве default-router используется IP-адрес VRRP;
- установить в качестве необходимого режима работы резервирования active-standby;
- клиентская подсеть: 192.0.2.0/24.

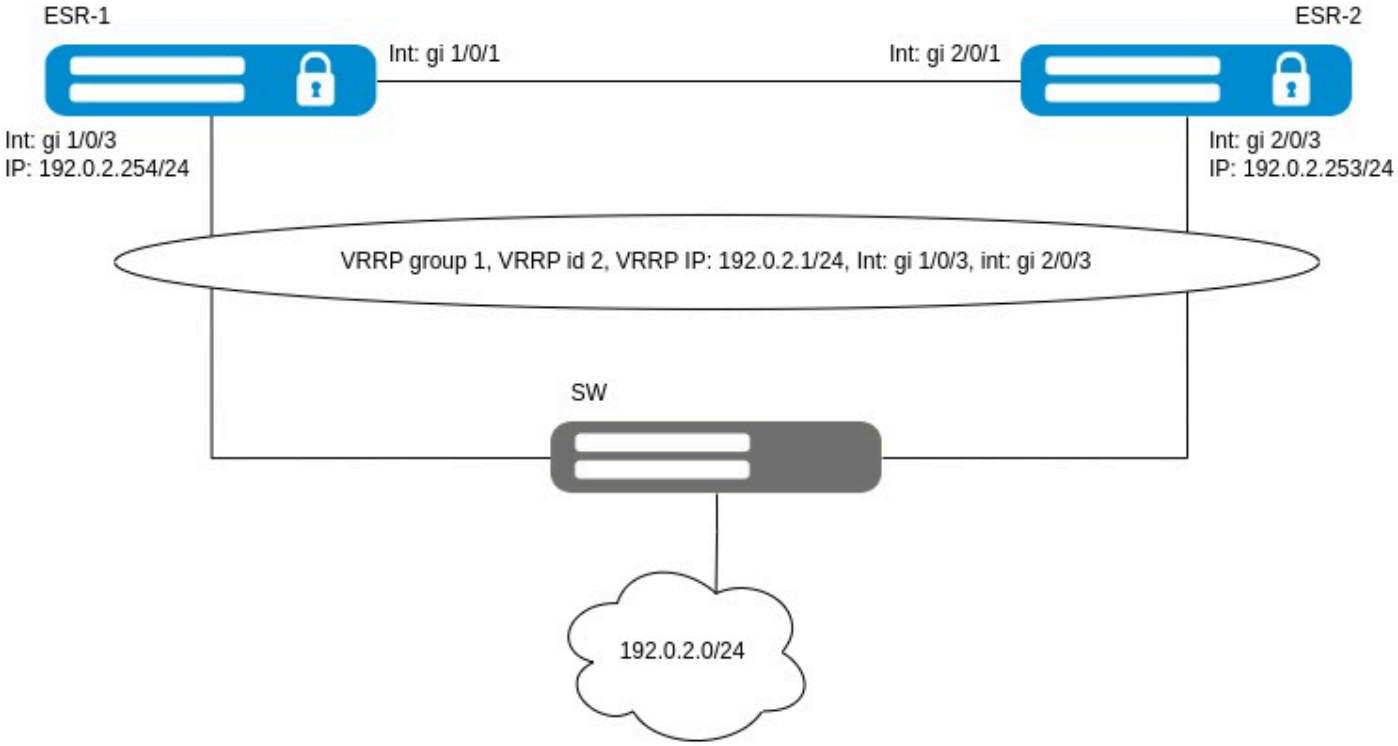


Схема реализации DHCP failover

Исходная конфигурация кластера:

ESR-1

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address a2:00:00:10:c0:00
  exit
  unit 2
    mac-address a2:00:00:10:d0:00
  exit
  enable
exit

hostname ESR-1 unit 1
hostname ESR-2 unit 2

object-group service DHCP_SERVER
  port-range 67
exit
object-group service DHCP_CLIENT
  port-range 68
exit

security zone SYNC
exit
security zone LAN
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  vrrp 1
    ip address 198.51.100.1/24
    priority 254 unit 1
    priority 253 unit 2
    group 1
    enable
  exit
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 1/0/3
  security-zone LAN
  ip address 192.0.2.254/24
  vrrp 2
    ip address 192.0.2.1/24
    group 1
    enable
  exit
exit
```

```
interface gigabitethernet 2/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/3
  security-zone LAN
  ip address 192.0.2.253/24
  vrrp 2
    ip address 192.0.2.1/24
    group 1
    enable
  exit
exit

security zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
exit
security zone-pair LAN self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
  rule 2
    action permit
    match protocol udp
    match source-port object-group DHCP_CLIENT
    match destination-port object-group DHCP_SERVER
    enable
  exit
exit

ip dhcp-server
ip dhcp-server pool TRUSTED
  network 192.0.2.0/24
  address-range 192.0.2.10-192.0.2.100
  default-router 192.0.2.1
exit
```

Решение:

Сконфигурируем object-group для настройки failover-сервисов:

ESR-1

```
ESR-1(config)# object-group network SYNC_SRC
ESR-1(config-object-group-network)# ip address-range 198.51.100.254 unit 1
ESR-1(config-object-group-network)# ip address-range 198.51.100.253 unit 2
ESR-1(config-object-group-network)# exit
ESR-1(config)# object-group network SYNC_DST
ESR-1(config-object-group-network)# ip address-range 198.51.100.253 unit 1
ESR-1(config-object-group-network)# ip address-range 198.51.100.254 unit 2
ESR-1(config-object-group-network)# exit
```

Перейдем к настройке общих параметров для failover-сервисов, а именно к выбору: IP-адреса, с которого будут отправляться сообщения для синхронизации, IP-адреса получателя сообщений для синхронизации и VRRP-группу, на основе которой определяется состояние (основной/резервный) маршрутизатора при работе failover-сервисов:

ESR-1

```
ESR-1(config)# ip failover
ESR-1(config-failover)# local-address object-group SYNC_SRC
ESR-1(config-failover)# remote-address object-group SYNC_DST
ESR-1(config-failover)# vrrp-group 1
ESR-1(config-failover)# exit
```

Перейдем к настройке резервирования DHCP-сервера, укажем режим работы резервирования и включим DHCP-failover:

ESR-1

```
ESR-1(config)# ip dhcp-server failover
ESR-1(config-dhcp-server-failover)# mode active-standby
ESR-1(config-dhcp-server-failover)# enable
ESR-1(config-dhcp-server-failover)# exit
```

⚠ Для работы в кластере необходимо использовать режим active-standby.

Создадим разрешающие правило для зоны безопасности SYNC, разрешив прохождение необходимого трафика для работы DHCP failover:

ESR-1

```
ESR-1(config)# object-group service SYNC
ESR-1(config-object-group-service)# port-range 873
ESR-1(config-object-group-service)# exit
ESR-1(config)# security zone-pair SYNC self
ESR-1(config-security-zone-pair)# rule 4
ESR-1(config-security-zone-pair-rule)# action permit
ESR-1(config-security-zone-pair-rule)# match protocol tcp
ESR-1(config-security-zone-pair-rule)# match destination-port object-group SYNC
ESR-1(config-security-zone-pair-rule)# enable
ESR-1(config-security-zone-pair-rule)# exit
ESR-1(config-security-zone-pair)# exit
```

Посмотреть состояние резервирования DHCP-сервера можно с помощью команды:

ESR-1

```
ESR-1# show ip dhcp server failover
VRF:                            --
    Mode:                       Active-Standby
    Role:                       Master
    State:                      Synchronized
    Last synchronization:       2025-02-12 07:56:40
```

Посмотреть состояние резервирования сессий DHCP можно с помощью команды:

ESR-1

```
ESR-1# show high-availability state
AP Tunnels:
    State:                        Disabled
    Last state change:            --
DHCP option 82 table:
    State:                        Disabled
    Last state change:            --
DHCP server:
VRF:                              --
    Mode:                         Active-Standby
    State:                        Successful synchronization
    Last synchronization:         2025-02-12 07:56:36
crypto-sync:
    State:                        Disabled
Firewall sessions and NAT translations:
    State:                        Disabled
```

Выданные адреса DHCP можно просмотреть с помощью команды:

ESR-1

```
ESR-1# show ip dhcp binding
IP address         MAC / Client ID                                                  Binding type
Lease expires at
----------------   --------------------------------------------------------------   ------------
--------------------
192.0.2.10         e4:5a:d4:01:18:04                                                active
2025-02-13 07:56:09
```

Пример настройки нескольких экземпляров DHCP failover, каждый в своем VRF

Задача:

Настроить два экземпляра DHCP failover, каждый в своём VRF, в кластере маршрутизаторов ESR-1 и ESR-2 со следующими параметрами:

- в качестве default-router используется IP-адрес VRRP;
- установить в качестве необходимого режима работы резервирования active-standby;
- настроить приоритеты у разных DHCP failover так, чтобы один из юнитов кластера был Master в одном VRF, а в другом был Backup;
- клиентская подсеть в первом VRF: 192.0.2.0/24;
- клиентская подсеть в втором VRF: 128.66.0.0/24.

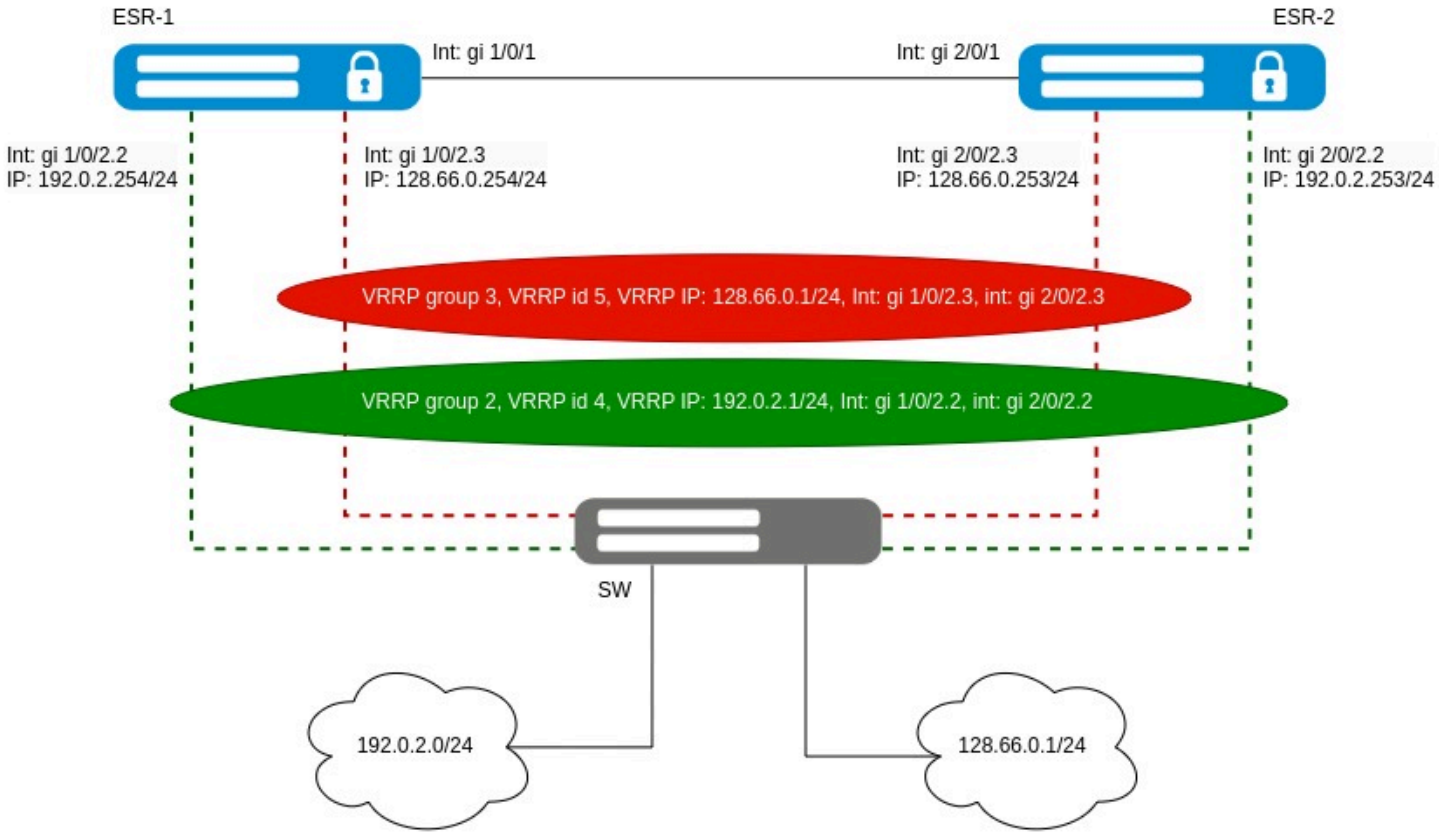


Схема реализации DHCP failover в нескольких VRF

Исходная конфигурация кластера:

ESR-1

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address a2:00:00:10:c0:00
  exit
  unit 2
    mac-address a2:00:00:10:d0:00
  exit
  enable
exit

hostname ESR-1 unit 1
hostname ESR-2 unit 2

object-group service DHCP_SERVER
  port-range 67
exit
object-group service DHCP_CLIENT
  port-range 68
exit

ip vrf LAN_ONE
exit
ip vrf LAN_TWO
exit

security zone SYNC
exit
security zone LAN_ONE
  ip vrf forwarding LAN_ONE
exit
security zone LAN_TWO
  ip vrf forwarding LAN_TWO
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  vrrp 1
    ip address 198.51.100.1/24
    priority 254 unit 1
    priority 253 unit 2
    group 1
    enable
  exit
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
exit
interface gigabitethernet 1/0/2.2
```

```
  ip vrf forwarding LAN_ONE
  security-zone LAN_ONE
  ip address 192.0.2.254/24
  vrrp 4
    ip address 192.0.2.1/24
    priority 120
    group 2
    enable
  exit
exit
interface gigabitethernet 1/0/2.3
  ip vrf forwarding LAN_TWO
  security-zone LAN_TWO
  ip address 128.66.0.254/24
  vrrp 5
    ip address 128.66.0.1/24
    priority 110
    group 3
    enable
  exit
exit
interface gigabitethernet 2/0/1
  mode switchport
exit
interface gigabitethernet 2/0/2.2
  ip vrf forwarding LAN_ONE
  security-zone LAN_ONE
  ip address 192.0.2.253/24
  vrrp 4
    ip address 192.0.2.1/24
    priority 110
    group 2
    enable
  exit
exit
interface gigabitethernet 2/0/2.3
  ip vrf forwarding LAN_TWO
  security-zone LAN_TWO
  ip address 128.66.0.253/24
  vrrp 5
    ip address 128.66.0.1/24
    priority 120
    group 3
    enable
  exit
exit

security zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
exit
security zone-pair LAN_ONE self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
```

```
  rule 2
    action permit
    match protocol udp
    match source-port object-group DHCP_CLIENT
    match destination-port object-group DHCP_SERVER
    enable
  exit
exit
security zone-pair LAN_TWO self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
  rule 2
    action permit
    match protocol udp
    match source-port object-group DHCP_CLIENT
    match destination-port object-group DHCP_SERVER
    enable
  exit
exit

ip dhcp-server vrf LAN_ONE
ip dhcp-server pool LAN_ONE vrf LAN_ONE
  network 192.0.2.0/24
  address-range 192.0.2.10-192.0.2.253
  default-router 192.0.2.1
exit
ip dhcp-server vrf LAN_TWO
ip dhcp-server pool LAN_TWO vrf LAN_TWO
  network 128.66.0.0/24
  address-range 128.66.0.10-128.66.0.253
  default-router 128.66.0.1
exit
```

Решение:

Сконфигурируем object-group для настройки DHCP failover-сервисов:

ESR-1

```
ESR-1(config)# object-group network DST_LAN_ONE
ESR-1(config-object-group-network)# ip address-range 192.0.2.253 unit 1
ESR-1(config-object-group-network)# ip address-range 192.0.2.254 unit 2
ESR-1(config-object-group-network)# exit
ESR-1(config)# object-group network DST_LAN_TWO
ESR-1(config-object-group-network)# ip address-range 128.66.0.253 unit 1
ESR-1(config-object-group-network)# ip address-range 128.66.0.254 unit 2
ESR-1(config-object-group-network)# exit
ESR-1(config)# object-group network SRC_LAN_ONE
ESR-1(config-object-group-network)# ip address-range 192.0.2.254 unit 1
ESR-1(config-object-group-network)# ip address-range 192.0.2.253 unit 2
ESR-1(config-object-group-network)# exit
ESR-1(config)# object-group network SRC_LAN_TWO
ESR-1(config-object-group-network)# ip address-range 128.66.0.254 unit 1
ESR-1(config-object-group-network)# ip address-range 128.66.0.253 unit 2
ESR-1(config-object-group-network)# exit
```

Перейдем к настойке ip failover для каждого VRF, настроим там local-address/remote-address и укажем привязки к соответствующим VRRP-group, на основе которых будет определяться, кто из маршрутизаторов будет выдавать адреса:

ESR-1

```
ESR-1(config)# ip failover vrf LAN_ONE
ESR-1(config-failover)# local-address object-group SRC_LAN_ONE
ESR-1(config-failover)# remote-address object-group DST_LAN_ONE
ESR-1(config-failover)# vrrp-group 2
ESR-1(config-failover)# exit
ESR-1(config)# ip failover vrf LAN_TWO
ESR-1(config-failover)# local-address object-group SRC_LAN_TWO
ESR-1(config-failover)# remote-address object-group DST_LAN_TWO
ESR-1(config-failover)# vrrp-group 3
ESR-1(config-failover)# exit
```

Перейдем к настройке DHCP failover, каждый в своем VRF. Для каждого экземпляра необходимо указать режим работы Active-Standby, а также включить его:

ESR-1

```
ESR-1(config)# ip dhcp-server failover vrf LAN_ONE
ESR-1(config-dhcp-server-failover)# mode active-standby
ESR-1(config-dhcp-server-failover)# enable
ESR-1(config-dhcp-server-failover)# exit
ESR-1(config)# ip dhcp-server failover vrf LAN_TWO
ESR-1(config-dhcp-server-failover)# mode active-standby
ESR-1(config-dhcp-server-failover)# enable
ESR-1(config-dhcp-server-failover)# exit
```

Разрешим в настройках firewall работу dhcp-failover в соответствующих зонах:

ESR-1

```
ESR-1(config)# object-group service SYNC
ESR-1(config-object-group-service)# port-range 873
ESR-1(config-object-group-service)# exit
ESR-1(config)# security zone-pair LAN_ONE self
ESR-1(config-security-zone-pair)# rule 3
ESR-1(config-security-zone-pair-rule)# action permit
ESR-1(config-security-zone-pair-rule)# match protocol tcp
ESR-1(config-security-zone-pair-rule)# match destination-port object-group SYNC
ESR-1(config-security-zone-pair-rule)# enable
ESR-1(config-security-zone-pair-rule)# exit
ESR-1(config-security-zone-pair)# exit
ESR-1(config)# security zone-pair LAN_TWO self
ESR-1(config-security-zone-pair)# rule 3
ESR-1(config-security-zone-pair-rule)# action permit
ESR-1(config-security-zone-pair-rule)# match protocol tcp
ESR-1(config-security-zone-pair-rule)# match destination-port object-group SYNC
ESR-1(config-security-zone-pair-rule)# enable
ESR-1(config-security-zone-pair-rule)# exit
ESR-1(config-security-zone-pair)# exit
ESR-1(config)# exi
```

Посмотреть статус работы DHCP-failover можно с помощью команды, один из экземпляров должен быть в Role - Master, второй в Role - Backup:

ESR-1

```
ESR-1# show ip dhcp server failover vrf LAN_ONE
VRF:                            LAN_ONE
    Mode:                       Active-Standby
    Role:                       Master
    State:                      Synchronized
    Last synchronization:       2025-02-18 09:34:44
ESR-1# show ip dhcp server failover vrf LAN_TWO
VRF:                            LAN_TWO
    Mode:                       Active-Standby
    Role:                       Backup
    State:                      Synchronized
    Last synchronization:       2025-02-18 09:34:46
```

Также статусы работы DHCP-серверов можно посмотреть с помощью команды:

ESR-1

```
ESR-1# show high-availability state
DHCP server:
VRF:                              LAN_TWO
    Mode:                         Active-Standby
    State:                        Successful synchronization
    Last synchronization:         2025-02-18 09:34:30
VRF:                              LAN_ONE
    Mode:                         Active-Standby
    State:                        Successful synchronization
    Last synchronization:         2025-02-18 09:34:28
crypto-sync:
    State:                        Disabled
Firewall sessions and NAT translations:
    State:                        Disabled
```

Выданные адреса DHCP можно просмотреть с помощью команды:

ESR-1

```
ESR-1# show ip dhcp binding vrf LAN_ONE
IP address         MAC / Client ID                                                  Binding type
Lease expires at
----------------   --------------------------------------------------------------   ------------
--------------------
192.0.2.10         50:52:e5:02:0c:00                                                active
2025-02-19 09:34:06
ESR-1# show ip dhcp binding vrf LAN_TWO
IP address         MAC / Client ID                                                  Binding type
Lease expires at
----------------   --------------------------------------------------------------   ------------
--------------------
128.66.0.10        50:6d:ae:02:0e:00                                                active
2025-02-19 09:34:09
```

16.2.7 Настройка SNMP

Протокол SNMP (Simple Network Management Protocol) реализует модель «менеджер–агент» для централизованного управления сетевыми устройствами: агенты, установленные на устройствах, собирают данные, структурированные в MIB, а менеджер запрашивает информацию, мониторит состояние сети, контролирует производительность и вносит изменения в конфигурацию оборудования.

Подробный алгоритм настройки SNMP описан в разделе Настройка SNMP-сервера и отправки SNMP TRAP.

Пример настройки

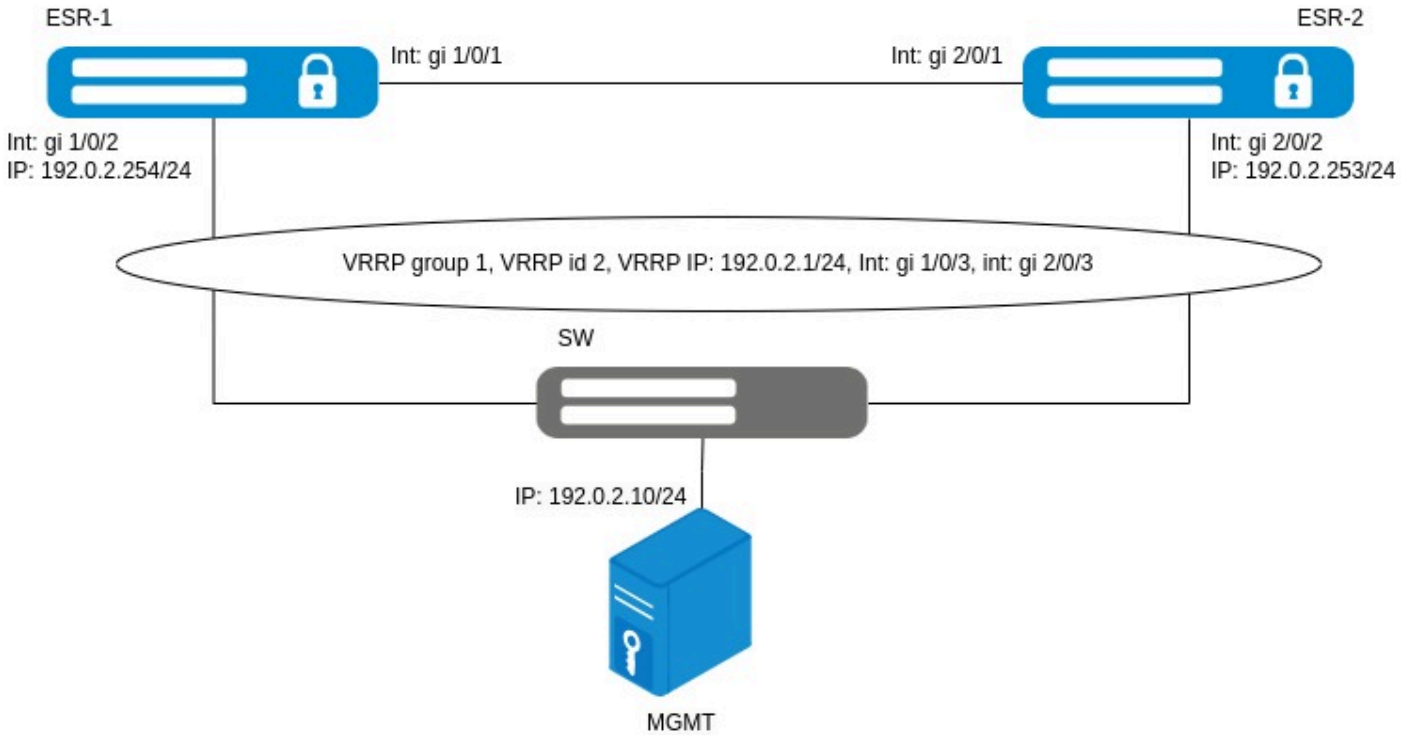


Схема реализации SNMP

Задача:

- обеспечить возможность мониторинга сети через management-интерфейс каждого устройства в кластере:
- обеспечить возможность мониторинга состояния сети и внесения изменений в конфигурацию устройства, выполняющего роль VRRP Master;
- устройство управления (MGMT) доступно по IP-адресу 192.0.2.10.

Исходная конфигурация кластера:

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address a2:00:00:10:c0:00
  exit
  unit 2
    mac-address a2:00:00:10:d0:00
  exit
  enable
exit

hostname ESR-1 unit 1
hostname ESR-2 unit 2

security zone SYNC
exit
security zone MGMT
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  vrrp 1
    ip address 198.51.100.1/24
    priority 254 unit 1
    priority 253 unit 2
    group 1
    enable
  exit
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 1/0/2
  security-zone MGMT
  ip address 192.0.2.254/24
  vrrp 2
    ip address 192.0.2.1/24
    group 1
    enable
  exit
exit
interface gigabitethernet 2/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/2
  security-zone MGMT
  ip address 192.0.2.253/24
  vrrp 2
    ip address 192.0.2.1/24
    group 1
```

```
    enable
  exit
exit

security zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
exit
security zone-pair MGMT self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
exit
```

Решение:

Создадим профиль SNMP-портов, предоставляющий доступ в MGMT зону безопасности:

ESR-1

```
ESR-1(config)# object-group service SNMP
ESR-1(config-object-group-service)# port-range 161
ESR-1(config-object-group-service)# port-range 162
ESR-1(config-object-group-service)# exit
```

Добавим правило, предусматривающее проверку, что порт назначения UDP-пакетов соответствует профилю SNMP-портов:

ESR-1

```
ESR-1(config)# security zone-pair MGMT self
ESR-1(config-security-zone-pair)# rule 2
ESR-1(config-security-zone-pair-rule)# action permit
ESR-1(config-security-zone-pair-rule)# match protocol udp
ESR-1(config-security-zone-pair-rule)# match destination-port object-group SNMP
ESR-1(config-security-zone-pair-rule)# enable
ESR-1(config-security-zone-pair-rule)# exit
ESR-1(config-security-zone-pair)# exit
```

Активируем SNMP-сервер, настроив параметр snmp-community для обеспечения аутентификации и корректного доступа к данным мониторинга:

ESR-1

```
ESR-1(config)# snmp-server
ESR-1(config)# snmp-server community cluster rw
```

Благодаря данной настройке обеспечивается возможность централизованного мониторинга и управления юнитами кластера как отдельными устройствами, так и устройством, выполняющим роль VRRP Master:

ESR-1

```
snmpset -v2c -c cluster 192.0.2.253 .1.3.6.1.2.1.1.5.0 s 'ESR-1'
SNMPv2-MIB::sysName.0 = STRING: ESR-1
snmpset -v2c -c cluster 192.0.2.254 .1.3.6.1.2.1.1.5.0 s 'ESR-2'
SNMPv2-MIB::sysName.0 = STRING: ESR-2
snmpset -v2c -c cluster 192.0.2.1 .1.3.6.1.2.1.1.5.0 s 'VRRP-Master'
SNMPv2-MIB::sysName.0 = STRING: VRRP-Master
```

16.2.8 Настройка Source NAT

Source NAT (SNAT) представляет собой механизм, осуществляющий замену исходного IP-адреса в заголовках IP-пакетов, проходящих через сетевой шлюз. При передаче трафика из внутренней (локальной) сети в внешнюю (публичную) сеть исходный адрес заменяется на один из назначенных публичных IP-адресов шлюза. В ряде случаев осуществляется дополнительное преобразование исходного порта (NATP − Network Address and Port Translation), что обеспечивает корректное направление обратного трафика. При поступлении пакетов из публичной сети в локальную происходит обратная процедура − восстановление оригинальных значений IP-адреса и порта для обеспечения корректной маршрутизации внутри внутренней сети.

Алгоритм Source NAT описан в разделе Алгоритм настройки Source NAT.

Пример настройки

Задача:

- предоставить доступ в Интернет хостам, находящимся в локальной сети;
- клиентская подсеть: 192.0.2.0/24;
- публичный IP-адрес − VIP-адрес на интерфейсе.

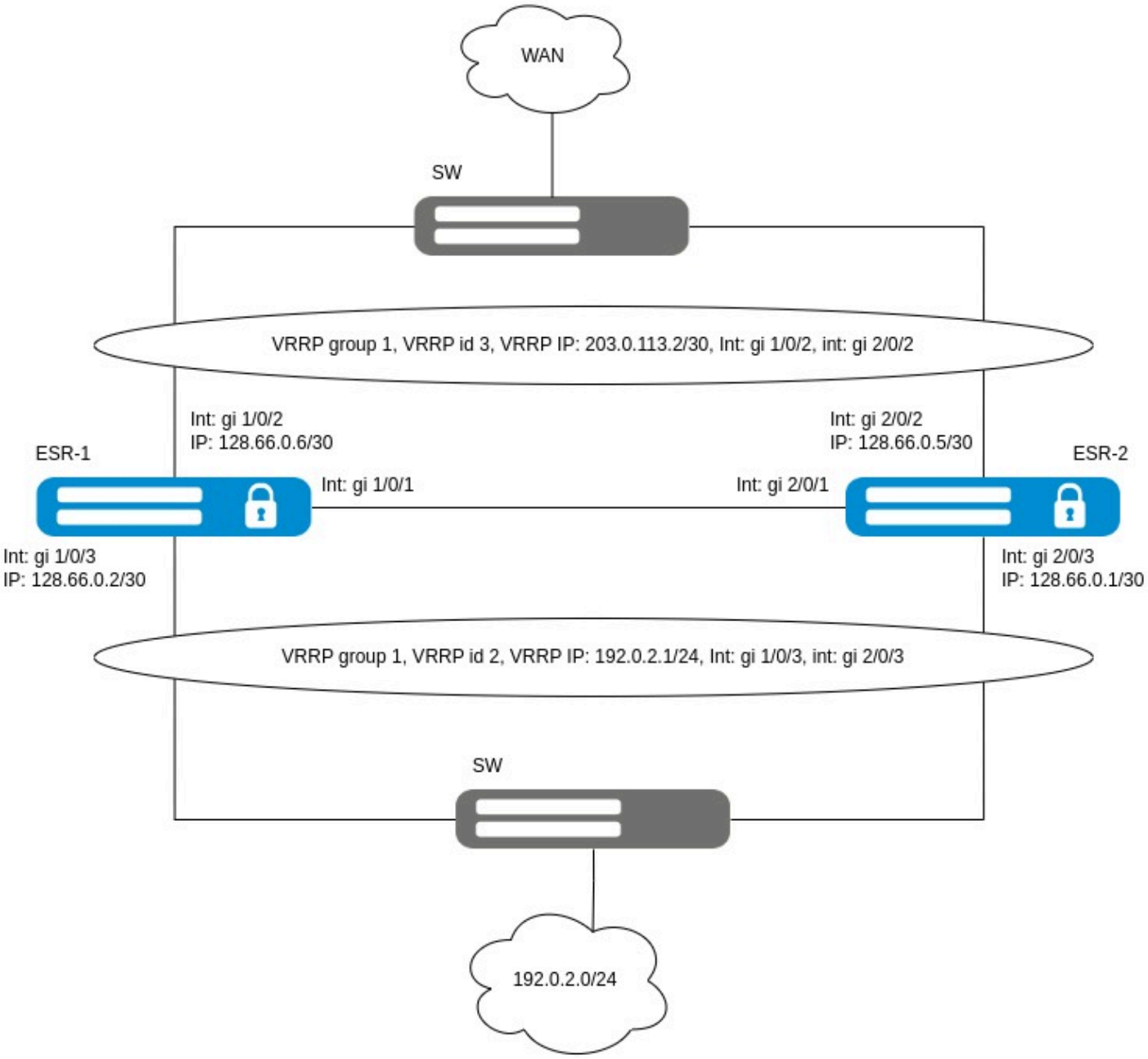


Схема реализации Source NAT

Исходная конфигурация кластера:

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address a2:00:00:10:c0:00
  exit
  unit 2
    mac-address a2:00:00:10:d0:00
  exit
  enable
exit

hostname ESR-1 unit 1
hostname ESR-2 unit 2

security zone SYNC
exit
security zone LAN
exit
security zone WAN
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  vrrp 1
    ip address 198.51.100.1/24
    priority 254 unit 1
    priority 253 unit 2
    group 1
    enable
  exit
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 1/0/2
  security-zone WAN
  ip address 128.66.0.6/30
  vrrp 3
    ip address 203.0.113.2/30
    group 1
    enable
  exit
exit
interface gigabitethernet 1/0/3
  security-zone LAN
  ip address 128.66.0.2/30
  vrrp 2
    ip address 192.0.2.1/24
    group 1
    enable
  exit
```

```
exit
interface gigabitethernet 2/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/2
  security-zone WAN
  ip address 128.66.0.5/30
  vrrp 3
    ip address 203.0.113.2/30
    group 1
    enable
  exit
exit
interface gigabitethernet 2/0/3
  security-zone LAN
  ip address 128.66.0.1/30
  vrrp 2
    ip address 192.0.2.1/24
    group 1
    enable
  exit
exit

security zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
exit
security zone-pair LAN self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
exit
security zone-pair WAN self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
exit
security zone-pair LAN WAN
  rule 1
    action permit
    enable
  exit
exit
```

Решение:

Создадим список IP-адресов, которые будут иметь возможность выхода в Интернет:

ESR-1

```
ESR-1(config)# object-group network INTERNET_USERS
ESR-1(config-object-group-network)# ip address-range 192.0.2.2-192.0.2.255
ESR-1(config-object-group-network)# exit
```

Создадим пул исходных NAT-адресов, в который включим виртуальный IP-адрес (VIP), назначенный WAN-интерфейсу:

ESR-1

```
ESR-1(config)# nat source
ESR-1(config-snat)# pool TRANSLATE_ADDRESS
ESR-1(config-snat-pool)# ip address-range 203.0.113.2
ESR-1(config-snat-pool)# exit
```

Добавим набор правил SNAT. В атрибутах набора укажем применение правил исключительно для пакетов, направляемых в зону WAN. При этом правила осуществляют проверку адреса источника на принадлежность к пулу INTERNET_USERS и выполняют трансляцию исходного адреса в VIP IP-адрес интерфейса:

ESR-1

```
ESR-1(config-snat)# ruleset SNAT
ESR-1(config-snat-ruleset)# to zone WAN
ESR-1(config-snat-ruleset)# rule 1
ESR-1(config-snat-rule)# match source-address object-group INTERNET_USERS
ESR-1(config-snat-rule)# action source-nat pool TRANSLATE_ADDRESS
ESR-1(config-snat-rule)# enable
ESR-1(config-snat-rule)# exit
ESR-1(config-snat-ruleset)# exit
ESR-1(config-snat)# exit
```

Просмотр таблицы NAT трансляций осуществляется посредством следующей команды:

ESR-1

```
ESR-1# show ip nat translations
Prot   Inside source           Inside destination      Outside source          Outside
destination     Pkts         Bytes
----   ---------------------   ---------------------   ---------------------
---------------------   ----------   ----------
tcp    192.0.2.10:45838        203.0.113.1:22          203.0.113.2:45838
203.0.113.1:22          --           --
```

16.2.9 Настройка Destination NAT

Функция Destination NAT (DNAT) выполняет преобразование IP-адреса назначения в заголовках пакетов, проходящих через сетевой шлюз. DNAT применяется для перенаправления трафика, адресованного на IP-адрес в публичном сегменте сети, на «реальный» IP-адрес сервера, расположенного в локальной сети за шлюзом.

Алгоритм настройки Destination NAT описан в разделе Алгоритм настройки DNAT.

Пример настройки

Задача:

- организовать публичный доступа к серверу, находящемуся в частной сети и не имеющему публичного сетевого адреса;
- сервер доступен по адресу: 192.0.2.10/24;

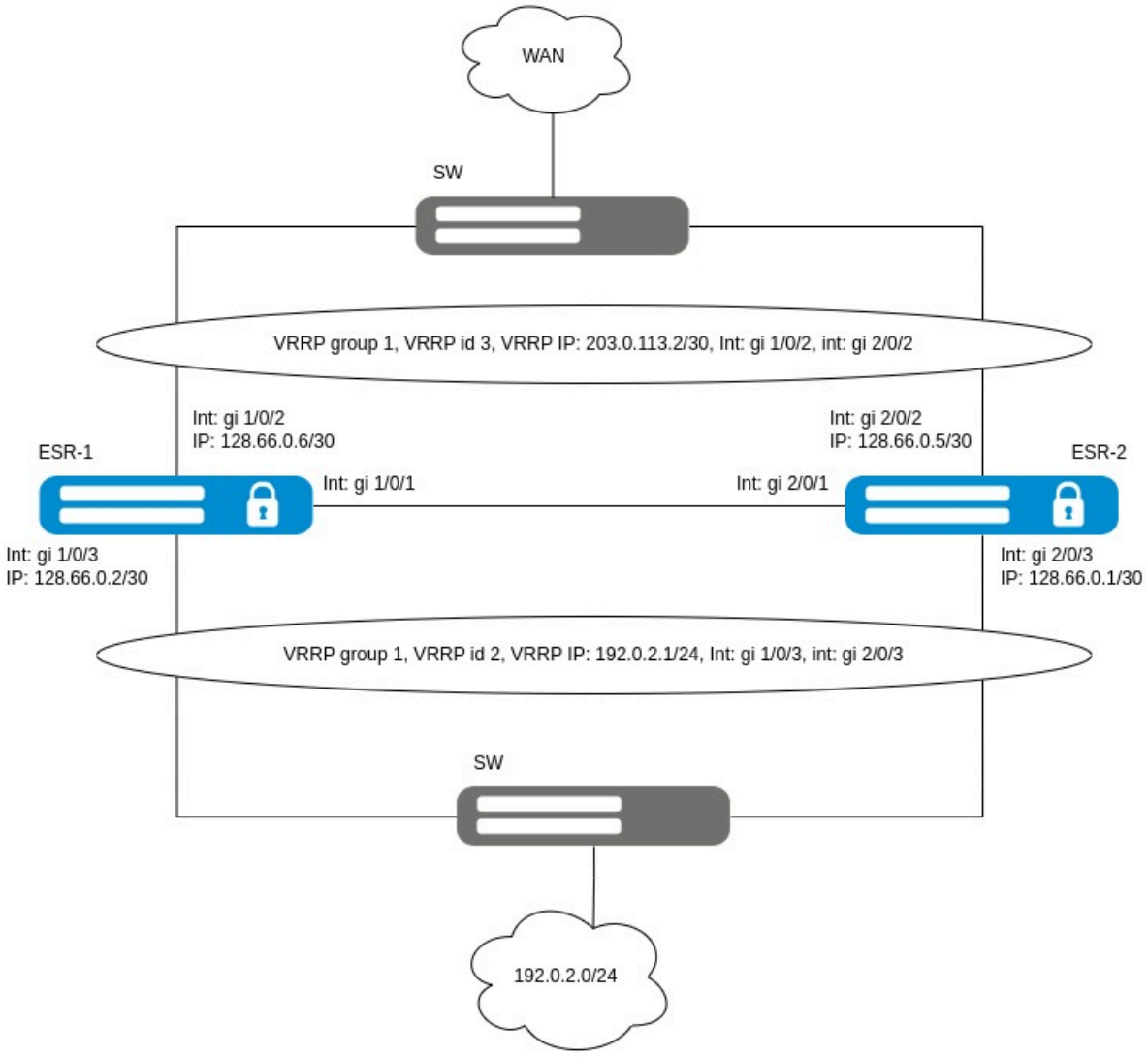


Схема реализации Destination NAT

Исходная конфигурация кластера:

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address a2:00:00:10:c0:00
  exit
  unit 2
    mac-address a2:00:00:10:d0:00
  exit
  enable
exit

hostname ESR-1 unit 1
hostname ESR-2 unit 2

security zone SYNC
exit
security zone LAN
exit
security zone WAN
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  vrrp 1
    ip address 198.51.100.1/24
    priority 254 unit 1
    priority 253 unit 2
    group 1
    enable
  exit
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 1/0/2
  security-zone WAN
  ip address 128.66.0.6/30
  vrrp 3
    ip address 203.0.113.2/30
    group 1
    enable
  exit
exit
interface gigabitethernet 1/0/3
  security-zone LAN
  ip address 128.66.0.2/30
  vrrp 2
    ip address 192.0.2.1/24
    group 1
    enable
  exit
```

```
exit
interface gigabitethernet 2/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/2
  security-zone WAN
  ip address 128.66.0.5/30
  vrrp 3
    ip address 203.0.113.2/30
    group 1
    enable
  exit
exit
interface gigabitethernet 2/0/3
  security-zone LAN
  ip address 128.66.0.1/30
  vrrp 2
    ip address 192.0.2.1/24
    group 1
    enable
  exit
exit

security zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
exit
security zone-pair LAN self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
exit
security zone-pair WAN self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
exit
```

Решение:

Создадим профиль адреса сервера из WAN-сети, с которого будем принимать:

ESR-1

```
ESR-1(config)# object-group network INTERNAL
ESR-1(config-object-group-network)# ip address-range 203.0.113.2
ESR-1(config-object-group-network)# exit
```

Создадим профиль сервиса, доступ к которому будем предоставлять:

ESR-1

```
ESR-1(config)# object-group service SERVER_DMZ
ESR-1(config-object-group-service)# port-range 22
ESR-1(config-object-group-service)# exit
```

Войдем в режим конфигурирования функции DNAT и создадим пул адресов, в которые будут транслироваться адреса пакетов, поступающие на адрес 1.2.3.4 из внешней сети:

ESR-1

```
ESR-1(config)# nat destination
ESR-1(config-dnat)# pool DMZ
ESR-1(config-dnat-pool)# ip address 192.0.2.10
ESR-1(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 WAN. 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):

ESR-1

```
ESR-1(config-dnat)# ruleset DNAT_SERVER_DMZ
ESR-1(config-dnat-ruleset)# from zone WAN
ESR-1(config-dnat-ruleset)# rule 1
ESR-1(config-dnat-rule)# match protocol tcp
ESR-1(config-dnat-rule)# match destination-address object-group INTERNAL
ESR-1(config-dnat-rule)# match destination-port object-group SERVER_DMZ
ESR-1(config-dnat-rule)# action destination-nat pool DMZ
ESR-1(config-dnat-rule)# enable
ESR-1(config-dnat-rule)# exit
ESR-1(config-dnat-ruleset)# exit
ESR-1(config-dnat)# exit
```

Добавим правило, которое проверяет применение правил исключительно к пакетам, поступающим из зоны WAN. Набор правил включает требования соответствия по адресу назначения (match destination-address) и протоколу. Дополнительно в наборе определено действие (action destination-nat), которое применяется к данным, удовлетворяющим указанным критериям:

ESR-1

```
ESR-1(config)# security zone-pair WAN LAN
ESR-1(config-security-zone-pair)# rule 1
ESR-1(config-security-zone-pair-rule)# action permit
ESR-1(config-security-zone-pair-rule)# match protocol tcp
ESR-1(config-security-zone-pair-rule)# match destination-port object-group SERVER_DMZ
ESR-1(config-security-zone-pair-rule)# match destination-nat
ESR-1(config-security-zone-pair-rule)# enable
ESR-1(config-security-zone-pair-rule)# exit
ESR-1(config-security-zone-pair)# exit
```

Просмотр таблицы NAT-трансляций осуществляется посредством следующей команды:

ESR-1

```
ESR-1# show ip nat translations
Prot   Inside source           Inside destination      Outside source          Outside
destination     Pkts         Bytes
----   ---------------------   ---------------------   ---------------------
---------------------   ----------   ----------
tcp    203.0.113.1:41296       192.0.2.10:22           203.0.113.1:41296
203.0.113.2:22          --           --
```

16.2.10 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.

Алгоритм настройки описан в разделе Алгоритм настройки BGP.

Пример настройки eBGP с общим IP-адресом

Задача:

Настроить BGP-протокол в кластере маршрутизаторов ESR-1 и ESR-2 со следующими параметрами:

- соседство устанавливается только с Active-устройством;
- клиентская подсеть: 192.0.2.0/24;
- анонсирование подсетей, подключенных напрямую;
- собственная AS 64500;
- соседство – подсеть 203.0.113.0/24, vrrp IP-адрес для подключения 203.0.113.1, IP-адрес соседа 203.0.113.2, 64501.

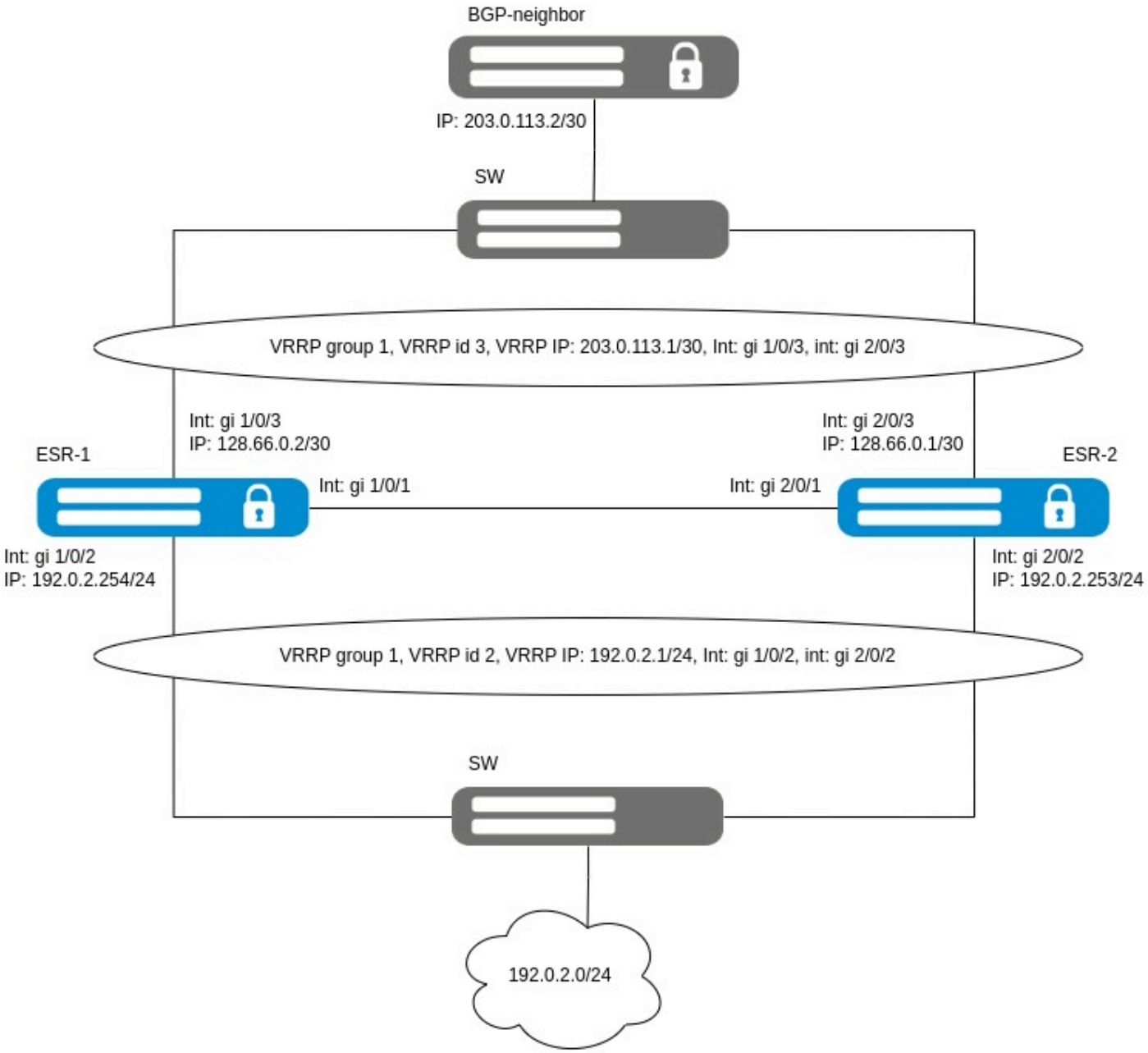


Схема реализации eBGP с общим IP-адресом

Исходная конфигурация кластера:

ESR-1

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address a2:00:00:10:c0:00
  exit
  unit 2
    mac-address a2:00:00:10:d0:00
  exit
  enable
exit

hostname ESR-1 unit 1
hostname ESR-2 unit 2

security zone SYNC
exit
security zone LAN
exit
security zone WAN
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  vrrp 1
    ip address 198.51.100.1/24
    priority 254 unit 1
    priority 253 unit 2
    group 1
    enable
  exit
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 1/0/2
  security-zone LAN
  ip address 192.0.2.254/24
  vrrp 2
    ip address 192.0.2.1/24
    group 1
    enable
  exit
exit
interface gigabitethernet 1/0/3
  security-zone WAN
  ip address 128.66.0.2/30
  vrrp 3
    ip address 203.0.113.1/30
```

```
    group 1
    enable
  exit
exit
interface gigabitethernet 2/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/2
  security-zone LAN
  ip address 192.0.2.253/24
  vrrp 2
    ip address 192.0.2.1/24
    group 1
    enable
  exit
exit
interface gigabitethernet 2/0/3
  security-zone WAN
  ip address 128.66.0.1/30
  vrrp 3
    ip address 203.0.113.1/30
    group 1
    enable
  exit
exit

security zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
exit
security zone-pair LAN self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
  rule 2
    action permit
    match protocol ah
    enable
  exit
exit
security zone-pair WAN self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
exit
```

Решение:

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

```
ESR-1(config)# object-group service og_bgp
ESR-1(config-object-group-service)# port-range 179
ESR-1(config-object-group-service)# exit
ESR-1(config)# security zone WAN
ESR-1(config-security-zone)# exit
ESR-1(config)# security zone-pair WAN self
ESR-1(config-security-zone-pair)# rule 2
ESR-1(config-security-zone-pair-rule)# match protocol tcp
ESR-1(config-security-zone-pair-rule)# match destination-port object-group og_bgp
ESR-1(config-security-zone-pair-rule)# action permit
ESR-1(config-security-zone-pair-rule)# enable
ESR-1(config-security-zone-pair-rule)# exit
ESR-1(config-security-zone-pair)# exit
```

Создадим route-map, который будет использоваться в дальнейшем при настройке разрешающих анонсов роутерам из другой AS. В route-map запретим анонсировать подсеть для cluster-interface:

```
ESR-1(config)# route-map bgp-out
ESR-1(config-route-map)# rule 1
ESR-1(config-route-map-rule)# match ip address 198.51.100.0/24
ESR-1(config-route-map-rule)# action deny
ESR-1(config-route-map-rule)# exit
ESR-1(config-route-map)# rule 2
ESR-1(config-route-map-rule)# action permit
ESR-1(config-route-map-rule)# exit
ESR-1(config-route-map)# exit
```

Создадим BGP-процесс для AS 64500 и войдем в режим конфигурирования параметров процесса:

```
ESR-1(config)# router bgp 64500
```

Сконфигурируем анонсирование подсетей, подключенных напрямую:

```
ESR-1(config-bgp)# address-family ipv4 unicast
ESR-1(config-bgp-af)# redistribute connected
ESR-1(config-bgp-af)# exit
```

Создадим eBGP с вышестоящим роутером:

```
ESR-1(config-bgp)# neighbor 203.0.113.2
ESR-1(config-bgp-neighbor)# remote-as 64501
ESR-1(config-bgp-neighbor)# update-source 203.0.113.1
```

И включим обмен IPv4-маршрутами:

```
ESR-1(config-bgp-neighbor)# address-family ipv4 unicast
ESR-1(config-bgp-neighbor-af)# route-map bgp-out out
ESR-1(config-bgp-neighbor-af)# enable
ESR-1(config-bgp-neighbor-af)# exit
```

Включим работу протокола:

```
ESR-1(config-bgp-neighbor)# enable
ESR-1(config-bgp-neighbor)# exit
ESR-1(config-bgp)# enable
ESR-1(config-bgp)# exit
```

Применим конфигурацию на Active-устройстве.

Информацию о BGP-пирах можно посмотреть командой **show bgp neighbors**:

```
ESR-1# show bgp neighbors
BGP neighbor is 203.0.113.1
    BGP state:                          Established
    Type:                               Static neighbor
    Neighbor address:                   203.0.113.1
    Neighbor AS:                        64501
    Neighbor ID:                        203.0.113.1
    Neighbor caps:                      refresh enhanced-refresh restart-aware AS4
    Session:                            external AS4
    Source address:                     203.0.113.2
    Weight:                             0
    Hold timer:                         124/180
    Keepalive timer:                    27/60
    RR client:                          No
    Address family ipv4 unicast:
      Send-label:                       No
      Default originate:                No
      Default information originate:    No
      Outgoing route-map:               bgp-out
      Preference:                       170
      Remove private AS:                No
      Next-hop self:                    No
      Next-hop unchanged:               No
    Uptime (d,h:m:s):                   00,00:03:13
```

```
ESR-2# show bgp neighbors
BGP neighbor is 203.0.113.2
    BGP state:                          Active
    Type:                               Static neighbor
    Neighbor address:                   203.0.113.1
    Neighbor AS:                        64501
    Connect delay:                      2/5
    Last error:                         Socket: Network is unreachable
```

Таблицу маршрутов протокола BGP можно просмотреть с помощью команды:

```
ESR-1# show bgp ipv4 unicast neighbor 203.0.113.1 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 192.0.2.0/24         203.0.113.2          --      --          --     64500 ?
*  u 192.0.2.0/24         203.0.113.2          --      --          --     64500 ?
*> u 128.66.0.0/30        203.0.113.2          --      --          --     64500 ?
*> u 203.0.113.0/30       203.0.113.2          --      --          --     64500 ?
ESR-1# show bgp ipv4 unicast neighbor 203.0.113.1 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 0.0.0.0/0            203.0.113.1          --      100         0      64501 ?
```

⚠ В случае выхода из строя Active-устройства BGP будет полностью переустанавливаться со Standby-устройством.

Пример настройки eBGP с каждым участником кластера по индивидуальным IP-адресам

Задача:

Настроить BGP-протокол в кластере маршрутизаторов ESR-1 и ESR-2 со следующими параметрами:

- соседство устанавливается с каждым маршрутизатором в кластере индивидуально;
- клиентская подсеть: 192.0.2.0/24;
- анонсирование подсетей, подключенных напрямую;
- собственная AS 64500;
- соседство для ESR-1 – подсеть 203.0.113.0/30, IP-адрес для подключения 203.0.113.1, IP-адрес соседа 203.0.113.2, 64501;
- соседство для ESR-2 – подсеть 203.0.113.4/30, IP-адрес для подключения 203.0.113.5, IP-адрес соседа 203.0.113.6, 64502.

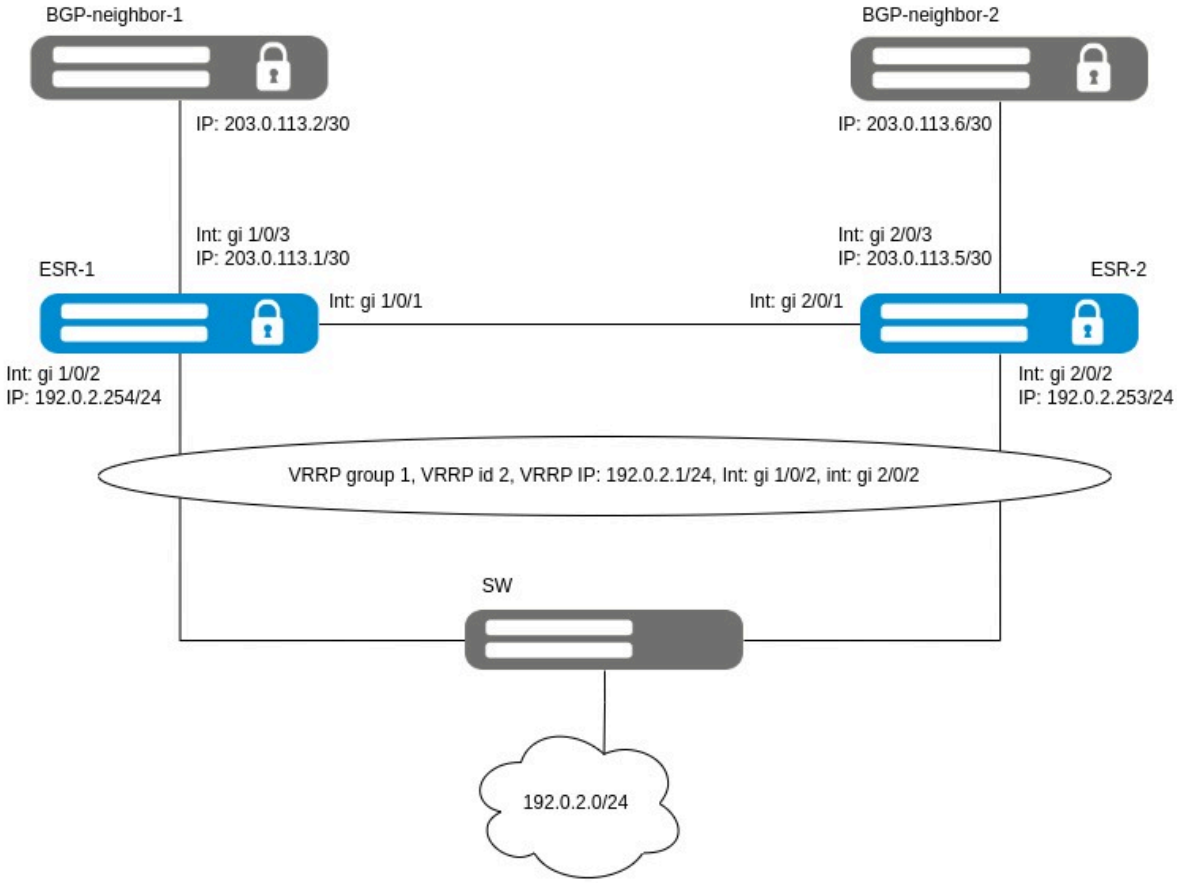


Схема реализации eBGP с каждым участником кластера по индивидуальным IP-адресам

Исходные конфигурации маршрутизаторов в кластере:

ESR-1

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address a2:00:00:10:c0:00
  exit
  unit 2
    mac-address a2:00:00:10:d0:00
  exit
  enable
exit

hostname ESR-1 unit 1
hostname ESR-2 unit 2

security zone SYNC
exit
security zone LAN
exit
security zone WAN
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  vrrp 1
    ip address 198.51.100.1/24
    priority 254 unit 1
    priority 253 unit 2
    group 1
    enable
  exit
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 1/0/2
  security-zone LAN
  ip address 192.0.2.254/24
  vrrp 2
    ip address 192.0.2.1/24
    group 1
    enable
  exit
exit

interface gigabitethernet 1/0/3
  security-zone WAN
  ip address 203.0.113.1/30
exit
```

```
interface gigabitethernet 2/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/2
  security-zone LAN
  ip address 192.0.2.253/24
  vrrp 2
    ip address 192.0.2.1/24
    group 1
    enable
  exit
exit

interface gigabitethernet 2/0/3
  security-zone WAN
  ip address 203.0.113.5/30
exit

security zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
exit
security zone-pair LAN self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
  rule 2
    action permit
    match protocol ah
    enable
  exit
exit
security zone-pair WAN self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
exit
```

Решение:

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

```
ESR-1(config)# object-group service og_bgp
ESR-1(config-object-group-service)# port-range 179
ESR-1(config-object-group-service)# exit
ESR-1(config)# security zone-pair WAN self
ESR-1(config-security-zone-pair)# rule 2
ESR-1(config-security-zone-pair-rule)# match protocol tcp
ESR-1(config-security-zone-pair-rule)# match destination-port object-group og_bgp
ESR-1(config-security-zone-pair-rule)# action permit
ESR-1(config-security-zone-pair-rule)# enable
ESR-1(config-security-zone-pair-rule)# exit
ESR-1(config-security-zone-pair)# exit
```

Создадим track для последующего управления анонсами маршрутов в кластере:

```
ESR-1(config)# track 1
ESR-1(config-track)# track vrrp id 1 state not master
ESR-1(config-track)# enable
ESR-1(config-track)# exit
```

Создадим route-map, который будет использоваться в дальнейшем при настройке разрешающих анонсов роутерам из другой AS. В route-map запретим анонсировать подсеть для cluster-interface, а также настроим управление as-path prepend для управлениями анонсами bgp:

```
ESR-1(config)# route-map bgp-out
ESR-1(config-route-map)# rule 1
ESR-1(config-route-map-rule)# match ip address 198.51.100.0/24
ESR-1(config-route-map-rule)# action deny
ESR-1(config-route-map-rule)# exit
ESR-1(config-route-map)# rule 2
ESR-1(config-route-map-rule)# action set as-path prepend 64500 track 1
ESR-1(config-route-map-rule)# action permit
ESR-1(config-route-map-rule)# exit
ESR-1(config-route-map)# exit
```

Создадим BGP-процесс для AS 64500 для ESR-1 и войдем в режим конфигурирования параметров процесса:

```
ESR-1(config)# router bgp 64500 unit 1
```

Сконфигурируем анонсирование подсетей, подключенных напрямую:

```
ESR-1(config-bgp)# address-family ipv4 unicast
ESR-1(config-bgp-af)# redistribute connected
ESR-1(config-bgp-af)# exit
```

Создадим eBGP с вышестоящим роутером:

```
ESR-1(config-bgp)# neighbor 203.0.113.2
ESR-1(config-bgp-neighbor)# remote-as 64501
ESR-1(config-bgp-neighbor)# update-source 203.0.113.1
```

И включим обмен IPv4-маршрутами:

```
ESR-1(config-bgp-neighbor)# address-family ipv4 unicast
ESR-1(config-bgp-neighbor-af)# route-map bgp-out out
ESR-1(config-bgp-neighbor-af)# enable
ESR-1(config-bgp-neighbor-af)# exit
```

Включим работу протокола:

```
ESR-1(config-bgp-neighbor)# enable
ESR-1(config-bgp-neighbor)# exit
ESR-1(config-bgp)# enable
ESR-1(config-bgp)# exit
```

Создадим BGP процесс для AS 64500 для ESR-2 и войдем в режим конфигурирования параметров процесса:

```
ESR-1(config)# router bgp 64500 unit 2
```

Сконфигурируем анонсирование подсетей, подключенных напрямую:

```
ESR-1(config-bgp)# address-family ipv4 unicast
ESR-1(config-bgp-af)# redistribute connected
ESR-1(config-bgp-af)# exit
```

Создадим eBGP с вышестоящим роутером:

```
ESR-1(config-bgp)# neighbor 203.0.113.6
ESR-1(config-bgp-neighbor)# remote-as 64502
ESR-1(config-bgp-neighbor)# update-source 203.0.113.5
```

И включим обмен IPv4-маршрутами:

```
ESR-1(config-bgp-neighbor)# address-family ipv4 unicast
ESR-1(config-bgp-neighbor-af)# route-map bgp-out out
ESR-1(config-bgp-neighbor-af)# enable
ESR-1(config-bgp-neighbor-af)# exit
```

Включим работу протокола:

```
ESR-1(config-bgp-neighbor)# enable
ESR-1(config-bgp-neighbor)# exit
ESR-1(config-bgp)# enable
ESR-1(config-bgp)# exit
```

Применим конфигурацию на Active-устройстве.

Информацию о BGP-пирах можно посмотреть командой:

```
ESR-1# show bgp neighbors
BGP neighbor is 203.0.113.2
    BGP state:                          Established
    Type:                               Static neighbor
    Neighbor address:                   203.0.113.2
    Neighbor AS:                        64501
    Neighbor ID:                        203.0.113.2
    Neighbor caps:                      refresh enhanced-refresh restart-aware AS4
    Session:                            external AS4
    Source address:                     203.0.113.1
    Weight:                             0
    Hold timer:                         107/180
    Keepalive timer:                    20/60
    RR client:                          No
    Address family ipv4 unicast:
      Send-label:                       No
      Default originate:                No
      Default information originate:    No
      Outgoing route-map:               bgp-out
      Preference:                       170
      Remove private AS:                No
      Next-hop self:                    No
      Next-hop unchanged:               No
    Uptime (d,h:m:s):                   00,00:00:28
```

```
ESR-2# show bgp neighbors
BGP neighbor is 203.0.113.6
    BGP state:                          Established
    Type:                               Static neighbor
    Neighbor address:                   203.0.113.6
    Neighbor AS:                        64502
    Neighbor ID:                        203.0.113.6
    Neighbor caps:                      refresh enhanced-refresh restart-aware AS4
    Session:                            external AS4
    Source address:                     203.0.113.5
    Weight:                             0
    Hold timer:                         144/180
    Keepalive timer:                    29/60
    RR client:                          No
    Address family ipv4 unicast:
      Send-label:                       No
      Default originate:                No
      Default information originate:    No
      Outgoing route-map:               bgp-out
      Preference:                       170
      Remove private AS:                No
      Next-hop self:                    No
      Next-hop unchanged:               No
    Uptime (d,h:m:s):                   00,00:00:20
```

Таблицу маршрутов протокола BGP можно просмотреть с помощью команды:

```
ESR-1# show bgp ipv4 unicast neighbor 203.0.113.2 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 192.0.2.0/24         203.0.113.1          --      --          --     64500 ?
*  u 192.0.2.0/24         203.0.113.1          --      --          --     64500 ?
*> u 203.0.113.0/30       203.0.113.1          --      --          --     64500 ?
ESR-1# show bgp ipv4 unicast neighbor 203.0.113.2 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 0.0.0.0/0            203.0.113.2          --      100         0      64501 ?
```

```
ESR-2# show bgp ipv4 unicast neighbor 203.0.113.6 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 192.0.2.0/24         203.0.113.5          --      --          --     64500 64500 ?
*> u 203.0.113.4/30       203.0.113.5          --      --          --     64500 64500 ?
ESR-2# show bgp ipv4 unicast neighbor 203.0.113.6 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 0.0.0.0/0            203.0.113.6          --      100         0      64502 ?
```

16.2.11 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.

Алгоритм настройки описан в разделе Алгоритм настройки DMVPN.

Пример настройки в кластере DMVPN Single Hub Dual Cloud схемы

Задача:

Организовать DMVPN между офисами компании, используя mGRE-туннели, NHRP (Next Hop Resolution Protocol), протокол динамической маршрутизации (BGP), IPsec. В данном примере будет HUB-маршрутизатор, который находится в кластере, и два филиала. HUB – это DMVPN-сервер (NHS), а филиалы – DMPVN-клиенты (NHC).

HUB внешний IP-адрес через Cloud_one — 198.51.100.2/30;
HUB внешний IP-адрес через Cloud_two — 198.51.100.6/30;

SPOKE-1 внешний IP-адрес — 198.51.100.10/30;
SPOKE-2 внешний IP-адрес — 198.51.100.14/30.

Параметры IPsec VPN:

IKE:

- группа Диффи-Хэллмана: 19;
- алгоритм шифрования: AES256;
- алгоритм аутентификации: SHA2-256.

IPsec:

- группа Диффи-Хэллмана: 19;
- алгоритм шифрования: AES256;
- алгоритм аутентификации: SHA2-256.

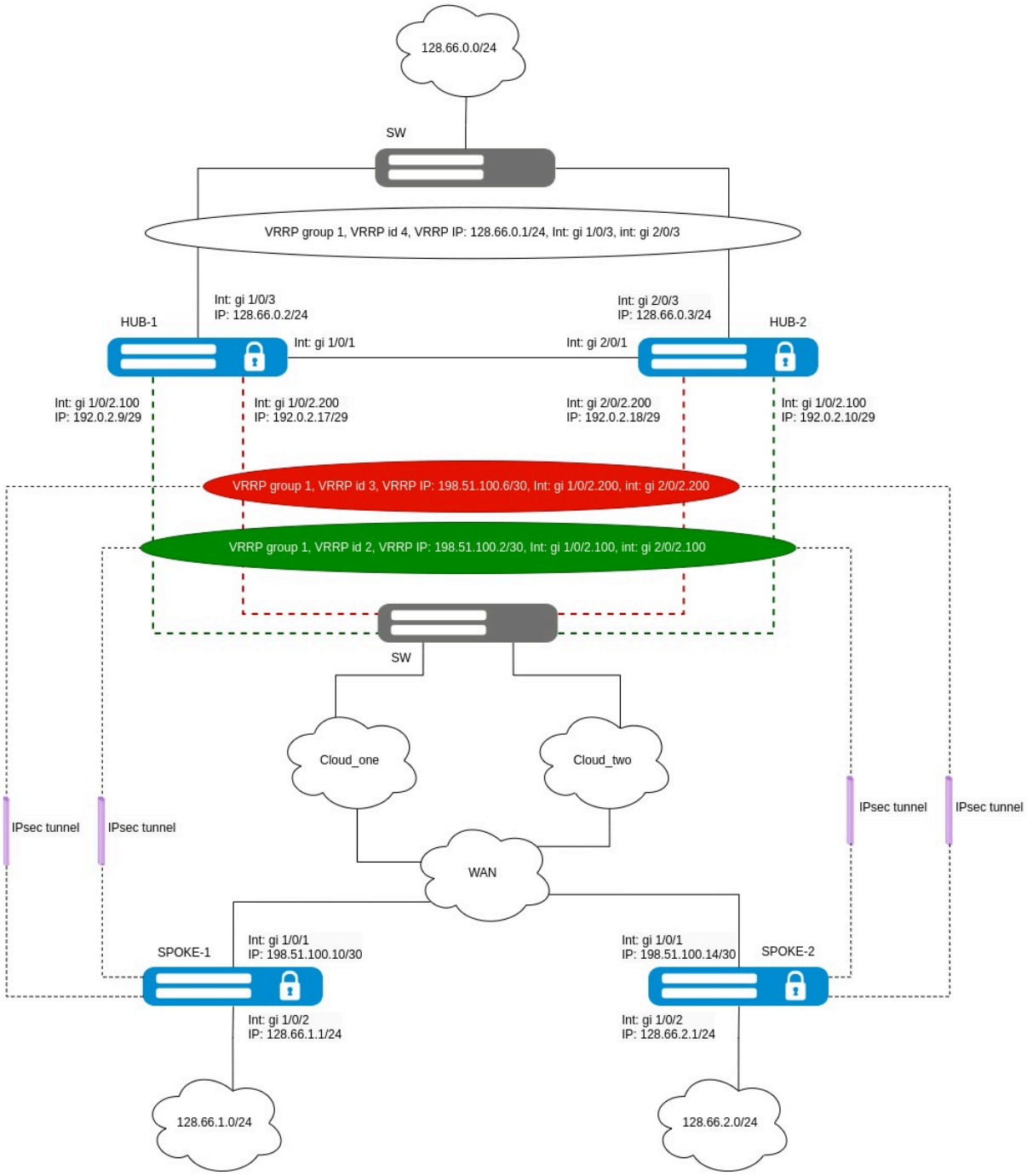


Схема реализации DMVPN Single Hub Dual Cloud в кластере

Исходная конфигурация CLUSTER-HUB:

HUB-1

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address a2:00:00:10:a0:00
  exit
  unit 2
    mac-address a2:00:00:10:b0:00
  exit
  enable
exit

hostname HUB-1 unit 1
hostname HUB-2 unit 2

security zone SYNC
exit
security zone LAN
exit
security zone WAN
exit

ip access-list extended LOCAL_1
  rule 1
    action permit
    match source-address 198.51.100.2 255.255.255.255
    enable
  exit
exit
ip access-list extended LOCAL_2
  rule 1
    action permit
    match source-address 198.51.100.6 255.255.255.255
    enable
  exit
exit

route-map PBR_LOCAL
  rule 1
    match ip access-group LOCAL_1
    action set ip next-hop verify-availability 198.51.100.1 1
  exit
  rule 2
    match ip access-group LOCAL_2
    action set ip next-hop verify-availability 198.51.100.5 1
  exit
exit
route-map DMVPN_BGP_OUT_CLOUD_TWO
  rule 1
    match ip address 0.0.0.0/0
    action set metric bgp 2000
  exit
exit
route-map DMVPN_BGP_OUT_CLOUD_ONE
  rule 1
```

```
    match ip address 0.0.0.0/0
    action set metric bgp 1000
  exit
exit

ip local policy route-map PBR_LOCAL

bridge 1
  vlan 1
  security-zone SYNC
  ip address 192.0.2.5/29 unit 1
  ip address 192.0.2.6/29 unit 2
  vrrp 1
    ip address 192.0.2.1/29
    priority 5 unit 1
    priority 6 unit 2
    group 1
    enable
  exit
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 1/0/2.100
  security-zone WAN
  ip address 192.0.2.9/29
  vrrp 2
    ip address 198.51.100.2/30
    group 1
    enable
  exit
  wan load-balance nexthop 198.51.100.1
  wan load-balance enable
exit
interface gigabitethernet 1/0/2.200
  security-zone WAN
  ip address 192.0.2.17/29
  vrrp 3
    ip address 198.51.100.6/30
    group 1
    enable
  exit
  wan load-balance nexthop 198.51.100.5
  wan load-balance enable
exit
interface gigabitethernet 1/0/3
  security-zone LAN
  ip address 128.66.0.2/24
  vrrp 4
    ip address 128.66.0.1/24
    group 1
    enable
  exit
exit
interface gigabitethernet 2/0/1
  mode switchport
  spanning-tree disable
```

```
exit
interface gigabitethernet 2/0/2.100
  security-zone WAN
  ip address 192.0.2.10/29
  vrrp 2
    ip address 198.51.100.2/30
    group 1
    enable
  exit
  wan load-balance nexthop 198.51.100.1
  wan load-balance enable
exit
interface gigabitethernet 2/0/2.200
  security-zone WAN
  ip address 192.0.2.18/29
  vrrp 3
    ip address 198.51.100.6/30
    group 1
    enable
  exit
  wan load-balance nexthop 198.51.100.5
  wan load-balance enable
exit
interface gigabitethernet 2/0/3
  security-zone LAN
  ip address 128.66.0.3/24
  vrrp 4
    ip address 128.66.0.1/24
    group 1
    enable
  exit
exit

security zone-pair SYNC self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
exit
security zone-pair LAN self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
  rule 2
    action permit
    match protocol ah
    enable
  exit
exit
security zone-pair WAN self
  rule 1
    action permit
    match protocol vrrp
    enable
  exit
  rule 2
    action permit
```

```
    match protocol ah
    enable
  exit
exit

ip route 0.0.0.0/0 wan load-balance rule 1

wan load-balance rule 1
  outbound interface gigabitethernet 1/0/2.100
  outbound interface gigabitethernet 1/0/2.200
  outbound interface gigabitethernet 2/0/2.200
  outbound interface gigabitethernet 2/0/2.100
  enable
exit
```

Исходная конфигурация SPOKE-1:

SPOKE-1

```
hostname SPOKE-1

security zone LAN
exit
security zone WAN
exit

interface gigabitethernet 1/0/1
  security-zone WAN
  ip address 198.51.100.10/30
exit
interface gigabitethernet 1/0/2
  security-zone LAN
  ip address 128.66.1.1/24
exit

ip route 198.51.100.0/30 198.51.100.9
ip route 198.51.100.12/30 198.51.100.9
ip route 198.51.100.4/30 198.51.100.9
```

Исходная конфигурация SPOKE-2:

SPOKE-2

```
hostname SPOKE-2

security zone LAN
exit
security zone WAN
exit

interface gigabitethernet 1/0/1
  security-zone WAN
  ip address 198.51.100.14/30
exit
interface gigabitethernet 1/0/2
  security-zone LAN
  ip address 128.66.2.1/24
exit

ip route 198.51.100.0/30 198.51.100.13
ip route 198.51.100.4/30 198.51.100.13
ip route 198.51.100.8/30 198.51.100.13
```

Решение:

- **Конфигурирование HUB**

Создадим туннели mGRE, каждый через свой CLOUD, определим принадлежность к зоне безопасности, настроим NHRP и включим туннель и NHRP командой **enable**:

```
HUB-1(config)# security zone DMVPN_C_ONE
HUB-1(config-security-zone)# exit
HUB-1(config)# security zone DMVPN_C_TWO
HUB-1(config-security-zone)# exit
HUB-1(config)# tunnel gre 1
HUB-1(config-gre)# key 1000
HUB-1(config-gre)# ttl 64
HUB-1(config-gre)# mtu 1400
HUB-1(config-gre)# multipoint
HUB-1(config-gre)# security-zone DMVPN_C_ONE
HUB-1(config-gre)# local address 198.51.100.2
HUB-1(config-gre)# ip address 203.0.113.1/25
HUB-1(config-gre)# ip tcp adjust-mss 1360
HUB-1(config-gre)# ip nhrp redirect
HUB-1(config-gre)# ip nhrp multicast dynamic
HUB-1(config-gre)# ip nhrp enable
HUB-1(config-gre)# enable
HUB-1(config-gre)# exit
HUB-1(config)# tunnel gre 2
HUB-1(config-gre)# key 2000
HUB-1(config-gre)# ttl 64
HUB-1(config-gre)# mtu 1400
HUB-1(config-gre)# multipoint
HUB-1(config-gre)# security-zone DMVPN_C_TWO
HUB-1(config-gre)# local address 198.51.100.6
HUB-1(config-gre)# ip address 203.0.113.129/25
HUB-1(config-gre)# ip tcp adjust-mss 1360
HUB-1(config-gre)# ip nhrp redirect
HUB-1(config-gre)# ip nhrp multicast dynamic
HUB-1(config-gre)# ip nhrp enable
HUB-1(config-gre)# enable
HUB-1(config-gre)# exit
```

Произведём настройку протокола динамической маршрутизации для Hub. В примере это будет eBGP, для которого необходимо явно разрешить анонсирование подсетей.

Так как в примере используется два CLOUD, необходимо сделать один из них более приоритетным, используя route-map.

Для ускорения переключения в случае выхода из строя Active устройства в кластере включим также bfd для BGP, а также уменьшим таймер error-wait.

```
HUB-1(config)# route-map DMVPN_BGP_OUT_CLOUD_ONE
HUB-1(config-route-map)# rule 1
HUB-1(config-route-map-rule)# match ip address 0.0.0.0/0
HUB-1(config-route-map-rule)# action set metric bgp 1000
HUB-1(config-route-map-rule)# exit
HUB-1(config-route-map)# exit
HUB-1(config)# route-map DMVPN_BGP_OUT_CLOUD_TWO
HUB-1(config-route-map)# rule 1
HUB-1(config-route-map-rule)# match ip address 0.0.0.0/0
HUB-1(config-route-map-rule)# action set metric bgp 2000
HUB-1(config-route-map-rule)# exit
HUB-1(config-route-map)# exit
HUB-1(config)# router bgp 64500
HUB-1(config-bgp)# default-information-originate
HUB-1(config-bgp)# timers error-wait 5 10
HUB-1(config-bgp)# peer-group DMVPN_CLOUD_ONE
HUB-1(config-bgp-group)# remote-as 64501
HUB-1(config-bgp-group)# update-source 203.0.113.1
HUB-1(config-bgp-group)# fall-over bfd
HUB-1(config-bgp-group)# address-family ipv4 unicast
HUB-1(config-bgp-group-af)# route-map DMVPN_BGP_OUT_CLOUD_ONE out
HUB-1(config-bgp-group-af)# next-hop-self
HUB-1(config-bgp-group-af)# enable
HUB-1(config-bgp-group-af)# exit
HUB-1(config-bgp-group)# exit
HUB-1(config-bgp)# peer-group DMVPN_CLOUD_TWO
HUB-1(config-bgp-group)# remote-as 64501
HUB-1(config-bgp-group)# update-source 203.0.113.129
HUB-1(config-bgp-group)# fall-over bfd
HUB-1(config-bgp-group)# address-family ipv4 unicast
HUB-1(config-bgp-group-af)# route-map DMVPN_BGP_OUT_CLOUD_TWO out
HUB-1(config-bgp-group-af)# next-hop-self
HUB-1(config-bgp-group-af)# enable
HUB-1(config-bgp-group-af)# exit
HUB-1(config-bgp-group)# exit
HUB-1(config-bgp)# listen-range 203.0.113.0/25
HUB-1(config-bgp-listen)# peer-group DMVPN_CLOUD_ONE
HUB-1(config-bgp-listen)# enable
HUB-1(config-bgp-listen)# exit
HUB-1(config-bgp)# listen-range 203.0.113.128/25
HUB-1(config-bgp-listen)# peer-group DMVPN_CLOUD_TWO
HUB-1(config-bgp-listen)# enable
HUB-1(config-bgp-listen)# exit
HUB-1(config-bgp)# address-family ipv4 unicast
HUB-1(config-bgp-af)# redistribute static
HUB-1(config-bgp-af)# exit
HUB-1(config-bgp)# enable
HUB-1(config-bgp)# exit
```

Произведём настройку IPsec для Hub, для начала настроим ike proposal, ike policy и ike gateway. В ike gateway дополнительно настроим dpd, для ускорения перестроения туннелей в случае если выйдет из строя Active-устройство:

```
HUB-1(config)# security ike proposal ike_proposal
HUB-1(config-ike-proposal)# authentication algorithm sha2-256
HUB-1(config-ike-proposal)# encryption algorithm aes256
HUB-1(config-ike-proposal)# dh-group 19
HUB-1(config-ike-proposal)# exit
HUB-1(config)#
HUB-1(config)# security ike policy ike_policy
HUB-1(config-ike-policy)# pre-shared-key ascii-text encrypted 8CB5107EA7005AFF
HUB-1(config-ike-policy)# proposal ike_proposal
HUB-1(config-ike-policy)# exit
HUB-1(config)# security ike gateway ike_gateway_cloud_one
HUB-1(config-ike-gw)# version v2-only
HUB-1(config-ike-gw)# ike-policy ike_policy
HUB-1(config-ike-gw)# local address 198.51.100.2
HUB-1(config-ike-gw)# local network 198.51.100.2/32 protocol gre
HUB-1(config-ike-gw)# remote address any
HUB-1(config-ike-gw)# remote network any protocol gre
HUB-1(config-ike-gw)# mode policy-based
HUB-1(config-ike-gw)# mobike disable
HUB-1(config-ike-gw)# dead-peer-detection action clear
HUB-1(config-ike-gw)# dead-peer-detection interval 10
HUB-1(config-ike-gw)# dead-peer-detection timeout 5
HUB-1(config-ike-gw)# exit
HUB-1(config)# security ike gateway ike_gateway_cloud_two
HUB-1(config-ike-gw)# version v2-only
HUB-1(config-ike-gw)# ike-policy ike_policy
HUB-1(config-ike-gw)# local address 198.51.100.6
HUB-1(config-ike-gw)# local network 198.51.100.6/32 protocol gre
HUB-1(config-ike-gw)# remote address any
HUB-1(config-ike-gw)# remote network any protocol gre
HUB-1(config-ike-gw)# mode policy-based
HUB-1(config-ike-gw)# mobike disable
HUB-1(config-ike-gw)# dead-peer-detection action clear
HUB-1(config-ike-gw)# dead-peer-detection interval 10
HUB-1(config-ike-gw)# dead-peer-detection timeout 5
HUB-1(config-ike-gw)# exit
HUB-1(config)#
HUB-1(config)# security ike session uniqueids replace
```

Затем настроим IPsec proposal, IPsec policy и IPsec vpn туннели через каждый CLOUD:

```
HUB-1(config)# security ipsec proposal ipsec_proposal
HUB-1(config-ipsec-proposal)# authentication algorithm sha2-256
HUB-1(config-ipsec-proposal)# encryption algorithm aes256
HUB-1(config-ipsec-proposal)# pfs dh-group 19
HUB-1(config-ipsec-proposal)# exit
HUB-1(config)# security ipsec policy ipsec_policy
HUB-1(config-ipsec-policy)# proposal ipsec_proposal
HUB-1(config-ipsec-policy)# exit
HUB-1(config)# security ipsec vpn ipsec_dynamic_cloud_one
HUB-1(config-ipsec-vpn)# type transport
HUB-1(config-ipsec-vpn)# ike establish-tunnel route
HUB-1(config-ipsec-vpn)# ike gateway ike_gateway_cloud_one
HUB-1(config-ipsec-vpn)# ike ipsec-policy ipsec_policy
HUB-1(config-ipsec-vpn)# enable
HUB-1(config-ipsec-vpn)# exit
HUB-1(config)# security ipsec vpn ipsec_dynamic_cloud_two
HUB-1(config-ipsec-vpn)# type transport
HUB-1(config-ipsec-vpn)# ike establish-tunnel route
HUB-1(config-ipsec-vpn)# ike gateway ike_gateway_cloud_two
HUB-1(config-ipsec-vpn)# ike ipsec-policy ipsec_policy
HUB-1(config-ipsec-vpn)# enable
HUB-1(config-ipsec-vpn)# exit
```

Скорректируем правила зоны безопасности WAN, разрешим протоколы для GRE over IPSec-туннеля:

```
HUB-1(config)# object-group service ISAKMP_PORT
HUB-1(config-object-group-service)# port-range 500
HUB-1(config-object-group-service)# port-range 4500
HUB-1(config-object-group-service)# exit
HUB-1(config)# security zone-pair WAN self
HUB-1(config-security-zone-pair)# rule 3
HUB-1(config-security-zone-pair-rule)# action permit
HUB-1(config-security-zone-pair-rule)# match protocol udp
HUB-1(config-security-zone-pair-rule)# match destination-port object-group ISAKMP_PORT
HUB-1(config-security-zone-pair-rule)# enable
HUB-1(config-security-zone-pair-rule)# exit
HUB-1(config-security-zone-pair)# rule 4
HUB-1(config-security-zone-pair-rule)# action permit
HUB-1(config-security-zone-pair-rule)# match protocol esp
HUB-1(config-security-zone-pair-rule)# enable
HUB-1(config-security-zone-pair-rule)# exit
HUB-1(config-security-zone-pair)# rule 5
HUB-1(config-security-zone-pair-rule)# action permit
HUB-1(config-security-zone-pair-rule)# match protocol gre
HUB-1(config-security-zone-pair-rule)# enable
HUB-1(config-security-zone-pair-rule)# exit
HUB-1(config-security-zone-pair)# exit
```

Настроим правила зон безопасности DMVPN_C_ONE и DMVPN_C_TWO, разрешим прохождение трафика для протоколов BGP, BFD, ICMP:

```
HUB-1(config)# object-group service BGP
HUB-1(config-object-group-service)# port-range 179
HUB-1(config-object-group-service)# exit
HUB-1(config)# object-group service BFD
HUB-1(config-object-group-service)# port-range 3784
HUB-1(config-object-group-service)# exit
HUB-1(config)# security zone-pair DMVPN_C_ONE self
HUB-1(config-security-zone-pair)# rule 1
HUB-1(config-security-zone-pair-rule)# action permit
HUB-1(config-security-zone-pair-rule)# match protocol icmp
HUB-1(config-security-zone-pair-rule)# enable
HUB-1(config-security-zone-pair-rule)# exit
HUB-1(config-security-zone-pair)# rule 2
HUB-1(config-security-zone-pair-rule)# action permit
HUB-1(config-security-zone-pair-rule)# match protocol tcp
HUB-1(config-security-zone-pair-rule)# match destination-port object-group BGP
HUB-1(config-security-zone-pair-rule)# enable
HUB-1(config-security-zone-pair-rule)# exit
HUB-1(config-security-zone-pair)# rule 3
HUB-1(config-security-zone-pair-rule)# action permit
HUB-1(config-security-zone-pair-rule)# match protocol udp
HUB-1(config-security-zone-pair-rule)# match destination-port object-group BFD
HUB-1(config-security-zone-pair-rule)# enable
HUB-1(config-security-zone-pair-rule)# exit
HUB-1(config-security-zone-pair)# exit
HUB-1(config)# security zone-pair DMVPN_C_TWO self
HUB-1(config-security-zone-pair)# rule 1
HUB-1(config-security-zone-pair-rule)# action permit
HUB-1(config-security-zone-pair-rule)# match protocol icmp
HUB-1(config-security-zone-pair-rule)# enable
HUB-1(config-security-zone-pair-rule)# exit
HUB-1(config-security-zone-pair)# rule 2
HUB-1(config-security-zone-pair-rule)# action permit
HUB-1(config-security-zone-pair-rule)# match protocol tcp
HUB-1(config-security-zone-pair-rule)# match destination-port object-group BGP
HUB-1(config-security-zone-pair-rule)# enable
HUB-1(config-security-zone-pair-rule)# exit
HUB-1(config-security-zone-pair)# rule 3
HUB-1(config-security-zone-pair-rule)# action permit
HUB-1(config-security-zone-pair-rule)# match protocol udp
HUB-1(config-security-zone-pair-rule)# match destination-port object-group BFD
HUB-1(config-security-zone-pair-rule)# enable
HUB-1(config-security-zone-pair-rule)# exit
HUB-1(config-security-zone-pair)# exit
```

Скорректируем правила зоны безопасности LAN, разрешим прохождение трафика между зонами LAN и DMVPN_C_ONE/DMVPN_C_TWO:

```
HUB-1(config)# security zone-pair LAN DMVPN_C_ONE
HUB-1(config-security-zone-pair)# rule 1
HUB-1(config-security-zone-pair-rule)# action permit
HUB-1(config-security-zone-pair-rule)# enable
HUB-1(config-security-zone-pair-rule)# exit
HUB-1(config-security-zone-pair)# exit
HUB-1(config)# security zone-pair LAN DMVPN_C_TWO
HUB-1(config-security-zone-pair)# rule 1
HUB-1(config-security-zone-pair-rule)# action permit
HUB-1(config-security-zone-pair-rule)# enable
HUB-1(config-security-zone-pair-rule)# exit
HUB-1(config-security-zone-pair)# exit
HUB-1(config)# security zone-pair DMVPN_C_ONE LAN
HUB-1(config-security-zone-pair)# rule 1
HUB-1(config-security-zone-pair-rule)# action permit
HUB-1(config-security-zone-pair-rule)# enable
HUB-1(config-security-zone-pair-rule)# exit
HUB-1(config-security-zone-pair)# exit
HUB-1(config)# security zone-pair DMVPN_C_TWO LAN
HUB-1(config-security-zone-pair)# rule 1
HUB-1(config-security-zone-pair-rule)# action permit
HUB-1(config-security-zone-pair-rule)# enable
HUB-1(config-security-zone-pair-rule)# exit
HUB-1(config-security-zone-pair)# exit
```

- **Конфигурирование SPOKE-1**

Создадим туннели mGRE, каждый через свой CLOUD, определим принадлежность к зоне безопасности, настроим NHRP и включим туннель и NHRP командой **enable**:

```
SPOKE-1(config)# security zone DMVPN_C_TWO
SPOKE-1(config-security-zone)# exit
SPOKE-1(config)# security zone DMVPN_C_ONE
SPOKE-1(config-security-zone)# exit
SPOKE-1(config)# tunnel gre 1
SPOKE-1(config-gre)# key 1000
SPOKE-1(config-gre)# ttl 64
SPOKE-1(config-gre)# mtu 1400
SPOKE-1(config-gre)# multipoint
SPOKE-1(config-gre)# security-zone DMVPN_C_ONE
SPOKE-1(config-gre)# local address 198.51.100.10
SPOKE-1(config-gre)# ip address 203.0.113.2/25
SPOKE-1(config-gre)# ip tcp adjust-mss 1360
SPOKE-1(config-gre)# ip nhrp holding-time 60
SPOKE-1(config-gre)# ip nhrp shortcut
SPOKE-1(config-gre)# ip nhrp map 203.0.113.1 198.51.100.2
SPOKE-1(config-gre)# ip nhrp nhs 203.0.113.1
SPOKE-1(config-gre)# ip nhrp multicast nhs
SPOKE-1(config-gre)# ip nhrp enable
SPOKE-1(config-gre)# enable
SPOKE-1(config-gre)# exit
SPOKE-1(config)# tunnel gre 2
SPOKE-1(config-gre)# key 2000
SPOKE-1(config-gre)# ttl 64
SPOKE-1(config-gre)# mtu 1400
SPOKE-1(config-gre)# multipoint
SPOKE-1(config-gre)# security-zone DMVPN_C_TWO
SPOKE-1(config-gre)# local address 198.51.100.10
SPOKE-1(config-gre)# ip address 203.0.113.130/25
SPOKE-1(config-gre)# ip tcp adjust-mss 1360
SPOKE-1(config-gre)# ip nhrp holding-time 60
SPOKE-1(config-gre)# ip nhrp shortcut
SPOKE-1(config-gre)# ip nhrp map 203.0.113.129 198.51.100.6
SPOKE-1(config-gre)# ip nhrp nhs 203.0.113.129
SPOKE-1(config-gre)# ip nhrp multicast nhs
SPOKE-1(config-gre)# ip nhrp enable
SPOKE-1(config-gre)# enable
SPOKE-1(config-gre)# exit
```

Произведём настройку протокола динамической маршрутизации для SPOKE-1. В примере это будет eBGP, для которого необходимо явно разрешить анонсирование подсетей. Анонсируем LAN подсети в сторону HUB используя network в address-family.

Для ускорения переключения в случае выхода из строя Active-устройства в кластере включим также bfd для BGP, а также уменьшим таймер error-wait.

```
SPOKE-1(config)# route-map DMVPN_BGP_OUT
SPOKE-1(config-route-map)# rule 1
SPOKE-1(config-route-map-rule)# exit
SPOKE-1(config-route-map)# exit
SPOKE-1(config)# router bgp 64501
SPOKE-1(config-bgp)# timers error-wait 5 10
SPOKE-1(config-bgp)# neighbor 203.0.113.1
SPOKE-1(config-bgp-neighbor)# remote-as 64500
SPOKE-1(config-bgp-neighbor)# allow-local-as 10
SPOKE-1(config-bgp-neighbor)# update-source 203.0.113.2
SPOKE-1(config-bgp-neighbor)# fall-over bfd
SPOKE-1(config-bgp-neighbor)# address-family ipv4 unicast
SPOKE-1(config-bgp-neighbor-af)# route-map DMVPN_BGP_OUT out
SPOKE-1(config-bgp-neighbor-af)# enable
SPOKE-1(config-bgp-neighbor-af)# exit
SPOKE-1(config-bgp-neighbor)# enable
SPOKE-1(config-bgp-neighbor)# exit
SPOKE-1(config-bgp)# neighbor 203.0.113.129
SPOKE-1(config-bgp-neighbor)# remote-as 64500
SPOKE-1(config-bgp-neighbor)# allow-local-as 10
SPOKE-1(config-bgp-neighbor)# update-source 203.0.113.130
SPOKE-1(config-bgp-neighbor)# fall-over bfd
SPOKE-1(config-bgp-neighbor)# address-family ipv4 unicast
SPOKE-1(config-bgp-neighbor-af)# route-map DMVPN_BGP_OUT out
SPOKE-1(config-bgp-neighbor-af)# enable
SPOKE-1(config-bgp-neighbor-af)# exit
SPOKE-1(config-bgp-neighbor)# enable
SPOKE-1(config-bgp-neighbor)# exit
SPOKE-1(config-bgp)# address-family ipv4 unicast
SPOKE-1(config-bgp-af)# network 128.66.1.0/24
SPOKE-1(config-bgp-af)# exit
SPOKE-1(config-bgp)# enable
SPOKE-1(config-bgp)# exit
```

Произведём настройку IPsec для SPOKE-1, настроим ike proposal, ike policy и ike gateway. В ike gateway дополнительно настроим dpd для ускорения перестроения туннелей, в случае если выйдет из строя Active-устройство:

```
SPOKE-1(config)# security ike proposal ike_proposal
SPOKE-1(config-ike-proposal)# authentication algorithm sha2-256
SPOKE-1(config-ike-proposal)# encryption algorithm aes256
SPOKE-1(config-ike-proposal)# dh-group 19
SPOKE-1(config-ike-proposal)# exit
SPOKE-1(config)# security ike policy ike_policy
SPOKE-1(config-ike-policy)# pre-shared-key ascii-text encrypted 8CB5107EA7005AFF
SPOKE-1(config-ike-policy)# proposal ike_proposal
SPOKE-1(config-ike-policy)# exit
SPOKE-1(config)# security ike gateway ike_gateway_cloud_one
SPOKE-1(config-ike-gw)# version v2-only
SPOKE-1(config-ike-gw)# ike-policy ike_policy
SPOKE-1(config-ike-gw)# local address 198.51.100.10
SPOKE-1(config-ike-gw)# local network 198.51.100.10/32 protocol gre
SPOKE-1(config-ike-gw)# remote address 198.51.100.2
SPOKE-1(config-ike-gw)# remote network 198.51.100.2/32 protocol gre
SPOKE-1(config-ike-gw)# mode policy-based
SPOKE-1(config-ike-gw)# mobike disable
SPOKE-1(config-ike-gw)# dead-peer-detection action clear
SPOKE-1(config-ike-gw)# dead-peer-detection interval 10
SPOKE-1(config-ike-gw)# dead-peer-detection timeout 5
SPOKE-1(config-ike-gw)# exit
SPOKE-1(config)# security ike gateway ike_gateway_cloud_two
SPOKE-1(config-ike-gw)# version v2-only
SPOKE-1(config-ike-gw)# ike-policy ike_policy
SPOKE-1(config-ike-gw)# local address 198.51.100.10
SPOKE-1(config-ike-gw)# local network 198.51.100.10/32 protocol gre
SPOKE-1(config-ike-gw)# remote address 198.51.100.6
SPOKE-1(config-ike-gw)# remote network 198.51.100.6/32 protocol gre
SPOKE-1(config-ike-gw)# mode policy-based
SPOKE-1(config-ike-gw)# mobike disable
SPOKE-1(config-ike-gw)# dead-peer-detection action clear
SPOKE-1(config-ike-gw)# dead-peer-detection interval 10
SPOKE-1(config-ike-gw)# dead-peer-detection timeout 5
SPOKE-1(config-ike-gw)# exit
SPOKE-1(config)# security ike gateway ike_gateway_to_spokes
SPOKE-1(config-ike-gw)# version v2-only
SPOKE-1(config-ike-gw)# ike-policy ike_policy
SPOKE-1(config-ike-gw)# local address 198.51.100.10
SPOKE-1(config-ike-gw)# local network 198.51.100.10/32 protocol gre
SPOKE-1(config-ike-gw)# remote id any
SPOKE-1(config-ike-gw)# remote address any
SPOKE-1(config-ike-gw)# remote network any protocol gre
SPOKE-1(config-ike-gw)# mode policy-based
SPOKE-1(config-ike-gw)# mobike disable
SPOKE-1(config-ike-gw)# dead-peer-detection action clear
SPOKE-1(config-ike-gw)# dead-peer-detection interval 10
SPOKE-1(config-ike-gw)# dead-peer-detection timeout 5
SPOKE-1(config-ike-gw)# exit
```

Затем настроим IPsec proposal, IPsec policy и IPsec vpn туннели через каждый CLOUD:

```
SPOKE-1(config)# security ipsec proposal ipsec_proposal
SPOKE-1(config-ipsec-proposal)# authentication algorithm sha2-256
SPOKE-1(config-ipsec-proposal)# encryption algorithm aes256
SPOKE-1(config-ipsec-proposal)# pfs dh-group 19
SPOKE-1(config-ipsec-proposal)# exit
SPOKE-1(config)# security ipsec policy ipsec_policy
SPOKE-1(config-ipsec-policy)# proposal ipsec_proposal
SPOKE-1(config-ipsec-policy)# exit
SPOKE-1(config)# security ipsec vpn ipsec_dynamic_to_spoke
SPOKE-1(config-ipsec-vpn)# type transport
SPOKE-1(config-ipsec-vpn)# ike establish-tunnel route
SPOKE-1(config-ipsec-vpn)# ike gateway ike_gateway_to_spokes
SPOKE-1(config-ipsec-vpn)# ike ipsec-policy ipsec_policy
SPOKE-1(config-ipsec-vpn)# enable
SPOKE-1(config-ipsec-vpn)# exit
SPOKE-1(config)# security ipsec vpn ipsec_static_cloud_one
SPOKE-1(config-ipsec-vpn)# type transport
SPOKE-1(config-ipsec-vpn)# ike establish-tunnel route
SPOKE-1(config-ipsec-vpn)# ike gateway ike_gateway_cloud_one
SPOKE-1(config-ipsec-vpn)# ike ipsec-policy ipsec_policy
SPOKE-1(config-ipsec-vpn)# enable
SPOKE-1(config-ipsec-vpn)# exit
SPOKE-1(config)# security ipsec vpn ipsec_static_cloud_two
SPOKE-1(config-ipsec-vpn)# type transport
SPOKE-1(config-ipsec-vpn)# ike establish-tunnel route
SPOKE-1(config-ipsec-vpn)# ike gateway ike_gateway_cloud_two
SPOKE-1(config-ipsec-vpn)# ike ipsec-policy ipsec_policy
SPOKE-1(config-ipsec-vpn)# enable
SPOKE-1(config-ipsec-vpn)# exit
```

Скорректируем правила зоны безопасности WAN, разрешим протоколы для GRE over IPSec-туннеля:

```
SPOKE-1(config)# object-group service ISAKMP_PORT
SPOKE-1(config-object-group-service)# port-range 500
SPOKE-1(config-object-group-service)# port-range 4500
SPOKE-1(config-object-group-service)# exit
SPOKE-1(config)#  security zone-pair WAN self
SPOKE-1(config-security-zone-pair)# rule 1
SPOKE-1(config-security-zone-pair-rule)# action permit
SPOKE-1(config-security-zone-pair-rule)# match protocol udp
SPOKE-1(config-security-zone-pair-rule)# match destination-port object-group ISAKMP_PORT
SPOKE-1(config-security-zone-pair-rule)# enable
SPOKE-1(config-security-zone-pair-rule)# exit
SPOKE-1(config-security-zone-pair)# rule 2
SPOKE-1(config-security-zone-pair-rule)# action permit
SPOKE-1(config-security-zone-pair-rule)# match protocol esp
SPOKE-1(config-security-zone-pair-rule)# enable
SPOKE-1(config-security-zone-pair-rule)# exit
SPOKE-1(config-security-zone-pair)# rule 3
SPOKE-1(config-security-zone-pair-rule)# action permit
SPOKE-1(config-security-zone-pair-rule)# match protocol gre
SPOKE-1(config-security-zone-pair-rule)# enable
SPOKE-1(config-security-zone-pair-rule)# exit
SPOKE-1(config-security-zone-pair)# exit
```

Настроим правила зон безопасности DMVPN_C_ONE и DMVPN_C_TWO, разрешим прохождение трафика для протоколов BGP, BFD, ICMP:

```
SPOKE-1(config)# object-group service BGP
SPOKE-1(config-object-group-service)# port-range 179
SPOKE-1(config-object-group-service)# exit
SPOKE-1(config)# object-group service BFD
SPOKE-1(config-object-group-service)# port-range 3784
SPOKE-1(config-object-group-service)# exit
SPOKE-1(config)# security zone-pair DMVPN_C_ONE self
SPOKE-1(config-security-zone-pair)# rule 1
SPOKE-1(config-security-zone-pair-rule)# action permit
SPOKE-1(config-security-zone-pair-rule)# match protocol icmp
SPOKE-1(config-security-zone-pair-rule)# enable
SPOKE-1(config-security-zone-pair-rule)# exit
SPOKE-1(config-security-zone-pair)# rule 2
SPOKE-1(config-security-zone-pair-rule)# action permit
SPOKE-1(config-security-zone-pair-rule)# match protocol tcp
SPOKE-1(config-security-zone-pair-rule)# match destination-port object-group BGP
SPOKE-1(config-security-zone-pair-rule)# enable
SPOKE-1(config-security-zone-pair-rule)# exit
SPOKE-1(config-security-zone-pair)# rule 3
SPOKE-1(config-security-zone-pair-rule)# action permit
SPOKE-1(config-security-zone-pair-rule)# match protocol udp
SPOKE-1(config-security-zone-pair-rule)# match destination-port object-group BFD
SPOKE-1(config-security-zone-pair-rule)# enable
SPOKE-1(config-security-zone-pair-rule)# exit
SPOKE-1(config-security-zone-pair)# exit
SPOKE-1(config)# security zone-pair DMVPN_C_TWO self
SPOKE-1(config-security-zone-pair)# rule 1
SPOKE-1(config-security-zone-pair-rule)# action permit
SPOKE-1(config-security-zone-pair-rule)# match protocol icmp
SPOKE-1(config-security-zone-pair-rule)# enable
SPOKE-1(config-security-zone-pair-rule)# exit
SPOKE-1(config-security-zone-pair)# rule 2
SPOKE-1(config-security-zone-pair-rule)# action permit
SPOKE-1(config-security-zone-pair-rule)# match protocol tcp
SPOKE-1(config-security-zone-pair-rule)# match destination-port object-group BGP
SPOKE-1(config-security-zone-pair-rule)# enable
SPOKE-1(config-security-zone-pair-rule)# exit
SPOKE-1(config-security-zone-pair)# rule 3
SPOKE-1(config-security-zone-pair-rule)# action permit
SPOKE-1(config-security-zone-pair-rule)# match protocol udp
SPOKE-1(config-security-zone-pair-rule)# match destination-port object-group BFD
SPOKE-1(config-security-zone-pair-rule)# enable
SPOKE-1(config-security-zone-pair-rule)# exit
SPOKE-1(config-security-zone-pair)# exit
```

Скорректируем правила зоны безопасности LAN, разрешим прохождение трафика между зонами LAN и DMVPN_C_ONE/DMVPN_C_TWO:

```
SPOKE-1(config)# security zone-pair LAN DMVPN_C_ONE
SPOKE-1(config-security-zone-pair)# rule 1
SPOKE-1(config-security-zone-pair-rule)# action permit
SPOKE-1(config-security-zone-pair-rule)# enable
SPOKE-1(config-security-zone-pair-rule)# exit
SPOKE-1(config-security-zone-pair)# exit
SPOKE-1(config)# security zone-pair LAN DMVPN_C_TWO
SPOKE-1(config-security-zone-pair)# rule 1
SPOKE-1(config-security-zone-pair-rule)# action permit
SPOKE-1(config-security-zone-pair-rule)# enable
SPOKE-1(config-security-zone-pair-rule)# exit
SPOKE-1(config-security-zone-pair)# exit
SPOKE-1(config)# security zone-pair DMVPN_C_ONE LAN
SPOKE-1(config-security-zone-pair)# rule 1
SPOKE-1(config-security-zone-pair-rule)# action permit
SPOKE-1(config-security-zone-pair-rule)# match protocol icmp
SPOKE-1(config-security-zone-pair-rule)# enable
SPOKE-1(config-security-zone-pair-rule)# exit
SPOKE-1(config-security-zone-pair)# exit
SPOKE-1(config)# security zone-pair DMVPN_C_TWO LAN
SPOKE-1(config-security-zone-pair)# rule 1
SPOKE-1(config-security-zone-pair-rule)# action permit
SPOKE-1(config-security-zone-pair-rule)# match protocol icmp
SPOKE-1(config-security-zone-pair-rule)# enable
SPOKE-1(config-security-zone-pair-rule)# exit
SPOKE-1(config-security-zone-pair)# exit
```

- **Конфигурирование SPOKE-2**

Создадим туннели mGRE, каждый через свой CLOUD, определим принадлежность к зоне безопасности, настроим NHRP и включим туннель и NHRP командой **enable**:

```
SPOKE-2(config)# security zone DMVPN_C_TWO
SPOKE-2(config-security-zone)# exit
SPOKE-2(config)# security zone DMVPN_C_ONE
SPOKE-2(config-security-zone)# exit
SPOKE-2(config)# tunnel gre 1
SPOKE-2(config-gre)# key 1000
SPOKE-2(config-gre)# ttl 64
SPOKE-2(config-gre)# mtu 1400
SPOKE-2(config-gre)# multipoint
SPOKE-2(config-gre)# security-zone DMVPN_C_ONE
SPOKE-2(config-gre)# local address 198.51.100.14
SPOKE-2(config-gre)# ip address 203.0.113.3/25
SPOKE-2(config-gre)# ip tcp adjust-mss 1360
SPOKE-2(config-gre)# ip nhrp holding-time 60
SPOKE-2(config-gre)# ip nhrp shortcut
SPOKE-2(config-gre)# ip nhrp map 203.0.113.1 198.51.100.2
SPOKE-2(config-gre)# ip nhrp nhs 203.0.113.1
SPOKE-2(config-gre)# ip nhrp multicast nhs
SPOKE-2(config-gre)# ip nhrp enable
SPOKE-2(config-gre)# enable
SPOKE-2(config-gre)# exit
SPOKE-2(config)# tunnel gre 2
SPOKE-2(config-gre)# key 2000
SPOKE-2(config-gre)# ttl 64
SPOKE-2(config-gre)# mtu 1400
SPOKE-2(config-gre)# multipoint
SPOKE-2(config-gre)# security-zone DMVPN_C_TWO
SPOKE-2(config-gre)# local address 198.51.100.14
SPOKE-2(config-gre)# ip address 203.0.113.131/25
SPOKE-2(config-gre)# ip tcp adjust-mss 1360
SPOKE-2(config-gre)# ip nhrp holding-time 60
SPOKE-2(config-gre)# ip nhrp shortcut
SPOKE-2(config-gre)# ip nhrp map 203.0.113.129 198.51.100.6
SPOKE-2(config-gre)# ip nhrp nhs 203.0.113.129
SPOKE-2(config-gre)# ip nhrp multicast nhs
SPOKE-2(config-gre)# ip nhrp enable
SPOKE-2(config-gre)# enable
SPOKE-2(config-gre)# exit
```

Произведём настройку протокола динамической маршрутизации для SPOKE-1. В примере это будет eBGP, для которого необходимо явно разрешить анонсирование подсетей. Анонсируем LAN-подсети в сторону HUB, используя network в address-family.

Для ускорения переключения в случае выхода из строя Active-устройства в кластере включим также bfd для BGP, а также уменьшим таймер error-wait.

```
SPOKE-2(config)# route-map DMVPN_BGP_OUT
SPOKE-2(config-route-map)# rule 1
SPOKE-2(config-route-map-rule)# exit
SPOKE-2(config-route-map)# exit
SPOKE-2(config)# router bgp 64501
SPOKE-2(config-bgp)# timers error-wait 5 10
SPOKE-2(config-bgp)# neighbor 203.0.113.1
SPOKE-2(config-bgp-neighbor)# remote-as 64500
SPOKE-2(config-bgp-neighbor)# allow-local-as 10
SPOKE-2(config-bgp-neighbor)# update-source 203.0.113.3
SPOKE-2(config-bgp-neighbor)# fall-over bfd
SPOKE-2(config-bgp-neighbor)# address-family ipv4 unicast
SPOKE-2(config-bgp-neighbor-af)# route-map DMVPN_BGP_OUT out
SPOKE-2(config-bgp-neighbor-af)# enable
SPOKE-2(config-bgp-neighbor-af)# exit
SPOKE-2(config-bgp-neighbor)# enable
SPOKE-2(config-bgp-neighbor)# exit
SPOKE-2(config-bgp)# neighbor 203.0.113.129
SPOKE-2(config-bgp-neighbor)# remote-as 64500
SPOKE-2(config-bgp-neighbor)# allow-local-as 10
SPOKE-2(config-bgp-neighbor)# update-source 203.0.113.131
SPOKE-2(config-bgp-neighbor)# fall-over bfd
SPOKE-2(config-bgp-neighbor)# address-family ipv4 unicast
SPOKE-2(config-bgp-neighbor-af)# route-map DMVPN_BGP_OUT out
SPOKE-2(config-bgp-neighbor-af)# enable
SPOKE-2(config-bgp-neighbor-af)# exit
SPOKE-2(config-bgp-neighbor)# enable
SPOKE-2(config-bgp-neighbor)# exit
SPOKE-2(config-bgp)# address-family ipv4 unicast
SPOKE-2(config-bgp-af)# network 128.66.2.0/24
SPOKE-2(config-bgp-af)# exit
SPOKE-2(config-bgp)# enable
SPOKE-2(config-bgp)# exit
```

Произведём настройку IPsec для SPOKE-1, настроим ike proposal, ike policy и ike gateway. В ike gateway дополнительно настроим dpd, для ускорения перестроения туннелей, в случае если выйдет из строя Active-устройство:

```
SPOKE-2(config)# security ike proposal ike_proposal
SPOKE-2(config-ike-proposal)# authentication algorithm sha2-256
SPOKE-2(config-ike-proposal)# encryption algorithm aes256
SPOKE-2(config-ike-proposal)# dh-group 19
SPOKE-2(config-ike-proposal)# exit
SPOKE-2(config)# security ike policy ike_policy
SPOKE-2(config-ike-policy)# pre-shared-key ascii-text encrypted 8CB5107EA7005AFF
SPOKE-2(config-ike-policy)# proposal ike_proposal
SPOKE-2(config-ike-policy)# exit
SPOKE-2(config)# security ike gateway ike_gateway_cloud_one
SPOKE-2(config-ike-gw)# version v2-only
SPOKE-2(config-ike-gw)# ike-policy ike_policy
SPOKE-2(config-ike-gw)# local address 198.51.100.14
SPOKE-2(config-ike-gw)# local network 198.51.100.14/32 protocol gre
SPOKE-2(config-ike-gw)# remote address 198.51.100.2
SPOKE-2(config-ike-gw)# remote network 198.51.100.2/32 protocol gre
SPOKE-2(config-ike-gw)# mode policy-based
SPOKE-2(config-ike-gw)# mobike disable
SPOKE-2(config-ike-gw)# dead-peer-detection action clear
SPOKE-2(config-ike-gw)# dead-peer-detection interval 10
SPOKE-2(config-ike-gw)# dead-peer-detection timeout 5
SPOKE-2(config-ike-gw)# exit
SPOKE-2(config)# security ike gateway ike_gateway_cloud_two
SPOKE-2(config-ike-gw)# version v2-only
SPOKE-2(config-ike-gw)# ike-policy ike_policy
SPOKE-2(config-ike-gw)# local address 198.51.100.14
SPOKE-2(config-ike-gw)# local network 198.51.100.14/32 protocol gre
SPOKE-2(config-ike-gw)# remote address 198.51.100.6
SPOKE-2(config-ike-gw)# remote network 198.51.100.6/32 protocol gre
SPOKE-2(config-ike-gw)# mode policy-based
SPOKE-2(config-ike-gw)# mobike disable
SPOKE-2(config-ike-gw)# dead-peer-detection action clear
SPOKE-2(config-ike-gw)# dead-peer-detection interval 10
SPOKE-2(config-ike-gw)# dead-peer-detection timeout 5
SPOKE-2(config-ike-gw)# exit
SPOKE-2(config)# security ike gateway ike_gateway_to_spokes
SPOKE-2(config-ike-gw)# version v2-only
SPOKE-2(config-ike-gw)# ike-policy ike_policy
SPOKE-2(config-ike-gw)# local address 198.51.100.14
SPOKE-2(config-ike-gw)# local network 198.51.100.14/32 protocol gre
SPOKE-2(config-ike-gw)# remote id any
SPOKE-2(config-ike-gw)# remote address any
SPOKE-2(config-ike-gw)# remote network any protocol gre
SPOKE-2(config-ike-gw)# mode policy-based
SPOKE-2(config-ike-gw)# mobike disable
SPOKE-2(config-ike-gw)# dead-peer-detection action clear
SPOKE-2(config-ike-gw)# dead-peer-detection interval 10
SPOKE-2(config-ike-gw)# dead-peer-detection timeout 5
SPOKE-2(config-ike-gw)# exit
```

Затем настроим IPsec proposal, IPsec policy и IPsec vpn туннели через каждый CLOUD:

```
SPOKE-2(config)# security ipsec proposal ipsec_proposal
SPOKE-2(config-ipsec-proposal)# authentication algorithm sha2-256
SPOKE-2(config-ipsec-proposal)# encryption algorithm aes256
SPOKE-2(config-ipsec-proposal)# pfs dh-group 19
SPOKE-2(config-ipsec-proposal)# exit
SPOKE-2(config)# security ipsec policy ipsec_policy
SPOKE-2(config-ipsec-policy)# proposal ipsec_proposal
SPOKE-2(config-ipsec-policy)# exit
SPOKE-2(config)# security ipsec vpn ipsec_dynamic_to_spoke
SPOKE-2(config-ipsec-vpn)# type transport
SPOKE-2(config-ipsec-vpn)# ike establish-tunnel route
SPOKE-2(config-ipsec-vpn)# ike gateway ike_gateway_to_spokes
SPOKE-2(config-ipsec-vpn)# ike ipsec-policy ipsec_policy
SPOKE-2(config-ipsec-vpn)# enable
SPOKE-2(config-ipsec-vpn)# exit
SPOKE-2(config)# security ipsec vpn ipsec_static_cloud_one
SPOKE-2(config-ipsec-vpn)# type transport
SPOKE-2(config-ipsec-vpn)# ike establish-tunnel route
SPOKE-2(config-ipsec-vpn)# ike gateway ike_gateway_cloud_one
SPOKE-2(config-ipsec-vpn)# ike ipsec-policy ipsec_policy
SPOKE-2(config-ipsec-vpn)# enable
SPOKE-2(config-ipsec-vpn)# exit
SPOKE-2(config)# security ipsec vpn ipsec_static_cloud_two
SPOKE-2(config-ipsec-vpn)# type transport
SPOKE-2(config-ipsec-vpn)# ike establish-tunnel route
SPOKE-2(config-ipsec-vpn)# ike gateway ike_gateway_cloud_two
SPOKE-2(config-ipsec-vpn)# ike ipsec-policy ipsec_policy
SPOKE-2(config-ipsec-vpn)# enable
SPOKE-2(config-ipsec-vpn)# exit
```

Скорректируем правила зоны безопасности WAN, разрешим протоколы для GRE over IPSec-туннеля:

```
SPOKE-2(config)# object-group service ISAKMP_PORT
SPOKE-2(config-object-group-service)# port-range 500
SPOKE-2(config-object-group-service)# port-range 4500
SPOKE-2(config-object-group-service)# exit
SPOKE-2(config)#  security zone-pair WAN self
SPOKE-2(config-security-zone-pair)# rule 1
SPOKE-2(config-security-zone-pair-rule)# action permit
SPOKE-2(config-security-zone-pair-rule)# match protocol udp
SPOKE-2(config-security-zone-pair-rule)# match destination-port object-group ISAKMP_PORT
SPOKE-2(config-security-zone-pair-rule)# enable
SPOKE-2(config-security-zone-pair-rule)# exit
SPOKE-2(config-security-zone-pair)# rule 2
SPOKE-2(config-security-zone-pair-rule)# action permit
SPOKE-2(config-security-zone-pair-rule)# match protocol esp
SPOKE-2(config-security-zone-pair-rule)# enable
SPOKE-2(config-security-zone-pair-rule)# exit
SPOKE-2(config-security-zone-pair)# rule 3
SPOKE-2(config-security-zone-pair-rule)# action permit
SPOKE-2(config-security-zone-pair-rule)# match protocol gre
SPOKE-2(config-security-zone-pair-rule)# enable
SPOKE-2(config-security-zone-pair-rule)# exit
SPOKE-2(config-security-zone-pair)# exit
```

Настроим правила зон безопасности DMVPN_C_ONE и DMVPN_C_TWO, разрешим прохождение трафика для протоколов BGP, BFD, ICMP:

```
SPOKE-2(config)# object-group service BGP
SPOKE-2(config-object-group-service)# port-range 179
SPOKE-2(config-object-group-service)# exit
SPOKE-2(config)# object-group service BFD
SPOKE-2(config-object-group-service)# port-range 3784
SPOKE-2(config-object-group-service)# exit
SPOKE-2(config)# security zone-pair DMVPN_C_ONE self
SPOKE-2(config-security-zone-pair)# rule 1
SPOKE-2(config-security-zone-pair-rule)# action permit
SPOKE-2(config-security-zone-pair-rule)# match protocol icmp
SPOKE-2(config-security-zone-pair-rule)# enable
SPOKE-2(config-security-zone-pair-rule)# exit
SPOKE-2(config-security-zone-pair)# rule 2
SPOKE-2(config-security-zone-pair-rule)# action permit
SPOKE-2(config-security-zone-pair-rule)# match protocol tcp
SPOKE-2(config-security-zone-pair-rule)# match destination-port object-group BGP
SPOKE-2(config-security-zone-pair-rule)# enable
SPOKE-2(config-security-zone-pair-rule)# exit
SPOKE-2(config-security-zone-pair)# rule 3
SPOKE-2(config-security-zone-pair-rule)# action permit
SPOKE-2(config-security-zone-pair-rule)# match protocol udp
SPOKE-2(config-security-zone-pair-rule)# match destination-port object-group BFD
SPOKE-2(config-security-zone-pair-rule)# enable
SPOKE-2(config-security-zone-pair-rule)# exit
SPOKE-2(config-security-zone-pair)# exit
SPOKE-2(config)# security zone-pair DMVPN_C_TWO self
SPOKE-2(config-security-zone-pair)# rule 1
SPOKE-2(config-security-zone-pair-rule)# action permit
SPOKE-2(config-security-zone-pair-rule)# match protocol icmp
SPOKE-2(config-security-zone-pair-rule)# enable
SPOKE-2(config-security-zone-pair-rule)# exit
SPOKE-2(config-security-zone-pair)# rule 2
SPOKE-2(config-security-zone-pair-rule)# action permit
SPOKE-2(config-security-zone-pair-rule)# match protocol tcp
SPOKE-2(config-security-zone-pair-rule)# match destination-port object-group BGP
SPOKE-2(config-security-zone-pair-rule)# enable
SPOKE-2(config-security-zone-pair-rule)# exit
SPOKE-2(config-security-zone-pair)# rule 3
SPOKE-2(config-security-zone-pair-rule)# action permit
SPOKE-2(config-security-zone-pair-rule)# match protocol udp
SPOKE-2(config-security-zone-pair-rule)# match destination-port object-group BFD
SPOKE-2(config-security-zone-pair-rule)# enable
SPOKE-2(config-security-zone-pair-rule)# exit
SPOKE-2(config-security-zone-pair)# exit
```

Скорректируем правила зоны безопасности LAN, разрешим прохождение трафика между зонами LAN и DMVPN_C_ONE/DMVPN_C_TWO:

```
SPOKE-2(config)# security zone-pair LAN DMVPN_C_ONE
SPOKE-2(config-security-zone-pair)# rule 1
SPOKE-2(config-security-zone-pair-rule)# action permit
SPOKE-2(config-security-zone-pair-rule)# enable
SPOKE-2(config-security-zone-pair-rule)# exit
SPOKE-2(config-security-zone-pair)# exit
SPOKE-2(config)# security zone-pair LAN DMVPN_C_TWO
SPOKE-2(config-security-zone-pair)# rule 1
SPOKE-2(config-security-zone-pair-rule)# action permit
SPOKE-2(config-security-zone-pair-rule)# enable
SPOKE-2(config-security-zone-pair-rule)# exit
SPOKE-2(config-security-zone-pair)# exit
SPOKE-2(config)# security zone-pair DMVPN_C_ONE LAN
SPOKE-2(config-security-zone-pair)# rule 1
SPOKE-2(config-security-zone-pair-rule)# action permit
SPOKE-2(config-security-zone-pair-rule)# match protocol icmp
SPOKE-2(config-security-zone-pair-rule)# enable
SPOKE-2(config-security-zone-pair-rule)# exit
SPOKE-2(config-security-zone-pair)# exit
SPOKE-2(config)# security zone-pair DMVPN_C_TWO LAN
SPOKE-2(config-security-zone-pair)# rule 1
SPOKE-2(config-security-zone-pair-rule)# action permit
SPOKE-2(config-security-zone-pair-rule)# match protocol icmp
SPOKE-2(config-security-zone-pair-rule)# enable
SPOKE-2(config-security-zone-pair-rule)# exit
SPOKE-2(config-security-zone-pair)# exit
```

Проверка работы:

Состояние IPsec-туннелей можно посмотреть командой:

```
HUB-1# show security ipsec vpn status
Name                              Local host        Remote host       Initiator spi
Responder spi        State
-------------------------------   ---------------   ---------------   ------------------
------------------   -----------
ipsec_dynamic_cloud_one           198.51.100.2      198.51.100.14     0x22d11891e06edf92
0x40469d552e93e47c   Established
ipsec_dynamic_cloud_two           198.51.100.6      198.51.100.14     0x61f7a205eeef5d06
0x141239e7309d351c   Established
ipsec_dynamic_cloud_one           198.51.100.2      198.51.100.10     0x3dbf984518584d5e
0x08563e2683776071   Established
ipsec_dynamic_cloud_two           198.51.100.6      198.51.100.10     0x500adbe8428c7d35
0x9c83c7a2255cb0ed   Established
```

```
SPOKE-1# show security ipsec vpn status
Name                              Local host        Remote host       Initiator spi
Responder spi        State
-------------------------------   ---------------   ---------------   ------------------
------------------   -----------
ipsec_static_cloud_one            198.51.100.10     198.51.100.2      0x3dbf984518584d5e
0x08563e2683776071   Established
ipsec_static_cloud_two            198.51.100.10     198.51.100.6      0x500adbe8428c7d35
0x9c83c7a2255cb0ed   Established
```

```
SPOKE-2# show security ipsec vpn status
Name                              Local host        Remote host       Initiator spi
Responder spi        State
-------------------------------   ---------------   ---------------   ------------------
------------------   -----------
ipsec_static_cloud_one            198.51.100.14     198.51.100.2      0x22d11891e06edf92
0x40469d552e93e47c   Established
ipsec_static_cloud_two            198.51.100.14     198.51.100.6      0x61f7a205eeef5d06
0x141239e7309d351c   Established
```

Состояние NHRP-записей можно посмотреть командой:

```
HUB-1# show ip nhrp peers
 Flags: E - unique, R - nhs, U - used, L - lower-up
        C - connected, G - group, Q - qos, N - nat
        P - protected, I - Redirect-ignored, X - undefined

Tunnel address         NBMA address       Tunnel      Expire      Created          Type
Flags
                                                      (h:m:s)     (d,h:m:s)
--------------------   ----------------   ---------   ---------   --------------
---------------   ----------
203.0.113.2            198.51.100.10      gre 1       00:00:51    00,00:04:41      dynamic
LCP
203.0.113.3            198.51.100.14      gre 1       00:00:48    00,00:04:44      dynamic
LCP
203.0.113.130          198.51.100.10      gre 2       00:00:51    00,00:04:41      dynamic
LCP
203.0.113.131          198.51.100.14      gre 2       00:00:48    00,00:04:44      dynamic
LCP
```

```
SPOKE-1# show ip nhrp peers
 Flags: E - unique, R - nhs, U - used, L - lower-up
        C - connected, G - group, Q - qos, N - nat
        P - protected, I - Redirect-ignored, X - undefined

Tunnel address         NBMA address       Tunnel      Expire      Created          Type
Flags
                                                      (h:m:s)     (d,h:m:s)
--------------------   ----------------   ---------   ---------   --------------
---------------   ----------
203.0.113.1            198.51.100.2       gre 1       --          00,00:00:13
static            RULCP
203.0.113.129          198.51.100.6       gre 2       --          00,00:00:13
static            RULCP
```

```
SPOKE-2# show ip nhrp peers
 Flags: E - unique, R - nhs, U - used, L - lower-up
        C - connected, G - group, Q - qos, N - nat
        P - protected, I - Redirect-ignored, X - undefined

Tunnel address         NBMA address       Tunnel      Expire      Created          Type
Flags
                                                      (h:m:s)     (d,h:m:s)
--------------------   ----------------   ---------   ---------   --------------
---------------   ----------
203.0.113.1            198.51.100.2       gre 1       --          00,00:00:16
static            RULCP
203.0.113.129          198.51.100.6       gre 2       --          00,00:00:16
static            RULCP
```

17 Управление удаленным доступом

- Настройка сервера удаленного доступа к корпоративной сети по PPTP-протоколу
- Настройка сервера удаленного доступа к корпоративной сети по L2TP over IPsec протоколу
- Настройка сервера удаленного доступа к корпоративной сети по OpenVPN-протоколу
- Настройка сервера удаленного доступа к корпоративной сети по WireGuard-протоколу
- Настройка клиента удаленного доступа по протоколу PPPoE
- Настройка клиента удаленного доступа по протоколу PPTP
- Настройка клиента удаленного доступа по протоколу L2TP
- Настройка клиента удаленного доступа по протоколу WireGuard

17.1 Настройка сервера удаленного доступа к корпоративной сети по PPTP-протоколу

PPTP (англ. Point-to-Point Tunneling Protocol) – туннельный протокол типа точка-точка, позволяющий компьютеру устанавливать защищённое соединение с сервером за счёт создания специального туннеля в обычной незащищенной сети. PPTP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например, Интернет. PPTP может также использоваться для организации туннеля между двумя локальными сетями. PPTP использует дополнительное TCP-соединение для обслуживания туннеля.

17.1.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать профиль PPTP-сервера.	**esr(config)# remote-access pptp <NAME>**	<NAME> – имя профиля PPTP-сервера, задаётся строкой до 31 символа.
2	Указать описание конфигурируемого сервера (необязательно).	**esr(config-pptp-server)# description <DESCRIPTION>**	<DESCRIPTION> – описание PPTP-сервера, задаётся строкой до 255 символов.
3	Указать IP-адрес, который должен обрабатывать PPTP-сервер.	**esr(config-pptp-server)# outside-address { object-group <OBJ-GROUP-NETWORK-NAME> | ip-address <ADDR> | interface { <IF> | <TUN> } }**	<OBJ-GROUP-NETWORK-NAME> – имя профиля, содержащего IP-адрес, который должен слушать PPTP-сервер, задаётся строкой до 31 символа; <ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IF> – тип и идентификатор интерфейса маршрутизатора; <TUN> – тип и номер туннеля маршрутизатора.

Шаг	Описание	Команда	Ключи
4	Указать IP-адрес локального шлюза.	**esr(config-pptp-server)# local-address { object-group <OBJ-GROUP-NETWORK-NAME > | ip-address <ADDR> }**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит IP-адрес локального шлюза, задаётся строкой до 31 символа; <ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
5	Указать список IP-адресов, из которого PPTP выдаются динамические IP-адреса удаленным пользователям.	**esr(config-pptp-server)# remote-address { object-group <OBJ-GROUP-NETWORK-NAME > | address-range <FROM-ADDR>-<TO-ADDR> }**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит список IP-адресов удаленных пользователей, задаётся строкой до 31 символа; <FROM-ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <TO-ADDR> – конечный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
6	Выбрать режим аутентификации PPTP-клиентов.	**esr(config-pptp-server)# authentication mode { local | radius }**	• local – аутентификация пользователя по локальной базе. • radius – аутентификация пользователя по базе RADIUS-сервера. На маршрутизаторе должен быть сконфигурирован механизм взаимодействия с RADIUS-сервером см. раздел Алгоритм настройки AAA по протоколу RADIUS.
7	Разрешить необходимые методы аутентификации удаленных пользователей.	**esr(config-pptp-server)# authentication method <METHOD>**	<METHOD> – метод аутентификации, принимает значения [chap, mschap, mschap-v2, eap, pap]. По умолчанию разрешен только chap.

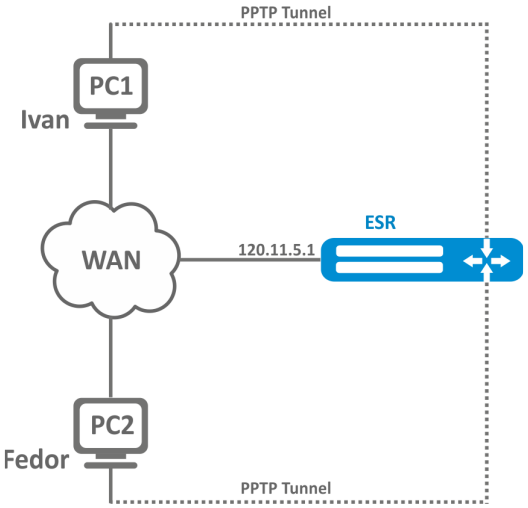
Шаг	Описание	Команда	Ключи
8	Указать имя пользователя (при использовании локальной аутентификации пользователей).	**esr(config-pptp-server) username < NAME >**	<NAME> – имя пользователя, задаётся строкой до 12 символов.
9	Указать пароль пользователя (при использовании локальной аутентификации пользователей).	**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 (необязательно).	**esr(config-pptp-server)# dscp <DSCP>**	<DSCP>– dscp-приоритет исходящих пакетов [0..63].
14	Включить шифрование MPPE для PPTP-соединений (необязательно).	**esr(config-pptp-server)# encryption mppe**	
15	Указать размер MTU (MaximumTransmitionUnit) для сервера (не обязательно). MTU более 1500 будет активно только в случае применения команды "system jumbo-frames".	**esr(config-pptp-server) mtu <MTU>**	<MTU> – значение MTU, принимает значения в диапазоне [1280..1500]. Значение по умолчанию: 1500.
16	Указать список DNS-серверов, которые будут использовать удаленные пользователи (необязательно).	**esr(config-pptp-server)# dns-servers object-group <OBJ-GROUP-NETWORK -NAME >**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, содержащего адреса необходимых DNS-серверов, задаётся строкой до 31 символа.
17	Указать список WINS-серверов, которые будут использовать удаленные пользователи (необязательно).	**esr(config-pptp-server)# wins-servers object-group <OBJ-GROUP-NETWORK-NAME >**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, содержащего адреса необходимых WINS-серверов, задаётся строкой до 31 символа.

17.1.2 Пример настройки

Задача:

Настроить PPTP-сервер на маршрутизаторе.

- адрес PPTP-сервера – 120.11.5.1;
- шлюз внутри туннеля для подключающихся клиентов – 10.10.10.1;
- пул IP-адресов для выдачи 10.10.10.5-10.10.10.25;
- DNS-серверы: 8.8.8.8, 8.8.8.4;
- учетные записи для подключения – fedor, ivan.



Решение:

Создадим профиль адресов, содержащий адрес, который должен слушать сервер:

```
esr# configure
esr(config)# object-group network pptp_outside
esr(config-object-group-network)# ip address-range 120.11.5.1
esr(config-object-group-network)# exit
```

Создадим профиль адресов, содержащий адрес локального шлюза:

```
esr(config)# object-group network pptp_local
esr(config-object-group-network)# ip address-range 10.10.10.1
esr(config-object-group-network)# exit
```

Создадим профиль адресов, содержащий адреса клиентов:

```
esr(config)# object-group network pptp_remote
esr(config-object-group-network)# ip address-range 10.10.10.5-10.10.10.25
esr(config-object-group-network)# exit
```

Создадим профиль адресов, содержащий адреса, которые будут использовать удаленные пользователи:

```
esr(config)# object-group network pptp_dns
esr(config-object-group-network)# ip address-range 8.8.8.8,8.8.8.4
esr(config-object-group-network)# exit
```

Создадим PPTP-сервер и привяжем вышеуказанные профили:

```
esr(config)# remote-access pptp remote-workers
esr(config-pptp)# local-address object-group pptp_local
esr(config-pptp)# remote-address object-group pptp_remote
esr(config-pptp)# outside-address object-group pptp_outside
esr(config-pptp)# dns-servers object-group pptp_dns
```

Выберем метод аутентификации пользователей PPTP-сервера:

```
esr(config-pptp)# authentication mode local
```

Укажем зону безопасности, к которой будут относиться сессии пользователей:

```
esr(config-pptp)# security-zone VPN
```

Создадим PPTP-пользователей *Ivan* и *Fedor* для PPTP-сервера:

```
esr(config-pptp)# username ivan
esr(config-pptp-user)# password ascii-text password1
esr(config-pptp-user)# enable
esr(config-pptp-user)# exit
esr(config-pptp)# username fedor
esr(config-pptp-user)# password ascii-text password2
esr(config-pptp-user)# enable
esr(config-pptp-user)# exit
esr(config-pptp)# exit
```

Включим PPTP-сервер:

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

После применения конфигурации маршрутизатор будет прослушивать 120.11.5.1:1723. Состояние сессий PPTP-сервера можно посмотреть командой:

```
esr# show remote-access status pptp server remote-workers
```

Счетчики сессий PPTP-сервера можно посмотреть командой:

```
esr# show remote-access counters pptp server remote-workers
```

Очистить счетчики сессий PPTP-сервера можно командой:

```
esr# clear remote-access counters pptp server remote-workers
```

Завершить сессию пользователя fedor PPTP-сервера можно одной из следующих команд:

```
esr# clear remote-access session pptp username fedor
esr# clear remote-access session pptp server remote-workers username fedor
```

Конфигурацию PPTP-сервера можно посмотреть командой:

```
esr# show remote-access configuration pptp remote-workers
```

⚠ Помимо создания PPTP-сервера необходимо в firewall открыть TCP-порт 1723 для обслуживания соединений и разрешить протокол GRE(47) для туннельного трафика.

17.2 Настройка сервера удаленного доступа к корпоративной сети по L2TP over IPsec протоколу

L2TP (англ. Layer 2 Tunneling Protocol – протокол туннелирования второго уровня) – туннельный протокол, использующийся для поддержки виртуальных частных сетей. L2TP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например, Интернет. L2TP может также использоваться для организации туннеля между двумя локальными сетями. L2TP использует дополнительное UDP-соединение для обслуживания туннеля. L2TP-протокол не предоставляет средств шифрования данных и поэтому он обычно используется в связке с группой протоколов IPsec, которая предоставляет безопасность на пакетном уровне.

17.2.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать профиль L2TP-сервера.	**esr(config)# remote-access l2tp <NAME>**	<NAME> – имя профиля L2TP-сервера, задаётся строкой до 31 символа.
2	Указать описание конфигурируемого сервера (необязательно).	**esr(config-l2tp-server)# description <DESCRIPTION>**	<DESCRIPTION> – описание L2TP-сервера, задаётся строкой до 255 символов.

Шаг	Описание	Команда	Ключи
3	Указать IP-адрес, который должен слушать L2TP-сервер.	**esr(config-l2tp-server)# outside-address { object-group <NAME> | ip-address <ADDR> | interface { <IF> | <TUN> } }**	<OBJ-GROUP-NETWORK-NAME> – имя профиля содержащего IP-адрес, который должен слушать L2TP-сервер, задаётся строкой до 31 символа; <ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IF> – тип и идентификатор интерфейса маршрутизатора; <TUN> – тип и номер туннеля маршрутизатора.
4	Указать IP-адрес локального шлюза либо отключить firewall для PPTP-сервера.	**esr(config-l2tp-server)# local-address { object-group <OBJ-GROUP-NETWORK -NAME> | ip-address <ADDR> }**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит IP-адрес локального шлюза, задаётся строкой до 31 символа; <ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
5	Указать список IP-адресов из которого L2TP выдаются динамические IP-адреса удаленным пользователям.	**esr(config-l2tp-server)# remote-address { object-group <OBJ-GROUP-NETWORK -NAME > | address-range <FROM-ADDR>-<TO-ADDR> }**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит список IP-адресов удаленных пользователей, задаётся строкой до 31 символа; <FROM-ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <TO-ADDR> – конечный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Шаг	Описание	Команда	Ключи
6	Выбрать режим аутентификации L2TP-клиентов.	**esr(config-l2tp-server)# authentication mode { local | radius }**	• local – аутентификация пользователя по локальной базе. • radius – аутентификация пользователя по базе RADIUS-сервера. На маршрутизаторе должен быть сконфигурирован механизм взаимодействия с RADIUS-сервером см. раздел Алгоритм настройки AAA по протоколу RADIUS.
7	Разрешить необходимые методы аутентификации удаленных пользователей.	**esr(config-l2tp-server)# authentication method <METHOD>**	<METHOD> – метод аутентификации, принимает значения [chap, mschap, mschap-v2, eap, pap]. По умолчанию разрешен только chap.
8	Включить L2TP-сервер в зону безопасности и настроить правила взаимодействия между зонами (см. раздел Конфигурирование Firewall).	**esr(config-l2tp-server)# security-zone <NAME>**	<NAME> – имя зоны безопасности, задаётся строкой до 31 символа.
9	Указать имя пользователя (при использовании локальной базы аутентификации).	**esr(config-l2tp-server) username < NAME >**	<NAME> – имя пользователя, задаётся строкой до 12 символов.
10	Указать пароль пользователя (при использовании локальной базы аутентификации).	**esr(config-l2tp-user) password ascii-text { <PASSWORD> | encrypted <PASSWORD> }**	<PASSWORD> – пароль пользователя, задается строкой до 32 символов.
11	Включить пользователя (при использовании локальной базы аутентификации).	**esr(config-l2tp-user) enable**	
12	Выбрать метод аутентификации по ключу для IKE-соединения (по умолчанию).	**esr(config-l2tp-server)# ipsec authentication method pre-shared-key**	

Шаг	Описание	Команда	Ключи
13	Указать общий секретный ключ для аутентификации, который должен совпадать у обоих сторон, устанавливающих туннель.	**esr(config-l2tp-server)# ipsec authentication pre-shared-key { ascii-text { <TEXT> | encrypted <ENCRYPTED-TEXT> } | hexadecimal {<HEX> | encrypted <ENCRYPTED-HEX> } }**	<TEXT> – строка [1..64] ASCII-символов; <HEX> – число размером [1..32] байт задаётся строкой [2..128] символов в шестнадцатеричном формате (0xYYYY...) или (YYYY...). <ENCRYPTED-TEXT> – зашифрованный пароль размером [1..32] байт, задаётся строкой [2..128] символов; <ENCRYPTED-HEX> – зашифрованное число размером [2..64] байт, задаётся строкой [2..256] символов.
14	Ограничить используемые методы аутентификации и шифрования протокола ike (необязательно).	**esr(config-l2tp-server)# ipsec ike proposal <NAME>**	<NAME> – имя ранее созданного профиля протокола IKE, задаётся строкой до 31 символа.
15	Ограничить используемые методы аутентификации и шифрования протокола ipsec (необязательно).	**esr(config-l2tp-server)# ipsec proposal <NAME>**	<NAME> – имя ранее созданного профиля IPsec, задаётся строкой до 31 символа.
16	Включить сервер.	**esr(config-l2tp-server)# enable**	
17	Указать DSCP-приоритет исходящих пакетов.	**esr(config-l2tp-server)# dscp <DSCP>**	<DSCP> – DSCP-приоритет исходящих пакетов [0..63].
18	Указать размер MTU (MaximumTransmitionUnit) для сервера (необязательно). MTU более 1500 будет активно только в случае применения команды "system jumbo-frames".	**esr(config-l2tp-server) mtu <MTU>**	<MTU> – значение MTU, принимает значения в диапазоне [1280..1500]. Значение по умолчанию: 1500.
19	Указать список DNS-серверов, которые будут использовать удаленные пользователи (необязательно).	**esr(config-l2tp-server)# dns-servers object-group <OBJ-GROUP-NETWORK -NAME >**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, содержащего, который содержит адреса необходимых DNS-серверов, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
20	Указать список WINS-серверов, которые будут использовать удаленные пользователи (необязательно).	**esr(config-l2tp-server)# wins-servers object-group <OBJ-GROUP-NETWORK -NAME >**	<OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, который содержит адреса необходимых WINS-серверов, задаётся строкой до 31 символа.

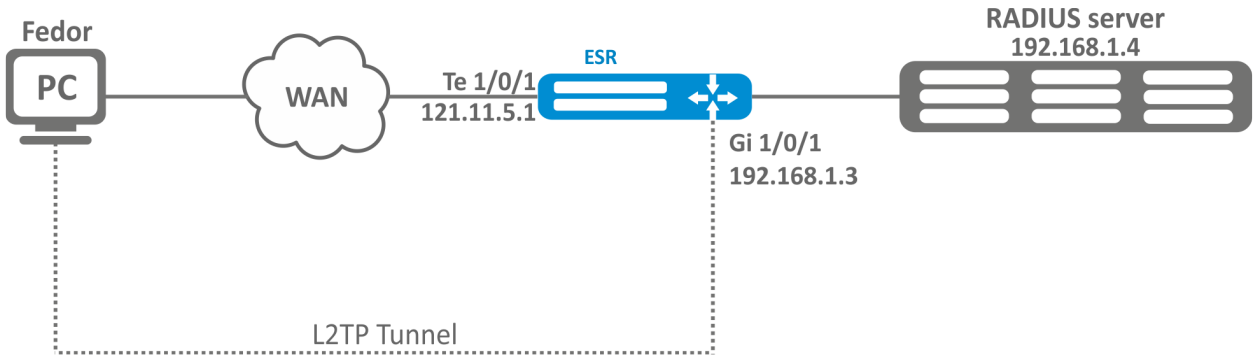
17.2.2 Пример настройки

Задача:

Настроить L2TP-сервер на маршрутизаторе для подключения удаленных пользователей к ЛВС. Аутентификация пользователей проходит на RADIUS-сервере.

- адрес L2TP-сервера – 120.11.5.1;
- шлюз внутри туннеля – 10.10.10.1;
- адрес RADIUS-сервера – 192.168.1.4.

Для IPsec используется метод аутентификации по ключу: ключ — «password».



Решение:

Предварительно нужно выполнить следующие действия:

- Настроить подключение к RADIUS-серверу;
- Настроить зоны для интерфейсов te1/0/1 и gi1/0/1;
- Указать IP-адреса для интерфейсов te1/0/1 и te1/0/1.

Создадим профиль адресов, содержащий адрес локального шлюза:

```
esr(config)# object-group network l2tp_local
esr(config-object-group-network)# ip address-range 10.10.10.1
esr(config-object-group-network)# exit
```

Создадим профиль адресов, содержащий DNS-серверы:

```
esr(config)# object-group network pptp_dns
esr(config-object-group-network)# ip address-range 8.8.8.8
esr(config-object-group-network)# ip address-range 8.8.4.4
esr(config-object-group-network)# exit
```

Создадим L2TP-сервер и привяжем к нему вышеуказанные профили:

```
esr(config)# remote-access l2tp remote-workers
esr(config-l2tp)# local-address ip-address 10.10.10.1
esr(config-l2tp)# outside-address ip-address 120.11.5.1
esr(config-l2tp)# dns-server object-group l2tp_dns
```

Выберем метод аутентификации пользователей L2TP-сервера:

```
esr(config-l2tp)# authentication mode radius
```

Укажем зону безопасности, к которой будут относиться сессии пользователей:

```
esr(config-l2tp)# security-zone VPN
```

Выберем метод аутентификации первой фазы IKE и зададим ключ аутентификации:

```
esr(config-l2tp)# ipsec authentication method psk
esr(config-l2tp)# ipsec authentication pre-shared-key ascii-text password
```

Включим L2TP-сервер:

```
esr(config-l2tp)# enable
```

После применения конфигурации маршрутизатор будет прослушивать IP-адрес 120.11.5.1 и порт 1701.
Состояние сессий L2TP-сервера можно посмотреть командой:

```
esr# show remote-access status l2tp server remote-workers
```

Счетчики сессий L2TP-сервера можно посмотреть командой:

```
esr# show remote-access counters l2tp server remote-workers
```

Очистить счетчики сессий L2TP-сервера можно командой:

```
esr# clear remote-access counters l2tp server remote-workers
```

Завершить сессию пользователя fedor L2TP-сервера можно одной из следующих команд:

```
esr# clear remote-access session l2tp username fedor
esr# clear remote-access session l2tp server remote-workers username fedor
```

Конфигурацию L2TP-сервера можно посмотреть командой:

```
esr# show remote-access configuration l2tp remote-workers
```

⚠ Помимо создания L2TP-сервера необходимо в firewall открыть UDP-порты 500, 1701, 4500 для обслуживания соединений и разрешить протоколы ESP (50) и GRE (47) для туннельного трафика.

17.3 Настройка сервера удаленного доступа к корпоративной сети по OpenVPN-протоколу

OpenVPN — полнофункциональное средство для построения виртуальных частных сетей (Virtual Private Networks, VPN), организации удалённого доступа и решения ряда других задач, связанных с безопасностью передачи данных, базирующееся на SSL.

17.3.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать профиль OpenVPN-сервера.	**esr(config)# remote-access openvpn <NAME>**	<NAME> – имя профиля OpenVPN-сервера, задаётся строкой до 31 символа.
2	Указать описание конфигурируемого сервера (необязательно).	**esr(config-openvpn-server)# description <DESCRIPTION>**	<DESCRIPTION> – описание OpenVPN-сервера, задаётся строкой до 255 символов.
3	Указать подсеть, из которой выдаются IP-адреса пользователям (только для tunnel ip).	**esr(config-openvpn-server)# network <ADDR/LEN>**	<ADDR/LEN> – адрес подсети, имеет следующий формат: AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [16..29].
4	Указать инкапсулируемый протокол.	**esr(config-openvpn-server)# protocol <PROTOCOL>**	<PROTOCOL> – тип инкапсуляции, возможные значения: • TCP-инкапсуляция в TCP-сегменты; • UDP-инкапсуляция в UDP-дейтаграммы.
5	Определить тип соединения с частной сетью через OpenVPN-сервер.	**esr(config-openvpn-server)# tunnel <TYPE>**	<TYPE> – инкапсулирующий протокол, принимает значения: • ip – соединение точка-точка; • ethernet – подключение к L2-домену.

Шаг	Описание	Команда	Ключи
6	Указать список IP-адресов, из которого OpenVPN-сервером выдаются динамические IP-адреса удаленным пользователям в режиме L2 (только для tunnel ethernet).	**esr(config-openvpn-server)# address-range <FROM-ADDR>-<TO-ADDR>**	<FROM-ADDR> – начальный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <TO-ADDR> – конечный IP-адрес диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
7	Включить клиентские соединения по OpenVPN в L2-домен (только для tunnel ethernet).	**esr(config-openvpn-server)# bridge-group <BRIDGE-ID>**	<BRIDGE-ID> – идентификационный номер моста.
8	Указать сертификаты и ключи.	**esr(config-openvpn-server)# crypto <CERTIFICATE-TYPE> <NAME>**	<CERTIFICATE-TYPE> – тип сертификата или ключа, может принимать следующие значения: • ca – сертификат удостоверяющего сервера; • crl – список отозванных сертификатов; • dh – ключ Диффи-Хеллмана; • cert – публичный сертификат сервера; • private-key – приватный ключ сервера; • ta – HMAC-ключ. <NAME> – имя сертификата или ключа, задаётся строкой до 31 символа.
9	Указать контейнер PKCS12 (необязательно.) **Примечание**: контейнер обязательно должен включать в себя сертификат удостоверяющего центра, публичный сертификат сервера и приватный ключ сервера. Применение сертификатов или контейнера является взаимоисключающим, т. е. необходимо указывать или сертификаты, или контейнер.	**esr(config-openvpn-server)# crypto pfx <NAME> [password ascii-text <PASSWORD>]**	<NAME> – имя PKCS12-контейнера, задаётся строкой до 31 символа. <PASSWORD> – пароль от PKCS12-контейнера.

Шаг	Описание	Команда	Ключи
10	Выбрать алгоритм шифрования, используемый при передачи данных.	**esr(config-openvpn-server)# encryption algorithm <ALGORITHM>**	<ALGORITHM> – идентификатор протокола шифрования, принимает значения: 3des,blowfish128, aes128.
11	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.
12	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.
13	Определить подсеть для указанного пользователя OpenVPN-сервера.	**esr(config-openvpn-user)# subnet <ADDR/LEN>**	<ADDR/LEN> – адрес подсети, имеет следующий формат: AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [16..32].
14	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].
15	Включить профиль OpenVPN-сервера.	**esr(config-openvpn-server)# enable**	
16	Включить блокировку передачи данных между клиентами (необязательно).	**esr(config-openvpn-server)# client-isolation**	
17	Устанавливается максимальное количество одновременных пользовательских сессий (необязательно).	**esr(config-openvpn-server)# client-max <VALUE>**	<VALUE> – максимальное количество пользователей, принимает значения [1..65535].
18	Включается механизм сжатия передаваемых данных между клиентами и сервером OpenVPN (необязательно).	**esr(config-openvpn-server)# compression**	

Шаг	Описание	Команда	Ключи
19	Указать список DNS-серверов, которые будут использовать удаленные пользователи (необязательно).	**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];
20	Указать TCP-/UDP-порт, который будет прослушиваться OpenVPN-сервером (необязательно).	**esr(config-openvpn-server)# port <PORT>**	<PORT> – TCP-/UDP-порт, принимает значения [1..65535]. Значение по умолчанию: 1194.
21	Включить анонсирование маршрута по умолчанию для OpenVPN-соединений, что приводит к замене маршрута по умолчанию на клиентской стороне (необязательно).	**esr(config-openvpn-server)# redirect-gateway**	
22	Включить анонсирование указанных подсетей, шлюзом является IP-адрес OpenVPN-сервера (необязательно).	**esr(config-openvpn-server)# route <ADDR/LEN>**	<ADDR/LEN> – адрес подсети, имеет следующий формат: AAA.BBB.CCC.DDD/EE – IP-адрес подсети с маской в форме префикса, где AAA-DDD принимают значения [0..255] и EE принимает значения [1..32].
23	Указать временной интервал, по истечению которого встречная сторона считается недоступной (необязательно).	**esr(config-openvpn-server)# timers holdtime <TIME>**	<TIME> – время в секундах, принимает значения [2..65535]. Значение по умолчанию: 120.
24	Указать временной интервал, по истечению которого идет проверка соединения со встречной стороной (необязательно).	**esr(config-openvpn-server)# timers keepalive <TIME>**	<TIME> – время в секундах, принимает значения [1..65535]. Значение по умолчанию: 10.
25	Разрешить подключаться к OpenVPN-серверу нескольким пользователям с одним сертификатом.	**esr(config-openvpn-server)# duplicate-cn**	
26	Указать список WINS-серверов, которые будут использовать удаленные пользователи (необязательно).	**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].

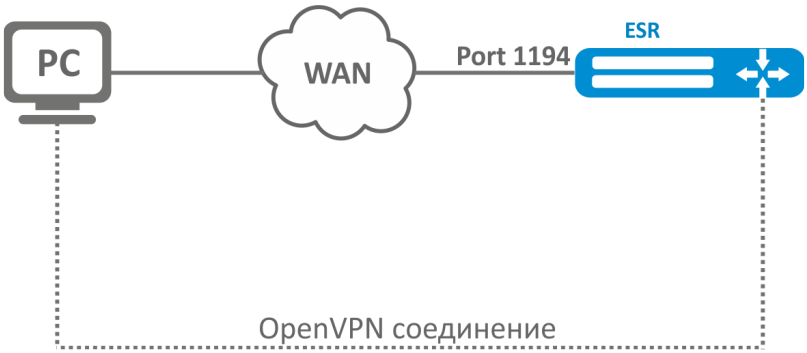
Шаг	Описание	Команда	Ключи
27	Изменить алгоритм аутентификации OpenVPN-клиентов (необязательно).	**esr(config-openvpn-server)# authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм аутентификации: • 8-128 bits key size: md4, rsa-md4, md5, rsa-md5, mdc2, rsa-mdc2 • 8-160 bits key size: sha, sha1, rsa-sha, rsa-sha1, rsa-sha1-2, dsa, dsa-sha, dsa-sha1, dsa-sha1-old, ripemd160, rsa-ripemd160, ecdsa-with-sha1 • 8-224 bits key size: sha-224, rsa-sha-224 • 8-256 bits key size: sha-256, rsa-sha-256 • 8-384 bits key size: sha-384, rsa-sha-384 • 8-512 bits key size: sha-512, rsa-sha-512, whirlpool Значение по умолчанию: sha.

17.3.2 Пример настройки

Задача:

Настроить OpenVPN-сервер в режиме L3 на маршрутизаторе для подключения удаленных пользователей к ЛВС.

- подсеть OpenVPN-сервера – 10.10.100.0/24;
- режим – L3;
- аутентификация на основе сертификатов.



Решение:

Предварительно нужно выполнить следующие действия:

- Подготовить сертификаты и ключи:
  - Сертификат Удостоверяющего Центра (CA),
  - Ключ и сертификат для OpenVPN-сервера,

- Ключ Диффи-Хэллмана и HMAC для TLS.

  ИЛИ

- Контейнер PKSC12, содержащий в себе сертификат Удостоверяющего Центра (CA) и ключ и сертификат для OpenVPN-туннеля.

- 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 crypto:cert/ca.crt
esr# copy tftp://192.168.16.10:/dh.pem crypto:dh/dh.pem
esr# copy tftp://192.168.16.10:/server.key crypto:private-key/server.key
esr# copy tftp://192.168.16.10:/server.crt crypto:cert/server.crt
esr# copy tftp://192.168.16.10:/ta.key crypto:ta/ta.key
```

Или импортируем PKCS12-контейнер:

```
esr# copy tftp://192.168.0.1:/container.p12 crypto:pfx/cont.p12
```

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-openvpn)# route 10.10.0.0/20
esr(config-openvpn)# dns-server 10.10.1.1
```

Укажем ранее импортированные сертификаты и ключи, которые будут использоваться OpenVPN-сервером:

```
esr(config-openvpn)# crypto ca ca.crt
esr(config-openvpn)# crypto dh dh.pem
esr(config-openvpn)# crypto private-key server.key
esr(config-openvpn)# crypto cert server.crt
esr(config-openvpn)# crypto ta ta.key
```

Или укажем импортированный контейнер, DH и TA ключи указываются:

```
esr(config-openvpn)# crypto dh dh.pem
esr(config-openvpn)# crypto ta ta.key
esr(config-openvpn)# crypto pfx pfx.p12
```

Укажем зону безопасности, к которой будут относиться сессии пользователей:

```
esr(config-openvpn)# security-zone VPN
```

Выберем алгоритм шифрования aes128:

```
esr(config-openvpn)# encryption algorithm aes128
```

Включим OpenVPN-сервер:

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

После применения конфигурации маршрутизатор будет прослушивать порт 1194 (используется по умолчанию).

Состояние сессий OpenVPN-сервера можно посмотреть командой:

```
esr# show remote-access status openvpn server AP
```

Счетчики сессий OpenVPN-сервера можно посмотреть командой:

```
esr# show remote-access counters openvpn server AP
```

Очистить счетчики сессий OpenVPN-сервера можно командой:

```
esr# clear remote-access counters openvpn server AP
```

Завершить сессию пользователя fedor OpenVPN-сервера можно одной из следующих команд:

```
esr# clear remote-access session openvpn username fedor
esr# clear remote-access session openvpn server AP username fedor
```

Конфигурацию OpenVPN-сервера можно посмотреть командой:

```
esr# show remote-access configuration openvpn AP
```

⚠ Помимо создания OpenVPN-сервера необходимо в firewall открыть TCP-порт 1194.

17.4 Настройка сервера удаленного доступа к корпоративной сети по WireGuard-протоколу

WireGuard – простой, быстрый и современный VPN, использующий современную криптографию (ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24, HKDF). WireGuard надежно инкапсулирует IP-пакеты поверх UDP. В основе WireGuard лежит концепция под названием «Маршрутизация криптоключей», которая работает путем связывания открытых ключей со списком IP-адресов туннеля, разрешенным находиться внутри туннеля. Каждый сетевой интерфейс имеет закрытый ключ и список пиров. У каждого узла есть открытый ключ. Открытые ключи короткие и простые и используются узлами для аутентификации друг друга. Их можно передавать для использования в файлах конфигурации

любым внешним методом аналогично тому, как можно отправить открытый ключ SSH для доступа к серверу.

17.4.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать профиль WireGuard-сервера.	**esr(config)# remote-access wireguard <NAME>**	<NAME> – имя профиля WireGuard-сервера, задаётся строкой до 31 символа.
2	Указать описание конфигурируемого сервера (необязательно).	**esr(config-wireguard-server)# description <DESCRIPTION>**	<DESCRIPTION> – описание WireGuard-сервера, задаётся строкой до 255 символов.
3	Определить статический IP-адрес конфигурируемого сервера.	**esr(config-wireguard-server)# local-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].
4	Указать UDP-порт, который будет прослушиваться WireGuard-сервером (необязательно).	**esr(config-wireguard-server)# port <PORT>**	<PORT> – UDP-порт, принимает значения [1..65535].
5	Отключить функции Firewall или включить WireGuard-сервер в зону безопасности и настроить правила взаимодействия между зонами (см. раздел Конфигурирование Firewall).	**esr(config-wireguard-server)# ip firewall disable**	
		esr(config-wireguard-server)# security-zone <NAME>	<NAME> – имя зоны безопасности, задаётся строкой до 31 символа.
6	Задать MTU (необязательно).	**esr(config-wireguard-server)# mtu <MTU>**	<MTU> – 552–10000. Значение по умолчанию: 1500.
7	Указать приватный ключ WireGuard-сервера.	**esr(config-wireguard-server)# private-key <NAME>**	<NAME> – имя приватного ключа, задаётся строкой до 31 символа.
8	Включить профиль WireGuard-сервера.	**esr(config-wireguard-server)# enable**	
9	Перейти к настройке разрешённых туннелей WireGuard-сервера.	**esr(config-wireguard-server)# peer <COUNT>**	<COUNT> – номер соответствующего пира, принимает значения [1..16].
10	Указать описание туннеля (необязательно).	**esr(config-wireguard-server-peer)# description <DESCRITPION>**	<DESCRIPTION> – описание WireGuard-сервера, задаётся строкой до 255 символов.

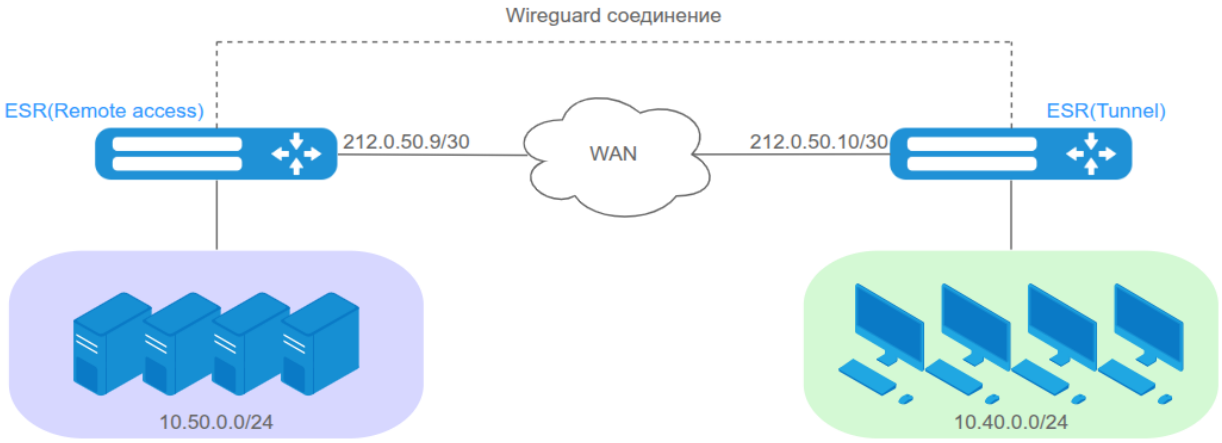
Шаг	Описание	Команда	Ключи
11	Указать публичный ключ туннеля.	**esr(config-wireguard-server-peer)# public-key <NAME>**	<NAME> – имя публичного ключа, задаётся строкой до 31 символа.
12	Указать pre-shared-key для настраиваемого туннеля (необязательно).	**esr(config-wireguard-server-peer)# pre-shared-key <TYPE> <WORD>**	<TYPE> – тип аргумента, устанавливаемый в качестве симметричного ключа: • **ascii-text** – указать симметричный ключ в виде ASCII-текста, который будет сконвертирован в формат Base64; • **base64** – указать симметричный ключ в формате Base64; • **encrypted** – указать симметричный ключ в зашифрованном виде. <WORD> – вводимый симметричный ключ. В зависимости от типа аргумента имеет длину 32 символа для ascii-text, 44 символа для формата base64 и 64 символа для зашифрованного вида.
13	Указать список IP-адресов, которым будет разрешено находиться внутри туннеля.	**esr(config-wireguard-server-peer)# access-addresses <TYPE> {<FROM-ADDR> - <TO-ADDR> | <OBJ-GROUP-NETWORK-NAME> | <ADDR/LEN>}**	<TYPE> – тип аргумента, устанавливаемый в качестве адреса: • **address-range** – указать диапазон IPv4-адресов; • **object-group** – указать имя профиля; • **prefix** – указать адрес подсети и префикс. <FROM-ADDR> – начальный IP-адрес диапазона; <TO-ADDR> – конечный IP-адрес диапазона; <OBJ-GROUP-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа; <ADDR/LEN> – IP-адрес и маска подсети.
14	Включить туннель.	**esr(config-wireguard-server-peer)# enable**	

17.4.2 Пример настройки

Задача:

Настроить WireGuard-сервер на маршрутизаторе для подключения удаленных пользователей к серверам организации.

- адресация внутри туннеля – 110.0.0.0/30;
- порт подключения к серверу – 43020;
- адрес WireGuard-сервера внутри туннеля – 110.0.0.1.



Решение:

Создадим ключевую пару x25519, которая будет использоваться в работе WireGuard:

```
esr# crypto generate private-key x25519 filename wg_server_private.key
esr# crypto generate public-key x25519 private-key wg_server_private.key filename
wg_server_public.key
```

Для успешной работы необходимо совершить обмен открытыми криптографическими ключами с удаленной стороной любым удобным способом. На данном этапе настройки открытым криптографическим ключом является файл с именем **wg_server_public.key**, который хранится в **crypto:public-key**:

```
esr# show crypto certificates public-key
File name
------------------------------------------------------------------------------------------------
---------------
wg_server_public.key
```

Создадим object-group network со списком IP-адресов, которым будет разрешено прохождение через туннель:

```
esr(config)# object-group network WG_CLIENTS
esr(config-object-group-network)# ip address-range 10.40.0.10-10.40.0.20
```

Создадим профиль WireGuard-сервера, зададим локальный адрес сервера, порт для прослушивания и выставим MTU:

```
esr(config)# remote-access wireguard WG
esr(config-wireguard-server)# local-address 110.0.0.1/30
esr(config-wireguard-server)# port 43020
esr(config-wireguard-server)# mtu 1420
```

Укажем приватный ключ сервера и отключим Firewall:

```
esr(config-wireguard-server)# private-key wg_server_private.key
esr(config-wireguard-server)# ip firewall disable
```

Перейдём в настройки разрешённого туннеля, укажем связку публичного ключа клиента и разрешённого IP-адреса:

```
esr(config-wireguard-server)# peer 1
esr(config-wireguard-server-peer)# public-key wg_client_public.key
esr(config-wireguard-server-peer)# access-addresses object-group WG_CLIENTS
```

Для усиления криптостойкости установим заранее известный симметричный ключ:

```
esr(config-wireguard-server-peer)# pre-shared-key base64
r4u48oYTouJ+j1GrAtVWRIZqlQ2YLjEZEvc+Yttc6R4=
```

Включим туннель и WireGuard-сервер:

```
esr(config-wireguard-server-peer)# enable
esr(config-wireguard-server-peer)# exit
esr(config-wireguard-server)# enable
```

После применения конфигурации маршрутизатор будет прослушивать порт 43020.

Счётчики сессий WireGuard-сервера можно посмотреть командой:

```
esr# show remote-access counters wireguard server WG
```

Очистить счётчики сессий WireGuard-сервера можно командой:

```
esr# clear remote-access counters wireguard server WG
```

Конфигурацию WireGuard-сервера можно посмотреть командой:

```
esr# show remote-access configuration wireguard WG
```

17.4.3 Пример настройки правил Firewall для совместной работы с WireGuard-сервером

Задача:

Настроить правила Firewall таким образом, чтобы разрешить обращения клиентов на 80 порт сервера 10.50.0.10, остальное взаимодействие запретить.

Решение:

Создадим зоны безопасности WAN, SERVERS, WIREGUARD и назначим их на соответствующие интерфейсы и включим Firewall:

```
esr(config)# security zone WAN
esr(config-security-zone)# exit
esr(config)# security zone SERVERS
esr(config-security-zone)# exit
esr(config)# security zone WIREGUARD
esr(config-security-zone)# exit
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# security-zone WAN
esr(config-if-gi)# no ip firewall disable
esr(config-if-gi)# exit
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# security-zone SERVERS
esr(config-if-gi)# no ip firewall disable
esr(config-if-gi)# exit
esr(config)# remote-access wireguard WG
esr(config-wireguard-server)# security-zone WIREGUARD
esr(config-wireguard-server)# no ip firewall disable
esr(config-wireguard-server)# exit
```

Создадим правила, разрешающие работу WireGuard:

```
esr(config)# security zone-pair WAN self
esr(config-security-zone-pair)# rule 10
esr(config-security-zone-pair-rule)# description "Permit wireguard-traffic"
esr(config-security-zone-pair-rule)# action permit
esr(config-security-zone-pair-rule)# match protocol udp
esr(config-security-zone-pair-rule)# match destination-port port-range 43020
esr(config-security-zone-pair-rule)# enable
esr(config-security-zone-pair-rule)# exit
esr(config-security-zone-pair)# rule 100
esr(config-security-zone-pair-rule)# action deny
esr(config-security-zone-pair-rule)# enable
esr(config-security-zone-pair-rule)# exit
esr(config-security-zone-pair)# exit
```

Создадим правила, разрешающие обращения на 80 порт сервера 10.50.0.10 из туннеля WireGuard:

```
esr(config)# security zone-pair WIREGUARD SERVERS
esr(config-security-zone-pair)# rule 10
esr(config-security-zone-pair-rule)# action permit
esr(config-security-zone-pair-rule)# match protocol tcp
esr(config-security-zone-pair-rule)# match destination-address address-range 10.50.0.10
esr(config-security-zone-pair-rule)# match destination-port port-range 80
esr(config-security-zone-pair-rule)# enable
esr(config-security-zone-pair-rule)# exit
esr(config-security-zone-pair)# rule 100
esr(config-security-zone-pair-rule)# action deny
esr(config-security-zone-pair-rule)# enable
esr(config-security-zone-pair-rule)# exit
esr(config-security-zone-pair)# exit
```

Проверим работоспособность:

```
esr@client:~$ ping 10.50.0.10 -c 4
PING 10.50.0.10 (10.50.0.10) 56(84) bytes of data.

--- 10.50.0.10 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3090ms


esr@client:~$ hping3 10.50.0.10 -c 4 -S -p 80
HPING 10.50.0.10 (ens3 10.50.0.10): S set, 40 headers + 0 data bytes
len=46 ip=10.50.0.10 ttl=62 DF id=0 sport=80 flags=RA seq=0 win=0 rtt=2.0 ms
len=46 ip=10.50.0.10 ttl=62 DF id=0 sport=80 flags=RA seq=1 win=0 rtt=2.8 ms
len=46 ip=10.50.0.10 ttl=62 DF id=0 sport=80 flags=RA seq=2 win=0 rtt=2.6 ms
len=46 ip=10.50.0.10 ttl=62 DF id=0 sport=80 flags=RA seq=3 win=0 rtt=2.3 ms

--- 10.50.0.10 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 2.0/2.4/2.8 ms
```

17.5 Настройка клиента удаленного доступа по протоколу PPPoE

PPPoE – это туннелирующий протокол (tunneling protocol), который позволяет инкапсулировать IP PPP через соединения Ethernet и обладает программными возможностями PPP-соединений, что позволяет использовать его для виртуальных соединений на соседнюю Ethernet-машину и устанавливать соединение точка-точка, которое используется для транспортировки IP-пакетов, а также работает с возможностями PPP. Это позволяет применять традиционное PPP-ориентированное ПО для настройки соединения, которое использует не последовательный канал, а пакетно-ориентированную сеть (например, Ethernet), чтобы организовать классическое соединение с логином и паролем для Интернет-соединений. Кроме того, IP-адрес по другую сторону соединения назначается, только когда PPPoE-соединение открыто, позволяя динамическое переиспользование IP-адресов.

17.5.1 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 (необязательно).	**esr(config-pppoe)# description <DESCRIPTION>**	<DESCRIPTION> – описание PPPoE-туннеля, задаётся строкой до 255 символов.
3	Указать имя экземпляра VRF, в котором будут использоваться PPPoE-клиент (необязательно).	**esr(config-pppoe)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.
4	Указать интерфейс, через который будет устанавливаться PPPoE соединение.	**esr(config-pppoe)# interface <IF>**	<IF> – интерфейс или группа интерфейсов.
5	Указать имя пользователя и пароль для подключения к PPPoE-серверу.	**esr(config-pppoe)# username <NAME> password ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<NAME> – имя пользователя, задаётся строкой до 31 символа; <CLEAR-TEXT> – пароль, задаётся строкой [8 .. 64] символов; <ENCRYPTED-TEXT> – зашифрованный пароль, задаётся строкой [16..128] символов.
6	Включить PPPoE-туннель в зону безопасности и настроить правила взаимодействия между зонами (см. раздел Конфигурирование Firewall).	**esr(config-pppoe)# security-zone <NAME>**	<NAME> – имя зоны безопасности, задаётся строкой до 31 символа.
7	Активировать конфигурируемый профиль.	**esr(config-pppoe)# enable**	
8	Указать метод аутентификации (необязательно).	**esr(config-pppoe)# authentication method <METHOD>**	<METHOD> – метод аутентификации, возможные значения: chap, mschap, mschap-v2, eap, pap. Значение по умолчанию: chap.
9	Игнорировать dns-сервер через данный PPoE-туннель (необязательно).	**esr(config-pppoe)# ignore nameserver**	

Шаг	Описание	Команда	Ключи
10	Включить отказ от получения маршрута по умолчанию от PPPoE-сервера (необязательно).	**esr(config-pppoe)# ignore-default-route**	
11	Указать интервал времени, за который усредняется статистика о нагрузке (необязательно).	**esr(config-pppoe)# load-average <TIME>**	<TIME> – интервал времени в секундах от 5 до 150 (по умолчанию 5 с).
12	Указать размер MTU (MaximumTransmitionUnit) для PPPoE-туннеля. MTU более 1500 будет активно только если применена команда **system jumbo-frames** (необязательно).	**esr(config-pppoe)# mtu <MTU>**	<MTU> – значение MTU, принимает значения в диапазоне [552..1500]. Значение по умолчанию: 1500.
13	Изменить количество неудачных data-link тестов перед разрывом сессии (необязательно).	**esr(config-pppoe)# ppp failure-count <NUM>**	<NUM> – количество неудачных data-link тестов, задается в диапазоне [1..100]. Значение по умолчанию: 10.
14	Изменить интервал времени в секундах, по истечении которого маршрутизатор отправляет keepalive-сообщение (необязательно).	**esr(config-pppoe)# ppp timeout keepalive <TIME >**	<TIME> – время в секундах, задается в диапазоне [1..32767]. Значение по умолчанию: 10.
15	Переопределить значение поля MSS (Maximum segment size) во входящих TCP-пакетах (необязательно).	**esr(config-pppoe)# ip tcp adjust-mss <MSS>**	<MSS> – значение MSS, принимает значения в диапазоне [500..1460]. Значение по умолчанию: 1460.
16	Включить запись статистики использования текущего туннеля (необязательно).	**esr(config-pppoe)# history statistics**	

Также для PPPoE-клиента возможно настроить:

- QoS в базовом или расширенном режимах (см. раздел Управление QoS);
- Proxy (см. раздел Проксирование HTTP/HTTPS-трафика);
- Мониторинг траффика (см. разделы Настройка Netflow и Настройка sFlow).

17.5.2 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.

⚠ Интерфейс, с которого будет осуществляться PPPoE-соединение, должен работать в режиме routerport (кроме случаев использования bridge).



Решение:

Предварительно должен быть настроен PPPoE-сервер с соответствующими учетными записями. Также на устройстве должны быть настроены зоны безопасности и описаны правила их взаимодействия.

Зайдем в режим конфигурирования PPPoE-туннеля и зададим пользователя и пароль для подключения к PPPoE-серверу:

```
esr# configure
esr(config)# tunnel pppoe 1
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
```

Настроим зону безопасности,:

```
esr(config-pppoe)# security-zone untrust
```

Опционально для PPPoE-туннеля можно указать следующие параметры:

- Изменить метод аутентификации:

```
esr(config-pppoe)# authentication method
  METHOD  Select PPP authentication method:
                chap
                mschap
                mschap-v2
                eap
                pap
```

- Игнорировать полученный маршрут по умолчанию, выданные PPPoE-сервером:

```
esr(config-pppoe)# ignore-default-route
```

- Переопределить значение поля MSS (Maximum segment size) во входящих TCP-пакетах:

```
esr(config-pppoe)# ip tcp adjust-mss 1452
```

- Указать размер MTU (Maximum Transmition Unit):

```
esr(config-pppoe)# mtu 1496
```

- Изменить количество неудачных data-link тестов перед разрывом сессии:

```
esr(config-pppoe)# ppp failure-count 15
```

- Установить интервал времени в секундах, по истечении которого маршрутизатор отправляет keepalive-сообщение:

```
esr(config-pppoe)# ppp timeout keepalive 15
```

Состояние PPPoE-туннеля можно посмотреть командой:

```
esr# show tunnels status pppoe 1
```

Счетчики входящих и отправленных пакетов PPPoE-туннеля можно посмотреть командой:

```
esr# show tunnels counters pppoe 1
```

Конфигурацию PPPoE-туннеля можно посмотреть командой:

```
esr# show tunnels configuration pppoe 1
```

17.6 Настройка клиента удаленного доступа по протоколу PPTP

PPTP (англ. Point-to-Point Tunneling Protocol) – туннельный протокол типа точка-точка, позволяющий устанавливать защищённое соединение за счёт создания специального туннеля в обычной незащищенной сети. PPTP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например, Интернет. PPTP может также использоваться для организации туннеля между двумя локальными сетями. PPTP использует дополнительное TCP-соединение для обслуживания туннеля.

17.6.1 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 (необязательно).	**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 (необязательно)	**esr(config-pptp)# mtu <MTU>**	<MTU> – значение MTU, принимает значения в диапазоне [552..10000]. Значение по умолчанию: 1500.

Шаг	Описание	Команда	Ключи
7	Указать пользователя и установить пароль в открытой или зашифрованной форме для аутентификации удаленной стороны.	**esr(config-pptp)# username <NAME> password ascii-text { <WORD> | encrypted <HEX> }**	<NAME> – имя пользователя, задается строкой до 31 символа. <WORD> – пароль в открытой форме, задается строкой [8..64] символов, может включать символы [0-9a-fA-F]. <HEX> – пароль в зашифрованной форме, задается строкой [16..128] символов.
8	Активировать туннель.	**esr(config-pptp)# enable**	
9	Переопределить значение поля MSS (Maximum segment size) во входящих TCP-пакетах (необязательно).	**esr(config-pptp)# ip tcp adjust-mss <MSS>**	<MSS> – значение MSS, принимает значения в диапазоне [500..1460]. Значение по умолчанию: 1460.
10	Игнорировать dns-сервер через данный PPTP-туннель (необязательно).	**esr(config-pptp)# ignore nameserver**	
11	Игнорировать маршрут по умолчанию через данный PPTP-туннель (необязательно)	**esr(config-pptp)# ignore-default-route**	
12	Задать интервал времени, за который усредняется статистика о нагрузке на туннель (необязательно).	**esr(config-pptp)# load-average <TIME>**	<TIME> – интервал в секундах, принимает значения [5..150] Значение по умолчанию: 5.
13	Указать метод аутентификации (необязательно).	**esr(config-pptp)# authentication method <METHOD>**	<METHOD> – метод аутентификации, возможные значения: chap, mschap, mschap-v2, eap, pap. Значение по умолчанию: chap.
14	Включить запись статистики использования текущего туннеля (не обязательно).	**esr(config-pptp)# history statistics**	
15	Изменить интервал времени в секундах, по истечении которого маршрутизатор отправляет keepalive-сообщение (необязательно).	**esr(config-pptp)# ppp timeout keepalive <TIME >**	<TIME> – время в секундах, задается в диапазоне [1..32767]. Значение по умолчанию: 10.

Шаг	Описание	Команда	Ключи
16	Изменить количество неудачных data-link тестов перед разрывом сессии (необязательно).	**esr(config-pptp)# ppp failure-count <NUM>**	<NUM> – количество неудачных data-link тестов, задается в диапазоне [1..100]. Значение по умолчанию: 10.

17.6.2 Пример настройки

Задача:

Настроить PPTP-туннель на маршрутизаторе:

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



Решение:

Создадим туннель PPTP:

```
esr(config)# tunnel pptp 1
```

Укажем учетную запись (пользователя Ivan) для подключения к серверу:

```
esr(config-pptp)# username ivan password ascii-text simplepass
```

Укажем удаленный шлюз:

```
esr(config-pptp)# remote address 20.20.0.1
```

Укажем зону безопасности:

```
esr(config-pptp)# security-zone VPN
```

Включим туннель PPTP:

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

Состояние туннеля можно посмотреть командой:

```
esr# show tunnels status pptp
```

Счетчики входящих и отправленных пакетов можно посмотреть командой:

```
esr# show tunnels counters pptp
```

Конфигурацию туннеля можно посмотреть командой:

```
esr# show tunnels configuration pptp
```

17.7 Настройка клиента удаленного доступа по протоколу L2TP

L2TP (англ. Layer 2 Tunneling Protocol – протокол туннелирования второго уровня) – туннельный протокол, использующийся для поддержки виртуальных частных сетей. L2TP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например, Интернет. L2TP может также использоваться для организации туннеля между двумя локальными сетями. L2TP использует дополнительное UDP-соединение для обслуживания туннеля. L2TP-протокол не предоставляет средств шифрования данных и поэтому он обычно используется в связке с группой протоколов IPsec, которая предоставляет безопасность на пакетном уровне.

17.7.1 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 (необязательно).	**esr(config-l2tp)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задаётся строкой до 31 символа.
3	Указать описание конфигурируемого туннеля (необязательно).	**esr(config-l2tp)# description <DESCRIPTION>**	<DESCRIPTION> – описание туннеля, задается строкой до 255 символов.
4	Включить L2TP-туннель в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall (см. раздел Конфигурирование Firewall).	**esr(config-l2tp)# security-zone <NAME>**	<NAME> – имя зоны безопасности, задаётся строкой до 31 символа.
		esr(config-l2tp)# ip firewall disable	
5	Установить удаленный IP-адрес для установки туннеля.	**esr(config-l2tp)# remote address <ADDR>**	<ADDR> – IP-адрес локального шлюза, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Шаг	Описание	Команда	Ключи
6	Указать пользователя и установить пароль в открытой или зашифрованной форме для аутентификации удалённой стороны.	**esr(config-l2tp)# username <NAME> password ascii-text { <WORD> | encrypted <HEX> }**	<NAME> – имя пользователя, задается строкой до 31 символа. <WORD> – пароль в открытой форме, задается строкой [8..64] символов, может включать символы [0-9a-fA-F]. <HEX> – пароль в зашифрованной форме, задается строкой [16..128] символов.
7	Выбрать метод аутентификации по ключу для IKE-соединения.	**esr(config-l2tp)# ipsec authentication method pre-shared-key**	
8	Указать общий секретный ключ для аутентификации, который должен совпадать у обоих сторон, устанавливающих туннель.	**esr(config-l2tp)# ipsec authentication pre-shared-key { ascii-text { <TEXT> | encrypted <ENCRYPTED-TEXT> } | hexadecimal {<HEX> | encrypted <ENCRYPTED-HEX> } }**	<TEXT> – строка [1..64] ASCII-символов; <HEX> – число размером [1..32] байт, задаётся строкой [2..128] символов в шестнадцатеричном формате (0xYYYY...) или (YYYY...); <ENCRYPTED-TEXT> – зашифрованный пароль размером [1..32] байт, задаётся строкой [2..128] символов; <ENCRYPTED-HEX> – зашифрованное число размером [2..64] байт, задаётся строкой [2..256] символов.
9	Ограничить используемые методы аутентификации и шифрования протокола IKE (необязательно).	**esr(config-l2tp)# ipsec ike proposal <NAME>**	<NAME> – имя ранее созданного профиля протокола IKE, задаётся строкой до 31 символа.
10	Включить пересогласование ключей до разрыва IKE-соединения (необязательно)	**esr(config-l2tp)# ipsec ike rekey enable**	
11	Ограничить используемые методы аутентификации и шифрования протокола IPsec (не обязательно).	**esr(config-l2tp)# ipsec proposal <NAME>**	<NAME> – имя ранее созданного профиля IPsec, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
12	Определяется номер UDP-порта по которому устанавливается соединение с l2tp-сервером (необязательно).	**esr(config-l2tp)# port <PORT>**	<PORT> – номер UDP-порта, задаётся в диапазоне [1024..65535]. Значение по умолчанию: 1701.
13	Активировать туннель.	**esr(config-l2tp)# enable**	
14	Установить размер MTU (MaximumTransmitionUnit) для туннеля (необязательно).	**esr(config-l2tp)# mtu <MTU>**	<MTU> – значение MTU, принимает значения в диапазоне [552..10000]. Значение по умолчанию: 1500.
15	Игнорировать dns-сервер через данный L2TP-туннель (необязательно).	**esr(config-l2tp)# ignore nameserver**	
16	Игнорировать маршрут по умолчанию через данный L2TP-туннель (необязательно)	**esr(config-l2tp)# ignore-default-route**	
17	Указать метод аутентификации (необязательно).	**esr(config-l2tp)# authentication method <METHOD>**	<METHOD> – метод аутентификации, возможные значения: chap, mschap, mschap-v2, eap, pap Значение по умолчанию: chap.
18	Задать интервал времени, за который усредняется статистика о нагрузке на туннель (необязательно).	**esr(config-l2tp)# load-average <TIME>**	<TIME> – интервал в секундах, принимает значения [5..150] Значение по умолчанию: 5.
19	Изменить интервал времени в секундах, по истечении которого маршрутизатор отправляет keepalive-сообщение (необязательно).	**esr(config-l2tp)# ppp timeout keepalive <TIME >**	<TIME> – время в секундах, задается в диапазоне [1..32767]. Значение по умолчанию: 10.
20	Изменить количество неудачных data-link тестов перед разрывом сессии (необязательно).	**esr(config-l2tp)# ppp failure-count <NUM>**	<NUM> – количество неудачных data-link тестов, задается в диапазоне [1..100]. Значение по умолчанию: 10.
Также для L2TP-клиента возможно настроить QoS в базовом или расширенном режимах (см. раздел Управление QoS).			

17.7.2 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
```

17.8 Настройка клиента удаленного доступа по протоколу WireGuard

WireGuard — простой, быстрый и современный VPN, использующий современную криптографию (ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24, HKDF). WireGuard надежно инкапсулирует IP-пакеты поверх UDP. В основе WireGuard лежит концепция под названием «Маршрутизация криптоключей», которая работает путем связывания открытых ключей со списком IP-адресов туннеля, которым разрешено находиться внутри туннеля. Каждый сетевой интерфейс имеет закрытый ключ и список пиров. У каждого узла есть открытый ключ. Открытые ключи короткие и простые и используются узлами для аутентификации друг друга. Их можно передавать для использования в файлах конфигурации любым внешним методом, аналогично тому, как можно отправить открытый ключ SSH для доступа к серверу.

17.8.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать WireGuard-туннель и перейти в режим его конфигурирования.	**esr(config)# tunnel wireguard <INDEX>**	<INDEX> – идентификатор туннеля в диапазоне: [1..16].
2	Указать экземпляр VRF, в котором будет работать данный Wireguard-туннель (необязательно).	**esr(config-wireguard)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задаётся строкой до 31 символа.
3	Указать описание конфигурируемого туннеля (необязательно).	**esr(config-wireguard)# description <DESCRIPTION>**	<DESCRIPTION> – описание туннеля, задается строкой до 255 символов.
4	Включить Wireguard-туннель в зону безопасности и настроить правила взаимодействия между зонами или отключить firewall (см. раздел Конфигурирование Firewall).	**esr(config-wireguard)# security-zone <NAME>**	<NAME> – имя зоны безопасности, задаётся строкой до 31 символа.
		esr(config-wireguard)# ip firewall disable	
5	Определить статический IP-адрес конфигурируемого туннеля.	**esr(config-wireguard)# 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].

Шаг	Описание	Команда	Ключи
6	Задать MTU (необязательно).	**esr(config-wireguard)# mtu <MTU>**	<MTU> – 552–10000. Значение по умолчанию: 1500.
7	Указать приватный ключ WireGuard-клиента.	**esr(config-wireguard)# private-key <NAME>**	<NAME> – имя приватного ключа, задается строкой до 31 символа.
8	Перейти к настройке разрешенных пиров	**esr(config-wireguard)# peer <COUNT>**	<COUNT> – номер соответствующего пира, принимает значения [1..16].
9	Указать описание пира (необязательно).	**esr(config-wireguard-peer)# description <DESCRIPTION>**	<DESCRIPTION> – описание туннеля, задается строкой до 255 символов.
10	Задать значение keepalive (необязательно).	**esr(config-wireguard-peer)# keepalive timeout <SEC>**	<SEC> – количество секунд, принимает значения [1..32767].
11	Указать публичный ключ WireGuard-пира.	**esr(config-wireguard-peer)# public-key <NAME>**	<NAME> – имя приватного ключа, задается строкой до 31 символа.
12	Указать pre-shared-key для настраиваемого пира (необязательно).	**esr(config-wireguard-peer)# pre-shared-key <TYPE> <WORD>**	<TYPE> – тип аргумента, устанавливаемый в качестве симметричного ключа: • **ascii-text** – указать симметричный ключ в виде ASCII-текста, который будет сконвертирован в формат Base64; • **base64** – указать симметричный ключ в формате Base64; • **encrypted** – указать симметричный ключ в зашифрованном виде. <WORD> - вводимый симметричный ключ. В зависимости от типа аргумента имеет длину 32 символа для ascii-text, 44 символа для формата base64 и 64 символа для зашифрованного вида.

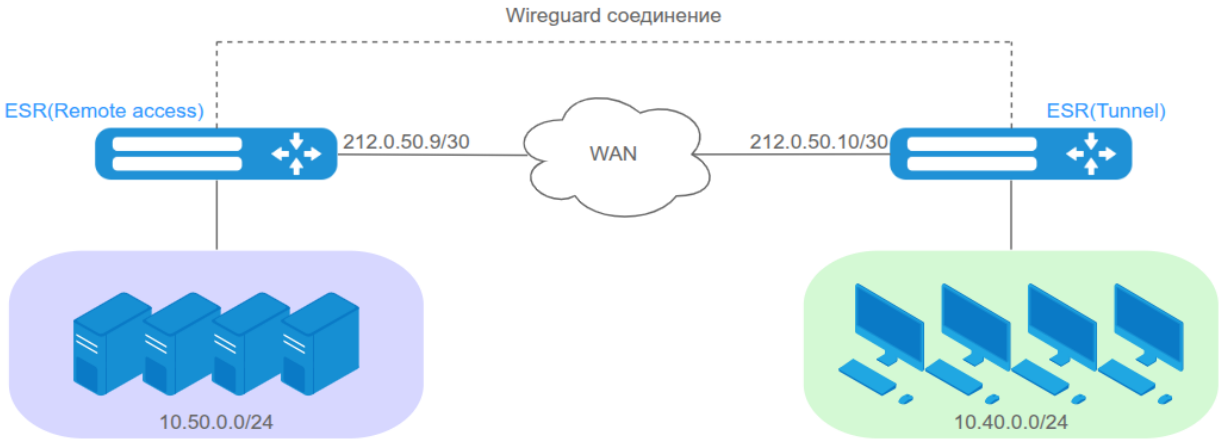
Шаг	Описание	Команда	Ключи
13	Указать IP-адрес удаленного пира.	**esr(config-wireguard-peer)# remote address <ADDR>**	<ADDR> – IP-адрес локального шлюза, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
14	Указать UDP-порт удаленного пира.	**esr(config-wireguard-peer)# remote port <PORT>**	<PORT>– UDP-порт, принимает значения [1..65535].
15	Указать список IP-адресов, которым будет разрешено находиться внутри туннеля.	**esr(config-wireguard-peer)# access-addresses <TYPE> {<FROM-ADDR> - <TO-ADDR> | <OBJ-GROUP-NETWORK-NAME> | <ADDR/LEN>}**	<TYPE> – тип аргумента, устанавливаемый в качестве адреса: • **address-range** – указать диапазон IPv4-адресов; • **object-group** – указать имя профиля; • **prefix** – указать адрес подсети и префикс. <FROM-ADDR> – начальный IP-адрес диапазона; <TO-ADDR> – конечный IP-адрес диапазона; <OBJ-GROUP-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа; <ADDR/LEN> – IP-адрес и маска подсети.
16	Активировать пир.	**esr(config-wireguard-peer)# enable**	
17	Активировать туннель.	**esr(config-wireguard)# enable**	
18	Задать интервал времени, за который усредняется статистика о нагрузке на туннель (необязательно).	**esr(config-wireguard)# load-average <TIME>**	<TIME> – интервал в секундах, принимает значения [5..150] Значение по умолчанию: 5.
19	Включить запись статистики использования текущего туннеля (необязательно).	**esr(config-wireguard)# history statistics**	

17.8.2 Пример настройки

Задача:

Настроить WireGuard-клиента на маршрутизаторе:

- адресация внутри туннеля – 110.0.0.0/30;
- порт подключения к серверу – 43020;
- адрес WireGuard-клиента внутри туннеля – 110.0.0.2;
- адрес удаленного сервера – 212.0.50.9.



Решение:

Создадим ключевую пару x25519, которая будет использоваться в работе WireGuard:

```
esr# crypto generate private-key x25519 filename wg_client_private.key
esr# crypto generate public-key x25519 private-key wg_client_private.key filename
wg_client_public.key
```

Для успешной работы необходимо совершить обмен открытыми криптографическими ключами с удаленной стороной любым удобным способом. На данном этапе настройки открытым криптографическим ключом является файл с именем **wg_client_public.key**, который хранится в **crypto:public-key**:

```
esr# show crypto certificates public-key
File name
------------------------------------------------------------------------------------------------------
---------------
wg_client_public.key
```

Создадим object-group network, в которой будет указан список IP-адресов, которым будет разрешено проходить через туннель:

```
esr(config)# object-group network WG_SERVERS
esr(config-object-group-network)# ip address-range 10.50.0.10-10.50.0.15
```

Создадим WireGuard-туннель, зададим локальный адрес и выставим MTU:

```
esr(config)# tunnel wireguard 1
esr(config-wireguard)# ip address 110.0.0.2/30
esr(config-wireguard)# mtu 1420
```

Укажем приватный ключ клиента и отключим Firewall:

```
esr(config-wireguard)# private-key wg_client_private.key
esr(config-wireguard)# ip firewall disable
```

Перейдем в настройки разрешённого пира, укажем связку публичного ключа сервера и разрешённого IP-адреса, а также укажем адрес и порт удаленного сервера:

```
esr(config-wireguard)# peer 1
esr(config-wireguard-peer)# public-key wg_server_public.key
esr(config-wireguard-peer)# access-addresses object-group WG_SERVERS
esr(config-wireguard-peer)# remote address 212.0.50.9
esr(config-wireguard-peer)# remote port 43020
```

Для усиления криптостойкости установим заранее известный симметричный ключ:

```
esr(config-wireguard-peer)# pre-shared-key base64 r4u48oYTouJ+j1GrAtVWRIZqlQ2YLjEZEvc+Yttc6R4=
```

Включим пир и WireGuard-туннель:

```
esr(config-wireguard-peer)# enable
esr(config-wireguard-peer)# exit
esr(config-wireguard)# enable
```

Попробуем отправить ICMP с рабочего ПК сотрудника (10.40.0.10) на удаленный сервер (10.50.0.10):

```
esr@client:~$ ping 10.50.0.10 -c 4
PING 10.50.0.10 (10.50.0.10) 56(84) bytes of data.
64 bytes from 10.50.0.10: icmp_seq=1 ttl=62 time=1.85 ms
64 bytes from 10.50.0.10: icmp_seq=2 ttl=62 time=1.47 ms
64 bytes from 10.50.0.10: icmp_seq=3 ttl=62 time=1.97 ms
64 bytes from 10.50.0.10: icmp_seq=4 ttl=62 time=1.72 ms

--- 10.50.0.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.465/1.753/1.974/0.188 ms
```

С помощью команды **monitor** можно убедиться, что ICMP-пакеты проходят через wireguard туннель:

```
esr# monitor wireguard 1
06:54:36.536109 ip: (tos 0x0, ttl 63, id 22999, offset 0, flags [DF], proto ICMP (1), length
84)
    10.40.0.10 > 10.50.0.10: ICMP echo request, id 1568, seq 12, length 64
06:54:36.537358 ip: (tos 0x0, ttl 63, id 32883, offset 0, flags [none], proto ICMP (1), length
84)
    10.50.0.10 > 10.40.0.10: ICMP echo reply, id 1568, seq 12, length 64


esr# monitor gigabitethernet 1/0/1
06:54:36.536109 50:1f:e6:04:51:00 > 50:dd:a1:04:50:00, ethertype IPv4 (0x0800), length 170:
(tos 0x0, ttl 64, id 21376, offset 0, flags [none], proto UDP (17), length 156)
    212.0.50.10.40548 > 212.0.50.9.43020: UDP, length 128
06:54:36.537358 50:dd:a1:04:50:00 > 50:1f:e6:04:51:00, ethertype IPv4 (0x0800), length 170:
(tos 0x0, ttl 64, id 41730, offset 0, flags [none], proto UDP (17), length 156)
    212.0.50.9.43020 > 212.0.50.10.40548: UDP, length 128
```

Счётчики сессий WireGuard-туннеля можно посмотреть командой:

```
esr# show tunnels counters wireguard 1
```

Очистить счётчики сессий WireGuard-туннеля можно командой:

```
esr# clear tunnels counters wireguard 1
```

Конфигурацию WireGuard-туннеля можно посмотреть командой:

```
esr# show tunnels configuration wireguard 1
```

18 Управление сервисами

- Настройка DHCP-сервера
  - Алгоритм настройки
  - Пример настройки
- Конфигурирование Destination NAT
  - Алгоритм настройки
  - Пример настройки Destination NAT
- Конфигурирование Source NAT
  - Алгоритм настройки
  - Пример настройки 1
  - Пример настройки 2
- Конфигурирование Static NAT
  - Алгоритм настройки
  - Пример настройки Static NAT
- Настройка NTP
  - Алгоритм настройки
  - Пример настройки

18.1 Настройка DHCP-сервера

Встроенный DHCP-сервер маршрутизатора может быть использован для настройки сетевых параметров устройств в локальной сети. DHCP-сервер маршрутизаторов способен передавать дополнительные опции на сетевые устройства, например:

- default-router – IP-адрес маршрутизатора, используемого в качестве шлюза по умолчанию;
- domain-name – доменное имя, которое должен будет использовать клиент при разрешении имен хостов через Систему Доменных Имен (DNS);
- dns-server – список адресов серверов доменных имен в данной сети, о которых должен знать клиент. Адреса серверов в списке располагаются в порядке убывания предпочтения.

18.1.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Включить IPv4/IPv6 DHCP-сервер.	**esr(config)# ip dhcp-server [vrf <VRF>]**	<VRF> – имя экземпляра VRF, в рамках которого будет работать DHCP-сервер. Задается строкой до 31 символа.
		esr(config)# ipv6 dhcp-server [vrf <VRF>]	
2	Задать значение кода DSCP для использования в IP-заголовке исходящих пакетов DHCP-сервера (не обязательно).	**esr(config)# ip dhcp-server dscp <DSCP>**	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 61.

Шаг	Описание	Команда	Ключи
3	Создать пул IPv4/IPv6-адресов DHCP-сервера и перейти в режим его конфигурирования.	**esr(config)# ip dhcp-server pool <NAME> [vrf <VRF>]**	<NAME> – имя пула IPv4/IPv6-адресов DHCP-сервера, задаётся строка до 31 символа. <VRF> – имя экземпляра VRF, в рамках которого будет работать данный пул IP-адресов DHCP-сервера. Задается строкой до 31 символа
		esr(config)# ipv6 dhcp-server pool <NAME> [vrf <VRF>]	
4	Задать IPv4/IPv6-адрес и маску для подсети, из которой будет выделен пул IPv4/IPv6-адресов.	**esr(config-dhcp-server)# network <ADDR/LEN>**	<ADDR/LEN> – IP-адрес и префикс подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].
		esr(config-ipv6-dhcp-server)# network <IPV6-ADDR/LEN>	<IPV6-ADDR/LEN> – IP-адрес и префикс подсети, задаётся в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128].
5	Добавить диапазон IPv4/IPv6-адресов к пулу адресов, конфигурируемого DHCP-сервера.	**esr(config-dhcp-server)# address-range <FROM-ADDR>-<TO-ADDR>**	<FROM-ADDR> – начальный IP-адрес диапазона; <TO-ADDR> – конечный IP-адрес диапазона, Адреса задаются в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Можно указать до 32 диапазонов IP-адресов, список задаётся через запятую.

Шаг	Описание	Команда	Ключи
		esr(config-ipv6-dhcp-server)# address-range <FROM-ADDR>-<TO-ADDR>	<FROM-ADDR> – начальный IPv6-адрес диапазона; <TO-ADDR> – конечный IP-адрес диапазона; Адреса задаются в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
6	Добавить IPv4/IPv6-адрес для определенного физического адреса к пулу адресов конфигурируемого DHCP-сервера (не обязательно).	**esr(config-dhcp-server)# address <ADDR> {mac-address <MAC> | client-identifier <CI>}**	<ADDR> – IP-адрес клиента, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <MAC> – MAC-адрес клиента, которому будет выдан IP-адрес, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]. <CI> – идентификатор клиента согласно DHCP Option 61. Может быть задан в одном из следующих видов: • HH:HH:HH:HH:HH:HH:HH: – идентификатор клиента в шестнадцатеричной форме и MAC-адрес клиента; • STRING – текстовая строка длиной от 1 до 64 символов.
		esr(config-ipv6-dhcp-server)# address <ADDR> mac-address <MAC>	<IPV6-ADDR> – IPv6-адрес клиента, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <MAC> – MAC-адрес клиента, которому будет выдан IPv6-адрес, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF].

Шаг	Описание	Команда	Ключи
7	Задать список IPv4-адресов шлюзов по умолчанию, которые DHCP-сервер будет сообщать клиентам, используя DHCP-опцию 3.	**esr(config-dhcp-server)# default-router <ADDR>**	<ADDR> – IP-адрес шлюза по умолчанию, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Можно указать до 8 IP-адресов, список задаётся через запятую.
8	Задать DNS-имя сетевого домена. Имя домена передаётся клиентам в составе DHCP-опции 15 (не обязательно).	**esr(config-dhcp-server)# domain-name <NAME>**	<NAME> – DNS-имя домена клиента, задаётся строкой до 255 символов.
		esr(config-ipv6-dhcp-server)# domain-name <NAME>	
9	Задать список IPv4/IPv6-адресов DNS-серверов. Список передаётся клиентам в составе DHCP-опции 6 (не обязательно).	**esr(config-dhcp-server)# dns-server <ADDR>**	<ADDR> – IP-адрес DNS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Можно указать до 8 IP-адресов, список задаётся через запятую.
		esr(config-ipv6-dhcp-server)# dns-server <IPV6-ADDR>	<IPV6-ADDR> – IPv6-адрес DNS-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. Можно указать до 8 IPv6-адресов, список задаётся через запятую.
10	Задать максимальное время аренды IP-адресов (не обязательно). Если DHCP-клиент запрашивает время аренды, превосходящее максимальное значение, то будет установлено время, заданное этой командой.	**esr(config-dhcp-server)# max-lease-time <TIME>**	<TIME> – максимальное время аренды IP-адреса, задаётся в формате DD:HH:MM, где: • DD – количество дней, принимает значения [0..364]; • HH – количество часов, принимает значения [0..23]; • MM – количество минут, принимает значения [0..59]. Значение по умолчанию: 1 день.
		esr(config-ipv6-dhcp-server)# max-lease-time <TIME>	

Шаг	Описание	Команда	Ключи
11	Задать время аренды, на которое клиенту будет выдан IP-адрес (не обязательно). Данное время будет использоваться если клиент не запрашивал определенное время аренды.	**esr(config-dhcp-server)# default-lease-time <TIME>**	<TIME> – максимальное время аренды IP-адреса, задаётся в формате DD:HH:MM, где: • DD – количество дней, принимает значения [0..364]; • HH – количество часов, принимает значения [0..23]; • MM – количество минут, принимает значения [0..59]. Значение по умолчанию: 12 часов.
		esr(config-ipv6-dhcp-server)# default-lease-time <TIME>	
12	Создать идентификатор класса поставщика (DHCP Опция 60) (не обязательно).	**esr(config)# ip dhcp-server vendor-class-id <NAME>**	<NAME> – идентификатор класса поставщика, задаётся строкой до 31 символа.
		esr(config)# ipv6 dhcp-server vendor-class-id <NAME>	
13	Задать специфическую информацию поставщика (DHCP Опция 43).	**esr(config-dhcp-vendor-id)# vendor-specific-options <HEX>**	<HEX> – специфическая информация поставщика, задаётся в шестнадцатеричном формате до 128 символов.
		esr(config-ipv6-dhcp-vendor-id)# vendor-specific-options <HEX>	
14	Задать IP-адрес NetBIOS-сервера (DHCP опция 44) (не обязательно).	**esr(config-dhcp-server)# netbios-nameserver <ADDR>**	<ADDR> – IP-адрес NetBIOS-сервера задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Можно задать до 4 IP-адресов.
15	Задать IP-адрес tftp-сервера (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].

⚠ Для продления ресурса внутреннего flash-накопителя информация о выданных сервером IP-адресах хранится в энергозависимой памяти. Поэтому стоит учитывать, что при перезагрузке маршрутизатора сервер начинает выдавать адреса заново. Занятость адресов будет проверяться с помощью ICMP-запросов.

18.1.2 Пример настройки

Задача:

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

Решение:

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

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

Создадим пул адресов с именем «Simple» и добавим в данный пул адресов диапазон IP-адресов для выдачи в аренду клиентам сервера. Укажем параметры подсети, к которой принадлежит данный пул, и время аренды для выдаваемых адресов:

```
esr# configure
esr(config)# ip dhcp-server pool Simple
esr(config-dhcp-server)# network 192.168.1.0/24
esr(config-dhcp-server)# address-range 192.168.1.100-192.168.1.125
esr(config-dhcp-server)# default-lease-time 1:00:00
```

Сконфигурируем передачу клиентам дополнительных сетевых параметров:

- маршрут по умолчанию: 192.168.1.1;
- имя домена: eltex.loc;
- список DNS-серверов: DNS1: 172.16.0.1, DNS2: 8.8.8.8.

```
esr(config-dhcp-server)# domain-name "eltex.loc"
esr(config-dhcp-server)# default-router 192.168.1.1
esr(config-dhcp-server)# dns-server 172.16.0.1,8.8.8.8
esr(config-dhcp-server)# exit
```

Для того чтобы DHCP-сервер мог раздавать IP-адреса из конфигурируемого пула, на маршрутизаторе должен быть создан IP-интерфейс, принадлежащий к той же подсети, что и адреса пула.

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

Для разрешения прохождения сообщений протокола DHCP к серверу необходимо создать соответствующие профили портов, включающие порт источника 68 и порт назначения 67, используемые протоколом DHCP, и создать разрешающее правило в политике безопасности для прохождения пакетов протокола UDP:

```
esr(config)# object-group service dhcp_server
esr(config-object-group-service)# port-range 67
esr(config-object-group-service)# exit
esr(config)# object-group service dhcp_client
esr(config-object-group-service)# port-range 68
esr(config-object-group-service)# exit
esr(config)# security zone-pair trusted self
esr(config-zone-pair)# rule 30
esr(config-zone-rule)# match protocol udp
esr(config-zone-rule)# match source-port object-group dhcp_client
esr(config-zone-rule)# match destination-port object-group dhcp_server
esr(config-zone-rule)# action permit
esr(config-zone-rule)# enable
esr(config-zone-rule)# exit
esr(config-zone-pair)# exit
```

Разрешим работу сервера:

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

Просмотреть список арендованных адресов можно с помощью команды:

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

Просмотреть сконфигурированные пулы адресов можно командами:

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

⚠ Конфигурирование настроек для IPv6 производится по аналогии с IPv4.

18.2 Конфигурирование Destination NAT

Функция Destination NAT (DNAT) состоит в преобразовании IP-адреса назначения у пакетов, проходящих через сетевой шлюз.

DNAT используется для перенаправления трафика, идущего на некоторый «виртуальный» адрес в публичной сети, на «реальный» сервер в локальной сети, находящийся за сетевым шлюзом. Эту функцию можно использовать для организации публичного доступа к серверам, находящимся в частной сети и не имеющим публичного сетевого адреса.

18.2.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим настройки сервиса трансляции адресов получателя.	**esr(config)# nat destination**	
2	Создать пул IP-адресов и/или TCP/UDP-портов с определённым именем (не обязательно).	**esr(config-dnat)# pool <NAME>**	<NAME> – имя пула NAT-адресов, задаётся строкой до 31 символа.
3	Установить внутренний IP-адрес, на который будет заменяться IP-адрес получателя.	**esr(config-dnat-pool)# ip address <ADDR>**	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
4	Установить внутренний TCP/UDP-порт, на который будет заменяться TCP/UDP-порт получателя.	**esr(config-dnat-pool)# ip port <PORT>**	<PORT> – TCP/UDP-порт, принимает значения [1..65535].
5	Создать группу правил с определённым именем.	**esr(config-dnat)# ruleset <NAME>**	<NAME> – имя группы правил, задаётся строкой до 31 символа.
6	Указать экземпляр VRF, в котором будет работать данная группа правил (не обязательно).	**esr(config-dnat-ruleset)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.
7	Задать область применения группы правил. Правила будут применяться только для трафика, идущего из определенной зоны или интерфейса.	**esr(config-dnat-ruleset)# from { zone <NAME> | interface <IF> | tunnel <TUN> | default }**	<NAME> – имя зоны изоляции; <IF> – имя интерфейса устройства; <TUN> – имя туннеля устройства. default – обозначает группу правил для всего трафика, источник которого не попал под критерии других групп правил.
8	Задать правило с определённым номером. Правила обрабатываются в порядке возрастания.	**esr(config-dnat-ruleset)# rule <ORDER>**	<ORDER> – номер правила, принимает значения [1...10000].

9	Задать IP-адреса {отправителя | получателя}, для которых должно срабатывать правило.	**esr(config-dnat-rule)# match [not] {source|destination}-address { address-range { <ADDR>[-<ADDR>] } | prefix { <ADDR/LEN> } | object-group { network <OBJ-GROUP-NETWORK-NAME> } }**	**address-range** <ADDR>[-<ADDR>] – диапазон IP-адресов для правил NAT. Если не указывать IP-адрес конца диапазона, то в качестве IP-адреса для срабатывания правила используется только IP-адрес начала диапазона. Параметр задаётся в виде A.B.C.D, где каждая часть принимает значения [0..255]; **prefix** <ADDR/LEN> – IP-подсеть, используемая для срабатывания правила NAT. Параметр задаётся в виде A.B.C.D/E, где каждая часть A – D принимает значения [0..255] и E принимает значения [1..32]; **object-group network** <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.
10	Задать сервисы (TCP/UDP-портов) {отправителя | получателя}, для которых должно срабатывать правило (не обязательно).	**esr(config-dnat-rule)# match [not] {source|destination}-port <TYPE> {<PORT-SET-NAME> | <FORM-PORT> - <TO-PORT>}**	<TYPE> – тип аргумента, устанавливаемый в качестве адреса: • **address-range** – указать диапазон IPv4/IPv6 адресов; • **object-group** – указать имя профиля; • **any** – установить в качестве адреса любой адрес. <PORT-SET-NAME> – имя профиля порта, задаётся строкой до 31 символа; <FROM-PORT> – начальный порт диапазона; <TO-PORT> – конечный порт диапазона.

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, icmp6, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rsvp, l2tp, gre. Значение «any» указывает на любой тип протокола. <ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF].
12	Задать тип и код сообщений протокола ICMP, для которых должно срабатывать правило (если в качестве протокола выбран ICMP) (не обязательно).	**esr(config-dnat-rule)# match [not] icmp {<ICMP_TYPE><ICMP_CODE> | <TYPE-NAME>}**	<ICMP_TYPE> – тип сообщения протокола ICMP, принимает значения [0..255]. <ICMP_CODE> – код сообщения протокола ICMP, принимает значения [0..255]. Значение «any» указывает на любой код сообщения. <TYPE-NAME> – имя типа ICMP-сообщения.
13	Задать действие «трансляция адреса и порта получателя» для трафика, удовлетворяющего критериям, заданным командами «match».	**esr(config-dnat-rule)# action destination-nat { off | pool <NAME> | netmap <ADDR/LEN> }**	off – трансляция отключена; pool <NAME> – имя пула, содержащего набор IP-адресов и/или TCP/UDP-портов; netmap <ADDR/LEN> – IP-адрес и маска подсети, используемые при трансляции. Параметр задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].
14	Активировать конфигурируемое правило.	**esr(config-dnat-rule)# enable**	

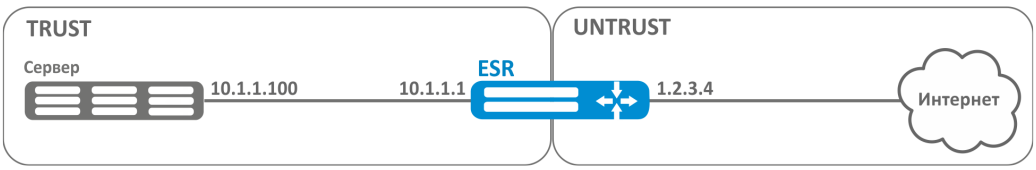
15	Включить функцию отслеживания сессий уровня приложений для протоколов FTP, SIP, H323, netbios-ns, PPTP (не обязательно).	**esr(config)# ip firewall sessions tracking** **{<PROTOCOL> | sip [port <OBJECT-GROUP-SERVICE>] | all}**	all – включает функцию отслеживания сессий уровня приложений для всех доступных протоколов; <PROTOCOL> – протокол уровня приложений, сессии которого должны отслеживаться, принимает значения [ftp, h323, pptp, netbios-ns]; <OBJECT-GROUP-SERVICE> – имя профиля TCP/UDP-портов sip-сессии, задаётся строкой до 31 символа. Если группа не указана, то отслеживание сессий sip будет осуществляться для порта 5060.
16	Включить функцию трансляции IP-адресов в заголовках уровня приложений (не обязательно).	**esr(config)# nat alg {<PROTOCOL> | all}**	all – включает трансляцию IP-адресов в заголовках всех доступных протоколов. <PROTOCOL> – протокол уровня приложений, в заголовках которого должна работать трансляция адресов, принимает значения [ftp, h323, pptp, netbios-ns, gre, sip, tftp].

При использовании ключа *not* правило будет срабатывать для значений, которые не входят в указанный профиль.
Каждая команда «match» может содержать ключ «not». При использовании данного ключа под правило будут подпадать пакеты, не удовлетворяющие заданному критерию.
Более подробная информация о командах для настройки маршрутизатора содержится в справочнике команд CLI.

18.2.2 Пример настройки Destination NAT

Задача:

Организовать доступ из публичной сети, относящейся к зоне «UNTRUST», к серверу локальной сети в зоне «TRUST». Адрес сервера в локальной сети – 10.1.1.100. Сервер должен быть доступным извне по адресу 1.2.3.4, доступный порт 80.



Решение:

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

```
esr# configure
esr(config)# security zone UNTRUST
esr(config-zone)# exit
esr(config)# security zone TRUST
esr(config-zone)# exit
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)#   security-zone TRUST
esr(config-if-gi)#   ip address 10.1.1.1/25
esr(config-if-gi)# exit
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip address 1.2.3.4/29
esr(config-if-te)# security-zone UNTRUST
esr(config-if-te)# exit
```

Создадим профили IP-адресов и портов, которые потребуются для настройки правил Firewall и правил DNAT.

- NET_UPLINK – профиль адресов публичной сети;
- SERVER_IP – профиль адресов локальной сети;
- SRV_HTTP – профиль портов.

```
esr(config)# object-group network NET_UPLINK
esr(config-object-group-network)# ip address 1.2.3.4
esr(config-object-group-network)# exit
```

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

```
esr(config)# object-group network SERVER_IP
esr(config-object-group-network)# ip address 10.1.1.100
esr(config-object-group-network)# exit
```

Войдем в режим конфигурирования функции DNAT и создадим пул адресов и портов назначения, в которые будут транслироваться адреса пакетов, поступающие на адрес 1.2.3.4 из внешней сети.

```
esr(config)# nat destination
esr(config-dnat)# pool SERVER_POOL
esr(config-dnat-pool)# ip address 10.1.1.100
esr(config-dnat-pool)# ip port 80
esr(config-dnat-pool)# exit
```

Создадим набор правил «DNAT», в соответствии с которыми будет производиться трансляция адресов. В атрибутах набора укажем, что правила применяются только для пакетов, пришедших из зоны «UNTRUST». Набор правил включает в себя требования соответствия данных по адресу и порту назначения (match destination-address, match destination-port) и по протоколу. Кроме этого в наборе

задано действие, применяемое к данным, удовлетворяющим всем правилам (action destination-nat). Набор правил вводится в действие командой **enable**.

```
esr(config-dnat)# ruleset DNAT
esr(config-dnat-ruleset)# from zone UNTRUST
esr(config-dnat-ruleset)# rule 1
esr(config-dnat-rule)# match destination-address object-group NET_UPLINK
esr(config-dnat-rule)# match protocol tcp
esr(config-dnat-rule)# match destination-port object-group 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 object-group network SERVER_IP
esr(config-zone-pair-rule)# match destination-nat
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
esr(config)# exit
```

Произведенные настройки можно посмотреть с помощью команд:

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

18.3 Конфигурирование Source NAT

Функция Source NAT (SNAT) используется для подмены адреса источника у пакетов, проходящих через сетевой шлюз. При прохождении пакетов из локальной сети в публичную сеть адрес источника заменяется на один из публичных адресов шлюза. Дополнительно к адресу источника может применяться замена порта источника. При прохождении пакетов из публичной сети в локальную происходит обратная подмена адреса и порта.

Функция SNAT может быть использована для предоставления доступа в Интернет компьютерам, находящимся в локальной сети. При этом не требуется назначения публичных IP-адресов этим компьютерам.

18.3.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим настройки сервиса трансляции адресов отправителя.	**esr(config)# nat source**	
2	Создать пул IP-адресов и/или TCP/UDP-портов с определённым именем (не обязательно).	**esr(config-snat)# pool <NAME>**	<NAME> – имя пула NAT-адресов, задаётся строкой до 31 символа.
3	Установить диапазон IP-адресов, для которых будет заменяться IP-адрес отправителя.	**esr(config-snat-pool)# ip address-range <IP>[-<ENDIP>]**	<IP> – IP-адрес начала диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <ENDIP> – IP-адрес конца диапазона, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Если не указывать IP-адрес конца диапазона, то в качестве IP-адреса для трансляции используется только IP-адрес начала диапазона.
4	Задать диапазон внешних TCP/UDP-портов, на которые будет заменяться TCP/UDP-порт отправителя.	**esr(config-snat-pool)# ip port-range <PORT>[-<ENDPORT>]**	<PORT> – TCP/UDP-порт начала диапазона, принимает значения [1..65535]; <ENDPORT> – TCP/UDP-порт конца диапазона, принимает значения [1..65535]. Если не указывать TCP/UDP-порт конца диапазона, то в качестве TCP/UDP-порта для трансляции используется только TCP/UDP-порт начала диапазона.
5	Установить внешний TCP/UDP-порт, на который будет заменяться TCP/UDP-порт отправителя.	**esr(config-snat-pool)# ip port <PORT>**	<PORT> – TCP/UDP-порт, принимает значения [1..65535].
6	Включить функции NAT persistent.	**esr(config-snat-pool)# persistent**	
7	Создать группу правил с определённым именем.	**esr(config-snat)# ruleset <NAME>**	<NAME> – имя группы правил, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
8	Указать экземпляр VRF, в котором будет работать данная группа правил (не обязательно).	**esr(config-snat-ruleset)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.
9	Задать область применения группы правил. Правила будут применяться только для трафика, идущего в определенную зону или интерфейс.	**esr(config-snat-ruleset)# to { zone <NAME> | interface <IF> tunnel <TUN> | | default }**	<NAME> – имя зоны изоляции; <IF> – имя интерфейса устройства; <TUN> – имя туннеля устройства default – обозначает группу правил для всего трафика, источник которого не попал под критерии других групп правил.
10	Задать правило с определённым номером. Правила обрабатываются в порядке возрастания.	**esr(config-snat-ruleset)# rule <ORDER>**	<ORDER> – номер правила, принимает значения [1..10000].
11	Задать профиль IP-адресов {отправителя | получателя}, для которых должно срабатывать правило.	**esr(config-dnat-rule)# match [not] {source|destination}-address { address-range { <ADDR>[-<ADDR>] } | prefix { <ADDR/LEN> } | object-group { network <OBJ-GROUP-NETWORK-NAME> } }**	**address-range** <ADDR>[-<ADDR>] – диапазон IP-адресов для правил NAT. Если не указывать IP-адрес конца диапазона, то в качестве IP-адреса для срабатывания правила используется только IP-адрес начала диапазона. Параметр задаётся в виде A.B.C.D, где каждая часть принимает значения [0..255]; **prefix** <ADDR/LEN> – IP-подсеть, используемая для срабатывания правила NAT. Параметр задаётся в виде A.B.C.D/E, где каждая часть A – D принимает значения [0..255] и E принимает значения [1..32]; **object-group network** <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
12	Задать профиль IP-адресов {отправителя | получателя}, для которых должно срабатывать правило (не обязательно).	**esr(config-snat-rule)# match [not] {source | destination}-port <TYPE> {<PORT-SET-NAME> | <FROM-PORT> - <TO-PORT>}**	<TYPE> – тип аргумента, устанавливаемый в качестве адреса: • **address-range** – указать диапазон IPv4/IPv6 адресов; • **object-group** – указать имя профиля; • **any** – установить в качестве адреса любой адрес. <PORT-SET-NAME> – имя профиля порта, задаётся строкой до 31 символа; <FROM-PORT> – начальный порт диапазона; <TO-PORT> – конечный порт диапазона.
13	Установить имя или номер IP-протокола, для которого должно срабатывать правило (не обязательно).	**esr(config-snat-rule)# match [not] {protocol|protocol-id} <TYPE>**	<TYPE> – тип протокола, принимает значения: esp, icmp, icmp6, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rsvp, l2tp, gre. Значение «any» указывает на любой тип протокола; <ID> – идентификационный номер IP-протокола, принимает значения [0x00-0xFF].
14	Задать тип и код сообщений протокола ICMP, для которых должно срабатывать правило (не обязательно).	**esr(config-snat-rule)# match [not] icmp {<ICMP_TYPE><ICMP_CODE> | <TYPE-NAME>}**	<ICMP_TYPE> – тип сообщения протокола ICMP, принимает значения [0..255]; <ICMP_CODE> – код сообщения протокола ICMP, принимает значения [0..255]. Значение «any» указывает на любой код сообщения; <TYPE-NAME> – имя типа ICMP сообщения

Шаг	Описание	Команда	Ключи
15	Задать действие «трансляция адреса и порта отправителя» для трафика, удовлетворяющего критериям, заданным командами «match».	**esr(config-snat-rule)# action source-nat { off | pool <NAME> | netmap <ADDR/LEN> [static] | interface [FIRST_PORT – LAST_PORT] }**	off – трансляция отключена; pool<NAME> – имя пула, содержащего набор IP-адресов и/или TCP/UDP-портов; netmap <ADDR/LEN> – IP-адрес и маска подсети, используемые при трансляции; static – опция для организации статического NAT. Параметр задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. interface [FIRST_PORT – LAST_PORT] – задаёт трансляцию в IP-адрес интерфейса. Если дополнительно задан диапазон TCP/UDP-портов, то трансляция будет происходить только для TCP/UDP-портов отправителя, входящих в указанный диапазон.
16	Активировать конфигурируемое правило.	**esr(config-snat-rule)# enable**	

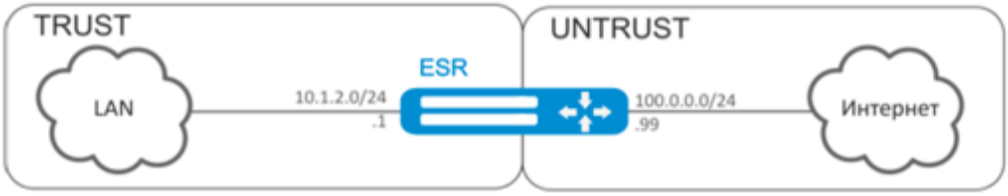
Шаг	Описание	Команда	Ключи
17	Включить функцию отслеживания сессий уровня приложений для протоколов FTP, SIP, H323, netbios-ns, PPTP (не обязательно).	**esr(config)# ip firewall sessions tracking** **{<PROTOCOL> | sip [port <OBJECT-GROUP-SERVICE>] | all}**	all – включает функцию отслеживания сессий уровня приложений для всех доступных протоколов <PROTOCOL> – протокол уровня приложений, сессии которого должны отслеживаться, принимает значения [ftp, h323, pptp, netbios-ns]. <OBJECT-GROUP-SERVICE> – имя профиля TCP/UDP-портов sip-сессии, задаётся строкой до 31 символа. Если группа не указана, то отслеживание сессий sip будет осуществляться для порта 5060.
18	Включить функцию трансляции IP-адресов в заголовках уровня приложений (не обязательно).	**esr(config)# nat alg {<PROTOCOL> | all}**	all – включает трансляцию IP-адресов в заголовках всех доступных протоколов. <PROTOCOL> – протокол уровня приложений, в заголовках которого должна работать трансляция адресов, принимает значения [ftp, h323, pptp, netbios-ns, gre, sip, tftp].

⚠ При использовании ключа not правило будет срабатывать для значений, которые не входят в указанный профиль.
Каждая команда «match» может содержать ключ «not». При использовании данного ключа под правило будут подпадать пакеты, не удовлетворяющие заданному критерию.
Более подробная информация о командах для настройки маршрутизатора содержится в справочнике команд CLI.

18.3.2 Пример настройки 1

Задача:

Настроить доступ пользователей локальной сети 10.1.2.0/24 к публичной сети с использованием функции Source NAT. Задать диапазон адресов публичной сети для использования SNAT 100.0.0.100-100.0.0.249.



Решение:

Конфигурирование начнем с создания зон безопасности, настройки сетевых интерфейсов и определения их принадлежности к зонам безопасности. Создадим доверенную зону «TRUST» для локальной сети и зону «UNTRUST» для публичной сети.

```
esr# configure
esr(config)# security zone UNTRUST
esr(config-zone)# exit
esr(config)# security zone TRUST
esr(config-zone)# exit
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 10.1.2.1/24
esr(config-if-gi)# security-zone TRUST
esr(config-if-gi)# exit
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip address 100.0.0.99/24
esr(config-if-te)# security-zone UNTRUST
esr(config-if-te)# exit
```

Для конфигурирования функции SNAT и настройки правил зон безопасности потребуется создать профиль адресов локальной сети «LOCAL_NET», включающий адреса, которым разрешен выход в публичную сеть, и профиль адресов публичной сети «PUBLIC_POOL».

```
esr(config)# object-group network LOCAL_NET
esr(config-object-group-network)# ip address-range 10.1.2.2-10.1.2.254
esr(config-object-group-network)# exit
esr(config)# object-group network PUBLIC_POOL
esr(config-object-group-network)# ip address-range 100.0.0.100-100.0.0.249
esr(config-object-group-network)# exit
```

Для пропуска трафика из зоны «TRUST» в зону «UNTRUST» создадим пару зон и добавим правила, разрешающие проходить трафику в этом направлении. Дополнительно включена проверка адреса источника данных на принадлежность к диапазону адресов «LOCAL_NET» для соблюдения ограничения на выход в публичную сеть. Действие правил разрешается командой **enable**.

```
esr(config)# security zone-pair TRUST UNTRUST
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# match source-address object-group network 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 object-group network LOCAL_NET
esr(config-snat-rule)# action source-nat pool TRANSLATE_ADDRESS
esr(config-snat-rule)# enable
esr(config-snat-rule)# exit
esr(config-snat-ruleset)# exit
```

Для того чтобы маршрутизатор отвечал на запросы протокола ARP для адресов, входящих в публичный пул, необходимо запустить сервис ARP Proxy. Сервис ARP Proxy настраивается на интерфейсе, которому принадлежит IP-адрес из подсети профиля адресов публичной сети «PUBLIC_POOL».

```
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip nat proxy-arp PUBLIC_POOL
```

Для того чтобы устройства локальной сети могли получить доступ к публичной сети, на них должна быть настроена маршрутизация – адрес 10.1.2.1 должен быть назначен адресом шлюза.

На самом маршрутизаторе также должен быть создан маршрут для направления на публичную сеть. Этот маршрут может быть назначен маршрутом по умолчанию с помощью следующей команды.

```
esr(config)# ip route 0.0.0.0/0 100.0.0.1
esr(config)# exit
```

18.3.3 Пример настройки 2

Задача:

Настроить доступ пользователей локальной сети 21.12.2.0/24 к публичной сети с использованием функции Source NAT без использования межсетевого экрана (firewall). Диапазон адресов публичной сети для использования SNAT 200.10.0.100-200.10.0.249.



Решение:

Конфигурирование начнем с настройки сетевых интерфейсов и отключения межсетевого:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 21.12.2.1/24
esr(config-if-gi)# ip firewall disable
esr(config-if-gi)# exit
```

```
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip address 200.10.0.1/24
esr(config-if-te)# ip firewall disable
esr(config-if-te)# exit
```

Для конфигурирования функции SNAT потребуется создать профиль адресов локальной сети «LOCAL_NET», включающий адреса, которым разрешен выход в публичную сеть, и профиль адресов публичной сети «PUBLIC_POOL»:

```
esr(config)# object-group network LOCAL_NET
esr(config-object-group-network)# ip address-range 21.12.2.2-21.12.2.254
esr(config-object-group-network)# exit

esr(config)# object-group network PUBLIC_POOL
esr(config-object-group-network)# ip address-range 200.10.0.100-200.10.0.249
esr(config-object-group-network)# exit
```

Конфигурируем сервис SNAT.

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

```
esr(config)# nat source
esr(config-snat)# pool TRANSLATE_ADDRESS
esr(config-snat-pool)# ip address-range 200.10.0.100-200.10.0.249
esr(config-snat-pool)# exit
```

Вторым шагом создаётся набор правил SNAT. В атрибутах набора укажем, что правила применяются только для пакетов, направляющихся в публичную сеть через порт te1/0/1. Правила включают проверку адреса источника данных на принадлежность к пулу «LOCAL_NET»:

```
esr(config-snat)# ruleset SNAT
esr(config-snat-ruleset)# to interface te1/0/1
esr(config-snat-ruleset)# rule 1
esr(config-snat-rule)# match source-address object-group network LOCAL_NET
esr(config-snat-rule)# action source-nat pool TRANSLATE_ADDRESS
esr(config-snat-rule)# enable
esr(config-snat-rule)# exit
esr(config-snat-ruleset)# exit
```

Для того чтобы маршрутизатор отвечал на запросы протокола ARP для адресов, входящих в публичный пул, необходимо запустить сервис ARP Proxy. Сервис ARP Proxy настраивается на интерфейсе, которому принадлежит IP-адрес из подсети профиля адресов публичной сети «PUBLIC_POOL»:

```
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip nat proxy-arp PUBLIC_POOL
```

Для того чтобы устройства локальной сети могли получить доступ к публичной сети, на них должна быть настроена маршрутизация – адрес 21.12.2.1 должен быть назначен адресом шлюза.

На самом маршрутизаторе также должен быть создан маршрут для направления на публичную сеть. Этот маршрут может быть назначен маршрутом по умолчанию с помощью следующей команды:

```
esr(config)# ip route 0.0.0.0/0 200.10.0.254
esr(config)# exit
```

18.4 Конфигурирование Static NAT

Static NAT — статический NAT задает однозначное соответствие одного адреса другому. Иными словами, при прохождении через маршрутизатор, адрес меняется на другой строго заданный адрес, один-к-одному. Запись о такой трансляции хранится неограниченно долго, пока не будет произведена перенастройка NAT на маршрутизаторе.

18.4.1 Алгоритм настройки

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

18.4.2 Пример настройки Static NAT

Задача:

Настроить двухстороннюю и постоянную трансляцию из локальной сети для диапазона адресов 21.12.2.100-21.12.2.150 в публичную сеть 200.10.0.0/24. Диапазон адресов публичной сети для использования трансляции – 200.10.0.100-200.10.0.150.



Решение:

Начнем конфигурирование с настройки сетевых интерфейсов и отключения межсетевого экрана:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip address 21.12.2.1/24
esr(config-if-gi)# ip firewall disable
esr(config-if-gi)# exit
```

```
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip address 200.10.0.1/24
esr(config-if-te)# ip firewall disable
esr(config-if-te)# exit
```

Для конфигурирования Static NAT потребуется создать профиль адресов локальной сети «LOCAL_NET», включающий локальную подсеть:

```
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
```

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».

```
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 object-group network LOCAL_NET
esr(config-snat-rule)# action source-nat netmap 200.10.0.0/24 static
esr(config-snat-rule)# enable
esr(config-snat-rule)# exit
esr(config-snat-ruleset)# exit
```

Для того чтобы маршрутизатор отвечал на запросы протокола ARP для адресов, входящих в пул трансляции «PROXY», необходимо запустить сервис ARP Proxy. Сервис ARP Proxy настраивается на интерфейсе, которому принадлежит IP-адрес из подсети профиля адресов «PROXY».

```
esr(config)# interface tengigabitethernet 1/0/1
esr(config-if-te)# ip nat proxy-arp PROXY
```

Для того чтобы устройства локальной сети могли получить доступ к сети 200.10.0.0/24, на них должна быть настроена маршрутизация – адрес 21.12.2.1 должен быть назначен адресом шлюза.

Изменения конфигурации вступают в действие по команде применения.

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

Посмотреть активные трансляции можно с помощью команды:

```
esr# show ip nat translations
```

18.5 Настройка NTP

NTP (англ. *Network Time Protocol* — протокол сетевого времени) — сетевой протокол для синхронизации внутренних часов оборудования с использованием IP-сетей, использует для своей работы протокол UDP, учитывает время передачи и использует алгоритмы для достижения высокой точности синхронизации времени.

18.5.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Включить NTP.	**esr(config)# ntp enable**	
2	Задать IP-адрес NTP-сервера, либо участника NTP-синхронизации.	**esr(config)# ntp { pool | server | peer } { <IPV4> | <NAME> | IPV6}**	<IPV4> – IP-адрес назначения (шлюз), задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. <NAME> – DNS-имя сервера, задаётся строкой до 31 символа. <IPV6> – IP-адрес назначения (шлюз), задаётся в виде X:X:X:X::X, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF].
3	Включить отправку нескольких пакетов вместо одного при установке соединения.	**esr(config-ntp)# burst**	
4	Включить отправку нескольких пакетов вместо одного в случае разрыва соединения.	**esr(config-ntp)# iburst**	

Шаг	Описание	Команда	Ключи
5	Задать ключ для аутентификации (не обязательно).	**esr(config-ntp)# key <ID>**	<ID> – идентификатор ключа, задается в диапазоне [1..255].
6	Установить максимальное значение интервала времени между отправкой сообщений NTP-серверу (не обязательно).	**esr(config-ntp)# maxpoll <INTERVAL>**	<INTERVAL> – максимальное значение интервала опроса. Параметр команды используется как показатель степени двойки при вычислении длительности интервала в секундах, вычисляется путем возведения двойки в степень, заданную параметром команды, принимает значение [10..17]. Значение по умолчанию: 10 (2^{10}= 1024 секунды или 17 минут 4 секунды).
7	Установить минимальное значение интервала времени между отправкой сообщений NTP-серверу (не обязательно).	**esr(config-ntp)# minpoll <INTERVAL>**	<INTERVAL> – минимальное значение интервала опроса в секундах вычисляется путем возведения двойки в степень, заданную параметром команды, принимает значение [4..6]. Значение по умолчанию: 6 (2^{6}= 64 секунды или 1 минута 4 секунды).
8	Отметить данный NTP-сервер как предпочтительный (не обязательно).	**esr(config-ntp)# prefer**	
9	Определить список доверенных IP-адресов, с которыми может происходить обмен ntp-пакетами (не обязательно).	**esr(config)# ntp access-addresses <NAME>**	<NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.
10	Указать идентификатор ключа из профиля связки ключей (не обязательно).	**esr(config)# ntp authentication trusted-key <ID>**	<ID> – идентификатор ключа из профиля связки ключей.
11	Указать имя профиля связки ключей (не обязательно).	**esr(config)# ntp authentication key-chain <WORD>**	<WORD> – имя профиля связки ключей.
12	Активировать аутентификацию для NTP по ключу (не обязательно).	**esr(config)# ntp authentication enable**	

Шаг	Описание	Команда	Ключи
13	Включить режим приёма широковещательных сообщений NTP-серверов для глобальной конфигурации и всех существующих VRF (не обязательно).	**esr(config)# ntp broadcast-client enable**	
14	Задать значение кода DSCP для использования в IP-заголовке исходящих пакетов NTP-сервера (не обязательно).	**esr(config)# ntp dscp <DSCP>**	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 46.
15	Включить режим query-only, ограничивающий взаимодействие по NTP для определенного профиля IP-адресов (не обязательно).	**esr(config)# ntp object-group query-only <NAME>**	<NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.
16	Включить режим serve-only, ограничивающий взаимодействие по NTP для определенного профиля IP-адресов (не обязательно).	**esr(config)# ntp object-group serve-only <NAME>**	<NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.
17	Указать source-IP-адреса для NTP-пакетов для всех peer (не обязательно).	**esr(config)# ntp source address <ADDR>**	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
18	Задать текущие время и дату в ручном режиме (не обязательно).	**esr# set date <TIME> [<DAY> <MONTH> [<YEAR>]]**	<TIME> – устанавливаемое системное время, задаётся в виде HH:MM:SS, где: • HH – часы, принимает значение [0..23]; • MM – минуты, принимает значение [0 .. 59]; • SS – секунды, принимает значение [0 .. 59]. • <DAY> – день месяца, принимает значения [1..31]; <MONTH> – месяц, принимает значения [January/February/March/ April/May/June/July/August/ September/October/November/ December]; <YEAR> – год, принимает значения [2001..2037].

18.5.2 Пример настройки

Задача:

Настроить синхронизацию времени от NTP-сервера.

IP-адрес маршрутизатора ESR – 192.168.52.8,

IP-адрес NTP-сервера – 192.168.52.41.



Решение:

⚠ Предварительно нужно выполнить следующие действия:

- указать зону безопасности для интерфейса gi1/0/1;
- настроить IP-адрес для интерфейса gi1/0/1, чтобы обеспечить IP-связность с NTP-сервером.

Пример:

```
security zone untrust
exit
object-group service NTP
  port-range 123
exit
interface gigabitethernet 1/0/1
  security-zone untrust
  ip address 192.168.52.8/24
exit
security zone-pair untrust self
  rule 10
    action permit
    match protocol udp
    match destination-port object-group NTP
    enable
  exit
exit
```

Основной этап конфигурирования:

Включение синхронизации системных часов с удаленными серверами:

```
esr(config)# ntp enable
```

Настройка NTP-сервера:

```
esr-(config)# ntp server 192.168.52.41
```

Указать предпочтительность данного NTP-сервера (необязательно):

```
esr-1000(config-ntp)# prefer
```

Указать интервал времени между отправкой сообщений NTP-серверу:

```
esr(config-ntp)# minpoll 4
esr(config-ntp)# end
esr# commit
esr# confirm
```

Команда для просмотра текущей конфигурации протокола NTP:

```
esr# show ntp configuration
```

Команда для просмотра текущего состояния NTP-серверов (пиров):

```
esr# show ntp peers
```

19 Мониторинг

- Настройка Netflow
  - Алгоритм настройки
  - Пример настройки
- Настройка sFlow
  - Алгоритм настройки
  - Пример настройки
- Настройка SNMP
  - Алгоритм настройки
  - Пример настройки
- Настройка Zabbix-agent/proxy
  - Алгоритм настройки
  - Пример настройки zabbix-agent
  - Пример настройки zabbix-server
- Настройка Syslog
  - Алгоритм настройки
  - Пример настройки
- Проверка целостности
  - Процесс настройки
  - Пример конфигурации
- Настройка архивации конфигурации маршрутизатора
  - Процесс настройки
  - Пример конфигурации
- Настройка SLA
  - Алгоритм настройки SLA-теста
  - Настройка SLA-responder
  - Пример настройки ICMP-режима тестирования
  - Пример настройки UDP-режима тестирования
  - Алгоритм настройки параметров аутентификации
  - Пример конфигурации UDP-теста с аутентификацией по ключ-строке
  - Пример конфигурации UDP-теста с аутентификацией по связке ключей
  - Настройка пороговых значений
  - Измерение характеристик канала связи

19.1 Настройка Netflow

Netflow — сетевой протокол, предназначенный для учета и анализа трафика. Netflow позволяет передавать данные о трафике (адрес отправителя и получателя, порт, количество информации и др.) с сетевого оборудования (сенсора) на коллектор. В качестве коллектора может использоваться обычный сервер.

> В текущей реализации трафик, отброшенный маршрутизатором по каким-либо причинам, не будет учитываться в статистике.

19.1.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Задать версию Netflow-протокола.	**esr(config)# netflow version <VERSION>**	<VERSION> – версия Netflow-протокола: 5, 9 и 10.

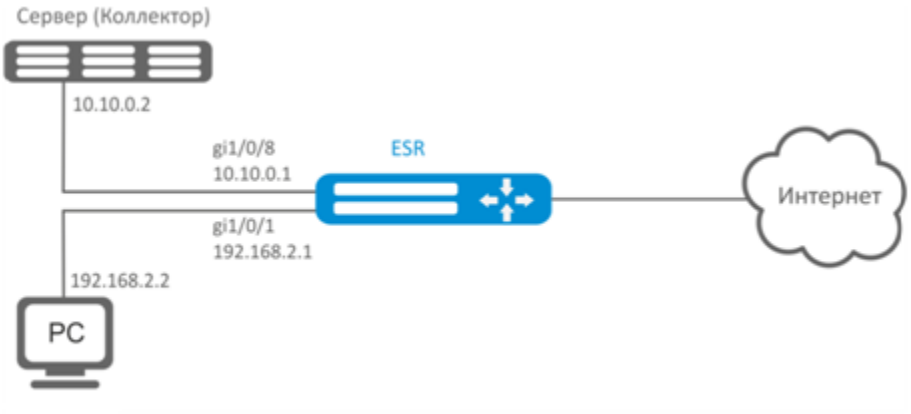
Шаг	Описание	Команда	Ключи
2	Установить максимальное количество наблюдаемых сессий.	**esr(config)# netflow max-flows <COUNT>**	<COUNT> – количество наблюдаемых сессий, принимает значение [10000..2000000]. Значение по умолчанию: 512000.
3	Установить интервал, по истечении которого информация об активных сессиях экспортируются на коллектор.	**esr(config)# netflow active-timeout <TIMEOUT>**	<TIMEOUT> – интервал времени, по истечении которого информация об активных сессиях экспортируются на коллектор, задается в секундах, принимает значение [5..36000]. Значение по умолчанию: 1800 секунд.
4	Установить интервал, по истечении которого информация об устаревших сессиях экспортируются на коллектор.	**esr(config)# netflow inactive-timeout <TIMEOUT>**	<TIMEOUT> – задержка перед отправкой информации об устаревших сессиях, задается в секундах, принимает значение [0..240]. Значение по умолчанию: 15 секунд.
5	Установить частоту отправки статистики на Netflow-коллектор.	**esr(config)# netflow refresh-rate <RATE>**	<RATE> – частота отправки статистики, задается в пакетах на поток, принимает значение [1..10000]. Значение по умолчанию: 10.
6	Активировать Netflow на маршрутизаторе.	**esr(config)# netflow enable**	
7	Создать коллектор Netflow и перейти в режим его конфигурирования.	**esr(config)# netflow collector <ADDR>**	<ADDR> – IP-адрес коллектора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
8	Установить порт Netflow-сервиса на сервере сбора статистики.	**esr(config-netflow-host)# port <PORT>**	<PORT> – номер UDP-порта, указывается в диапазоне [1..65535]. Значение по умолчанию: 2055.

Шаг	Описание	Команда	Ключи
9	Включить отправку статистики на Netflow-сервер в режим конфигурирования интерфейса/ туннеля/сетевого моста.	**esr(config-if-gi)# ip netflow export**	

19.1.2 Пример настройки

Задача:

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



Решение:

Предварительно необходимо настроить адресацию на интерфейсах.

Основной этап конфигурирования:

Укажем IP-адрес коллектора:

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

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

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

Активируем Netflow на маршрутизаторе:

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

Для просмотра статистики Netflow используется команда:

```
esr# show netflow statistics
```

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

19.2 Настройка sFlow

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

19.2.1 Алгоритм настройки

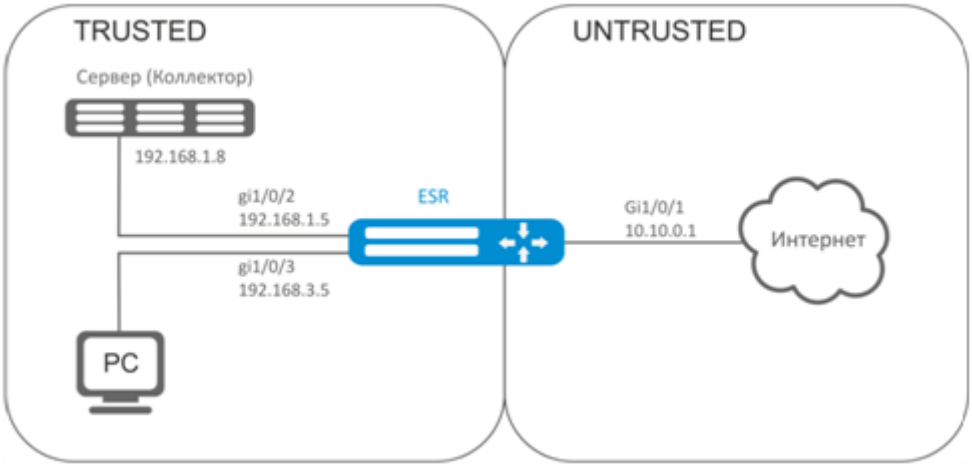
Шаг	Описание	Команда	Ключи
1	Установить частоту отправки пакетов пользовательского трафика в неизменном виде на sFlow-коллектор.	**esr(config)# sflow sampling-rate <RATE>**	<RATE> – частота отправки пакетов пользовательского трафика на коллектор, принимает значение [1..65535]. При значении частоты 10 на коллектор будет отправлен один пакет из десяти. Значение по умолчанию: 1000.
2	Установить интервал, по истечении которого происходит получение информации о счетчиках сетевого интерфейса.	**esr(config)# sflow poll-interval <TIMEOUT>**	<TIMEOUT> – интервал, по истечении которого происходит получение информации о счетчиках сетевого интерфейса, принимает значение [1..300] секунд. Значение по умолчанию: 10 секунд.
3	Создать коллектор sFlow и перейти в режим его конфигурирования.	**esr(config)# sflow collector <ADDR> [vrf <VRF>]**	<ADDR> – IP-адрес коллектора, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <VRF> – имя экземпляра VRF, задаётся строкой до 31 символа.
4	Указать порт sFlow-коллектора (необязательно).	**esr(config-sflow-host)# port <PORT>**	<PORT> – номер UDP-порта, указывается в диапазоне [1..65535].
5	Установить адрес sFlow-агента (необязательно).	**esr(config)# sflow agent-ip <ADDR>**	<ADDR> – IPv4/IPv6-адрес агента sFlow. Если команда не указана, то в качестве адреса агента будет использован случайный адрес из присутствующих в конфигурации.

Шаг	Описание	Команда	Ключи
6	Активировать сервис sFlow на маршрутизаторе.	**esr(config)# sflow enable**	
7	В режиме конфигурирования интерфейса/туннеля/сетевого моста включить отправку статистики sFlow.	**esr(config-if-gi)# ip sflow export**	

19.2.2 Пример настройки

Задача:

Организовать учет трафика между зонами trusted и untrusted.



Решение:

Для сетей ESR создадим две зоны безопасности:

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

Настроим сетевые интерфейсы и определим их принадлежность к зонам безопасности:

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

Укажем IP-адрес коллектора:

```
esr(config)# sflow collector 192.168.1.8
```

Включим экспорт статистики по протоколу sFlow для любого трафика в правиле «rule1» для направления TRUSTED-UNTRUSTED:

```
esr(config)# security zone-pair TRUSTED UNTRUSTED
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action sflow-sample
esr(config-zone-pair-rule)# match protocol any
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
```

Активируем sFlow на маршрутизаторе:

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

Настройка sFlow для учета трафика с интерфейса осуществляется аналогично настройке Netflow.

19.3 Настройка SNMP

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

19.3.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Включить SNMP-сервер.	**esr(config)# snmp-server**	

Шаг	Описание	Команда	Ключи
2	Определить community для доступа по протоколу SNMPv2c.	**esr(config)# snmp-server [encrypted] community <COMMUNITY> [<TYPE>] [{ <IP-ADDR> | <IPV6-ADDR> }] [client-list <OBJ-GROUP-NETWORK-NAME>] [<VERSION>] [view <VIEW-NAME>] [vrf <VRF>] [encrypt]**	encrypted – при добавлении данного параметра ввод названия сообщества <COMMUNITY> требуется производить в зашифрованном виде. <COMMUNITY> – сообщество для доступа по протоколу SNMP; <TYPE> – уровень доступа: • **ro** – доступ только для чтения; • **rw** – доступ для чтения и записи. <IP-ADDR> – IP-адрес клиента, которому предоставлен доступ, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> – IPv6-адрес клиента, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <OBJ-GROUP-NETWORK-NAME> – имя профиля IP-адресов, от которых обрабатываются snmp-запросы, задаётся строкой до 31 символа; <VERSION> – версия snmp, поддерживаемая данным community, принимает значения v1 или v2c; <VIEW-NAME> – имя профиля SNMP view, задаётся строкой до 31 символа; <VRF> – имя экземпляра VRF, из которого будет разрешен доступ, задается строкой до 31 символа. encrypt – при добавлении данного параметра название сообщества <COMMUNITY> будет отображаться в конфигурации устройства в зашифрованном виде.
3	Устанавливает значение переменной SNMP, содержащей контактную информацию.	**esr(config)# snmp-server contact <CONTACT>**	<CONTACT> – контактная информация, задается строкой до 255 символов.
4	Установить значение кода DSCP для использования в IP-заголовке исходящих пакетов SNMP-сервера (не обязательно).	**esr(config)# snmp-server dscp <DSCP>**	<DSCP> – значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 63.
5	Создать SNMPv3-пользователь.	**esr(config)# snmp-server user <NAME>**	<NAME> – имя пользователя, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
6	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.
7	Определить уровень доступа пользователя по протоколу SNMPv3.	**esr(config-snmp-user)# access <TYPE>**	<TYPE> – уровень доступа: • **ro** – доступ только для чтения; • **rw** – доступ для чтения и записи.
8	Определить режим безопасности пользователя по протоколу SNMPv3.	**esr(config-snmp-user)# authentication access <TYPE>**	<TYPE> – режим безопасности: • **auth** – используется только аутентификация; • **priv** – используется аутентификация и шифрование данных.
9	Определить алгоритм аутентификации SNMPv3-запросов.	**esr(config-snmp-user)# authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм шифрования: • **md 5** – пароль шифруется по алгоритму md5; • **sha 1** – пароль шифруется по алгоритму sha1.
10	Установить пароль для аутентификации SNMPv3-запросов.	**esr(config-snmp-user)# authentication key ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов; • **encrypted** – при указании команды задается зашифрованный пароль: <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).
11	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.
12	Указать vrf для SNMPv3-пользователя (не обязательно).	**esr-21(config-snmp-user)# ip vrf forwarding <VRF>**	<VRF> – имя экземпляра VRF, из которого будет разрешен доступ, задается строкой до 31 символа.

Шаг	Описание	Команда	Ключи
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: • **aes 128** – использовать алгоритм шифрования AES-128; • **des** – использовать алгоритм шифрования DES.
16	Установить пароль для шифрования передаваемых данных.	**esr(config-snmp-user)# privacy key ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<CLEAR-TEXT> – пароль, задаётся строкой от 8 до 16 символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).
17	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.
18	Включить передачу SNMP-уведомлений на указанный IP-адрес и перейти в режим настройки SNMP-уведомлений.	**esr(config)# snmp-server host { <IP-ADDR> | <IPV6-ADDR> } [vrf <VRF>]**	<IP-ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. <IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <VRF> – имя экземпляра VRF, в котором находится коллектор SNMP-уведомлений, задается строкой до 31 символа.
19	Определить порт коллектора SNMP-уведомлений на удаленном сервере (не обязательно).	**esr(config-snmp-host)# port <PORT>**	<PORT> – номер UDP-порта, указывается в диапазоне [1..65535]. Значение по умолчанию: 162.

Шаг	Описание	Команда	Ключи
20	Установить IP-адрес для отправки уведомлений на удаленный сервер.	**esr(config-snmp-host)# source-address { <ADDR> | <IPV6-ADDR> | object-group <NETWORK_OBJ_GROUP_NAME> }**	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве source address. Значение по умолчанию: IPv4/IPv6 – адрес интерфейса, ближайшего к удаленному SNMP-серверу.
21	Установить интерфейс или туннель маршрутизатора, IPv4/IPv6-адрес которого будет использоваться для отправки уведомлений на удаленный сервер.	**esr(config-snmp-host)# source-interface { <IF> | <TUN> }**	<IF> – имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора; <TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора.
22	Разрешить отправку SNMP-уведомлений различных типов.	**esr(config)# snmp-server enable traps <TYPE>**	<TYPE> – тип фильтруемых сообщений. Может принимать значения: config, entry, entry-sensor, environment, envmon, files-operations, flash, flash-operations, interfaces, links, ports, screens, snmp, syslog. Дополнительные параметры зависят от типа фильтра. См. справочник команд CLI.
23	Создать профиль snmp view, позволяющий разрешать или запрещать доступ к тем или иным OID для community (SNMPv2) и user (SNMPv3).	**esr(config)# snmp-server view <VIEW-NAME>**	<VIEW-NAME> – имя профиля SNMP view, задаётся строкой до 31 символа.

19.3.2 Пример настройки

Задача:

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



Решение:

Предварительно нужно выполнить следующие действия:

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

Основной этап конфигурирования:

Включаем SNMP-сервер:

```
esr(config)# snmp-server
```

Создаем пользователя SNMPv3:

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

Определим режим безопасности:

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

Определим алгоритм аутентификации для SNMPv3-запросов:

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

Установим пароль для аутентификации SNMPv3-запросов:

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

Определим алгоритм шифрования передаваемых данных:

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

Установим пароль для шифрования передаваемых данных:

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

Активируем SNMPv3-пользователя:

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

Определяем сервер-приемник Trap-PDU-сообщений:

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

19.4 Настройка Zabbix-agent/proxy

Zabbix-agent — агент, предназначенный для 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 сервис, способный собирать данные мониторинга с одного или нескольких наблюдаемых устройств и отправлять эту информацию Zabbix-серверу.

Текущая версия установленного агента (прокси) – 6.0.39.

19.4.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перейти в контекст настройки агента/proxy.	**esr(config-zabbix-agent)# zabbix-agent** **esr(config-zabbix-proxy)# zabbix-proxy**	
2	Указать имя узла сети (опционально). Для активного режима имя должно совпадать с именем узла сети на Zabbix-сервере.	**esr(config-zabbix-agent)# hostname <WORD>** **esr(config-zabbix-proxy)# hostname <WORD>**	<WORD> – имя узла сети, задается строкой до 255 символов.
3	Указать адрес Zabbix-сервера.	**esr(config-zabbix-agent)# server <ADDR>** **esr(config-zabbix-proxy)# server <ADDR>**	<ADDR> – IP-адрес сервера, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
4	Указать адрес сервера для активных проверок (при использовании активного режима).	**esr(config-zabbix-agent)# active-server <ADDR> <PORT>** **esr(config-zabbix-proxy)# active-server <ADDR> <PORT>**	<ADDR> – IP-адрес сервера, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. <PORT> – порт сервера, задается в диапазоне [1..65535]. Значение по умолчанию 10051.
5	Указать порт, который будет слушать агент/прокси (не обязательно).	**esr(config-zabbix-agent)# port <PORT>** **esr(config-zabbix-proxy)# port <PORT>**	<PORT> – порт, который слушает zabbix-агент/прокси, задается в диапазоне [1..65535]. Значение по умолчанию: 10050.

Шаг	Описание	Команда	Ключи
6	Разрешить выполнение удаленных команд zabbix-агентом (при использовании активного режима).	**esr(config-zabbix-agent)# remote-commands**	
7	Указать адрес, с которого будет осуществляться взаимодействием с сервером (не обязательно).	**esr(config-zabbix-agent)# source-address <ADDR>** **esr(config-zabbix-proxy)# source-address <ADDR>**	<ADDR> – IP-адрес сервера, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Значение по умолчанию: ближайший адрес по маршрутизации.
8	Указать максимальное время на обработку удаленных команд (не обязательно).	**esr(config-zabbix-agent)# timeout <TIME>** **esr(config-zabbix-proxy)# timeout <TIME>**	<TIME> – время ожидания, определяется в секундах [1..30]. Значение по умолчанию 3. Рекомендуется устанавливать максимальное значение, т. к. некоторые команды могут выполняться дольше значения по умолчанию. Если за указанное время команда не будет выполнена, то обработка команды будет прекращена.
9	Указать место хранения базы данных для Zabbix-proxy (не обязательно).	**esr(config-zabbix-proxy)# database <PATH>**	<PATH> – место хранения базы данных Zabbix-proxy. По умолчанию база данных Zabbix хранится в энергозависимой памяти маршрутизатора.
10	Указать интервал запроса конфигурации от Zabbix-сервера (не обязательно).	**esr(config-zabbix-proxy)# config-retrieve <TIME>**	<TIME> – время между опросами в секундах, принимает значения [1..604800]. Значение по умолчанию: 60.
11	Включить функционал агента/прокси.	**esr(config-zabbix-agent)# enable** **esr(config-zabbix-proxy)# enable**	
12	Разрешить из соответствующей зоны безопасности firewall обращение к маршрутизатору (в зону self) по TCP-портам 10050, 10051. См. раздел Конфигурирование Firewall.		

19.4.2 Пример настройки zabbix-agent



Задача:

Настроить взаимодействие между агентом и сервером для выполнения удаленных команд с сервера.

Решение:

В контексте настройки агента укажем адрес Zabbix-сервера и адрес, с которого будет осуществляться взаимодействие с сервером:

```
esr(config-zabbix-agent)# server 192.168.32.101
esr(config-zabbix-agent)# source-address 192.168.39.170
```

Для активации активного режима укажем hostname, active-server, а также включим выполнение удаленных команд:

```
esr(config-zabbix-agent)# hostname ESR-agent
esr(config-zabbix-agent)# active-server 192.168.32.101
esr(config-zabbix-agent)# remote-commands
```

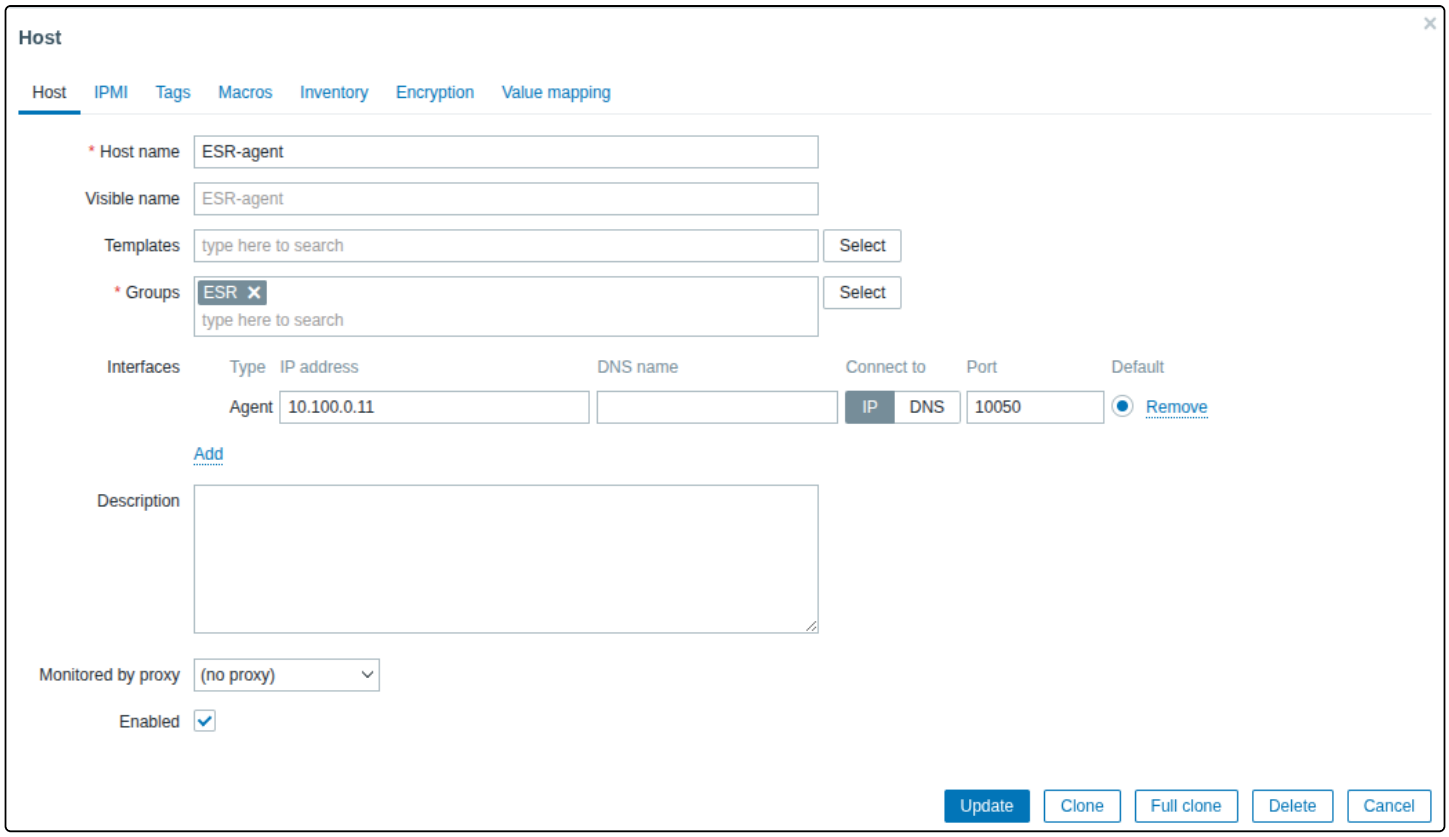
Зададим время выполнения удаленных команд и активируем функционал агента:

```
esr(config-zabbix-agent)# timeout 30
esr(config-zabbix-agent)# enable
```

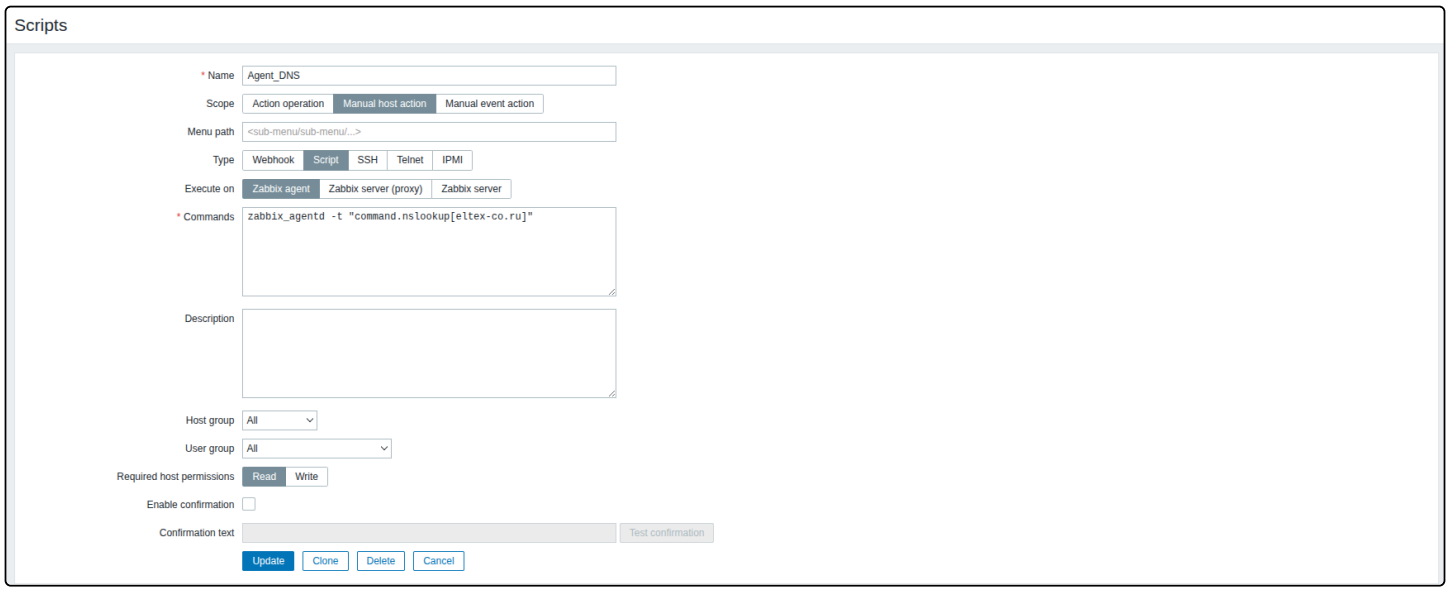
19.4.3 Пример настройки zabbix-server

Перед настройкой необходимо убедиться, что сервер и агент используют синхронизированное время UTC с учетом локальных часовых поясов.

Создадим узел сети:



Создадим скрипт (Администрирование -> Скрипты -> Создать скрипт)



Маршрутизаторы ESR поддерживают выполнение следующих привилегированных команд:

- **Ping**

```
zabbix_agentd -t "command.ping[ domain.local -c 15]"
```

Клиент (ESR), получивший данную команду от сервера, выполнит **ping** до заданного узла 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_agentd -t "command.ping_vrf[Backup, -c 15]"
```

Вышеупомянутая команда будет выполнена в заданном VRF с именем "Backup".

- **Fping**

```
zabbix_agentd -t "command.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_agentd -t "command.fping_vrf[Backup, domain.local]"
```

Команда будет выполнена в заданном VRF с именем "Backup".

- **Traceroute**

```
zabbix_agentd -t "command.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_agentd -t "command.traceroute_vrf[VRF, 192.168.32.101]"
```

- **Iperf**

```
zabbix_agentd -t "command.iperf[-c 192.168.32.101 -u -t 5 -i 1]"
```

Клиент (ESR), получивший данную команду от сервера, выполнит iperf до заданного сервера (в нашем примере до 192.168.32.101) и вернет результат серверу.

- **Iperf3**

```
zabbix_agentd -t "command.iperf3[-c 192.168.32.101 -t 5 -i 1]"
```

- **Iperf в VRF**

```
zabbix_agentd -t "command.iperf_vrf[VRF, -c 192.168.32.101 -t 5 -i 1]"
```

- **Iperf3 в VRF**

```
zabbix_agentd -t "command.iperf3_vrf[VRF,-c 192.168.32.101 -t 5 -i 1 ]"
```

- **Nslookup**

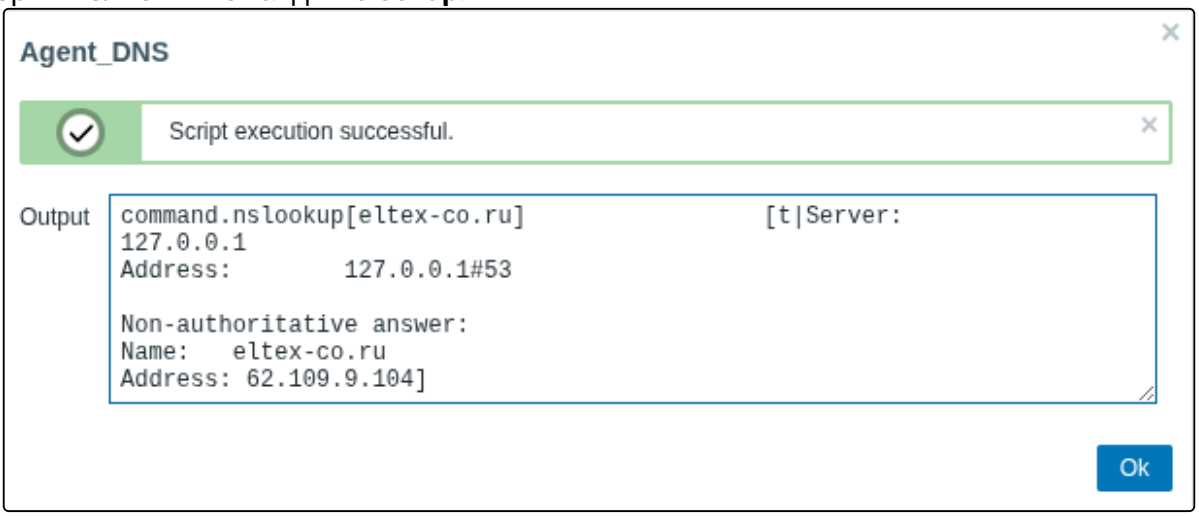
```
zabbix_agentd -t "command.nslookup[domain_name.local]"
```

Клиент (ESR), получивший данную команду от сервера, выполнит **nslookup** и вернет результат серверу.

- **Nslookup в VRF**

```
zabbix_agentd -t "command.nslookup_vrf[VRF,domain_name.local]"
```

Пример выполнения команды **nslookup**:



19.5 Настройка Syslog

Syslog (англ. *System Log* — системный журнал) — стандарт отправки и регистрации сообщений о происходящих в системе событиях, используется в сетях, работающих по протоколу IP.

19.5.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Включить отправку syslog-сообщений на snmp-сервер в виде snmp-trap.	**esr(config)# syslog snmp**	
2	Активировать или деактивировать отправку на snmp-сервер событий работы отдельных процессов маршрутизатора (не обязательно).	**esr(config-syslog-snmp)# match [not] process-name <PROCESS-NAME>**	<PROCESS-NAME> – см. в справочнике команд CLI. Если описаны разрешающие критерии (match process-name) – логируются только сообщения указанных процессов. Если указаны запрещающие критерии (match not process-name) – логируются сообщения всех не запрещенных процессов. По умолчанию разрешено логирование сообщений всех процессов.

Шаг	Описание	Команда	Ключи
3	Указать уровень важности сообщений, которые будут отправляться на snmp-сервер.	**esr(config-syslog-snmp)# severity <SEVERITY>**	<SEVERITY> – уровень важности сообщения, принимает значения (в порядке убывания важности): • **emerg** – в системе произошла критическая ошибка, система неработоспособна; • **alert** – сигналы тревоги, необходимо немедленное вмешательство персонала; • **crit** – критическое состояние системы, сообщение о событии; • **error** – сообщения об ошибках; • **warning** – предупреждения, неаварийные сообщения; • **notice** – сообщения о важных системных событиях; • **info** – информационные сообщения системы; • **debug** – отладочные сообщения, предоставляют пользователю информацию для корректной настройки системы; • **none** – отключает вывод syslog-сообщений.
4	Включить отображение syslog-сообщений при удаленных подключениях (Telnet, SSH) (не обязательно).	**esr(config)# syslog monitor**	
5	Активировать или деактивировать отображение при удаленных подключениях событий работы отдельных процессов маршрутизатора (не обязательно).	**esr(config-syslog-monitor)# match [not] process-name <PROCESS-NAME>**	<PROCESS-NAME> – описано во 2 пункте.
6	Указать уровень важности сообщений, которые будут отображаться при удаленных подключениях.	**esr(config-syslog-monitor)# severity <SEVERITY>**	<SEVERITY> – описано в 3 пункте.
7	Включить отображение syslog-сообщений при консольном подключении (не обязательно).	**esr(config)# syslog console**	

Шаг	Описание	Команда	Ключи
8	Активировать или деактивировать отображение при консольном подключении событий работы отдельных процессов маршрутизатора (не обязательно).	**esr(config-syslog-console)# match [not] process-name <PROCESS-NAME>**	<PROCESS-NAME> – описано во 2 пункте.
9	Указать уровень важности сообщений, которые будут отображаться при консольном подключении.	**esr(config-syslog-console)# severity <SEVERITY>**	<SEVERITY> – описано в 3 пункте.
10	Указать категорию сообщений, которые будут сохраняться в локальный syslog-файл или отправляться на удаленный syslog-сервер.	**esr(config)# syslog facility <FACILITY>**	<FACILITY> – категория сообщений, принимает значения [local0..local7].
11	Включить сохранение сообщений syslog в указанный файл журнала (при необходимости ведения локального syslog-файла).	**esr(config)# syslog file <NAME>**	<NAME> – имя файла, в который будет производиться запись сообщений заданного уровня, задается строкой до 31 символа.
12	Активировать или деактивировать сохранение в локальный syslog-файл событий работы отдельных процессов маршрутизатора (не обязательно).	**esr(config-syslog-file)# match [not] process-name <PROCESS-NAME>**	<PROCESS-NAME> – описано во 2 пункте.
13	Указать уровень важности сообщений, которые будут сохраняться в локальный syslog-файл.	**esr(config-syslog-file)# severity <SEVERITY>**	<SEVERITY> – описано в 3 пункте.
14	Указать максимальный размер файла журнала (не обязательно).	**esr(config)# syslog file-size <SIZE>**	<SIZE> – размер файла, принимает значение [10..10000000] Кбайт.
15	Задать максимальное количество файлов, сохраняемых при ротации (не обязательно).	**esr(config)# syslog max-files <NUM>**	<NUM> – максимальное количество файлов, принимает значения [1.. 1000].
16	Включить передачу сообщений syslog на удаленный syslog-сервер (при необходимости отправки сообщений на удаленный syslog-сервер).	**esr(config)#syslog host <HOSTNAME>**	<HOSTNAME> – наименование syslog-сервера, задаётся строкой до 31 символа. Используется только для идентификации сервера при конфигурировании. Значение «all» используется в команде no syslog host для удаления всех syslog-серверов;

Шаг	Описание	Команда	Ключи
17	Указать, что использовать в качестве значения поля HOSTNAME при передачи сообщений на удаленный syslog-сервер (не обязательно).	**esr(config-syslog-host)# identifier { fqdn | ip | hostname }**	fqdn – использовать в качестве значения полное имя устройства: hostname.domain_name. Используется только вместе с настроенным domain name; ip – использовать в качестве значения IP-адрес интерфейса устройства. Если не указан source-address, то в качестве значения будет использован IP-адрес интерфейса, за которым находится удаленный syslog-сервер; hostname – использовать в качестве значения имя устройства.
18	Указать IPv4/IPv6-адрес удаленного syslog-сервера.	**esr(config-syslog-host)# remote-address { <ADDR> | <IPV6-ADDR> }**	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
19	Указать IPv4/IPv6-адрес маршрутизатора, от которого будут отправляться пакеты на удаленный syslog-сервер (не обязательно).	**esr(config-syslog-host)# source-address { <ADDR> | <IPV6-ADDR> | object-group <NETWORK_OBJ_GROUP_NAME> }**	<ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве source address; Значение по умолчанию: IPv4/ IPv6-адрес интерфейса, с которого отправляется пакеты на удаленный syslog-сервер.

Шаг	Описание	Команда	Ключи
20	Указать транспортный протокол для передачи пакетов на удаленный syslog-сервер (не обязательно).	**esr(config-syslog-host)# transport { tcp | udp }**	<VRF> – имя экземпляра VRF, в котором доступен удаленный syslog-сервер, задается строкой до 31 символа; Значение по умолчанию: отсутствует (глобальная таблица маршрутизации).
21	Указать имя экземпляра VRF, в рамках которого будут отправляться пакеты на удаленный syslog-сервер (не обязательно).	**esr(config-syslog-host)# vrf <VRF>**	
22	Указать номер TCP/UDP-порта, на который будут отправляться пакеты с syslog-сообщениями (не обязательно).	**esr(config-syslog-host)# port <PORT>**	<PORT> – номер TCP/UDP-порта, на который будут отправляться пакеты с syslog-сообщениями. Значение по умолчанию: 514.
23	Активировать или деактивировать отправку на удаленный syslog-сервер событий работы отдельных процессов маршрутизатора (не обязательно).	**esr(config-syslog-host)# match [not] process-name <PROCESS-NAME>**	<PROCESS-NAME> – описано во 2 пункте.
24	Указать уровень важности сообщений, которые будут сохраняться в локальный syslog-файл.	**esr(config-syslog-host)# severity <SEVERITY>**	<SEVERITY> – описано в 3 пункте.
25	Включить вывод отладочных сообщений во время загрузки устройства (не обязательно).	**esr(config)#syslog reload debugging**	
26	Включить процесс логирования введенных команд пользователя на локальный syslog-сервер (не обязательно).	**esr(config)# syslog cli-commands**	
27	Включить нумерацию сообщений (не обязательно).	**esr(config)#syslog sequence-numbers**	
28	Включить точность даты сообщений до миллисекунд (не обязательно).	**esr(config)#syslog timestamp msec**	
29	Включить отображение имени процесса, который сформировал сообщение (не обязательно).	**esr(config)#syslog program-name**	

Шаг	Описание	Команда	Ключи
30	Включить регистрацию неудачных аутентификаций (не обязательно).	**esr(config)#logging login on-failure**	
31	Включить регистрацию изменений настроек системы аудита (не обязательно).	**esr(config)#logging syslog configuration**	
32	Включить регистрацию изменений настроек пользователя (не обязательно).	**esr(config)#logging userinfo**	

19.5.2 Пример настройки

Задача:

Настроить отправку сообщений для следующих системных событий:

- неудачная аутентификация пользователя;
- внесены изменения в конфигурацию логирования системных событий;
- старт/остановка системного процесса;
- внесены изменения в профиль пользователей.

IP-адрес маршрутизатора ESR – 192.168.52.8, IP-адрес Syslog-сервера – 192.168.52.41. Использовать параметры по умолчанию для отправки сообщений – протокол UDP порт 514.



Решение:

Предварительно нужно выполнить следующие действия:

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

Основной этап конфигурирования:

Создадим файл на маршрутизаторе для системного журнала, уровень сообщений для журналирования – info:

```
esr(config)# syslog file tmpsys:syslog/ESR
esr(config-syslog-file)# severity info
esr(config-syslog-file)# exit
```

Укажем IP-адрес и параметры удаленного syslog-сервера:

```
esr(config)# syslog host SERVER
esr(config-syslog-host)# remote-address 192.168.52.41
esr(config-syslog-host)# severity info
esr(config-syslog-host)# exit
```

Зададим логирование неудачных попыток аутентификации:

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

Зададим логирование изменений конфигурации syslog:

```
esr(config)# logging syslog configuration
```

Зададим логирование старта/остановки системных процессов:

```
esr(config)# logging service start-stop
```

Зададим логирование внесений изменений в профиль пользователей:

```
esr(config)# logging userinfo
```

Изменения конфигурации вступят в действие после применения:

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

Посмотреть текущую конфигурацию системного журнала:

```
esr# show syslog configuration
```

Посмотреть записи системного журнала:

```
esr# show syslog ESR
```

19.6 Проверка целостности

Проверка целостности подразумевает проверку целостности хранимых исполняемых файлов.

19.6.1 Процесс настройки

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

19.6.2 Пример конфигурации

Задача:

Проверить целостность файловой системы.

Решение:

Запускаем проверку целостности:

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

19.7 Настройка архивации конфигурации маршрутизатора

На маршрутизаторах ESR предусмотрена функция локального и/или удаленного копирования конфигурации по таймеру или при применении конфигурации.

19.7.1 Процесс настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим настройки параметров резервирования конфигурации.	**esr(config)# archive**	
2	Установить тип сохранения резервных конфигураций маршрутизатора (не обязательно).	**esr(config-ahchive)# type <TYPE>**	<TYPE> – тип сохранения резервных конфигураций маршрутизатора. Принимает значения: • **local;** • **remote;** • **both.** Значение по умолчанию: remote.
3	Включить режим резервирования конфигурации по таймеру (не обязательно).	**esr(config-ahchive)# auto**	
4	Включить режим резервирования конфигурации после каждого успешного применения конфигурации (не обязательно).	**esr(config-ahchive)# by-commit**	

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..525600]. Значение по умолчанию: 720 минут.
7	Задать максимальное количество локально сохраняемых резервных копий конфигураций (не обязательно, актуально при типах local и both).	**esr(config-ahchive)# count-backup <NUM>**	<NUM> – максимальное количество локально сохраняемых резервных копий конфигураций. Принимает значения в диапазоне [1..100]. Значение по умолчанию: 1.

19.7.2 Пример конфигурации

Задача:

Настроить локальное и удаленное резервное копирование конфигурации маршрутизатора 1 раз в сутки и при успешном изменении конфигурации. Удаленные копии необходимо отправлять на tftp-сервер 172.16.252.77 в подпапку esr-example. Максимальное количество локальных копий – 30.

Решение:

Для успешной работы удаленной архивации конфигураций, между маршрутизатором и сервером должна быть организована IP-связность, настроены разрешения на прохождение tftp-трафика по сети и сохранения файлов на сервере.

Основной этап конфигурирования:

Перейти в режим конфигурирования резервного копирования конфигураций:

```
esr# configure
esr(config)# archive
```

Задать режим локального и удаленного резервного копирования конфигурации:

```
esr(config-archive)# 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. Посмотреть можно командой:

```
esr(config)# show archive configuration
```

19.8 Настройка SLA

IP SLA (Internet Protocol Service Level Agreement) — технология измерения активных компьютерных сетей. На маршрутизаторах ESR, сервис IP SLA использует непрерывную генерацию трафика для тестирования качественных и количественных характеристик каналов связи в сети передачи данных на базе протокола IP. Два основных понятия при рассмотрении сервиса IP-SLA: SLA-agent (SLA-sender) – тестирующий маршрутизатор, отправляющий запросы; SLA-responder – удаленный/тестируемый маршрутизатор или произвольный хост, принимающий запросы от SLA-sender.

19.8.1 Алгоритм настройки SLA-теста

Шаг	Описание	Команда	Ключи
1	Создать в системе новый SLA-тест и перейти в режим его конфигурирования.	**esr(config)# ip sla test <NUM>**	<NUM> – номер SLA-теста, задается в диапазоне [1..10000].
2	Задать режим тестирования канала связи и параметры тестирования. Разные режимы подразумевают различный набор параметров, которые необходимо указать. Для одного SLA-теста возможно указать только один набор параметров тестирования.		

Шаг	Описание	Команда	Ключи
2.1	Конфигурирование ICMP-режима тестирования канала связи.	**esr(config-sla-test)# icmp-echo { <DST-ADDRESS> | <IPV6-DST-ADDRESS> } { source-ip { <SRC-ADDRESS> <IPV6-SRC-ADDRESS> | object-group <NETWORK_OBJ_GROUP_NAME> } | source-interface { <IF> | <TUN> } } [interval <INTERVAL>] [num-packets <NUM-PACKETS>]**	<DST-ADDRESS> – IPv4-адрес, на который будут направляться тестовые пакеты. Задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-DST-ADDRESS> – IPv6-адрес, на который будут направляться тестовые пакеты. Задаётся в виде X:X:X:X::X, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF]; <SRC-ADDRESS> – IPv4-адрес, с которого будут отправляться тестовые пакеты. Задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-SRC-ADDRESS> – IPv6-адрес, с которого будут отправляться тестовые пакеты. Задаётся в виде X:X:X:X::X, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF]; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве source address; <IF> – тип и идентификатор интерфейса, IP-адрес которого будет использоваться в качестве адреса источника пакетов. Задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора; <TUN> – тип и идентификатор туннеля, IP-адрес которого будет использоваться в качестве адреса источника пакетов. Задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора;

Шаг	Описание	Команда	Ключи
		esr(config-sla-test)# icmp-jitter <DST-ADDRESS> { source-ip { <SRC-ADDRESS> | object-group <NETWORK_OBJ_GROUP_NAME> } | source-interface { <IF> | <TUN> } } [interval <INTERVAL>] [num-packets <NUM-PACKETS>]	<INTERVAL> – интервал между отправкой каждого последующего тестового пакета. Может принимать значение [1..255] миллисекунд; <NUM-PACKETS> – количество тестовых пакетов, отправляемых в рамках одной сессии тестирования. Может принимать значение [1..100000].

Шаг	Описание	Команда	Ключи
2.2	Конфигурирование UDP-режима тестирования канала связи. Для корректной работы UDP-режим предполагает сконфигурированный Eltex SLA-responder на удаленной стороне.	**esr(config-sla-test)# udp-jitter { <DST-ADDRESS> | <IPV6-DST-ADDRESS> } <DST-PORT> { source-ip { <SRC-ADDRESS> | <IPV6-SRC-ADDRESS> | object-group <NETWORK_OBJ_GROUP_NAME> } | source-interface { <IF> | <TUN> } } [source-port <SRC-PORT>] [interval <INTERVAL>] [num-packets <NUM-PACKETS>]**	<DST-ADDRESS> – IPv4-адрес, на который будут направляться тестовые пакеты. Задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-DST-ADDRESS> – IPv6-адрес, на который будут направляться тестовые пакеты. Задаётся в виде X:X:X:X::X, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF]; <DST-PORT> – номер UDP-порта назначения тестовых пакетов, принимает значения [1..65535]; <SRC-ADDRESS> – IPv4-адрес, с которого будут отправляться тестовые пакеты. Задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-SRC-ADDRESS> – IPv6-адрес, с которого будут отправляться тестовые пакеты. Задаётся в виде X:X:X:X::X, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF]; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве source address; <IF> – тип и идентификатор интерфейса, с IP-адреса которого будут отправляться тестовые пакеты. Задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора; <TUN> – тип и идентификатор туннеля, с IP-адреса которого будут отправляться тестовые пакеты. Задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора;

Шаг	Описание	Команда	Ключи
			<SRC-PORT> – номер UDP-порта источника тестовых пакетов, принимает значения [1..65535]; <INTERVAL> – интервал между отправкой каждого последующего тестового пакета. Может принимать значение [1..255] миллисекунд; <NUM-PACKETS> – количество тестовых пакетов, отправляемых в рамках одной сессии тестирования. Может принимать значение [1..100000].

Шаг	Описание	Команда	Ключи
2.3	Конфигурирование TCP-режима тестирования канала связи.	**esr(config-sla-test)# tcp-connect { <DST-ADDRESS> | <IPV6-DST-ADDRESS>} { source-ip { <SRC-ADDRESS> | <IPV6-SRC-ADDRESS> | object-group <NETWORK_OBJ_GROUP_NAME> } | source-interface { <IF> | <TUN> } } [source-port <SRC-PORT>]**	<DST-ADDRESS> – IPv4-адрес, на который будут направляться тестовые пакеты. Задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-DST-ADDRESS> – IPv6-адрес, на который будут направляться тестовые пакеты. Задаётся в виде X:X:X:X::X, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF]; <DST-PORT> – номер TCP-порта назначения тестовых пакетов, принимает значения [1..65535]; <SRC-ADDRESS> – IPv4-адрес, с которого будут отправляться тестовые пакеты. Задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-SRC-ADDRESS> – IPv6-адрес, с которого будут отправляться тестовые пакеты. Задаётся в виде X:X:X:X::X, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF]; <NETWORK_OBJ_GROUP_NAME> – список адресов, которые будут использоваться в качестве source address; <IF> – тип и идентификатор интерфейса, с IP-адреса которого будут отправляться тестовые пакеты. Задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора; <TUN> – тип и идентификатор туннеля, с IP-адреса которого будут отправляться тестовые пакеты. Задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора;

Шаг	Описание	Команда	Ключи
			<SRC-PORT> – номер TCP-порта источника тестовых пакетов, принимает значения [1..65535].
3	Установить значение dscp, которым будут помечаться тестовые пакеты (необязательно).	**esr(config-sla-test)# dscp <DSCP>**	<DSCP> – значение кода DSCP, может принимать значение [0..63].
4	Установить частоту перезапуска SLA-теста (необязательно).	**esr(config-sla-test)# frequency <TIME>**	<TIME> – частота перезапуска SLA-теста, может принимать значение [1..604800] секунд.
5	Установить размер исходящего тестового пакета (необязательно).	**esr(config-sla-test)# packet-size <SIZE>**	<SIZE> – размер тестового пакета SLA-теста, может принимать значение [70..10000] байт.
6	Установить максимальное время ожидания ответа от удаленной стороны на тестовый пакет (необязательно).	**esr(config-sla-test)# timeout <TIME>**	<TIME> – время ожидания ответного пакета от удаленной стороны, может принимать значение [1..4294967295] миллисекунд.
7	Установить значение TTL для исходящих пакетов SLA-теста (необязательно).	**esr(config-sla-test)# ttl <TTL>**	<TTL> – значение TTL, может принимать значение [1..255].
8	Указать экземпляр VRF,в адресном пространстве которого должен работать SLA-тест (если подразумевается конфигурацией).	**esr(config-sla-test)# vrf <VRF>**	<VRF> – имя экземпляра VRF, задаётся строкой до 31 символа.

Шаг	Описание	Команда	Ключи
9	Установить пороговые значения характеристик канала (необязательно).	**esr(config-sla-test)# thresholds <TYPE> { high <VALUE_H> | low <VALUE_L> | forward [{ high <VALUE_H> | low <VALUE_L> }] | reverse [{ high <VALUE_H> | low <VALUE_L> }] } [from-last <NUM-CHECK> { all | over <NUM-LIMIT> }]**	<TYPE> – тип отслеживаемой величины, может принимать значения: • delay – допустимые значения задержек в канале; • jitter – допустимые значения джиттера в канале; • losses – допустимые значения потерь пакетов в канале. <VALUE_H> – верхнее пороговое значение, при пересечении которого сессия тестирования будет считаться проваленной; <VALUE_L> – нижнее пороговое значение, при пересечении которого сессия тестирования будет вновь считаться успешной; <NUM-CHECKS> – количество итераций теста, в течение которых проверяется соблюдение пороговых значений характеристик канала; <NUM-LIMIT> – количество итераций теста с превышением установленного порога, после превышения которого тест считается проваленным.
10	Запретить фрагментацию тестовых пакетов (необязательно).	**esr(config-sla-test)# disallow-fragmentation**	
11	Установить количество записей о результатах тестирования, отображающихся в истории измерений (необязательно).	**esr(config-sla-test)# history <SIZE>**	<SIZE> – число сохраняемых результатов, может принимать значение [1..1000].
12	Задать описание SLA-теста (необязательно).	**esr(config-sla-test)# description <DESCRIPTION>**	<DESCRIPTION> – описание SLA-теста, задается строкой до 255 символов.
13	Настроить параметры аутентификации, согласно алгоритму настройки параметров аутентификации (только для UDP-тестов, необязательно).		

Шаг	Описание	Команда	Ключи
14	Активировать SLA-тест.	**esr(config-sla-test)# enable**	
15	Выйти из параметров конфигурирования SLA-теста.	**esr(config-sla-test)# exit**	
16	Задать расписание запуска активированных SLA-тестов.	**esr(configt)# ip sla schedule { <TEST-NUMBER> | all } [life { <LIFE-TIME> | forever }] [start-time { <MONTH> <DAY> <TIME> | now }]**	<TEST-NUMBER> – номер SLA-теста, может принимать значение [1..10000]. При использовании ключа "all" вместо номера, устанавливается расписание работы для всех активированных SLA-тестов; <LIFE-TIME> – время жизни теста, может принимать значение [1..2147483647] секунд; forever – время жизни теста не ограничено; <TIME> – время начала теста, задаётся в виде HH:MM:SS, где: HH – часы, может принимать значение [0..23]; MM – минуты, может принимать значение [0..59]; SS – секунды, может принимать значение [0..59]; <MONTH> – месяц начала теста, принимает значения [January / February / March / April / May / June / July / August / September / October / November / December]; <DAY> – день месяца начала теста, может принимать значение [1..31]; now – начать тест немедленно.

Шаг	Описание	Команда	Ключи
17	Активировать вывод информационных сообщений групп событий (необязательно). Каждая из групп активируется отдельно.	**esr(config)# ip sla logging <TYPE>**	<TYPE> – название группы информационных сообщений, может принимать значения: • error – отображение сообщений об ошибках в работе SLA-тестов, причинах их провала, а также ошибок в работе SLA-responder (если таковой сконфигурирован в системе); • delay – отображение сообщений о превышении/нормализации значений, установленных в thresholds delay; • jitter – отображение сообщений о превышении/нормализации значений, установленных в thresholds jitter; • losses – отображение сообщений о превышении/нормализации значений, установленных в thresholds losses; • status – отображение сообщений о смене статуса SLA-теста.
18	Активировать сервис SLA-agent.	**esr(config)# ip sla**	

19.8.2 Настройка SLA-responder

Шаг	Описание	Команда	Ключи
1	В режиме конфигурирования интерфейса на маршрутизаторе, который является удаленной стороной SLA-теста, активировать SLA-responder.	**esr(config-if-gi)# ip sla responder <TYPE>** **esr(config-if-gi)# ipv6 sla responder eltex**	<TYPE> – название целевой платформы SLA-agent, может принимать значения: • eltex – функционал Eltex SLA-responder для Eltex SLA-agent; • cisco – функционал Cisco SLA-responder для Cisco SLA-agent.
2	Установить UDP-порт, на котором будет идти прослушивание запросов аутентификации от SLA-agent (если при конфигурировании SLA-теста был указан порт прохождения контрольной фазы, отличный от порта по умолчанию).		

Шаг	Описание	Команда	Ключи
2.1	Конфигурирование UDP-порта для прослушивания запросов аутентификации от Eltex SLA-agent (необязательно).	**esr(config-if-gi)# ip sla responder eltex port <PORT>** **esr(config-if-gi)# ipv6 sla responder eltex port <PORT>**	<PORT> – номер UDP-порта, может принимать значение [1..65535].
2.2	Конфигурирование UDP-порта для прослушивания запросов аутентификации от Cisco SLA-agent (необязательно).	**esr(config-if-gi)# ip sla responder cisco port <PORT>**	<PORT> – номер UDP-порта, может принимать значение [1..65535].

19.8.3 Пример настройки ICMP-режима тестирования

Задача:

Настроить постоянную проверку доступности публичного DNS-сервера с IP-адресом 8.8.8.8. Интерфейс, имеющий доступ в сеть Интернет gi1/0/1, имеет адрес 192.168.44.15.

Решение:

Для выяснения сетевой доступности достаточной является проверка с помощью ICMP-запросов. Для этого настроим SLA-тест с типом icmp-echo и всеми параметрами по умолчанию:

```
esr# configure
esr(config)# ip sla test 1
esr(config-sla-test)# icmp-echo 8.8.8.8 source-ip 192.168.44.15
esr(config-sla-test)# enable
esr(config-sla-test)# exit
esr(config)# ip sla schedule 1 life forever start-time now
```

Также включим логирование событий смены статуса теста и сообщений о причинах неудачи (на случай, если адрес перестанет быть доступен).

```
esr(config)# ip sla logging status
esr(config)# ip sla logging error
esr(config)# ip sla
esr(config)# exit
esr# commit
```

После применения конфигурации тест стартует, и выводится сообщение о его текущем состоянии:

```
esr# 2023-12-13T14:01:55+00:00 %IP_SLA-I-STATUS: (test 1) State changed to success
```

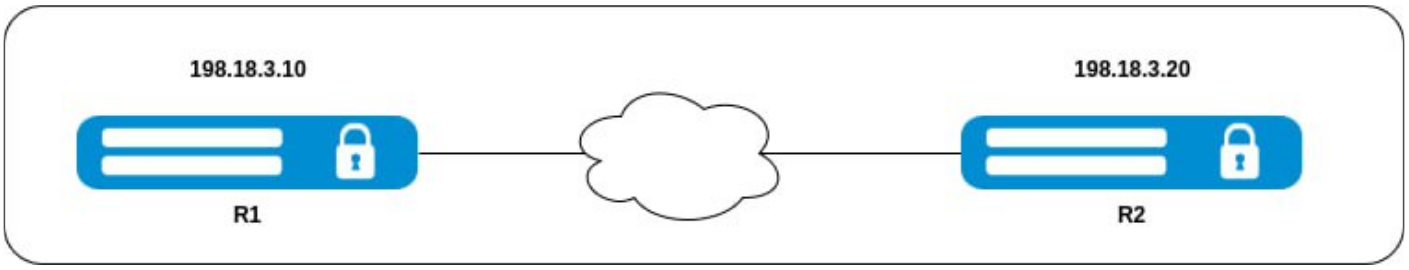
Сводную информацию о результате и конфигурации теста можно вывести командой:

```
esr# show ip sla test status
Test      Type           Source             Destination        Status         Last Run
-------   ------------   ----------------   ----------------   ------------
------------------
1         icmp-echo      192.168.44.15      8.8.8.8            Successful     1 second(s) ago
```

19.8.4 Пример настройки UDP-режима тестирования

Задача:

Настроить тестирование качества канала связи между двумя маршрутизаторами ELTEX. Маршрутизаторы находятся в одной подсети 198.18.3.0/24.



Решение:

Измерение качества канала связи (задержки, потери, дубликаты при передаче трафика и др.) возможно с использованием UDP-тестирования. Сконфигурируем SLA-тест с типом udp-jitter, который будет измерять количественные характеристики канала связи, а также сигнализировать о превышении установленных порогов.

Сконфигурируем на R1 SLA-тест udp-jitter с адресом назначения R2 (198.18.3.20). Поскольку ограничений на выбор портов не обозначено, воспользуемся портами 20002 на отправку и на получение. Также укажем интервал между пакетами, равный 10 мс, чтобы ускорить общий поток тестового трафика.

```
R1# configure
R1(config)# ip sla test 2
R1(config-sla-test)# udp-jitter 198.18.3.20 20002 source-ip 198.18.3.10 source-port 20002
 interval 10
```

Далее установим пороговые значения для информирования об ухудшении качества канала: максимальные значения двусторонней задержки – 15 мс, джиттера – 5мс и потерь – 5 пакетов (из 100 в настройках по умолчанию):

```
R1(config-sla-test)# thresholds delay high 15
R1(config-sla-test)# thresholds jitter forward high 5
R1(config-sla-test)# thresholds jitter reverse high 5
R1(config-sla-test)# thresholds losses high 5
```

Активируем тест и зададим расписание, согласно которому тест запустится немедленно и не будет иметь ограничений по следующим перезапускам:

```
R1(config-sla-test)# enable
R1(config)# ip sla schedule 2 start-time now life forever
```

Включим отображение всех групп сообщений, активируем сервис SLA-agent и применим конфигурацию:

```
R1(config)# ip sla logging status
R1(config)# ip sla logging error
R1(config)# ip sla logging delay
R1(config)# ip sla logging jitter
R1(config)# ip sla logging losses
R1(config)# ip sla
R1(config)# exit
R1# commit
```

Тест будет завершаться ошибкой до тех пор, пока не будет активирован Eltex SLA-responder на второй стороне – маршрутизаторе R2:

```
R1# 2023-12-13T14:01:55+00:00 %IP_SLA-I-STATUS: (test 2) State changed to fail
R1# 2023-12-13T14:01:55+00:00 %IP_SLA-E-ERROR: (test 2) Control phase failed: destination host
is not responding
```

Для этого перейдем в режим конфигурирования интерфейса, адрес которого ранее был указан как адрес назначения SLA-теста, и включим на нем Eltex SLA-responder:

```
R2(config)# interface gigabitethernet 1/0/1
R2(config-if-gi)# ip sla responder eltex
R2(config-if-gi)# exit
R2(config)# exit
R2# commit
```

Порт назначения пакетов аутентификации по умолчанию – 1800 и должен быть открыт на R2. Если прохождение трафика по данному порту запрещено, необходимо изменить настройку портов, воспользовавшись алгоритмом настройки параметров аутентификации, а также командами из раздела Настройка SLA-Responder.

После активации SLA-responder тест перейдет в состояние 'Успешно'.

```
2023-12-13T15:35:32+00:00 %IP_SLA-I-STATUS: (test 2) State changed to success
```

При ухудшении характеристик канала и, вследствие, превышения обозначенных пороговых значений, на R1 будут выводиться сообщения вида:

```
2023-12-13T15:59:22+00:00 %IP_SLA-I-DELAY: (test 2) Two-way delay is high: 50.71ms > 15ms
2023-12-13T16:00:40+00:00 %IP_SLA-I-LOSSES: (test 2) Total losses are high: 43 > 5
2023-12-13T16:04:04+00:00 %IP_SLA-I-JITTER: (test 2) One-way jitter in forward direction is
high: 9.41ms > 5ms
2023-12-13T16:04:04+00:00 %IP_SLA-I-JITTER: (test 2) One-way jitter in reverse direction is
high: 9.41ms > 5ms
```

Сам SLA-тест при этом перейдет в состояние Fail и будет оставаться в нем до тех пор, пока характеристики канала не вернутся в допустимые пределы.

Просмотреть результаты измерений теста можно командой:

```
R1# show ip sla test statistics 2
Test number:                                  2
Test status:                                  Successful
Transmitted packets:                          100
Lost packets:                                 39 (39.00%)
Lost packets in forward direction:            0 (0.00%)
Lost packets in reverse direction:            39 (39.00%)
One-way delay forward min/avg/max:            0.08/94.10/130.86 milliseconds
One-way delay reverse min/avg/max:            0.08/94.10/130.86 milliseconds
One-way jitter forward:                       35.94 milliseconds
One-way jitter reverse:                       35.94 milliseconds
Two-way delay min/avg/max:                    0.15/188.19/261.73 milliseconds
Duplicate packets:                            5
Out of sequence packets in forward direction: 0
Out of sequence packets in reverse direction: 40
```

19.8.5 Алгоритм настройки параметров аутентификации

Шаг	Описание	Команда	Ключи
1	В режиме конфигурирования SLA-теста, установить тип алгоритма, который будет использоваться при хешировании ключей аутентификации.	**esr(config-sla-test)# control-phase authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм хеширования, принимает значения [sha-256, hmac-sha-256].
2	Задать ключ, который будет использоваться в процессе прохождения контрольной фазы для аутентификации. Может быть использован один из двух видов ключей аутентификации: ключ-строка, указываемая непосредственно в режиме конфигурирования SLA-теста, и ключ, содержащийся в предварительно сконфигурированной связке ключей (key-chain).		
2.1	При использовании ключ-строки установить ее непосредственно в режиме конфигурирования SLA-теста.	**esr(config-sla-test)# control-phase authentication key-string ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<CLEAR-TEXT> – строка длиной от 8 до 16 символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).
2.2.1	При использовании ключа из связки ключей вернуться в общий режим конфигурирования, а затем создать новую связку ключей.	**esr(config)# key-chain <KEYCHAIN>**	<KEYCHAIN> – идентификатор связки ключей, задается строкой длиной до 16 символов.

Шаг	Описание	Команда	Ключи
2.2.2	В режиме конфигурирования связки ключей создать новый ключ.	**esr(config-key-chain)# key <NUM>**	<NUM> – номер-идентификатор ключа в связке ключей, может принимать значение [1..255].
2.2.3	Привязать к созданному ключу ключ-строку.	**esr(config-key-chain-key)# key-string ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<CLEAR-TEXT> – строка длиной от 8 до 16 символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).

Шаг	Описание	Команда	Ключи
2.2.4	Установить период времени, в течение которого данный ключ может использоваться для аутентификации исходящих пакетов (необязательно).	**esr(config-keychain-key)# send-lifetime <TIME_B> <DAY_B> <MONTH_B> <YEAR_B> <TIME_E> <DAY_E> <MONTH_E> <YEAR_E>**	<TIME_B> – устанавливаемое время начала действия ключа, задаётся в виде HH:MM:SS, где: HH – часы, принимает значение [0..23]; MM – минуты, принимает значение [0 .. 59]; SS – секунды, принимает значение [0 .. 59]. <DAY_B> – день месяца начала действия ключа, принимает значения [1..31]; <MONTH_B> – месяц начала использования ключа, принимает значения [January/ February/March/April/May/ June/July/August/September/ October/November/December]; <YEAR_B> – год начала использования ключа, принимает значения [2001..2037]; <TIME_E> – устанавливаемое время окончания действия ключа, задаётся в виде HH:MM:SS, где: HH – часы, принимает значение [0..23]; MM – минуты, принимает значение [0 .. 59]; SS – секунды, принимает значение [0 .. 59]. <DAY_E> – день месяца окончания действия ключа, принимает значения [1..31]; <MONTH_E> – месяц окончания действия ключа, принимает значения [January/ February/March/April/May/ June/July/August/September/ October /November/December]; <YEAR_E> – год окончания действия ключа, принимает значения [2001..2037].

Шаг	Описание	Команда	Ключи
2.2.5	Установить период времени, в течение которого данный ключ может использоваться для аутентификации входящих пакетов (необязательно).	**esr(config-keychain-key)# accept-lifetime <TIME_B> <DAY_B> <MONTH_B> <YEAR_B> <TIME_E> <DAY_E> <MONTH_E> <YEAR_E>**	<TIME_B> – устанавливаемое время начала действия ключа, задаётся в виде HH:MM:SS, где: HH – часы, принимает значение [0..23]; MM – минуты, принимает значение [0 .. 59]; SS – секунды, принимает значение [0 .. 59]. <DAY_B> – день месяца начала действия ключа, принимает значения [1..31]; <MONTH_B> – месяц начала использования ключа, принимает значения [January/ February/March/April/May/ June/July/August/September/ October/November/December]; <YEAR_B> – год начала использования ключа, принимает значения [2001..2037]; <TIME_E> – устанавливаемое время окончания действия ключа, задаётся в виде HH:MM:SS, где: HH – часы, принимает значение [0..23]; MM – минуты, принимает значение [0 .. 59]; SS – секунды, принимает значение [0 .. 59]. <DAY_E> – день месяца окончания действия ключа, принимает значения [1..31]; <MONTH_E> – месяц окончания действия ключа, принимает значения [January/ February/March/April/May/ June/July/August/September/ October /November/December]; <YEAR_E> – год окончания действия ключа, принимает значения [2001..2037].

Шаг	Описание	Команда	Ключи
2.2.6	Вернуться в общий режим конфигурирования и привязать ранее созданную связку ключей к сервису SLA.	**esr(config)# ip sla key-chain <KEYCHAIN>**	<KEYCHAIN> – идентификатор связки ключей, задается строкой длиной до 16 символов.
2.2.7	Перейти в режим конфигурирования ранее созданного SLA-теста и установить необходимый ключ из связки ключей, указав его номер.	**esr(config-sla-test)# control-phase authentication key-id <NUM>**	<NUM> – номер-идентификатор ключа в связке ключей, может принимать значение [1..255].
3	Указать порт, на который будут направляться пакеты для аутентификации в ходе контрольной фазы (необязательно).	**esr(config-sla-test)# control-phase destination-port <PORT>**	<PORT> – номер UDP-порта, может принимать значение [1..65535].
4	Указать порт, с которого будут отправляться пакеты для аутентификации в ходе контрольной фазы (необязательно).	**esr(config-sla-test)# control-phase source-port <PORT>**	<PORT> – номер UDP-порта, может принимать значение [1..65535].
5	Установить периодичность попыток повторного прохождения контрольной фазы в случае её неудачи.	**esr(config-sla-test)# control-phase retry <TIME>**	<TIME> – интервал между попытками, может принимать значение [1..86400] секунд.
6	Установить максимальное время ожидания ответного пакета аутентификации от удаленной стороны в ходе контрольной фазы.	**esr(config-sla-test)# control-phase timeout <TIME>**	<TIME> – время ожидания, может принимать значение [1..86400] секунд.
Далее необходимо симметрично настроить параметры аутентификации на удаленном маршрутизаторе (принимающая сторона).			
7	Перейти в режим конфигурирования сервиса SLA-responder.	**esr(config)# ip sla responder [vrf <VRF>]**	<VRF> – имя экземпляра VRF, задаётся строкой длиной до 31 символа. При указании данного параметра, SLA-responder включается в указанном VRF.
8	Установить максимальное время ожидания следующего тестового пакета (необязательно).	**esr(config-sla-responder)# timeout <TIME>**	<TIME> – время ожидания следующего пакета, может принимать значение [1..4294967295] миллисекунд.

Шаг	Описание	Команда	Ключи
9	Установить тип алгоритма, который будет использоваться при хешировании ключей аутентификации.	**esr(config-sla-responder)# authentication algorithm <ALGORITHM>**	<ALGORITHM> – алгоритм хеширования, принимает значения [sha-256, hmac-sha-256].
10	Задать ключ, который будет использоваться для аутентификации приходящих запросов от SLA-agent. Может быть использован один из двух видов ключей аутентификации: ключ-строка, указываемая непосредственно в режиме конфигурирования SLA-responder, и предварительно сконфигурированная связка ключей (key-chain).		
10.1	При использовании ключ-строки установить ее непосредственно в режиме конфигурирования SLA-responder.	**esr(config-sla-responder)# authentication key-string ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<CLEAR-TEXT> – строка длиной от 8 до 16 символов; <ENCRYPTED-TEXT> – зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).
10.2.1	При использовании связки ключей необходимо вернуться в общий режим конфигурирования, а затем создать новую связку ключей. Процесс создания повторяет создание связки на тестирующем маршрутизаторе и описан в рамках шагов 2.2.1 - 2.2.5 данного алгоритма.		
10.2.2	Привязать ранее созданную связку ключей к SLA-responder.	**esr(config-sla-responder)# authentication key-chain <KEYCHAIN>**	<KEYCHAIN> – идентификатор связки ключей, задается строкой длиной до 16 символов.

19.8.6 Пример конфигурации UDP-теста с аутентификацией по ключ-строке

Задача:

Установить нестандартные порты отправки и получения запросов аутентификации, а для аутентификации использовать ключ-строку. Базовый UDP-тест уже настроен.

Решение:

Конфигурация активного UDP-теста:

```
R-sender# show running-config sla
ip sla
ip sla logging error
ip sla logging status
ip sla test 1
  udp-jitter 10.0.0.1 20001 source-ip 10.0.0.2 source-port 20002
  enable
exit
ip sla schedule 1 life forever start-time now
```

```
R-responder# show running-config sla
interface gigabitethernet 1/0/3
  ip sla responder eltex
exit
```

Изменим порты отправки и получения запросов аутентификации (пакетов контрольной фазы). Для аутентификации будем использовать порт отправки – 50000 и порт получения – 49500. Для этого укажем их в параметрах SLA-теста:

```
R-sender# configure
R-sender(config)# ip sla test 1
R-sender(config)# ip sla test 1
R-sender(config-sla-test)# control-phase destination-port 49500
R-sender(config-sla-test)# control-phase source-port 50000
```

Таким образом, при каждом новом запуске SLA-теста первая пара запрос-ответ будет происходить по адресам 10.0.0.2:50000 ↔ 10.0.0.1:49500, а последующий тестовый трафик – 10.0.0.2:20002 ↔ 10.0.0.1:20001.

Здесь же укажем алгоритм для хеширования ключа и сам ключ:

```
R-sender(config-sla-test)# control-phase authentication algorithm sha-256
R-sender(config-sla-test)# control-phase authentication key-string ascii-text sla_password
R-sender(config-sla-test)# end
R-sender# commit
```

Далее необходимо продублировать эти параметры на ответной стороне. Для этого перейдем в режим конфигурирования интерфейса, который выступает SLA-Responder, и укажем порт прослушивания запросов аутентификации:

```
R-responder# configure
R-responder(config)# interface gigabitethernet 1/0/3
R-responder(config-if-gi)# ip sla responder eltex port 49500
R-responder(config-if-gi)# exit
R-responder(config)#
```

После этого необходимо перейти в параметры SLA-Responder и указать там тот же алгоритм хеширования и ключ-пароль:

```
R-responder(config)# ip sla responder
R-responder(config-sla-responder)# authentication algorithm sha-256
R-responder(config-sla-responder)# authentication key-string ascii-text sla_password
R-responder(config-sla-responder)# end
R-responder# commit
```

Таким образом конфигурации R-sender и R-responder:

```
R-sender# show running-config sla
ip sla
ip sla logging error
ip sla logging status
ip sla test 1
  control-phase destination-port 49500
  control-phase source-port 50000
  control-phase authentication algorithm sha-256
  control-phase authentication key-string ascii-text encrypted 8CB5107EA7005AFF2D
  udp-jitter 10.0.0.1 20001 source-ip 10.0.0.2 source-port 20002
  enable
exit
ip sla schedule 1 life forever start-time now
```

```
R-responder# show running-config sla
interface gigabitethernet 1/0/3
  ip sla responder eltex port 49500
  ip sla responder eltex
exit

ip sla responder
  authentication algorithm sha-256
  authentication key-string ascii-text encrypted 8CB5107EA7005AFF2D
exit
```

19.8.7 Пример конфигурации UDP-теста с аутентификацией по связке ключей

Задача:

Изменить конфигурацию, приведенную в примере выше, используя при этом связки ключей.

Решение:

После указания портов аутентификации, создадим связку ключей и новый ключ:

```
R-sender(config)# key-chain SLA_CHAIN
R-sender(config-key-chain)# key 1
R-sender(config-key-chain-key)# key-string ascii-text sla_password
R-sender(config-key-chain-key)# exit
R-sender(config-key-chain)# exit
R-sender(config)#
```

Привяжем созданную связку к SLA-agent, а ключ из связки привяжем к SLA-тесту:

```
R-sender(config)# ip sla key-chain SLA_CHAIN
R-sender(config)# ip sla test 1
R-sender(config-sla-test)# control-phase authentication key-id 1
R-sender(config-sla-test)# end
R-sender# commit
```

Аналогичные действия произведем на R-responder. Создадим связку ключей с необходимым ключом и привяжем связку к SLA-Responder:

```
R-responder(config)# key-chain SLA
R-responder(config-key-chain)# key 1
R-responder(config-key-chain-key)# key-string ascii-text sla_password
R-responder(config-key-chain-key)# exit
R-responder(config-key-chain)# exit
R-responder(config)# ip sla responder
R-responder(config-sla-responder)# authentication key-chain SLA
R-responder(config-sla-responder)# end
R-responder# commit
```

Таким образом конфигурации R-sender и R-responder:

```
R-sender# show running-config
key-chain SLA_CHAIN
  key 1
    key-string ascii-text encrypted 8FB80252A00E5BE802FA0217
  exit
exit

ip sla key-chain SLA_CHAIN
ip sla
ip sla logging error
ip sla logging status
ip sla test 1
  control-phase destination-port 49500
  control-phase source-port 50000
  control-phase authentication algorithm sha-256
  control-phase authentication key-id 1
  udp-jitter 10.0.0.1 20001 source-ip 10.0.0.2 source-port 20002
  enable
exit
ip sla schedule 1 life forever start-time now
```

```
R-responder# show running-config
key-chain SLA
  key 1
    key-string ascii-text encrypted 8FB80252A00E5BE802FA0217
  exit
exit

interface gigabitethernet 1/0/3
  ***
  ip sla responder eltex port 49500
  ip sla responder eltex
exit

ip sla responder
  authentication algorithm sha-256
  authentication key-chain SLA
exit
```

Использование связок ключей позволяет комбинировать различные уникальные пароли для аутентификации между SLA-agent и SLA-Responder.

19.8.8 Настройка пороговых значений

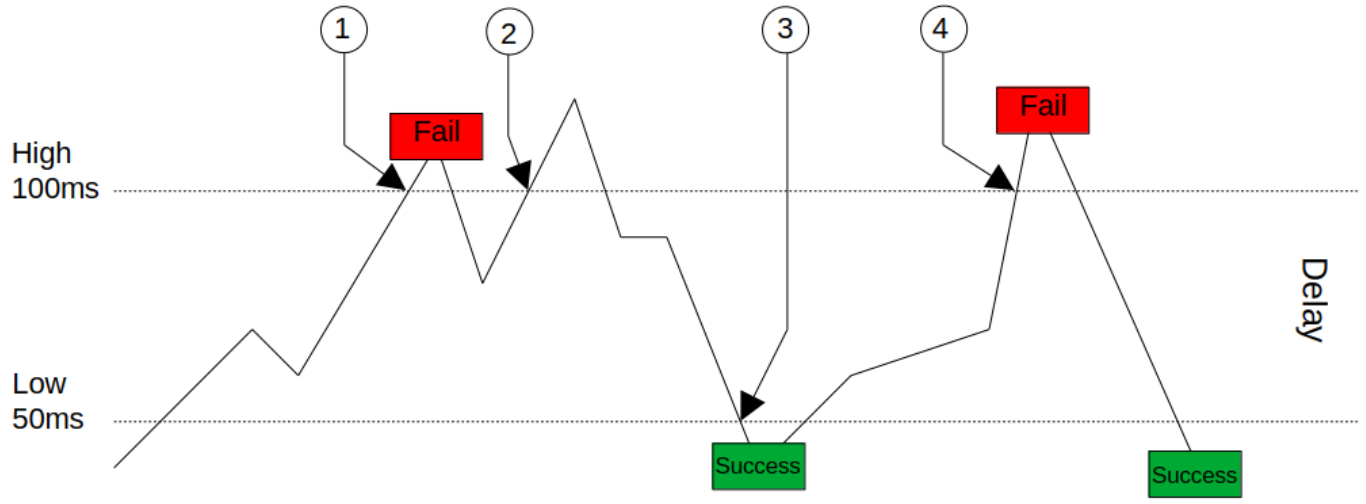
Для настройки реакции SLA-теста на определенные характеристики канала связи предусмотрен механизм активного реагирования на параметры thresholds.

Реагирование на качество канала связи может осуществляться по трём основных параметрам:

- Delay – измерение задержки между эталонным показателем интервала передачи очередного тестового пакета;
- Losses – измерение количества утерянных тестовых пакетов среди общего количества переданных пакетов;
- Jitter – измерение «дрожания» в канале, т. е. разброса во времени прохождения тестовых пакетов.

Для конфигурирования доступна настройка верхнего (high) и нижнего (low) пороговых значений для каждого из представленных параметров. Каждый из параметров может быть установлен как для одностороннего направления (forward/reverse), так и для двухстороннего (two-way).

Механизм активного изменения состояния SLA-теста при установленных пороговых значениях представлен на примере отслеживания показателя Delay с графиком значений величины во времени:



Событие	Описание
1	Первичное превышение верхнего порогового значения. Инициируется смена состояния SLA-теста на «Fail», отображается информационное сообщение о превышении установленного порога.
2	Повторное превышение верхнего порогового значения. Состояние SLA-теста неизменно (Fail), информационных сообщений не отображается. Для восстановления состояния теста ожидается снижение величины до значений меньших, чем установленный порог Low.
3	Понижение отслеживаемой величины до значений ниже установленного порога Low. Инициируется смена состояния SLA-теста на «Success», отображается информационное сообщение о нормализации показателя.
4	Очередная смена состояния SLA-теста, вызванная пересечением значения верхнего порога и предварительно нормализованным пересечением нижнего порога.

Пример конфигурации icmp-jitter SLA-теста с thresholds по показателю delay:

```
R-sender# show running-config sla
ip sla
ip sla logging delay
ip sla logging error
ip sla logging status
ip sla test 1
  icmp-jitter 198.18.0.100 source-ip 198.18.0.1 num-packets 150
  thresholds delay high 15
  thresholds delay low 8
  thresholds delay forward high 10
  thresholds delay forward low 5
  thresholds delay reverse high 10
  thresholds delay reverse low 5
  enable
exit
ip sla schedule all life forever start-time now
```

⚠ Нижний порог (low) допускается не устанавливать. В таком случае он принимается равным верхнему, и нормализация характеристики будет засчитываться при снижении значений до показателей ниже установленного уровня.

19.8.9 Измерение характеристик канала связи

Механизм IP-SLA позволяет производить замеры как двухсторонних (two-way/round), так и односторонних (forward/reverse) характеристик канала связи.

После первичной настройки IP-SLA-тестов и запроса статистики замеров может возникнуть ситуация, в которой односторонние характеристики в прямом и обратном направлениях равны друг другу, а также являются половиной от двухсторонних характеристик. Причиной такого поведения чаще всего является несоответствие вычисленной односторонней характеристики критериям проверки механизма IP-SLA.

Для корректного измерения односторонних параметров существует несколько обязательных критериев:

- **Оба узла** (SLA-пробер и ответчик) **должны быть синхронизованы по NTP**;
- Суммарное отклонение от NTP на обоих узлах не должно превышать значение двухсторонней характеристики;
- Значение односторонней характеристики не должно быть меньше 0, а также превышать значение двухсторонней характеристики.

Только при соблюдении данных критериев можно ожидать корректное вычисление всех характеристик канала передачи данных.

```
R-sender# show ntp peers
Clock is synchronized, stratum 5, reference is 192.168.32.1
    remote                                          vrf          refid             st   t
when   poll   reach   delay      offset     jitter
-   ---------------------------------------------   ----------   ---------------   --   -
----   ----   -----   --------   --------   --------
*   192.168.32.1                                                 172.16.5.63       4    s
10     16     255     0.183      -2.314     0.711
R-sender# show ip sla test statistics 2
Test number:                                  2
Description:                                  --
Test status:                                  Successful
Transmitted packets:                          100
Lost packets:                                 1 (1.00%)
Lost packets in forward direction:            1 (1.00%)
Lost packets in reverse direction:            0 (0.00%)
One-way delay forward min/avg/max:            23.19/24.61/30.57 milliseconds
One-way delay reverse min/avg/max:            46.26/47.25/55.28 milliseconds
One-way jitter forward:                       2.77 milliseconds
One-way jitter reverse:                       0.92 milliseconds
Two-way delay min/avg/max:                    70.26/71.85/80.03 milliseconds
Two-way jitter min/avg/max:                   2.01/3.02/3.92 milliseconds
Duplicate packets:                            0
Out of sequence packets in forward direction: 0
Out of sequence packets in reverse direction: 0
Number of successes:                          3 (100.00%)
Number of failures:                           0 (0.00%)
```

20 Управление BRAS (Broadband Remote Access Server)

- Алгоритм настройки
- Пример настройки с SoftWLC
- Пример настройки без SoftWLC

20.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Добавить RADIUS-сервер в список используемых серверов и перейти в режим его конфигурирования.	**esr(config)# radius-server host { <IP-ADDR> | <IPV6-ADDR> } [vrf <VRF>]** **esr(config-radius-server)#**	<IP-ADDR> – IP-адрес RADIUS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> – IPv6-адрес RADIUS-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <VRF> – имя экземпляра VRF, задается строкой до 31 символа.
2	Задать пароль для аутентификации на удаленном RADIUS-сервере.	**esr(config-radius-server)# key ascii-text { <TEXT> | encrypted <ENCRYPTED-TEXT> }**	<TEXT> – строка [8..16] ASCII-символов; <ENCRYPTED-TEXT> – зашифрованный пароль, размером [8..16] байт, задаётся строкой [16..32] символов.
3	Создать профиль AAA.	**esr(config)# aaa radius-profile <NAME>**	<NAME> – имя профиля сервера, задается строкой до 31 символа.
4	В профиле AAA указать RADIUS-сервер.	**esr(config-aaa-radius-profile)# radius-server host { <IP-ADDR> | <IPV6-ADDR> }**	<IP-ADDR> – IP-адрес RADIUS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> – IPv6-адрес RADIUS-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].

Шаг	Описание	Команда	Ключи
5	Создать DAS-сервер.	**esr(config)# das-server <NAME>**	<NAME> – имя DAS-сервера, задается строкой до 31 символа.
6	Задать пароль для аутентификации на удаленном DAS-сервере.	**esr(config-das-server)# key ascii-text {<TEXT>|encrypted <ENCRYPTED-TEXT> }**	<TEXT> – строка [8..16] ASCII-символов; <ENCRYPTED-TEXT> – зашифрованный пароль, размером [8..16] байт, задаётся строкой [16..32] символов.
7	Создать AAA DAS-профиль.	**esr(config)# aaa das-profile <NAME>**	<NAME> – имя DAS-профиля, задается строкой до 31 символа.
8	Указать DAS-сервер в DAS-профиле.	**esr(config-aaa-das-profile)# das-server <NAME>**	<NAME> – имя DAS-сервера, задается строкой до 31 символа.
9	Сконфигурировать BRAS.	**esr(config)# subscriber-control [vrf <VRF>]**	<VRF> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет работать контроль пользователей.
10	Выбрать профиль серверов динамической авторизации (DAS), на которые будут приходить CoA-запросы от PCRF.	**esr(config-subscriber-control)# aaa das-profile <NAME>**	<NAME> – имя профиля серверов динамической авторизации (DAS), задается строкой до 31 символа.
11	Выбрать профиль RADIUS-серверов для получения параметров сервисов пользователя.	**esr(config-subscriber-control)# aaa services-radius-profile <NAME>**	<NAME> – имя профиля RADIUS-серверов, задается строкой до 31 символа.
12	Выбрать профиль RADIUS-серверов для получения параметров сессии пользователя.	**esr(config-subscriber-control)# aaa sessions-radius-profile <NAME>**	<NAME> – имя профиля RADIUS-серверов, задается строкой до 31 символа.
13	Определить IP-адрес маршрутизатора, который будет использоваться в качестве IP-адреса источника в отправляемых RADIUS-пакетах.	**esr(config-subscriber-control)# nas-ip-address <ADDR>**	<ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
14	Включить аутентификацию сессий по MAC-адресу (необязательно).	**esr(config-subscriber-control)# session mac-authentication**	

Шаг	Описание	Команда	Ключи
15	Организовать прозрачное пропускание служебного трафика (DHCP, DNS и т. д.) на основе фильтров.	**esr(config-subscriber-control)# bypass-traffic-acl <NAME>**	<NAME> – имя привязываемого ACL, задается строкой до 31 символа.
16	Перейти в режим конфигурирования сервиса по умолчанию.	**esr(config-subscriber-control)# default-service**	
17	Привязать указанный QoS-класс к сервису по умолчанию.	**esr(config-subscriber-default-service)# class-map <NAME>**	<NAME> – имя привязываемого класса, задается строкой до 31 символа.
18	Указать имя списка URL, который будет использоваться для фильтрации HTTP/HTTPS-трафика не аутентифицированных пользователей.	**esr(config-subscriber-default-service)# filter-name { local<LOCAL-NAME>** | **remote<REMOTE-NAME> }**	<LOCAL-NAME> – имя профиля URL, задаётся строкой до 31 символа; <REMOTE-NAME> – имя списка URL на удаленном сервере, задаётся строкой до 31 символа.
19	Указать действия, которые должны быть применены для HTTP/HTTPS-пакетов, URL которых входит в список URL, назначенных командой «filter-name».	**esr(config-subscriber-default-service)# filter-action<ACT>**	<ACT> – назначаемое действие: • **permit** – прохождение трафика разрешается; • **deny** – прохождение трафика запрещается. redirect <URL> – будет выполнен редирект на указанный URL, задается строкой до 255 символов.
20	Указать действия, которые должны быть применены для HTTP/HTTPS-пакетов, URL которых не входит в список URL, назначенных командой «filter-name».	**esr(config-subscriber-default-service)# default-action<ACT>**	<ACT> – назначаемое действие: • **permit** – прохождение трафика разрешается; • **deny** – прохождение трафика запрещается. redirect <URL> – будет выполнен редирект на указанный URL, задается строкой до 255 символов.
21	Активировать профиль контроля пользователей.	**esr(config-subscriber-control)# enable**	

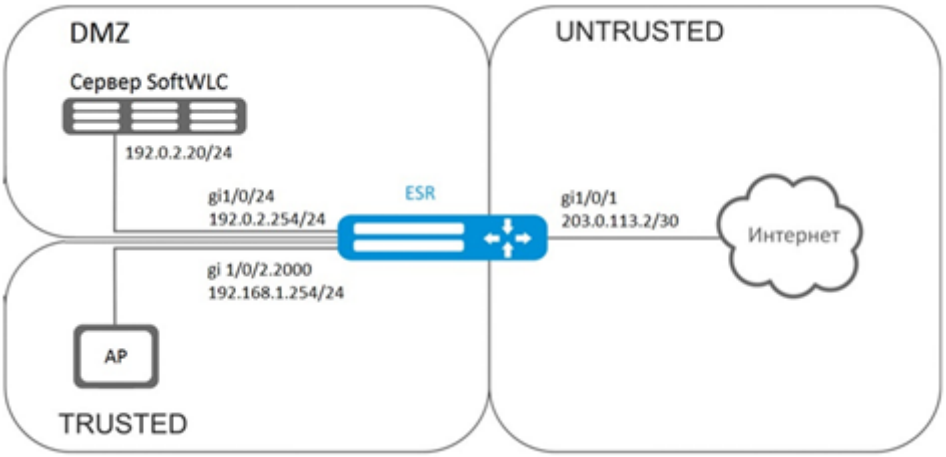
Шаг	Описание	Команда	Ключи
22	Изменить идентификатор сетевого интерфейса (физического, саб-интерфейса или сетевого моста) (необязательно).	**esr(config-if)# location <ID>**	<ID> – идентификатор сетевого интерфейса, задаётся строкой до 220 символов.
23	Включить контроль пользователей на интерфейсе.	**esr(config-if-gi)# 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 (необязательно).	**esr(config-subscriber-control)# quota-expired-reauth**	
25	Включить аутентификацию сессий по IP-адресу (необязательно).	**esr(config-subscriber-control)# session ip-authentication**	
26	Включить прозрачное пропускание трафика в состоянии backup для BRAS (необязательно).	**esr(config-subscriber-control)# backup traffic-processing transparent**	
27	Задать интервал, по истечении которого с устройства будут удалены неиспользуемые в текущий момент списки URL (необязательно).	**esr(config)# subscriber-control unused-filters-remove-delay <DELAY>**	<DELAY> – временной интервал в секундах, принимает значения [10800..86400].
28	Задать интервал, по истечении которого, если не было пакетов от пользователя, сессия считается устаревшей и удаляется с устройства (необязательно).	**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) (необязательно).	**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 (необязательно).	**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 (необязательно).	**esr(config-subscriber-control)# ip proxy http redirect-port <PORT>**	<PORT> – номер порта, указывается в диапазоне [1..65535].

Шаг	Описание	Команда	Ключи
32	Определить, с каких TCP-портов назначения трафик будет перенаправлен на HTTPS Proxy-сервер маршрутизатора (необязательно).	**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 (необязательно).	**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 (необязательно).	**esr(config-subscriber-control)# ip proxy source-address <ADDR>**	<ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
35	Задать URL-адрес сервера, предоставляющего списки приложений для фильтрации трафика (необязательно).	**esr(config)# subscriber-control apps-server-url <URL>**	<URL> – адрес ссылки, задаётся строкой от 8 до 255 символов.
36	Включить контроль приложений на интерфейсе (необязательно).	**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 (необязательно).	**esr(config-subscriber-control)# thresholds sessions-number high <Threshold>**	<Threshold> – количество сессий BRAS: • [0-50000] – для ESR-1700; • [0-10000] – для ESR-1200/1000/1500/1511 (rev.B)/3100/3150/3200/3200L/3250/3300/3350; • [0-1000] – для ESR-30/31/100/200.
38	Установить/сбросить нижнюю границу количества сессий BRAS (необязательно).	**esr(config-subscriber-control)# thresholds sessions-number low <Threshold>**	<Threshold> – количество сессий BRAS: • [0-50000] – для ESR-1700; • [0-10000] – для ESR-1200/1000/1500/1511 (rev.B)/3100/3150/3200/3200L/3250/3300/3350; • [0-1000] – для ESR-30/31/100/200.

20.2 Пример настройки с SoftWLC

Задача:

Предоставлять доступ до ресурсов сети Интернет, только для авторизованных пользователей.



Решение:

За хранение учетных данных пользователей и параметров тарифных планов отвечает сервер SoftWLC. Информацию по установке и настройке сервера SoftWLC можно найти по ссылкам ниже:

Общая статья о SoftWLC;

Установка SoftWLC.

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-if-sub)# bridge-group 1
esr(config-if-sub)# exit
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# service-policy dynamic downstream
esr (config-if-gi)# exit
```

⚠ Подключать клиентов необходимо через саб-интерфейсы в бриджи, причем от параметра location (см. 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 port-range 68
esr(config-acl-rule)# match destination-port port-range 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 port-range 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 укажем 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 object-group dhcp_client
esr(config-zone-pair-rule)# match destination-port object-group 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 object-group bras
esr(config-zone-pair-rule)# enable
esr (config-zone-pair-rule)# exit
esr(config-zone-pair)# rule 20
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-rule)# exit
esr(config)# security zone-pair dmz self
esr(config-zone-pair)# rule 20
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-rule)# exit
esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule 20
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match source-address any
esr(config-zone-pair-rule)# match destination-address any
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair-rule)# exit
```

Активируем DHCP-Relay:

```
esr(config)# ip dhcp-relay
```

Настроим SNAT в порт gigabitethernet 1/0/1:

```
esr(config)# nat source
esr(config-snat)# ruleset inet
esr(config-snat-ruleset)# to interface gigabitethernet 1/0/1
esr(config-snat-ruleset)# rule 10
esr(config-snat-rule)# match source-address any
esr(config-snat-rule)# action source-nat interface
esr(config-snat-rule)# enable
esr(config-snat-rule)# end
```

20.3 Пример настройки без SoftWLC

Задача:

Настроить BRAS без поддержки SoftWLC.

Дано:

Подсеть с клиентами 10.10.0.0/16, подсеть для работы с FreeRADIUS-сервером 192.168.1.1/24.

Решение:

Шаг 1:

Настройка RADIUS-сервера.

Для FreeRADIUS-сервера нужно задать подсеть, из которой могут приходить запросы и добавить список пользователей. Для этого в файл users в директории с файлами конфигурации FreeRADIUS-сервера нужно добавить:

Профиль пользователя:

```
<MACADDR> Cleartext-Password := <MACADDR>
```

#Имя пользователя

```
  User-Name = <USER_NAME>,
```

#Максимальное время жизни сессии

```
  Session-Timeout = <SECONDS>,
```

#Максимальное время жизни сессии при бездействии пользователя

```
  Idle-Timeout = <SECONDS>,
```

#Время на обновление статистики по сессии

```
  Acct-Interim-Interval = <SECONDS>,
```

#Имя сервиса для сессии (A – сервис включен, N – сервис выключен)

```
  Cisco-Account-Info = "{A|N}<SERVICE_NAME>"
```

Профиль сервиса:

```
<SERVICE_NAME> Cleartext-Password := <MACADDR>
```

#Соответствует имени class-map в настройках ESR

```
Cisco-AVPair = "subscriber:traffic-class=<CLASS_MAP>",
```

#Действие, которое применяет ESR к трафику (permit, deny, redirect)

```
Cisco-AVPair = "subscriber:filter-default-action=<ACTION>",
```

Возможность прохождения IP-потоков (enabled-uplink, enabled-downlink, enabled, disabled)

```
Cisco-AVPair = "subscriber:flow-status=<STATUS>"
```

В файл clients.conf нужно добавить подсеть, в которой находится ESR:

```
client ESR {
ipaddr = <SUBNET>
secret = <RADIUS_KEY>
}
```

В нашем случае настройка RADIUS-сервера будет выглядеть так:

в файл «clients.conf» добавляем строки:

```
client BRAS {
ipaddr = 192.168.1.1
secret = password
}
```

В файл «users» добавляем строки (вместо <MAC> нужно указать MAC-адрес клиента):

```
"54-E1-AD-8F-37-35" Cleartext-Password := "54-E1-AD-8F-37-35"
User-Name = "Bras_user",
Session-Timeout = 259200,
Idle-Timeout = 259200,
Cisco-AVPair += "subscriber:policer-rate-in=1000",
Cisco-AVPair += "subscriber:policer-rate-out=1000",
Cisco-AVPair += "subscriber:policer-burst-in=188",
Cisco-AVPair += "subscriber:policer-burst-out=188",
Cisco-Account-Info = "AINTERNET"
INTERNET Cleartext-Password := "INTERNET"
User-Name = "INTERNET",
Cisco-AVPair = "subscriber:traffic-class=INTERNET",
Cisco-AVPair += "subscriber:filter-default-action=permit"
```

Шаг 2:

Настройка ESR.

Для настройки функционала BRAS необходимо наличие лицензии BRAS.

```
esr(config)# do sh licence
Licence information
-------------------
Name:    Eltex
Version: 1.0
Type:    ESR-X
S/N:     NP00000000
MAC:     XX:XX:XX:XX:XX:XX
Features:
  BRAS - Broadband Remote Access Server
```

Настройка параметров для взаимодействия с RADIUS-сервером:

```
esr(config)# radius-server host 192.168.1.2
esr(config-radius-server)# key ascii-text encrypted 8CB5107EA7005AFF
esr(config-radius-server)# source-address 192.168.1.1
esr(config-radius-server)# exit
```

Создадим профиль AAA:

```
esr(config)#  aaa radius-profile bras_radius
esr(config-aaa-radius-profile)# radius-server host 192.168.1.2
esr(config-aaa-radius-profile)#  exit
esr(config)#  aaa radius-profile bras_radius_servers
esr(config-aaa-radius-profile)#  radius-server host 192.168.1.2
esr(config-aaa-radius-profile)#  exit
```

Укажем параметры к DAS-серверу:

```
esr(config)# das-server das
esr(config-das-server)# key ascii-text encrypted 8CB5107EA7005AFF
esr(config-das-server)#  exit
esr(config)#  aaa das-profile bras_das
esr(config-aaa-das-profile)#  das-server das
esr(config-aaa-das-profile)# exit
esr(config)#  vlan 10
esr(config-vlan)#  exit
```

Далее создаем правила для редиректа на портал и пропуска трафика в Интернет:

```
esr(config)#  ip access-list extended BYPASS
esr(config-acl)# rule 1
esr(config-acl-rule)#  action permit
esr(config-acl-rule)# match protocol udp
esr(config-acl-rule)#  match source-address any
esr(config-acl-rule)# match destination-address any
esr(config-acl-rule)#  match source-port port-range 68
esr(config-acl-rule)#  match destination-port port-range 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 port-range 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 port-range 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 port-range 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 port-range 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 port-range 8080
esr(config-acl-rule)# enable
esr(config-acl-rule)# exit
```

Настройка действия фильтрации по URL обязательна, необходимо настроить фильтрацию http-proxy на BRAS для неавторизованных пользователей:

```
esr(config)# object-group url defaultserv
esr(config-object-group-url)# url http://eltex.nsk.ru
esr(config-object-group-url)# url http://ya.ru
esr(config-object-group-url)# url https://ya.ru
esr(config-object-group-url)# exit
```

Сконфигурируем и включим BRAS, в качестве NAS IP указываем адрес интерфейса на стыке с RADIUS-сервером в данном примере – это IP-адрес интерфейса gigabitethernet 1/0/2:

```
esr(config)#  subscriber-control
esr(config-subscriber-control)# aaa das-profile bras_das
esr(config-subscriber-control)# aaa sessions-radius-profile bras_radius
esr(config-subscriber-control)# aaa services-radius-profile bras_radius_servers
esr(config-subscriber-control)# nas-ip-address 192.168.1.1
esr(config-subscriber-control)# session mac-authentication
esr(config-subscriber-control)# bypass-traffic-acl BYPASS
esr(config-subscriber-control)# default-service
esr(config-subscriber-default-service)# class-map BYPASS
esr(config-subscriber-default-service)# filter-name local defaultserv
esr(config-subscriber-default-service)# filter-action permit
esr(config-subscriber-default-service)# default-action redirect http://192.
168.1.2:8080/eltex_portal
esr(config-subscriber-default-service)# session-timeout 121
esr(config-subscriber-default-service)# exit
esr(config-subscriber-control)# enable
esr(config-subscriber-control)# exit
```

На интерфейсах, для которых требуется работа BRAS, произвести настройку (для успешного запуска требуется как минимум один интерфейс):

```
esr(config)#  bridge 10
esr(config-bridge)# vlan 10
esr(config-bridge)# ip firewall disable
esr(config-bridge)#  ip address 10.10.0.1/16
esr(config-bridge)#  ip helper-address 192.168.1.2
esr(config-bridge)# service-subscriber-control any
esr(config-bridge)# location USER
esr(config-bridge)#  protected-ports
esr(config-bridge)#  protected-ports exclude vlan
esr(config-bridge)# enable
esr(config-bridge)#  exit
```

Сконфигурируем порт в сторону RADIUS-сервера:

```
esr(config)# interface gigabitethernet 1/0/2
esr(config-if-gi)# ip firewall disable
esr(config-if-gi)# ip address 192.168.1.1/24
esr(config-if-gi)#  exit
```

Порт в сторону клиента:

```
esr(config)#  interface gigabitethernet 1/0/3.10
esr(config-if-sub)#  bridge-group 10
esr(config-if-sub)# ip firewall disable
esr(config-if-sub)#  exit
```

Настройка SNAT в порт gigabitethernet 1/0/2:

```
esr(config)# nat source
esr(config-snat)# ruleset factory
esr(config-snat-ruleset)# to interface gigabitethernet 1/0/2
esr(config-snat-ruleset)# rule 10
esr(config-snat-rule)# description "replace 'source ip' by outgoing interface ip address"
esr(config-snat-rule)# match protocol any
esr(config-snat-rule)# match source-address any
esr(config-snat-rule)# match destination-address any
esr(config-snat-rule)# action source-nat interface
esr(config-snat-rule)# enable
esr(config-snat-rule)# exit
esr(config-snat-ruleset)# exit
esr(config-snat)# exit
esr(config)# ip route 0.0.0.0/0 192.168.1.2
```

Изменения конфигурации вступят в действие после применения:

```
esr(config) # do commit
esr(config) # do confirm
```

Для просмотра информации и статистики по сессиям контроля пользователей – можно воспользоваться командой:

```
esr # sh subscriber-control sessions status

Session id      User name    IP address      MAC address       Interface          Domain
--------------------   ---------------  ---------------   -----------------
1729382256910270473    Bras_user   10.10.0.3  54:e1:ad:8f:37:35     gi1/0/3.10     --
```

21 Управление VoIP

- Алгоритм настройки SIP-профиля
- Алгоритм настройки FXS/FXO-портов
- Алгоритм настройки плана нумерации
- Алгоритм настройки PBX-сервера
- Алгоритм создания транка регистрации
- Пример настройки VoIP
- Пример настройки плана нумерации
- Настройка FXO-порта
- Пример настройки VoIP для регистрации FXS-портов на внешнем SIP-сервере
- Пример настройки VoIP на внутреннем pbx-сервере

VoIP (англ. *Voice over IP*) — набор протоколов, которые позволяют передавать речевую информацию посредством IP-сетей. В рамках данного устройства VoIP используется для подключения аналоговых телефонных аппаратов к IP-сети с возможностью совершения телефонных вызовов.

21.1 Алгоритм настройки SIP-профиля

Шаг	Описание	Команда	Ключи
1	Настройка SIP-профиля.	**esr(config)# sip profile <NUM>**	<NUM> – номер SIP-профиля, задается в виде цифры от 1 до 5.
2	Настройка основного SIP proxy-сервера и сервера регистрации.	**esr(config-sip-profile)# proxy primary**	
3	Настройка адреса SIP proxy-сервера.	**esr(config-voip-sip-proxy)# ip address proxy-server <IP>**	<IP> – IP-адрес proxy-сервера.
4	Настройка порта SIP proxy-сервера.	**esr(config-voip-sip-proxy)# ip port proxy-server <PORT>**	<PORT> – номер UDP-порта proxy-сервера, принимает значения [1..65535]. Если используется стандартный порт 5060, то его можно не указывать.
5	Настройка адреса сервера регистрации.	**esr(config-voip-sip-proxy)# ip address registration-server <IP>**	<IP> – IP-адрес сервера регистрации.
6	Настройка порта сервера регистрации.	**esr(config-voip-sip-proxy)# ip portregistration-server <PORT>**	<PORT> – номер UDP-порта сервера регистрации, принимает значения [1..65535]. Если используется стандартный порт 5060, то его можно не указывать.
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**	

21.2 Алгоритм настройки FXS/FXO-портов

Шаг	Описание	Команда	Ключи
1	Переход в режим конфигурирования FXO-/FXS-портов.	**esr(config)# interface voice-port <NUM>**	<NUM> – номер порта, принимает значение от 1 до 4.
2	Назначение абонентского номера, закрепленного за телефонным портом.	**esr(config-voice-port-fxs)# sip user phone <PHONE>**	<PHONE> – абонентский номер, закрепленный за телефонным портом, задается до 50 символов.
3	Назначение имя пользователя, сопоставленное с портом.	**esr-12v(config-voice-port-fxs)# sip user display-name <LOGIN>**	<LOGIN> – имя пользователя, которое отображается в поле Display-Name, задается стройкой до 31 символа.
4	Выбор SIP-профиля для конкретного порта.	**esr(config-voice-port-fxs)# profile sip <PROFILE>**	<PROFILE> – номер SIP-профиля, задается от 1 до 5.
5	Настройка логина для аутентификации.	**esr(config-voice-port-fxs)# authentication name <LOGIN>**	<LOGIN> – логин для аутентификации, задается строкой до 31 символа.
6	Настройка пароля для аутентификации.	**esr(config-voice-port-fxs)# authentication password <PASS>**	<PASS> – пароль для аутентификации, задается строкой до 16 символов.
7	Активация FXO-порта.	**esr(config)# interface voice-port <NUM>**	<NUM> – номер FXO-порта, принимает значение от 1 до 4.
8	Назначение абонентского номера, закрепленного за телефонным портом.	**esr(config-voice-port-fxo)# sip user phone <PHONE>**	<PHONE> – абонентский номер, закрепленный за телефонным портом.
9	Указание UDP-порта, с которого и на который FXO-комплект будет отправлять и принимать SIP-сообщения.	**esr(config-voice-port-fxo)# sip port <PORT>**	<PORT> – номер UDP-порта.
10	Назначение имени пользователя, сопоставленное с портом.	**esr(config-voice-port-fxo)# sip user display-name <LOGIN>**	<LOGIN> – имя пользователя, которое отображается в поле Display-Name, задается строкой до 31 символа.
11	Настройка логина для аутентификации.	**esr(config-voice-port-fxo)# authentication name <LOGIN>**	<LOGIN> – логин для аутентификации, задается строкой до 31 символа.

Шаг	Описание	Команда	Ключи
12	Настройка пароля для аутентификации.	**esr(config-voice-port-fxo)# authentication password <PASS>**	<PASS> – пароль для аутентификации, задается строкой до 16 символов.
13	Разрешение передачи номера в ТфОП.	**esr(config-voice-port-fxo)# pstn transmit-number**	
14	Запретить передачу префикса.	**esr(config-voice-port-fxo)# no pstn transmit-prefix**	
15	Активация услуги «Hostline PSTN to IP».	**esr(config-voice-port-fxo)# hotline ipt**	
16	Номер абонента, который будет получать вызовы с ТфОП.	**esr(config-voice-port-fxo)# hotline number ipt <PHONE>**	<PHONE> – номер телефона, на который осуществляется вызов при использовании услуги, принимает значение от 1 до 50. «Горячая/Теплая линия» в направлении из аналоговой телефонной линии в VoIP.

21.3 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 Управление VoIP.
3	Активация плана нумерации.	**esr(config-dial-ruleset)# enable**	

21.4 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	Выбор адреса источника для пакетов исходящих с PBX-сервера (не обязательно).	**esr(config-pbx)# source-address <ADDR>**	<ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
4	Создание плана маршрутизации.	**esr(config-pbx)# ruleset <rule_name>**	<rule_name> – имя плана маршрутизации, задается строкой до 31 символа.
5	Создание правила маршрутизации.	**esr(config-pbx-ruleset)# rule <rule_index>**	<rule_index> – номер правила в плане маршрутизации, принимает значение от 1 до 1000.
6	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 Управление VoIP.
7	Применение правила маршрутизации.	**esr(config-pbx-rule)# enable**	
8	Создание SIP-профиля на PBX-сервере.	**esr(config-pbx)# profile <PROFILE>**	<PROFILE> – имя SIP-профиля, используемого PBX-сервером, задается строкой до 31 символа.
9	Выбор кодека, поддерживаемого SIP-профилем.	**esr(config-pbx-profile)# codec allow { G711A(alaw) | G711U(ulaw) | G722 | G726 }**	
10	Выбор типа SIP-профиля.	**esr(config-pbx-profile)# client { peer | user | friend }**	• **peer** – входящие и исходящие звонки разрешены без авторизации. • **user** – разрешены только входящие звонки. • **friend** – комбинирует типы профилей peer и user.

Шаг	Описание	Команда	Ключи
11	Выбор политики взаимодействия с NAT (не обязательно).	**esr(config-pbx-profile)# nat { comedia | force-port | both }**	• **comedia** – отправить медиапоток на порт PBX, независимо от указаний SDP. • **force-port** – использовать rport, даже если его нет. • **both** – объединяет comedia и force-port.
12	Выбор плана маршрутизации, связанного с SIP-профилем.	**esr(config-pbx-profile)# ruleset <NAME>**	<NAME> – имя плана маршрутизации, задается строкой до 31 символа.
13	Создание абонента.	**esr(config-pbx)# user <user>**	<user> – номер телефона или имя пользователя, задается строкой до 31 символа.
14	Создание пароля для абонента (не обязательно).	**esr(config-pbx-user)# password <password>**	<password> – пароль, который будет использоваться пользователем для аутентификации, задается строкой до 16 символов.
15	Применение SIP-профиля для абонента.	**esr(config-pbx-user)# profile <SIPPROFILE>**	<SIPPROFILE> – SIP-профиль, используемый для данного абонента, задается строкой до 31 символа.

21.5 Алгоритм создания транка регистрации

Шаг	Описание	Команда	Ключи
1	Настройка PBX-сервера.	**esr(config)# pbx**	
2	Создание транка.	**esr(config-pbx)# register-server <name>**	<name> – имя транка, задается строкой до 31 символа.
3	Настройка адреса сервера регистрации.	**esr(config-pbx-reg-server)# ip address <IP>**	<IP> – адрес сервера, на котором происходит регистрация, может принимать значение IP-адреса или задаваться строкой до 31 символа.
4	Настройка порта сервера регистрации.	**esr(config-pbx-reg-server)# ip port <PORT>**	<PORT> – номер UDP-порта сервера регистрации, принимает значения [1..65535]. Если используется стандартный порт 5060, то его можно не указывать.
5	Задание аутентификационного имени.	**esr(config-pbx-reg-server)# username <user>**	<user> – имя пользователя для этого транка на вышестоящем домене, задается строкой до 31 символа.
6	Задание аутентификационного пароля.	**esr(config-pbx-reg-server)# authentication password <password>**	<password> – пароль для этого транка 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**	

21.6 Пример настройки VoIP

Задача:

Подключить аналоговые телефонные аппараты и факс-модемы к IP-сети посредством маршрутизатора ESR. В качестве proxy-сервера и сервера регистрации выступает SIP-сервер, находящийся на ESR.

Решение:



Настройка SIP-профиля:

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

Настройка основного SIP proxy-сервера и сервера регистрации:

```
esr(config-sip-profile)# proxy primary
```

Настройка адреса SIP proxy-сервера (в качестве SIP proxy-сервера использовать встроенный SIP-сервер):

```
esr(config-voip-sip-proxy)# ip address proxy-server 192.0.2.5
```

Настройка порта SIP proxy-сервера:

```
esr(config-voip-sip-proxy)# ip port proxy-server 5080
```

Если используется стандартный порт 5060, то его можно не указывать.

Если необходимо использовать регистрацию, то необходимо выполнить следующие пункты:

Настройка адреса сервера регистрации (в качестве сервера регистрации использовать встроенный SIP-сервер):

```
esr(config-voip-sip-proxy)# ip address registration-server 192.0.2.5
```

Настройка порта сервера регистрации:

```
esr(config-voip-sip-proxy)# ip port registration-server 5080
```

Если используется стандартный порт 5060, то его можно не указывать.

Активация регистрации:

```
esr(config-voip-sip-proxy)# registration
```

Активация proxy-сервера и сервера регистрации:

```
esr(config-voip-sip-proxy)# enable
```

На этом конфигурация SIP proxy-сервера и сервера регистрации закончена:

```
esr(config-voip-sip-proxy)# exit
```

Далее продолжается настройка SIP-профиля.

Настройка SIP-домена:

```
esr(config-sip-profile)# sip-domain address sipdomain.com
```

Если необходимо использовать SIP Domain для регистрации:

```
esr(config-sip-profile)# sip-domain registration enable
```

В такой конфигурации все вызовы будут направлены SIP proxy-серверу. Если необходимо указать другое направление для исходящих вызовов, то необходимо проделать следующее:

Создать план нумерации, см. раздел Управление VoIP.

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
```

21.7 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". Также данный план позволяет осуществлять 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.

21.8 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»:

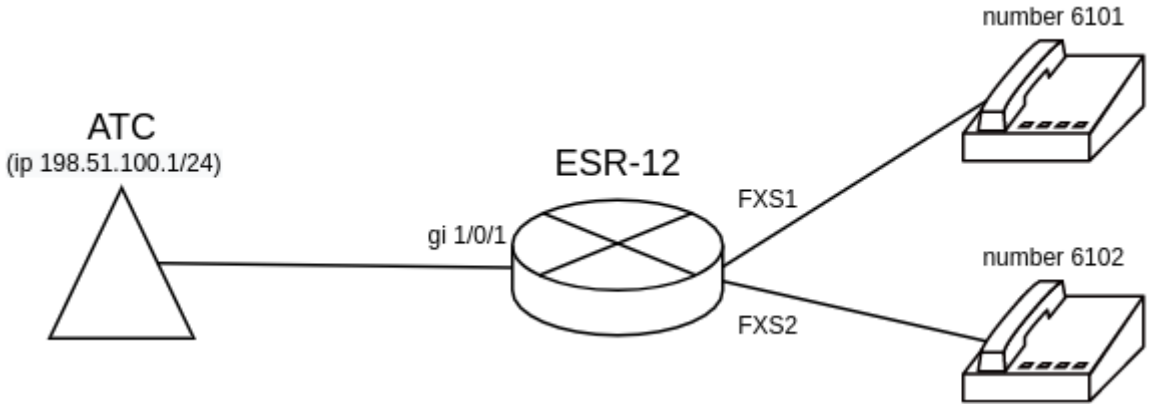
```
esr(config-voice-port-fxo)# hotline ipt
```

Указать номер абонента, который будет получать вызовы с ТфОП:

```
esr(config-voice-port-fxo)# hotline number ipt 305
```

21.9 Пример настройки VoIP для регистрации FXS-портов на внешнем SIP-сервере

Схема:



Задача:

Настроить VoIP для регистрации FXS-портов на внешнем SIP-сервере.

Решение:

Настроим sip-профиль. Необходимо настроить proxy-server для регистрации телефонов, подключенных к FXS-портам:

```
esr(config)# sip profile 1
esr(config-sip-profile)# enable
esr(config-sip-profile)# sip-domain address 198.51.100.1
esr(config-sip-profile)# proxy primary
esr(config-voip-sip-proxy)# enable
esr(config-voip-sip-proxy)# ip address proxy-server 198.51.100.1
esr(config-voip-sip-proxy)# registration
esr(config-voip-sip-proxy)# ip address registration-server 198.51.100.1
esr(config-voip-sip-proxy)# exit
esr(config-sip-profile)# exit
esr(config)#
```

Настроим FXS-порты. Укажем номер, параметры для аутентификации на внешнем сервере и sip-профиль:

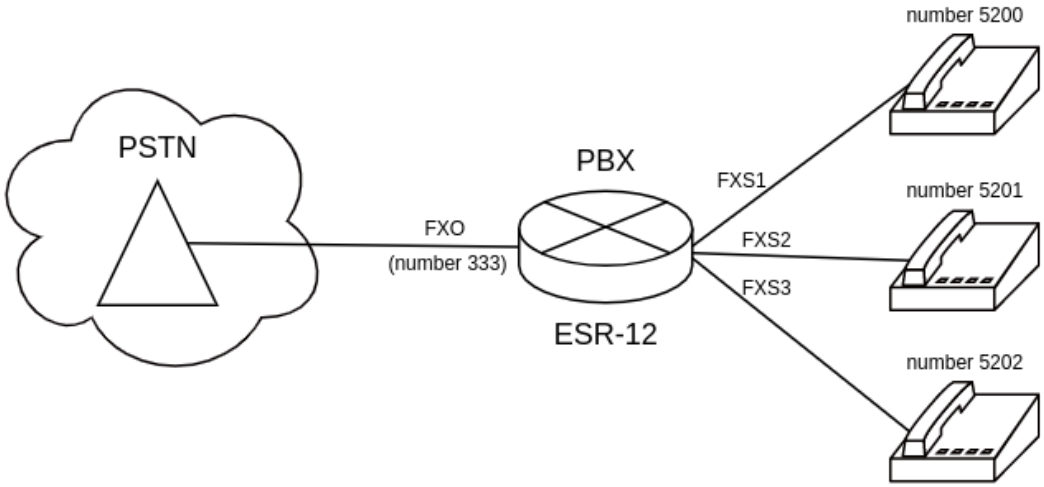
```
esr(config)# interface voice-port 1
esr(config-voice-port-fxs)# sip user phone 6101
esr(config-voice-port-fxs)# authentication name as-phone
esr(config-voice-port-fxs)# authentication password password
esr(config-voice-port-fxs)# profile sip 1
esr(config-voice-port-fxs)# exit
esr(config)# interface voice-port 2
esr(config-voice-port-fxs)# sip user phone 6102
esr(config-voice-port-fxs)# authentication name as-phone
esr(config-voice-port-fxs)# authentication password password
esr(config-voice-port-fxs)# profile sip 1
esr(config-voice-port-fxs)# exit
esr(config)#
```

Для регистрации и прохождения VoIP-трафика за nat необходимо включить на маршрутизаторе tracking и nat для sip, и включить service-voip routing на интерфейсе, через который доступен SIP-сервер:

```
esr(config)# ip firewall sessions tracking sip
esr(config)# nat alg sip
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# service-voip routing
esr(config-if-gi)# exit
esr(config)#
```

21.10 Пример настройки VoIP на внутреннем pbx-сервере

Схема:



Задача:

Настроить регистрацию телефонов, подключенных к FXS-порту, а также настроить регистрацию номера телефонной линии, подключенной к FXO-порту. Также необходимо настроить перевод звонков с FXO-порта на телефон с номером 5200.

Решение:

Настройка PBX.

Создадим pbx-сервер:

```
esr(config)# pbx
esr(config-pbx)#
```

⚠ Структура регулярного выражения pattern описана в разделе Управление VoIP.

Настроим контекст маршрутизации для FXO-порта (пример плана нумерации для перевода вызова на 5200-5202):

```
esr(config-pbx)# ruleset FXO
esr(config-pbx-ruleset)# rule 1
esr(config-pbx-rule)# pattern '_X.,1,Dial(SIP/5200&SIP/5201&SIP/5202)'
esr(config-pbx-rule)# enable
esr(config-pbx-rule)# exit
esr(config-pbx-ruleset)# exit
esr(config-pbx)#
```

Настроим контекст маршрутизации для FXS-портов (пример плана нумерации для набора номера 5200-5202):

```
esr(config-pbx)# ruleset main_rule
esr(config-pbx-ruleset)# rule 1
esr(config-pbx-rule)# pattern '_520[0-3],1,Dial(SIP/${EXTEN},,t)'
esr(config-pbx-rule)# enable
esr(config-pbx-rule)# exit
esr(config-pbx-ruleset)# exit
esr(config-pbx)#
```

Настроим sip-профиль для FXS-портов. Необходимо указать тип клиента, включить необходимые кодеки и подключить контекст маршрутизации:

```
esr(config-pbx)# profile fxs_ports
esr(config-pbx-profile)# client friend
esr(config-pbx-profile)# codec allow g711a
esr(config-pbx-profile)# codec allow g711u
esr(config-pbx-profile)# codec allow g729
esr(config-pbx-profile)# ruleset main_rule
esr(config-pbx-profile)# exit
esr(config-pbx)#
```

Настроим sip-профиль для FXO-портов. Необходимо указать тип клиента, включить необходимые кодеки, настроить invite-port, подключить контекст маршрутизации:

```
esr(config-pbx)# profile fxo_ports
esr(config-pbx-profile)# client friend
esr(config-pbx-profile)# codec allow g711a
esr(config-pbx-profile)# codec allow g711u
esr(config-pbx-profile)# security level invite-port
esr(config-pbx-profile)# ruleset FXO
esr(config-pbx-profile)# exit
esr(config-pbx)#
```

Настроим абонентов на сервере PBX:

```
esr(config-pbx)# user 5200
esr(config-pbx-user)# profile fxs_ports
esr(config-pbx-user)# exit
esr(config-pbx)# user 5201
esr(config-pbx-user)# profile fxs_ports
esr(config-pbx-user)# exit
esr(config-pbx)# user 5202
esr(config-pbx-user)# profile fxs_ports
esr(config-pbx-user)# exit
esr(config-pbx)# user 333
esr(config-pbx-user)# profile fxo_ports
esr(config-pbx-user)# exit
esr(config-pbx)#
```

Включим PBX-сервер:

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

Настроим FXS-порты. Укажем номер и sip-профиль:

```
esr(config)# interface voice-port 1
esr(config-voice-port-fxs)# sip user phone 5200
esr(config-voice-port-fxs)# profile pbx fxs_ports
esr(config-voice-port-fxs)# exit
esr(config)# interface voice-port 2
esr(config-voice-port-fxs)# sip user phone 5201
esr(config-voice-port-fxs)# profile pbx fxs_ports
esr(config-voice-port-fxs)# exit
esr(config)# interface voice-port 3
esr(config-voice-port-fxs)# sip user phone 5202
esr(config-voice-port-fxs)# profile pbx fxs_ports
esr(config-voice-port-fxs)# exit
esr(config)#
```

Настроим FXO-порт. Укажем номер и sip-profile, активируем услугу «Hostline PSTN to IP»: и укажем номер абонента, который будет получать вызовы с ТфОП:

```
esr(config)# interface voice-port 4
esr(config-voice-port-fxo)# sip user phone 333
esr(config-voice-port-fxo)# profile pbx fxo_ports
esr(config-voice-port-fxo)# hotline ipt
esr(config-voice-port-fxo)# hotline number ipt 5200
esr(config-voice-port-fxo)# exit
esr(config)#
```

22 Управление лицензированием

- Лицензирование через ELM
  - Периодичность обращений к ELM
  - Условия преждевременного сброса лицензии
  - Алгоритм настройки
  - Пример настройки
- Файловое лицензирование
- Лицензирование в кластере
  - Синхронизация файловых лицензий
  - Установка файловых лицензий

Для загрузки лицензий на устройство предусматривается два способа лицензирования:

1. Лицензирование через взаимодействие с системой лицензирования ELM (Eltex License Manager), осуществляющую функцию лицензирования программных и аппаратных продуктов компании «Элтекс».
2. Файловое лицензирование (только ESR)

22.1 Лицензирование через ELM

Онлайн-лицензирование поддерживается на vESR и ESR.

Существует 2 варианта работы с ELM:

- *Online ELM* — сервер лицензирования, расположенный на стороне компании «Элтекс». Установка дополнительного ПО не требуется.

Адрес ELM
`https://elm.eltex-co.ru:8099`

- *Offline ELM* — сервер лицензирования, устанавливаемый локально на стороне заказчика. Подходит для эксплуатации в закрытом контуре. Подробная информация об Offline ELM доступна в официальной документации Offline ELM.

В обоих вариантах необходимо, чтобы между сервером и устройством была сетевая доступность.

22.1.1 Периодичность обращений к ELM

1. При включении менеджера лицензирования на ESR (vESR) устройство сразу попытается обратиться за лицензией:

- в случае успешного обращения устройство начнет обращаться к серверу раз в час,
- в случае неуспешного обращения устройство будет пытаться получить лицензию раз в 15 минут.

2. В случае, если менеджер лицензирования был включен на момент перезапуска устройства, то после перезапуска устройство сразу обратиться за лицензией. При неудачной попытке:

- устройство будет пытаться получить лицензию раз в 5 минут (до сброса лицензии) если до перезапуска имелась действующая ELM-лицензия,
- устройство будет пытаться получить лицензию раз в 15 минут, если на момент перезапуска ELM-лицензии не было.

3. В случае сброса лицензии устройство будет пытаться получить лицензию раз в 15 минут.

22.1.2 Условия преждевременного сброса лицензии

Лицензия на устройстве будет преждевременно сброшена, если:

1. был отключен менеджер лицензирования на устройстве;
2. устройство не смогло в течение 168 часов успешно обратиться на ELM;
3. устройство после перезапуска не смогло в течение 15 минут обратиться на ELM.

Чтобы снова получить лицензию, необходимо успешное обращение устройства на ELM.

22.1.3 Алгоритм настройки

⚠ Перед настройкой менеджера лицензирования на vESR требуется указать в системных настройках серийный номер vESR и ключ лицензии ELM (см. Руководство по установке и настройке vESR, раздел Лицензирование vESR).

Шаг	Описание	Команда	Ключи
1	Перейти в конфигурирование менеджера лицензирования.	**esr (config)# licence-manager**	
2	Задать IP-адрес ELM-сервера.	**esr (config-licence-manager)# host address <A.B.C.D | WORD | X:X:X:X::X>**	<IP-ADDR> – IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> – IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]. WORD(1-31) – DNS-имя сервера.
3	Задать порт для подключения к ELM-серверу. (необязательно).	**esr (config-licence-manager)# host port <PORT>**	<PORT> – номер TCP/UDP-порта отправителя, принимает значения [1..65535], по умолчанию 8099.
4	Включить менеджер лицензирования.	**esr (config-licence-manager)# enable**	
5	Установить описание (необязательно).	**esr (config-licence-manager)# description <LINE>**	<LINE> – описание, задаётся строкой до 255 символов.
6	Задать текстовое имя устройства, которое передаётся на сервер ELM (необязательно).	**esr (config-licence-manager)# system-name <WORD>**	<WORD> – имя, задаётся строкой до 255 символов.

Шаг	Описание	Команда	Ключи
7	Задать текстовое описание, которое передаётся на сервер ELM (необязательно).	**esr (config-licence-manager)# location <WORD>**	<WORD> – описание, задаётся строкой до 255 символов.
8	Указать экземпляр VRF, в котором будет работать менеджер лицензирования (необязательно).	**esr (config-licence-manager)# ip vrf forwarding <VRF>**	<VRF> – имя VRF, задается строкой до 31 символа.
9	Задать значение DSCP, которое будет использоваться для маркировки трафика при обращениях к ELM-серверу (необязательно).	**esr(config-licence-manager)# dscp <DSCP>**	<DSCP> – значение DSCP, принимает значения [0..63], по умолчанию 48.

22.1.4 Пример настройки

В режиме конфигурирования licence-manager укажем адрес и порт ELM-сервера. Между устройством и ELM-сервером должна быть сетевая доступность.

```
esr(config-licence-manager)# host address elm.eltex-co.ru
esr(config-licence-manager)# host port 8099
esr(config-licence-manager)# enable
```

После включения менеджера лицензирования устройство попытается обратиться на указанный сервер.

Команда **show licence-manager status** выведет подробную информацию об обращениях на сервер лицензирования:

```
esr# show licence-manager status
ELM server type:                root
Last request status:            success
Last request to licence server: 2024-08-12 04:01:00
Next request to licence server: 2024-08-12 04:57:07
```

Команда **update licence-manager licence** позволит принудительно отправить запрос на ELM-сервер, не дожидаясь времени следующего запроса:

```
esr# update licence-manager licence
2024-08-12T04:01:00+00:00 %LICENCE-W-EVENT: Licence recieved from Eltex Licence Manager server
```

Команда **show licence** позволит вывести информацию о лицензиях на устройстве:

```
esr# show licence
ELM licence:
    Licence is valid from: 2025-08-18 08:43:44
    Licence expires:       2026-08-18 08:43:44

Feature                    Source  State   Value  Valid from          Expiries
-------------------------  ------  ------  -----  ------------------  --------------------
ESR-SECURITY-WF-KASPERSKY  ELM     Active  true   2024-06-15 23:47:04  2040-06-18 23:10:14
```

Как видно, у ELM-лицензий на месте Source указывается **ELM**.

22.2 Файловое лицензирование

Данный вид лицензирования поддерживается только на ESR.

Пример содержания файла лицензии

```
{
    "name": "Eltex",
    "version":  "1.0",
    "type": "ESR-200",
    "sn":   "NP10000001",
    "mac":  "A8:F9:4B:00:00:01",
    "publickey":    0,
    "features": "BRAS,IPS,WIFI",
    "sign": "4aafe3d7abfc0d995c1829c73967e23ec55f8e260567fdc9..."
}
```

Загрузка лицензии осуществляется в **system:licence** с помощью команды **copy**:

```
esr# copy tftp://<IP_address>:/NP10000001.lic system:licence
|****************************************| 100% (681B) Licence loaded successfully. Please
reboot system to apply changes.
```

После чего необходимо будет перезапустить устройство.

При выводе лицензий командой **show licence** такие лицензии помечаются как **File (v1)**:

```
esr# show licence
Feature   Source      State        Value   Valid from   Expiries
-------   ---------   ----------   -----   ----------   --------
BRAS      File (v1)   Active       true    --           --
BRAS      File (v1)   Candidate    true    --           --
IPS       File (v1)   Active       true    --           --
IPS       File (v1)   Candidate    true    --           --
WIFI      File (v1)   Active       true    --           --
WIFI      File (v1)   Candidate    true    --           --
```

Состояние **Active** говорит о том, что лицензия сейчас активна.

Состояние **Candidate** говорит о том, что лицензия будет применена при перезапуске.

22.3 Лицензирование в кластере

22.3.1 Синхронизация файловых лицензий

Для синхронизации файлов лицензий в кластере необходимо загрузить их все на Active-устройство командой **copy** в директорию **system:cluster-unit-licences**.

Все загруженные лицензии в данной директории передаются остальным участникам кластера.

Пример

```
ESR-1# copy tftp://<IP_address>:/licence system:cluster-unit-licences
|************************| 100% (680B) Licence loaded successfully.
```

⚠ На каждый ESR нужна отдельная лицензия (Wi-Fi, BRAS и т. д.).
Для активации функций кластера не нужна отдельная лицензия.

22.3.2 Установка файловых лицензий

Установить лицензию в кластере можно двумя способами:

1. Загрузить индивидуально лицензию на каждое устройство, как в случае с обычным ESR вне кластера.
2. Загрузить лицензию для Active-юнита в **system:licence** (данная лицензия также автоматически загрузится и в **system:cluster-unit-licences**), активировать её перезагрузкой, лицензии для Standby загрузить в **system:cluster-unit-licences** на Active-юните, после чего либо выполнить команду **sync cluster system force**, либо подключить Standby по ZTP.

Пример

```
ESR-1# copy tftp://<IP_address>:/licence system:cluster-unit-licences
|************************| 100% (680B) Licence loaded successfully.
ESR-1#
ESR-1#
ESR-1#
ESR-1# show cluster-unit-licences
Serial number     Features
---------------   ------------------------------------------------------------
NP0B003634        BRAS,IPS,WIFI
NP0B009033        BRAS,IPS,WIFI
ESR-1# sync cluster system force
```

23 Автоматическое развертывание

- Примеры использования автоматического развертывания
  - Автоматическое развертывание с использованием внешнего DHCP-сервера
  - Алгоритм настройки
  - Пример настройки
  - Автоматическое развертывание с загрузочного носителя
  - Пример настройки
  - Автоматическое развертывание нового юнита в кластере
  - Пример настройки

Автоматическое развертывание (ZTP) – позволяет автоматически конфигурировать или обновлять версию ПО устройства.

23.1 Примеры использования автоматического развертывания

23.1.1 Автоматическое развертывание с использованием внешнего DHCP-сервера

Автоматическое развертывание позволяет настроить устройство дистанционно при организации IP-связности, используя удаленный DHCP-сервер.

23.1.2 Алгоритм настройки

Шаг	Описание	Команда
1	Настроить получение адреса по DHCP.	
2	Включить загрузку конфигурации маршрутизатора при автоматическом развертывании.	**esr(config)# boot host auto-config**
3	Включить загрузку ПО маршрутизатора при автоматическом развертывании.	**esr(config)# boot host auto-update**

⚠ Команды активируются только после перезагрузки устройства.

⚠ При использовании в конфигурации одновременно **boot host auto-config** и **boot host auto-update** сначала выполнится обновление ПО, а затем будет выполнена загрузка конфигурации.

23.1.3 Пример настройки

Задача:

Используя автоматическое развертывание:

- обновить версию ПО;
- загрузить конфигурацию.

Исходная конфигурация устройства:

ESR-1

```
boot host auto-config
boot host auto-update

bridge 1
  vlan 1
  ip address dhcp
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
exit
```

> В качестве исходной конфигурации устройства также можно использовать factory-конфигурацию, т. к. она уже содержит в себе команды **boot host auto-config** и **boot host auto-update**, подключая устройство в сеть через порты, где настроен DHCP-клиент.

Решение:

На DHCP-сервере необходимо настроить:

- **filename** – указывает путь к скачиваемому файлу ПО на tftp-сервере;
- **option 66** – указывает адрес tftp-сервера, с которого будут загружаться ПО и конфигурация;
- **option 67** – указывает путь к скачиваемому конфигурационному файлу на tftp-сервере.

Пример настройки опций на DHCP-сервере

```
filename "esr.firmware";
option tftp-server-name "198.51.100.1";
option bootfile-name "esr-ztp-config.txt";
```

После настройки DHCP-сервера и активации команд для автоматического развертывания, при получении от DHCP-сервера DHCP Offer с опциями ESR начнет процесс автоматического развертывания.

Процесс автоматического развертывания можно отслеживать по логам в консоль.

ESR-1 | auto-update

```
%CFG_MGR-I-AUTOUPDATE: start with firmware file '198.51.100.1:/esr.firmware'
%FILE_MGR-I-INFO: operation started: 'copy tftp://198.51.100.1:/esr.firmware system:firmware'
 (index: 1, origin: Cfgsync-mgr)
%CFG_MGR-I-AUTOCONFIG: start with configuration file '198.51.100.1:/esr-ztp-config.txt'
%FIRMWARE-I-INFO: Verify firmware...
%FIRMWARE-I-INFO: Firmware version: 1.37.4 build 2[4b06f2c798] 2025-12-03 14:23:46
%FIRMWARE-I-INFO: Check firmware version...
%FIRMWARE-I-INFO: Writing data...
%FILE_MGR-I-INFO: operation is finished: 'copy tftp://198.51.100.1:/esr.firmware
system:firmware' (index: 1, origin: Cfgsync-mgr)
%CFG_MGR-I-AUTOUPDATE: firmware file loaded succesfully
%CFG_MGR-I-AUTOUPDATE: switch boot to image-1 (may take  up to 2 min)
%FILE_MGR-I-INFO: operation started: 'boot system image-1' (index: 2, origin: Cfgsync-mgr)
%FIRMWARE-I-INFO: Writing data...
%FILE_MGR-I-INFO: operation is finished: 'boot system image-1' (index: 2, origin: Cfgsync-mgr)
%CFG_MGR-I-AUTOUPDATE: completed successfully, reboot
```

ESR-1 | auto-config

```
%CFG_MGR-I-AUTOUPDATE: start with firmware file '198.51.100.1:/esr.firmware'
%FILE_MGR-I-INFO: operation started: 'copy tftp://198.51.100.1:/esr.firmware system:firmware'
 (index: 1, origin: Cfgsync-mgr)
%CFG_MGR-I-AUTOCONFIG: start with configuration file '198.51.100.1:/esr-ztp-config.txt'
%FIRMWARE-I-INFO: Verify firmware...
%FIRMWARE-I-INFO: Firmware version: 1.37.4 build 2[4b06f2c798] 2025-12-03 14:23:46
%FIRMWARE-I-INFO: Check firmware version...
%FILE_MGR-I-INFO: operation is finished: 'copy tftp://198.51.100.1:/esr.firmware
system:firmware' (index: 1, origin: Cfgsync-mgr)
%CFG_MGR-I-AUTOUPDATE: firmware file loaded (Firmware is same version.)
%CFG_MGR-I-AUTOUPDATE: loaded firmware have older or same version, nothing to update
%FILE_MGR-I-INFO: operation started: 'copy tftp://198.51.100.1:/esr-ztp-config.txt
system:candidate-config' (index: 2, origin: Cfgsync-mgr)
%FILE_MGR-I-INFO: operation is finished: 'copy tftp://198.51.100.1:/esr-ztp-config.txt
system:candidate-config' (index: 2, origin: Cfgsync-mgr)
%CFG_MGR-I-AUTOCONFIG: configuration file loaded succesfully
%SYS-W-EVENT: WARNING!!! the device can be accessed using the admin user with the default
 password
%SYS-W-EVENT: WARNING!!! 'boot host auto-config' will be disabled after reboot hardware
%SYS-W-EVENT: WARNING!!! 'boot host auto-update' will be disabled after reboot hardware
%LINK-W-DOWN: bridge 1 changed state to down
%CFG_MGR-I-AUTOCONFIG: completed successfully
```

23.1.4 Автоматическое развертывание с загрузочного носителя

Автоматическое развертывание с загрузочного носителя позволяет настроить устройство без организации IP-связности.

В процессе автоматического развертывания с загрузочного носителя будет загружена и применена на устройство конфигурация, файл для которой будет называться **startup-config.conf**.

23.1.5 Пример настройки

Задача:

Используя автоматическое развертывание с загрузочного носителя, обновить конфигурацию на устройстве.

> ⚠ После автоматического развертывания необходимо извлечь загрузочный носитель или удалить с него файл с загружаемой конфигурацией, иначе при последующей перезагрузке устройства все внесенные данные в конфигурацию будут потеряны.

Решение:

При загрузке устройства с загрузочным носителем, на котором будет находится файл конфигурации с наименованием **startup-config.conf**, будет загружена и применена данная конфигурация, что можно отследить по логам в консоли.

ESR

```
%SYS-W-EVENT: The configuration has been loaded from '/media/usb/FAT32/startup-config.conf'
 path successfully
```

23.1.6 Автоматическое развертывание нового юнита в кластере

Автоматическое развертывание позволяет настроить нового юнита в кластере дистанционно при организации IP-связности с Active-юнитом в кластере.

В процессе автоматического развертывания в кластере подключаемый юнит обновит: версию ПО, конфигурацию и время, а также загрузит функциональную лицензию, если она предварительно был загружена на Active-устройство.

23.1.7 Пример настройки

Задача:

Используя автоматическое развертывание в кластере, подключить новый юнит.

Исходная конфигурация Active-юнита в кластере:

ESR-1

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address 68:13:e2:e2:05:28
  exit
  unit 2
    mac-address 68:13:e2:e2:04:38
  exit
  enable
exit

hostname ESR-1 unit 1
hostname ESR-2 unit 2

security zone SYNC
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  vrrp 1
    ip address 198.51.100.1/24
    priority 254 unit 1
    priority 253 unit 2
    group 1
    enable
  exit
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/1
  mode switchport
  spanning-tree disable
exit

security zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
exit
```

⚠ MAC-адрес подключаемого юнита должен настроен на Active-устройстве до начала процесса ZTP.

Исходная конфигурация подключаемого юнита в кластере:

ESR-2

```
bridge 1
  vlan 1
  ip address dhcp
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
exit
```

⚠ В качестве исходной конфигурации устройства также можно использовать factory-конфигурацию, подключая устройство в сеть через порты, где настроен DHCP-клиент.

Решение:

После настройки Active-юнита и подключения нового юнита в сеть процесс автоматического развертывания запускается автоматически.

Отслеживать процесс автоматического развертывания при подключении нового юнита в кластер можно по логам в консоли.

ESR-1 | Active юнит

```
%CLUSTER-I-ZTP_INFO: from unit 2 'ESR-2': cluster detected by DHCP client
%CLUSTER-I-SYNC_SYSTEM_INFO: from unit 2 'ESR-2': start system synchronization with Active unit
%FILE_MGR-I-INFO: operation started: 'copy system:firmware flash:firmware' (index: 1, origin:
esrfs)
%FILE_MGR-I-INFO: operation is finished: 'copy system:firmware flash:firmware' (index: 1,
origin: esrfs)
%FILE_MGR-I-INFO: operation started: 'copy system:firmware flash:firmware' (index: 2, origin:
esrfs)
%FILE_MGR-I-INFO: operation is finished: 'copy system:firmware flash:firmware' (index: 2,
origin: esrfs)
%CLUSTER-I-SYNC_SYSTEM_INFO: from unit 2 'ESR-2': system will be rebooted for apply all changes
```

ESR-2 | Подключаемый unit

```
%CLUSTER-I-ZTP_INFO: cluster detected by DHCP client
%CLUSTER-I-SYNC_SYSTEM_INFO: start system synchronization with Active unit
%FILE_MGR-I-INFO: operation started: 'copy tftp://198.51.100.1:/ESR-running-config
system:candidate-config' (index: 2, origin: Cfgsync-mgr)
%FILE_MGR-I-INFO: operation is finished: 'copy tftp://198.51.100.1:/ESR-running-config
system:candidate-config' (index: 2, origin: Cfgsync-mgr)
%FILE_MGR-I-INFO: operation started: 'copy tftp://198.51.100.1:/ESR-30-active-firmware
system:firmware' (index: 3, origin: Cfgsync-mgr)
%FIRMWARE-I-INFO: Verify firmware...
%FIRMWARE-I-INFO: Firmware version: 1.37.4 build 2[4b06f2c798] 2025-12-03 14:23:46
%FIRMWARE-I-INFO: Check firmware version...
%FIRMWARE-I-INFO: Writing data...
%FILE_MGR-I-INFO: operation is finished: 'copy tftp://198.51.100.1:/ESR-30-active-firmware
system:firmware' (index: 3, origin: Cfgsync-mgr)
%FILE_MGR-I-INFO: operation started: 'boot system image-1' (index: 4, origin: Cfgsync-mgr)
%FIRMWARE-I-INFO: Writing data...
%FILE_MGR-I-INFO: operation is finished: 'boot system image-1' (index: 4, origin: Cfgsync-mgr)
%CLUSTER-I-SYNC_SYSTEM_INFO: system will be rebooted for apply all changes
%SYS-C-REBOOT: Cfgsync-mgr: Cluster unit synchronization completed at 10.03.2026 10:58:45
```

После автоматического развертывания убедимся, что подключаемый юнит готов к работе и все подсистемы синхронизированы.

ESR-1 | Active-юнит

```
ESR-1# show cluster status
Unit   Hostname               Role         MAC address         State            IP address
----   --------------------   ----------   -----------------   --------------   ---------------
1*     ESR-1                  Active       68:13:e2:e2:05:28   Joined           198.51.100.254
2      ESR-2                  Standby      68:13:e2:e2:04:38   Joined           198.51.100.253
ESR-1# show cluster sync status
System part              Synced
----------------------   ------
candidate-config         Yes
running-config           Yes
SW version               Yes
licence                  Yes
licence (After reboot)   Yes
date                     Yes
```

24 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-if-port-channel)# speed 10G
```

Как полностью очистить конфигурацию 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
```

В случае невозможности аутентификации на маршрутизаторе (неизвестен логин/пароль) конфигурацию можно сбросить к заводской следующим образом:

1. дождаться полной загрузки маршрутизатора
2. зажать функциональную кнопку "F" на 15 секунд
3. отпустить функциональную кнопку "F"
4. дождаться полной загрузки маршрутизатора с заводской конфигурацией

Как привязать subinterface к созданным VLAN?

При создании саб-интерфейса VLAN создается и привязывается автоматически (прямая зависимость индекс sub – VID).

```
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 0.0.0.0/0
```

Проблема прохождения асинхронного трафика

В случае организации сети с асинхронной маршрутизацией, Firewall будет запрещать "неправильный (ошибочный)" входящий трафик (не открывающий новое соединение и не принадлежащий никакому установленному соединению) из соображений безопасности.

Разрешающее правило в Firewall не решит поставленную задачу для подобных схем.

Решить задачу можно, отключив Firewall на входном интерфейсе:

```
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
```

25 Приложение A. Packet Flow

- Порядок обработки входящего/исходящего трафика сетевыми службами маршрутизаторов ESR
- Порядок обработки транзитного трафика сетевыми службами маршрутизаторов ESR

25.1 Порядок обработки входящего/исходящего трафика сетевыми службами маршрутизаторов ESR

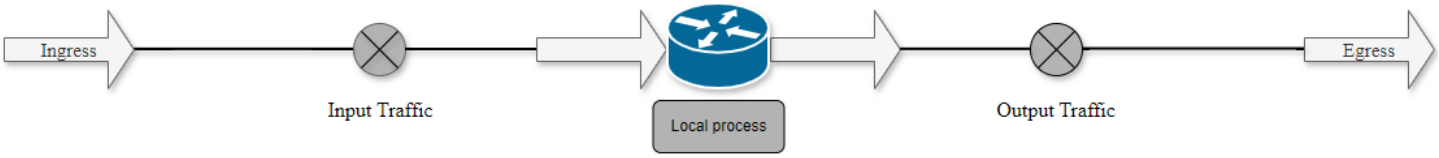


Таблица 1 – Порядок обработки входящего трафика

Шаг	Описание
1	Выполнение функций ACL на входящем трафике
2	Выполнение функций QoS (ограничение полосы пропускания, классификация и т. д.)
3	Выполнение функций DOS defense[1]. На данном этапе выполняются функции защиты от DDOS из разделов firewall screen dos-defense, firewall screen spy-blocking, firewall screen suspicious-packets
4	Инспектирование пакета сервисом IDS/IPS в режиме service-ips monitor[1]
5	Отключение функций Firewall командой ip firewall disable. Разрешение трафика исключает проверки на этапах 6, 13, 15
6	Выполнение правил между зонами any/self
7	Выполнение дефрагментации пакета
8	Выполнение начальных функций BRAS (инициализация соединений, сессий)[1]
9	Выполнение HTTP/HTTPs прокси[1]
10	Функции Destination NAT[1]
11	Routing Decision (FIB)
12	Выполнение функций DOS defense[1]. На этапе данном этапе выполняются специфичные функции защиты от DDOS из разделов firewall screen dos-defense, firewall screen spy-blocking, firewall screen suspicious-packets: ip firewall screen suspicious-packets large-icmp ip firewall screen dos-defense winnuke ip firewall screen spy-blocking port-scan
13	Выполнение правил между пользовательскими зонами / self
14	Разрешение служебного трафика кластера[1]

15	Передача пакета в DPI[1]
16	Передача пакета в Netflow/sFlow (Ingress)[1]
17	IPsec (decode)[1]. После выполнения этого шага происходит переход к п.1

Таблица 2 – Порядок обработки исходящего трафика

Шаг	Описание
1	Local Policy Based Routing[1]
2	Route Decision
3	Передача пакета в DPI[1]
4	tcp adjust-mss[1]
5	Netflow/sFlow (Egress)[1]
6	BRAS (для исходящих пакетов)[1]
7	Выполнение функций Source NAT[1]
8	IPsec (encode)[1]
9	Выполнение фрагментации пакетов
10	Выполнение функций QoS (ограничение полосы пропускания, классификация и т. д.)

[1]Данная функция выполняется только при наличии необходимых настроек.

25.2 Порядок обработки транзитного трафика сетевыми службами маршрутизаторов ESR



Таблица 3 – Порядок обработки транзитного трафика

Шаг	Описание
1	Выполнение функций ACL на входящем трафике
2	Выполнение функций QoS (ограничение полосы пропускания, классификация и т. д.)
3	Выполнение функций DOS defense[1]. На данном этапе выполняются функции защиты от DDOS из раздела firewall screen dos-defense, firewall screen spy-blocking, firewall screen suspicious-packets
4	Отключение функций Firewall командой ip firewall disable. Разрешение трафика исключает проверки на этапах 5, 15, 16
5	Выполнение правил между пользовательскими зонами / any
6	Выполнение дефрагментации пакета
7	Выполнение начальных функций BRAS (инициализация соединений, сессий)[1]
8	Разрешение трафика, исходящий порт которого voice-port. Разрешение трафика включается только в случае наличия настроенного voice-port.
9	Выполнение HTTP/HTTPS прокси[1]
10	Функции Destination NAT[1]
11	Policy Based Routing
12	Routing Decision (FIB)
Если пакет перед передачей необходимо обработать протоколом более высокого уровня, выполняются следующие действия:	
12.1	Выполнение функций DOS defense[1]. На данном этапе выполняются специфичные функции защиты от DDOS из разделов firewall screen dos-defense, firewall screen spy-blocking, firewall screen suspicious-packets: ip firewall screen suspicious-packets large-icmp ip firewall screen dos-defense winnuke ip firewall screen spy-blocking port-scan

Шаг	Описание
12.2	Передача пакета в DPI[1]
12.3	Передача пакета в Netflow/sFlow (Ingress)[1]
12.4	IPsec (decode)[1]. После выполнения этого шага происходит переход к п.1
13	tcp adjust-mss[1]
14	Выполнение функций DOS defense[1]. На данном этапе выполняются специфичные функции защиты от DDOS из разделов firewall screen dos-defense, firewall screen spy-blocking, firewall screen suspicious-packets: ip firewall screen suspicious-packets large-icmp ip firewall screen dos-defense winnuke ip firewall screen spy-blocking port-scan
15	Выполнение правил между пользовательскими зонами или внутри зоны, или между специальными зонами any/any
16	Передача пакета в DPI[1]
17	Разрешение трафика, исходящий порт которого voice-port. Разрешение трафика включается только в случае наличия настроенного voice-port.
18	Netflow/sFlow (Egress)[1]
19	Инспектирование пакета сервисом IPS/IDS в режиме service-ips inline[1]
20	BRAS (для исходящих пакетов)[1]
21	Выполнение функций Source NAT[1]
22	IPsec (encode)[1]
Если необходимо шифрование, то после этого процесса, выполняются следующие операции:	
22.1	Передача пакета в DPI[1]
22.2	tcp adjust-mss[1]
22.3	Netflow/sFflow (Egress)[1]
22.4	BRAS (для исходящих пакетов)
22.5	Выполнение функций Source NAT[1]

Шаг	Описание
23	Выполнение фрагментации пакетов
24	Выполнение функций QoS (ограничение полосы пропускания, классификация и т. д.)

⚠ [1]Данная функция выполняется только при наличии необходимых настроек.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения технической консультации по вопросам эксплуатации оборудования ООО «Предприятие «ЭЛТЕКС» вы можете обратиться в Сервисный центр компании:

Форма обратной связи на сайте: https://eltex.ru/support/

Servicedesk: https://servicedesk.eltex-co.ru

На официальном сайте компании вы можете найти техническую документацию и программное обеспечение для продукции ООО «Предприятие «ЭЛТЕКС», обратиться к базе знаний, оставить интерактивную заявку:

Официальный сайт компании: https://eltex.ru

База знаний: https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base

Центр загрузок: https://eltex.ru/download/