

Ethernet-коммутаторы

**MES2300-xx, MES3300-xx, MES3500I-10P, MES5312,
MES5316A, MES5324A, MES5332A, MES5310-48, MES5400-24,
MES5400-48, MES5410-48, MES5500-32**

Руководство по эксплуатации, версия ПО 6.6.4

| Версия документа | Дата выпуска | Содержание изменений |
|------------------|--------------|--|
| Версия 1.31 | 12.08.2024 | <p>Добавлены разделы:</p> <p>3.2.3 Установка устройства MES3500I-10P на DIN-рейку</p> <p>5.23.1 Диагностика медного кабеля</p> <p>4.5.1.2 Расширенная настройка уровня доступа</p> <p>5.23.1 Диагностика медного кабеля</p> <p>5.24.3 Настройка функции MAC Address Notification</p> <p>Изменения в разделах:</p> <p>2.1 Назначение</p> <p>2.2.8 Дополнительные функции</p> <p>2.3 Основные технические характеристики</p> <p>2.4.4 Световая индикация</p> <p>4.4 Режим работы коммутатора</p> <p>5.8 Конфигурация временных интервалов time-rang</p> <p>5.9.4 Настройка интерфейса IP</p> <p>5.11.3 Настройка технологии Multi-Switch Link Aggregation Group (MLAG)</p> <p>5.12 Настройка IPv4-адресации</p> <p>5.15.5.1 Настройка протокола STP, RSTP</p> <p>5.19.4 Протокол управления сетью (SNMP)</p> <p>5.29.1 Настройка QoS</p> <p>5.30.4 Настройка протокола BGP (Border Gateway Protocol)</p> <p>5.30.6 Настройка Route-Map</p> <p>Добавлено описание моделей коммутаторов MES2300B-24, MES2300DI-28, MES2300D-24P, MES3500I-10P, MES3300-48F, MES5310-48</p> |
| Версия 1.30 | 21.05.2024 | <p>Изменения в разделах:</p> <p>2.4.4 Световая индикация</p> <p>5.9.1 Параметры Ethernet-интерфейсов, Port-Channel и Loopback-интерфейсов</p> |
| Версия 1.29 | 18.04.2024 | <p>Добавлен раздел:</p> <p>5.24.7 Функционал First Hop Security</p> <p>Изменения в разделах:</p> <p>5.9.3 Настройка Private VLAN</p> <p>5.19.1 Механизм AAA</p> <p>5.30.3 Настройка протокола OSPF, OSPFv3</p> <p>5.31 Конфигурация VXLAN</p> <p>Добавлено описание моделей коммутаторов MES2300-24P, MES2300B-24F, MES3300-08F, MES3300-16F</p> |
| Версия 1.28 | 15.03.2024 | Добавлено описание модели коммутатора MES5410-48 |
| Версия 1.27 | 29.02.2024 | Синхронизация с версией ПО 6.6.2.9 |
| Версия 1.26 | 15.12.2023 | <p>Изменения в разделах:</p> <p>5.11.2 Протокол агрегации каналов LACP</p> <p>5.14.1 Протокол IPv6</p> <p>5.30.1 Конфигурация статической маршрутизации</p> <p>5.30.4 Настройка протокола BGP (Border Gateway Protocol)</p> <p>5.30.10 Настройка Virtual Router Redundancy Protocol (VRRP)</p> <p>Добавлено описание моделей коммутаторов MES2300-48P, MES2300B-48, MES3300-48</p> |
| Версия 1.25 | 09.10.2023 | Добавлено описание моделей коммутаторов MES2300-24, MES3300-24 |
| Версия 1.24 | 07.09.2023 | <p>Изменения в разделах:</p> <p>2.3 Основные технические характеристики</p> <p>5.30.10 Настройка Virtual Router Redundancy Protocol (VRRP)</p> |
| Версия 1.23 | 26.07.2023 | <p>Изменения в разделах:</p> <p>2.2.3 Функции второго уровня сетевой модели OSI</p> <p>5.4 Команды управления системой</p> <p>5.10 Storm Control для различного трафика (broadcast, multicast, unknown unicast)</p> <p>5.15.5.2 Настройка протокола MSTP</p> <p>5.17.5 Radius-авторизация запросов IGMP</p> <p>5.18.1 Протокол PIM</p> <p>5.24.3 Контроль протокола DHCP и опция 82</p> |

| | | |
|-------------|------------|--|
| | | <p>5.29.1 Настройка QoS 5.30.3 Настройка протокола OSPF, OSPFv3 5.30.12 Конфигурация виртуальной области маршрутизации (VRF lite)</p> <p>Добавлено описание моделей коммутаторов MES3300-24F</p> |
| Версия 1.22 | 7.04.2023 | <p>Изменения в разделах: 5.15.5 Семейство протоколов STP (STP, RSTP, MSTP), PVSTP+, RPVSTP+ 5.19.7 Настройка доступа</p> |
| Версия 1.21 | 10.03.2023 | <p>Добавлены разделы: 5.18.2 Функция PIM Snooping</p> <p>Изменения в разделах: 2.3 Основные технические характеристики 4.4 Режим работы коммутатора 5.15.2 Настройка протокола ARP 5.16 Voice VLAN 5.17.1 Функция посредника протокола IGMP (IGMP Snooping) 5.18.1 Протокол PIM 5.18.4 Функция IGMP Proxy 5.19.7.1 Telnet, SSH 5.24.2 Проверка подлинности клиента на основе порта (стандарт 802.1x) 5.30.1 Конфигурация статической маршрутизации 5.30.3 Настройка протокола OSPF, OSPFv3 5.30.10 Настройка Virtual Router Redundancy Protocol (VRRP) 5.30.12 Конфигурация виртуальной области маршрутизации (VRF lite) 5.31 Конфигурация VXLAN</p> |
| Версия 1.20 | 11.11.2022 | <p>Изменения в разделах: 5.9.1 Параметры Ethernet-интерфейсов, Port-Channel и Loopback-интерфейсов</p> |
| Версия 1.19 | 30.09.2022 | <p>Изменения в разделах: 5.15.5.1 Настройка протокола STP, RSTP 5.30.1 Конфигурация статической маршрутизации</p> |
| Версия 1.18 | 29.07.2022 | <p>Добавлены разделы: 5.31 Конфигурация VXLAN</p> <p>Изменения в разделах: 2.3 Основные технические характеристики 2.4 Конструктивное исполнение 5.15.5.1 Настройка протокола STP, RSTP 5.18.1 Протокол PIM</p> <p>Добавлено описание моделей коммутаторов MES5400-24, MES5400-48</p> |
| Версия 1.18 | 05.03.2022 | <p>Добавлены разделы: 5.15.8 Настройка функции Flex-link 5.11.3 Настройка технологии Multi-Switch Link Aggregation Group (MLAG) 5.24 IP Service Level Agreements (IP SLA)</p> <p>Изменения в разделах: 5.11 Группы агрегации каналов – Link Aggregation Group (LAG) 5.12 Настройка IPv4-адресации</p> |
| Версия 1.17 | 31.01.2022 | <p>Добавлены разделы: 5.15.8 Настройка функции Flex-link 5.15.9 Настройка функции Layer 2 Protocol Tunneling (L2PT)</p> <p>Изменения в разделах: 4.3 Загрузочное меню 5.9.2 Настройка VLAN и режимов коммутации интерфейсов 5.17.1 Функция посредника протокола IGMP (IGMP Snooping) 5.21 Зеркалирование (мониторинг) портов 5.29.1 Настройка 6.1 Меню Startup</p> |
| Версия 1.16 | 18.06.2021 | <p>Изменения в разделах: 2.3 Основные технические характеристики 5.12 Настройка IPv4-адресации</p> |

| | | |
|---------------------------------|-------------------|--|
| | | 5.15.5 Семейство протоколов STP (STP, RSTP, MSTP) |
| Версия 1.15 | 09.02.2021 | <p>Добавлены разделы:</p> <p>5.6.3 Команды для резервирования конфигурации</p> <p>5.17.4 Функция ограничения multicast-трафика</p> <p>5.17.5 RADIUS-авторизация запросов IGMP</p> <p>5.30.6 Настройка Route-Map</p> <p>5.30.7 Настройка Prefix-List</p> <p>5.30.9 Балансировка нагрузки Equal-Cost Multi-Path (ECMP)</p> <p>Изменения в разделах:</p> <p>2.2.3 Функции второго уровня сетевой модели OSI</p> <p>2.3 Основные технические характеристики</p> <p>2.4.4 Световая индикация</p> <p>4.5.1 Базовая настройка коммутатора</p> <p>4.5.2 Настройка параметров системы безопасности</p> <p>5.4 Команды управления системой</p> <p>5.6.2 Команды для работы с файлами</p> <p>5.9.1 Параметры Ethernet-интерфейсов, Port-Channel и Loopback-интерфейсов</p> <p>5.9.2 Настройка VLAN и режимов коммутации интерфейсов</p> <p>5.10 Storm Control для различного трафика (broadcast, multicast, unknown unicast)</p> <p>5.15.1 Настройка протокола DNS – системы доменных имен</p> <p>5.15.5 Семейство протоколов STP (STP, RSTP, MSTP)</p> <p>5.17.1 Функция посредника протокола IGMP (IGMP Snooping)</p> <p>5.19.1 Механизм AAA</p> <p>5.20 Журнал аварий, протокол SYSLOG</p> <p>5.24.1 Функции обеспечения защиты портов</p> <p>5.29.2 Статистика QoS</p> <p>5.30.3 Настройка протокола OSPF, OSPFv3</p> |
| Версия 1.14 | 24.11.2020 | <p>Изменения в разделах:</p> <p>2.3 Основные технические характеристики</p> <p>5.6.2 Команды для работы с файлами</p> <p>5.26 Конфигурация DHCP-сервера</p> |
| Версия 1.13 | 12.06.2020 | <p>Добавлены разделы:</p> <p>5.30.8 Настройка связки ключей</p> <p>Изменения в разделах:</p> <p>2.2 Функции коммутатора</p> <p>2.3 Основные технические характеристики</p> <p>5.1 Базовые команды</p> <p>5.9 Конфигурация интерфейсов и VLAN</p> <p>5.17 Групповая адресация</p> <p>5.19 Функции управления</p> |
| Версия 1.12 | 20.11.2019 | <p>Изменения в разделах:</p> <p>2.3 Основные технические характеристики</p> |
| Версия 1.11 | 15.10.2019 | <p>Изменения в разделах:</p> <p>5.11 Группы агрегации каналов – Link Aggregation Group (LAG)</p> <p>5.19.4 Протокол управления сетью (SNMP)</p> |
| Версия 1.10 | 20.05.2019 | <p>Добавлено описание моделей коммутаторов MES5316A, MES5324A, MES5332A</p> |
| Версия программного обеспечения | 6.6.4 | |

| | | |
|-------|---|----|
| 1 | ВВЕДЕНИЕ | 9 |
| 2 | ОПИСАНИЕ ИЗДЕЛИЯ..... | 10 |
| 2.1 | Назначение | 10 |
| 2.2 | Функции коммутатора | 11 |
| 2.2.1 | Базовые функции | 11 |
| 2.2.2 | Функции при работе с MAC-адресами | 11 |
| 2.2.3 | Функции второго уровня сетевой модели OSI | 12 |
| 2.2.4 | Функции третьего уровня сетевой модели OSI | 14 |
| 2.2.5 | Функции QoS..... | 14 |
| 2.2.6 | Функции обеспечения безопасности | 15 |
| 2.2.7 | Функции управления коммутатором | 16 |
| 2.2.8 | Дополнительные функции | 17 |
| 2.3 | Основные технические характеристики | 17 |
| 2.4 | Конструктивное исполнение | 34 |
| 2.4.1 | Внешний вид и описание передней панели устройства | 34 |
| 2.4.2 | Задняя панель устройства | 42 |
| 2.4.3 | Боковые панели устройства | 46 |
| 2.4.4 | Световая индикация | 49 |
| 2.5 | Комплект поставки | 54 |
| 3 | УСТАНОВКА И ПОДКЛЮЧЕНИЕ | 55 |
| 3.1 | Крепление кронштейнов..... | 55 |
| 3.2 | Установка устройства в стойку..... | 57 |
| 3.2.1 | Установка устройств MES2300-xx, MES3300-xx, MES5312, MES53xxA, MES5400-xx | 57 |
| 3.2.1 | Установка устройств MES5410-48, MES5500-32 | 57 |
| 3.2.2 | Размещение коммутаторов в стойке | 58 |
| 3.2.3 | Установка устройства MES3500I-10P на DIN-рейку | 59 |
| 3.3 | Установка модулей питания | 60 |
| 3.4 | Подключение питающей сети | 60 |
| 3.5 | Установка и удаление SFP-трансиверов | 61 |
| 4 | НАЧАЛЬНАЯ НАСТРОЙКА КОММУТАТОРА..... | 63 |
| 4.1 | Настройка терминала | 63 |
| 4.2 | Включение устройства..... | 63 |
| 4.3 | Загрузочное меню | 64 |
| 4.4 | Режим работы коммутатора | 65 |
| 4.5 | Настройка функций коммутатора | 69 |
| 4.5.1 | Базовая настройка коммутатора | 69 |
| 4.5.2 | Настройка параметров системы безопасности | 73 |
| 4.5.3 | Настройка баннера | 74 |
| 5 | УПРАВЛЕНИЕ УСТРОЙСТВОМ. ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ..... | 75 |
| 5.1 | Базовые команды | 75 |
| 5.2 | Фильтрация сообщений командной строки..... | 77 |
| 5.3 | Настройка макрокоманд..... | 78 |
| 5.4 | Команды управления системой | 79 |
| 5.5 | Команды для настройки параметров для задания паролей | 86 |
| 5.6 | Работа с файлами..... | 87 |
| 5.6.1 | Описание аргументов команд | 87 |
| 5.6.2 | Команды для работы с файлами | 88 |
| 5.6.3 | Команды для резервирования конфигурации | 89 |
| 5.6.4 | Команды для автоматического обновления и конфигурации | 90 |
| 5.7 | Настройка системного времени | 92 |
| 5.8 | Конфигурация временных интервалов time-range..... | 96 |
| 5.9 | Конфигурация интерфейсов и VLAN..... | 97 |

| | | |
|---------|--|-----|
| 5.9.1 | Параметры Ethernet-интерфейсов, Port-Channel и Loopback-интерфейсов | 97 |
| 5.9.2 | Настройка VLAN и режимов коммутации интерфейсов | 107 |
| 5.9.3 | Настройка Private VLAN | 113 |
| 5.9.4 | Настройка интерфейса IP | 117 |
| 5.9.5 | Selective Q-in-Q | 117 |
| 5.10 | Storm Control для различного трафика (broadcast, multicast, unknown unicast) | 119 |
| 5.11 | Группы агрегации каналов – Link Aggregation Group (LAG) | 120 |
| 5.11.1 | Статические группы агрегации каналов..... | 122 |
| 5.11.2 | Протокол агрегации каналов LACP | 122 |
| 5.11.3 | Настройка технологии Multi-Switch Link Aggregation Group (MLAG) | 123 |
| 5.12 | Настройка IPv4-адресации | 126 |
| 5.13 | Настройка Green Ethernet | 128 |
| 5.14 | Настройка IPv6-адресации | 129 |
| 5.14.1 | Протокол IPv6 | 129 |
| 5.15 | Настройка протоколов | 132 |
| 5.15.1 | Настройка протокола DNS – системы доменных имен | 132 |
| 5.15.2 | Настройка протокола ARP | 134 |
| 5.15.3 | Настройка протокола GVRP | 136 |
| 5.15.4 | Механизм обнаружения петель (loopback-detection) | 138 |
| 5.15.5 | Семейство протоколов STP (STP, RSTP, MSTP), PVSTP+, RPVSTP+ | 139 |
| 5.15.6 | Настройка протокола G.8032v2 (ERPS) | 147 |
| 5.15.7 | Настройка протокола LLDP | 149 |
| 5.15.8 | Настройка протокола OAM | 155 |
| 5.15.9 | Настройка функции Flex-link | 158 |
| 5.15.10 | Настройка функции Layer 2 Protocol Tunneling (L2PT)..... | 159 |
| 5.16 | Voice VLAN | 162 |
| 5.17 | Групповая адресация..... | 164 |
| 5.17.1 | Функция посредника протокола IGMP (IGMP Snooping) | 164 |
| 5.17.2 | Правила групповой адресации (multicast addressing) | 168 |
| 5.17.3 | MLD Snooping – протокол контроля многоадресного трафика в IPv6..... | 175 |
| 5.17.4 | Функция ограничения multicast-трафика..... | 177 |
| 5.17.5 | RADIUS-авторизация запросов IGMP | 178 |
| 5.18 | Маршрутизация многоадресного трафика..... | 180 |
| 5.18.1 | Протокол PIM | 180 |
| 5.18.2 | Функция PIM Snooping | 183 |
| 5.18.3 | Протокол MSDP | 184 |
| 5.18.4 | Функция IGMP Proxy | 186 |
| 5.19 | Функции управления | 188 |
| 5.19.1 | Механизм AAA..... | 188 |
| 5.19.2 | Протокол RADIUS..... | 193 |
| 5.19.3 | Протокол TACACS+ | 195 |
| 5.19.4 | Протокол управления сетью (SNMP) | 197 |
| 5.19.5 | Протокол удалённого мониторинга сети (RMON) | 201 |
| 5.19.6 | Списки доступа ACL для управления устройством..... | 207 |
| 5.19.7 | Настройка доступа | 209 |
| 5.20 | Журнал аварий, протокол SYSLOG..... | 213 |
| 5.21 | Зеркалирование (мониторинг) портов | 216 |
| 5.22 | Функция sFlow | 217 |
| 5.23 | Функции диагностики физического уровня..... | 219 |
| 5.23.1 | Диагностика медного кабеля..... | 220 |
| 5.23.2 | Диагностика оптического трансивера..... | 220 |
| 5.24 | IP Service Level Agreements (IP SLA)..... | 222 |
| 5.24 | Функции обеспечения безопасности | 225 |
| 5.24.1 | Функции обеспечения защиты портов..... | 225 |

| | | |
|---------|---|-----|
| 5.24.2 | Проверка подлинности клиента на основе порта (стандарт 802.1x)..... | 227 |
| 5.24.3 | Настройка функции MAC Address Notification | 234 |
| 5.24.4 | Контроль протокола DHCP и опция 82 | 236 |
| 5.24.5 | Защита IP-адреса клиента (IP source Guard) | 242 |
| 5.24.6 | Контроль протокола ARP (ARP Inspection) | 244 |
| 5.24.7 | Функционал First Hop Security..... | 247 |
| 5.25 | Функции DHCP Relay агента..... | 253 |
| 5.26 | Конфигурация DHCP-сервера..... | 255 |
| 5.27 | Конфигурация ACL (списки контроля доступа)..... | 258 |
| 5.27.1 | Конфигурация ACL на базе IPv4 | 260 |
| 5.27.2 | Конфигурация ACL на базе IPv6 | 264 |
| 5.27.3 | Конфигурация ACL на базе MAC | 267 |
| 5.28 | Конфигурация защиты от DoS-атак | 269 |
| 5.29 | Качество обслуживания – QoS..... | 271 |
| 5.29.1 | Настройка QoS..... | 271 |
| 5.29.2 | Статистика QoS | 282 |
| 5.30 | Конфигурация протоколов маршрутизации..... | 283 |
| 5.30.1 | Конфигурация статической маршрутизации | 283 |
| 5.30.2 | Настройка протокола RIP..... | 285 |
| 5.30.3 | Настройка протокола OSPF, OSPFv3 | 288 |
| 5.30.4 | Настройка протокола BGP (Border Gateway Protocol)..... | 295 |
| 5.30.5 | Настройка протокола IS-IS..... | 306 |
| 5.30.6 | Настройка Route-Map | 312 |
| 5.30.7 | Настройка Prefix-List..... | 314 |
| 5.30.8 | Настройка связки ключей..... | 315 |
| 5.30.9 | Балансировка нагрузки Equal-Cost Multi-Path (ECMP) | 317 |
| 5.30.10 | Настройка Virtual Router Redundancy Protocol (VRRP) | 318 |
| 5.30.11 | Настройка протокола Bidirectional Forwarding Detection (BFD) | 320 |
| 5.30.12 | Конфигурация виртуальной области маршрутизации (VRF lite)..... | 321 |
| 5.31 | Конфигурация VXLAN..... | 322 |
| 6 | СЕРВИСНОЕ МЕНЮ, СМЕНА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ | 328 |
| 6.1 | Меню Startup..... | 328 |
| 6.2 | Обновление программного обеспечения с сервера TFTP | 329 |
| 6.2.1 | Обновление системного программного обеспечения | 329 |
| | ПРИЛОЖЕНИЕ А. ПРИМЕРЫ ПРИМЕНЕНИЯ И КОНФИГУРАЦИИ УСТРОЙСТВА | 331 |
| | ПРИЛОЖЕНИЕ Б. КОНСОЛЬНЫЙ КАБЕЛЬ..... | 333 |
| | ПРИЛОЖЕНИЕ В. ПОДДЕРЖИВАЕМЫЕ ЗНАЧЕНИЯ ETHERTYPE | 334 |
| | ПРИЛОЖЕНИЕ Г. ОПИСАНИЕ ПРОЦЕССОВ КОММУТАТОРА | 335 |

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». |
| « / » | Данный знак в описании команды указывает на значение по умолчанию. |
| <i>Курсив Calibri</i> | Курсивом Calibri указываются переменные или параметры, которые необходимо заменить соответствующим словом или строкой. |
| Полужирный | Полужирным шрифтом выделены примечания и предупреждения. |
| <Полужирный курсив> | Полужирным курсивом в угловых скобках указываются названия клавиш на клавиатуре. |
| Courier New | Полужирным Шрифтом Courier New записаны примеры ввода команд. |
| <code>Courier New</code> | Шрифтом Courier New в рамке с тенью указаны результаты выполнения команд. |

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.

1 ВВЕДЕНИЕ

В последние годы наблюдается тенденция к осуществлению масштабных проектов по построению сетей связи в соответствии с концепцией NGN. 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.

Передача информации на больших скоростях, особенно в сетях крупного масштаба, подразумевает выбор такой топологии сети, которая позволяет гибко осуществлять распределение высокоскоростных потоков.

Коммутаторы серий MES2300, MES3300, MES53xxA, MES5400-xx, MES5410-48, MES5500-32 могут использоваться на сетях крупных предприятий и предприятий малого и среднего бизнеса (SMB), в операторских сетях. Они обеспечивают высокую производительность, гибкость, безопасность, многоуровневое качество обслуживания (QoS). Коммутаторы MES2300-24, MES2300-24P, MES2300B-24F, MES3300-24, MES3300-08F, MES3300-16F, MES3300-24F, MES5312, MES5316A, MES5324A, MES5332A, MES5400-24, MES5400-48, MES5410-48, MES5500-32 обладают повышенной надежностью за счет резервирования узлов, определяющих бесперебойность функционирования – модулей питания и модулей вентиляции.

Коммутаторы MES5400-24, MES5400-48, MES5410-48, MES5500-32 отвечают требованиям центров обработки данных к Top-of-Rack и End-of-Row-коммутаторам и требованиям операторов к оборудованию сетей агрегации и магистральных сетей, обеспечивая высокую производительность и экономически эффективное решение.

В настоящем руководстве изложены назначение, технические характеристики, рекомендации по начальной настройке, синтаксис команд для конфигурации, мониторинга и обновления программного обеспечения коммутаторов.

2 ОПИСАНИЕ ИЗДЕЛИЯ

2.1 Назначение

Коммутаторы MES5400-24, MES5400-48, MES5410-48, MES5500-32 — это высокопроизводительные устройства, предназначенные для использования в центрах обработки данных (ЦОД) в качестве Top-of-Rack или End-of-Row коммутаторов, а также в сетях агрегации и магистральных сетях операторов связи.

Коммутаторы MES5400-24, MES5400-48 оснащены интерфейсами 1000BASE-X/10GBASE-R и 40GBASE-R/100GBASE-R. В режиме расщепления HG-интерфейса поддерживается работа на скоростях 1 Гбит/с, 10 Гбит/с и 25 Гбит/с. Режим расщепления позволяет расщепить до 6 HG-интерфейсов, что в сумме дает 24 TWE-интерфейса¹.

Коммутатор MES5410-48 оснащен интерфейсами 10GBASE-R/25GBASE-R и 40GBASE-R/100GBASE-R. В режиме расщепления HG-интерфейса поддерживается работа на скоростях 1 Гбит/с, 10 Гбит/с и 25 Гбит/с. Режим расщепления позволяет расщепить до 6 HG-интерфейсов, что в сумме дает 24 TWE-интерфейса.

Коммутатор MES5500-32 оснащен интерфейсами 10GBASE-R и 40GBASE-R/100GBASE-R. В режиме расщепления HG-интерфейса поддерживается работа на скоростях 1 Гбит/с, 10 Гбит/с и 25 Гбит/с. Режим расщепления позволяет расщепить до 30 HG-интерфейсов, что в сумме дает 120 TWE-интерфейсов.

Порты коммутаторов поддерживают работу на скоростях 1 Гбит/с (SFP), 10 Гбит/с (SFP+), 25 Гбит/с (SFP28), 40 Гбит/с (QSFP+) и 100 Гбит/с (QSFP28). Неблокируемая коммутационная матрица позволяет осуществлять корректную обработку пакетов при максимальной нагрузке, сохраняя при этом минимальные и предсказуемые задержки для всех типов трафика.

Схема вентиляции front-to-back обеспечивает эффективное охлаждение при использовании устройств в условиях современных ЦОД.

Надежность коммутаторов обеспечена за счет резервирования источников питания и системы охлаждения и развитой системы мониторинга аппаратной части устройств. Коммутаторы имеют возможность горячей замены модулей питания и вентиляционных модулей, обеспечивая бесперебойное функционирование сети оператора.

Коммутаторы агрегации серий MES2300, MES3300, MES53xxA — это высокопроизводительные устройства, оснащенные интерфейсами 10GBASE-R, 1000BASE-X и предназначенные для использования в операторских сетях в качестве устройств агрегации и в небольших центрах обработки данных (ЦОД).

Порты устройства поддерживают работу на скоростях 1 Гбит/с (SFP), 10 Гбит/с (SFP+), что обеспечивает гибкость в использовании и возможность постепенного перехода на более высокие скорости передачи данных. Неблокируемая коммутационная матрица позволяет осуществлять корректную обработку пакетов при максимальных нагрузках, сохраняя при этом минимальные и предсказуемые задержки на всех типах трафика.

¹ Для модели MES5400-24 в режиме расщепления доступны интерфейсы HG3–HG6. Для модели MES5400-24 rev.В данного ограничения нет.

Схема вентиляции front-to-back обеспечивает эффективное охлаждение при использовании устройств в условиях современных ЦОД.

Дублированные вентиляторы и источники питания постоянного или переменного тока в сочетании с развитой системой мониторинга аппаратной части устройства позволяют получить высокие показатели надежности. Устройства имеют возможность горячей замены модулей питания и вентиляционных модулей, обеспечивая бесперебойность функционирования сети оператора.

Промышленные коммутаторы MES3500I-10P предназначены для организации защищенных отказоустойчивых сетей передачи данных на объектах, где необходимо выполнение требований по устойчивости к воздействиям различного вида температурным и механическим воздействиям, вибрации и др.

2.2 Функции коммутатора

2.2.1 Базовые функции

В таблице 1 приведен список базовых функций устройств, доступных для администрирования.

Таблица 1 – Базовые функции устройства

| | |
|---|---|
| Защита от блокировки очереди (HOL) | Блокировка возникает в случаях перегрузки выходных портов устройства трафиком от нескольких входных портов. Это приводит к задержкам передачи данных и потере пакетов. |
| Поддержка сверхдлинных кадров (Jumbo frames) | Способность поддерживать передачу сверхдлинных кадров, что позволяет передавать данные меньшим числом пакетов. Это снижает объем служебной информации, время обработки и перерывы. |
| Управление потоком (IEEE 802.3X) | Управление потоком позволяет соединять низкоскоростное устройство с высокоскоростным. Для предотвращения переполнения буфера низкоскоростное устройство имеет возможность отправлять пакет PAUSE, тем самым информируя высокоскоростное устройство о необходимости сделать паузу при передаче пакетов. |
| Работа в стеке устройств | Коммутатор поддерживает объединение нескольких устройств в стек. В этом случае коммутаторы рассматриваются как единое устройство с общими настройками. Возможны две топологии построения стека – кольцо и цепочка. При этом параметры портов всех устройств, включенных в стек можно задать с коммутатора, работающего в режиме «мастер». Стекирование устройств позволяет снизить трудоемкость управления сетью. |

2.2.2 Функции при работе с MAC-адресами

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

Таблица 2 – Функции работы с MAC-адресами

| | |
|----------------------------|---|
| Таблица MAC-адресов | Коммутатор составляет в памяти таблицу, в которой устанавливается соответствие между MAC-адресами и узлами портов коммутатора. |
| Режим обучения | В отсутствие обучения данные, поступающие на какой-либо порт, передаются на все остальные порты коммутатора. В режиме обучения коммутатор анализирует кадры и, определив MAC-адрес отправителя, заносит его в таблицу коммутации. Впоследствии кадр Ethernet, предназначенный для хоста, MAC-адрес которого уже есть в таблице, передается только через указанный в таблице порт. |

| | |
|--|--|
| Поддержка передачи на несколько MAC-адресов (MAC Multicast Support) | Данная функция позволяет устанавливать соединения «один ко многим» и «многие ко многим». Таким образом, кадр, адресованный многоадресной группе, передается на каждый порт, входящий в группу. |
| Автоматическое время хранения MAC-адресов (Automatic Aging for MAC Addresses) | Если от устройства с определенным MAC-адресом за определенный период времени не поступают пакеты, то запись для данного адреса устаревает и удаляется. Это позволяет поддерживать таблицу коммутации в актуальном состоянии. |
| Статические записи MAC (Static MAC Entries) | Сетевой коммутатор позволяет пользователю определить статические записи соответствий MAC-адресов, которые сохраняются в таблице коммутации. |

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)

| | |
|---|---|
| Функция IGMP Snooping | Реализация протокола IGMP позволяет на основе информации, полученной при анализе содержимого IGMP-пакетов, определить, какие устройства в сети участвуют в группах многоадресной рассылки, и адресовать трафик на соответствующие порты. |
| Функция MLD Snooping | Реализация протокола MLD позволяет устройству минимизировать многоадресный IPv6-трафик. |
| Защита от «шторма» (Broadcast, multicast, unknown unicast Storm Control) | «Шторм» – это размножение broadcast-, multicast-, unknown unicast-пакетов в каждом узле, которое приводит к лавинообразному росту их числа и парализует работу сети. Коммутаторы имеют функцию, позволяющую ограничить скорость передачи многоадресных и широковещательных кадров, принятых и переданных коммутатором. |
| Зеркалирование портов (Port Mirroring) | Зеркалирование портов позволяет дублировать трафик наблюдаемых портов, пересылая входящие и/или исходящие пакеты на контролирующий порт. У пользователя коммутатора есть возможность задать контролирующий и контролируемые порты и выбрать тип трафика (входящий и/или исходящий), который будет передан на контролирующий порт. |
| Изоляция портов (Protected ports) | Данная функция позволяет назначить порту его uplink-порт, на который безусловно будет перенаправляться весь трафик, обеспечивая тем самым изоляцию с другими портами (в пределах одного коммутатора), находящихся в этом же широковещательном домене (VLAN) в пределах одного коммутатора. |
| Private VLAN Edge | Данная функция позволяет изолировать группу портов (в пределах одного коммутатора), находящихся в одном широковещательном домене между собой, позволяя при этом обмен трафиком с другими портами, находящимися в этом же широковещательном домене, но не принадлежащими к этой группе. |
| Private VLAN (light version) | Обеспечивает изоляцию между устройствами, находящимися в одном широковещательном домене, в пределах всей L2-сети. Реализованы только два режима работы порта Promiscuous и Isolated (Isolated-порты не могут обмениваться друг с другом). |
| Поддержка протокола STP (Spanning Tree Protocol) | Spanning Tree Protocol — сетевой протокол, основной задачей которого является приведение сети Ethernet с избыточными соединениями к древовидной топологии, исключающей петли. Коммутаторы обмениваются конфигурационными сообщениями, используя кадры специального формата, и выборочно включают и отключают передачу на порты. |

| | |
|--|---|
| <p>Поддержка протокола RSTP (IEEE 802.1w Rapid spanning tree protocol)</p> | <p>Rapid (быстрый) STP (RSTP) – является усовершенствованием протокола STP, характеризуется меньшим временем приведения сети к древовидной топологии и имеет более высокую устойчивость.</p> |
| <p>Протокол ERPS (Ethernet Ring Protection Switching)</p> | <p>Протокол предназначен для повышения устойчивости и надежности сети передачи данных, имеющей кольцевую топологию, за счет снижения времени восстановления сети в случае аварии. Время восстановления не превышает 1 секунды, что существенно меньше времени перестройки сети при использовании протоколов семейства spanning tree.</p> |
| <p>Поддержка VLAN</p> | <p>VLAN – это группа портов коммутатора, образующих одну широковещательную область (домен). Коммутатор поддерживает различные средства классификации пакетов для определения их принадлежности к определенной VLAN.</p> |
| <p>Поддержка протокола OAM (Operation, Administration, and Maintenance, IEEE 802.3ah)</p> | <p>Ethernet OAM (Operation, Administration, and Maintenance), IEEE 802.3ah – функции уровня канала передачи данных представляют собой протокол мониторинга состояния канала. В этом протоколе для передачи информации о состоянии канала между непосредственно подключенными устройствами Ethernet используются блоки данных протокола OAM (OAMPDU). Оба устройства должны поддерживать стандарт IEEE 802.3ah.</p> |
| <p>Поддержка GVRP (GARP VLAN)</p> | <p>Протокол регистрации GARP VLAN обеспечивает динамическое добавление/удаление групп VLAN на портах коммутатора. Если включен протокол GVRP, коммутатор определяет, а затем распространяет данные о принадлежности к VLAN на все порты, являющиеся частью активной топологии.</p> |
| <p>Поддержка VLAN на базе портов (Port-Based VLAN)</p> | <p>Распределение по группам VLAN выполняется по входящим портам. Данное решение позволяет использовать на каждом порту только одну группу VLAN.</p> |
| <p>Поддержка 802.1Q</p> | <p>IEEE 802.1Q – открытый стандарт, который описывает процедуру тегирования трафика для передачи информации о принадлежности к VLAN. Позволяет использовать несколько групп VLAN на одном порту.</p> |
| <p>Объединение каналов с использованием LACP</p> | <p>Протокол LACP обеспечивает автоматическое объединение отдельных связей между двумя устройствами (коммутатор–коммутатор или коммутатор–сервер) в единый канал передачи данных. В протоколе постоянно определяется возможность объединения каналов, и в случае отказа соединения, входящего в объединенный канал, его трафик автоматически перераспределяется по не отказавшим компонентам объединенного канала.</p> |
| <p>Создание групп LAG</p> | <p>В устройствах поддерживается функция создания групп каналов. Агрегация каналов (Link aggregation, trunking) или IEEE 802.3ad – технология объединения нескольких физических каналов в один логический. Это способствует не только увеличению пропускной способности магистральных каналов коммутатор-коммутатор или коммутатор-сервер, но и повышению их надежности. Возможны три типа балансировки – на основании MAC-адресов, на основании IP-адресов и на основании порта (socket) назначения. Группа LAG состоит из портов с одинаковой скоростью, работающих в дуплексном режиме.</p> |
| <p>Поддержка Auto Voice VLAN</p> | <p>Предоставляет возможность идентифицировать голосовой трафик на основании OUI (Organizationally Unique Identifier – первые 24 бита MAC-адреса). Если в MAC-таблице коммутатора присутствует MAC-адрес с OUI голосового шлюза или же IP-телефона, то данный порт автоматически добавляется в voice vlan (идентификация по протоколу SIP или же по MAC-адресу получателя не поддерживается).</p> |

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)

| | |
|---|--|
| Клиенты BootP и DHCP (Dynamic Host Configuration Protocol) | Устройства способны автоматически получать IP-адрес по протоколу BootP/DHCP. |
| Статические IP-маршруты | Администратор коммутатора имеет возможность добавлять и удалять статические записи в таблицу маршрутизации. |
| Протокол ARP (Address Resolution Protocol) | ARP – протокол сопоставления IP-адреса и физического адреса устройства. Соответствие устанавливается на основе анализа ответа от узла сети, адрес узла запрашивается в широковещательном пакете. |
| Протокол RIP (Routing Information Protocol) | Протокол динамической маршрутизации, который позволяет маршрутизаторам обновлять маршрутную информацию, получая ее от соседних маршрутизаторов. В задачи протокола входит определение оптимального маршрута на основании данных о количестве промежуточных узлов. |
| Функция IGMP Проху | IGMP Проху – функция упрощенной маршрутизации многоадресных данных между сетями. Для управления маршрутизацией используется протокол IGMP. |
| Протокол OSPF | Протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути алгоритм Дейкстры. Протокол OSPF распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы. |
| Протокол BGP | BGP (Border Gateway Protocol — протокол граничного шлюза) является протоколом маршрутизации между автономными системами (AS). Маршрутизаторы обмениваются информацией о маршрутах к сетям назначения. |
| Протокол VRRP | Протокол VRRP предназначен для резервирования маршрутизаторов, выполняющих роль шлюза по умолчанию. Это достигается путём объединения IP-интерфейсов группы маршрутизаторов в один виртуальный, который будет использоваться как шлюз по умолчанию для компьютеров в сети. |
| Протокол PIM | PIM-протокол многоадресной маршрутизации для IP-сетей, созданный для решения проблем групповой маршрутизации. PIM базируется на традиционных маршрутных протоколах (например, Border Gateway Protocol), вместо того, чтобы создавать собственную сетевую топологию. PIM использует unicast-таблицу маршрутизации для проверки RPF. Эта проверка выполняется маршрутизаторами, чтобы убедиться, что передача многоадресного трафика выполняется по пути без петель. |
| Протокол MSDP | Протокол для обмена информацией об источниках мультикаста между различными RP в PIM. |

2.2.5 Функции QoS

В таблице 5 приведены основные функции качества обслуживания (Quality of Service).

Таблица 5 – Основные функции качества обслуживания

| | |
|--|---|
| Поддержка приоритетных очередей | Устройство поддерживает приоритизацию исходящего трафика по очередям на каждом порту. Распределение пакетов по очередям может производиться в результате классификации пакетов по различным полям в заголовках пакетов. |
|--|---|

| | |
|--|--|
| <p>Поддержка класса обслуживания 802.1p</p> | <p>Стандарт 802.1p специфицирует метод указания приоритета кадра и алгоритм использования приоритета в целях своевременной доставки чувствительного к временным задержкам трафика. Стандарт 802.1p определяет восемь уровней приоритетов. Коммутаторы могут использовать значение приоритета 802.1p для распределения кадров по приоритетным очередям.</p> |
|--|--|

2.2.6 Функции обеспечения безопасности

Таблица 6 – Функции обеспечения безопасности

| | |
|---|---|
| <p>DHCP snooping</p> | <p>Функция коммутатора, предназначенная для защиты от атак с использованием протокола DHCP. Обеспечивает фильтрацию DHCP-сообщений, поступивших с ненадежных портов путем построения и поддержания базы данных привязки DHCP (DHCP snooping binding database). DHCP snooping выполняет действия брандмауэра между ненадежными портами и серверами DHCP.</p> |
| <p>Опция 82 протокола DHCP</p> | <p>Опция, которая позволяет проинформировать DHCP-сервер о том, с какого DHCP-ретранслятора и через какой порт пришел запрос. По умолчанию коммутатор, использующий функцию DHCP snooping, обнаруживает и отбрасывает любой DHCP-запрос, содержащий опцию 82, который он получил через ненадежный (untrusted) порт.</p> |
| <p>UDP relay</p> | <p>Перенаправление широковещательного UDP-трафика на указанный IP-адрес.</p> |
| <p>Функции DHCP-сервера</p> | <p>DHCP-сервер осуществляет централизованное управление сетевыми адресами и соответствующими конфигурационными параметрами, автоматически предоставляя их клиентам.</p> |
| <p>IP Source address guard</p> | <p>Функция коммутатора, которая ограничивает IP-трафик, фильтруя его на основании таблицы соответствий базы данных привязки DHCP – DHCP snooping и статически сконфигурированных IP-адресов. Функция используется для борьбы с подменой IP-адресов.</p> |
| <p>Dynamic ARP Inspection (Protection)</p> | <p>Функция коммутатора, предназначенная для защиты от атак с использованием протокола ARP. Сообщение, которое поступает с ненадежного порта, подвергается проверке – соответствует ли IP-адрес в теле принятого ARP-сообщения IP-адресу отправителя. Если адреса не совпадают, то коммутатор отбрасывает пакет.</p> |
| <p>L2 – L3 – L4 ACL (Access Control List)</p> | <p>На основе информации, содержащейся в заголовках уровней 2, 3 и 4, у администратора есть возможность настроить правила, согласно которым пакет будет обработан либо отброшен.</p> |
| <p>Time-Based ACL</p> | <p>Позволяет сконфигурировать временные рамки, в течение которых данный ACL будет действовать.</p> |
| <p>Поддержка заблокированных портов</p> | <p>Основная функция блокировки – повысить безопасность сети, предоставляя доступ к порту коммутатора только для устройств, имеющих MAC-адреса, закрепленные за этим портом.</p> |
| <p>Проверка подлинности на основе порта (802.1x)</p> | <p>Проверка подлинности IEEE 802.1x представляет собой механизм контроля доступа к ресурсам через внешний сервер. Прошедшие проверку подлинности пользователи получают доступ к ресурсам выбранной сети.</p> |

2.2.7 Функции управления коммутатором

Таблица 7 – Основные функции управления коммутаторами

| | |
|---|--|
| Загрузка и выгрузка файла настройки | Параметры устройств сохраняются в файле настройки, который содержит данные конфигурации как всей системы в целом, так и определенного порта устройства. |
| Протокол TFTP (Trivial File Transfer Protocol) | Протокол TFTP используется для операций записи и чтения файлов. Протокол основан на транспортном протоколе UDP. Устройства поддерживают загрузку и передачу по данному протоколу файлов настройки и образов программного обеспечения. |
| Протокол SCP (Secure Copy) | Протокол SCP используется для операций записи и чтения файлов. Протокол основан на сетевом протоколе SSH. Устройства поддерживают загрузку и передачу по данному протоколу файлов настройки и образов программного обеспечения. |
| Удаленный мониторинг (RMON) | Удаленный мониторинг (RMON) – средство мониторинга компьютерных сетей, расширение SNMP. Совместимые устройства позволяют собирать диагностические данные с помощью станции управления сетью. RMON – это стандартная база MIB, в которой определены текущая и предыдущая статистика уровня MAC и объекты управления, предоставляющие данные в реальном времени. |
| Протокол SNMP | Протокол SNMP используется для мониторинга и управления сетевым устройством. Для управления доступом к системе определяется список записей сообщества, каждая из которых содержит привилегии доступа. |
| Интерфейс командной строки (CLI) | Управление коммутаторами 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 | Syslog – протокол, обеспечивающий передачу сообщений о происходящих в системе событиях, а также уведомлений об ошибках удаленным серверам. |
| SNTP (Simple Network Time Protocol) | Протокол <i>SNTP</i> – протокол синхронизации времени сети, гарантирует точность синхронизации времени сетевого устройства с сервером до миллисекунды. |
| Traceroute | Traceroute – служебная функция, предназначенная для определения маршрутов передачи данных в IP-сетях. |
| Управление контролируемым доступом – уровни привилегий | Администратор может определить уровни привилегий доступа для пользователей устройства и характеристики для каждого уровня привилегий (только для чтения – 1 уровень, полный доступ – 15 уровень). |
| Блокировка интерфейса управления | Коммутатор способен устанавливать запрет доступа к каждому интерфейсу управления (SNMP, CLI). Запрет может быть установлен отдельно для каждого типа доступа: Telnet (CLI over Telnet Session); Secure Shell (CLI over SSH); SNMP. |
| Локальная аутентификация | Для локальной аутентификации поддерживается хранение паролей в базе данных коммутатора. |
| Фильтрация IP-адресов для SNMP | Доступ по SNMP разрешается для определенных IP-адресов, являющихся членами SNMP-сообщества. |
| Клиент RADIUS | Протокол RADIUS используется для аутентификации, авторизации и учета. Сервер RADIUS использует базу данных пользователей, которая содержит данные проверки подлинности для каждого пользователя. Коммутаторы содержат клиентскую часть протокола RADIUS. |

| | |
|---|--|
| TACACS+ (Terminal Access Controller Access Control System) | Устройство предоставляет поддержку проверки подлинности клиентов посредством протокола TACACS+. Протокол TACACS+ обеспечивает централизованную систему безопасности для проверки пользователей, получающих доступ к устройству, а также централизованную систему управления при соблюдении совместимости с RADIUS и другими процессами проверки подлинности. |
| Сервер SSH | Функция сервера SSH позволяет клиенту SSH установить с устройством защищенное соединение для управления им. |
| Поддержка макрокоманд | Данная функция предоставляет возможность создавать макрокоманды, представляющие собой набор команд, и применять их для конфигурации устройства. |

2.2.8 Дополнительные функции

В таблице 8 приведены дополнительные функции устройства.

Таблица 8 – Дополнительные функции устройства

| | |
|---|---|
| Диагностика оптического трансивера | Устройство позволяет тестировать оптический трансивер. При тестировании отслеживаются такие параметры, как ток и напряжение питания, температура трансивера. Для реализации требуется поддержка этих функций в трансивере. |
| Green Ethernet | Данный механизм позволяет коммутатору снизить энергопотребление за счет отключения неактивных электрических портов. |
| Соответствие стандарту МЭК 61850 | Коммутатор обладает всеми необходимыми характеристиками для работы с протоколами MMS, GOOSE, SV: <ul style="list-style-type: none"> - Малая величина задержки GOOSE-сообщения при передаче; - Умение распознавать Ethernet GOOSE-сообщения; - Умение работать с тегом виртуальной сети и тегом приоритета IEEE 802.1Q GOOSE-сообщения; - Поддержка передачи multicast-сообщений и возможность работы с определенным стандартом МЭК 61850 диапазоном групп вещания. |

2.3 Основные технические характеристики

Основные технические параметры коммутаторов приведены в таблице 9.

Таблица 9 – Основные технические характеристики

| Общие параметры | | |
|-----------------|--------------|--|
| Интерфейсы | MES2300-24 | 24 × 10/100/1000BASE-T 4 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) |
| | MES2300B-24 | 24 × 10/100/1000BASE-T 4 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) |
| | MES2300B-24F | 20 × 1000BASE-X/100BASE-FX (SFP) 4 × 10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 4 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) |
| | MES2300-24P | 24 × 10/100/1000BASE-T (RJ-45) PoE/PoE+ 4 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) |

| | |
|--------------|---|
| MES2300D-24P | 24 × 10/100/1000BASE-T (RJ-45) PoE/PoE+ 4 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) |
| MES2300DI-28 | 24 × 10/100/1000BASE-T 4 × 10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 1 × Консольный порт RS-232 (RJ-45) 1 × USB 2.0 |
| MES2300-48P | 48 × 10/100/1000BASE-T PoE/PoE+ 4 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) |
| MES2300B-48 | 48 × 10/100/1000BASE-T 4 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) |
| MES3300-08F | 4 × 1000BASE-X/100BASE-FX (SFP) 4 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 4 × 10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 1 × Консольный порт RS-232 (RJ-45) 1 × 10/100/1000BASE-T (OOB) |
| MES3300-16F | 12 × 1000BASE-X/100BASE-FX (SFP) 4 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 4 × 10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 1 × Консольный порт RS-232 (RJ-45) 1 × 10/100/1000BASE-T (OOB) |
| MES3300-24 | 24 × 10/100/1000BASE-T 4 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × 10/100/1000BASE-T (OOB) 1 × Консольный порт RS-232 (RJ-45) |
| MES3300-24F | 20 × 1000BASE-X/100BASE-FX (SFP) 4 × 10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo 4 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × 10/100/1000BASE-T (OOB) 1 × Консольный порт RS-232 (RJ-45) |
| MES3300-48 | 48 × 10/100/1000BASE-T 4 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × 10/100/1000BASE-T (OOB) 1 × Консольный порт RS-232 (RJ-45) |
| MES3300-48F | 48 × 1000BASE-X/100BASE-FX (SFP) 4 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) |
| MES3500I-10P | 8 × 10/100/1000BASE-T PoE/PoE+ (RJ-45) 4 × 100BASE-FX/1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) |
| MES5310-48 | 1 × 10/100/1000BASE-T (OOB) 48 × 1000BASE-X (SFP)/10GBASE-R (SFP+) 6 × 40GBASE-R4 (QSFP+)/100GBASE-R4 (QSFP28) 1 × Консольный порт RS-232 (RJ-45) 1 × USB 2.0 |
| MES5312 | 1 × 10/100/1000BASE-T (OOB) 12 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) |

| | | |
|--------------------------|---|---|
| | MES5316A | 1 × 10/100/1000BASE-T (OOB) 16 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) 1 × USB 2.0 |
| | MES5324A | 1 × 10/100/1000BASE-T (OOB) 24 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) 1 × USB 2.0 |
| | MES5332A | 1 × 10/100/1000BASE-T (OOB) 32 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 1 × Консольный порт RS-232 (RJ-45) 1 × USB 2.0 |
| | MES5310-48 | 1 × 10/100/1000BASE-T (OOB) 48 × 1000BASE-X (SFP)/10GBASE-R (SFP+) 6 × 40GBASE-R4 (QSFP+)/100GBASE-R4 (QSFP28) 1 × Консольный порт RS-232 (RJ-45) 1 × USB 2.0 |
| | MES5400-24 | 1 × 10/100/1000BASE-T (OOB) 24 × 1000BASE-X (SFP)/10GBASE-R (SFP+) 6 × 40GBASE-R4 (QSFP+)/100GBASE-R4 (QSFP28) 1 × Консольный порт RS-232 (RJ-45) 1 × USB 2.0 |
| | MES5400-48 | 1 × 10/100/1000BASE-T (OOB) 48 × 1000BASE-X (SFP)/10GBASE-R (SFP+) 6 × 40GBASE-R4 (QSFP+)/100GBASE-R4 (QSFP28) 1 × Консольный порт RS-232 (RJ-45) 1 × USB 2.0 |
| | MES5410-48 | 1 × 10/100/1000BASE-T (OOB) 48 × 1000BASE-X (SFP)/10GBASE-R (SFP+)/25GBASE-R (SFP28) 6 × 40GBASE-R4 (QSFP+)/100GBASE-R4 (QSFP28) 1 × Консольный порт RS-232 (RJ-45) 1 × USB 2.0 |
| | MES5500-32 | 1 × 10/100/1000BASE-T (OOB) 2 × 10GBASE-R (SFP+) 32 × 40GBASE-R4 (QSFP+)/100GBASE-R4 (QSFP28) 1 × Консольный порт RS-232 (RJ-45) 1 × USB 2.0 |
| Скорость передачи данных | | Оптические интерфейсы 1/10/25/100 Гбит/с Электрические интерфейсы 10/100/1000 Мбит/с |
| Пропускная способность | MES2300DI-28 | 56 Гбит/с |
| | MES3300-08F | 96 Гбит/с |
| | MES3300-16F | 112 Гбит/с |
| | MES2300-24 MES2300B-24 MES2300B-24F MES2300D-24P MES2300-24P MES3300-24 MES3300-24F | 128 Гбит/с |
| | MES2300-48P MES2300B-48 MES3300-48 MES3300-48F | 176 Гбит/с |
| | | |
| | | |

| | | |
|--|---|-------------|
| | MES3500I-10P | 24 Гбит/с |
| | MES5312 | 240 Гбит/с |
| | MES5316A | 320 Гбит/с |
| | MES5324A | 480 Гбит/с |
| | MES5332A | 640 Гбит/с |
| | MES5400-24 | 1,68 Тбит/с |
| | MES5310-48 MES5400-48 | 2,16 Тбит/с |
| | MES5410-48 | 3,6 Тбит/с |
| | MES5500-32 | 6,4 Тбит/с |
| Производительность на пакетах длиной 64 байта ¹ | MES2300DI-28 | 41,6 MPPS |
| | MES2300D-24P | 95,2 MPPS |
| | MES3300-08F | 71,4 MPPS |
| | MES3300-16F | 88,3 MPPS |
| | MES2300-24P | 94,49 MPPS |
| | MES2300-24 MES2300B-24 MES2300B-24F MES3300-24 MES3300-24F | 95,2 MPPS |
| | MES2300-48P MES2300B-48 MES3300-48 MES3300-48F | 130,95 MPPS |
| | MES3500I-10P | 17,8 MPPS |
| | MES5312 | 178 MPPS |
| | MES5316A MES5324A MES5332A | 238 MPPS |
| | MES5400-24 | 878,3 MPPS |
| | MES5310-48 | 1028,5 MPPS |
| | MES5400-48 | 1041,5 MPPS |
| | MES5410-48 | 2467 MPPS |
| | MES5500-32 | 1995 MPPS |
| Объем буферной памяти | MES2300-24 MES2300B-24 MES2300B-24F MES2300-24P MES2300D-24P MES2300DI-28 MES3300-24 MES3300-08F MES3300-16F MES3300-24F MES3500I-10P | 1,5 Мбайт |

¹ Значения указаны для односторонней передачи.

| | | |
|------------------------|--|----------------------|
| | MES5312 | 2 Мбайт |
| | MES2300-48P MES2300B-48 MES3300-48 MES3300-48F MES5316A MES5324A MES5332A | 3 Мбайт |
| | MES5310-48 MES5400-24 MES5400-48 | 12 Мбайт |
| | MES5410-48 MES5500-32 | 24 Мбайт |
| Объем ОЗУ (DDR3) | MES5312 MES5316A MES5324A MES5332A | 1 Гбайт ¹ |
| Объем ОЗУ (DDR4) | MES2300-24 MES2300B-24 MES2300B-24F MES2300-24P MES2300D-24P MES2300DI-28 MES2300-48P MES2300B-48 MES3300-24 MES3300-08F MES3300-16F MES3300-24F MES3300-48 MES3300-48F MES3500I-10P | 2 Гбайт |
| | MES5310-48 MES5400-24 MES5400-48 MES5410-48 MES5500-32 | 8 Гбайт |
| Объем ПЗУ (NAND Flash) | MES2300-24 MES2300-24P MES2300B-24F MES2300-48P MES2300B-48 MES3300-24 MES3300-24F MES3300-48 MES3300-48F MES3500I-10P | 512 Мбайт |
| | MES5312 MES5316A MES5324A MES5332A | 1 Гбайт |

¹ Объем ОЗУ для моделей MES5316A rev.C, MES5324A rev.C, MES5332A rev.C, MES5316A rev.C1, MES5324A rev.C1 — 2 Гбайт.

| | | |
|---------------------------|--|--|
| Объем ПЗУ (embedded uSSD) | MES5310-48 MES5400-24 MES5400-48 MES5410-48 MES5500-32 | 8 Гбайт |
| Таблица MAC-адресов | MES2300-24 MES2300B-24 MES2300B-24F MES2300-24P MES2300D-24P MES2300-48P MES2300B-48 MES2300DI-28 MES3300-24 MES3300-08F MES3300-16F MES3300-24F MES3300-48 MES3300-48F MES3500I-10P | 16384 |
| | MES5312 MES5316A MES5324A MES5332A | 32768 |
| | MES5310-48 MES5400-24 | 65536 |
| | MES5400-48 | 262144 |
| | MES5410-48 MES5500-32 | 131072 ¹ /262144 ² |
| Количество ARP-записей | MES2300-24 ³ MES2300B-24 ³ MES2300B-24F ³ MES2300-24P ³ MES2300D-24P ³ MES2300DI-28 ³ MES2300-48 ³ MES2300B-48 ³ | 2039 |
| | MES3300-24 ³ MES3300-08F ³ MES3300-16F ³ MES3300-24F ³ MES3300-48 ³ MES3300-48F ³ MES3500I-10P ³ | 4087 |

¹ Максимальное значение для режима распределения системных ресурсов mid-l3-mid-l2.

² Максимальное значение для режима распределения системных ресурсов min-l3-max-l2.

³ Для каждого хоста в ARP-таблице создается запись в таблице маршрутизации.

| | | |
|---|---|--|
| | MES5312 ¹ MES5316A ¹ MES5324A ¹ MES5332A ¹ | 8183 |
| | MES5310-48 ¹ | 32695 |
| | MES5400-24 ¹ | 32759 |
| | MES5400-48 ¹ | 131063 |
| | MES5410-48 ¹ MES5500-32 ¹ | 65527 ² /98304 ³ |
| Поддержка VLAN | | Согласно 802.1Q до 4094 активных VLAN |
| Количество групп L2 Multicast (IGMP snooping) | MES2300-24 MES2300B-24 MES2300D-24P MES2300DI-28 MES2300-48P MES2300B-48 | 2048 |
| | MES3300-24 MES3300-08F MES3300-16F MES3300-24F MES3300-48 MES3300-48F MES3500I-10P MES5312 MES5316A MES5324A MES5332A MES5310-48 MES5400-24 MES5400-48 | 4092 |
| | MES5410-48 | 4088 |
| | MES5500-32 | 4090 |
| | | |
| Количество правил SQinQ | MES2300-24 MES2300B-24 MES2300D-24P MES2300DI-28 MES2300-48P MES2300B-48 | 988 (ingress), 988 (egress) |

¹ Для каждого хоста в ARP-таблице создается дополнительная запись в таблице коммутации. Количество ARP-записей с установленной лицензией EVPN для MES5312, MES5316A, MES5324A, MES5332A – 6135, для MES5400-24 – 30711, для MES5400-48 – 129015, для MES5310-48 – 30647, для MES5410-48, MES5500-32: 63479 для режима mid-l3-mid-l2, 96247 для режима min-l3-max-l2.

² Максимальное значение для режима распределения системных ресурсов mid-l3-mid-l2.

³ Максимальное значение для режима распределения системных ресурсов min-l3-max-l2.

| | | |
|------------------------------|---|--|
| | MES3300-24 MES3300-08F MES3300-16F MES3300-24F MES3300-48 MES3300-48F MES3500I-10P MES5310-48 MES5312 MES5316A MES5324A MES5332A MES5400-24 MES5400-48 | 1320 (ingress), 1320 (egress) |
| Количество правил MAC ACL | MES2300-24 MES2300B-24 MES2300B-24F MES2300-24P MES2300D-24P MES2300DI-28 MES2300-48P MES2300B-48 | 1966 |
| | MES3500I-10P | 2999 |
| | MES3300-24 MES3300-08F MES3300-16F MES3300-24F MES3300-48 MES3300-48F | 3000 |
| | MES5312 | 6072 |
| | MES5316A MES5324A MES5332A | 3000 |
| | MES5310-48 MES5400-24 | 6063 |
| | MES5400-48 | 10737 |
| | MES5410-48 MES5500-32 | 4577 |
| | Количество правил IPv4/IPv6 ACL | MES2300-24 MES2300B-24 MES2300B-24F MES2300-24P MES2300D-24P MES2300DI-28 MES2300-48P MES2300B-48 |
| MES3500I-10P | | 2999/1499 |

| | | |
|--|--|------------------------|
| | MES3300-24 MES3300-08F MES3300-16F MES3300-24F MES3300-48 MES3300-48F MES5316A MES5324A MES5332A | 2999/1500 |
| | MES5312 | 6072/3049 |
| | MES5310-48 MES5400-24 | 6063/3035 |
| | MES5400-48 | 10737/5367 |
| | MES5410-48 MES5500-32 | 4577/2288 |
| Количество ACL | MES2300-24 MES2300B-24 MES2300B-24F MES2300-24P MES2300D-24P MES2300DI-28 MES2300-48P MES2300B-48 | 2048 |
| | MES3300-24 MES3300-24F MES3300-48 MES3300-48F MES3500I-10P MES5316A MES5324A MES5332A | 3072 |
| | MES5312 MES5310-48 MES5400-24 MES5410-48 MES5500-32 | 6144 |
| | MES5400-48 | 12288 |
| | Количество правил ACL в одном ACL | 256 |
| Количество маршрутов L3 Unicast ¹ | MES2300-24 MES2300B-24 MES2300B-24F MES2300-24P MES2300D-24P MES2300DI-28 MES2300-48P MES2300B-48 | 4066 IPv4 1015 IPv6 |

¹ Маршруты IPv4/IPv6 Unicast/Multicast используют общие аппаратные ресурсы.

| | | |
|--|--|--|
| | MES3300-24 MES3300-08F MES3300-16F MES3300-24F MES3300-48 MES3300-48F | 13278 IPv4 3316 IPv6 |
| | MES3500I-10P | 13280 IPv4 3317 IPv6 |
| | MES5312 MES5316A MES5324A MES5332A | 16286 IPv4 4070 IPv6 |
| | MES5400-24 MES5400-48 | 32669 IPv4 8165 IPv6 |
| | MES5310-48 | 32707 IPv4 8165 IPv6 |
| | MES5410-48 MES5500-32 | 292000 ¹ /16000 ² IPv4 73000 ¹ /4000 ² IPv6 |
| Количество маршрутов L3 Multicast (IGMP Proxy, PIM) ³ | MES2300-24 MES2300B-24 MES2300B-24F MES2300-24P MES2300D-24P MES2300DI-28 MES2300-48P MES2300B-48 | 2029 IPv4 505 IPv6 |
| | MES3300-24 MES3300-08F MES3300-16F MES3300-24F MES3300-48 MES3300-48F | 4087 IPv4 1642 IPv6 |
| | MES3500I-10P | 4087 IPv4 1657 IPv6 |
| | MES5312 MES5316A MES5324A MES5332A | 8143 IPv4 2033 IPv6 |
| | MES5310-48 | 16335 IPv4 4079 IPv6 |
| | MES5400-24 MES5400-48 | 16324 IPv4 4079 IPv6 |
| | MES5410-48 MES5500-32 | 146000 ¹ /8000 ² IPv4 36500 ¹ /2000 ² IPv6 |

¹ Максимальное значение для режима распределения системных ресурсов mid-l3-mid-l2.


² Максимальное значение для режима распределения системных ресурсов min-l3-max-l2.

³ Маршруты IPv4/IPv6 Unicast/Multicast используют общие аппаратные ресурсы.


| | | |
|---|--|-----|
| Количество VRRP-маршрутизаторов | MES2300-24 MES2300B-24 MES2300B-24F MES2300-24P MES2300D-24P MES2300DI-28 MES2300B-48 MES3300-24 MES3300-16F MES3300-24F MES3300-48 MES3300-48F MES3500I-10P | 255 |
| | MES5312 MES5316A MES5324A MES5332A MES5310-48 MES5400-24 MES5400-48 MES5410-48 MES5500-32 | 127 |
| Максимальное количество ECMP-маршрутов | MES2300-24 MES2300B-24 MES2300B-24F MES2300-24P MES2300D-24P MES2300DI-28 MES2300-48P MES2300B-48 MES3300-24 MES3300-08F MES3300-16F MES3300-24F MES3300-48 MES3300-48F MES3500I-10P | 8 |
| | MES5312 MES5316A MES5324A MES5332A MES5310-48 MES5400-24 MES5400-48 MES5410-48 MES5500-32 | 64 |

| | | |
|-------------------------------|---|--------------------------------|
| Количество VRF | MES2300-24 MES2300B-24 MES2300B-24F MES2300-24P MES2300D-24P MES2300DI-28 MES2300-48P MES2300B-48 MES3300-08F MES3300-16F MES3300-24F MES3300-48 MES3300-48F MES3500I-10P MES5312 MES5316A MES5324A MES5332A | 16 (включая VRF по умолчанию) |
| | MES5310-48 MES5400-24 MES5400-48 MES5410-48 MES5500-32 | 251 (включая VRF по умолчанию) |
| Количество L3-интерфейсов | MES2300-24 MES2300B-24 MES2300B-24F MES2300-24P MES2300D-24P MES2300DI-28 MES2300-48P MES2300B-48 | 2032 |
| | MES3300-24 MES3300-08F MES3300-16F MES3300-24F MES3300-48 MES3300-48F MES3500I-10P MES5310-48 MES5312 MES5316A MES5324A MES5332A MES5400-24 MES5400-48 MES5410-48 MES5500-32 | 2050 |
| Максимальное количество VXLAN | MES5312 MES5316A MES5324A MES5332A | 2094 |
| | MES5410-48 | 4083 |
| | MES5310-48 MES5400-24 MES5400-48 MES5500-32 | 4093 |

| | | |
|---|--|--|
| Количество виртуальных Loopback-интерфейсов | | 64 |
| Агрегация каналов (LAG) | MES2300-24 MES2300B-24 MES2300B-24F MES2300-24P MES2300D-24P MES2300DI-28 MES2300-48P MES2300B-48 MES3300-24 MES3300-08F MES3300-16F MES3300-24F MES3300-48 MES3300-48F MES3500I-10P | 32 группы, до 8 портов в каждой |
| | MES5312 MES5316A MES5324A MES5332A MES5310-48 MES5400-24 MES5400-48 MES5410-48 MES5500-32 | 128 групп, до 8 портов в каждой |
| Количество экземпляров MSTP | | 64 |
| Количество экземпляров PVST | | 64 |
| Количество DHCP pool | | 16 |
| Качество обслуживания QoS | | 8 выходных очередей для каждого порта |
| Сверхдлинные кадры (jumbo frames) | | Максимальный размер пакетов 10240 байт |
| Стекирование | | До 8 устройств (кроме MES3500I-10P) |
| Соответствие стандартам | | IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z Fiber Gigabit Ethernet IEEE 802.3x Full Duplex, Flow Control IEEE 802.3ad Link Aggregation (LACP) IEEE 802.1p Traffic Class IEEE 802.1q VLAN IEEE 802.1v IEEE 802.3 ac IEEE 802.1d Spanning Tree Protocol (STP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) IEEE 802.1x Authentication МЭК 61850 |
| Управление | | |
| Локальное управление | | Console |
| Удаленное управление | | SNMP, Telnet, SSH, web |

| Физические характеристики и условия окружающей среды | | |
|--|--|--|
| Источники питания | MES2300DI-28 MES2300-48P MES3300-24 MES3300-08F MES3300-16F MES3300-24F MES3300-48 MES3300-48F MES5312 MES5316A MES5324A MES5332A MES5310-48 MES5400-24 MES5410-48 MES5500-32 | <p>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.</p> |
| | MES2300B-24 MES2300B-24F MES2300B-48 | <p>Сеть переменного тока: 100–240 В, 50–60 Гц Сеть постоянного тока: 12 В Характеристики зарядного устройства: - ток заряда: 1±0.1 А — MES2300B-48. - напряжение срабатывания расцепителя нагрузки — 10–10,5 В; - пороговое напряжение индикации низкого заряда — 11 В.</p> <p> Сечение провода для подключения АКБ не менее 1,5 мм. Для MES2300B-48 рекомендуется использовать АКБ емкостью не менее 9 Аh.</p> |
| | MES5400-48 | <p>Сеть переменного тока: 176–264 В, 50–60 Гц Сеть постоянного тока: 36–72 В Варианты питания: - один источник питания постоянного или переменного тока; - два источника питания постоянного или переменного тока с возможностью горячей замены.</p> |
| | MES2300-24 | Сеть переменного тока: 100–240 В, 50–60 Гц |
| | MES2300-24P | Сеть переменного тока: 200–240 В, 50–60 Гц |
| | MES2300D-24P | <p>Сеть переменного тока: 200–240 В, 50–60 Гц Варианты питания: - один источник питания переменного тока; - два источника питания переменного тока с возможностью горячей замены.</p> |
| | MES3500I-10P | <p>сеть постоянного тока: с включенной функцией PoE: 45–57 В; с отключенной функцией PoE: 20–57 В</p> |
| | Потребляемая мощность | MES2300-24 |
| MES2300B-24 | | Не более 50 Вт |
| MES2300-24P | | Не более 445 Вт (с учётом нагрузки PoE) |
| MES2300D-24P | | Не более 850 Вт (с учётом нагрузки PoE) |
| MES2300DI-28 | | Не более 31 Вт |
| MES2300-48P | | Не более 1600 Вт (с учётом нагрузки PoE) |

| | | |
|--|-----------------------------|---|
| | MES2300B-24F MES2300B-48 | Не более 55 Вт |
| | MES3300-24 | Не более 33 Вт |
| | MES3300-08F | Не более 29 Вт |
| | MES3300-16F | Не более 37 Вт |
| | MES3300-24F | Не более 45 Вт |
| | MES3300-48 | Не более 45 Вт |
| | MES3300-48F | Не более 89 Вт |
| | MES3500I-10P | Не более 270 Вт (с учётом нагрузки PoE) |
| | MES5312 | Не более 25 Вт |
| | MES5316A | Не более 58 Вт |
| | MES5324A | Не более 73 Вт |
| | MES5332A | Не более 85 Вт |
| | MES5310-48 | Не более 170 Вт |
| | MES5400-24 | Не более 150 Вт |
| | MES5400-48 | Не более 170 Вт |
| | MES5410-48 | Не более 360 Вт |
| | MES5500-32 | Не более 400 Вт |
| Потребляемая мощность без учета заряда АКБ | MES2300B-24 | 24 Вт |
| | MES2300B-24F MES2300B-48 | 40 Вт |
| Бюджет PoE | MES2300-24P | 380 Вт |
| | MES2300D-24P | 720 Вт |
| | MES2300-48P | 1450 Вт |
| | MES3500I-10P | 240 Вт |
| Тепловыделение | MES2300-24 | 20 Вт |
| | MES2300B-24 | 27 Вт |
| | MES2300-24P | 65 Вт |
| | MES2300D-24P | 130 Вт |
| | MES2300DI-28 | 31 Вт |
| | MES2300-48P | 150 Вт |
| | MES2300B-24F MES2300B-48 | 43 Вт |
| | MES3300-24 | 33 Вт |
| | MES3300-08F | 29 Вт |
| | MES3300-16F | 37 Вт |
| | MES3300-24F MES3300-48 | 45 Вт |
| | MES3300-48F | 89 Вт |
| | MES3500I-10P | 30 Вт |
| | MES5312 | 25 Вт |

| | | | |
|--------------------------------|---|-------------------|--|
| | MES5316A | 58 Вт | |
| | MES5324A | 73 Вт | |
| | MES5332A | 85 Вт | |
| | MES5310-48 | 170 Вт | |
| | MES5400-24 | 150 Вт | |
| | MES5400-48 | 170 Вт | |
| | MES5410-48 | 360 Вт | |
| | MES5500-32 | 400 Вт | |
| Интервал рабочих температур | MES2300-24 MES2300B-24 MES2300D-24P MES2300B-48 MES2300-24P | От -20 до +50 °C | |
| | MES2300B-24F | От -20 до +65 °C | |
| | MES2300DI-28 | От -40 до +60 °C | |
| | MES2300-48P | От -10 до +50 °C | |
| | MES3500I-10P | От -40 до +70 °C | |
| | MES3300-24 MES3300-08F MES3300-16F MES3300-24F MES3300-48 MES3300-48F MES5312 MES5316A MES5324A MES5332A | От -10 до +45 °C | |
| | MES5310-48 MES5400-24 MES5400-48 MES5410-48 MES5500-32 | От 0 до +45 °C | |
| | Интервал температуры хранения | | Интервал температуры хранения от -50 до +70 °C  Перед первым включением после хранения при температуре меньшей, чем -20 °C, или при большей, чем +50 °C, требуется выдержать коммутатор при комнатной температуре не менее четырёх часов. |
| | Относительная влажность при эксплуатации (без образования конденсата) | | Не более 80 % |
| | Относительная влажность при хранении (без образования конденсата) | | От 10 до 95 % |
| Габаритные размеры (Ш × В × Г) | MES2300-24 MES2300B-24 | 430 × 44 × 204 мм | |
| | MES2300B-24F | 430 × 44 × 305 мм | |
| | MES2300-24P | 430 × 44 × 203 мм | |
| | MES2300D-24P | 440 × 44 × 425 мм | |
| | MES2300-48P | 440 × 44 × 490 мм | |

| | | | |
|--------------|---|-------------------|---------|
| | MES2300B-48 | 440 × 44 × 280 мм | |
| | MES3300-24 | 430 × 44 × 330 мм | |
| | MES2300DI-28 MES3300-08F MES3300-16F MES3300-24F | 430 × 44 × 305 мм | |
| | MES3300-48 MES3300-48F | 440 × 44 × 330 мм | |
| | MES3500I-10P | 85 × 175 × 115 мм | |
| | MES5312 | 430 × 44 × 230 мм | |
| | MES5316A MES5324A MES5332A | 430 × 44 × 275 мм | |
| | MES5400-24 | 440 × 44 × 321 мм | |
| | MES5310-48 MES5400-48 | 440 × 44 × 447 мм | |
| | MES5410-48 | 440 × 44 × 536 мм | |
| | MES5500-32 | 440 × 44 × 534 мм | |
| | Macca | MES2300-24 | 2,94 кг |
| | | MES2300B-24 | 2,79 кг |
| MES2300B-24F | | 4,08 кг | |
| MES2300-24P | | 3,2 кг | |
| MES2300D-24P | | 6,85 кг | |
| MES2300DI-28 | | 4,95 кг | |
| MES2300-48P | | 9,98 кг | |
| MES2300B-48 | | 4,1 кг | |
| MES3300-24 | | 5,13 кг | |
| MES3300-08F | | 4,64 кг | |
| MES3300-16F | | 4,89 кг | |
| MES3300-24F | | 5,04 кг | |
| MES3300-48 | | 5,67 кг | |
| MES3300-48F | | 5,68 кг | |
| MES3500I-10P | | 1,76 кг | |
| MES5312 | | 3,8 кг | |
| MES5316A | | 3,6 кг | |
| MES5324A | | 3,7 кг | |
| MES5332A | | 3,8 кг | |
| MES5310-48 | | 8,7 кг | |
| MES5400-24 | | 6,36 кг | |
| MES5400-48 | | 8,7 кг | |
| MES5410-48 | 12,1 кг | | |
| MES5500-32 | 11,8 кг | | |



Тип питания устройства определяется при заказе.

2.4 Конструктивное исполнение

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

Ethernet-коммутаторы MES2300-24, MES2300B-24, MES2300B-24F, MES2300-24P, MES2300D-24P, MES2300DI-28, MES2300-48P, MES2300B-48, MES3300-24, MES3300-08F, MES3300-16F, MES3300-24F, MES3300-48, MES3300-48F, MES3500I-10P, MES5310-48, MES5312, MES5316A, MES5324A, MES5332A, MES5400-24, MES5400-48, MES5410-48, MES5500-32 выполнены в металлическом корпусе с возможностью установки в 19" каркас, высота корпуса 1U.

2.4.1 Внешний вид и описание передней панели устройства

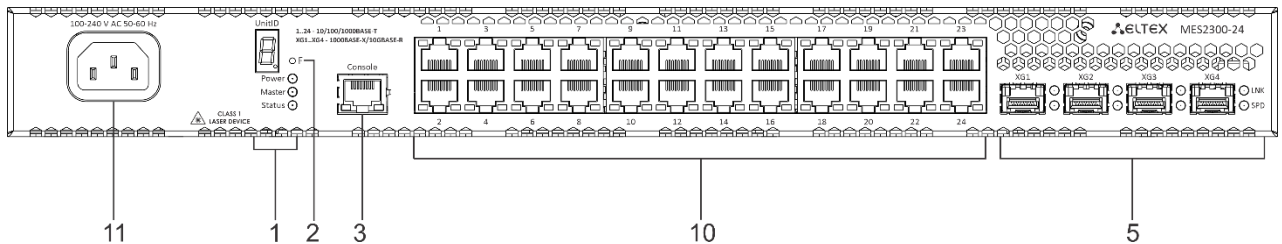


Рисунок 1 – Передняя панель MES2300-24

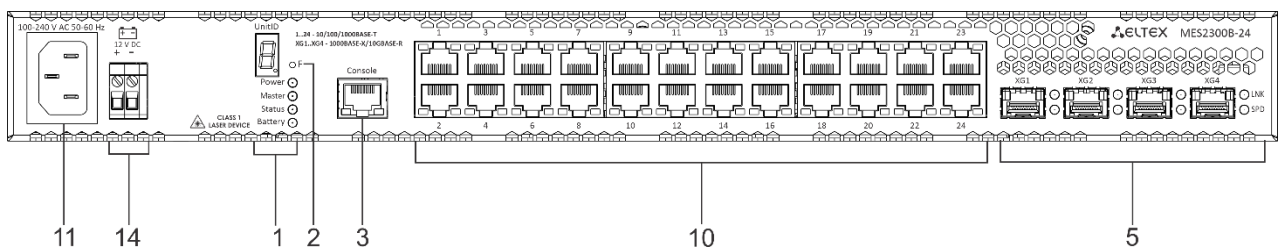


Рисунок 2 – Передняя панель MES2300B-24

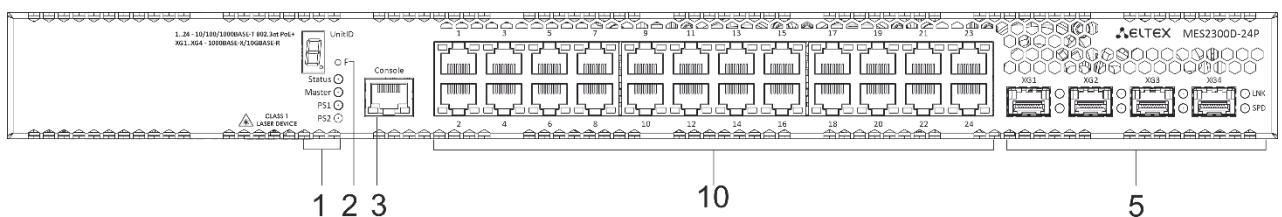


Рисунок 3 – Передняя панель MES2300D-24P

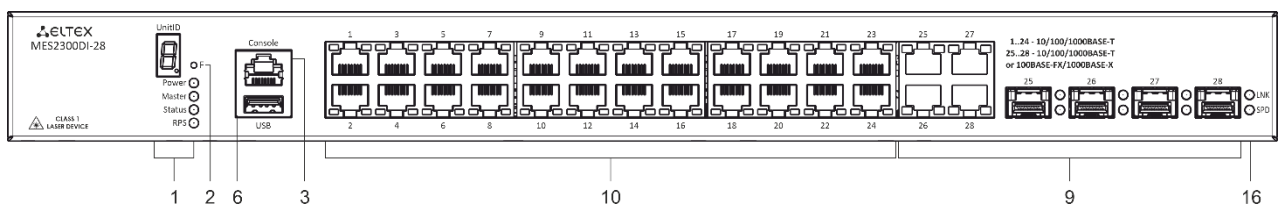


Рисунок 4 – Передняя панель MES2300DI-28

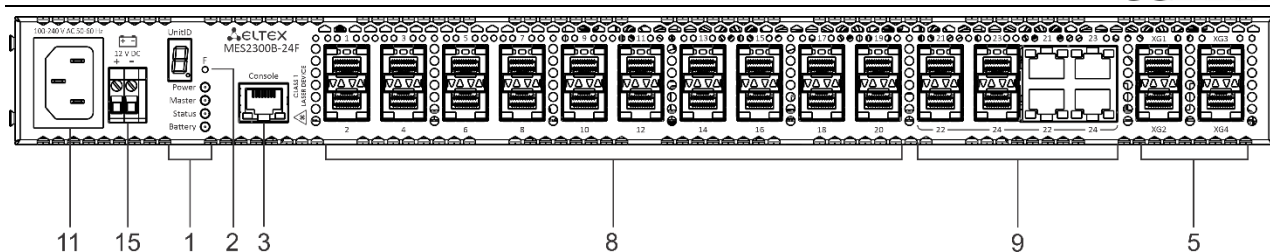


Рисунок 5 – Передняя панель MES2300B-24F

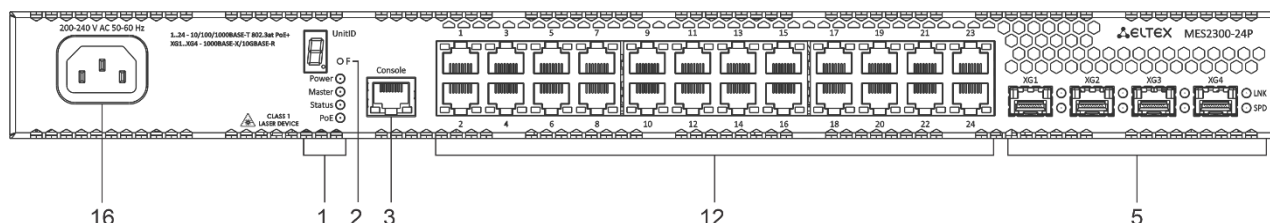


Рисунок 6 – Передняя панель MES2300-24P

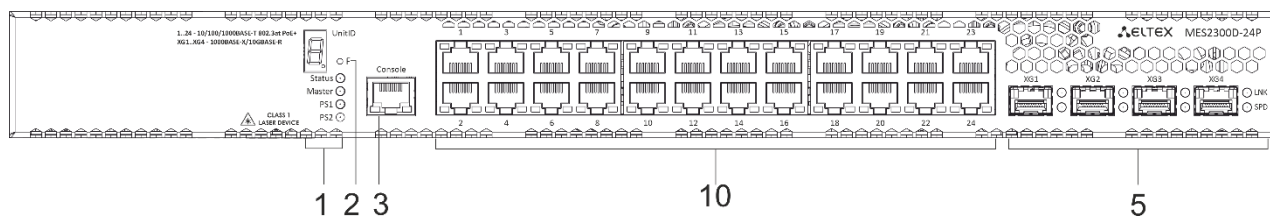


Рисунок 7 – Передняя панель MES2300D-24P

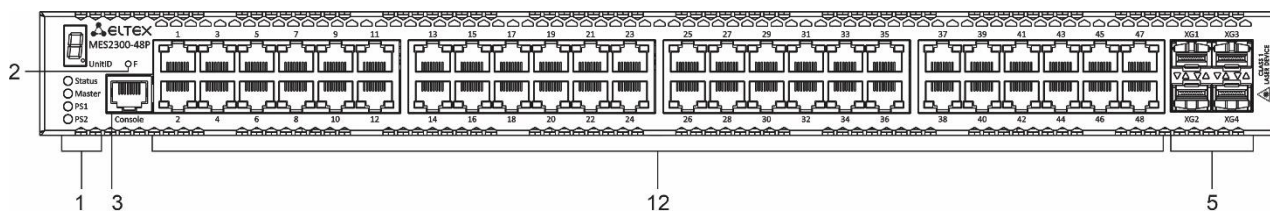


Рисунок 8 – Передняя панель MES2300-48P

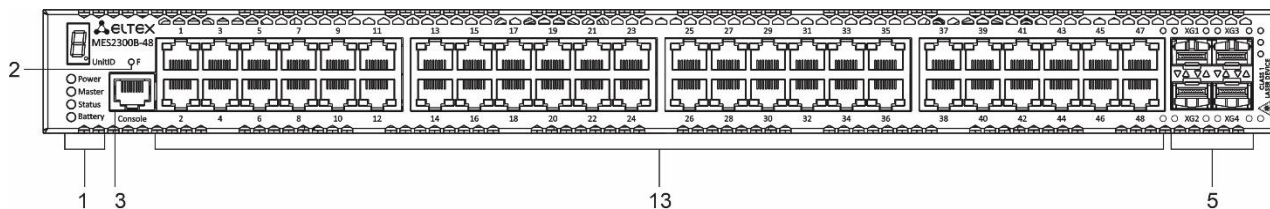


Рисунок 9 – Передняя панель MES2300B-48

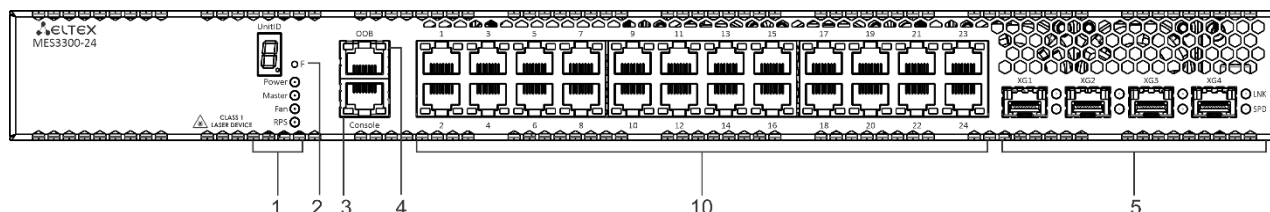


Рисунок 10 – Передняя панель MES3300-24

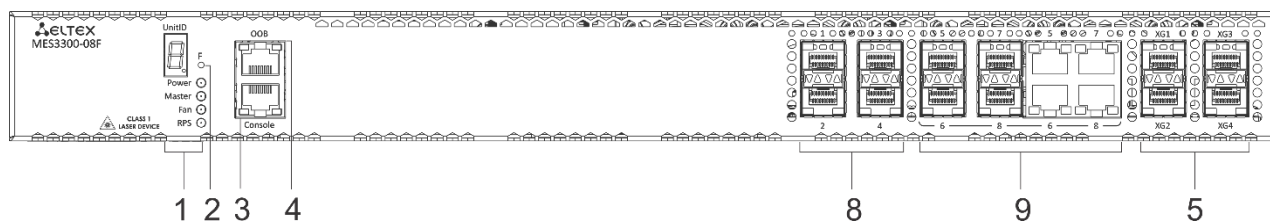


Рисунок 11 – Передняя панель MES3300-08F

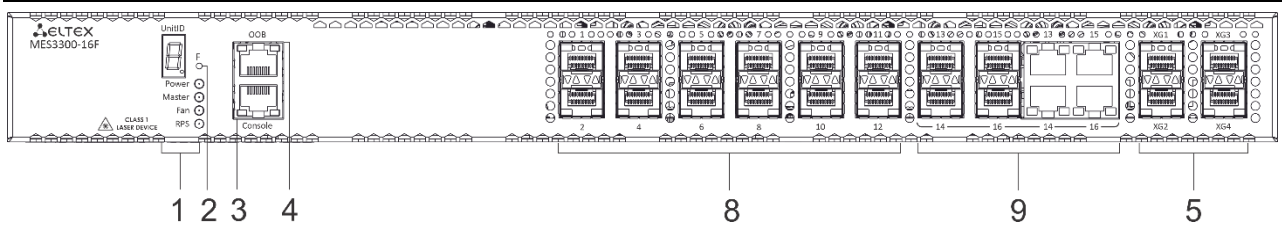


Рисунок 12 – Передняя панель MES3300-16F

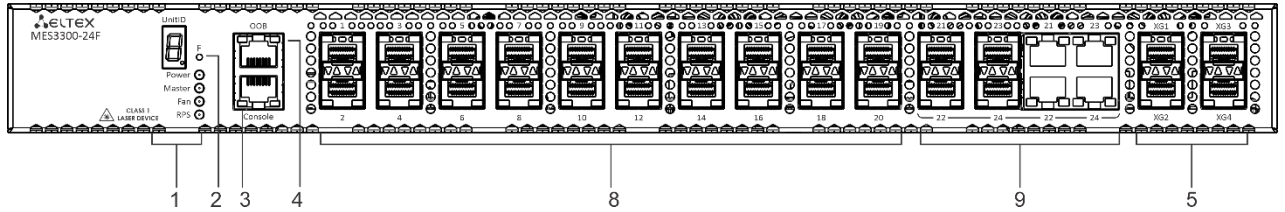


Рисунок 13 – Передняя панель MES3300-24F

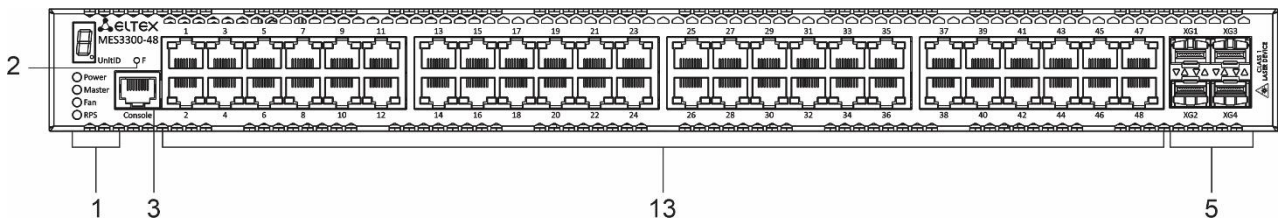


Рисунок 14 – Передняя панель MES3300-48

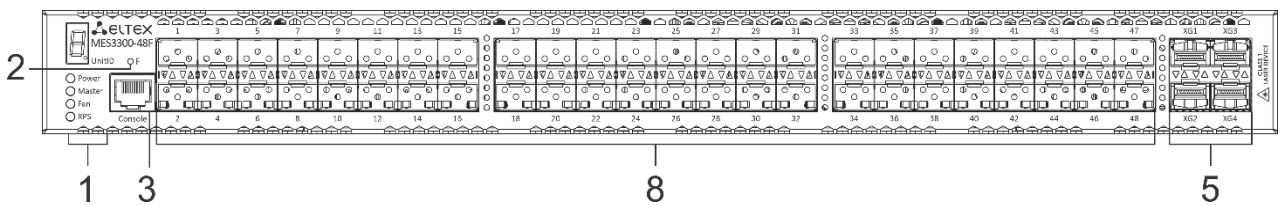


Рисунок 15 – Передняя панель MES3300-48F

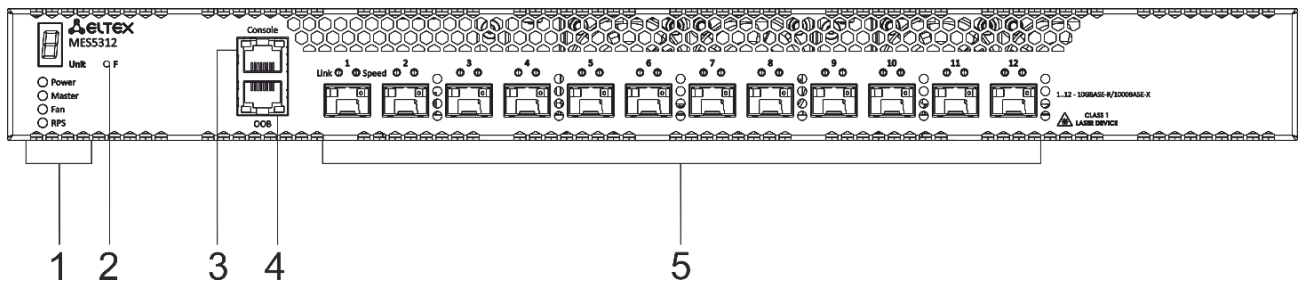


Рисунок 16 – Передняя панель MES5312

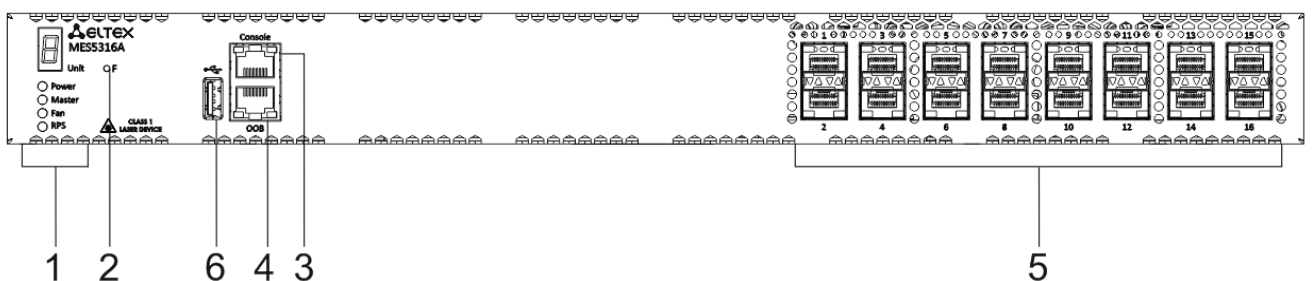


Рисунок 17 – Передняя панель MES5316A

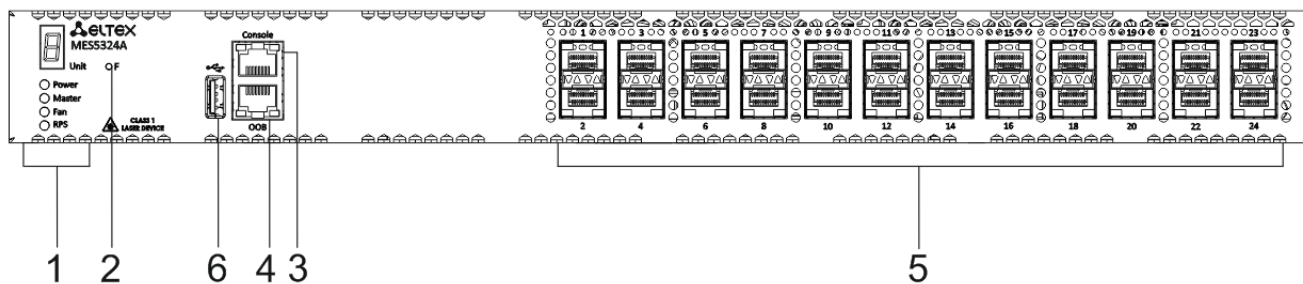


Рисунок 18 – Передняя панель MES5324A

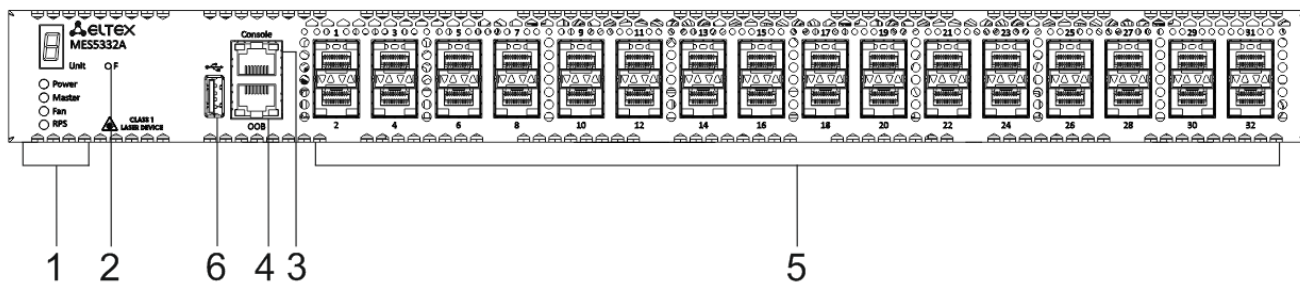


Рисунок 19 – Передняя панель MES5332A

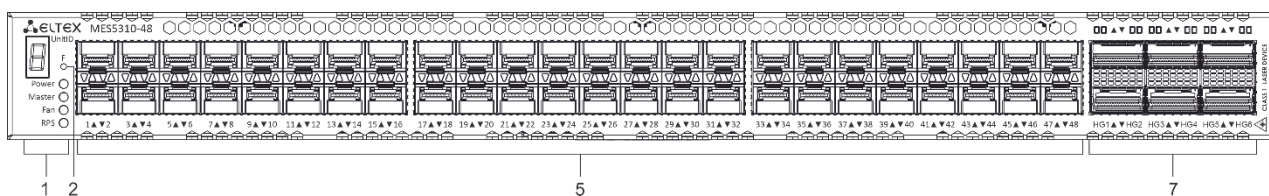


Рисунок 20 – Передняя панель MES5310-48

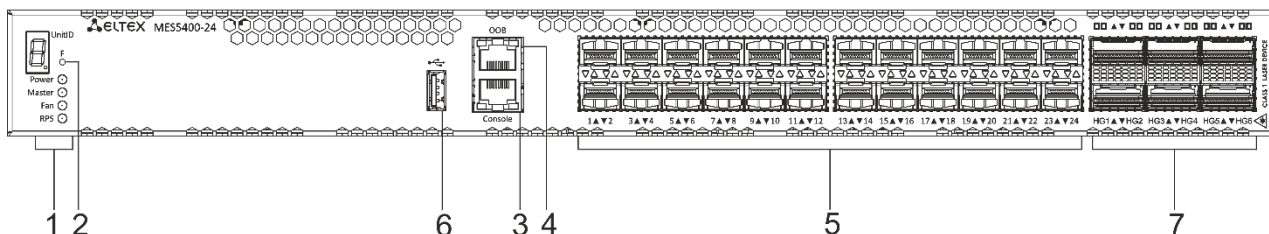


Рисунок 21 – Передняя панель MES5400-24

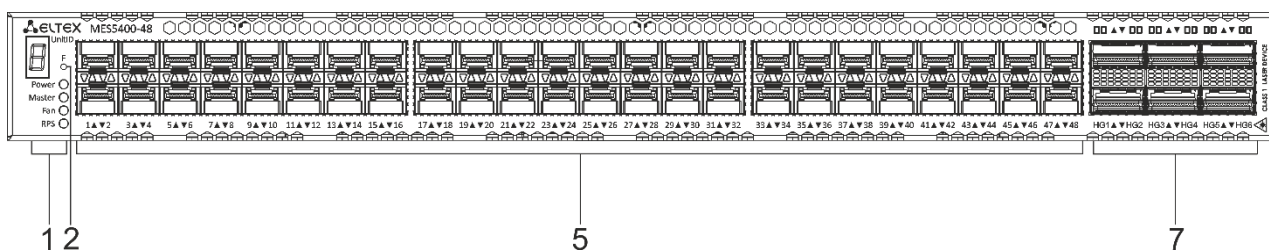


Рисунок 22 – Передняя панель MES5400-48

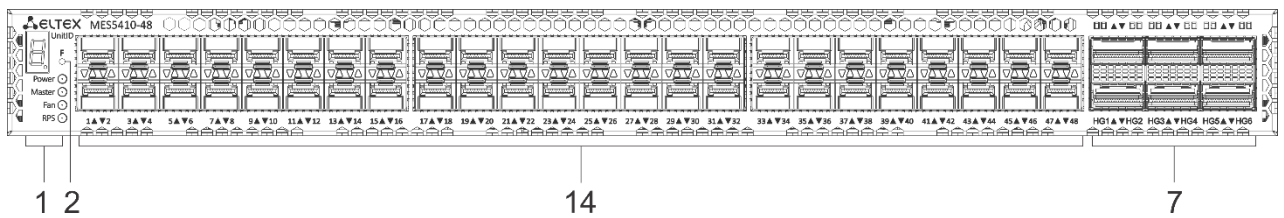


Рисунок 23 – Передняя панель MES5410-48

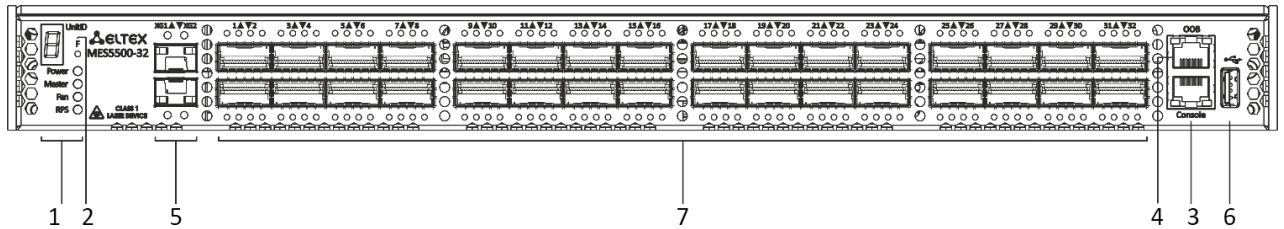



Рисунок 24 – Передняя панель MES5500-32

В таблице 10 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели коммутаторов.

Таблица 10 – Описание разъемов, индикаторов и органов управления передней панели MES2300-24, MES2300B-24, MES2300B-24F, MES2300-24P, MES2300D-24P, MES2300DI-28, MES2300-48P, MES2300B-48, MES3300-24, MES3300-08F, MES3300-16F, MES3300-24F, MES3300-48, MES3300-48F, MES5310-48, MES5312, MES5316A, MES5324A, MES5332A, MES5400-24, MES5400-48, MES5410-48, MES5500-32

| № | Элемент передней панели | Описание |
|---|-------------------------|---|
| 1 | Unit ID | Индикатор номера устройства в стеке. |
| | Power | Индикатор питания устройства. |
| | Master | Индикатор режима работы устройства (ведущий/ведомый). |
| | Fan | Индикатор работы вентиляторов. |
| | RPS | Индикатор резервного электропитания. |
| 2 | F | Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: - при нажатии на кнопку длительностью менее 10 с происходит перезагрузка устройства; - при нажатии на кнопку длительностью более 10 с происходит сброс настроек устройства до заводской конфигурации. |
| 3 | Console | Консольный порт для локального управления устройством. Распиновка разъема следующая: 1 не используется 2 не используется 3 RX 4 GND 5 GND 6 TX 7 не используется 8 не используется Распайка консольного кабеля приведена в разделе «Приложение Б. Консольный кабель». |

| | | | |
|----|---|--|---|
| 4 | OOB | | Порт (out-of-band) 10/100/1000BASE-T (RJ-45) для удаленного управления устройством. Управление осуществляется по сети, отдельно с каналом передачи данных. |
| 5 | [1-12] | MES5312 | Слоты для установки трансиверов 10G SFP+/1G SFP. |
| | [1-16] | MES5316A | |
| | [1-24] | MES5324A | |
| | [1-32] | MES5332A | |
| | [1-24] | MES5400-24 | |
| | [1-48] | MES5310-48 MES5400-48 | |
| | [XG1-XG2] | MES5500-32 | |
| | [XG1-XG4] | MES2300B-24F MES2300-24P MES2300-48P MES2300B-48 MES3300-24 MES3300-08F MES3300-16F MES3300-24F MES3300-48 | |
| 6 |  | MES5316A MES5324A MES5332A MES5310-48 MES5400-24 MES5410-48 MES5500-32 | USB-порт. |
| 7 | [HG1-HG6] [HG1-HG32] | MES5310-48 MES5400-24 MES5400-48 MES5410-48 MES5500-32 | Слоты для установки трансиверов 40G QSFP+/100G QSFP28. |
| 8 | [1-20] | MES2300B-24F MES3300-24F | Слоты для установки трансиверов 1000BASE-X/100BASE-FX (SFP). |
| | [1-4] | MES3300-08F | |
| | [1-12] | MES3300-16F | |
| | [1-48] | MES3300-48F | |
| 9 | [5-8] | MES3300-08F | 4 порта 10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo. |
| | [13-16] | MES3300-16F | |
| | [21-24] | MES2300B-24F MES3300-24F | |
| 10 | [1-24] | MES2300-24 MES2300B-24 MES2300DI-28 MES3300-24 | Порты 10/100/1000BASE-T. |
| | [1-48] | MES2300B-48 MES3300-48 | |

| | | | |
|----|--------------------------|-----------------------------|---|
| 11 | 100-240 V AC 50-60 Hz | MES2300-24 MES2300B-24F | Разъем для подключения к источнику электропитания переменного тока. |
| 12 | [1-24] | MES2300-24P MES2300D-24P | Порты 10/100/1000BASE-T (RJ-45) PoE/PoE+. |
| | [1-48] | MES2300-48P | |
| 13 | [1-48] | MES5410-48 | Слоты для установки трансиверов 1G SFP/10G SFP+/25G SFP28. |
| 14 | 12 V DC | MES2300B-24F | Клеммы для подключения аккумуляторной батареи 12 В. |
| 15 | 200-240 V AC 50-60 Hz | MES2300B-24 MES2300-24P | Разъем для подключения к источнику электропитания переменного тока. |
| 16 | Link/Speed | MES2300DI-28 | Световая индикация состояния оптических интерфейсов. |

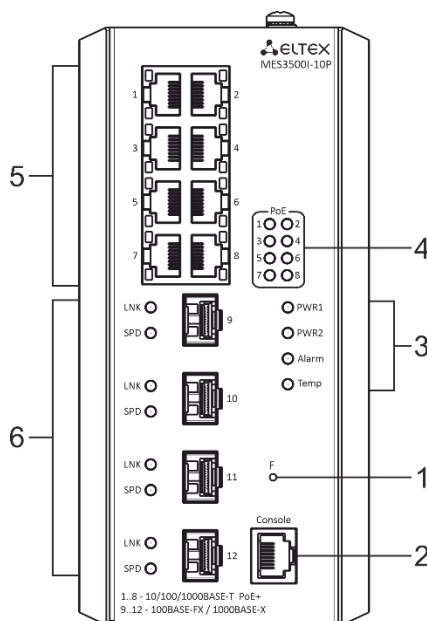


Рисунок 25 – Передняя панель MES3500I-10P

В таблице Таблица 11 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели коммутатора MES3500I-10P.

Таблица 11 – Описание разъемов, индикаторов и органов управления передней панели MES3500I-10P

| № | Элемент передней панели | Описание |
|---|-------------------------|--|
| 1 | F | Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: - при нажатии на кнопку длительностью менее 10 с происходит перезагрузка устройства; - при нажатии на кнопку длительностью более 10 с происходит сброс настроек устройства до заводской конфигурации. |
| 2 | Console | Консольный порт для локального управления устройством. |
| 3 | PWR1, PWR2 | Индикаторы питания устройства. |
| | Alarm | Индикатор аварии. |
| | Temp | Индикатор температуры. |
| 4 | [1-8] | Световая индикация PoE. |

| | | |
|---|--------|---|
| 5 | [1-8] | Порты 10/100/1000BASE-T PoE/PoE+ (RJ-45). |
| 6 | [9-12] | Порты 100BASE-FX/1000BASE-X (SFP). |

Внешний вид верхней панели коммутаторов MES3508, MES3508P и MES3510P приведен на рисунке ниже.

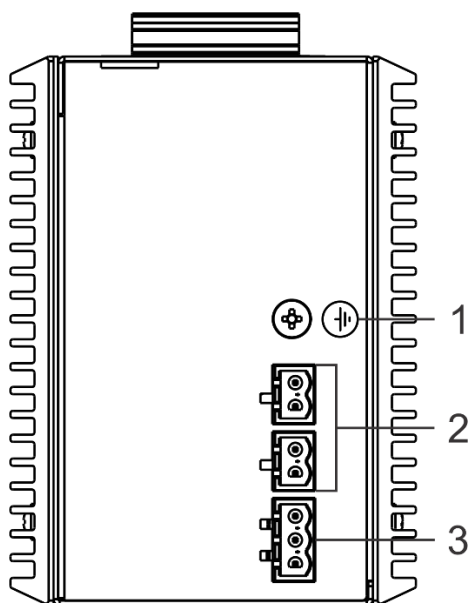



Рисунок 26 – Верхняя панель MES3500I-10P

Таблица 12 – Описание разъемов, индикаторов и органов управления верхней панели MES3500I-10P

| № | Элемент передней панели | Описание |
|---|---|---|
| 1 | Клемма заземления  | Клемма для заземления устройства. |
| 2 | 48 (45 ~ 57) VDC | Разъемы для подключения к источникам электропитания постоянного тока. |
| 3 | 12VDC max 5A | Релейный выход аварийной сигнализации: 1 А, 24 В DC. |

2.4.2 Задняя панель устройства

Внешний вид задней панели коммутаторов MES2300-24, MES2300B-24, MES2300B-24F, MES2300-24P, MES2300D-24P, MES2300DI-28, MES2300-48P, MES2300B-48, MES3300-24, MES3300-08F, MES3300-16F, MES3300-24F, MES3300-48, MES3300-48F, MES5310-48, MES5312, MES5316A, MES5324A, MES5332A, MES5400-24, MES5400-48, MES5410-48, MES5500-32 приведен на рисунках ниже.

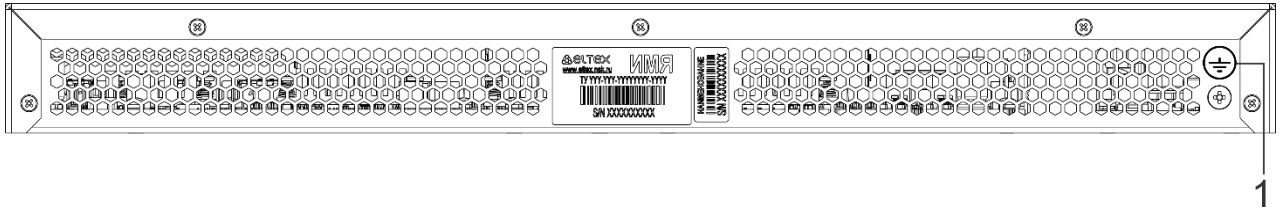


Рисунок 27 – Задняя панель MES2300-24, MES2300B-24

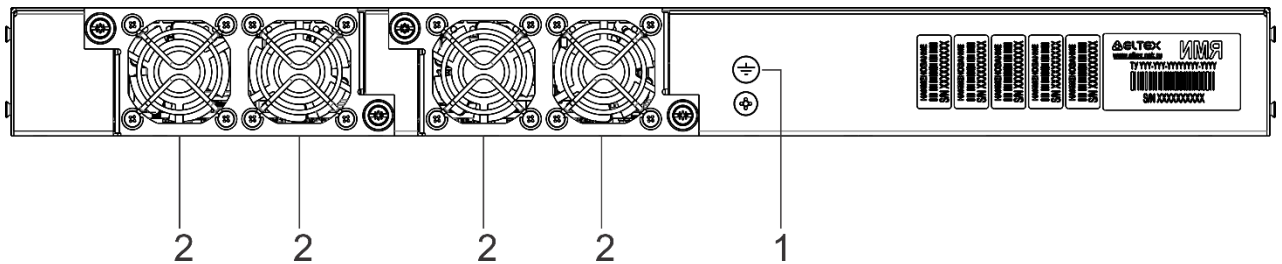


Рисунок 28 – Задняя панель MES2300B-24F

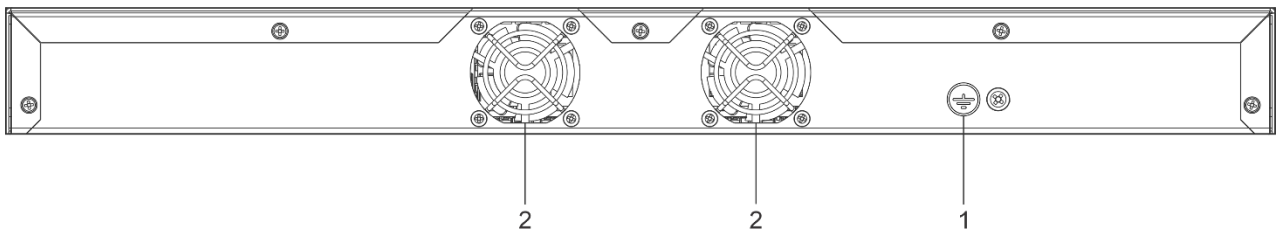


Рисунок 29 – Задняя панель MES2300-24P

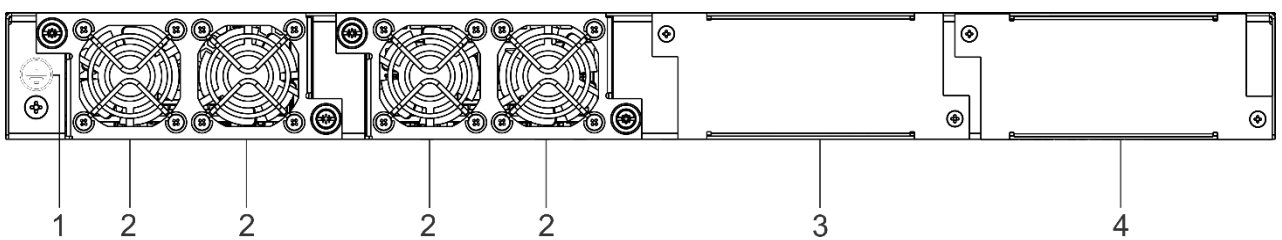


Рисунок 30 – Задняя панель MES2300D-24P

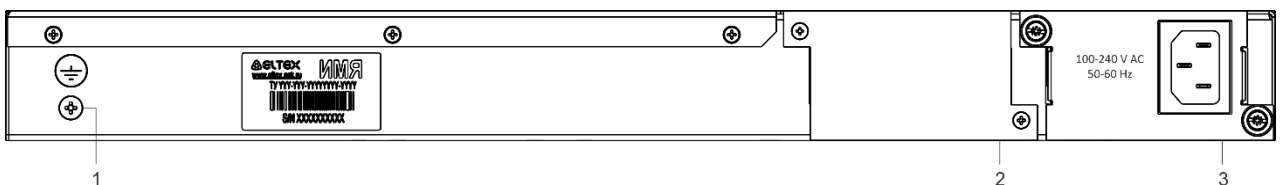


Рисунок 31 – Задняя панель MES2300DI-28

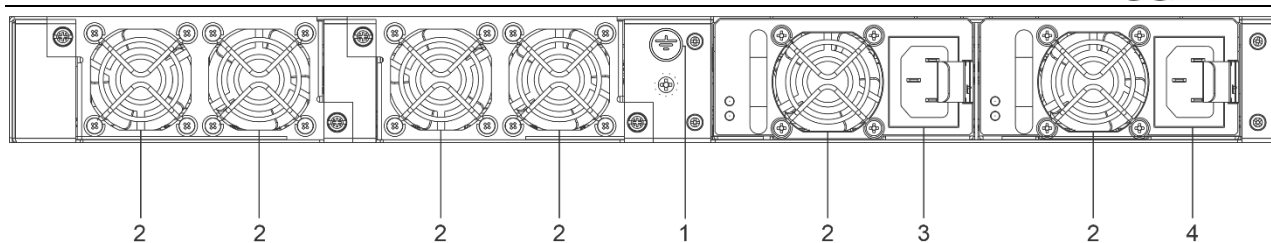


Рисунок 32 – Задняя панель MES2300-48P

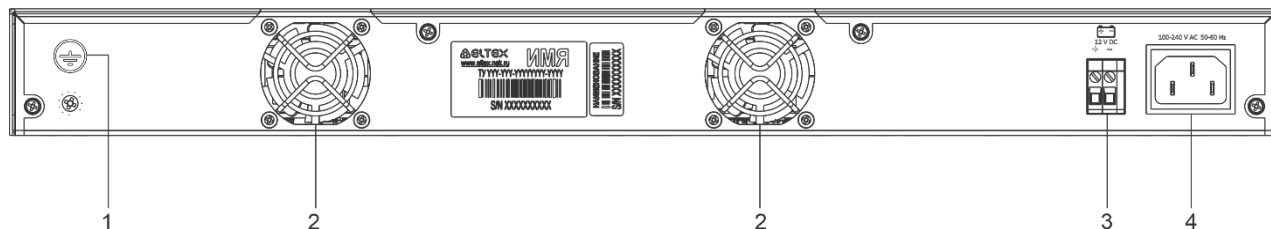


Рисунок 33 – Задняя панель MES2300B-48

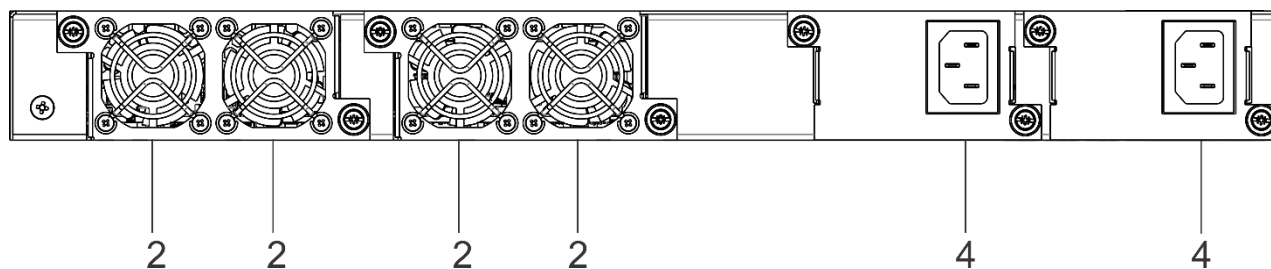


Рисунок 34 – Задняя панель MES3300-24

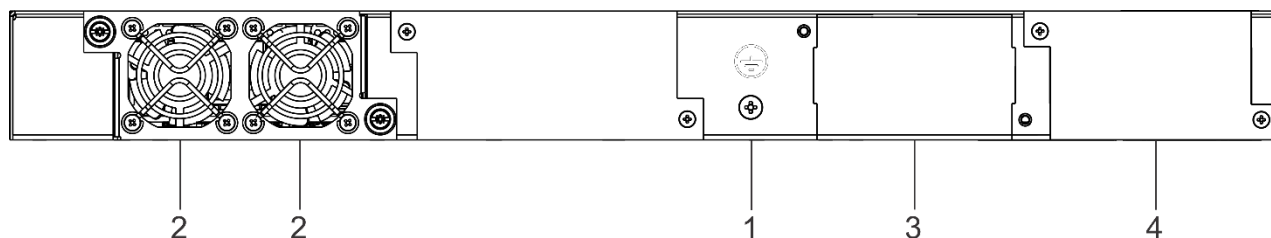


Рисунок 35 – Задняя панель MES3300-08F

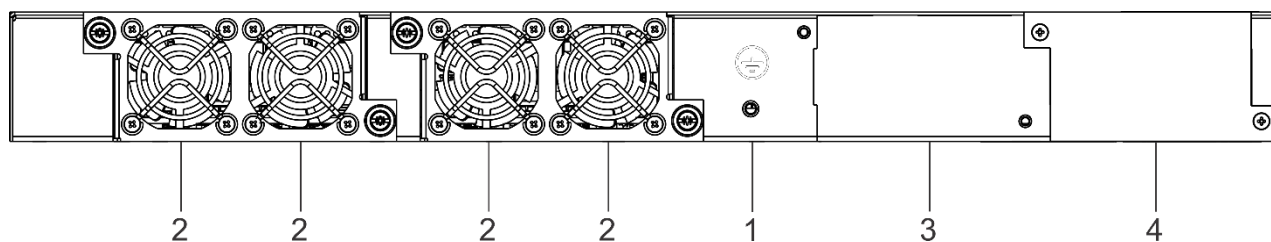


Рисунок 36 – Задняя панель MES3300-16F

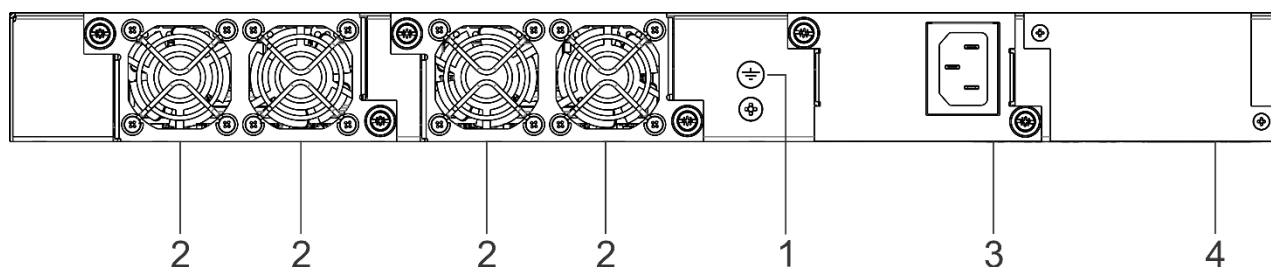


Рисунок 37 – Задняя панель MES3300-24F

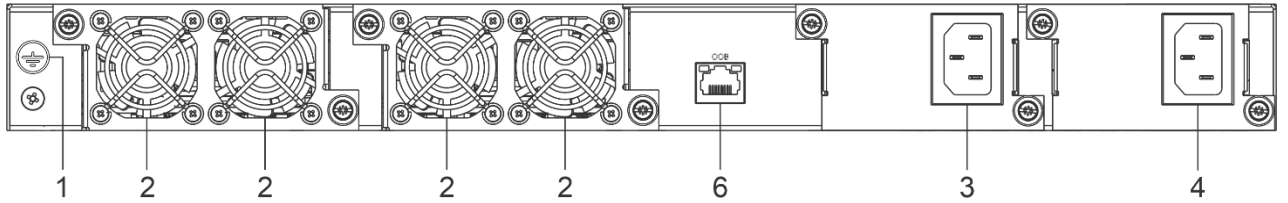


Рисунок 38 – Задняя панель MES3300-48, MES3300-48F

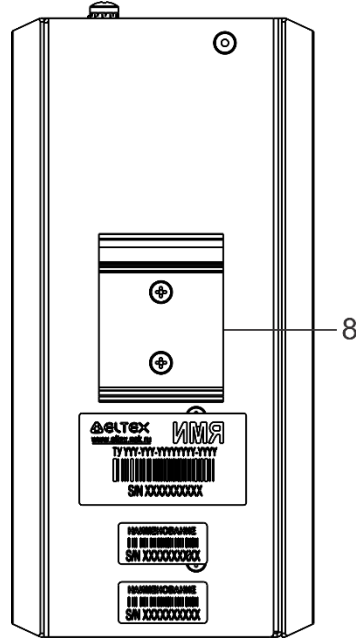


Рисунок 39 – Задняя панель MES3500I-10P

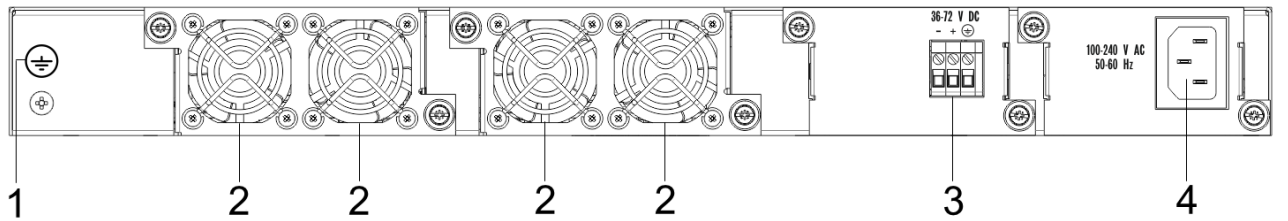


Рисунок 40 – Задняя панель MES5312, MES5324A, MES5332A

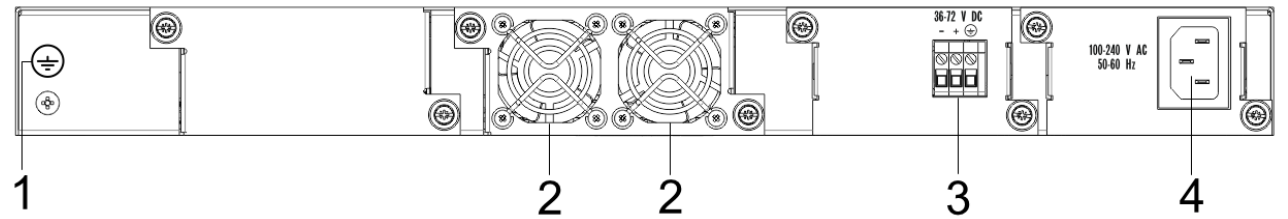


Рисунок 41 – Задняя панель MES5316A

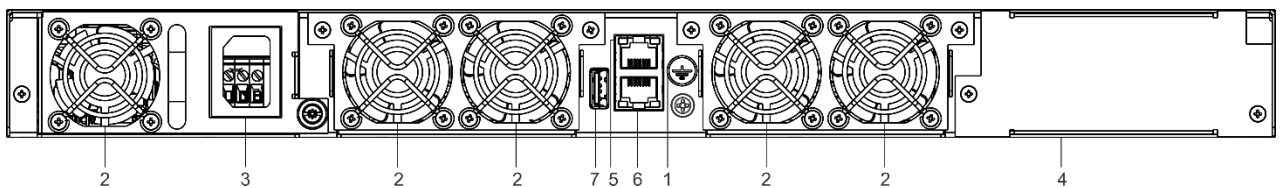


Рисунок 42 – Задняя панель MES5310-48

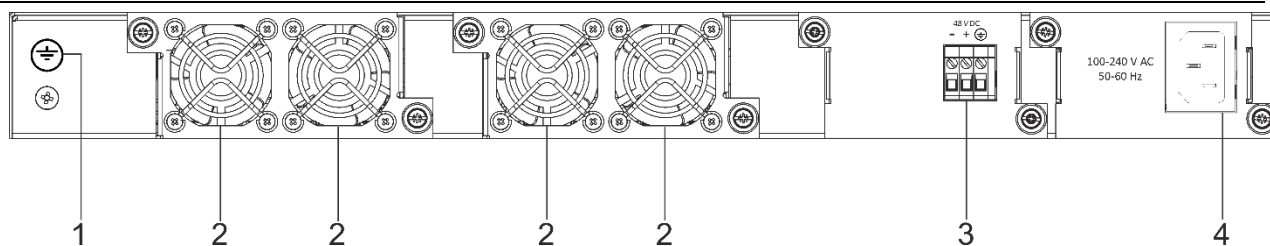


Рисунок 43 – Задняя панель MES5400-24

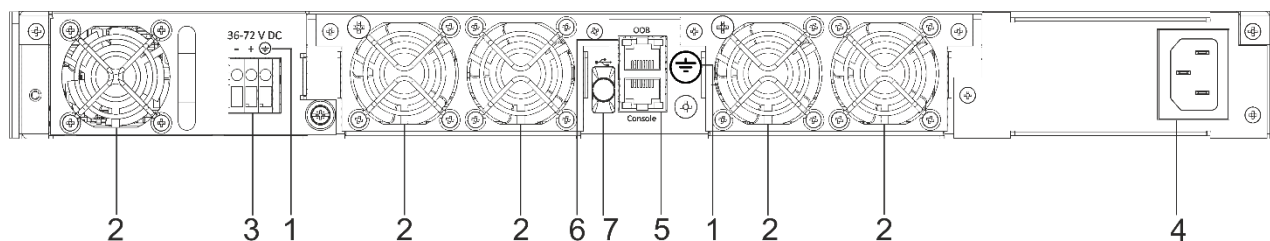


Рисунок 44 – Задняя панель MES5400-48

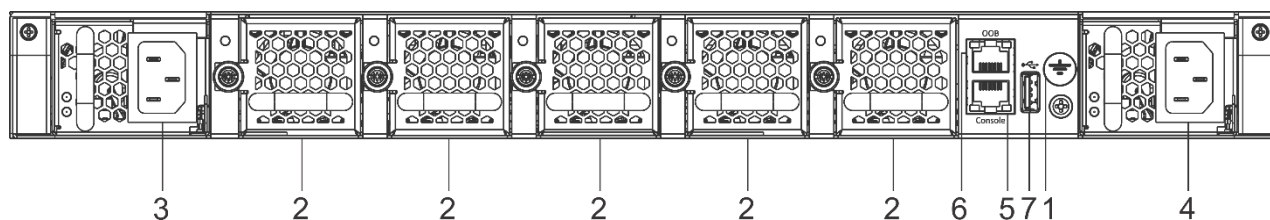


Рисунок 45 – Задняя панель MES5410-48

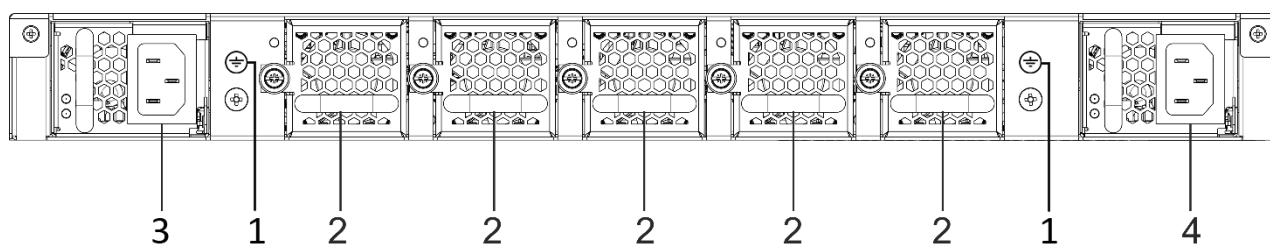


Рисунок 46 – Задняя панель MES5500-32

В таблице 11 приведен перечень разъемов, расположенных на задней панели коммутаторов MES2300-24, MES2300B-24, MES2300B-24F, MES2300-24P, MES2300D-24P, MES2300DI-28, MES2300-48P, MES2300B-48, MES3300-24, MES3300-08F, MES3300-16F, MES3300-24F, MES3300-48, MES3300-48F, MES3500I-10P, MES5310-48, MES5312, MES5316A, MES5324A, MES5332A, MES5400-24, MES5400-48, MES5410-48, MES5500-32.

Таблица 13 – Описание разъемов задней панели коммутаторов MES2300-24, MES2300B-24, MES2300B-24F, MES2300-24P, MES2300D-24P, MES2300DI-28, MES2300-48P, MES2300B-48, MES3300-24, MES3300-08F, MES3300-16F, MES3300-24F, MES3300-48, MES3300-48F, MES3500I-10P, MES5310-48, MES5312, MES5316A, MES5324A, MES5332A, MES5400-24, MES5400-48, MES5410-48, MES5500-32

| № | Элемент задней панели | Описание |
|---|------------------------------------|--|
| 1 | Клемма заземления | Клемма для заземления устройства. |
| 2 | Вентиляторы | Вентиляторы для охлаждения устройства. |
| 3 | Слоты для установки блоков питания | Слот для установки резервного блока питания AC или DC. |
| 4 | | Слот для установки основного блока питания AC или DC. |

| | | | |
|---|-----------|---|---|
| 5 | Console | | Консольный порт для локального управления устройством. |
| 6 | OOB | MES3300-48 MES3300-48F MES5310-48 MES5410-48 MES5400-48 | Порт (out-of-band) 10/100/1000BASE-T (RJ-45) для удаленного управления устройством. Управление осуществляется по сети, отдельно с каналом передачи данных. |
| 7 | | | USB-порт. |
| 8 | Кронштейн | MES3500I-10P | Кронштейн для установки устройства на DIN-рейку. |

2.4.3 Боковые панели устройства

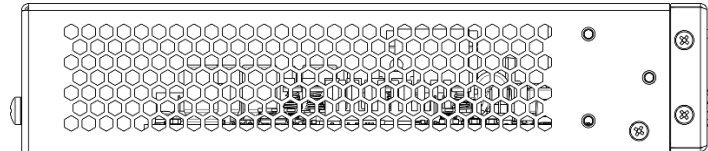


Рисунок 47 – Левая боковая панель MES2300-24, MES2300B-24, MES2300-24P

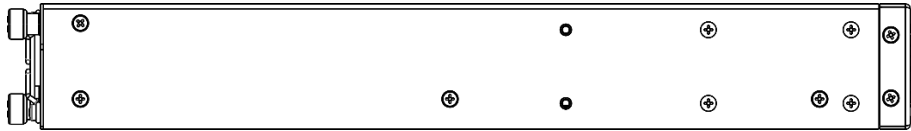


Рисунок 48 – Левая боковая панель MES2300B-24F

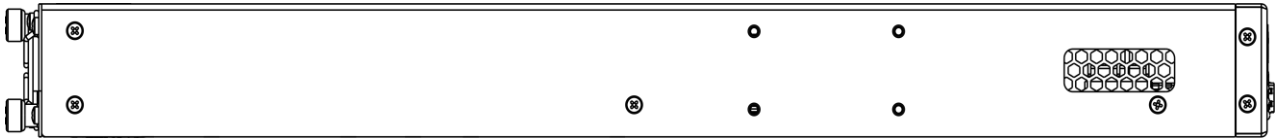


Рисунок 49 – Левая боковая панель MES2300D-24P

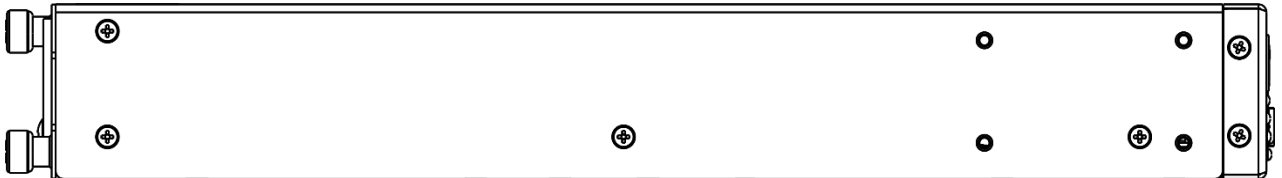


Рисунок 50 – Левая боковая панель MES2300DI-28

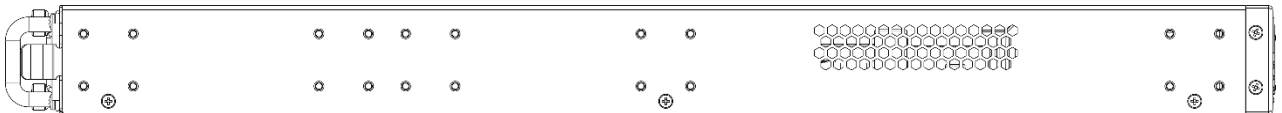


Рисунок 51 – Левая боковая панель MES2300-48P



Рисунок 52 – Левая боковая панель MES2300B-48

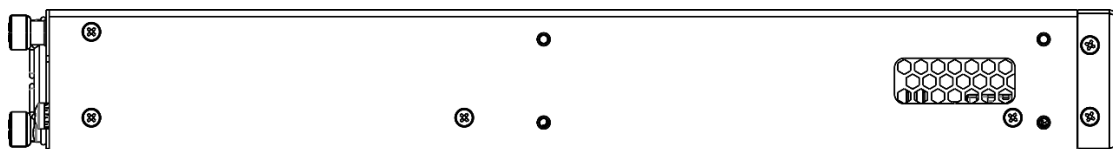


Рисунок 53 – Левая боковая панель MES3300-24

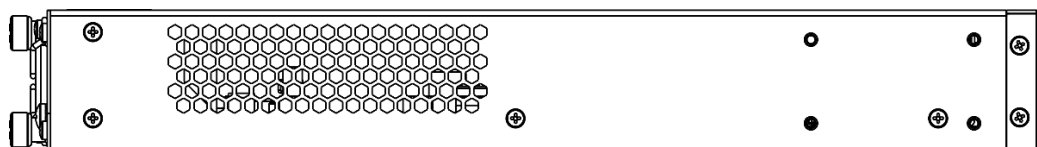


Рисунок 54 – Левая боковая панель MES3300-08F

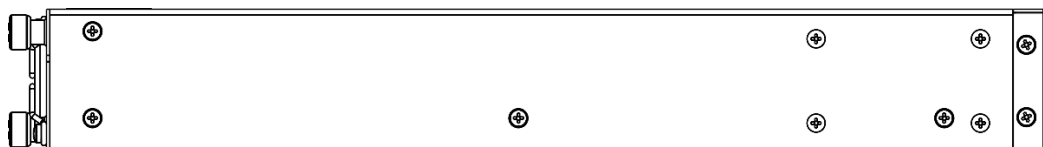


Рисунок 55 – Левая боковая панель MES3300-16F

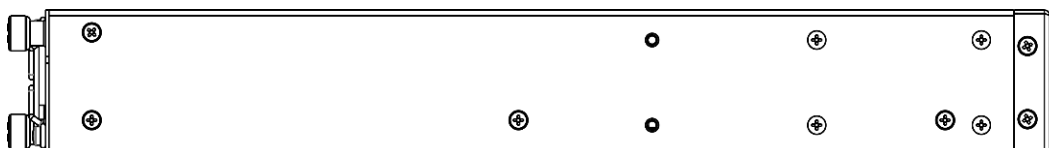


Рисунок 56 – Левая боковая панель MES3300-24F



Рисунок 57 – Левая боковая панель MES3300-48

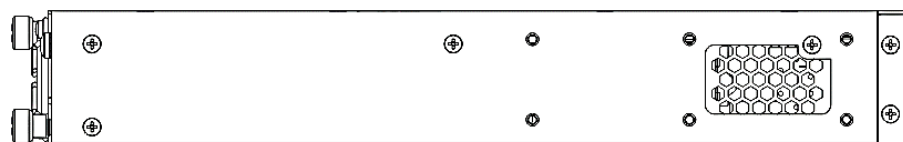


Рисунок 58 – Левая боковая панель MES5316A, MES5324A, MES5332A

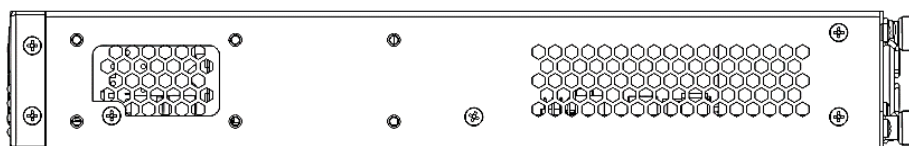


Рисунок 59 – Правая боковая панель MES5316A, MES5324A, MES5332A

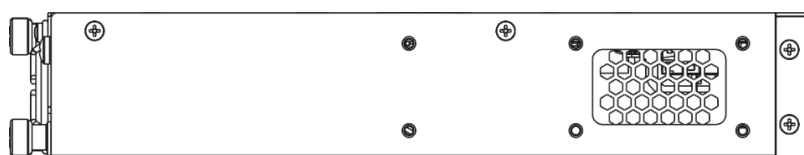


Рисунок 60 – Левая боковая панель MES5312

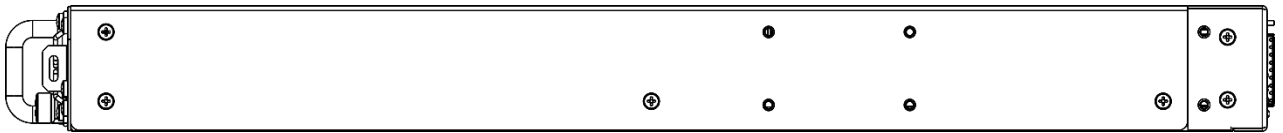


Рисунок 61 – Левая боковая панель MES5310-48

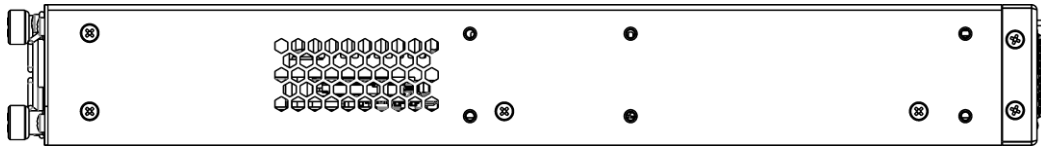


Рисунок 62 – Левая боковая панель MES5400-24

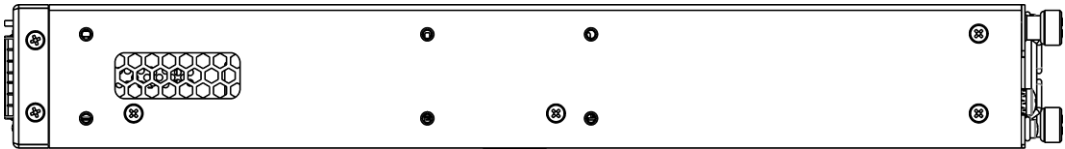


Рисунок 63 – Правая боковая панель MES5400-24

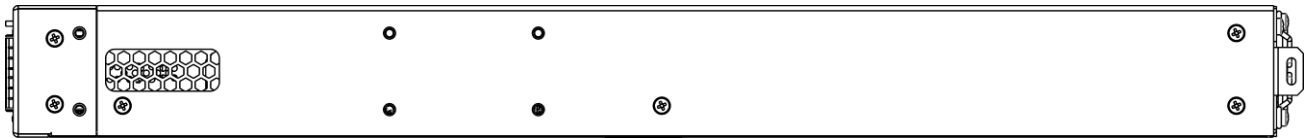


Рисунок 64 – Правая боковая панель MES5400-48

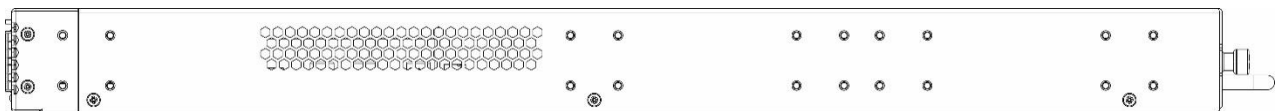


Рисунок 65 – Правая боковая панель MES5410-48

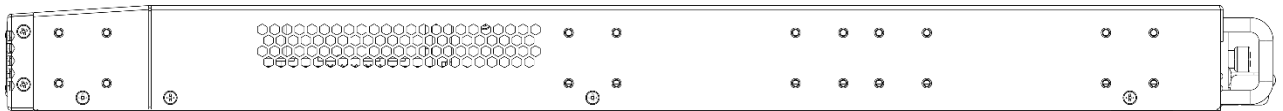


Рисунок 66 – Правая боковая панель MES5500-32

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 Световая индикация

Состояние интерфейсов Ethernet для моделей MES2300-24, MES3300-24, MES3300-24F, MES5312, MES53xxA, MES5400-xx, MES5410-48 индицируется двумя светодиодными индикаторами, *LINK/ACT* зеленого цвета и *SPEED* янтарного цвета. Расположение светодиодов показано на рисунках ниже.

Link   Speed

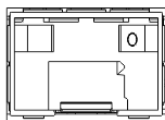


Рисунок 67 – Внешний вид одинарного разъема SFP/SFP+

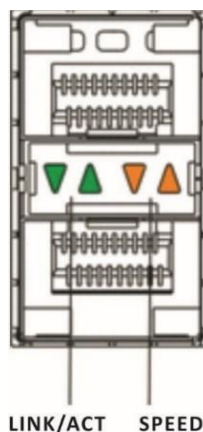


Рисунок 68 – Внешний вид сдвоенного разъема SFP/SFP+/SFP28

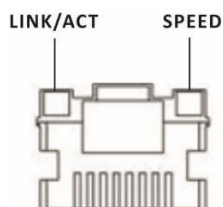


Рисунок 69 – Внешний вид разъема RJ-45

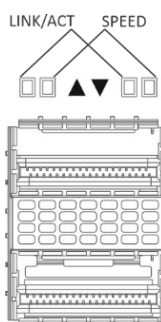


Рисунок 70 – Внешний вид разъема QSFP+ и QSFP28 для MES5400-xx, MES5410-48

Для модели MES5500-32 состояние интерфейсов QSFP28 индицируется четырьмя светодиодными индикаторами зеленого и янтарного цветов: данные индикаторы могут принимать как роль LINK, так и SPEED, их состояния описаны в таблицах 19, 20, 21. Для каждого режима работы порта индикаторы имеют различное назначение. Ввиду этого в таблицах 19, 20, 21 данные индикаторы будут пронумерованы как «индикатор 1», «индикатор 2», «индикатор 3», «индикатор 4».

Состояние интерфейсов XG-портов индицируется двумя светодиодными индикаторами, LINK/ACT зеленого цвета и SPEED янтарного цвета. Расположение светодиодов показано на рисунках ниже.

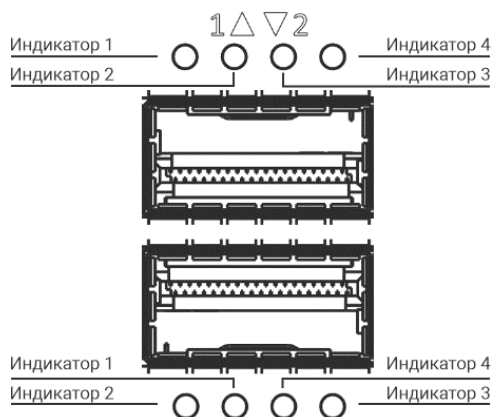


Рисунок 71 – Внешний вид разъема QSFP+ и QSFP28 для MES5500-32

Таблица 14 – Световая индикация состояния интерфейсов QSFP28

| <i>Свечение индикатора SPEED</i> | <i>Свечение индикатора LINK/ACT</i> | <i>Состояние интерфейса Ethernet</i> |
|----------------------------------|-------------------------------------|--|
| Выключен | Выключен | Порт выключен или соединение не установлено. |
| Выключен | Горит постоянно | Установлено соединение на скорости 40 Гбит/с. |
| Горит постоянно | Горит постоянно | Установлено соединение на скорости 100 Гбит/с. |
| X | Мигание | Идет передача данных. |

Таблица 15 – Световая индикация состояния интерфейсов SFP28

| <i>Свечение индикатора SPEED</i> | <i>Свечение индикатора LINK/ACT</i> | <i>Состояние интерфейса Ethernet</i> |
|----------------------------------|-------------------------------------|---|
| Выключен | Выключен | Порт выключен или соединение не установлено. |
| Выключен | Горит постоянно | Установлено соединение на скорости 10 Гбит/с. |
| Горит постоянно | Горит постоянно | Установлено соединение на скорости 25 Гбит/с. |
| X | Мигание | Идет передача данных. |

Таблица 16 – Световая индикация состояния интерфейсов SFP+

| <i>Свечение индикатора SPEED</i> | <i>Свечение индикатора LINK/ACT</i> | <i>Состояние интерфейса Ethernet</i> |
|----------------------------------|-------------------------------------|---|
| Выключен | Выключен | Порт выключен или соединение не установлено. |
| Выключен | Горит постоянно | Установлено соединение на скорости 1 Гбит/с. |
| Горит постоянно | Горит постоянно | Установлено соединение на скорости 10 Гбит/с. |
| X | Мигание | Идет передача данных. |

Таблица 17 – Световая индикация состояния интерфейсов SFP

| <i>Свечение индикатора SPEED</i> | <i>Свечение индикатора LINK/ACT</i> | <i>Состояние интерфейса Ethernet</i> |
|----------------------------------|-------------------------------------|--|
| Выключен | Выключен | Порт выключен или соединение не установлено. |
| Выключен | Горит постоянно | Установлено соединение на скорости 100 Мбит/с. |
| Горит постоянно | Горит постоянно | Установлено соединение на скорости 1 Гбит/с. |
| X | Мигание | Идет передача данных. |

Таблица 18 – Световая индикация состояния Ethernet-портов 10/100/1000BASE-T

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

Таблица 19 – Световая индикация состояния интерфейсов QSFP28 для MES5500-32

| <i>Состояние индикатора</i> | | | | <i>Состояние интерфейса Ethernet</i> |
|-----------------------------|--------------------------|--------------------------|--------------------------|--|
| <i>Индикатор 1</i> | <i>Индикатор 2</i> | <i>Индикатор 3</i> | <i>Индикатор 4</i> | |
| Выключен | Выключен | Выключен | Выключен | Порт выключен или соединение не установлено. |
| Горит постоянно зеленым | Горит постоянно янтарным | Горит постоянно янтарным | Выключен | Установлено соединение на скорости 40 Гбит/с. |
| Горит постоянно зеленым | Горит постоянно янтарным | Горит постоянно янтарным | Горит постоянно янтарным | Установлено соединение на скорости 100 Гбит/с. |
| Мигание | X | X | X | Идет передача данных. |

Таблица 20 – Световая индикация состояния интерфейсов QSFP28 для MES5500-32 в режиме расщепления

| <i>Состояние индикатора</i> | | | | <i>Состояние интерфейса Ethernet</i> |
|-----------------------------|-------------------------|-------------------------|-------------------------|---|
| <i>Индикатор 1</i> | <i>Индикатор 2</i> | <i>Индикатор 3</i> | <i>Индикатор 4</i> | |
| Выключен | Выключен | Выключен | Выключен | Порт выключен или соединение не установлено. |
| Горит постоянно зеленым | Горит постоянно зеленым | Горит постоянно зеленым | Горит постоянно зеленым | Установлено соединение на скорости 1 Гбит/с. |
| Горит постоянно зеленым | Горит постоянно зеленым | Горит постоянно зеленым | Горит постоянно зеленым | Установлено соединение на скорости 10 Гбит/с. |

| | | | | |
|-------------------------|-------------------------|-------------------------|-------------------------|---|
| Горит постоянно зеленым | Горит постоянно зеленым | Горит постоянно зеленым | Горит постоянно зеленым | Установлено соединение на скорости 25 Гбит/с. |
| Мигание | Мигание | Мигание | Мигание | Идет передача данных. |

Таблица 21 – Световая индикация состояния интерфейсов SFP+ для MES5500-32

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

Индикатор *Unit ID* (1-8) служит для обозначения номера устройства в стеке. Системные индикаторы (Power, Master, Fan, RPS) служат для определения состояния работы узлов коммутаторов.

Таблица 22 – Световая индикация системных индикаторов

| Название индикатора | Функция индикатора | Состояние индикатора | | Состояние устройства |
|---------------------|--|----------------------------|---|---|
| <i>Power</i> | Состояние источников питания | Выключен | | Питание выключено. |
| | | Зеленый, горит постоянно | | Питание включено, нормальная работа устройства. |
| | | Оранжевый | MES5312 MES5316A MES5324A MES5332A | Отсутствие первичного питания основного источника (при питании устройства от резервного источника) или авария вторичного источника. |
| | | Красный | MES2300B-24F MES2300-24P MES3300-24 MES3300-08F MES3300-16F MES3300-24F MES3300-48 MES3300-48F MES5400-24 MES5400-48 MES5410-48 MES5500-32 | |
| <i>Master</i> | Признак ведущего устройства при работе в стеке | Зеленый, горит постоянно | | Устройство является «мастером» стека. |
| | | Выключен | | Устройство не является «мастером» в стеке. |
| <i>Status</i> | Индикатор состояния устройства | MES2300-24P MES2300-48P | Зеленый, горит постоянно | Все внутренние системы работают в штатном режиме. |
| | | | Красный, горит постоянно | Возможная неисправность вентиляторов, высокая температура на одном из термодатчиков. Ошибки PoE (только для MES2300-48P). |
| <i>Fan</i> | Состояние вентилятора охлаждения | Зеленый, горит постоянно | | Все вентиляторы исправны. |
| | | Красный, горит постоянно | | Отказ одного или более вентиляторов. |
| <i>RPS</i> | Режим работы резервного | Зеленый, горит постоянно | | Резервный источник подключен и работает нормально. |

| | | | | |
|------|---|--------------------------|--------------------------|---|
| | источника питания | Красный, горит постоянно | | Отсутствие первичного питания резервного источника или его неисправность. |
| | | Выключен | | Резервный источник не подключен. |
| PoE | Состояние PoE | MES2300-24P | Зеленый, горит постоянно | Подключен потребитель PoE хотя бы в один порт. |
| | | | Красный, горит постоянно | Авария PoE (порт в состоянии перегрузки, глобальная авария PoE). |
| | | | Выключен | Потребители PoE не подключены. |
| PS1 | Состояние блока питания Main | MES2300-48P | Зеленый, горит постоянно | Блок питания подключен и запитан, есть выходной ток с блока питания. |
| | | | Красный, горит постоянно | Блок питания установлен, но отсутствует входное напряжение/ нет выходного тока с блока питания. |
| PS2 | Состояние блока питания Redudant | MES2300-48P | Зеленый, горит постоянно | Блок питания подключен и запитан, есть выходной ток с блока питания. |
| | | | Красный, горит постоянно | Блок питания установлен, но отсутствует входное напряжение/ нет выходного тока с блока питания. |
| PWR1 | Индикаторы состояния питания устройства | MES3500I-10P | Зеленый, горит постоянно | Подано питание на ввод PWR1. |
| | | | Выключен | Питание на ввод PWR1 не подано. |
| PWR2 | | | Зеленый, горит постоянно | Подано питание на ввод PWR2. |
| | | | Выключен | Питание на ввод PWR2 не подано. |
| Temp | Индикатор температуры | | Красный, горит постоянно | Перегрев устройства. |
| | | | Выключен | Нормальная работа, перегрева нет. |
| PoE | Индикаторы состояния PoE | | Зеленый, горит постоянно | Подключен потребитель PoE в соответствующий порт. |
| | | | Выключен | Потребитель PoE не подключен в соответствующий порт. |

2.5 Комплект поставки

В базовый комплект поставки входят:

- Ethernet-коммутатор;
- Комплект крепежа в стойку;
- Шнур питания Евровилка-C13, 1.8м (только для MES2300-24, MES2300B-24F, MES2300-24P, MES2300B-48);
- Шнур питания ПВС 2х1.5, 2м (только для MES2300B-24F, MES2300B-48, MES3500I-10P);
- Разъем кабельной части 2EDGK-5.08-02P-14-00AH — 2 шт. (только для MES3500I-10P);
- Разъем кабельной части 2EDGK-5.08-03P-14-00AH — 1 шт. (только для MES3500I-10P);
- Памятка о документации;
- Сертификат соответствия;
- Паспорт.

По заказу покупателя в комплект поставки опционально могут быть включены:

- Руководство по эксплуатации на CD-диске;
- Консольный кабель;
- Модуль питания PM160-220/12 (для MES3300-08F, MES3300-16F, MES3300-24, MES3300-24F, MES3300-48, MES5312, для серии MES53xxA, MES5400-24);
- Модуль питания PM350-220/12 (для MES5400-48);
- Модуль питания PM600-220/12 (для MES5410-48, MES5500-32);
- Модуль питания PM950-220/56 (для MES2300-48P);
- Шнур питания Евровилка-C13, 1.8м (в случае комплектации модулем питания PM160-220/12, PM350-220/12, PM600-220/12 или PM950-220/56);
- Модуль питания PM100-48/12 (для MES3300-08F, MES3300-16F, MES3300-24, MES3300-24F, MES3300-48, MES5312, для серии MES53xxA);
- Модуль питания PM160-48/12 (для MES5400-24);
- Модуль питания PM350-48/12 (для MES5400-48);
- Модуль питания PM600-48/12 (для MES5410-48, MES5500-32);
- Модуль питания PM950-48/56 (для MES2300-48P);
- Шнур питания ПВС (в случае комплектации модулем питания PM100-48/12, PM160-48/12, PM350-48/12, PM600-48/12 или PM950-48/56);
- SFP/SFP+/SFP28/QSFP+/QSFP28 трансиверы.

3 УСТАНОВКА И ПОДКЛЮЧЕНИЕ

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

3.1 Крепление кронштейнов

В комплект поставки устройства входят кронштейны для установки в стойку и винты для крепления кронштейнов к корпусу устройства. На кронштейнах расположены шесть крепежных отверстий для разных вариантов крепления, что позволяет регулировать расстояние между передней панелью и дверцей серверного шкафа (рисунки 59–61). Для установки кронштейнов выберите один из вариантов крепления:

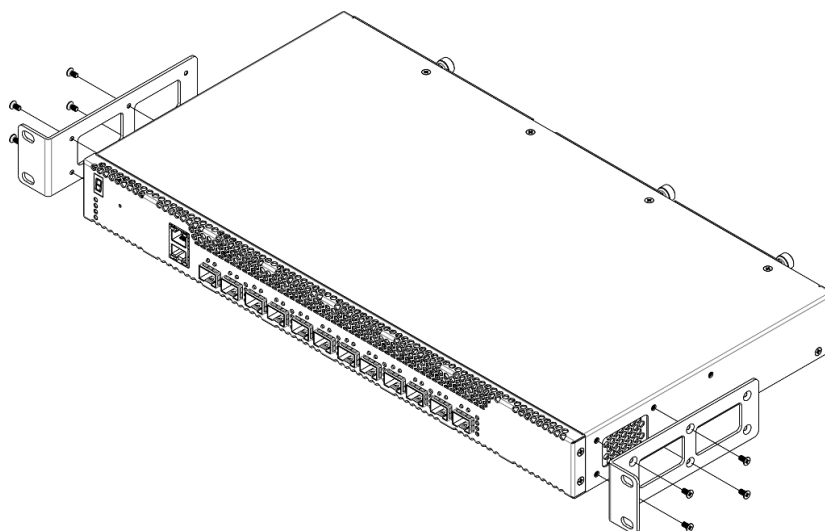


Рисунок 72 – Вариант крепления кронштейнов №1

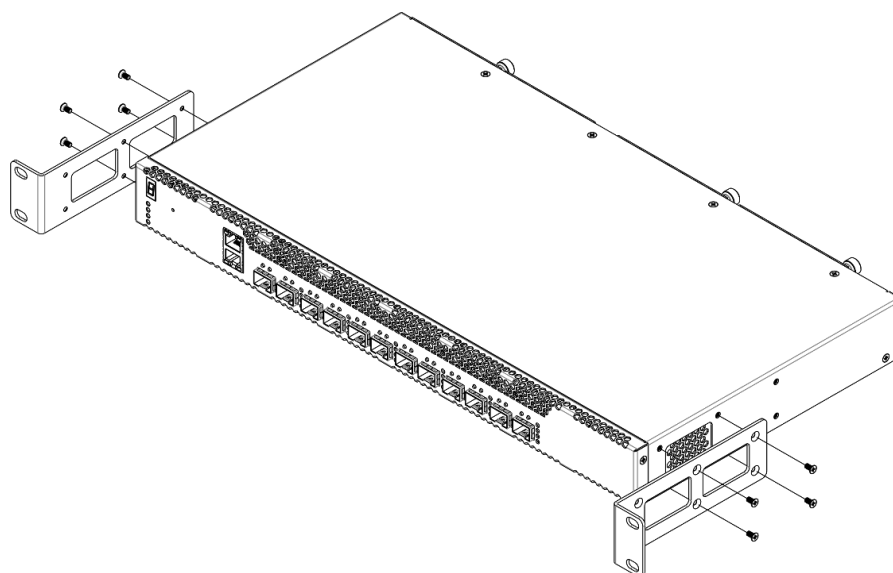


Рисунок 73 – Вариант крепления кронштейнов №2

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

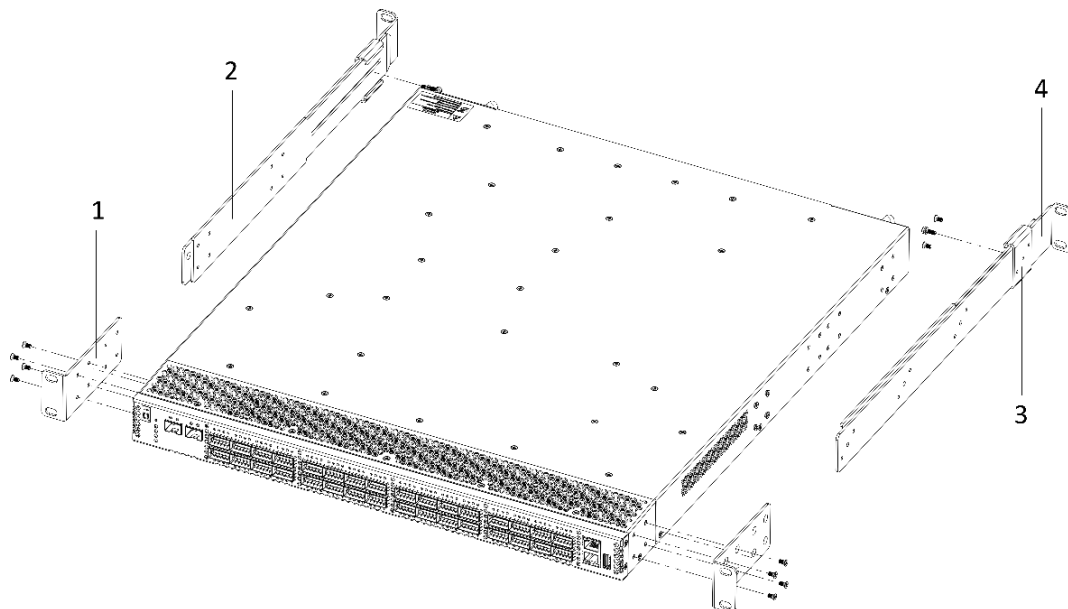


Рисунок 74 – Вариант крепления кронштейнов для MES5410-48, MES5500-32

Для деталей кронштейна предусмотрено несколько положений, зависящих от глубины используемой стойки. Минимальная глубина, на которую рассчитан кронштейн — 537.5 мм, максимальная — 787.5 мм.

1. Выберите необходимое положение детали 1 (два варианта положения). Совместите четыре отверстия на детали 1 с четырьмя отверстиями на боковой панели устройства. С помощью отвертки прикрепите деталь кронштейна винтами к корпусу.
2. Выберите необходимое положение детали 2 (два варианта положения). Совместите восемь отверстий на детали 2 с восемью отверстиями на боковой панели устройства. С помощью отвертки прикрепите деталь кронштейна винтами к корпусу.
3. Выберите необходимое положение детали 3 (четыре варианта положения). Совместите три отверстия на детали 3 с такими же выбранными отверстиями на детали 4. С помощью отвертки соедините детали винтами с внутренней стороны кронштейна, закручивая только крайние винты.
4. Повторите шаги 1–4 с другой боковой панелью устройства.
5. Далее производится установка устройства в стойку (см. раздел 3.2).

3.2 Установка устройства в стойку

3.2.1 Установка устройств MES2300-xx, MES3300-xx, MES5312, MES53xxA, MES5400-xx

Для установки устройства в стойку:

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

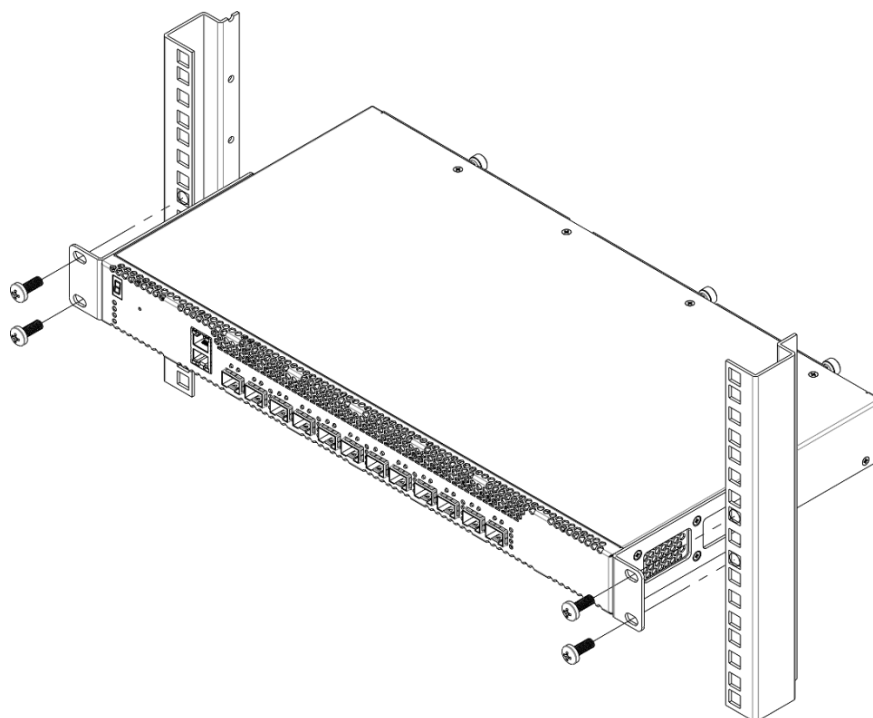


Рисунок 75 – Установка устройства в стойку

3.2.1 Установка устройств MES5410-48, MES5500-32

Для установки устройств MES5410-48, MES5500-32 в стойку:

1. Зафиксируйте деталь 4 на направляющей стойки с помощью винтов.
2. Вставьте устройство в стойку, используя деталь 3 как направляющую.
3. Зафиксируйте деталь 1 на направляющей стойки.
4. Используя отвертку, зафиксируйте центральный винт, соединяющий детали 2 и 3.

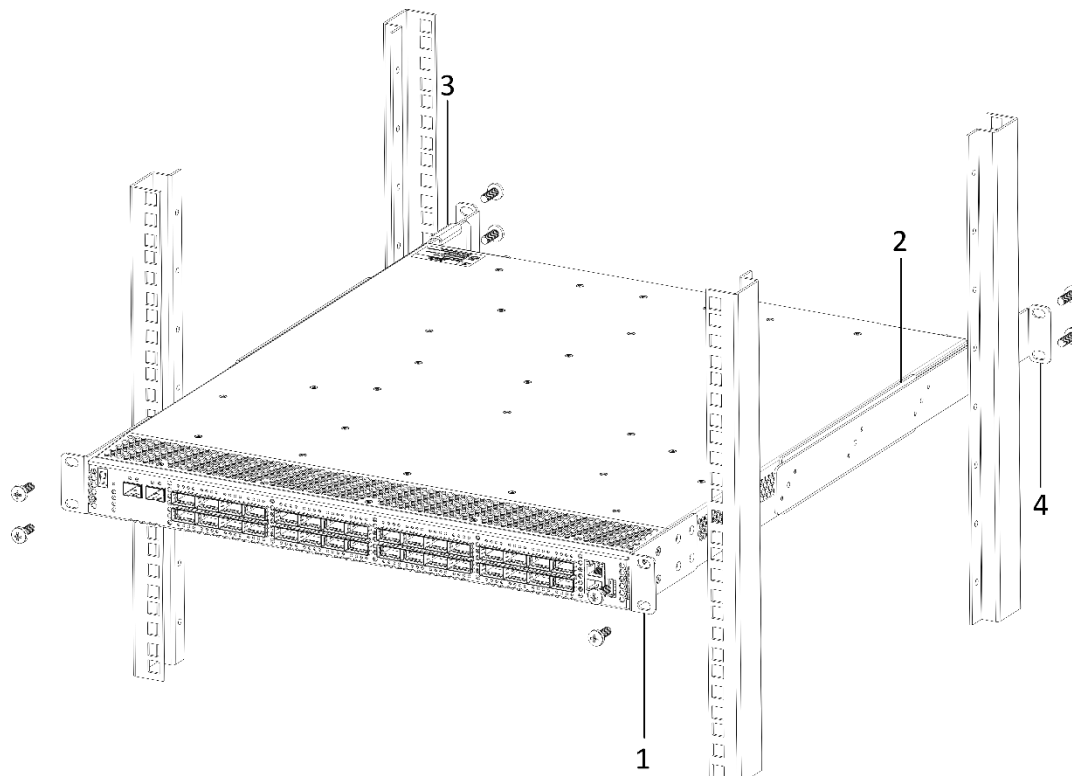


Рисунок 76 – Установка устройства MES5500-32 в стойку

3.2.2 Размещение коммутаторов в стойке

На рисунке ниже приведен пример размещения коммутаторов MES5312 в стойке.



Рисунок 77 – Размещение коммутаторов MES5312 в стойке



Аналогично происходит размещение остальных коммутаторов в стойке.



Не закрывайте вентиляционные отверстия, а также вентиляторы, расположенные на задней панели, посторонними предметами во избежание перегрева компонентов коммутатора и нарушения его работы.

3.2.3 Установка устройства MES3500I-10P на DIN-рейку



Устройство MES3500I-10P устанавливается вертикально, так как боковые панели обеспечивают теплоотвод.

Для установки устройства на DIN-рейку:

1. Наклонить корпус устройства верхней частью от себя и приложить к DIN-рейке так, чтобы её верхняя кромка оказалась за проволочной пружиной.
2. Надавить на корпус устройства сверху.
3. Не снимая давления, прижать нижнюю часть корпуса устройства к DIN-рейке до защелкивания.

Для демонтажа устройства с DIN-рейки:

1. Надавить на корпус устройства сверху.
2. Не снимая давления, потянуть нижнюю часть устройства на себя.
3. Приподняв корпус, снять устройство с DIN-рейки.

3.3 Установка модулей питания

Коммутатор может работать с одним или двумя модулями питания. Установка второго модуля питания необходима в случае использования устройства в условиях, требующих повышенной надежности.

Места для установки модулей питания с электрической точки зрения равноценны. С точки зрения использования устройства, модуль питания, находящийся ближе к краю, считается основным, ближе к центру – резервным. Модули питания могут устанавливаться и извлекаться без выключения устройства. При установке или извлечении дополнительного модуля питания коммутатор продолжает работу без перезапуска.



Перед обслуживанием изделия, ремонтом или другими аналогичными действиями отключите изделие от всех источников питания.

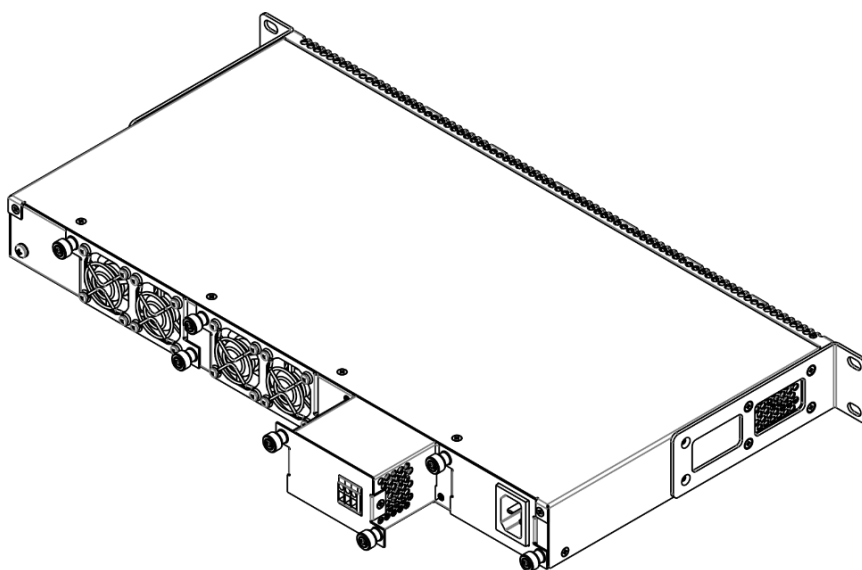


Рисунок 78 – Установка модулей питания

Состояние модулей питания может быть проверено по индикации на передней панели коммутатора (см. раздел 2.4.4) или по диагностике, доступной через интерфейсы управления коммутатором.



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

3.4 Подключение питающей сети

1. Прежде чем к устройству будет подключена питающая сеть, необходимо заземлить корпус устройства. Заземление необходимо выполнять изолированным многожильным проводом. Устройство заземления и сечение заземляющего провода должны соответствовать требованиям ПУЭ.



Подключение должно осуществляться квалифицированным специалистом.

2. Если предполагается подключение компьютера или иного оборудования к консольному порту коммутатора, 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. При подключении к сети постоянного тока используйте провод сечением не менее 1 мм² и соблюдайте полярность, указанную на блоке питания.



Во избежание возникновения короткого замыкания при подключении к сети постоянного тока рекомендуется произвести зачистку провода на длину 9 мм.



Цепь питания постоянным током должна содержать устройство отключения питания с физическим разъединением соединения (выключатель, разъем, контактор, автоматический выключатель и т.п.).

4. Включите питание устройства и убедитесь в отсутствии аварий по состоянию индикаторов на передней панели.

3.5 Установка и удаление SFP-трансиверов



Только для MES5500-32: во избежание повреждения устройства при одновременном использовании портов XG1 и XG2 необходимо использовать SFP+ трансиверы с типом разъема LC или SFP+ Direct Attached Cable (DAC).



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

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

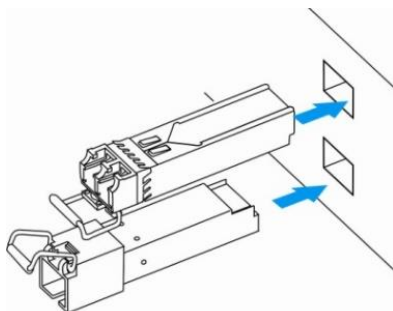


Рисунок 79 – Установка SFP-трансиверов

2. Надавите на модуль. Когда он встанет на место, вы услышите характерный щелчок.

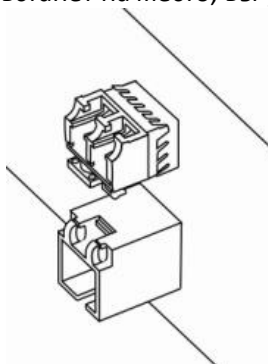


Рисунок 80 – Установленные SFP-трансиверы

Для удаления трансивера:

1. Откройте защелку модуля.

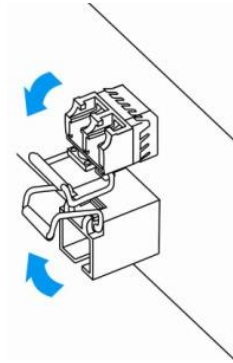


Рисунок 81 – Открытие защелки SFP-трансиверов

2. Извлеките модуль из слота.

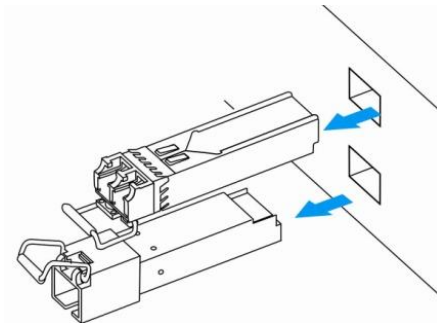


Рисунок 82 – Извлечение SFP-трансиверов

4 НАЧАЛЬНАЯ НАСТРОЙКА КОММУТАТОРА

4.1 Настройка терминала

На компьютере запустить программу эмуляции терминала (HyperTerminal, TeraTerm, Minicom) и произвести следующие настройки:

- выбрать соответствующий последовательный порт;
- установить скорость передачи данных – 115200 бод;
- задать формат данных: 8 бит данных, 1 стоповый бит, без контроля четности;
- отключить аппаратное и программное управление потоком данных;
- задать режим эмуляции терминала VT100 (многие терминальные программы используют данный режим эмуляции терминала в качестве режима по умолчанию).

4.2 Включение устройства

Установить соединение консоли коммутатора (порт «console») с разъемом последовательного интерфейса компьютера, на котором установлено программное обеспечение эмуляции терминала.

Включить устройство. При каждом включении коммутатора запускается процедура «тестирования системы при включении» (POST), которая позволяет определить работоспособность устройства перед загрузкой исполняемой программы в оперативную память (ОЗУ).

Отображение хода выполнения процедуры POST на коммутаторах MES5312:

```

BootROM 1.43
Booting from SPI flash

General initialization - Version: 1.0.0
Serdes initialization - Version: 1.0.2
PEX: pexIdx 0, detected no link
PEX: pexIdx 0, detected no link
PEX: pexIdx 0, detected no link
DDR3 Training Sequence - Ver TIP-1.55.0
DDR3 Training Sequence - Switching XBAR Window to FastPath Window
DDR3 Training Sequence - Ended Successfully
BootROM: Image checksum verification PASSED

ROS Booton: Jun 13 2018 17:16:12 ver. 1.0

Press x to choose XMODEM...
Booting from SPI flash
Tuned RAM to 512M

Running UBOOT...

U-Boot 2013.01 (Jun 22 2018 - 10:36:09)

Loading system/images/active-image ...
Uncompressing Linux... done, booting the kernel.

Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.
```

Спустя две секунды после завершения процедуры POST начинается автозагрузка программного обеспечения коммутатора. Для выполнения специальных процедур используется меню Startup, войти в которое можно, прервав загрузку нажатием клавиши **<Esc>** или **<Enter>** в течение этого времени.

После успешной загрузки коммутатора появится системное приглашение интерфейса командной строки CLI.

```
>lcli

Console baud-rate auto detection is enabled, press Enter twice to complete the
detection process

User Name:
Detected speed: 115200

User Name:admin
Password:***** (admin)

console#
```



Для быстрого вызова справки о доступных командах используйте комбинацию клавиш **<Shift>** и **<?>**.

4.3 Загрузочное меню

Для входа в загрузочное меню следует подключиться к устройству через интерфейс RS-232, перезагрузить устройство и в течение двух секунд после завершения процедуры POST нажать «ESC» или «ENTER»:

```
U-Boot 2013.01 (Jul 05 2021 - 13:21:16) Eltex version: 2014_T3.0_eng_dropv6 6.2.2

Loading system/images/active-image ...
Uncompressing Linux... done, booting the kernel.

Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.
```

Вид загрузочного меню:

```
Startup Menu

[1] Image menu
[2] Restore Factory Defaults
[3] Boot password
[4] Password Recovery Procedure
[5] Back
Enter your choice or press 'ESC' to exit:
```

Таблица 23 – Функции интерфейса загрузочного меню

| Функция | Описание |
|-----------------------------|--|
| Image menu | Выбрать активный образа системного ПО. |
| Restore Factory Defaults | Восстановить заводские настройки. |
| Boot password | Установить/удалить пароль на bootrom. |
| Password Recovery Procedure | Сбросить настройки аутентификации. |
| Back | Продолжить загрузку. |

4.4 Режим работы коммутатора

Коммутаторы серий MES2300-xx, MES3300-xx, MES5312, MES53xxA, MES5400-xx, MES5410-48, MES5500-32 работают в режиме стекирования¹.

Стек функционирует как единое устройство и может объединять до 8 коммутаторов одной и той же модели, имеющих следующие роли, определяемые их порядковыми номерами (UID):

- *Master* (UID устройства 1 или 2), с него происходит управление всеми устройствами в стеке.
- *Backup* (UID устройства 1 или 2) – устройство, подчиняющееся master. Дублирует все настройки, и, в случае выхода управляющего устройства из строя, берет на себя функции управления стеком.
- *Slave* (UID устройств от 3 до 8) – устройства, подчиняющиеся master. Не может работать в автономном режиме (если отсутствует master).



Для корректной работы стека необходим хотя бы один юнит с ролью master и один юнит с ролью backup.



Интерфейсы в режиме стекирования работают только на максимальной скорости интерфейса.

В режиме стекирования для синхронизации коммутаторы MES2300-24, MES3300-24, MES3300-24F, MES5312, MES5316A, MES5316A rev.C, MES5316A rev.C1, MES5324A, MES5324A rev.C, MES5324A rev.C1, MES5332A, MES5332A rev.C используют XG-порты, а коммутаторы MES5400-24, MES5400-48, MES5410-48, MES5500-32 используют HG-порты. При этом указанные порты не участвуют в передаче данных. Возможно стекирование коммутаторов только одной модели и с тем же количеством портов, к примеру, стекируются друг с другом MES5316A и MES5316A. Стекировать коммутаторы MES53xxA с коммутаторами MES53xxA rev.C и MES53xxA rev.C1 невозможно ввиду аппаратных различий этих моделей устройств. Возможны две топологии синхронизирующихся устройств – кольцевая и линейная. Рекомендуется использовать кольцевую топологию для повышения отказоустойчивости стека.

По умолчанию коммутатор является мастером, все порты участвуют в передаче данных.



Поддержана процедура автообновления на версию ПО с Master-коммутатора при добавлении новых юнитов в уже существующий стек.



Для коммутаторов MES2300/3300 работа стека из 4-8 юнитов поддерживается с версии 6.6.3.8.

¹ Функционал NSF (Non-Stop Forwarding) будет реализован ориентировочно в 2Q2025.

Таблица 24 – Матрица стекирования для MES2300-xx/MES3300-xx

| | MES2300-24 | MES2300B-24F | MES2300-24P | MES2300B-48 | MES2300-48P | MES3300-08F | MES3300-16F | MES3300-24 | MES3300-24F | MES3300-48 | MES3300-48F |
|--------------|------------|--------------|-------------|-------------|-------------|-------------|-------------|------------|-------------|------------|-------------|
| MES2300-24 | + | + | . | . | . | . | . | . | . | . | . |
| MES2300B-24F | + | + | . | . | . | . | . | . | . | . | . |
| MES2300-24P | . | . | + | . | . | . | . | . | . | . | . |
| MES2300B-48 | . | . | . | + | . | . | . | . | . | . | . |
| MES2300-48P | . | . | . | . | + | . | . | . | . | . | . |
| MES3300-08F | . | . | . | . | . | + | + | + | + | . | . |
| MES3300-16F | . | . | . | . | . | + | + | + | + | . | . |
| MES3300-24 | . | . | . | . | . | + | + | + | + | . | . |
| MES3300-24F | . | . | . | . | . | + | + | + | + | . | . |

| | | | | | | | | | | | | |
|-------------|---|---|---|---|---|---|---|---|---|---|---|---|
| MES3300-48F | . | . | . | . | . | . | . | . | . | . | + | + |
| MES3300-48 | . | . | . | . | . | . | . | . | . | . | + | + |

Таблица 25 – Матрица стекирования для MES53xxA

| | MES5316A | MES5316A rev.C | MES5316A rev.C1 | MES5324A | MES5324A rev.C | MES5324A rev.C1 | MES5332A | MES5332A rev.C |
|-----------------|----------|----------------|-----------------|----------|----------------|-----------------|----------|----------------|
| MES5316A | + | . | . | . | . | . | . | . |
| MES5316A rev.C | . | + | + | . | . | . | . | . |
| MES5316A rev.C1 | . | + | + | . | . | . | . | . |
| MES5324A | . | . | . | + | . | . | . | . |
| MES5324A rev.C | . | . | . | . | + | + | . | . |
| MES5324A rev.C1 | . | . | . | . | + | + | . | . |
| MES5332A | . | . | . | . | . | . | + | . |
| MES5332A rev.C | . | . | . | . | . | . | . | + |

Таблица 26 – Матрица стекирования для MES5400-xx, MES5500-32

| | MES5400-24 | MES5400-48 | MES5410-24 | MES5500-32 |
|------------|------------|------------|------------|------------|
| MES5400-24 | + | - | - | - |
| MES5400-48 | - | + | - | - |
| MES5410-24 | - | - | + | - |
| MES5500-32 | - | - | - | + |

Настройка стекирования коммутаторов

Запрос командной строки имеет следующий вид:

```
console (config) #
```

Таблица 27 – Базовые команды

| Команда | Значение/Значение по умолчанию | Действие |
|--|---------------------------------------|---|
| stack configuration links te <i>te_port hu hu_port</i> | - | Назначает интерфейсы для синхронизации работы коммутатора в стеке. Минимальное количество — 2 , максимальное — 2. |
| stack configuration unit-id <i>unit_id</i> | unit_id: (1..8, auto)/auto | Назначает номер устройства «unit-id» локальному устройству (на котором выполнена команда). Смена номера устройства произойдёт после перезагрузки коммутатора. |
| no stack configuration | | Удаление настроек стека. |
| stack unit <i>unit_id</i> | unit_id: (1..8, all) | Переход к конфигурированию юнита в стеке. |

Пример

- Объединить в стек два коммутатора MES5312. Назначить вторым юнитом, использовать интерфейсы te1-2 в качестве стекирующих.

```
console#config
console (config) #stack configuration unit-id 2 links te1-2
console (config) #
```

Команды режима Privileged EXEC

Запрос командной строки имеет следующий вид:

```
console#
```

Таблица 28 – Базовые команды, доступные в режиме EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|---|--------------------------------|---|
| <code>show stack</code> | - | Отображает информацию об устройствах, входящих в стек. |
| <code>show stack configuration</code> | - | Отображает информацию о стекирующих интерфейсах юнитов в стеке. |
| <code>show stack links [details]</code> | - | Расширенное отображение информации о стекирующих интерфейсах. |

- Пример использования команды `show stack links`:

```
console# show stack links
```

```
Topology is Chain
```

| Unit Id | Active Links | Neighbor Links | Operational Link Speed | Down/Standby Links |
|---------|--------------|----------------|------------------------|--------------------|
| 1 | te1/0/1 | te2/0/2 | 10G | te1/0/2 |
| 2 | te2/0/2 | te1/0/1 | 10G | te2/0/1 |



Устройства с одинаковыми идентификаторами «Unit ID» не могут работать в одном стеке.

4.5 Настройка функций коммутатора

Функции по начальному конфигурированию устройства можно разделить на два типа.

- **Базовая настройка** – включает в себя определение базовых функций конфигурации и настройку динамических IP-адресов.
- **Настройка параметров системы безопасности** – включает управление системой безопасности на основе механизма AAA (Authentication, Authorization, Accounting).



При перезагрузке устройства все несохраненные данные будут утеряны. Для сохранения любых внесенных изменений в настройку коммутатора используется следующая команда:

```
console# write
```

4.5.1 Базовая настройка коммутатора

Для начала конфигурации устройства необходимо подключить устройство к компьютеру через последовательный порт. Запустить на компьютере программу эмуляции терминала согласно пункту 4.1 «Настройка терминала».

Во время начальной настройки можно определить интерфейс, который будет использоваться для подключения к устройству удаленно.

Базовая настройка включает следующее:

1. Задание пароля для пользователя «admin» (с уровнем привилегий – 15).
2. Создание новых пользователей.
3. Настройка статического IP-адреса, маски подсети и шлюза по умолчанию.
4. Получение IP-адреса от сервера DHCP.
5. Настройка параметров протокола SNMP.

4.5.1.1 Задание пароля для пользователя «admin» и создание новых пользователей



Для обеспечения защищенного входа в систему необходимо назначить пароль привилегированному пользователю «admin».

Имя пользователя и пароль вводится при входе в систему во время сеансов администрирования устройства. Для создания нового пользователя системы или настройки любого из параметров – имени пользователя, пароля, уровня привилегий, используются команды:

```
console# configure
console(config)# username name password password privilege {1-15}
```



Уровень привилегий 1 разрешает доступ к устройству, но запрещает настройку. Уровень привилегий 15 разрешает как доступ, так и настройку устройства.

Пример команд для задания пользователю «admin» пароля «eltex» и создания пользователя «operator» с паролем «pass» и уровнем привилегий 1:

```
console# configure
console(config)# username admin password eltex
console(config)# username operator password pass privilege 1
console(config)# exit
console#
```

4.5.1.2 Расширенная настройка уровня доступа

На устройстве существует возможность распределения прав пользователей в зависимости от уровня привилегий, на котором каждый из пользователей был создан. Конкретному уровню привилегий присваивается набор команд, которые могут выполняться пользователями с уровнем не ниже заданного.



Коммутатор поддерживает систему наследования набора команд от более низких уровней привилегий.



Привилегии выстраиваются только для конкретно заданного узла. Каждую команду необходимо прописывать явно, не используя сокращенные формы.

Команды режима глобального конфигурирования

Запрос командной строки в режиме глобального конфигурирования имеет следующий вид:

```
console(config)#
```

Таблица 29 – Команды для настройки расширенного доступа

| Команда | Значение/Значение по умолчанию | Действие |
|---|---|---|
| <code>privilege context level command</code> | level: (1..15); /уровень привилегий команд режима EXEC — 1, всех остальных команд — 15 | Присваивает указанному уровню привилегий заданную команду. - <i>context</i> — режим работы командной строки; - <i>level</i> — уровень привилегий, на котором будет доступна настраиваемая команда; - <i>command</i> — команда. |
| <code>no privilege context level command</code> | | Удаляет доступ к команде с уровня, на котором команда была разрешена. |

Пример настройки набора команд для пользователя «admin» с 4 уровнем привилегий и набора команд для пользователя «user» с 10 уровнем привилегий:

```
console# configure
console(config)# username admin password pass1 privilege 4
console(config)# username user password pass2 privilege 10
console(config)# privilege exec 4 configure terminal
console(config)# privilege exec 4 show running-config
console(config)# privilege config 10 vlan database
console(config)# privilege config-vlan 10 vlan
```

Теперь для локальных пользователей, чей уровень привилегий выше или равен 4, станет доступен вывод команды **show running-config**, но не будет доступна настройка **vlan**. Для пользователей, уровень привилегий которых соответствует 10 и выше, будет доступна настройка и **vlan**, и вывод команды **show running-config**.

4.5.1.3 Настройка статического IP-адреса, маски подсети и шлюза по умолчанию

Для возможности управления коммутатором из сети необходимо назначить устройству IP-адрес, маску подсети и, в случае управления из другой сети, шлюз по умолчанию. IP-адрес можно назначить любому интерфейсу – VLAN, физическому порту, группе портов (по умолчанию на интерфейсе VLAN 1 назначен IP-адрес 192.168.1.239, маска 255.255.255.0). IP-адрес шлюза должен принадлежать к той же подсети, что и один из IP-интерфейсов устройства.



В случае если IP-адрес настраивается для интерфейса физического порта или группы портов, этот интерфейс удаляется из группы VLAN, которой он принадлежал.



IP-адрес 192.168.1.239 существует до тех пор, пока на любом интерфейсе статически или по DHCP не создан другой IP-адрес.



При удалении всех IP-адресов коммутатора доступ к нему будет осуществляться по IP-адресу 192.168.1.239/24.

- Пример команд настройки IP-адреса для интерфейса VLAN 1.

Параметры интерфейса:

IP-адрес, назначаемый для интерфейса VLAN 1 – 192.168.16.144

Маска подсети – 255.255.255.0

IP-адрес шлюза по умолчанию – 192.168.16.1

```
console# configure
console(config)# interface vlan 1
console(config-if)# ip address 192.168.16.144 /24
console(config-if)# exit
console(config)# ip default-gateway 192.168.16.1
console(config)# exit
console#
```

Для того чтобы убедиться, что адрес был назначен интерфейсу, введите команду:

```
console# show ip interface vlan 1
```

| IP Address | I/F | I/F Status admin/oper | Type | Directed Broadcast | Prec | Redirect | Status |
|-------------------|--------|--------------------------|--------|-----------------------|------|----------|--------|
| 192.168.16.144/24 | vlan 1 | UP/DOWN | Static | disable | No | enable | Valid |

4.5.1.4 Получение IP-адреса от сервера DHCP

Для получения IP-адреса может использоваться протокол DHCP, в случае если в сети присутствует сервер DHCP. IP-адрес от сервера DHCP можно получать через любой интерфейс – VLAN, физический порт, группу портов.



По умолчанию DHCP-клиент включен на интерфейсе VLAN 1.

Пример настройки, предназначенной для получения динамического IP-адреса от DHCP-сервера на интерфейсе vlan 1:

```
console# configure
console(config)# interface vlan 1
console(config-if)# ip address dhcp
console(config-if)# exit
console#
```

Для того чтобы убедиться, что адрес был назначен интерфейсу, введите команду:

```
console# show ip interface vlan 1
```

| IP Address | I/F | I/F Status admin/oper | Type | Directed Broadcast | Prec | Redirect | Status |
|---------------|--------|--------------------------|------|-----------------------|------|----------|--------|
| 10.10.10.3/24 | vlan 1 | UP/UP | DHCP | disable | No | enable | Valid |

4.5.1.5 Настройка параметров протокола SNMP для доступа к устройству

Устройство содержит встроенный агент SNMP и поддерживает версии протокола v1/v2c/v3. Агент SNMP поддерживает набор стандартных переменных MIB.

Для возможности администрирования устройства посредством протокола SNMP необходимо создать хотя бы одну строку сообщества. Коммутаторы поддерживают три типа строк сообщества:

- **ro** – определяет доступ только на чтение;
- **rw** – определяет доступ на чтение и запись;
- **su** – определяет доступ SNMP-администратора;

Наиболее распространено использование строк сообщества *public* – с доступом только для чтения объектов MIB и *private* – с доступом на чтение и изменение объектов MIB. Для каждого сообщества можно задать IP-адрес станции управления.

Пример создания сообщества *private* с доступом на чтение и запись и IP-адресом станции управления 192.168.16.44:

```
console# configure
console(config)# snmp-server server
```

```
console(config)# snmp-server community private rw 192.168.16.44
console(config)# exit
console#
```

Для просмотра созданных строк сообщества и настроек SNMP используется команда:

```
console# show snmp
```

```
SNMP is enabled.

SNMP traps Source IPv4 interface:
SNMP informs Source IPv4 interface:
SNMP traps Source IPv6 interface:
SNMP informs Source IPv6 interface:
```

| Community-String | Community-Access | View name | IP address | Mask |
|------------------|------------------|-----------|--------------|------|
| private | read write | Default | 192.168.16.1 | 44 |

```
Community-String  Group name      IP address      Mask      Version  Type
-----
Traps are enabled.
Authentication-failure trap is enabled.

Version 1,2 notifications
Target Address    Type      Community      Version    Udp      Filter      To      Retries
                  Type
-----
Version 3 notifications
Target Address    Type      Username      Security   Udp      Filter      To      Retries
                  Type      Level         Port      name      Sec
-----
System Contact:
System Location:
```

4.5.2 Настройка параметров системы безопасности

Для обеспечения безопасности системы используется механизм AAA (аутентификация, авторизация, учёт). Для шифрования данных используется механизм SSH.

- *Authentication* (аутентификация) — сопоставление запроса существующей учётной записи в системе безопасности.
- *Authorization* (авторизация, проверка уровня доступа) — сопоставление учётной записи в системе (прошедшей аутентификацию) и определённых полномочий.
- *Accounting* (учёт) — слежение за потреблением ресурсов пользователем.

При использовании настроек устройства по умолчанию имя пользователя – **admin**, пароль – **admin**. Пароль назначается пользователем. В случае если пароль утрачен, можно перезагрузить устройство и через серийный порт прервать загрузку, нажав клавишу **<Esc>** или **<Enter>** в течение первых двух секунд после появления сообщения автозагрузки. Откроется меню **Startup**, в котором нужно запустить процедуру восстановления пароля ([2] Password Recovery Procedure).



Пользователь по умолчанию (admin/admin) существует до тех пор, пока не создан любой другой пользователь с уровнем привилегий 15.



При удалении всех созданных пользователей с 15 уровнем привилегий доступ к коммутатору будет осуществляться под пользователем по умолчанию (admin/admin).

Для обеспечения первоначальной безопасности пароль в системе можно задать для сервисов:

- Консоль (подключение через серийный порт);
- Telnet;
- SSH.

4.5.2.1 Установка пароля для консоли

```
console(config)# aaa authentication login default line
console(config)# aaa authentication enable default line
console(config)# line console
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password console
```

В ответ на приглашение ввести пароль во время регистрации в устройстве через сеанс консоли введите пароль – **console**.

4.5.2.2 Установка пароля для Telnet

```
console(config)# aaa authentication login default line
console(config)# aaa authentication enable default line
console(config)# ip telnet server
console(config)# line telnet
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password telnet
```

В ответ на приглашение ввести пароль во время регистрации в устройстве через сеанс Telnet введите пароль – **telnet**.

4.5.2.3 Установка пароля для SSH

```
console(config)# aaa authentication login default line
console(config)# aaa authentication enable default line
console(config)# ip ssh server
console(config)# line ssh
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password ssh
```

В ответ на приглашение ввести пароль во время регистрации в устройстве через сеанс SSH введите пароль – **ssh**.

4.5.3 Настройка баннера

Для удобства эксплуатации устройства можно задать баннер – сообщение, содержащее любую информацию. Например:

```
console(config)# banner exec;
```

```
Role: Core switch
Location: Objedineniya 9, str.
```

5 УПРАВЛЕНИЕ УСТРОЙСТВОМ. ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ

Для конфигурации настроек коммутатора используется несколько режимов. В каждом режиме доступен определенный список команд. Ввод символа «?» служит для просмотра набора команд, доступных в каждом из режимов.

Для перехода из одного режима в другой используются специальные команды. Перечень существующих режимов и команд входа в режим:

Командный режим (EXEC), данный режим доступен сразу после успешной загрузки коммутатора и ввода имени пользователя и пароля (для непривилегированного пользователя). Приглашение системы в этом режиме состоит из имени устройства (host name) и символа “>”.

```
console>
```

Привилегированный командный режим (Privileged EXEC), данный режим доступен сразу после успешной загрузки коммутатора, ввода имени пользователя и пароля. Приглашение системы в этом режиме состоит из имени устройства (host name) и символа “#”.

```
console#
```

Режим глобальной конфигурации (global configuration), данный режим предназначен для задания общих настроек коммутатора. Команды режима глобальной конфигурации доступны из любого подрежима конфигурации. Вход в режим осуществляется командой **configure**.

```
console# configure
console(config)#
```

Режим конфигурации терминала (line configuration), данный режим предназначен для конфигурации, связанной с работой терминала. Вход в режим осуществляется из режима глобальной конфигурации.

```
console(config)# line {console | telnet | ssh}
console(config-line)#
```

5.1 Базовые команды

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 30 – Базовые команды, доступные в режиме EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|----------------------|--------------------------------|--|
| enable [priv] | priv: (1..15)/15 | Переключиться в привилегированный режим (если значение не указано – то уровень привилегий 15). |
| login | - | Завершение текущей сессии и смена пользователя. |
| exit | - | Закрывает активную терминальную сессию. |
| help | - | Запрос справочной информации о работе интерфейса командной строки. |
| show history | - | Показать историю команд, введенных в текущей терминальной сессии. |

| | | |
|-----------------------------------|---|---|
| show privilege | - | Показать уровень привилегий текущего пользователя. |
| terminal history | -/функция включена | Включить функцию сохранения истории введенных команд для текущей терминальной сессии. |
| terminal no history | | Отключить функцию сохранения истории введенных команд для текущей терминальной сессии. |
| terminal history size size | size: (10..207)/10 | Изменить размер буфера истории введенных команд для текущей терминальной сессии. |
| terminal no history size | | Установить значение по умолчанию. |
| terminal datadump | -/вывод команд разделяется по страницам | Отобразить вывод команд без разделения на страницы (разделение вывода справки по страницам осуществляется строкой: More: <space>, Quit: q or CTRL+Z, One line: <return>). |
| terminal no datadump | | Установить значение по умолчанию. |
| terminal prompt | -/функция включена | Включить подтверждение перед выполнением некоторых команд. |
| terminal no prompt | | Отключить подтверждение перед выполнением некоторых команд. |
| show banner [login exec] | - | Отображает конфигурацию баннеров. |

Команды режима Privileged EXEC

Запрос командной строки имеет следующий вид:

```
console#
```

Таблица 31 – Базовые команды, доступные в режиме Privileged EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|----------------------------|---------------------------------------|---|
| disable [priv] | priv: (1, 7, 15)/1 | Вернуться в командный режим (EXEC) из привилегированного командного режима (Privileged EXEC). |
| configure[terminal] | - | Перейти в режим конфигурации. |
| debug-mode | - | Перейти в режим отладки. |

Команды, доступные во всех режимах конфигурации

Запрос командной строки имеет один из следующих видов:

```
console#
console(config)#
console(config-line)#
```

Таблица 32 – Базовые команды, доступные во всех режимах конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|----------------|---------------------------------------|--|
| exit | - | Выйти из любого режима конфигурации на уровень выше в иерархии команд CLI. |
| end | - | Выйти из любого режима конфигурации в командный режим (Privileged EXEC). |
| do | - | Выполнить команду командного уровня (EXEC) из любого режима конфигурации. |
| help | - | Выводит справку по используемым командам. |

Команды режима глобальной конфигурации

Запрос командной строки имеет следующий вид:

```
console (config) #
```

Таблица 33 – Базовые команды, доступные в режиме конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--------------------------------------|---------------------------------------|---|
| banner exec d message_text d | - | Задать текст сообщения exec (пример: пользователь успешно вошел в систему) и включить вывод на экран. - <i>d</i> – разделитель; - <i>message_text</i> – текст сообщения (в строке до 510 символов, общее 2000 символов). |
| no banner exec | | Удалить текст сообщения exec. |
| banner login d message_text d | - | Задать текст сообщения login (информационное сообщение, которое отображается перед вводом имени пользователя и пароля), и включить вывод на экран. - <i>d</i> – разделитель; - <i>message_text</i> – текст сообщения (в строке до 510 символов, общее 2000 символов). |
| no banner login | | Удалить текст сообщения login. |

Команды режима конфигурации терминала

Запрос командной строки в режиме конфигурации терминала имеет следующий вид:

```
console (config-line) #
```

Таблица 34 – Базовые команды, доступные в режиме конфигурации терминала

| Команда | Значение/Значение по умолчанию | Действие |
|-----------------------------|---------------------------------------|--|
| history | -/функция включена | Включить функцию сохранения истории введенных команд. |
| no history | | Выключить функцию сохранения истории введенных команд. |
| history size size | size: (10..207)/10 | Изменить размер буфера истории введенных команд. |
| no history size | | Установить значение по умолчанию. |
| exec-timeout timeout | timeout: (0..65535)/10 минут | Задать тайм-аут текущей терминальной сессии в минутах. |
| no exec-timeout | | Установить значение по умолчанию. |

5.2 Фильтрация сообщений командной строки

Фильтрация сообщений позволяет уменьшить объем отображаемых данных в ответ на запросы пользователя и облегчить поиск необходимой информации. Для фильтрации информации требуется добавить в конец командной строки символ «|» и использовать одну из опций фильтрации, перечисленных в таблице.

Таблица 35 – Команды режима глобальной конфигурации

| Метод | Значение/Значение по умолчанию | Действие |
|------------------------|---------------------------------------|--|
| begin pattern | - | Ищет первое совпадение с шаблоном в начале строки и выводит все строки за ней. |
| include pattern | | Выводит все строки, содержащие шаблон. |
| exclude pattern | | Выводит все строки, не содержащие шаблон. |

5.3 Настройка макрокоманд

Данная функция позволяет создавать унифицированные наборы команд – макросы, которые можно впоследствии применять в процессе конфигурации.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 36 – Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---------------------------------------|--|
| macro name <i>word</i> | word: (1..32) символов | Создает новый набор команд, если набор с таким именем существует – перезаписывает его. Набор команд вводится построчно. Закончить макрос можно с помощью символа "@". Максимальная длина макроса – 510 символов. |
| no macro name <i>word</i> | | Удаляет указанный макрос. |
| macro global apply <i>word</i> | word: (1..32) символов | Применяет указанный макрос. |
| macro global trace <i>word</i> | word: (1..32) символов | Проверяет указанный макрос на валидность. |
| macro global description <i>word</i> | word: (1..160) символов | Создает строку-дескриптор глобального макроса. |
| no macro global description | | Удаляет строку-дескриптор. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 37 – Команды режима EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|--|--|
| macro apply <i>word</i> | word: (1..32) символов | Применяет указанный макрос. |
| macro trace <i>word</i> | | Проверяет указанный макрос на валидность. |
| show parser macro [{brief description [interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> }] name <i>word</i> }] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128); word: (1..32) символов | Отображает параметры настроенных макросов на устройстве. |

Команды режима конфигурации интерфейса

Вид запроса командной строки режима конфигурации интерфейса:

```
console (config-if) #
```

Таблица 38 – Команды режима конфигурации интерфейса

| Команда | Значение/Значение по умолчанию | Действие |
|-------------------------------|---------------------------------------|---|
| macro apply word | word: (1..32) символов | Применяет указанный макрос. |
| macro trace word | word: (1..32) символов | Проверяет указанный макрос на валидность. |
| macro description word | word: (1..160) символов | Устанавливает строку-дескриптор макроса. |
| no macro description | | Удаляет строку-дескриптор. |


5.4 Команды управления системой



Команды режима EXEC


Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 39 – Команды управления системой в режиме EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|--|--|--|
| ping [ip] {A.B.C.D host} [vrf vrf_name] [size size] [count count] [timeout timeout] [source A.B.C.D] | vrf_name: (1..32) символа; host: (1..158) символов; size: (64..1518)/64 байт; count: (0..65535)/4; timeout: (50..65535)/2000 мс | Команда служит для передачи запросов (ICMP Echo-Request) протокола ICMP указанному узлу сети, а также для контроля поступающих ответов (ICMP Echo-Reply). - <i>vrf_name</i> – имя виртуальной области маршрутизации; - <i>A.B.C.D</i> – IPv4-адрес узла сети; - <i>host</i> – доменное имя узла сети; - <i>size</i> – размер пакета для отправки, количество байт в пакете; - <i>count</i> – количество пакетов для передачи; - <i>timeout</i> – время ожидания ответа на запрос. |
| ping ipv6 {A.B.C.D.E.F host} [size size] [count count] [timeout timeout] [source A.B.C.D.E.F] | host: (1..158) символов; size: (68..1518)/68 байт; count: (0..65535)/4; timeout: (50..65535)/2000 мс | Команда служит для передачи запросов (ICMP Echo-Request) протокола ICMP указанному узлу сети, а также для контроля поступающих ответов (ICMP Echo-Reply). - <i>A.B.C.D.E.F</i> – IPv6-адрес узла сети; - <i>host</i> – доменное имя узла сети; - <i>size</i> – размер пакета для отправки, количество байт в пакете; - <i>count</i> – количество пакетов для передачи; - <i>timeout</i> – время ожидания ответа на запрос. |
| traceroute ip {A.B.C.D host} [vrf vrf_name] [size size] [ttl ttl] [count count] [timeout timeout] [source ip_address] | vrf_name: (1..32) символа; host: (1..158) символов; size: (64..1518)/64 байт; ttl: (1..255)/30; count: (1..10)/3; timeout: (1..60)/3 с; | Определение маршрута трафика до узла назначения. - <i>vrf_name</i> – имя виртуальной области маршрутизации; - <i>A.B.C.D</i> – IPv4-адрес узла сети. - <i>host</i> – доменное имя узла сети; - <i>size</i> – размер пакета для отправки, количество байт в пакете; - <i>ttl</i> – максимальное количество участков в маршруте; - <i>count</i> – количество попыток передачи пакета на каждом участке; - <i>timeout</i> – время ожидания ответа на запрос; - <i>IP_address</i> – IP-адрес интерфейса коммутатора, используемый для передачи пакетов;  Описание ошибок при выполнении команд и результатов приведено в таблицах 41, 42. |

| | | |
|--|---|---|
| traceroute ipv6 {A.B.C.D.E.F host} [size size] [ttl ttl] [count count] [timeout timeout] [source ip_address] | host: (1..158) символов; size: (66..1518)/66 Байт; ttl: (1..255)/30; count: (1..10)/3; timeout: (1..60) /3 с; | Определение маршрута трафика до узла назначения. - A.B.C.D.E.F – IPv6-адрес узла сети. - host – доменное имя узла сети; - size – размер пакета для отправки, количество байт в пакете; - ttl – максимальное количество участков в маршруте; - count – количество попыток передачи пакета на каждом участке; - timeout – время ожидания ответа на запрос; - IP_address – IP-адрес интерфейса коммутатора, используемый для передачи пакетов.  Описание ошибок при выполнении команд и результатов приведено в таблицах 41, 42. |
| telnet {A.B.C.D host} [port] [keyword1...] | host: (1..158) символов; port: (1..65535)/23 | Открытие TELNET-сессии для узла сети. - A.B.C.D – IPv4-адрес узла сети; - host – доменное имя узла сети; - port – TCP-порт, по которому работает служба Telnet; - keyword – ключевое слово.  Описание специальных команд Telnet и ключевых слов приведено в таблицах 43, 44. |
| ssh {A.B.C.D host} [port] [keyword1...] | host: (1..158) символов; port: (1..65535)/22; | Открытие SSH-сессии для узла сети. - A.B.C.D – IPv4-адрес узла сети; - host – доменное имя узла сети; - port – TCP-порт, по которому работает служба SSH; - keyword – ключевое слово.  Описание ключевых слов приведено в таблице 44. |
| resume [connection] | connection: (1..5)/последняя установленная сессия | Переключение на другую установленную Telnet-сессию. - connection – номер установленной telnet-сессии. |
| show users [accounts] | - | Отображение информации о пользователях, использующих ресурсы устройства. |
| show sessions | - | Отображение информации об открытых сессиях к удаленным устройствам. |
| show system | - | Вывод системной информации. |
| show system id [unit unit] | unit: (1..8)/- | Отображение серийного номера устройства. - unit – номер устройства в стеке. |
| show system [unit unit] | unit: (1..8)/- | Отображение системной информации коммутатора. - unit – номер устройства в стеке. |
| show system fans [unit unit] | unit: (1..8)/- | Отображение информации о состоянии вентиляторов. - unit – номер устройства в стеке. |
| show system power-supply | - | Отображение информации о состоянии источников питания. |
| show system sensors | - | Отображение информации температурных датчиков. |
| show version | - | Отображение текущей версии системного программного обеспечения устройства. |
| show hardware version | - | Отображает информацию об аппаратной версии платы |
| show system router resources | - | Отображение размера и занятости аппаратных таблиц устройства (маршрутизации, соседей, интерфейсов). |
| show system tcam utilization [unit unit] | unit: (1..8)/- | Отображение загрузки ресурсов памяти TCAM (определенно адресуемая память). - unit – номер устройства в стеке. |
| show tasks utilization | - | Отображение уровня загрузки ресурсов центрального процессора коммутатора для каждого системного процесса. |

| | | |
|--|--------------------------------------|---|
| show tech-support [config memory] | <p style="text-align: center;">-</p> | <p>Отображение информации об устройстве, необходимой для начальной диагностики проблем.</p> <p> Вывод команды представляет собой комбинацию выводов перечисленных ниже команд:</p> <ul style="list-style-type: none"> • show clock • show system • show version • show bootvar • show running-config • show ip interface • show ipv6 interface • show spanning-tree active • show stack • show stack configuration • show stack links details • show interfaces status • show interfaces counters • show interfaces utilization • show interfaces te1/0/xx • show fiber-ports optical-transceiver • show interfaces channel-group • show cpu utilization • show cpu input-rate detailed • show tasks utilization • show mac address-table count • show arp • show errdisable interfaces • show vlan • show ip igmp snooping groups • show ip igmp snooping mrouter • show ipv6 mld snooping groups • show ipv6 mld snooping mrouter • show logging file • show logging • show users • show sessions • show system router resource • show system tcam utilization |
| show system forwarding resources | <p style="text-align: center;">-</p> | <p>Отобразить текущий, устанавливаемый после перезагрузки и доступные для использования режимы распределения аппаратных ресурсов.</p> |



Команда «show sessions» отображает все удаленные соединения только из текущей сессии. Данная команда используется следующим образом:

1. Выполнить подключение к удалённому устройству с коммутатора с помощью Telnet или SSH;
2. Вернуться в родительскую сессию (на коммутатор). Для этого нажать комбинацию клавиш <Ctrl+Shift+6>, отпустить и нажать <x> (икс). Произойдёт переход в родительскую сессию;
3. Выполнить команду «show sessions». В таблице должны присутствовать все исходящие соединения в текущей сессии;
4. Для того чтобы вернуться к сессии удалённого устройства, необходимо выполнить команду «resume N», где N – номер соединения из вывода команды «show sessions».

Запрос командной строки в режиме Privileged EXEC имеет следующий вид:

```
console#
```

Таблица 40 – Команды управления системой в режиме Privileged EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|---|
| reload [unit <i>unit_id</i>] | unit_id: (1..8)/- | Команда служит для перезапуска устройства. - <i>unit_id</i> – номер устройства в стеке. |
| reload in { <i>minutes</i> <i>hh:mm</i> } | minutes: (1..999); hh: (0..23), mm: (0..59). | Установка промежутка времени, через который произойдет отложенная перезагрузка устройства. |
| reload at <i>hh:mm</i> | hh: (0..23), mm: (0..59). | Установка времени перезагрузки устройства. |
| reload cancel | - | Отмена отложенного перезапуска. |
| boot password <i>password</i> | - | Установка пароля на bootrom. |
| no boot password | - | Удаление пароля на bootrom. |
| show cpu utilization | - | Отображение статистики по уровню загрузки ресурсов центрального процессора. |
| show cpu input rate | - | Отображение статистики по скорости входящих кадров, обрабатываемых процессором. |
| show cpu input-rate detailed | - | Отображение статистики по скорости входящих кадров, обрабатываемых процессором по типу трафика. |
| show cpu thresholds | - | Отображение списка настроенных порогов для CPU. |
| show memory thresholds | - | Отображение списка настроенных порогов для RAM. |
| show sensor thresholds | - | Отображение списка порогов для датчиков. |
| show storage thresholds | - | Отображение списка порогов для разделов устройств. |
| show storage devices | - | Отображение значений объема и свободной памяти ПЗУ. |

- Пример использования команды **traceroute**:

```
console# traceroute ip eltex.com
```

```
Tracing the route to eltex.com (148.21.11.69) form , 30 hops max, 18 byte packets
Type Esc to abort.
 1 gateway.eltex (192.168.1.101)  0 msec 0 msec 0 msec
 2 eltexsrv (192.168.0.1) 0 msec 0 msec 0 msec
 3 * * *
```

Таблица 41 – Описание результатов выполнения команды **traceroute**

| Поле | Описание |
|----------------------|---|
| 1 | Порядковый номер маршрутизатора в пути к указанному узлу сети. |
| gateway.eltex | Сетевое имя этого маршрутизатора. |
| 192.168.1.101 | IP-адрес этого маршрутизатора. |
| 0 msec 0 msec 0 msec | Время, за которое пакет был передан и вернулся от маршрутизатора. Указывается для каждой попытки передачи пакета. |

При выполнении команды **traceroute** могут произойти ошибки, описание ошибок приведено в таблице 42.

Таблица 42 – Ошибки при выполнении команды **traceroute**

| Символ ошибки | Описание |
|---------------|---------------------------------------|
| * | Тайм-аут при попытке передачи пакета. |

| | |
|---|--|
| ? | Неизвестный тип пакета. |
| A | Административно недоступен. Обычно происходит при блокировании исходящего трафика по правилам в таблице доступа ACL. |
| F | Требуется фрагментация и установка битов DF. |
| H | Узел сети недоступен. |
| N | Сеть недоступна. |
| P | Протокол недоступен. |
| Q | Источник подавлен. |
| R | Истекло время повторной сборки фрагмента. |
| S | Ошибка исходящего маршрута. |
| U | Порт недоступен. |

Программное обеспечение Telnet коммутаторов поддерживает специальные команды – функции контроля терминала. Для входа в режим специальных команд во время активной Telnet-сессии используется комбинация клавиш **<Ctrl+shift+6>**.

Таблица 43 – Специальные команды Telnet

| Специальная команда | Назначение |
|----------------------------|---|
| ^^ b | Передать по telnet разрыв соединения. |
| ^^ c | Передать по telnet прерывание процесса (IP). |
| ^^ h | Передать по telnet удаление символа (EC). |
| ^^ o | Передать по telnet прекращение вывода (AO). |
| ^^ t | Передать по telnet сообщение «Are You There?» (AYT) для контроля подключения. |
| ^^ u | Передать по telnet стирание строки (EL). |
| ^^ x | Возврат в режим командной строки. |

Также возможно использование дополнительных опций при открытии Telnet- и SSH-сессий:

Таблица 44 – Ключевые слова, используемые при открытии Telnet- и SSH-сессий


| Опция | Описание |
|-------------------|--|
| /echo | Локально включает функцию <i>echo</i> (подавление вывода на консоль). |
| /password | Определяет пароль для входа на SSH-сервер. |
| /quiet | Не допускает вывод всех сообщений программного обеспечения Telnet. |
| /source-interface | Определяет интерфейс-источник. |
| /stream | Включает обработку потока, который разрешает незащищенное TCP-соединение без контроля последовательностей Telnet. Поточное соединение не обрабатывает Telnet-опции и может использоваться для подключения к портам, на которых запущены программы копирования UNIX-to-UNIX (UUCP) либо другие протоколы, не являющиеся Telnet-протоколами. |
| /user | Определяет имя пользователя для входа на SSH-сервер. |

Команды режима глобальной конфигурации



Запрос командной строки в режиме глобальной конфигурации имеет следующий вид:

```
console (config) #
```

Таблица 45 – Команды управления системой в режиме глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--|--|---|
| <code>hostname name</code> | name: (1..160) | Команда служит для задания сетевого имени устройства. |
| <code>no hostname</code> | символов/- | Вернуть сетевое имя устройства в значение по умолчанию. |
| <code>service tasks-utilization</code> | -/включено | Разрешить устройству программно измерять уровень загрузки ресурсов центрального процессора коммутатора для каждого системного процесса. |
| <code>no service tasks-utilization</code> | | Запретить устройству программно измерять уровень загрузки ресурсов центрального процессора коммутатора для каждого системного процесса. |
| <code>service cpu-utilization</code> | -/включено | Разрешить устройству программно измерять уровень загрузки ресурсов центрального процессора коммутатора. |
| <code>no service cpu-utilization</code> | | Запретить устройству программно измерять уровень загрузки ресурсов центрального процессора коммутатора. |
| <code>service cpu-input-rate</code> | -/включено | Разрешить устройству программно измерять скорость входящих кадров, обрабатываемых центральным процессором коммутатора. |
| <code>no service cpu-input-rate</code> | | Запретить устройству программно измерять скорость входящих кадров, обрабатываемых центральным процессором коммутатора. |
| <code>service cpu-rate-limits traffic pps</code> | traffic: (http, telnet, ssh, snmp, ip, link-local, arp, arp-inspection, stp-bpdu, routing, ip-options, other-bpdu, dhcp-snooping, igmp-snooping, mld-snooping, sflow, ace, ip-error, other, vrrp, multicast-routing, multicast-rpf-fail, tcp-syn); pps: 8..2048 | Установка на CPU ограничения скорости входящих кадров для определенного типа трафика. - pps — пакетов в секунду.  Реализует функцию CoPP (Control plane protection). |
| <code>no service cpu-rate-limits traffic</code> | | Восстанавливает значение pps по умолчанию для определенного трафика. |
| <code>service password-recovery</code> | -/enabled | Разрешить восстановление пароля через загрузочное меню «password recovery procedure» с сохранением конфигурации. |
| <code>no service password-recovery</code> | | Разрешить восстановление пароля через загрузочное меню «password recovery procedure» с удалением конфигурации. |
| <code>link-flap prevention enable</code> | -/enabled | Включить предотвращение флаппинга линка. |
| <code>link-flap prevention disable</code> | | Отключить предотвращение флаппинга линка. |
| <code>service mirror-configuration</code> | -/enabled | Создавать резервную копию текущей конфигурации. |
| <code>no service mirror-configuration</code> | | Отключить копирование текущей конфигурации. |
| <code>cpu threshold index index interval relation value [flap-interval flap_interval] [severity level] [notify {enable disable}] [recovery-notify {enable disable}]</code> | index: (0..4294967295); interval: (5sec, 1min, 5min); relation: (greater-than, greater-or-equal, less-than, less-or-equal, equal-to, not-equal-to); value: (0..100) процентов; flap_interval: (0..100)/0 процентов; severity: (emerg, alert, crit, err, warning, notice, info, debug)/alert | Задать порог для загрузки CPU. - index — произвольный индекс порога; - interval — интервал измерения загрузки CPU. Значение загрузки CPU за этот интервал будет сравниваться с пороговым; - relation — отношение между загрузкой CPU и пороговым значением, необходимое для срабатывания порога; - value — значение порога; - flap_interval — значение, определяющее момент восстановления порога после срабатывания; - severity — уровень важности трапов для этого порога; - notify — включает/отключает отправку трапов о срабатывании порога; - recovery-notify — включает/отключает отправку трапов о восстановлении порога. |
| <code>no cpu threshold index index</code> | | Удалить порог с заданным индексом. |

| | | |
|--|---|---|
| memory threshold index <i>index relation value</i> [flap-interval <i>flap_interval</i>] [severity level] [notify {enable disable}] [recovery-notify {enable disable}] | index: (0..4294967295); relation: (greater-than, greater-or-equal, less-than, less-or-equal, equal-to, not-equal-to); value: (0..100) процентов; flap_interval: (0..100)/0 процентов; severity: (emerg, alert, crit, err, warning, notice, info, debug)/alert | Задать порог для объема свободной памяти RAM. - <i>index</i> — произвольный индекс порога; - <i>relation</i> — отношение между объемом свободной памяти и пороговым значением, необходимое для срабатывания порога; - <i>value</i> — значение порога; - <i>flap_interval</i> — значение, определяющее момент восстановления порога после срабатывания; - <i>severity</i> — уровень важности трапов для этого порога; - notify — включает/отключает отправку трапов о срабатывании порога; - recovery-notify — включает/отключает отправку трапов о восстановлении порога. |
| no memory threshold index <i>index</i> | | Удалить порог с заданным индексом. |
| sensor threshold fan <i>fan_num unit-id unit_id index relation value</i> [flap-interval <i>flap_interval</i>] [severity level] [notify {enable disable}] [recovery-notify {enable disable}] | fan_num: (1..63); unit_id: (1..8); index: (0..4294967295); relation: (greater-than, greater-or-equal, less-than, less-or-equal, equal-to, not-equal-to); value: (0..100000000) оборотов/мин; flap_interval: (0..1000000000)/0 оборотов/мин; severity: (emerg, alert, crit, err, warning, notice, info, debug)/alert | Задать порог для датчика скорости вращения вентилятора. - <i>fan_num</i> — номер вентилятора; - <i>unit_id</i> — номер юнита, на котором находится вентилятор; - <i>index</i> — произвольный индекс порога; - <i>relation</i> — отношение между скоростью вращения вентилятора и пороговым значением, необходимое для срабатывания порога; - <i>value</i> — значение порога; - <i>flap_interval</i> — значение, определяющее момент восстановления порога после срабатывания; - <i>severity</i> — уровень важности трапов для этого порога; - notify — включает/отключает отправку трапов о срабатывании порога; - recovery-notify — включает/отключает отправку трапов о восстановлении порога. |
| no sensor threshold fan <i>fan_num unit-id unit_id index</i> | | Удалить порог с заданным индексом для вентилятора <i>fan_num</i> на юните <i>unit_id</i> . |
| sensor threshold thermal-sensor <i>sensor_num unit-id unit_id index relation value</i> [flap-interval <i>flap_interval</i>] [severity level] [notify {enable disable}] [recovery-notify {enable disable}] | sensor_num: (1..63); unit_id: (1..8); index: (0..4294967295); relation: (greater-than, greater-or-equal, less-than, less-or-equal, equal-to, not-equal-to); value: (-1000000000..1000000000) °C; flap_interval: (0..1000000000)/0 °C; severity: (emerg, alert, crit, err, warning, notice, info, debug)/alert | Задать порог для датчика температуры. - <i>sensor_num</i> — номер термодатчика; - <i>unit_id</i> — номер юнита, на котором находится термодатчик; - <i>index</i> — произвольный индекс порога; - <i>relation</i> — отношение между температурой и пороговым значением, необходимое для срабатывания порога; - <i>value</i> — значение порога; - <i>flap_interval</i> — значение, определяющее момент восстановления порога после срабатывания; - <i>severity</i> — уровень важности трапов для этого порога; - notify — включает/отключает отправку трапов о срабатывании порога; - recovery-notify — включает/отключает отправку трапов о восстановлении порога. |
| no sensor threshold thermal-sensor <i>sensor_num unit-id unit_id index</i> | | Удалить порог с заданным индексом для термодатчика <i>sensor_num</i> на юните <i>unit_id</i> . |
| storage threshold index <i>interval relation value</i> [flap-interval <i>flap_interval</i>] [severity level] [notify {enable disable}] [recovery-notify {enable disable}] | index: (0..4294967295); relation: (greater-than, greater-or-equal, less-than, less-or-equal, equal-to, not-equal-to); value: (0..100) процентов; interval: (0..100)/0 процентов; severity: (emerg, alert, crit, err, warning, notice, info, debug)/alert; | Задать порог для объема свободной памяти на ПЗУ. - <i>index</i> — произвольный индекс порога; - <i>relation</i> — отношение между объемом свободной памяти и пороговым значением, необходимое для срабатывания порога; - <i>value</i> — значение порога; - <i>flap_interval</i> — значение, определяющее момент восстановления порога после срабатывания; - <i>severity</i> — уровень важности трапов для этого порога; - notify — включает/отключает отправку трапов о срабатывании порога; - recovery-notify — включает/отключает отправку трапов о восстановлении порога. |
| no storage threshold index <i>index</i> | | Удалить порог с заданным индексом. |

| | | |
|---|--|---|
| <code>reset-button {enable disable reset-only}</code> | <code>-/enable</code> | Настройка реакции коммутатора на нажатие кнопки F. - enable – при нажатии на кнопку длительностью менее 10 сек, происходит перезагрузка устройства; при нажатии на кнопку длительностью более 10 сек, происходит сброс устройства до заводской конфигурации; - disable – не реагировать (отключена); - reset-only – только перезагрузка. |
| <code>system forwarding resources mode {mid-I3-mid-I2 min-I3-max-I2}</code> | mode: mid-I3-mid-I2, min-I3-max-I2/ mid-I3-mid-I2 | Установить режим распределения аппаратных ресурсов mid-I3-mid-I2: - объем таблицы MAC до 128K адресов; - объем таблицы FIB до 288K маршрутов; - объем таблицы ARP до 64K записей. min-I3-max-I2: - объем таблицы MAC до 256K адресов; - объем таблицы FIB до 16K маршрутов; - объем таблицы ARP до 96K записей.  Команда поддерживается только на MES5410-48 и MES5500-32.  Настройка вступит в силу только после перезагрузки устройства. |
| <code>no system forwarding resources</code> | - | Установить режим распределения аппаратных ресурсов по умолчанию. |

5.5 Команды для настройки параметров для задания паролей

Данный комплекс команд предназначен для задания минимальной сложности пароля, а также для задания времени действия пароля.

Команды режима глобальной конфигурации

Запрос командной строки в режиме глобальной конфигурации имеет следующий вид:

```
console (config) #
```

Таблица 46 – Команды управления системой в режиме глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---------------------------------------|--|
| <code>passwords aging age</code> | age: (0..365)/180 дней | Задаёт время жизни паролей. По истечении заданного срока будет предложено сменить пароль. Значение 0 говорит о том, что время жизни паролей не задано. |
| <code>no passwords aging</code> | | Восстанавливает значение по умолчанию. |
| <code>passwords complexity enable</code> | -/выключено | Включает ограничение на формат пароля. |
| <code>no passwords complexity enable</code> | | Выключает ограничение на формат пароля. |
| <code>passwords complexity min-classes value</code> | value: (0..4)/3 | Включает ограничение, задающее минимальное количество классов символов (строчные буквы, заглавные буквы, цифры, символы). |
| <code>no passwords complexity min-classes</code> | | Восстанавливает значение по умолчанию. |
| <code>passwords complexity min-length value</code> | value: (0..64)/8 | Включает ограничение на минимальную длину пароля. |
| <code>no passwords complexity min-length</code> | | Восстанавливает значение по умолчанию. |
| <code>passwords complexity no-repeat number</code> | number: (0..16)/3 | Включает ограничение, задающее максимальное количество последовательно повторяющихся символов в новом пароле. |
| <code>no passwords complexity no-repeat</code> | | Восстанавливает значение по умолчанию. |

| | | |
|---|----------------------------|---|
| passwords complexity not-current | -/enabled | Запрещает при смене пароля использовать в качестве нового старый. |
| no passwords complexity not-current | | Разрешает использовать старый пароль при смене. |
| passwords complexity not-username | -/enabled | Запрещает использовать в качестве пароля имя пользователя. |
| no passwords complexity not-username | | Разрешает использовать в качестве пароля имя пользователя. |
| passwords lockout value | value: (1..5)/выключено | Задаёт ограничение на количество неверных попыток входа на коммутатор. После последней неправильной попытки ввести пароль пользователь блокируется. |
| no passwords lockout | | Выключает ограничение на количество неверных попыток входа. |

Таблица 47 – Команды управления системой в режиме Privileged EXEC


| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|-------------------------------------|---------------------------------------|--|
| show passwords configuration | - | Отображает информацию об ограничениях на пароли. |
| set username name active | name: (1..20) символов | Разблокирует пользователя, заблокированного после неудачных попыток входа на коммутатор. |

5.6 Работа с файлами

5.6.1 Описание аргументов команд

При осуществлении операций над файлами, в качестве аргументов команд выступают адреса URL – определители местонахождения ресурса. Описание ключевых слов, используемых в операциях, приведено в таблице 48.

Таблица 48 – Список ключевых слов и их описание


| <i>Ключевое слово</i> | <i>Описание</i> |
|-----------------------|--|
| flash:// | Исходный адрес или адрес места назначения для энергонезависимой памяти. Энергонезависимая память используется по умолчанию, если адрес URL определен без префикса (префиксами являются: flash:, tftp:, scp:...). |
| running-config | Файл текущей конфигурации. |
| mirror-config | Копия файла текущей конфигурации. |
| startup-config | Файл первоначальной конфигурации. |
| active-image | Файл с активным образом. |
| inactive-image | Файл с неактивным образом. |
| tftp:// | Исходный адрес или адрес места назначения для TFTP-сервера. Синтаксис: tftp://host/[directory/] filename vrf name . - <i>host</i> – IPv4-адрес или сетевое имя устройства; - <i>directory</i> – каталог; - <i>filename</i> – имя файла; - <i>name</i> – название vrf.  Если vrf не используется, команду vrf name можно не указывать. |
| scp:// | Исходный адрес или адрес места назначения для SSH-сервера. Синтаксис: scp://[username[:password]@]host/[directory/] filename - <i>username</i> – имя пользователя; - <i>password</i> – пароль пользователя; - <i>host</i> – IPv4-адрес или сетевое имя устройства; - <i>directory</i> – каталог; - <i>filename</i> – имя файла. |
| logging | Файл с историей команд. |

5.6.2 Команды для работы с файлами

Запрос командной строки в режиме Privileged EXEC имеет следующий вид:

```
console#
```

Таблица 49 – Команды для работы с файлами в режиме Privileged EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|---|---|---|
| <code>copy source_url destination_url</code> | source_url: (1..160) символов; destination_url: (1..160) символов; | Копирование файла из местоположения источника в местоположение назначения. - <i>source_url</i> – местоположение копируемого файла; - <i>destination_url</i> – адрес места назначения, куда файл будет скопирован. |
| <code>copy source_url running-config</code> | | Копирование файла конфигурации с сервера в текущую конфигурацию. |
| <code>copy running-config destination_url</code> | | Сохранение текущей конфигурации на сервере. |
| <code>copy startup-config destination_url</code> | | Сохранение первоначальной конфигурации на сервере. |
| <code>copy running-config startup-config</code> | - | Сохранение текущей конфигурации в первоначальную конфигурацию. |
| <code>copy running-config file</code> | - | Сохранение текущей конфигурации в заданный резервный файл конфигурации. |
| <code>copy startup-config file</code> | - | Сохранение первоначальной конфигурации в заданный резервный файл конфигурации. |
| <code>boot config source_url</code> | - | Копирование файла конфигурации с сервера в файл первоначальной конфигурации. |
| <code>dir [flash:path dir_name]</code> | - | Отображает список файлов в указанном каталоге. |
| <code>more {flash:file startup-config running-config mirror-config active-image inactive-image logging file}</code> | file: (1..160) символов | Отображает содержимое файла. - startup-config – отображает содержимое файла первоначальной конфигурации; - running-config – отображает содержимое файла текущей конфигурации; - flash: – отображает файлы с флеш-памяти устройства; - mirror-config – отображает содержимое файла текущей конфигурации с зеркала; - active-image – отображает версию текущего файла образа ПО. - inactive-image – отображает версию неактивного файла образа ПО. - logging – отображает содержимое файла журнала. - <i>file</i> – имя файла.  Файлы отображаются в формате ASCII. |
| <code>delete url</code> | - | Удаление файла. |
| <code>delete startup-config</code> | - | Удаления файла первоначальной конфигурации. |
| <code>boot system source_url</code> | - | Копирование файла ПО с сервера в неактивную область памяти на место резервного ПО. |
| <code>boot system inactive-image</code> | - | Загрузиться с неактивного образа ПО. |

| | | |
|--|--|--|
| show {startup-config running-config} [brief detailed interfaces {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> oob port-channel group vlan <i>vlan_id</i> tunnel <i>tunnel_id</i> loopback <i>loopback_id</i> }] | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); group: (1..128); <i>vlan_id</i> : (1..4094); <i>tunnel_id</i> : (1..16); <i>loopback_id</i> : (1..64) | Отображает содержимое файла первоначальной конфигурации (startup-config) или текущей конфигурации (running-config). - interfaces – конфигурация интерфейсов коммутатора - физических интерфейсов, групп интерфейсов (port-channel), VLAN-интерфейсов, oob-порта, интерфейса замыкания на себя, туннелей. Следующие опции доступны при выводе текущей конфигурации: - brief – вывод конфигурации без двоичных данных, например, SSH и SSL ключей. - detailed – вывод конфигурации с включением двоичных данных |
| show bootvar | - | Показывает активный файл системного ПО, который устройство загружает при запуске. |
| write [memory] | - | Сохранение текущей конфигурации в файл первоначальной конфигурации. |
| boot license source_url | - | Загрузить на устройство файл лицензии. |
| delete license [word] | - | Удалить с устройства все установленные файлы лицензий. - <i>word</i> – указать имя файла лицензии, который должен быть удален. |
| rename url new_url | url, new_url: (1..160) символов | Изменение имени файла. - <i>url</i> – текущее имя файла; - <i>new-url</i> – новое имя файла. |



Сервер TFTP не может быть адресом источника и адресом назначения для одной команды копирования.

Примеры использования команд

- Удалить файл *test* из энергонезависимой памяти:

```
console# delete flash:test
Delete flash:test? [confirm]
```

Результат выполнения команды: после подтверждения файл будет удален.

5.6.3 Команды для резервирования конфигурации

В данном разделе описаны команды, предназначенные для настройки резервирования конфигурации по таймеру или при сохранении текущей конфигурации на flash-накопителе.

Команды режима глобальной конфигурации

Запрос командной строки в режиме глобальной конфигурации имеет следующий вид:

```
console(config)#
```

Таблица 50 – Команды управления системой в режиме глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|-----------------------------|---------------------------------------|---|
| backup server server | server: (1..22) символов | Указание сервера, на который будет производиться резервирование конфигурации. Строка в формате «tftp://XXX.XXX.XXX.XXX» или «scp://[[username]][:[password]]@]host» |
| no backup server | | Удаление сервера для резервирования. |
| backup path path | path: (1..128) символов | Указание пути расположения файла на сервере и префикса файла. При сохранении к префиксу будет добавляться текущая дата и время в формате ггггммддччммсс. |
| no backup path | | Удаление пути для резервирования. |

| | | |
|---------------------------------|------------------------------------|---|
| backup history enable | -/выключено | Включить сохранение истории резервных копий. |
| no backup history enable | | Отключить сохранение истории резервных копий. |
| backup time-period timer | timer: (1..35791394)/720 мин | Указание промежутка времени, по истечении которого будет осуществляться автоматическое резервирование конфигурации. |
| no backup time-period | | Восстанавливает значение по умолчанию |
| backup auto | -/выключено | Включение автоматического резервирования конфигурации. |
| no backup auto | | Установка значения по умолчанию. |
| backup write-memory | -/выключено | Включение резервирования конфигурации при сохранении пользователем конфигурации на flash-накопитель. |
| no backup write-memory | | Установка значения по умолчанию. |

Таблица 51 – Команды управления системой в режиме Privileged EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|----------------------------|---------------------------------------|--|
| show backup | - | Отображает информацию о настройках резервирования конфигурации |
| show backup history | - | Отображает историю успешно сохраненных на сервер конфигураций. |

5.6.4 Команды для автоматического обновления и конфигурации

Процесс автоматического обновления

Коммутатор запускает процесс автоматического обновления, базирующийся на DHCP, если он включен и имя текстового файла (DHCP-опция 43, 125), содержащего имя образа ПО, было предоставлено сервером DHCP.

Процесс автоматического обновления состоит из следующих этапов:

1. Коммутатор загружает текстовый файл и читает из него имя файла образа ПО на TFTP-сервере;
2. Коммутатор скачивает первый блок (512 байт) образа ПО с TFTP-сервера, в котором содержится версия ПО;
3. Коммутатор сравнивает версию файла образа ПО, полученного с TFTP-сервера, с версией активного образа ПО коммутатора. Если они отличаются, коммутатор загружает образ ПО с TFTP-сервера вместо неактивного образа ПО коммутатора и делает данный образ активным;
4. Если образ ПО был загружен, то коммутатор перезагружается.

Процесс автоматического конфигурирования

Коммутатор запускает процесс автоматического конфигурирования, базирующийся на DHCP, при выполнении следующих условий:

- в конфигурации разрешено автоматическое конфигурирование;
- ответ DHCP-сервера содержит IP-адрес TFTP-сервера (DHCP-опция 66) и имя файла конфигурации (DHCP-опция 67) в формате ASCII.



Полученный файл конфигурации добавляется к текущей (running) конфигурации.

Команды режима глобальной конфигурации

Запрос командной строки в режиме глобальной конфигурации имеет следующий вид:

```
console (config) #
```

Таблица 52 – Команды управления системой в режиме глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|---------------------------------|---------------------------------------|--|
| boot host auto-config | -/включено | Включение автоматической конфигурации, базирующейся на DHCP. |
| no boot host auto-config | | Выключение автоматической конфигурации, базирующейся на DHCP. |
| boot host auto-update | -/включено | Включение автоматического обновления ПО, базирующегося на DHCP. |
| no boot host auto-update | | Выключение автоматического обновления ПО, базирующегося на DHCP. |

Команды режима Privileged EXEC

Запрос командной строки в режиме Privileged EXEC имеет следующий вид:

```
console#
```

Таблица 53 – Команды управления системой в режиме Privileged EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|------------------|---------------------------------------|--|
| show boot | - | Просмотр настроек автоматического обновления и конфигурации. |

- Пример конфигурации ISC DHCP Server:

```
option image-filename code 125 = {
unsigned integer 32, #enterprise-number. Идентификатор производителя, всегда равен
35265 (Eltex)
unsigned integer 8, #data-len. Длина всех данных опции. Равна длине строки sub-
option-data + 2.
unsigned integer 8, #sub-option-code. Код подопции, всегда равен 1
unsigned integer 8, #sub-option-len. Длина строки sub-option-data
text #sub-option-data. Имя текстового файла, содержащего имя
образа ПО
};

host mes2124-test {
hardware ethernet a8:f9:4b:85:a2:00; #mac-адрес коммутатора
filename "mesXXX-test.cfg"; #имя конфигурации коммутатора
option image-filename 35265 18 1 16 "mesXXX-401.ros"; #имя текстового
файла, содержащего имя образа ПО
next-server 192.168.1.3; #IP-адрес TFTP сервера
fixed-address 192.168.1.36; #IP-адрес коммутатора
}
```

5.7 Настройка системного времени



По умолчанию автоматический переход на летнее время осуществляется в соответствии со стандартами США и Европы. В конфигурации могут быть заданы любые дата и время для перехода на летнее время и обратно.

Команды режима Privileged EXEC

Запрос командной строки в режиме Privileged EXEC имеет следующий вид:

```
console#
```

Таблица 54 – Команды настройки системного времени в режиме Privileged EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|---|
| <code>clock set hh:mm:ss day month year</code> <code>clock set hh:mm:ss month day year</code> | hh: (0..23); mm: (0..59); ss: (0..59); day: (1..31); month: (Jan..Dec); year: (2000..2037) | Ручная установка системного времени (команда доступна только для привилегированного пользователя). - <i>hh</i> – часы, <i>mm</i> – минуты, <i>ss</i> – секунды; - <i>day</i> – день; <i>month</i> – месяц; <i>year</i> – год. |
| <code>show sntp configuration</code> | - | Показывает конфигурацию протокола SNTP. |
| <code>show sntp status</code> | - | Показывает статус протокола SNTP. |

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 55 – Команды настройки системного времени в режиме EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|--------------------------------|--------------------------------|---|
| <code>show clock</code> | - | Показывает системное время и дату. |
| <code>show clock detail</code> | | Дополнительно отображает параметры часового пояса и перехода на летнее время. |

Команды режима глобальной конфигурации

Запрос командной строки в режиме глобальной конфигурации имеет следующий вид:

```
console(config)#
```

Таблица 56 – Список команд для настройки системного времени в режиме глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|---|------------------------------------|--|
| <code>clock source {sntp browser}</code> | -/внешний источник не используется | Использование внешнего источника для установки системного времени. |
| <code>no clock source {sntp browser}</code> | | Запрещает использование внешнего источника для установки системного времени. |

| | | |
|--|--|--|
| clock timezone <i>zone</i> <i>hours_offset [minutes</i> <i>minutes_offset]</i> | zone: (1..4) символов/ нет описания зоны; hours_offset: (-12..+13)/0; minutes_offset: (0..59)/0; | Устанавливает значение часового пояса. - <i>zone</i> – слово, сформированное из первых букв словосочетания, которое оно заменяет (описание зоны); - <i>hours_offset</i> – часовое смещение относительно нулевого меридиана UTC; - <i>minutes_offset</i> – минутное смещение относительно нулевого меридиана UTC. |
| no clock timezone | | Устанавливает значение по умолчанию. |
| clock summer-time zone date <i>date month year hh:mm date</i> <i>month year hh:mm [offset]</i> | zone: (1..4) символа/ нет описания зоны; date: (1..31); month: (Jan..Dec); year: (2000 ..2037); hh: (0..23); mm: (0..59); week: (1-5); day: (sun..sat); offset: (1..1440)/60 мин; По умолчанию переход на летнее время выключен | Задаёт дату и время для автоматического перехода на летнее время и возврата обратно (для определённого года). Первым в команде указывается описание зоны, вторым время для перехода на летнее время и третьим время для возврата. - <i>zone</i> – слово, сформированное из первых букв словосочетания, которое оно заменяет (описание зоны); - <i>date</i> – число; - <i>month</i> – месяц; - <i>year</i> – год; - <i>hh</i> – часы, <i>mm</i> – минуты; - <i>offset</i> – количество минут, добавляемых при переходе на летнее время. |
| clock summer-time zone date <i>month date year hh:mm month</i> <i>date year hh:mm [offset]</i> | | Задаёт дату и время для автоматического перехода на летнее время и возврата обратно в режиме ежегодного. - <i>zone</i> – слово, сформированное из первых букв словосочетания, которое оно заменяет (описание зоны); - <i>usa</i> – установить правила перехода на летнее время, используемые в США (переход во второе воскресенье марта, обратно в первое воскресенье ноября, в 2 часа утра по местному времени); - <i>eu</i> – установить правила перехода на летнее время, используемые Евросоюзом (переход в последнее воскресенье марта, обратно в последнее воскресенье октября, в 1 час утра по Гринвичу); - <i>hh</i> – часы, <i>mm</i> – минуты; - <i>week</i> – неделя месяца; - <i>day</i> – день недели; - <i>month</i> – месяц; - <i>offset</i> – количество добавляемых минут при переходе на летнее время. |
| clock summer-time zone recurring { <i>usa</i> <i>eu</i> { <i>first</i> <i>last</i> <i>week</i> } <i>day month hh:mm</i> { <i>first</i> <i>last</i> <i>week</i> } <i>day month</i> <i>hh:mm</i> } [<i>offset</i>] | | Отключает автоматический переход на летнее время. |
| no clock summer-time | | |
| sntp authentication-key <i>number md5 value</i> | number: (1..4294967295); value: (1..32) символов; По умолчанию проверка подлинности отключена | Устанавливает ключ проверки подлинности для протокола SNTP. - <i>number</i> – номер ключа; - <i>value</i> – значение ключа; - <i>encrypted</i> – задать значение ключа в зашифрованном виде. |
| encrypted sntp authentication-key <i>number</i> <i>md5 value</i> | | Удаляет ключ проверки подлинности для протокола SNTP. |
| no sntp authentication-key <i>number</i> | | |
| sntp authenticate | -/проверка подлинности не требуется | Требуется проверка подлинности для получения информации от NTP-серверов. |
| no sntp authenticate | | Устанавливает значение по умолчанию. |
| sntp trusted-key <i>key_number</i> | key_number: (1..4294967295); По умолчанию проверка подлинности отключена | Осуществляет проверку подлинности системы, от которой синхронизируется с помощью SNTP по заданному ключу. - <i>key_number</i> – номер ключа. |
| no sntp trusted-key <i>key_number</i> | | Устанавливает значение по умолчанию. |
| sntp broadcast client enable { <i>both</i> <i>ipv4</i> <i>ipv6</i> } | -/запрещено | Разрешает работу ширококвещательных SNTP-клиентов. |
| no sntp broadcast client enable | | Устанавливает значение по умолчанию. |
| sntp anycast client enable { <i>both</i> <i>ipv4</i> <i>ipv6</i> } | -/запрещено | Разрешает работу SNTP-клиентам, поддерживающим метод рассылки пакетов, позволяющий посылать данные ближайшему устройству из группы получателей. |
| no sntp anycast client enable | | Устанавливает значение по умолчанию. |

| | | |
|--|--|--|
| sntp client enable {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> oob vlan <i>vlan_id</i> } | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..32); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..128); <i>vlan_id</i> (1..4094) /запрещено | Разрешает работу SNTP-клиентам, поддерживающим метод рассылки пакетов, позволяющий посылать данные ближай- шему устройству из группы получателей, а также широкопеча- тельным SNTP-клиентам для выбранного интерфейса. - подробное описание интерфейсов изложено в разделе «Кон- фигурация интерфейсов». |
| no sntp client enable {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> oob vlan <i>vlan_id</i> } | | Устанавливает значение по умолчанию. |
| sntp unicast client enable | -/запрещено | Разрешает работу одноадресных SNTP-клиентов. |
| no sntp unicast client enable | | Устанавливает значение по умолчанию. |
| sntp unicast client poll | -/запрещено | Разрешает последовательный опрос заданных одноадресных SNTP-серверов. |
| no sntp unicast client poll | | Устанавливает значение по умолчанию. |
| sntp server { <i>ipv4_address</i> <i>ipv6_address</i> <i>ipv6_link_local_address</i> { <i>vlan</i> <i>{integer}</i> <i>ch</i> { <i>integer</i> } <i>isatap</i> <i>{integer}</i> } <i>{physical_port_name}</i> } <i>hostname</i> } [poll] [key <i>keyid</i>] | <i>hostname</i> : (1..158) символов; <i>keyid</i> : (1..4294967295) | Задает адрес SNTP-сервера. - <i>ipv4_address</i> – IPv4-адрес узла сети; - <i>ipv6_address</i> – IPv6-адрес узла сети; - <i>ipv6z-address</i> – IPv6z-адрес узла сети для ping. Формат адреса <i>ipv6_link_local_address</i> { <i>interface_name</i> : <i>ipv6_link_local_address</i> – локальный IPv6 адрес канала; <i>interface_name</i> – имя исходящего интерфейса задается в сле- дующем формате: <i>vlan</i> { <i>integer</i> } <i>ch</i> { <i>integer</i> } <i>isatap</i> { <i>integer</i> } { <i>physical_port_name</i> } - <i>hostname</i> – доменное имя узла сети; - <i>poll</i> – включает опрос; - <i>keyid</i> – идентификатор ключа. |
| no sntp server { <i>ipv4_address</i> <i>ipv6_address</i> <i>ipv6_link_local_address</i> { <i>vlan</i> <i>{integer}</i> <i>ch</i> { <i>integer</i> } <i>isatap</i> <i>{integer}</i> } <i>{physical_port_name}</i> } <i>hostname</i> } | | Удаление сервера из списка NTP-серверов. |
| clock dhcp timezone | -/запрещено | Разрешает получение таких данных как часовой пояс и летнее время от DHCP-сервера. |
| no clock dhcp timezone | | Запрещает получения таких данных как часовой пояс и летнее время от DHCP-сервера. |

Команды режима конфигурации интерфейса

Запрос командной строки в режиме конфигурации интерфейса имеет следующий вид:

```
console (config-if) #
```

Таблица 57 – Список команд для настройки системного времени в режиме конфигурации интерфейса

| Команда | Значение/Значение по умолчанию | Действие |
|------------------------------|---------------------------------------|---|
| sntp client enable | -/запрещено | Разрешает работу SNTP-клиенту, который поддерживает метод рассылки пакетов, позволяющий посылать данные устройству ближайшему из группы получателей, а также ширококвещательному SNTP-клиенту на настраиваемом интерфейсе (Ethernet, port-channel, VLAN). |
| no sntp client enable | | Устанавливает значение по умолчанию. |

Примеры выполнения команд

- Отобразить системное время, дату и данные по часовой зоне:

```
console# show clock detail
```

```
15:29:08 PDT(UTC-7) Jun 17 2009
Time source is SNTP

Time zone:
Acronym is PST
Offset is UTC-8

Summertime:
Acronym is PDT
Recurring every year.
Begins at first Sunday of April at 2:00.
```

Статус процесса синхронизации времени отображается с помощью дополнительно символа перед значением времени.

Пример:

```
*15:29:08 PDT(UTC-7) Jun 17 2009
```

Используются следующие обозначения:

- точка (.) означает, что время достоверно, но нет синхронизации с сервером SNTP;
- отсутствие символа означает, что время достоверно и синхронизация есть;
- звездочка (*) означает, что время недостоверно.

- Задать дату и время на системных часах: 7 марта 2009 года, 13:32

```
console# clock set 13:32:00 7 Mar 2009
```

- Отобразить статус протокола SNTP:

```
console# show sntp status
```

```
Clock is synchronized, stratum 3, reference is 10.10.10.1, unicast

Unicast servers:

Server           : 10.10.10.1
Source           : Static
Stratum          : 3
Status           : up
Last Response    : 10:37:38.0 UTC Jun 22 2016
Offset           : 1040.1794181 mSec
Delay            : 0 mSec

Anycast server:

Broadcast:
```

В примере выше системное время синхронизировано от сервера 10.10.10.1, последний ответ получен в 10:37:38, несовпадение системного времени с временем на сервере составило 1.04 с.

5.8 Конфигурация временных интервалов time-range

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console (config) #
```

Таблица 58 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|---------------------------------------|---------------------------------------|---|
| time-range <i>time_name</i> | time_name: (0..32) символа | Создание time-range и вход в режим конфигурации временных интервалов. - time_name – имя профиля настроек time-range. |
| no time-range <i>time_name</i> | | Удалить временной интервал. |

Команды режима конфигурации временных интервалов

```
console# configure
console (config) # time-range range_name
console (config-time-range) #
```

Таблица 59 – Команды режима конфигурации временного интервала

| Команда | Значение/Значение по умолчанию | Действие |
|---|--|---|
| absolute {end start} <i>hh:mm date month year</i> | hh: (0..23); mm: (0..59); date: (1..31); month: (jan..dec); year: (2000..2097) | Задать начало и (или) конец временного интервала в формате: час: минута день месяц год. |
| no absolute {end start} | | Удалить временной интервал. |
| periodic list <i>hh:mm to hh:mm {all weekday}</i> | hh: (0..23); mm: (0..59); weekday: (mon...sun) | Задать временной интервал в течение одного из дней недели или каждого дня недели. |
| no periodic list <i>hh:mm to hh:mm {all weekday}</i> | | Удалить временной интервал. |
| periodic weekday <i>hh:mm to weekday hh:mm</i> | hh: (0..23); mm: (0..59); weekday: (mon...sun) | Задать временной интервал в течение недели. |
| no periodic weekday <i>hh:mm to weekday hh:mm</i> | | Удалить временной интервал. |

Команды режима конфигурации интерфейсов Ethernet и Port-Channel

Вид запроса командной строки в режиме конфигурации интерфейсов:

```
console (config-if) #
```

Таблица 60 – Команды режима конфигурации интерфейсов Ethernet и Port-Channel

| Команда | Значение/Значение по умолчанию | Действие |
|--|---------------------------------------|--|
| operation time <i>time_name</i> | time_name: (0..32) символа | Задать time-range, определяющий временной интервал, в котором интерфейс будет находиться в состоянии Up. - time_name – имя профиля настроек time-range. |
| no operation time | | Удалить временной интервал. |

5.9 Конфигурация интерфейсов и VLAN

5.9.1 Параметры Ethernet-интерфейсов, Port-Channel и Loopback-интерфейсов

Команды режима конфигурации интерфейса (диапазона интерфейсов)

```
console# configure
console(config)# interface {gigabitethernet gi_port | tengigabitethernet
te_port | twentyfivegigabitethernet twe_port | hundredgigabitethernet
hu_port | oob | port-channel group | range {...} | loopback loopback_id }
console(config-if)#
```

Данный режим доступен из режима конфигурации и предназначен для задания параметров конфигурации интерфейса (порта коммутатора или группы портов, работающих в режиме разделения нагрузки) либо диапазона интерфейсов.

Выбор интерфейса осуществляется при помощи команд из таблицы ниже.

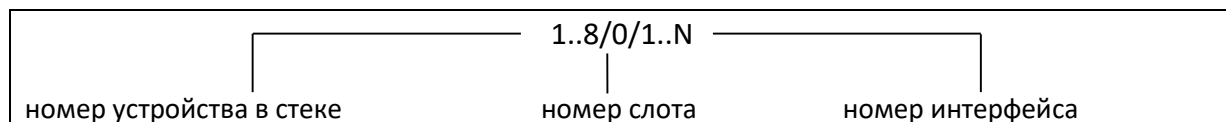
Таблица 61 – Команды выбора интерфейса для коммутаторов

| Команда | Назначение |
|---|--|
| interface gigabitethernet gi_port | Для настройки 1G-интерфейсов. |
| interface tengigabitethernet te_port | Для настройки 10G-интерфейсов. |
| interface twentyfivegigabitethernet twe_port | Для настройки 25G-интерфейсов. |
| interface hundredgigabitethernet hu_port | Для настройки 100G-интерфейсов. |
| interface port-channel group | Для настройки групп каналов. |
| interface oob | Для настройки интерфейса управления (интерфейс управления присутствует не на всех коммутаторах). |
| interface loopback loopback_id | Для настройки виртуальных интерфейсов. |

где:

- *group* – порядковый номер группы, общее количество согласно таблице 9 (строка «Агрегация каналов (LAG)»);
- *gi_port* – порядковый номер 1G-интерфейса, задается в виде: 1..8/0/1..48;
- *te_port* – порядковый номер 10G-интерфейса, задается в виде: 1..8/0/1..48;
- *twe_port* – порядковый номер 25G-интерфейса, задается в виде: 1..8/0/1..120;
- *hu_port* – порядковый номер 100G-интерфейса, задается в виде: 1..8/0/1..32;
- *loopback_id* – порядковый номер виртуального интерфейса, общее количество согласно таблице 9 (строка «Количество виртуальных Loopback-интерфейсов»).

Запись интерфейса



Команды, введенные в режиме конфигурации интерфейса, применяются к выбранному интерфейсу.

Ниже приведены команды для входа в режим настройки десятого Ethernet-интерфейса первого устройства в стеке и входа в режим настройки группы каналов 1.

```
console# configure
console(config)# interface tengigabitethernet 1/0/10
console(config-if)#
```

```

console# configure
console(config)# interface hundredgigabitethernet 1/0/10
console(config-if)#
console# configure
console(config)# interface port-channel 1
console(config-if)#

```

Выбор диапазона интерфейсов осуществляется при помощи команд:

- **interface range gigabitethernet portlist** — для настройки диапазона gigabitethernet-интерфейсов;
- **interface range tengigabitethernet portlist** – для настройки диапазона tengigabitethernet-интерфейсов;
- **interface range twentyfivegigabitethernet portlist** – для настройки диапазона twentyfivegigabitethernet-интерфейсов;
- **interface range hundredgigabitethernet portlist** – для настройки диапазона hundredgigabitethernet-интерфейсов;
- **interface range port-channel grouplist** – для настройки диапазона групп портов.

Команды, введенные в данном режиме, применяются к выбранному диапазону интерфейсов.

Ниже приведены команды для входа в режим настройки диапазона Ethernet-интерфейсов с 1 по 10 всех групп портов.

```

console# configure
console(config)# interface range gigabitethernet 1/0/1-10
console(config-if)#

console# configure
console(config)# interface range tengigabitethernet 1/0/1-10
console(config-if)#

console# configure
console(config)# interface range twentyfivegigabitethernet 1/0/1-10
console(config-if)#

console# configure
console(config)# interface range hundredgigabitethernet 1/0/1-10
console(config-if)#

console# configure
console(config)# interface range port-channel 1-10
console(config-if)#

```

Таблица 62 – Команды режима конфигурации интерфейсов Ethernet и Port-Channel

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--------------------------|---------------------------------------|---|
| shutdown | -/включен | Выключить конфигурируемый интерфейс (Ethernet, port-channel). |
| no shutdown | | Включить конфигурируемый интерфейс. |
| description descr | descr: (1..64) символов/нет описания | Добавить описание интерфейса (Ethernet, port-channel). |
| no description | | Удалить описание интерфейса. |
| speed mode | mode: (10, 100, 1000, 10000) | Задать скорость передачи данных (Ethernet). |
| no speed | | Установить значение по умолчанию. |
| duplex mode | mode: (full, half)/full | Задать режим дуплекса интерфейса (полнодуплексное соединение, полудуплексное соединение, Ethernet). |

| | | |
|---|--|--|
| no duplex | | Установить значение по умолчанию. |
| negotiation [cap1 [cap2...cap5]] | cap: (10f, 10h, 100f, 100h, 1000f, 10000f) | Включает автосогласование для скорости и дуплекса на настраиваемом интерфейсе. Можно указать определенные совместимости параметра автосогласования, если параметры не заданы, то поддерживаются все совместимости (Ethernet, port-channel). |
| no negotiation | | Выключает автосогласование для скорости и дуплекса на настраиваемом интерфейсе. |
| negotiation bypass | -/long | Режим установления связи в обход процедуры автосогласования, если партнер на встречной стороне не отвечает со стандартным таймаутом процесса автосогласования (negotiation timeout long). |
| negotiation bypass forced | | Режим установления связи в обход процедуры автосогласования, если партнер на встречной стороне не отвечает с минимальным таймаутом процесса автосогласования (negotiation timeout short). |
| flowcontrol mode | mode: (on, off, auto)/off | Задать режим управления потоком flowcontrol (включить, отключить или автосогласование). Автосогласование flowcontrol работает только в случае, если режим автосогласования negotiation включен на настраиваемом интерфейсе (Ethernet, port-channel). |
| no flowcontrol | | Отключить режим управления потоком. |
| back-pressure | -/выключен | Включает функцию «обратного давления» на настраиваемом интерфейсе (Ethernet). |
| no back-pressure | | Выключает функцию «обратного давления» на настраиваемом интерфейсе. |
| load-average period | period: (5..300)/15 | Установить период, в течение которого собирается статистика о нагрузке на интерфейсе. |
| no load-average | | Установить значение по умолчанию. |
| unidirectional send-only | -/выключено | Включает порт, оснащенный двунаправленными приемопередатчиками, в режим однонаправленной передачи. |
| no unidirectional | | Установить значение по умолчанию. |
| hardware profile portmode {1x100g 4x25g} | -/1x40g | Переключить режим интерфейсов HG. <input checked="" type="checkbox"/> Настройка применяется после сохранения конфигурации и перезагрузки устройства. <input checked="" type="checkbox"/> Поддерживается работа с breakout-кабелями 100G-4x25g и 40G-4x10g. |
| fec cl74 | | -/выключен |
| fec cl91 | Включить режим прямой коррекции ошибок cl91 на интерфейсе 25G. | |
| fec off | - | Отключить режим прямой коррекции ошибок. |
| speed mode | mode: (10, 100, 1000, 10000, 25000, 40000, 100000) | Задать скорость передачи данных (Ethernet). <input checked="" type="checkbox"/> Доступность конфигурирования скоростных режимов зависит от типа интерфейса устройства. |
| no speed | | Установить значение по умолчанию. |



На MES5400-24 в режиме расщепления могут работать 100G-интерфейсы HG3–HG6. На интерфейсах HG1, HG2 данный режим не поддерживается. На MES5400-24 rev.B поддержка расщепления есть на всех 100G-интерфейсах.



На MES5500-32 в режиме расщепления доступно максимум 30 100G-интерфейсов.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 63 – Команды режима общих настроек интерфейса Ethernet и Port-Channel

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|---|
| port jumbo-frame | -/запрещено | Разрешает коммутатору работать с кадрами большого размера. <input checked="" type="checkbox"/> Значение maximum transmission unit (MTU) по умолчанию 1500 байт. <input checked="" type="checkbox"/> Настройка вступит в силу только после перезагрузки устройства. <input checked="" type="checkbox"/> Значение maximum transmission unit (MTU) при настройке port jumbo-frame 10240 байт. |
| no port jumbo-frame | | Запрещает коммутатору работать с кадрами большого размера. |
| errdisable recovery cause {all loopback-detection port-security dot1x-src-address acl-deny stp-bpdu-guard stp-loopback-guard udld storm-control link-flapping} | -/запрещено | Включить автоматическую активацию интерфейса после его отключения в следующих случаях: - loopback-detection – обнаружение петель; - port-security – нарушение безопасности для port security; - dot1x-src-address – непрохождение аутентификации, основанной на MAC-адресах пользователей; - acl-deny – несоответствие спискам доступа (ACL); - stp-bpdu-guard – активация защиты BPDU Guard (передача не санкционированного пакета BPDU через интерфейс); - stp-loopback-guard – обнаружение петель протоколом STP; - udld – активация защиты UDLD; - storm-control – защита от «шторма» для различного трафика; - link-flapping – флаппинг линка. |
| no errdisable recovery cause {all loopback-detection port-security dot1x-src-address acl-deny stp-bpdu-guard stp-loopback-guard udld storm-control link-flapping} | | Установить значение по умолчанию. |
| errdisable recovery interval seconds | seconds: (30..86400)/300 секунд | Установить временной интервал для автоматического повторного включения интерфейса. |
| no errdisable recovery interval | | Установить значение по умолчанию. |
| snmp trap link-status | -/включено | Включает отправку SNMP trap-сообщений о состоянии интерфейсных линков. |
| no snmp trap link-status | | Отключает отправку SNMP trap-сообщений. |
| default interface [range] {ip ip_address oob gigabitethernet gi_port TenGigabitEthernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port Port-Channel group Loopback loopback_id Vlan vlan_id} | ip_address: A.B.C.D; gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); tve_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128); loopback_id: (1); vlan_id: (1..4094) | Сброс настроек интерфейса или группы интерфейсов на значения, установленные по умолчанию. |

Команды режима EXEC

Вид запроса командной строки в режиме EXEC:

```
console#
```

Таблица 64 – Команды режима EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|-----------------------|--------------------------------|--|
| clear counters | - | Сброс статистики для всех интерфейсов. |

| | | |
|--|---|---|
| clear counters {oob gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> } | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..128) | Сброс статистики для интерфейса. |
| set interface active { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> } | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..128) | Активирует порт или группу портов, выключенных командой shutdown . |
| show interfaces configuration {oob gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> detailed} | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..128) | Показать конфигурацию интерфейсов. |
| show interfaces status | - | Показать состояние всех интерфейсов. |
| show interfaces status {oob gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> detailed} | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..128) | Показать состояние Ethernet-порта, группы портов. |
| show interfaces advertise | - | Показать параметры автосогласования, объявленные для всех интерфейсов. |
| show interfaces advertise {oob gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> detailed} | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..128) | Показать параметры автосогласования, объявленные для Ethernet-порта, группы портов. |
| show interfaces description | - | Показать описания всех интерфейсов. |
| show interfaces description {oob gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> detailed} | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..128) | Показать описание Ethernet-порта, группы портов. |
| show interfaces counters | - | Показать статистику для всех интерфейсов. |
| show interfaces counters {oob gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> detailed} | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..128) | Показать статистику для интерфейса. |
| show interfaces utilization | - | Показать статистику по нагрузке для всех интерфейсов. |
| show interfaces utilization { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> } | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..128) | Показать статистику по нагрузке для Ethernet-интерфейса. |

| | | |
|--|--|--|
| show interfaces { gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group} | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Показать сводную информацию о состоянии, настройке и статистике порта. |
| show ports jumbo-frame | - | Показать настройку jumbo-frames в коммутаторе. |
| show errdisable recovery | - | Показать настройки для автоматической повторной активации порта. |
| show errdisable interfaces { gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group} | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Показать причину отключения порта, группы портов и состояние автоматической активации. |
| show hardware profile portmode | - | Показать режим работы родительского интерфейса и номера портов, на которые родительский интерфейс расщеплен. |

Примеры выполнения команд

- Показать состояние интерфейсов:

```
console# show interfaces status
```

| Port | Type | Duplex | Speed | Neg | Flow ctrl | Link State | Back Pressure | Mdix Mode |
|----------|-----------|--------|-------|----------|--------------|-------------|---------------|-----------|
| te1/0/3 | 10G-Fiber | Full | 1000 | Disabled | Off | Up | Disabled | Off |
| te1/0/4 | 10G-Fiber | -- | -- | -- | -- | Down | -- | -- |
| te1/0/5 | 10G-Fiber | -- | -- | -- | -- | Down | -- | -- |
| te1/0/6 | 10G-Fiber | -- | -- | -- | -- | Down | -- | -- |
| te1/0/7 | 10G-Fiber | -- | -- | -- | -- | Down | -- | -- |
| te1/0/8 | 10G-Fiber | -- | -- | -- | -- | Down | -- | -- |
| te1/0/9 | 10G-Fiber | -- | -- | -- | -- | Down | -- | -- |
| te1/0/10 | 10G-Fiber | -- | -- | -- | -- | Down | -- | -- |
| te1/0/11 | 10G-Fiber | -- | -- | -- | -- | Down | -- | -- |
| te1/0/12 | 10G-Fiber | -- | -- | -- | -- | Down | -- | -- |
| Ch | Type | Duplex | Speed | Neg | Flow control | Link State | | |
| Po1 | -- | -- | -- | -- | -- | Not Present | | |
| Po2 | -- | -- | -- | -- | -- | Not Present | | |
| Po3 | -- | -- | -- | -- | -- | Not Present | | |
| Po4 | -- | -- | -- | -- | -- | Not Present | | |
| Po5 | -- | -- | -- | -- | -- | Not Present | | |
| Po6 | -- | -- | -- | -- | -- | Not Present | | |
| Po7 | -- | -- | -- | -- | -- | Not Present | | |
| Po8 | -- | -- | -- | -- | -- | Not Present | | |
| Po9 | -- | -- | -- | -- | -- | Not Present | | |
| Po10 | -- | -- | -- | -- | -- | Not Present | | |
| Po11 | -- | -- | -- | -- | -- | Not Present | | |
| Po12 | -- | -- | -- | -- | -- | Not Present | | |
| Po13 | -- | -- | -- | -- | -- | Not Present | | |
| Po14 | -- | -- | -- | -- | -- | Not Present | | |

| | | | | | | |
|------|-----------|--------|-------|-----|------------|-------------|
| Po15 | -- | -- | -- | -- | -- | Not Present |
| Po16 | -- | -- | -- | -- | -- | Not Present |
| Po17 | -- | -- | -- | -- | -- | Not Present |
| Po18 | -- | -- | -- | -- | -- | Not Present |
| Po19 | -- | -- | -- | -- | -- | Not Present |
| Po20 | -- | -- | -- | -- | -- | Not Present |
| Po21 | -- | -- | -- | -- | -- | Not Present |
| Po22 | -- | -- | -- | -- | -- | Not Present |
| Po23 | -- | -- | -- | -- | -- | Not Present |
| Po24 | -- | -- | -- | -- | -- | Not Present |
| Po25 | -- | -- | -- | -- | -- | Not Present |
| Po26 | -- | -- | -- | -- | -- | Not Present |
| Po27 | -- | -- | -- | -- | -- | Not Present |
| Po28 | -- | -- | -- | -- | -- | Not Present |
| Po29 | -- | -- | -- | -- | -- | Not Present |
| Po30 | -- | -- | -- | -- | -- | Not Present |
| Po31 | -- | -- | -- | -- | -- | Not Present |
| Po32 | -- | -- | -- | -- | -- | Not Present |
| Oob | Type | Duplex | Speed | Neg | Link State | |
| oob | 1G-Copper | -- | -- | -- | Down | |

Показать параметры автосогласования:

console# **show interfaces advertise**

| Port | Type | Neg | Preferred | Operational Link Advertisement |
|----------|-----------|----------|-----------|--------------------------------|
| te1/0/3 | 10G-Fiber | Disabled | -- | -- |
| te1/0/4 | 10G-Fiber | Disabled | -- | -- |
| te1/0/5 | 10G-Fiber | Disabled | -- | -- |
| te1/0/6 | 10G-Fiber | Disabled | -- | -- |
| te1/0/7 | 10G-Fiber | Disabled | -- | -- |
| te1/0/8 | 10G-Fiber | Disabled | -- | -- |
| te1/0/9 | 10G-Fiber | Disabled | -- | -- |
| te1/0/10 | 10G-Fiber | Disabled | -- | -- |
| te1/0/11 | 10G-Fiber | Disabled | -- | -- |
| te1/0/12 | 10G-Fiber | Disabled | -- | -- |
| Ch | Type | Neg | Preferred | Operational Link Advertisement |
| Po1 | Unknown | Enabled | Slave | -- |
| Po2 | Unknown | Enabled | Slave | -- |
| Po3 | Unknown | Enabled | Slave | -- |
| Po4 | Unknown | Enabled | Slave | -- |
| Po5 | Unknown | Enabled | Slave | -- |
| Po6 | Unknown | Enabled | Slave | -- |
| Po7 | Unknown | Enabled | Slave | -- |
| Po8 | Unknown | Enabled | Slave | -- |
| Po9 | Unknown | Enabled | Slave | -- |
| Po10 | Unknown | Enabled | Slave | -- |
| Po11 | Unknown | Enabled | Slave | -- |
| Po12 | Unknown | Enabled | Slave | -- |
| Po13 | Unknown | Enabled | Slave | -- |
| Po14 | Unknown | Enabled | Slave | -- |
| Po15 | Unknown | Enabled | Slave | -- |
| Po16 | Unknown | Enabled | Slave | -- |
| Po17 | Unknown | Enabled | Slave | -- |
| Po18 | Unknown | Enabled | Slave | -- |
| Po19 | Unknown | Enabled | Slave | -- |
| Po20 | Unknown | Enabled | Slave | -- |
| Po21 | Unknown | Enabled | Slave | -- |
| Po22 | Unknown | Enabled | Slave | -- |
| Po23 | Unknown | Enabled | Slave | -- |
| Po24 | Unknown | Enabled | Slave | -- |
| Po25 | Unknown | Enabled | Slave | -- |
| Po26 | Unknown | Enabled | Slave | -- |
| Po27 | Unknown | Enabled | Slave | -- |

| | | | | |
|-------|---------|---------|--------------------------------|----|
| Po28 | Unknown | Enabled | Slave | -- |
| Po29 | Unknown | Enabled | Slave | -- |
| Po30 | Unknown | Enabled | Slave | -- |
| Po31 | Unknown | Enabled | Slave | -- |
| Po32 | Unknown | Enabled | Slave | -- |
| Oob | Type | Neg | Operational Link Advertisement | |
| ----- | | | | |
| oob | 1G- | Enabled | | -- |

Показать статистику по интерфейсам:

console# **show interfaces counters**

| Port | InUcastPkts | InMcastPkts | InBcastPkts | InOctets |
|---------|--------------|--------------|--------------|-----------|
| te1/0/1 | 0 | 0 | 0 | 0 |
| te1/0/2 | 0 | 0 | 0 | 0 |
| | | | | |
| te1/0/5 | 0 | 0 | 0 | 0 |
| te1/0/6 | 0 | 2 | 0 | 2176 |
| te1/0/7 | 0 | 1 | 0 | 4160 |
| te1/0/8 | 0 | 0 | 0 | 0 |
| | | | | |
| Port | OutUcastPkts | OutMcastPkts | OutBcastPkts | OutOctets |
| te1/0/1 | 0 | 0 | 0 | 0 |
| te1/0/2 | 0 | 0 | 0 | 0 |
| te1/0/3 | 0 | 0 | 0 | 0 |
| te1/0/4 | 0 | 0 | 0 | 0 |
| te1/0/5 | 0 | 0 | 0 | 0 |
| te1/0/6 | 0 | 545 | 83 | 62186 |
| te1/0/7 | 0 | 1424 | 216 | 164048 |
| te1/0/8 | 0 | 0 | 0 | 0 |
| te1/0/9 | 0 | 0 | 0 | 0 |
| | | | | |
| OOB | InUcastPkts | InMcastPkts | InBcastPkts | InOctets |
| oob | 0 | 13 | 0 | 1390 |
| OOB | OutUcastPkts | OutMcastPkts | OutBcastPkts | OutOctets |
| oob | 3 | 616 | 0 | 39616 |

- Показать статистику по группе каналов 1:

console# **show interfaces counters port-channel 1**

| Ch | InUcastPkts | InMcastPkts | InBcastPkts | InOctets |
|-----|--------------|--------------|--------------|-----------|
| Po1 | 111 | 0 | 0 | 9007 |
| Ch | OutUcastPkts | OutMcastPkts | OutBcastPkts | OutOctets |
| Po1 | 0 | 6 | 3 | 912 |

Alignment Errors: 0
 FCS Errors: 0
 Single Collision Frames: 0
 Multiple Collision Frames: 0
 SQE Test Errors: 0
 Deferred Transmissions: 0
 Late Collisions: 0
 Excessive Collisions: 0
 Carrier Sense Errors: 0

```
Oversize Packets: 0
Internal MAC Rx Errors: 0
Symbol Errors: 0
Received Pause Frames: 0
Transmitted Pause Frames: 0
```

- Показать настройку jumbo-frames в коммутаторе:

```
console# show ports jumbo-frame
```

```
Jumbo frames are disabled
Jumbo frames will be disabled after reset
```

- Показать режим работы родительского интерфейса и номера портов, на которые родительский интерфейс расщеплен:

```
console# show hardware profile portmode
```

| Interface | Port Mode after reset | Port Mode | Expanded interfaces |
|-----------|-----------------------|-----------|---------------------|
| hu1/0/1 | 4x25G | 4x25G | twe1/0/1-4 |
| hu1/0/2 | 4x25G | 4x25G | twe1/0/5-8 |
| hu1/0/3 | 1x100G | 1x100G | twe1/0/9-12 |
| hu1/0/4 | 1x100G | 1x100G | twe1/0/13-16 |
| hu1/0/5 | 1x100G | 1x100G | twe1/0/17-20 |
| hu1/0/6 | 1x100G | 1x100G | twe1/0/21-24 |
| hu2/0/1 | 4x25G | 1x100G | twe2/0/1-4 |
| hu2/0/2 | 1x100G | 1x100G | twe2/0/5-8 |
| hu2/0/3 | 1x100G | 1x100G | twe2/0/9-12 |
| hu2/0/4 | 1x100G | 1x100G | twe2/0/13-16 |
| hu2/0/5 | 1x100G | 1x100G | twe2/0/17-20 |
| hu2/0/6 | 1x100G | 1x100G | twe2/0/21-24 |
| hu3/0/1 | 1x100G | 1x100G | twe3/0/1-4 |
| hu3/0/2 | 1x100G | 1x100G | twe3/0/5-8 |
| hu3/0/3 | 1x100G | 1x100G | twe3/0/9-12 |
| hu3/0/4 | 1x100G | 1x100G | twe3/0/13-16 |
| hu3/0/5 | 1x100G | 1x100G | twe3/0/17-20 |
| hu3/0/6 | 1x100G | 1x100G | twe3/0/21-24 |
| hu4/0/1 | 1x100G | 1x100G | twe4/0/1-4 |
| hu4/0/2 | 1x100G | 1x100G | twe4/0/5-8 |
| hu4/0/3 | 1x100G | 1x100G | twe4/0/9-12 |
| hu4/0/4 | 1x100G | 1x100G | twe4/0/13-16 |
| hu4/0/5 | 1x100G | 1x100G | twe4/0/17-20 |
| hu4/0/6 | 1x100G | 1x100G | twe4/0/21-24 |
| hu5/0/1 | 1x100G | 1x100G | twe5/0/1-4 |
| hu5/0/2 | 1x100G | 1x100G | twe5/0/5-8 |
| hu5/0/3 | 1x100G | 1x100G | twe5/0/9-12 |
| hu5/0/4 | 1x100G | 1x100G | twe5/0/13-16 |
| hu5/0/5 | 1x100G | 1x100G | twe5/0/17-20 |
| hu5/0/6 | 1x100G | 1x100G | twe5/0/21-24 |
| hu6/0/1 | 1x100G | 1x100G | twe6/0/1-4 |
| hu6/0/2 | 1x100G | 1x100G | twe6/0/5-8 |
| hu6/0/3 | 1x100G | 1x100G | twe6/0/9-12 |
| hu6/0/4 | 1x100G | 1x100G | twe6/0/13-16 |
| hu6/0/5 | 1x100G | 1x100G | twe6/0/17-20 |
| hu6/0/6 | 1x100G | 1x100G | twe6/0/21-24 |
| hu7/0/1 | 1x100G | 1x100G | twe7/0/1-4 |
| hu7/0/2 | 1x100G | 1x100G | twe7/0/5-8 |
| hu7/0/3 | 1x100G | 1x100G | twe7/0/9-12 |
| hu7/0/4 | 1x100G | 1x100G | twe7/0/13-16 |
| hu7/0/5 | 1x100G | 1x100G | twe7/0/17-20 |

| | | | |
|---------|--------|--------|--------------|
| hu7/0/6 | 1x100G | 1x100G | twe7/0/21-24 |
| hu8/0/1 | 1x100G | 1x100G | twe8/0/1-4 |
| hu8/0/2 | 1x100G | 1x100G | twe8/0/5-8 |
| hu8/0/3 | 1x100G | 1x100G | twe8/0/9-12 |
| hu8/0/4 | 1x100G | 1x100G | twe8/0/13-16 |
| hu8/0/5 | 1x100G | 1x100G | twe8/0/17-20 |
| hu8/0/6 | 1x100G | 1x100G | twe8/0/21-24 |

Таблица 65 – Описание счетчиков

| Счетчик | Описание |
|----------------------------------|---|
| <i>InOctets</i> | Количество принятых байтов. |
| <i>InUcastPkts</i> | Количество принятых одноадресных пакетов. |
| <i>InMcastPkts</i> | Количество принятых многоадресных пакетов. |
| <i>InBcastPkts</i> | Количество принятых широковещательных пакетов. |
| <i>OutOctets</i> | Количество переданных байтов. |
| <i>OutUcastPkts</i> | Количество переданных одноадресных пакетов. |
| <i>OutMcastPkts</i> | Количество переданных многоадресных пакетов. |
| <i>OutBcastPkts</i> | Количество переданных широковещательных пакетов. |
| <i>Alignment Errors</i> | Количество принятых кадров с нарушенной целостностью (с количеством байт не соответствующим длине) и не прошедших проверку контрольной суммы (FCS). |
| <i>FCS Errors</i> | Количество принятых кадров с количеством байт, соответствующим длине, но не прошедших проверку контрольной суммы (FCS). |
| <i>Single Collision Frames</i> | Количество кадров, вовлеченных в единичную коллизию, но впоследствии переданных успешно. |
| <i>Multiple Collision Frames</i> | Количество кадров, вовлеченных более чем в одну коллизию, но впоследствии переданных успешно. |
| <i>Deferred Transmissions</i> | Количество кадров, для которых первая попытка передачи отложена из-за занятости среды передачи. |
| <i>Late Collisions</i> | Количество случаев, когда коллизия зафиксирована после того, как в канал связи уже были переданы первые 64 байт (slotTime) пакета. |
| <i>Excessive Collisions</i> | Количество кадров, которые не были переданы из-за избыточного количества коллизий. |
| <i>Carrier Sense Errors</i> | Количество случаев, когда состояние контроля несущей было потеряно, либо не утверждено при попытке передачи кадра. |
| <i>Oversize Packets</i> | Количество принятых пакетов, размер которых превышает максимальный разрешенный размер кадра. |
| <i>Internal MAC Rx Errors</i> | Количество кадров, которые не были приняты успешно из-за внутренней ошибки приема на уровне MAC. |
| <i>Symbol Errors</i> | <p>Для интерфейса, работающего в режиме 100 Мб/с – количество случаев, когда имелся недопустимый символ данных, в то время как правильная несущая была представлена.</p> <p>Для интерфейса, работающего в полудуплексном режиме 1000 Мб/с – количество случаев, когда средства приема заняты в течение времени, равному или большему чем размер слота (slotTime), и в течение которого имелось хотя бы одно событие, которое заставляет PHY выдавать ошибку приема данных (Data reception error) или ошибку несущей (Carrier extend error) на GMII.</p> <p>Для интерфейса, работающего в полном дуплексном режиме 1000 Мб/с – количество случаев, когда средства приема заняты в течение времени, равному или большему чем минимальный размер кадра (minFrameSize), и в течение которого имелось хотя бы одно событие, которое заставляет PHY выдавать ошибку приема данных (Data reception error) на GMII.</p> |
| <i>Received Pause Frames</i> | Количество принятых управляющих MAC-кадров с кодом операции PAUSE. |

| | |
|---------------------------------|--|
| <i>Transmitted Pause Frames</i> | Количество переданных управляющих MAC-кадров с кодом операции PAUSE. |
|---------------------------------|--|

5.9.2 Настройка VLAN и режимов коммутации интерфейсов

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console (config) #
```

Таблица 66 – Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---------------------------------------|--|
| vlan database | - | Перейти в режим конфигурации VLAN. |
| vlan prohibit-internal-usage {add VLANlist remove VLANlist except VLANlist none} | VLANlist: (2..4094) | <ul style="list-style-type: none"> - add – добавить указанные VLAN ID в перечень запрещенных для внутреннего использования; - remove – удалить указанные VLAN ID из перечня запрещенных для внутреннего использования; - except – добавить в перечень запрещенных для внутреннего использования все VLAN ID, за исключением указанных в качестве параметра; - none – очистить перечень VLAN ID, запрещенных для внутреннего использования. |
| vlan mode {basic tr101} | -/basic | Включить возможность добавления на физическом интерфейсе в режиме customer сразу двух идентификаторов VLAN. |

Команды режима конфигурации VLAN

Вид запроса командной строки в режиме конфигурации VLAN:

```
console# configure
console (config) # vlan database
console (config-vlan) #
```

Данный режим доступен из режима глобальной конфигурации и предназначен для задания параметров конфигурации VLAN.

Таблица 67 – Команды режима конфигурации VLAN

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|--|---|
| vlan VLANlist [name VLAN_name] | VLANlist: (2..4094) VLAN_name: (1..32) | Добавить VLAN или несколько VLAN. |
| no vlan VLANlist | символа | Удалить VLAN или несколько VLAN. |
| map protocol protocol [encaps] protocols-group group | protocol: (ip, ipx, ipv6, arp, (0600-ffff (hex))*); | Привязать протокол к группе протоколов, ассоциированных вместе. |
| no map protocol protocol [encaps] | encaps: (ethernet, rfc1042, llcOther); ethernet group: (1..2147483647); | Удалить привязку. *- номер протокола (16 бит). |
| map mac mac_address {host mask} macs-group group | mask: (9..48) | Привязать MAC-адрес или диапазон MAC-адресов по маске к группе MAC-адресов. |
| no map mac mac_address {host mask} | | Удалить привязку. |
| map subnet ip_address mask subnets-group group | mask: (1..32); group: (1..2147483647) | Привязать IP-адрес или диапазон IP-адресов по маске к группе IP-адресов. |

| | | |
|--|--|-------------------|
| <code>no map subnet ip_address mask</code> | | Удалить привязку. |
|--|--|-------------------|

Команды режима конфигурации интерфейса (диапазона интерфейсов) VLAN

Вид запроса командной строки в режиме конфигурации интерфейса VLAN:

```
console# configure
console(config)# interface {vlan vlan_id | range vlan VLANlist}
console(config-if)#
```

Данный режим доступен из режима конфигурации и предназначен для задания параметров конфигурации интерфейса VLAN либо диапазона интерфейсов.

Выбор интерфейса осуществляется при помощи команды:

```
interface vlan vlan_id
```

Выбор диапазона интерфейсов осуществляется при помощи команды:

```
interface range vlan VLANlist
```

Ниже приведены команды для входа в режим настройки интерфейса VLAN 1 и входа в режим настройки группы VLAN 1, 3, 7.

```
console# configure
console(config)# interface vlan 1
console(config-if)#
console# configure
console(config)# interface range vlan 1,3,7
console(config-if)#
```

Таблица 68 – Команды режима конфигурации интерфейса VLAN

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|------------------------|--|-----------------------------------|
| <code>name name</code> | name: (1..32) | Добавить имя VLAN. |
| <code>no name</code> | символов/имя соответствует номеру VLAN | Установить значение по умолчанию. |

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet, интерфейса группы портов:


```
console# configure
console(config)# interface {tengigabitethernet te_port |
twentyfivegigabitethernet twe_port | hundredgigabitethernet hu_port | oob
| port-channel group | range {...}}
console(config-if)#
```

Данный режим доступен из режима конфигурации и предназначен для задания параметров конфигурации интерфейса (порта коммутатора или группы портов, работающих в режиме разделения нагрузки) либо диапазона интерфейсов.

Порт может работать в четырех режимах:

- *access* – интерфейс доступа – нетегированный интерфейс для одной VLAN;
- *trunk* – интерфейс, принимающий только тегированный трафик, за исключением одного VLAN, который может быть добавлен с помощью команды *switchport trunk native vlan*;
- *general* – интерфейс с полной поддержкой 802.1q, принимает как тегированный, так и нетегированный трафик;
- *customer* – Q-in-Q интерфейс.

Таблица 69 – Команды режима конфигурации интерфейса Ethernet

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|---|
| switchport mode mode | mode: (access, trunk, general, customer)/access | Задать режим работы порта в VLAN. - <i>mode</i> – режим работы порта в VLAN. |
| no switchport mode | | Установить значение по умолчанию. |
| switchport access vlan vlan_id | vlan_id: (1..4094)/1 | Добавить VLAN для интерфейса доступа. - <i>vlan_id</i> – идентификационный номер VLAN. |
| no switchport access vlan | | Установить значение по умолчанию. |
| switchport access acceptable-frame-type {untagged-only all} | -/принимать все типы кадров | Принимать на интерфейсе только кадры определенного типа: - untagged-only — только нетегированные; - all — все кадры. |
| no switchport access acceptable-frame-type | | Принимать на интерфейсе все типы кадров. |
| switchport trunk allowed vlan vlan_list | vlan_list: (2..4094) | Указать список VLAN для интерфейса. - <i>vlan_list</i> – список VLAN ID. Диапазон номеров VLAN можно задать перечислением через запятую или указать начальное и конечное значения диапазона через дефис "-".  Текущий список VLAN на интерфейсе будет заменён на указанный в команде. |
| no switchport trunk allowed vlan | | Удалить список VLAN для интерфейса. |
| switchport trunk allowed vlan add vlan_list | vlan_list: (2..4094, all) | Добавить список VLAN для интерфейса к текущим VLAN. - <i>vlan_list</i> – список VLAN ID. Диапазон номеров VLAN можно задать перечислением через запятую или указать начальное и конечное значения диапазона через дефис "-". |
| switchport trunk allowed vlan remove vlan_list | | Удалить список VLAN для интерфейса. |
| switchport trunk native vlan vlan_id | vlan_id: (1..4094)/1 | Добавляет номер VLAN в качестве Default VLAN для данного интерфейса. Весь нетегированный трафик, поступающий на данный порт, определяется в данную VLAN. - <i>vlan_id</i> – идентификационный номер VLAN. |
| no switchport trunk native vlan | | Установить значение по умолчанию. |
| switchport trunk allowed vlan all | -/выключено | Автоматически добавляет все доступные VLAN для данного интерфейса. |
| no switchport trunk allowed vlan all | | Отключает автоматическое добавление VLAN. |
| switchport general allowed vlan add vlan_list [tagged untagged] | vlan_list: (2..4094, all) | Добавить список VLAN для интерфейса. - tagged – порт будет передавать тегированные пакеты для VLAN; - untagged – порт будет передавать нетегированные пакеты для VLAN. - <i>vlan_list</i> – список VLAN ID. Диапазон VLAN можно задать перечислением через запятую или указать начальное и конечное значения диапазона через дефис "-". |
| switchport general allowed vlan remove vlan_list | | Удалить список VLAN для интерфейса. |

| | | |
|--|--|---|
| switchport general pvid <i>vlan_id</i> | vlan_id: (1..4094)/1 – если установлен VLAN по умолчанию | Добавить идентификатор VLAN порта (PVID) для основного интерфейса. - <i>vlan_id</i> – идентификационный номер VLAN порта. |
| no switchport general pvid | | Установить значение по умолчанию. |
| switchport general ingress-filtering disable | -/фильтрация включена | Выключить для основного интерфейса фильтрацию входящих пакетов на основе присвоенного им значения VLAN ID. |
| no switchport general ingress-filtering disable | | Включить для основного интерфейса фильтрацию входящих пакетов на основе присвоенного им значения VLAN ID. Если фильтрация включена, и пакет не входит в группу VLAN с присвоенным пакету значением VLAN ID, то пакет отбрасывается. |
| switchport general acceptable-frame-type {tagged-only untagged-only all} | -/принимать все типы кадров | Принимать на интерфейсе только кадры определенного типа: - tagged-only – только тегируемые; - untagged-only – только не тегируемые; - all – все кадры. |
| no switchport general acceptable-frame-type | | Принимать на интерфейсе все типы кадров. |
| switchport general map protocols-group group vlan <i>vlan_id</i> | vlan_id: (1..4094) group: (1.. 2147483647) | Установить правило классификации VLAN для интерфейса, основанное на привязке к протоколу. - <i>group</i> – идентификационный номер группы; - <i>vlan_id</i> – идентификационный номер VLAN. |
| no switchport general map protocols-group group | | Удалить правило классификации. |
| switchport general map macs-group group vlan <i>vlan_id</i> | vlan_id: (1..4094) group: (1..2147483647) | Установить правило классификации VLAN для интерфейса, основанное на привязке к MAC-адресу. - <i>group</i> – идентификационный номер группы; - <i>vlan_id</i> – идентификационный номер VLAN. |
| no switchport general map macs-group group | | Удалить правило классификации. |
| switchport general map protocols-group group vlan <i>vlan_id</i> | vlan_id: (1..4094) group: (1.. 2147483647) | Установить правило классификации VLAN для интерфейса, основанное на привязке к протоколу. - <i>group</i> – идентификационный номер группы; - <i>vlan_id</i> – идентификационный номер VLAN. |
| no switchport general map protocols-group group | | Удалить правило классификации. |
| switchport general map subnets-group group vlan <i>vlan_id</i> | vlan_id: (1..4094) group: (1.. 2147483647) | Установить правило классификации VLAN для интерфейса, основанное на привязке к IP-адресу. |
| no switchport general map subnets-group group | | Удалить правило классификации. |
| switchport customer vlan <i>vlan_id</i> | vlan_id: (1..4094)/1 | Добавить VLAN для пользовательского интерфейса. - <i>vlan_id</i> – идентификационный номер VLAN. |
| switchport customer vlan <i>vlan_id inner-vlan vlan_id</i> | | Добавить к входящим нетегируемым пакетам на клиентском порту внутренний 802.1q заголовок — C-VLAN (inner-vlan) и внешний 802.1q заголовок, содержащий pvid дополнительной VLAN (S-VLAN).  Для работы этой команды необходимо включить глобально режим «vlan mode tr101». |
| no switchport customer vlan | | Установить значение по умолчанию. |
| switchport customer multicast-tv vlan add <i>vlan_list</i> | vlan_list: (2..4094, all) | Разрешает принимать многоадресный трафик из указанных VLAN (не являющихся VLAN пользовательского интерфейса) на настраиваемом интерфейсе, совместно с пользователями других пользовательских портов, принимающих многоадресный трафик из данных VLAN. - <i>vlan_list</i> – список VLAN ID. Диапазон VLAN можно задать перечислением через запятую или указать начальное и конечное значения диапазона через дефис "-". |
| switchport customer multicast-tv vlan remove <i>vlan_list</i> | | Запрещает принимать многоадресный трафик на настраиваемом интерфейсе. |
| switchport protected-port | -/выключено | Переводит порт в режим изоляции внутри группы портов. |
| no switchport protected-port | | Восстанавливает значение по умолчанию. |

| | | |
|---|--|---|
| switchport forbidden default-vlan | По умолчанию членство в дефолтной VLAN разрешено | Запретить добавление дефолтной VLAN порту. |
| no switchport forbidden default-vlan | | Установить значение по умолчанию. |
| switchport default-vlan tagged | - | Установить порт как тегирующий в дефолтной VLAN. |
| no switchport default-vlan tagged | | Установить значение по умолчанию. |
| switchport dot1q ethertype egress stag ethertype | ethertype: (1..ffff) (hex)/8100 | Заменить TPID (Tag Protocol ID) в 802.1q VLAN-тегах пакетов, исходящих с данного интерфейса. Допустимые значения EtherType см. Приложение В. Поддерживаемые значения Ethertype. |
| no switchport dot1q ethertype egress stag | | Заменить ethertype исходящего с интерфейса пакета на значение по умолчанию. |
| switchport dot1q ethertype ingress stag add ethertype | ethertype: (1..ffff) (hex) | Добавить TPID в таблицу классификаторов VLAN. Допустимые значения EtherType см. Приложение В. Поддерживаемые значения Ethertype. |
| switchport dot1q ethertype ingress stag remove ethertype | | Удалить TPID из таблицы классификаторов VLAN. |

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 70 – Команды режима Privileged EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---------------------------------|---------------------------------------|--|
| show vlan | - | Показать информацию по всем VLAN. |
| show vlan tag vlan_id | vlan_id: (1..4094) | Показать информацию по VLAN, поиск по идентификатору. |
| show vlan internal usage | - | Показать список VLAN для внутреннего использования коммутатором. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 71 – Команды режима EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---|--|
| show vlan multicast-tv vlan vlan_id | vlan_id: (1..4094) | Показать порты-источники и приемники многоадресного трафика в данной VLAN. Порты источники могут как передавать, так и принимать многоадресный трафик. |
| show vlan protocols-groups | - | Показать информацию о группах протоколов. |
| show vlan macs-groups | - | Показать информацию о группах MAC-адресов. |
| show interfaces switchport {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group} | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Показать конфигурацию порта, группы портов. |

| | | |
|---|--|---|
| <pre>show interfaces protected-ports [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group detailed]</pre> | <pre>gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128)</pre> | <p>Показать состояние портов: в режиме Private VLAN Edge, в private-vlan-edge-сообществе.</p> |
|---|--|---|

Примеры выполнения команд

- Показать информацию о всех VLAN:

```
console# show vlan
```

```
Created by: D-Default, S-Static, G-GVRP, R-Radius Assigned VLAN, V-Voice VLAN
```

| Vlan | Name | Tagged Ports | UnTagged Ports | Created by |
|------|------|--------------|----------------|------------|
| 1 | 1 | | te1/0/1-12 | D |
| | | | Pol-16 | |
| 2 | 2 | | | S |
| 3 | 3 | | | S |
| 4 | 4 | | | S |
| 5 | 5 | | | S |
| 6 | 6 | | | S |
| 8 | 8 | | | S |

Показать порты источники и приемники многоадресного трафика в VLAN 4:

```
console# show vlan multicast-tv vlan 4
```

```
Source ports : te0/1
Receiver ports: te0/2,te0/4,te0/8
```

- Показать информацию о группах протоколов:

```
console# show vlan protocols-groups
```

| Encapsulation | Protocol | Group Id |
|---------------|----------|----------|
| 0x800 (IP) | Ethernet | 1 |
| 0x806 (ARP) | Ethernet | 1 |
| 0x86dd (IPv6) | Ethernet | 3 |

- Показать конфигурацию порта TenGigabitEthernet 1/0/1:

```
console# show interfaces switchport TengigabitEthernet 1/0/1
```

```
Gathering information...

Name: te1/0/1
Switchport: enable
Administrative Mode: access
Operational Mode: not present
Access Mode VLAN: 1
Access Multicast TV VLAN: none
Trunking Native Mode VLAN: 1
Trunking VLANs: 1-3
                  4-4094 (Inactive)

General PVID: 1
General VLANs: none
General Egress Tagged VLANs: none
General Forbidden VLANs: none
```

```

General Ingress Filtering: enabled
General Acceptable Frame Type: all
General GVRP status: disabled
Customer Mode VLAN: none
Customer Multicast TV VLANs: none
Private-vlan promiscuous-association primary VLAN: none
Private-vlan promiscuous-association Secondary VLANs: none
Private-vlan host-association primary VLAN: none
Private-vlan host-association Secondary VLAN: none

```

Classification rules:

```

Classification type Group ID VLAN ID
-----

```

5.9.3 Настройка Private VLAN

Технология Private VLAN (PVLAN) позволяет производить разграничение трафика на втором уровне модели OSI между портами коммутатора, которые находятся в одном широковещательном домене.

На коммутаторах может быть сконфигурировано три типа PVLAN портов:

- promiscuous – порт, который способен обмениваться данными между любыми интерфейсами, включая isolated и community-порты PVLAN;
- isolated – порт, который полностью изолирован от других портов внутри одного и того же PVLAN, но не от promiscuous-портов. PVLANы 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 – 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.

Процесс выполнения функции дополнительного разделения портов с помощью технологии Private VLAN представлен на рисунке 83.

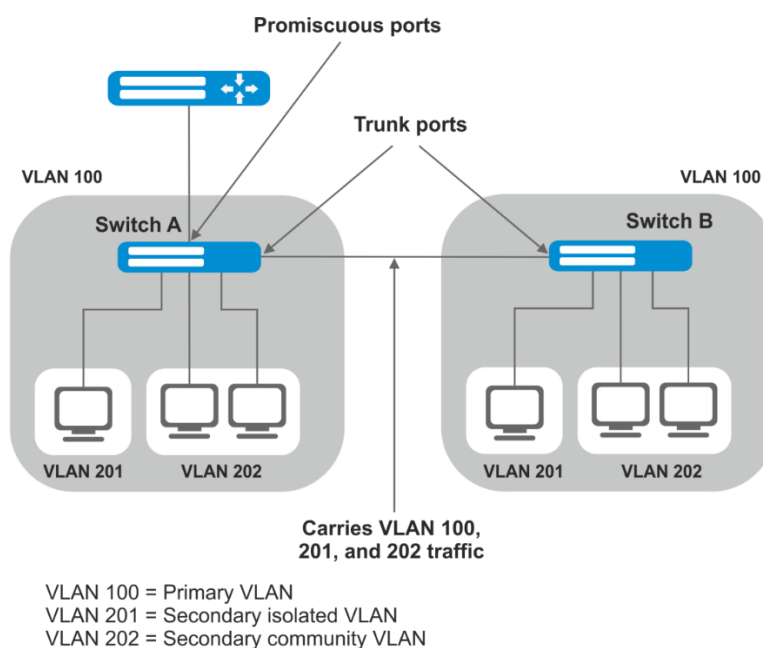


Рисунок 83 – Пример работы технологии Private VLAN

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet, интерфейса Vlan, интерфейса группы портов:

```
console# configure
console(config)# interface {gigabitethernet gi_port | tengigabitethernet
te_port | twentyfivegigabitethernet twe_port | hundredgigabitethernet
hu_port | port-channel group | range {...} | vlan vlan_id}
console(config-if)#
```

Таблица 72 – Команды режима конфигурации интерфейса Ethernet

| Команда | Значение/Значение по умолчанию | Действие |
|---|---|--|
| switchport mode private-vlan {promiscuous host} | - | Задать режим работы порта в VLAN. |
| no switchport mode | | Установить значение по умолчанию. |
| switchport mode private-vlan trunk {promiscuous secondary} | - | Задать режим работы порта в VLAN Trunk. |
| no switchport mode private-vlan trunk | | Установить значение по умолчанию. |
| switchport private-vlan mapping [trunk] primary_vlan [add remove secondary_vlan] | primary_vlan: (1..4094); secondary_vlan: (1..4094) | Добавить (удалить) основную и второстепенные VLAN на promiscuous интерфейс. <input checked="" type="checkbox"/> На один promiscuous интерфейс нельзя добавить больше одной primary vlan. |
| no switchport private-vlan mapping | | Удалить основную и второстепенные VLAN. |
| switchport private-vlan host-association primary_vlan secondary_vlan | primary_vlan: (1..4094) secondary_vlan: (1..4094) | Добавить primary и secondary vlan на host интерфейс. <input checked="" type="checkbox"/> На один host интерфейс нельзя добавить больше одной secondary vlan. |
| no switchport private-vlan host-association | | Удалить основную и второстепенные VLAN. |
| switchport private-vlan association trunk primary_vlan secondary_vlan | primary_vlan: (1..4094); secondary_vlan: (1..4094) | Добавить primary и secondary vlan на интерфейс trunk-secondary. <input checked="" type="checkbox"/> На один promiscuous интерфейс trunk-secondary нельзя добавить больше одной secondary vlan. |
| no switchport private-vlan association trunk | | Удалить основную и второстепенные VLAN. |
| switchport private-vlan trunk allowed vlan add vlan | vlan: (1..4094) | Добавить на PVLAN Trunk-интерфейс VLAN, не участвующей в PVLAN. |
| switchport private-vlan trunk allowed vlan remove vlan | | Удалить на PVLAN Trunk-интерфейсе VLAN, не участвующей в PVLAN. |
| switchport private-vlan trunk native vlan vlan | vlan: (1..4094)/1 | Добавить номер VLAN, не участвующей в PVLAN, в качестве Default VLAN для PVLAN Trunk-интерфейса. |
| no switchport private-vlan trunk native vlan | | Установить значение по умолчанию. |

Таблица 73 – Команды режима конфигурации интерфейса VLAN

| Команда | Значение/Значение по умолчанию | Действие |
|--|--------------------------------|--|
| private-vlan {primary isolated community} | | Включить механизм Private VLAN и задать тип интерфейса. |
| no private-vlan | | Отключить механизм Private VLAN. |
| private-vlan association [add remove] | secondary_vlan (1..4094) | Добавить (удалить) привязку второстепенной VLAN к основной. Настройка применима только для primary VLAN. |
| no private-vlan association | | Удалить привязку второстепенной VLAN к основной. |



Максимальное количество второстепенных VLAN – 256.

Максимальное количество community VLAN, которые могут быть ассоциированы с одной основной VLAN – 8.

Пример настройки интерфейсов коммутатора Switch A (рисунок 70 — Пример работы технологии Private VLAN)

- promiscuous-порт — interface gigabitethernet 1/0/4
- isolated-порт — gigabitethernet 1/0/1
- community-порт — gigabitethernet 1/0/2, 1/0/3.

```
interface gigabitethernet 1/0/1
switchport mode private-vlan host
description Isolate
switchport forbidden default-vlan
switchport private-vlan host-association 100 201
exit
!
interface gigabitethernet 1/0/2
switchport mode private-vlan host
description Community-1
switchport forbidden default-vlan
switchport private-vlan host-association 100 202
exit
!
interface gigabitethernet 1/0/3
switchport mode private-vlan host
description Community-2
switchport forbidden default-vlan
switchport private-vlan host-association 100 202
exit
!
interface gigabitethernet 1/0/4
switchport mode private-vlan promiscuous
description to_Router
switchport forbidden default-vlan
switchport private-vlan mapping 100 add 201-202
exit
!
interface tengigabitethernet 1/0/1
switchport mode trunk
switchport trunk allowed vlan add 100,201-202
description trunk-sw1-sw2
switchport forbidden default-vlan
exit
!
interface vlan 100
name primary
private-vlan primary
private-vlan association add 201-202
exit
!
interface vlan 201
name isolate
private-vlan isolated
exit
!
interface vlan 202
name community
```

Пример настройки интерфейсов при работе технологии

- trunk-isolated порт — interface gigabitethernet 1/0/1;
- trunk-community порт — gigabitethernet 1/0/2, 1/0/3;
- trunk-promiscuous порт — gigabitethernet 1/0/4.

```
interface gigabitethernet 1/0/1
switchport mode private-vlan trunk secondary
description Trunk-Isolated
switchport private-vlan trunk allowed vlan add 301
switchport private-vlan association trunk 100 201
exit
!
interface gigabitethernet 1/0/2
switchport mode private-vlan trunk secondary
description Trunk-Community
switchport private-vlan trunk allowed vlan add 301
switchport private-vlan association trunk 100 202
exit
!
interface gigabitethernet 1/0/3
switchport mode private-vlan trunk secondary
description Trunk-Community
switchport private-vlan trunk allowed vlan add 301
switchport private-vlan trunk native vlan 302
switchport private-vlan association trunk 100 202
exit
!
interface gigabitethernet 1/0/4
switchport mode private-vlan trunk promiscuous
description Trunk-Promiscuous
switchport private-vlan trunk allowed vlan add 301
switchport private-vlan mapping trunk 100 add 201-202
exit
!
interface tengigabitethernet 1/0/1
switchport mode trunk
switchport trunk allowed vlan add 100,201-202
description trunk-sw1-sw2
switchport forbidden default-vlan
exit
!
interface vlan 100
name primary
private-vlan primary
private-vlan association add 201-202
exit
!
interface vlan 201
name isolate
private-vlan isolated
exit
!
interface vlan 202
name community
private-vlan community
```

5.9.4 Настройка интерфейса IP

IP-интерфейс создаётся при назначении IP-адреса на любой из интерфейсов устройства gigabitethernet, tengigabitethernet, hundredgigabitethernet, oob, port-channel или vlan.

Вид запроса командной строки в режиме конфигурации интерфейса IP.

```
console# configure
console(config)# interface ip A.B.C.D
console(config-ip)#
```

Данный режим доступен из режима конфигурации и предназначен для задания параметров конфигурации интерфейса IP.

Таблица 74 – Команды режима конфигурации интерфейса IP

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|-------------------------------------|---------------------------------------|--|
| directed-broadcast | -/выключено | Включает функцию перевода IP directed-broadcast пакета в стандартный широковещательный пакет и разрешает передачу через выбранный интерфейс. |
| no directed-broadcast | | Запрещает трансляцию IP directed-broadcast пакетов. |
| helper-address ip_address | ip_address: A.B.C.D | Включает переадресацию широковещательных UDP-пакетов на определенный адрес. - ip_address – IP-адрес назначения, на который будут перенаправляться пакеты. |
| no helper-address ip_address | | Отключает переадресацию широковещательных UDP-пакетов. |
| ip redirects | -/выключено | Включает генерацию маршрутизатором сообщений ICMP Redirect. |
| no ip redirects | | Отключает отправку ICMP Redirect. |

Примеры выполнения команд

- Включить функцию directed-broadcast:

```
console# configure
console(config)#interface PortChannel 1
console(config-if)#ip address 100.0.0.1 /24
console(config-if)#exit
console(config)# interface ip 100.0.0.1
console(config-ip)# directed-broadcast
```

5.9.5 Selective Q-in-Q

Данный функционал позволяет на основе сконфигурированных правил фильтрации по номерам внутренних VLAN (Customer VLAN) производить добавление внешнего SPVLAN (Service Provider's VLAN), подменять Customer VLAN, а также запрещать прохождение трафика.

Для устройства создается список правил, на основании которого будет обрабатываться трафик.

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet и Port-Channel

Вид запроса командной строки режима конфигурации интерфейса конфигурации:

```
console# configure
console(config)# interface {gigabitethernet gi_port | tengigabitethernet
te_port | twentyfivegigabitethernet twe_port | hundredgigabitethernet
hu_port | port-channel group | range {...}}
console(config-if)#
```

Таблица 75 – Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---|---|
| selective-qinq list ingress add_vlan vlan_id [ingress_vlan ingress_vlan_id] | vlan_id: (1..4094) ingress_vlan_id: (1..4094) | Создает правило, на основании которого к входящему пакету с внешней меткой ingress_vlan_id будет добавляться вторая метка vlan_id. Если ingress_vlan_id не указывать – правило будет применяться ко всем входящим пакетам, к которым не были применены другие правила («правило по умолчанию»). |
| selective-qinq list ingress deny [ingress_vlan ingress_vlan_id] | ingress_vlan_id: (1..4094) | Создает запрещающее правило, на основании которого входящие пакеты с внешней меткой тега ingress_vlan_id будут отбрасываться. Если ingress_vlan_id не указывается – будут отбрасываться все входящие пакеты. |
| selective-qinq list ingress permit [ingress_vlan ingress_vlan_id] | ingress_vlan_id: (1..4094) | Создает разрешающее правило, на основании которого входящие пакеты с внешней меткой тега ingress_vlan_id будут передаваться без изменений. Если ingress_vlan_id не указывается – будут передаваться все входящие пакеты без изменений. |
| selective-qinq list ingress override_vlan vlan_id [ingress_vlan ingress_vlan_id] | vlan_id: (1..4094); ingress_vlan_id: (1..4094) | Создает правило, на основании которого внешняя метка ingress_vlan_id входящего пакета будет заменяться на vlan_id. Если ingress_vlan_id не указывать – правило будет применяться ко всем входящим пакетам. |
| no selective-qinq list ingress [ingress_vlan vlan_id] | vlan_id: (1..4094) | Удаляет указанное правило selective qinq для входящих пакетов. Команда без параметра «ingress_vlan» удаляет правило по умолчанию. |
| selective-qinq list egress override_vlan vlan_id [ingress_vlan ingress_vlan_id] | vlan_id (1..4094); ingress_vlan_id: (1..4094) | Создает правило, на основании которого внешняя метка ingress_vlan_id исходящего пакета будет заменяться на vlan_id. |
| no selective-qinq list egress ingress_vlan vlan_id | vlan_id: (1-4094) | Удаляет список правил selective qinq для исходящих пакетов. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 76 – Команды режима EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---|---|
| show selective-qinq | - | Отображает список правил selective qinq. |
| show selective-qinq interface {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group} | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Отображает список правил selective qinq для указанного порта. |

Примеры выполнения команд

- Создать правило, на основании которого, внешняя метка входящего пакета 11 будет заменяться на 10.

```
console# configure
console(config)# interface tengigabitethernet 1/0/1
console(config-if)# selective-qinq list ingress override vlan 10
ingress-vlan 11
console(config-if)# end
```

5.10 Storm Control для различного трафика (broadcast, multicast, unknown unicast)

«Шторм» возникает вследствие чрезмерного количества broadcast-, multicast-, unknown unicast-сообщений, одновременно передаваемых по сети через один порт, что приводит к перегрузке ресурсов сети и появлению задержек. «Шторм» может возникнуть при наличии «закольцованных» сегментов в сети Ethernet.

Коммутатор измеряет скорость принимаемого широковещательного, многоадресного и неизвестного одноадресного трафика для портов с включенным контролем широковещательного «шторма» и отбрасывает пакеты, если скорость превышает заданное максимальное значение.

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet, интерфейса группы портов:

```
console(config-if)#
```

Таблица 77 – Команды режима конфигурации интерфейса Ethernet

| Команда | Значение/Значение по умолчанию | Действие |
|---|---|--|
| storm-control multicast [registered unregistered] {level level kbps kbps} [trap] [shutdown] | level: (1..100); kbps: (1..10000000) | Включает контроль многоадресного трафика: - registered – зарегистрированного; - unregistered – незарегистрированного. - level – объем трафика в процентах от пропускной способности интерфейса; - kbps – объем трафика. При обнаружении многоадресного трафика интерфейс может быть отключен (shutdown) или добавлена запись в журнал сообщений (trap). |
| no storm-control multicast | | Выключает контроль многоадресного трафика. |
| storm-control multicast [registered unregistered] {pps pps} [trap] [shutdown] | pps: (125.. 19531250) | Включает контроль многоадресного трафика: - registered – зарегистрированного; - unregistered – незарегистрированного. - pps – количество пакетов в секунду. При обнаружении многоадресного трафика интерфейс может быть отключен (shutdown) или добавлена запись в журнал сообщений (trap). |
| no storm-control multicast | | Выключает контроль многоадресного трафика. |
| storm-control unicast {level level kbps kbps} [trap] [shutdown] | level: (1..100); kbps: (1..10000000) | Включает контроль неизвестного одноадресного трафика. - level – объем трафика в процентах от пропускной способности интерфейса; - kbps – объем трафика. При обнаружении неизвестного одноадресного трафика интерфейс может быть отключен (shutdown) или добавлена запись в журнал сообщений (trap). |
| no storm-control unicast | | Выключает контроль одноадресного трафика. |

| | | |
|--|---|--|
| storm-control unicast { pps pps} [trap] [shutdown] | pps: (125.. 19531250) | Включает контроль неизвестного одноадресного трафика. - pps – количество пакетов в секунду. При обнаружении неизвестного одноадресного трафика интерфейс может быть отключен (shutdown) или добавлена запись в журнал сообщений (trap). |
| no storm-control unicast | | Выключает контроль одноадресного трафика. |
| storm-control broadcast {level level kbps kbps} [trap] [shutdown] | level: (1..100); kbps: (1..10000000) | Включает контроль ширококвещательного трафика. - level – объем трафика в процентах от пропускной способности интерфейса; - kbps – объем трафика. При обнаружении ширококвещательного трафика интерфейс может быть отключен (shutdown) или добавлена запись в журнал сообщений (trap). |
| no storm-control broadcast | | Выключает контроль ширококвещательного трафика. |
| storm-control broadcast {pps pps} [trap] [shutdown] | pps: (125.. 19531250) | Включает контроль ширококвещательного трафика. - pps – количество пакетов в секунду. При обнаружении ширококвещательного трафика интерфейс может быть отключен (shutdown) или добавлена запись в журнал сообщений (trap). |
| no storm-control broadcast | | Выключает контроль ширококвещательного трафика. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 78 – Команды режима EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|--|--|
| show storm-control interface [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); tve_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Показывает конфигурацию функции контроля «шторма» для указанного порта либо всех портов. |

Примеры выполнения команд

- Включить контроль ширококвещательного, многоадресного и одноадресного трафика на третьем интерфейсе Ethernet. Установить скорость для контролируемого трафика – 5000 Кб/с: для ширококвещательного, 30% полосы пропускания для всего многоадресного, 70% для неизвестного одноадресного.

```
console# configure
console(config)# interface TengigabitEthernet 1/0/3
console(config-if)# storm-control broadcast kbps 5000 shutdown
console(config-if)# storm-control multicast level 30 trap
console(config-if)# storm-control unicast level 70 trap
```

5.11 Группы агрегации каналов – Link Aggregation Group (LAG)

Коммутаторы обеспечивают поддержку групп агрегации каналов LAG в количестве согласно таблице 9 (строка «Агрегация каналов (LAG)»). Каждая группа портов должна состоять из интерфейсов Ethernet с одинаковой скоростью, работающих в дуплексном режиме. Объединение портов в группу увеличивает пропускную способность канала между взаимодействующими устройствами и повышает отказоустойчивость. Группа портов является для коммутатора одним логическим портом.

Устройство поддерживает два режима работы группы портов – статическая группа и группа, работающая по протоколу LACP. Работа по протоколу LACP описана в соответствующем разделе конфигурации.



Если для интерфейса произведены настройки, то для добавления его в группу следует вернуть настройки по умолчанию.

Добавление интерфейсов в группу агрегации каналов доступно только в режиме конфигурации интерфейса Ethernet.

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

```
console (config-if) #
```

Таблица 79 – Команды режима конфигурации интерфейса Ethernet

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---------------------------------------|--|
| <code>channel-group group mode mode</code> | group: (1..128); mode: (on, auto) | Добавить ethernet-интерфейс в группу портов. - <i>on</i> – добавить порт в канал без LACP; - <i>auto</i> – добавить порт в канал с LACP в режиме «active». |
| <code>no channel-group</code> | | Удалить Ethernet-интерфейс из группы портов. |

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console# configure  
console (config) #
```

Таблица 80 – Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---------------------------------------|---|
| <code>port-channel load-balance {src-dst-mac-ip src-dst-mac src-dst-ip src-dst-mac-ip-port dst-mac dst-ip src-mac src-ip} [mpls-aware]</code> | —/src-dst-mac-ip | Задаёт механизм балансировки нагрузки для стратегии ECMP и для группы агрегированных портов. - src-dst-mac-ip — механизм балансировки основывается на MAC-адресе и IP-адресе; - src-dst-mac — механизм балансировки основывается на MAC-адресе; - src-dst-ip — механизм балансировки основывается на IP-адресе; - src-dst-mac-ip-port — механизм балансировки основывается на MAC-адресе, IP-адресе и TCP/UDP-порте; - dst-mac — механизм балансировки основывается на MAC-адресе получателя; - dst-ip — механизм балансировки основывается на IP-адресе получателя; - src-mac — механизм балансировки основывается на MAC-адресе отправителя; - src-ip — механизм балансировки основывается на IP-адресе отправителя; - mpls-aware — включение парсинга L3/L4-заголовков пакетов с MPLS-метками для всего устройства. Актуально только с режимами балансировки по L3/L4-заголовкам пакета. |
| <code>no port-channel load-balance</code> | | Возврат к настройкам балансировки нагрузки по умолчанию. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 81 – Команды режима EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---------------------------------------|--|
| <code>show interfaces channel-group [group]</code> | group: (1..128) | Показывает информацию по группе каналов. |

5.11.1 Статические группы агрегации каналов

Функцией статических групп LAG является объединение нескольких физических каналов в один, что позволяет увеличить пропускную способность канала и повысить его отказоустойчивость. Для статических групп приоритет использования каналов в объединенном пучке не задается.



Для включения работы интерфейса в составе статической группы используйте команду `channel-group {group} mode on` в режиме конфигурации соответствующего интерфейса.

5.11.2 Протокол агрегации каналов LACP

Функцией протокола Link Aggregation Control Protocol (LACP) является объединение нескольких физических каналов в один. Агрегирование каналов используется для увеличения пропускной способности канала и повышения его отказоустойчивости. LACP позволяет передавать трафик по объединенным каналам в соответствии с заданными приоритетами.



Для включения работы интерфейса по протоколу LACP используйте команду `channel-group {group} mode auto` в режиме конфигурации соответствующего интерфейса.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console (config) #
```

Таблица 82 – Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---------------------------------------|--------------------------------------|
| <code>lasp system-priority value</code> | value: (1..65535)/1 | Устанавливает приоритет системы. |
| <code>no lasp system-priority</code> | | Устанавливает значение по умолчанию. |

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

```
console (config-if) #
```

Таблица 83 – Команды режима конфигурации интерфейса Ethernet

| Команда | Значение/Значение по умолчанию | Действие |
|------------------------------------|---|--|
| lACP timeout {long short} | По умолчанию используется значение long | Устанавливает административный таймаут протокола LACP: - long – длительное время таймаута; - short – малое время таймаута. |
| no lACP timeout | | Устанавливает значение по умолчанию. |
| lACP port-priority value | value: (1..65535)/1 | Устанавливает приоритет интерфейса Ethernet. |
| no lACP port-priority | | Устанавливает значение по умолчанию. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 84 – Команды режима EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|---|---|--|
| show lACP {gigabitEthernet gi_port tengigabitEthernet te_port twentyfivegigabitEthernet twe_port hundredgigabitEthernet hu_port } [parameters statistics protocol-state] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Показывает информацию о протоколе LACP для интерфейса Ethernet. Если дополнительные параметры не используются, то будет показана вся информация. - parameters – показывает параметры настройки протокола; - statistics – показывает статистику работы протокола; - protocol-state – показывает состояние работы протокола. |
| show lACP port-channel [group] | group: (1..128) | Показывает информацию о протоколе LACP для группы портов. |

Примеры выполнения команд

- Создать первую группу портов, работающую по протоколу LACP и включающую два интерфейса Ethernet – 3 и 4. Скорость работы группы – 1000 Мбит/с. Установить приоритет системы – 6, приоритеты 12 и 13 для портов 3 и 4 соответственно.

```
console# configure
console(config)# lACP system-priority 6
console(config)# interface port-channel 1
console(config-if)# speed 10000
console(config-if)# exit
console(config)# interface TengigabitEthernet 1/0/3
console(config-if)# speed 10000
console(config-if)# channel-group 1 mode auto
console(config-if)# lACP port-priority 12
console(config-if)# exit
console(config)# interface TengigabitEthernet 1/0/4
console(config-if)# speed 10000
console(config-if)# channel-group 1 mode auto
console(config-if)# lACP port-priority 13
console(config-if)# exit
```

5.11.3 Настройка технологии Multi-Switch Link Aggregation Group (MLAG)

Как и LAG, виртуальные LAG позволяют объединить одну или несколько Ethernet-линий для увеличения скорости и обеспечения отказоустойчивости. MLAG так же известна как VPC (Virtual port-channel). При обычном LAG агрегированные линии должны быть на одном физическом

устройстве, в случае же с VPC агрегированные линии находятся на разных физических устройствах. Функция VPC позволяет соединить два физических устройства в одно виртуальное.



При настройке VPC на одноранговых коммутаторах должна быть одинаковая версия программного обеспечения.



VPC Port-Channel контролируются только коммутатором с ролью Primary, коммутатор Secondary использует настройки Primary.



Нельзя использовать настройку `switchport forbidden default-vlan` для peer-link, так как трафик протокола VPC ходит untagged в default vlan.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 85 — Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--------------------------------------|--------------------------------|--|
| <code>vpc domain domain_id</code> | domain_id: (1..255) | Создает VPC-домен. На одном устройстве может быть создан только один домен VPC. На парных устройствах должен быть одинаковый VPC-домен. |
| <code>no vpc domain domain_id</code> | | Удаляет VPC-домен с устройства. |
| <code>vpc group group_id</code> | group_id: (1..63) | Создает VPC-группу. Для каждого агрегированного интерфейса должна быть создана отдельная VPC-группа. На парных устройствах номера VPC-групп должны совпадать. Суммарное количество VPC-групп не может превысить 48. |
| <code>no vpc group group_id</code> | | Удаляет VPC-группу с устройства. |
| <code>vpc</code> | —/выключено | Включает режим VPC. Используется после конфигурации VPC. |
| <code>no vpc</code> | | Выключает режим VPC. |

Команды режима конфигурации VPC

Вид запроса командной строки режима конфигурации VPC:

```
console(config)# vpc domain domain_id
console(config-vpcdomain)#
```

Таблица 86 — Команды режима конфигурации VPC

| Команда | Значение/Значение по умолчанию | Действие |
|------------------------------|--------------------------------|--|
| <code>peer link group</code> | group: (1..48) | Назначает Port-Channel в качестве peer-link. |
| <code>no peer link</code> | | Исключает Port-Channel из участия в VPC. |
| <code>peer detection</code> | —/выключено | Включает peer detection protocol. Peer-detection — дополнительный механизм, обеспечивающий функционирование VPC в случае обрыва peer-link. Поэтому запрещается использование peer-link для организации интерфейса peer-detection. |

| | | |
|--|-------------------------------|--|
| no peer detection | | Выключает peer detection protocol. |
| peer detection interval msec | msec: (200..4000)/700 ms | Задает интервал отправки сообщений peer detection protocol. |
| no peer detection interval | | Устанавливает значение по умолчанию. |
| peer detection timeout msec | msec: (700..14000)/3500ms | Задать время ожидания ответа peer detection protocol. |
| no peer detection timeout | | Устанавливает значение по умолчанию. |
| peer detection ipaddr dest_ipaddress source_ipaddress [port udp_port] | udp_port: (1..65535)/50000 | Настраивает IP-адрес получателя пакетов, IP-адрес отправителя и UDP порт для peer detection protocol. |
| no peer detection ipaddr | | Устанавливает значение по умолчанию. |
| peer keepalive | — | Включает службу keepalive. |
| no peer keepalive | | Выключает службу keepalive. |
| peer keepalive timeout sec | sec: (2..15)/5 | Задать время ожидания ответа на запрос целостности peer-link. |
| no peer keepalive timeout | | Устанавливает значение по умолчанию. |
| role priority value | value: (1..255)/100 | Устанавливает приоритет устройства. Устройство с меньшим значением будет назначено Primary. |
| no role priority | | Устанавливает значение по умолчанию. |
| system mac-addr mac_address | — | Устанавливает MAC-адрес системы для отправки в VPC порты. |
| no system mac-addr | | Устанавливает значение по умолчанию. |
| system priority value | value: (1..65535)/32767 | Устанавливает приоритет системы для отправки в VPC порты. Должен быть одинаковый на обоих устройствах. |
| no system | | Устанавливает значение по умолчанию. |

Команды режима конфигурации VPC

Вид запроса командной строки режима конфигурации VPC-group:

```
console(config)# vpc group group-id
console(config-group)#
```

Таблица 87 — Команды режима конфигурации VPC

| Команда | Значение/Значение по умолчанию | Действие |
|----------------------------|---------------------------------------|--|
| domain domain_id | domain_id: (1..255) | Устанавливает VPC-group членом VPC-домена. |
| no domain domain_id | | Исключает VPC-group из VPC-домена. |
| vpc-port group | group: (1..48) | Добавляет Port-Channel в VPC-группу. |
| no vpc-port group | | Исключает Port-Channel из VPC-группы. |

Команды режима EXES

Вид запроса командной строки режима EXES:

```
console#
```

Таблица 88 — Команды режима EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---------------------------------------|---|
| <code>show vpc</code> | — | Отображает информацию о конфигурации VPC. |
| <code>show vpc group id</code> | — | Отображает информацию о текущем состоянии VPC Group id. |
| <code>show vpc peer-detection</code> | — | Отображает состояние службы peer detection protocol. |
| <code>show vpc role</code> | — | Отображает информацию о роли устройства. |
| <code>show vpc statistics peer { keepalive link detection }</code> | — | Отображает состояние счетчиков службы VPC. |

5.12 Настройка IPv4-адресации

В данном разделе описаны команды для настройки статических параметров IP-адресации, таких как IP-адрес, маска подсети, шлюз по умолчанию. Настройка протоколов DNS и ARP описана в соответствующих разделах документации.

Команды режима конфигурации интерфейса Ethernet, интерфейса группы портов, VLAN, Loopback

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet, интерфейса группы портов, интерфейса VLAN, интерфейса Loopback.

```
console (config-if) #
```

Таблица 89 – Команды режима конфигурации интерфейса

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---------------------------------------|--|
| <code>ip address ip_address {mask prefix_length}</code> | prefix_length: (8..32) | Назначение заданному интерфейсу IP-адреса и маски подсети. <input checked="" type="checkbox"/> Значение маски может быть записано либо в формате X.X.X.X, либо в формате /N, где N – количество единиц в двоичном представлении маски. |
| <code>no ip address [IP_address]</code> | | Удаление IP-адреса интерфейса. |
| <code>ip address dhcp</code> | - | Получение IP-адреса для настраиваемого интерфейса от DHCP-сервера. <input checked="" type="checkbox"/> Не используется для loopback-интерфейса. |
| <code>no ip address dhcp</code> | | Запрет использования протокола DHCP для получения IP-адреса выбранным интерфейсом. |
| <code>ip unnumbered {vlan vlan_id loopback loop-back_id}</code> | vlan_id: (1..4094); loopback_id: (1) | Разрешает конфигурируемому интерфейсу заимствовать IP-адреса VLAN и Loopback-интерфейса. |
| <code>no ip unnumbered</code> | | Отключает функцию заимствования адреса. |
| <code>ip icmp unreachable disable</code> | -/включено | Выключение отправки icmp unreachable. |
| <code>no ip icmp unreachable disable</code> | | Включение отправки icmp unreachable. |
| <code>ip vrf {vrf_name}</code> | vrf_name: (1..32) символа | Добавление интерфейса в указанный VRF. <input checked="" type="checkbox"/> Для интерфейса OOB и дефолтной VLAN перед добавлением в VRF необходимо ввести «no ip address dhcp». Также «no ip address dhcp» нужно повторять при очередных сменах VRF. |
| <code>no ip vrf</code> | | Получение IP-адреса для настраиваемого интерфейса от DHCP-сервера. <input checked="" type="checkbox"/> Удаление интерфейса из ранее указанного VRF. |

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console (config) #
```

Таблица 90 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--|---------------------------------------|--|
| ip default-gateway <i>ip_address</i> | -/шлюз по умолчанию | Задаёт для коммутатора адрес шлюза по умолчанию. |
| no ip default-gateway | не задан | Удаляет назначенный адрес шлюза по умолчанию. |
| ip helper-address { <i>ip_interface</i> all} <i>ip_address</i> [<i>udp_port_list</i>] | -/выключено | Включает переадресацию широковещательных UDP-пакетов на определённый адрес. - <i>ip_interface</i> – IP-адрес интерфейса, для которого выполняется настройка; - all – позволяет выбрать все IP-интерфейсы устройства; - <i>ip_address</i> – IP-адрес назначения, на который будут перенаправляться пакеты. Значение 0.0.0.0 отключает переадресацию; - <i>udp_port_list</i> – список портов UDP. Широковещательный трафик, направленный на перечисленные в списке порты, подвергается переадресации. Максимальное общее количество портов и адресов на устройство - 128. |
| no ip helper-address { <i>ip_interface</i> all} <i>ip_address</i> | | Отменяет переадресацию на заданных интерфейсах. |

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 91 – Команды режима Privileged EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|---|---|--|
| clear host { <i>*</i> <i>word</i> } | <i>word</i> : (1..158) символов | Удаляет из памяти полученные по протоколу DHCP записи ответов имен интерфейсов и их IP-адресов. * – удалить все соответствия. |
| renew dhcp { <i>gigabitethernet gi_port</i> <i>tengigabitethernet te_port</i> <i>twentyfivegigabitethernet twe_port</i> <i>hundredgigabitethernet hu_port</i> <i>vlan vlan_id</i> <i>port-channel group</i> <i>oob</i> } [force-autoconfig] | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..128) <i>vlan_id</i> : (1..4094) | Отправляет запрос к DHCP-серверу на обновление IP-адреса. - force-autoconfig – при обновлении IP-адреса загружается конфигурация с TFTP-сервера. |
| show ip helper-address | - | Отображает таблицу переадресации широковещательных UDP-пакетов. |
| show ip unnumbered interface [<i>vlan vlan_id</i>] | <i>vlan_id</i> : (1..4094) | Показывает конфигурацию <code>ip unnumbered</code> для указанного интерфейса. |

Команды режима EXEC

Вид запроса командной строки в режиме Exec:

```
console>
```

Таблица 92 – Команды режима EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---|---|
| show ip interface [vrf vrf_name all] gigabitethernet gi_port te gigabitethernet te_port hundredgigabitethernet hu_port port-channel group loopback loopback_id vlan vlan_id tunnel tunnel oob] | vrf_name: (1..32) символа; te_port: (1..8/0/1..48); group: (1..128); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); loopback_id : (1...64); tunnel: (1..16); vlan_id: (1..4094) | Показывает конфигурацию IP-адресации для указанного интерфейса или области виртуальной маршрутизации (VRF). |

5.13 Настройка Green Ethernet

Green Ethernet – технология, позволяющая снизить энергопотребление устройства за счет отключения питания для неактивных электрических портов и изменения уровня передаваемого сигнала в зависимости от длины кабеля.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 93 – Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---------------------------------------|---|
| green-ethernet energy-detect | -/выключен | Включает энергосберегающий режим для неактивных портов. |
| no green-ethernet energy-detect | | Отключает энергосберегающий режим для неактивных портов. |
| green-ethernet short-reach | -/выключен | Включает энергосберегающий режим для портов, к которым подключаются устройства с длиной кабеля подключения меньше порогового значения, устанавливаемого с помощью команды green-ethernet short-reach threshold . |
| no green-ethernet short-reach | | Отключает энергосберегающий режим на основании длины кабеля. |

Команды режима конфигурации интерфейса

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

```
console(config-if)#
```

Таблица 94 – Команды режима конфигурации интерфейса Ethernet

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---------------------------------------|--|
| green-ethernet energy-detect | -/Включен | Включает энергосберегающий режим для интерфейса. |
| no green-ethernet energy-detect | | Отключает энергосберегающий режим для интерфейса. |
| green-ethernet short-reach | -/Включен | Включает энергосберегающий режим на основании длины кабеля. |
| no green-ethernet short-reach | | Отключает энергосберегающий режим на основании длины кабеля. |

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 95 – Команды режима Privileged EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|--|--|---|
| show green-ethernet [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port detailed] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Отображает статистику green-ethernet. |
| green-ethernet power-meter reset | - | Сбрасывает счетчик измерителя мощности. |

Примеры выполнения команд

- Отобразить статистику green-ethernet:

```
console# show green-ethernet detailed
```

```
Energy-Detect mode: Enabled
Short-Reach mode: Enabled
Disable Port LEDs mode: Disabled
Power Savings: 0% (0.00W out of maximum 0.00W)
Cumulative Energy Saved: 0 [Watt*Hour]
* Estimated Annual Power saving: NA [Watt*Hour]
Short-Reach cable length threshold: 50m

* Annual estimate is based on the saving during the previous week
NA - information for previous week is not available
```

| Port | Energy-Detect | | | Short-Reach | | | | VCT Cable Length |
|----------|---------------|------|---------|-------------|-------|------|--------|------------------|
| | Admin | Oper | Reason | Admin | Force | Oper | Reason | |
| te1/0/1 | on | off | Unknown | on | off | off | NP | |
| te1/0/3 | on | off | LT | on | off | off | LT | |
| te1/0/4 | on | off | LT | on | off | off | LT | |
| te1/0/5 | on | off | LT | on | off | off | LT | |
| te1/0/6 | on | off | LT | on | off | off | LT | |
| te1/0/7 | on | off | LT | on | off | off | LT | |
| te1/0/8 | on | off | LT | on | off | off | LT | |
| te1/0/9 | on | off | LT | on | off | off | LT | |
| te1/0/10 | on | off | LT | on | off | off | LT | |
| te1/0/11 | on | off | LT | on | off | off | LT | |
| te1/0/12 | on | off | LT | on | off | off | LT | |

5.14 Настройка IPv6-адресации

5.14.1 Протокол IPv6

Коммутаторы поддерживают работу по протоколу IPv6. Поддержка IPv6 является важным достоинством, поскольку протокол IPv6 призван, в перспективе, полностью заменить адресацию протокола IPv4. По сравнению с IPv4 протокол IPv6 имеет расширенное адресное пространство – 128

бит вместо 32. Адрес IPv6 представляет собой 8 блоков, разделенных двоеточием, в каждом блоке 16 бит, записанных в виде четырех шестнадцатеричных чисел.

Помимо увеличения адресного пространства протокол IPv6 имеет иерархическую схему адресации, обеспечивает агрегацию маршрутов, упрощает таблицу маршрутизации, при этом эффективность работы маршрутизатора повышается за счет механизма обнаружения соседних узлов.

Локальные адреса IPv6 (IPv6Z) в коммутаторе назначаются интерфейсам, поэтому при использовании IPv6Z-адресов в синтаксисе команд используется следующий формат:

`<ipv6-link-local-address>%<interface-name>`

где:

interface-name – имя интерфейса:

interface-name = `vlan<integer>` | `ch<integer>` | `<physical-port-name>`

integer = `<decimal-number>` | `<integer><decimal-number>`

decimal-number = 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9

physical-port-name = **tengigabitethernet** (1..8/0/1..32)



Если значение группы или нескольких групп подряд в адресе протокола IPv6 равно нулю – 0000, то данные группы могут быть опущены.

Например, адрес FE40:0000:0000:0000:0000:AD21:FE43 может быть сокращен до FE40::AD21:FE43. Сокращению не могут быть подвергнуты 2 разделенные нулевые группы из-за возникновения неоднозначности.



EUI-64 – это идентификатор, созданный на базе MAC-адреса интерфейса, являющийся 64 младшими битами IPv6-адреса. MAC-адрес разбивается на две части по 24 бита, между которыми добавляется константа FFFE.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

`console(config)#`

Таблица 96 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|---|
| <code>ipv6 default-gateway</code> <i>ipv6_address</i> | | Задаёт значение локального адреса IPv6-шлюза по умолчанию. |
| <code>no ipv6 default-gateway</code> <i>ipv6_address</i> | | Удаляет настройки IPv6-шлюза по умолчанию. |
| <code>ipv6 neighbor</code> <i>ipv6_address</i> { <code>gigabitethernet</code> <i>gi_port</i> <code>tengigabitethernet</code> <i>te_port</i> <code>twentyfivegigabitethernet</code> <i>twe_port</i> <code>hundredgigabitethernet</code> <i>hu_port</i> <code>port-channel group</code> <code>vlan</code> <i>vlan_id</i> } <i>mac_address</i> | <code>gi_port</code> : (1..8/0/1..48); <code>te_port</code> : (1..8/0/1..12); <code>twe_port</code> : (1..8/0/1..120); <code>hu_port</code> : (1..8/0/1..32); <code>group</code> : (1..128); <code>vlan_id</code> : (1..4094) | Создаёт статическое соответствие между MAC-адресом соседнего устройства и его IPv6-адресом. - <i>ipv6_address</i> – IPv6-адрес; - <i>mac_address</i> – MAC-адрес. |

| | | |
|--|---|---|
| no ipv6 neighbor [<i>ipv6_address</i>] [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet <i>twe_port </i> hundredgigabitethernet <i>hu_port port-channel group </i> vlan vlan_id] | | Удаляет статическое соответствие между MAC-адресом соседнего устройства и его IPv6-адресом. |
| ipv6 icmp error-interval <i>milliseconds [bucketsize]</i> | milliseconds: (0..2147483647)/100; | Задаёт ограничение скорости для ICMPv6-сообщений об ошибках. |
| no ipv6 icmp error-interval | bucketsize: (1..200)/10 | Устанавливает значение по умолчанию. |
| ipv6 route prefix/prefix_length {gateway} [metric] [distance <i>distance]</i> | prefix: X:X:X::X; prefix_length: (0..128); metric: (1..65535)/1; distance (1..255)/1 | Добавление статического маршрута IPv6 - <i>prefix</i> – сеть назначения; - <i>prefix_length</i> – префикс маски сети (количество единиц в маске); - <i>gateway</i> – шлюз для доступа к сети назначения; - <i>metric</i> – метрика для данного маршрута; - <i>distance</i> – административная дистанция маршрута. |
| no ipv6 route <i>prefix/prefix_length [gateway]</i> | | Удаление статического маршрута IPv6. |
| ipv6 unicast-routing | -/выключено | Включает перенаправление одноадресных пакетов. |
| no ipv6 unicast-routing | | Отключает перенаправление одноадресных пакетов. |
| ipv6 distance {ospf {inter-as intra-as} static} distance | distance (1..255)/static:1, OSPF intra-as:30, OSPF inter-as:110 | Устанавливает значение административной дистанции (AD) для всех маршрутов указанного типа. - ospf inter-as – устанавливает значение AD для межзональных маршрутов, принятых по протоколу OSPF; - ospf intra-as – устанавливает значение AD для внутризональных маршрутов, принятых по протоколу OSPF; - static – устанавливает значение AD для статических маршрутов. |
| no ipv6 distance {ospf {inter-as intra-as} static} | | Устанавливает значение по умолчанию. |

Команды режима конфигурации интерфейса (VLAN, Ethernet, Port-Channel)

Вид запроса командной строки режима конфигурации интерфейса:

```
console (config-if) #
```

Таблица 97 – Команды режима конфигурации интерфейса (Ethernet, VLAN, Port-channel)

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|--|
| ipv6 enable | -/выключено | Включает поддержку IPv6 на интерфейсе. |
| no ipv6 enable | | Отключает поддержку IPv6 на интерфейсе. |
| ipv6 address autoconfig | По умолчанию автоматическая конфигурация включена, адреса не назначены. | Включение автоматической конфигурации IPv6-адресов на интерфейсе. Адреса настраиваются в зависимости от префиксов, которые получены в сообщениях «Router Advertisement». |
| no ipv6 address autoconfig | | Устанавливает значение по умолчанию. |
| ipv6 address <i>ipv6_address/prefix_length</i> link-local | По умолчанию значение локального адреса: (FE80::EUI64) | Задаёт локальный IPv6-адрес интерфейса. Старшие биты локальных IP-адресов в IPv6 – FE80:: |
| no ipv6 address <i>[ipv6_address/prefix-length</i> link-local] | | Удаляет локальный IPv6-адрес. |
| ipv6 nd dad attempts <i>attempts_number</i> | (0..600)/1 | Задаёт количество сообщений-требований, передаваемых интерфейсом взаимодействующему устройству в случае обнаружения дубликации (коллизии) IPv6-адреса. |
| no ipv6 nd dad attempts | | Возвращает значение по умолчанию. |

| | | |
|---------------------------------|-------------------|--|
| ipv6 unreachable | -/enabled | Включение ICMPv6 сообщений о недостижимости адресата при передаче пакетов на определенный интерфейс. |
| no ipv6 unreachable | | Устанавливает значение по умолчанию. |
| ipv6 mld version version | version: (1..2)/2 | Определение версии протокола MLD для интерфейса. |
| no ipv6 mld version | | Устанавливает значение по умолчанию. |

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 98 – Команды режима Privileged EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|--|
| show ipv6 interface [brief gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port port-channel group loopback vlan vlan_id] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); tve_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128); vlan_id: (1..4094) | Показывает настройки протокола IPv6 для указанного интерфейса. |
| show ipv6 route [summary local connected static ospf icmp nd ipv6_address/ipv6_prefix interface { gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port port-channel group loopback vlan vlan_id}] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); tve_port: (1..8/0/1..120); group: (1..128); hu_port: (1..8/0/1..32); vlan_id: (1..4094) | Показывает таблицу IPv6-маршрутов. |
| show ipv6 neighbors {ipv6_address gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port port-channel group vlan vlan_id} | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); tve_port: (1..8/0/1..120); group: (1..128); hu_port: (1..8/0/1..32); vlan_id: (1..4094) | Показывает информацию о соседних IPv6-устройствах, содержащуюся в кэше. |
| clear ipv6 neighbors | - | Очищает кэш, содержащий информацию о соседних устройствах, работающих по протоколу IPv6. Информация о статических записях сохраняется. |
| show ipv6 distance | - | Показать значение административной дистанции для различных источников маршрута. |

5.15 Настройка протоколов

5.15.1 Настройка протокола DNS – системы доменных имен

Основной задачей протокола DNS является определение IP-адреса узла сети (хоста) по запросу, содержащему его доменное имя. База данных соответствий доменных имен узлов сети и соответствующих им IP-адресов ведется на DNS-серверах.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console (config) #
```

Таблица 99 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--|---------------------------------------|---|
| ip domain lookup | -/включено | Разрешает использование протокола DNS. |
| no ip domain lookup | | Запрещает использование протокола DNS. |
| ip name-server {server1_ipv4_address server1_ipv6_address server1_ipv6z_address} [server2_address] [...] | - | Определяет IPv4/IPv6-адреса для доступных DNS-серверов. |
| no ip name-server {server1_ipv4_address server1_ipv6_address server1_ipv6z_address} [server2_address] [...] | | Удаляет IP-адрес DNS-сервера из списка доступных. |
| ip domain name name | name: (1..158) символов | Определяет доменное имя по умолчанию, которое будет использоваться программой, для дополнения неправильных доменных имен (доменных имен без точки). Для доменных имен без точки в конец имени будет добавляться точка и указанное в команде доменное имя. |
| no ip domain name | | Удаляет доменное имя по умолчанию. |
| ip host name address1 [address2 ... address4] | name: (1..158) символов | Определяет статические соответствия имен узлов сети IP-адресам, добавляет установленное соответствие в кэш. Функция локального DNS. Можно определить до восьми IP-адресов на одно имя. |
| no ip host name | | Удаляет статические соответствия имен узлов сети IP-адресам. |

Команды режима EXEC

Вид запроса командной строки в режиме EXEC:

```
console#
```

Таблица 100 – Команды режима EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|------------------------------|---------------------------------------|---|
| clear host {name *} | name: (1..158) символов | Удаляет запись соответствия имени узла сети IP-адресу кэша либо все записи (*). |
| show hosts [name] | name: (1..158) символов | Отображает доменное имя по умолчанию, список DNS-серверов, статические и кэшированные соответствия имен узлов сети и IP-адресов. При использовании в команде имени узла сети, отображается соответствующий ему IP-адрес. |

Примеры использования команд

Использовать DNS-сервера по адресам 192.168.16.35 и 192.168.16.38, установить доменное имя по умолчанию – mes:

```
console# configure
console(config)# ip name-server 192.168.16.35 192.168.16.38
console(config)# ip domain name mes
```

Установить статическое соответствие: узел сети с именем eltex.mes имеет IP-адрес 192.168.16.39:

```
console# configure
console(config)# ip host eltex.mes 192.168.16.39
```

5.15.2 Настройка протокола ARP

ARP (Address Resolution Protocol — протокол разрешения адресов) — протокол канального уровня, выполняющий функцию определения MAC-адреса на основании содержащегося в запросе IP-адреса.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 101 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|---|--|---|
| arp <i>ip_address hw_address</i> [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group vlan <i>vlan_id</i> oob] | формат ip_addr: A.B.C.D; формат hw_address: H.H.H H:H:H:H:H:H H-H-H-H-H-H; te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128); vlan_id: (1..4094) | Добавляет статическую запись соответствия IP- и MAC-адресов в таблицу ARP для указанного в команде интерфейса. - <i>ip_address</i> – IP-адрес; - <i>hw_address</i> – MAC-адрес. |
| no arp <i>ip_address</i> [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group vlan <i>vlan_id</i> oob] | | Удаляет статическую запись соответствия IP- и MAC-адресов из таблицы ARP для указанного в команде интерфейса. |
| arp timeout <i>sec</i> | sec: (1..40000000)/60000 | Настраивает время жизни динамических записей в таблице ARP (сек). |
| no arp timeout | сек | Устанавливает значение по умолчанию. |
| ip arp proxy disable | | Отключает режим проксирования ARP-запросов для коммутатора. |
| no ip arp proxy disable | -/отключён | Включает режим проксирования ARP-запросов для коммутатора. |

| | | |
|---|---|---|
| anycast-gateway mac-address <i>mac_address</i> | формат <i>mac_address</i> : Н.Н.Н или Н:Н:Н:Н:Н:Н или Н-Н-Н-Н-Н-Н / виртуальный MAC- адрес не задан | Задаёт виртуальный MAC-адрес, который заменяет базовый MAC-адрес коммутатора в исходящих ARP-сообщениях. - <i>mac_address</i> – MAC-адрес. <input checked="" type="checkbox"/> В качестве виртуального MAC-адреса нельзя использовать следующие MAC-адреса: multicast, broadcast, VRRP MAC, базовый MAC-адрес коммутатора, базовый MAC-адрес какого-либо юнита из стека. |
| no anycast-gateway mac-address | | Устанавливает значение по умолчанию. |

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 102 – Команды режима Privileged EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|---|---|---|
| clear arp-cache | - | Удаляет все динамические записи из ARP-таблицы (команда доступна только для привилегированного пользователя). |
| show arp [<i>ip-address ip_address</i>] [<i>mac-address mac_address</i>] [<i>gigabitethernet gi_port</i> <i>tengigabitethernet te_port</i> <i>twentyfivegigabitethernet twe_port</i> <i>hundredgigabitethernet hu_port</i> <i>port-channel group</i> <i>oob</i>] | формат <i>ip_address</i> : А.В.С.Д формат <i>mac_address</i> : Н.Н.Н или Н:Н:Н:Н:Н:Н или Н-Н-Н-Н-Н-Н; <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..128) | Показывает записи ARP-таблицы: все записи, фильтр по IP-адресу; фильтр по MAC-адресу; фильтр по интерфейсу. - <i>ip_address</i> – IP-адрес; - <i>mac_address</i> – MAC-адрес. |
| show arp configuration | - | Показывает глобальную конфигурацию ARP и конфигурацию ARP для интерфейсов. |
| show ip anycast-gateway | - | Показывает конфигурацию anycast gateway. |

Команды режима конфигурации интерфейса

Вид запроса командной строки в режиме interface configuration:

```
console(config-if)#
```

Таблица 103 – Команды режима интерфейса Ethernet, группы интерфейсов интерфейса VLAN

| Команда | Значение/Значение по умолчанию | Действие |
|---------------------------|---------------------------------------|---|
| ip proxy-arp | -/включено | Включает режим проксирования ARP-запросов на настраиваемом интерфейсе. |
| no ip proxy-arp | | Отключает режим проксирования ARP-запросов на настраиваемом интерфейсе. |
| anycast-gateway | -/выключено | Включает опцию anycast gateway на интерфейсе. В исходящих ARP-сообщениях базовый MAC-адрес коммутатора заменяется на виртуальный MAC-адрес. <input checked="" type="checkbox"/> Виртуальный MAC-адрес должен быть задан командой anycast-gateway mac-address. |
| no anycast-gateway | | Устанавливает значение по умолчанию. |

Примеры использования команд

Добавить статическую запись в ARP-таблицу: IP-адрес 192.168.16.32, MAC-адрес 0:0:C:40:F:BC, установить время жизни динамических записей в ARP-таблице – 12000 секунд:

```
console# configure
console(config)# arp 192.168.16.32 00-00-0c-40-0f-bc tengigabitethernet
1/0/2
console(config)# arp timeout 12000
```

- Показать содержимое ARP-таблицы:

```
console# show arp
```

| VLAN | Interface | IP address | HW address | status |
|--------|-----------|--------------|-------------------|---------|
| vlan 1 | te0/12 | 192.168.25.1 | 02:00:2a:00:04:95 | dynamic |

5.15.3 Настройка протокола GVRP

GARP VLAN Registration Protocol (GVRP) – протокол VLAN-регистрации. Протокол позволяет распространить по сети идентификаторы VLAN. Основной функцией протокола GVRP является обнаружение информации об отсутствующих в базе данных коммутатора VLAN-сетях при получении сообщений GVRP. Получив информацию об отсутствующих VLAN, коммутатор добавляет ее в свою базу данных.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 104 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|-----------------------|--------------------------------|--|
| gvrp enable | -/выключен | Включает использование протокола GVRP-коммутатором. |
| no gvrp enable | | Выключает использование протокола GVRP-коммутатором. |

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet, интерфейса группы портов:

```
console# configure
console(config)# interface {gigabitethernet gi_port | tengigabitethernet
te_port | twentyfivegigabitethernet twe_port | hundredgigabitethernet
hu_port | port-channel group}
console(config-if)#
```

Таблица 105 – Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

| Команда | Значение/Значение по умолчанию | Действие |
|--------------------|--------------------------------|--|
| gvrp enable | -/выключен | Включает использование протокола GVRP на настраиваемом интерфейсе. |

| | | |
|-------------------------------------|--|---|
| no gvrp enable | | Выключает использование протокола GVRP на настраиваемом интерфейсе. |
| gvrp vlan-creation-forbid | -/разрешено | Запрещает динамическое изменение или создание VLAN для настраиваемого интерфейса. |
| no gvrp vlan-creation-forbid | | Разрешает динамическое изменение или создание VLAN для настраиваемого интерфейса. |
| gvrp registration-forbid | По умолчанию создание и регистрация VLAN на интерфейсе разрешена | Выполняет снятие регистрации для всех VLAN и не допускает создания или регистрации новых VLAN на данном интерфейсе. |
| no gvrp registration-forbid | | Устанавливает значение по умолчанию. |

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 106 – Команды режима Privileged EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|---|---|--|
| clear gvrp statistics [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port port-channel group] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); tve_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Очищает накопленную статистику протокола GVRP. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 107 – Команды режима EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|--|--|--|
| show gvrp configuration [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port port-channel group detailed] | | Показывает конфигурацию протокола GVRP для указанного интерфейса, либо для всех интерфейсов. |
| show gvrp statistics [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port port-channel group] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); tve_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Показывает накопленную статистику по протоколу GVRP для указанного интерфейса, либо для всех интерфейсов. |
| show gvrp error-statistics [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port port-channel group] | | Показывает статистику по ошибкам при работе протокола GVRP для указанного интерфейса, либо для всех интерфейсов. |

5.15.4 Механизм обнаружения петель (loopback-detection)

Данный механизм позволяет устройству отслеживать закольцованные порты. Петля на порту обнаруживается путём отсылки коммутатором кадра (frame) с MAC-адресом порта коммутатора в поле Source MAC и широковещательным (по умолчанию) адресом в поле Destination MAC.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console (config) #
```

Таблица 108 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--|--------------------------------|--|
| loopback-detection enable | -/выключено | Включает механизм обнаружения петель для коммутатора. |
| no loopback-detection enable | | Восстанавливает значение по умолчанию. |
| loopback-detection interval seconds | seconds: (10..60)/30 секунд | Устанавливает интервал между loopback-кадрами. - <i>seconds</i> – интервал времени между LBD-кадрами. |
| no loopback-detection interval | | Восстанавливает значение по умолчанию. |

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet, интерфейса группы портов:

```
console# configure
console (config) # interface {tengigabitethernet te_port |
twentyfivegigabitethernet twe_port | hundredgigabitethernet hu_port |
port-channel group}
console (config-if) #
```

Таблица 109 – Команды режима конфигурации интерфейса Ethernet, группы интерфейсов, интерфейса VLAN

| Команда | Значение/Значение по умолчанию | Действие |
|-------------------------------------|--------------------------------|--|
| loopback-detection enable | -/выключен | Включает механизм обнаружения петель на порту. |
| no loopback-detection enable | | Восстанавливает значение по умолчанию. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 110 – Команды режима EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|--|--|
| <code>show loopback-detection [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group detailed]</code> | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128). | Отображает состояние механизма loopback-detection. |

5.15.5 Семейство протоколов STP (STP, RSTP, MSTP), PVSTP+, RPVSTP+

Основной задачей протокола STP (Spanning Tree Protocol) является приведение сети Ethernet с множественными связями к древовидной топологии, исключающей циклы пакетов. Коммутаторы обмениваются конфигурационными сообщениями, используя кадры специального формата, и выборочно включают и отключают передачу на порты.

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

Протокол Multiple STP (MSTP) является наиболее современной реализацией STP, поддерживающей использование VLAN. MSTP предполагает конфигурацию необходимого количества экземпляров связующего дерева (spanning tree) вне зависимости от числа групп VLAN на коммутаторе. Каждый экземпляр может содержать несколько групп VLAN. Недостатком протокола MSTP является то, что на всех коммутаторах, взаимодействующих по MSTP, должны быть одинаково сконфигурированы группы VLAN.



Максимально допустимое количество экземпляров MSTP указано в таблице 9.

Механизм Multiprocess STP предназначен для создания независимых деревьев STP/RSTP/MSTP на портах устройства. Изменения состояния отдельного дерева не оказывают влияния на состояние других деревьев, что позволяет повысить устойчивость сети и сократить время перестроения дерева в случае отказов. При конфигурировании следует исключить возможность возникновения колец между портами-членами разных деревьев. Для обслуживания изолированных деревьев в системе создаётся отдельный процесс на каждое дерево. С процессом сопоставляются порты устройства, принадлежащие дереву.

5.15.5.1 Настройка протокола STP, RSTP

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 111 – Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|-------------------------------|---------------------------------------|---|
| <code>spanning-tree</code> | -/включено | Разрешает использование коммутатором протокола STP. |
| <code>no spanning-tree</code> | | Запрещает использование коммутатором протокола STP. |

| | | |
|---|--------------------------------|--|
| spanning-tree mode {stp rstp mstp pvst rapid-pvst} | -/RSTP | Устанавливает режим работы протокола STP: - stp – IEEE 802.1D Spanning Tree Protocol; - rstp – IEEE 802.1W Rapid Spanning Tree Protocol; - mstp – IEEE 802.1S Multiple Spanning Tree Protocol; - pvst – Cisco Per Vlan Spanning Tree Protocol; - rapid-pvst – Cisco Rapid Per Vlan Spanning Tree Protocol. |
| no spanning-tree mode | | Устанавливает значение по умолчанию. |
| spanning-tree forward-time seconds | seconds: (4..30)/15 сек | Устанавливает интервал времени, затрачиваемый на прослушивание и изучение состояний перед переключением в состояние передачи. |
| no spanning-tree forward-time | | Устанавливает значение по умолчанию. |
| spanning-tree hello-time seconds | seconds: (1..10)/2 сек | Устанавливает интервал времени между передачами широковещательных сообщений «Hello» к взаимодействующим коммутаторам. |
| no spanning-tree hello-time | | Устанавливает значение по умолчанию. |
| spanning-tree loopback-guard | -/запрещено | Разрешает защиту, выключающую интерфейс при получении своего BPDU. |
| no spanning-tree loopback-guard | | Запрещает защиту, выключающую интерфейс при получении своего BPDU. |
| spanning-tree max-age seconds | seconds: (6..40)/20 сек | Устанавливает время жизни связующего дерева STP. |
| no spanning-tree max-age | | Устанавливает значение по умолчанию. |
| spanning-tree priority prior_val | prior_val: (0..61440)/32768 | Настраивает приоритет связующего дерева STP. Значение приоритета должно быть кратно 4096. |
| no spanning-tree priority | | Устанавливает значение по умолчанию. |
| spanning-tree pathcost method {long short} | -/long | Устанавливает метод определения ценности пути. - long – значение ценности в диапазоне 1..200000000; - short – значение ценности в диапазоне 1..65535. |
| no spanning-tree pathcost method | | Устанавливает значение по умолчанию. |
| spanning-tree bpdu {filtering flooding} | -/flooding | Определяет режим обработки пакетов BPDU-интерфейсом, на котором выключен протокол STP. - filtering – на интерфейсе с выключенным протоколом STP BPDU-пакеты фильтруются; - flooding – на интерфейсе с выключенным протоколом STP нетегированные BPDU-пакеты передаются, тегированные – фильтруются. |
| no spanning-tree bpdu | | Устанавливает значение по умолчанию. |



При задании STP параметров forward-time, hello-time, max-age необходимо выполнение условия: $2*(\text{Forward-Delay} - 1) \geq \text{Max-Age} \geq 2*(\text{Hello-Time} + 1)$.

Команды режима конфигурации интерфейса Ethernet, интерфейса группы портов

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet, интерфейса группы портов:

```
console(config-if) #
```

Таблица 112 – Команды режима конфигурации интерфейса Ethernet, группы портов

| Команда | Значение/Значение по умолчанию | Действие |
|---------------------------------|--|---|
| spanning-tree disable | -/разрешено | Запрещает работу протокола STP на конфигурируемом интерфейсе. |
| no spanning-tree disable | | Разрешает работу протокола STP на конфигурируемом интерфейсе. |
| spanning-tree cost cost | cost: (1..200000000)/см. таблицу 96 | Устанавливает ценность пути через данный интерфейс. - cost – ценность пути. |
| no spanning-tree cost | | Устанавливает значение, определяемое на основании скорости порта и метода определения ценности пути, см.таблицу 113 |

| | | |
|--|--|---|
| spanning-tree port-priority priority | priority: (0..240)/128 | Устанавливает приоритет интерфейса в связующем дереве STP. <input checked="" type="checkbox"/> Значение приоритета должно быть кратно 16. |
| no spanning-tree port-priority | | Устанавливает значение по умолчанию. |
| spanning-tree portfast [auto] | -/auto | Включает режим, в котором порт при поднятии на нем линка сразу становится в состояние передачи, не дожидаясь истечения таймера. - auto – добавляет задержку 3 секунды перед переходом в состояние передачи. |
| no spanning-tree portfast | | Выключает режим моментального перехода в состояние передачи по поднятию «линка». |
| spanning-tree guard root | -/использование глобальной настройки | Включает защиту «корня» для всех связующих деревьев STP выбранного порта. - root – запрещает интерфейсу быть корневым портом коммутатора. |
| no spanning-tree guard | | Использует глобальную настройку. |
| spanning-tree bpduguard {enable disable} | -/выключено | Разрешает защиту, выключающую интерфейс при приеме пакетов BPDU. |
| no spanning-tree bpduguard | | Запрещает защиту, выключающую интерфейс при приеме пакетов BPDU. |
| spanning-tree link-type {point-to-point shared} | -/для дуплексного порта «точка-точка», для полудуплексного – «разветвленный» | Устанавливает протокол RSTP в передающее состояние и определяет тип связи для выбранного порта: - point-to-point – точка-точка; - shared – разветвленный. |
| no spanning-tree link-type | | Устанавливает значение по умолчанию. |
| spanning-tree bpdu {filtering flooding} | - | Определяет режим обработки пакетов BPDU-интерфейсом, на котором выключен протокол STP. - filtering – на интерфейсе с выключенным протоколом STP BPDU пакеты фильтруются; - flooding – на интерфейсе с выключенным протоколом STP нетегированные BPDU-пакеты передаются, тегированные – фильтруются. |
| no spanning-tree bpdu | | Устанавливает значение по умолчанию. |
| spanning-tree mac-address {dot1d dot1ad} | -/dot1d | Изменяет MAC-адрес, с которым отправляются и принимаются BPDU. - dot1d – отправляются и принимаются BPDU с MAC-адресом 01-80-C2-00-00-00; - dot1ad – отправляются и принимаются BPDU с MAC-адресом 01-80-C2-00-00-08. |
| no spanning-tree mac-address | | Устанавливает значение по умолчанию. |
| spanning-tree restricted-tcn | -/прием BPDU с флагом TCN разрешен | Запрещает прием BPDU с флагом TCN. |
| no spanning-tree restricted-tcn | | Разрешает прием BPDU с флагом TCN. |

Таблица 113 – Ценность пути, установленная по умолчанию (spanning-tree cost)

| Интерфейс | Метод определения ценности пути | |
|--------------------------------------|--|--------------|
| | Long | Short |
| GigabitEthernet (1000 Mbps) | 20000 | 4 |
| TenGigabit Ethernet (10000 Mbps) | 2000 | 2 |
| TwentyFiveGigaEthernet (25000 Mbps) | 800 | 1 |
| FortygigabitEthernet (40000 Mbps) | 500 | 1 |
| HundredGigabitEthernet (100000 Mbps) | 200 | 1 |



Для интерфейсов Port-channel начальная стоимость определяется стоимостью первого линка, вошедшего в состав Port-channel. При добавлении активных линков, начальная стоимость Port-channel делится на их количество.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 114 – Команды режима Privileged EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|--|--|
| show spanning-tree [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Показывает состояние протокола STP. |
| show spanning-tree detail [active blockedports] | - | Показывает подробную информацию о настройках протокола STP, информацию об активных или заблокированных портах. |
| clear spanning-tree detected-protocols [interface { gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group }] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Перезапускает процесс миграции протокола. Заново происходит пересчёт дерева STP. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 115 – Команды режима EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|--|---|
| show spanning-tree bpdu [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group detailed] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Показывает режим обработки пакетов BPDU на интерфейсах. |

5.15.5.2 Настройка протокола MSTP


Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 116 – Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---------------------------------------|---|
| spanning-tree | -/разрешено | Разрешает использование коммутатором протокола STP. |
| no spanning-tree | | Запрещает использование коммутатором протокола STP. |
| spanning-tree mode { stp rstp mstp } | -/RSTP | Устанавливает режим работы протокола STP. |
| no spanning-tree mode | | Устанавливает значение по умолчанию. |
| spanning-tree pathcost method { long short } | -/long | Устанавливает метод определения ценности пути. - long – значение ценности в диапазоне 1..200000000; - short – значение ценности в диапазоне 1..65535. |

| | | |
|--|--|---|
| no spanning-tree pathcost method | | Устанавливает значение по умолчанию. |
| spanning-tree mst instance_id priority priority | instance_id: (1..63); priority: (0..61440)/32768 | Устанавливает приоритет для данного коммутатора перед остальными, использующими общий экземпляр MSTP. - <i>instance_id</i> – экземпляр MST; - <i>priority</i> – приоритет коммутатора.  Значение приоритета должно быть кратно 4096. |
| no spanning-tree mst instance_id priority | | Устанавливает значение по умолчанию. |
| spanning-tree mst max-hops hop_count | hop_count: (1..40)/20 | Устанавливает максимальное количество транзитных участков для пакета BPDU, необходимых для формирования дерева и удержания информации о его строении. Если пакет уже прошел максимальное количество транзитных участков, то на следующем участке он отбрасывается. - <i>hop_count</i> – максимальное количество транзитных участков для пакета BPDU. |
| no spanning-tree mst max-hops | | Устанавливает значение по умолчанию. |
| spanning-tree mst configuration | - | Вход в режим конфигурации протокола MSTP. |

Команды режима конфигурации протокола MSTP

Вид запроса командной строки в режиме конфигурации протокола MSTP:

```
console# configure
console (config)# spanning-tree mst configuration
console (config-mst)#
```

Таблица 117 – Команды режима конфигурации протокола MSTP

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|---|
| instance instance_id vlan vlan_range | instance_id:(1..63); vlan_range: (1..4094) | Создает соответствие между экземпляром протокола MSTP и группами VLAN. - <i>instance-id</i> – идентификатор экземпляра протокола MSTP; - <i>vlan-range</i> – номер группы VLAN. |
| no instance instance_id vlan vlan_range | | Удаляет соответствие между экземпляром протокола MSTP и группами VLAN. |
| name string | string: (1..32) символа | Задает имя конфигурации MST. - <i>string</i> – имя конфигурации MST. |
| no name | | Удаляет имя конфигурации MST. |
| revision value | value: (0..65535)/0 | Задает номер ревизии конфигурации MST. - <i>value</i> – номер ревизии конфигурации MST. |
| no revision | | Устанавливает значение по умолчанию (<i>value</i>). |
| show {current pending} | - | Показывает текущую (current) либо ожидающую (pending) конфигурацию MST. |
| exit | - | Выход из режима конфигурации протокола MSTP с сохранением конфигурации. |
| abort | - | Выход из режима конфигурации протокола MSTP без сохранения конфигурации. |

Команды режима конфигурации интерфейса Ethernet, интерфейса группы портов

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet, интерфейса группы портов:

```
console (config-if) #
```

Таблица 118 – Команды режима конфигурации интерфейса Ethernet, группы портов

| Команда | Значение/Значение по умолчанию | Действие |
|---|---|--|
| spanning-tree guard root | -/защита выключена | Включает защиту «корня» для всех связующих деревьев STP выбранного порта. Данная защита запрещает интерфейсу быть корневым портом коммутатора. |
| no spanning-tree guard root | | Устанавливает значение по умолчанию. |
| spanning-tree mst instance-id guard root | instance_id: (1..63); /защита выключена | Включает защиту «корня» указанного экземпляра MSTP для выбранного интерфейса. Данная защита запрещает интерфейсу быть корневым портом коммутатора. - instance-id – идентификатор экземпляра протокола MSTP. |
| no spanning-tree mst instance-id guard root | | Устанавливает значение по умолчанию. |
| spanning-tree mst instance_id port-priority priority | instance_id: (1..63); priority: (0..240)/128 | Устанавливает приоритет интерфейса в экземпляре MSTP. - instance-id – идентификатор экземпляра протокола MSTP; - priority – приоритет интерфейса. Значение приоритета должно быть кратно 16. |
| no spanning-tree mst instance_id port-priority | | Устанавливает значение по умолчанию. |
| spanning-tree mst instance_id cost cost | instance_id: (1..63); cost: (1..200000000) | Устанавливает ценность пути через выбранный интерфейс для определенного экземпляра протокола MSTP. - instance-id – идентификатор экземпляра протокола MSTP; - cost – ценность пути. |
| no spanning-tree mst instance_id cost | | Устанавливает значение, определяемое на основании скорости порта и метода определения ценности пути. |
| spanning-tree port-priority priority | priority: (0..240)/128 | Устанавливает приоритет интерфейса в корневом связующем дереве MSTP. Значение приоритета должно быть кратно 16. |
| no spanning-tree port-priority | | Устанавливает значение по умолчанию. |
| spanning-tree restricted-tcn | -/прием BPDU с флагом TCN разрешен | Запрещает прием BPDU с флагом TCN. |
| no spanning-tree restricted-tcn | | Разрешает прием BPDU с флагом TCN. |

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 119 – Команды режима EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|--|--|---|
| show spanning-tree [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port port-channel group] [instance instance_id] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); tve_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128); instance_id: (1..63) | Показывает конфигурацию протокола STP. - instance_id – идентификатор экземпляра протокола MSTP. |
| show spanning-tree detail [active blockedports] [instance instance_id] | instance_id: (1..63) | Показывает подробную информацию о настройке протокола STP, информацию об активных или заблокированных портах. - active – просмотр информации об активных портах; - blockedports – просмотр информации о заблокированных портах; - instance_id – идентификатор экземпляра протокола MSTP. |
| show spanning-tree mst-configuration | - | Показывает информацию о сконфигурированных экземплярах MSTP. |

| | | |
|---|--|---|
| <pre>clear spanning-tree detected-protocols interface {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group}</pre> | <pre>gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128)</pre> | Перезапускает процесс миграции протокола. Заново происходит просчёт дерева STP. |
|---|--|---|

Примеры выполнения команд

- Включить поддержку протокола STP, установить значение приоритета связующего дерева RSTP – 12288, интервал forward-time – 20 секунд, интервал времени между передачами широкораспространяемых сообщений «Hello» – 5 секунд, время жизни связующего дерева – 38 секунд. Показать конфигурацию протокола STP:

```
console(config)# spanning-tree
console(config)# spanning-tree mode rstp
console(config)# spanning-tree priority 12288
console(config)# spanning-tree forward-time 20
console(config)# spanning-tree hello-time 5
console(config)# spanning-tree max-age 38
console(config)# exit
console# show spanning-tree
```

```
Spanning tree enabled mode RSTP
Default port cost method: short
Loopback guard: Disabled

Root ID      Priority    32768
Address      a8:f9:4b:7b:e0:40
This switch is the root
Hello Time   5 sec    Max Age 38 sec    Forward Delay 20 sec

Number of topology changes 0 last change occurred 23:45:41 ago
Times: hold 1, topology change 58, notification 5
      hello 5, max age 38, forward delay 20

Interfaces
Name        State    Prio.Nbr    Cost    Sts    Role    PortFast    Type
-----
te1/0/1     enabled  128.1       100     Dsbl   Dsbl    No          -
te1/0/2     disabled 128.2       100     Dsbl   Dsbl    No          -
te1/0/5     disabled 128.5       100     Dsbl   Dsbl    No          -
te1/0/6     enabled  128.6       4       Frw    Desg    Yes         P2P (RSTP)
te1/0/7     enabled  128.7       100     Dsbl   Dsbl    No          -
te1/0/8     enabled  128.8       100     Dsbl   Dsbl    No          -
te1/0/9     enabled  128.9       100     Dsbl   Dsbl    No          -
gi1/0/1     enabled  128.49      100     Dsbl   Dsbl    No          -
Po1        enabled  128.1000    4       Dsbl   Dsbl    No          -
```

5.15.5.3 Настройка протоколов PVSTP+, RPVSTP+

PVSTP+ (Per-VLAN Spanning Tree Protocol Plus) — одна из разновидностей протокола Spanning Tree, расширяющая функциональность STP для использования в отдельных VLAN. Применение данного протокола позволяет в каждом VLAN создать отдельный экземпляр STP. PVSTP+ совместим с STP.

Rapid (быстрый) PVSTP+ (RPVSTP+) является усовершенствованием протокола PVSTP+, характеризуется меньшим временем приведения сети к древовидной топологии и имеет более высокую устойчивость.



Всего поддержано 65 PVST/RPVST-инстанса. При этом нулевой используется для всех VLAN, в которых отключен PVST/RPVST. Каждому VLAN с включенным PVST/RPVST соответствует один PVST/RPVST инстанс.



Порты, на которых активны 65 и более VLAN, при переходе в режим PVST/RPVST временно блокируются, поэтому перед включением PVST/RPVST необходимо рассчитать количество используемых VLAN на кольцевых портах коммутатора. Если данное значение превышает 64, то первоначально нужно отключить PVST/RPVST в избыточных VLAN/RPVST командой "no spanning-tree vlan <VLAN ID>".



При включенном режиме PVST/RPVST коммутаторы MES обрабатывают PVST bpdu во всех VLAN. Поэтому в случаях, когда в кольце используются коммутаторы с количеством PVST/RPVST VLAN, превышающем 64, следует расширить лимиты обработки PVST bpdu-трафика на CPU. Для этого используется команда "service cpu-rate-limits other-bpdu 1024".



Если в процессе эксплуатации понадобится убрать VLAN из PVST/RPVST-инстансов и добавить новые, нужно произвести следующие действия:

- 1) Отключить STP в ненужных VLAN (команда «no spanning-tree vlan *vlan_list*» в глобальном режиме конфигурирования);
- 2) Включить STP в новых VLAN (команда «spanning-tree vlan *vlan_list*» в глобальном режиме конфигурирования).

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 120 — Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--|--|--|
| spanning-tree vlan <i>vlan_list</i> | vlan_list: (1..4094)/ по умолчанию все инстансы включены | Включить работу протокола PVSTP+, RPVSTP+ в указанных VLAN. |
| no spanning-tree vlan <i>vlan_list</i> | | Отключает работу протокола PVSTP+, RPVSTP+ в указанных VLAN. |
| spanning-tree vlan <i>vlan_list</i> forward-time <i>seconds</i> | vlan_list: (1..4094); seconds: (4..30)/15 сек | Устанавливает интервал времени, затрачиваемый на прослушивание и изучение состояний перед переключением в состояние передачи для указанных VLAN. Таймеры должны соответствовать следующей формуле: $2 * (\text{Forward-Time} - 1) \geq \text{Max-Age} \geq 2 * (\text{Hello-Time} + 1)$ |
| no spanning-tree vlan <i>vlan_list</i> forward-time | | Устанавливает значение по умолчанию. |
| spanning-tree vlan <i>vlan_list</i> hello-time <i>seconds</i> | vlan_list: (1..4094); seconds: (1..10)/2 сек | Устанавливает интервал времени между передачами широковещательных сообщений «Hello» к взаимодействующим коммутаторам для указанных VLAN. |
| no spanning-tree vlan <i>vlan_list</i> hello-time | | Устанавливает значение по умолчанию. |
| spanning-tree vlan <i>vlan_list</i> max-age <i>seconds</i> | vlan_list: (1..4094); seconds: (6..40)/20 сек | Устанавливает время жизни связующего дерева STP для указанных VLAN. |
| no spanning-tree vlan <i>vlan_list</i> max-age | | Устанавливает значение по умолчанию. |
| spanning-tree vlan <i>vlan_list</i> priority <i>priority_value</i> | vlan_list: (1..4094); | Настраивает приоритет связующего дерева STP. |

| | | |
|---|-------------------------------------|--|
| | priority_value: (0..61440)/32768 | <input checked="" type="checkbox"/> Значение выбирается из диапазона с шагом 4096. |
| no spanning-tree vlan <i>vlan_list priority</i> | | Устанавливает значение по умолчанию. |

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet

Вид запроса командной строки режима конфигурации интерфейса:

```
console(config-if) #
```

Таблица 121 — Команды режима конфигурации интерфейса Ethernet

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|---|
| spanning-tree vlan <i>vlan_list cost cost</i> | vlan_list: (1..4094); cost: (1..200000000) | Устанавливает ценность пути через данный интерфейс для указанных VLAN. - <i>cost</i> — ценность пути. |
| no spanning-tree vlan <i>vlan_list cost</i> | | Устанавливает значение, определяемое на основании скорости порта и метода определения ценности пути для указанных VLAN. |
| spanning-tree vlan <i>vlan_list port-priority priority_value</i> | vlan_list: (1..4094); priority_value: (0..240)/128 | Устанавливает приоритет интерфейса в корневом связующем дереве STP. <input checked="" type="checkbox"/> Значение выбирается из диапазона с шагом 16. |
| no spanning-tree vlan <i>vlan_list port-priority</i> | | Устанавливает значение по умолчанию. |
| spanning-tree vlan <i>vlan_list restricted-tcn</i> | -/прием BPDU с флагом TCN разрешен; vlan_list: (1..4094) | Запрещает прием BPDU с флагом TCN для указанных VLAN. |
| no spanning-tree vlan <i>vlan_list restricted-tcn</i> | | Разрешает прием BPDU с флагом TCN для указанных VLAN. |

5.15.6 Настройка протокола G.8032v2 (ERPS)

Протокол ERPS (Ethernet Ring Protection Switching) предназначен для повышения устойчивости и надежности сети передачи данных, имеющей кольцевую топологию, за счет снижения времени восстановления сети в случае аварии. Время восстановления не превышает 1 секунды, что существенно меньше времени перестройки сети при использовании протоколов семейства spanning tree.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config) #
```

Таблица 122 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|------------------------------------|---------------------------------------|--|
| erps | -/выключено | Разрешает работу протокола ERPS. |
| no erps | | Запрещает работу протокола ERPS. |
| erps vlan <i>vlan_id</i> | vlan_id: (1..4094) | Создание ERPS-кольца с идентификатором R-APS VLAN, по которой будет передаваться служебная информация и переход в режим конфигурации кольца. - <i>vlan_id</i> – номер R-APS VLAN. |
| no erps vlan <i>vlan_id</i> | | Удаление ERPS-кольца с идентификатором <i>vlan_id</i> . |

Команды режима конфигурации кольца

Вид запроса командной строки в режиме конфигурации кольца:

```
console (config-erps) #
```

Таблица 123 – Команды режима конфигурации ERPS-кольца

| Команда | Значение/Значение по умолчанию | Действие |
|---|---|---|
| protected vlan add <i>vlan_list</i> | vlan_list:(2..4094, all) | Добавляет диапазон VLAN в список защищенных VLAN. - <i>vlan_list</i> – список VLAN. Диапазон VLAN можно задать перечислением через запятую или указать начальное и конечное значения диапазона через дефис "-". |
| protected vlan remove <i>vlan_list</i> | vlan_list:(2..4094, all) | Удаляет диапазон VLAN из списка защищенных VLAN. - <i>vlan_list</i> – список VLAN для удаления. |
| port {west east} { tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> } | <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..128) | Выбор west (east)-порта коммутатора, включенного в кольцо. |
| no port {west east} | | Удаление west (east)-порта коммутатора, включенного в кольцо. |
| rpl {west east} {owner neighbor} | -/no rpl | Выбор RPL-порта коммутатора и его роли. - west – RPL-портом будет назначен west-порт; - east – RPL-портом будет назначен east-порт; - owner – коммутатор будет являться владельцем RPL-порта; - neighbor – коммутатор будет являться соседом владельца RPL-порта. |
| no rpl | | Удаление RPL-порта коммутатора. |
| level <i>level</i> | level: (0..7)/1 | Настройка уровня сообщений R-APS. Необходимо для прохождения сообщений через CFM MEP. - <i>level</i> – уровень сообщений R-APS. |
| no level | | Установка значения по умолчанию. |
| ring enable | -/выключено | Включение функционирования кольца. |
| no ring enable | | Выключение функционирования кольца. |
| version <i>version</i> | version: (1..2)/2 | Выбор режима совместимости с другими версиями протокола G.8032. - <i>version</i> – версия протокола G.8032. |
| no version | | Установка значения по умолчанию. |
| revertive | -/revertive | Выбор режима работы кольца. |
| no revertive | | Установка значения по умолчанию. |
| sub-ring vlan <i>vlan_id</i> | vlan_id:(1..4094) | Указание подкольца для данного кольца. - <i>vlan_id</i> – номер VLAN. |
| no sub-ring vlan <i>vlan_id</i> | | Удаление подкольца. |
| sub-ring vlan <i>vlan_id</i> [tc-propagation] | vlan_id:(1..4094) | Включить отправку сигнала очистки MAC-таблицы в основное кольцо при перестроении подкольца. |
| no sub-ring vlan <i>vlan_id</i> | | Отключить отправку сигнала очистки MAC-таблицы в основное кольцо при перестроении подкольца. |
| timer guard <i>value</i> | value:(10..2000) мс, кратное 10/500 мс | Установка таймера, блокирующего устаревшие R-APS сообщения. |
| no timer guard | | Установка значения по умолчанию. |
| timer holdoff <i>value</i> | value:(0..10000) мс, кратное 100 с точностью 5 мс/0 мс | Установка таймера задержки реакции коммутатора на изменение в состоянии. Вместо реакции на событие включается таймер, по истечении которого коммутатор информирует о своем состоянии. Предназначен для уменьшения флуда пакетов при флаппинге портов. |
| no timer holdoff | | Установка значения по умолчанию. |

| | | |
|------------------------------------|-------------------------|---|
| timer wtr value | value:(1..12) мин/5 мин | Установка таймера, который запускается на RPL Owner коммутаторе в revertive-режиме. Используется для предотвращения частых защитных переключений из-за сигналов о неисправностях. |
| no timer wtr | | Установка значения по умолчанию. |
| switch forced {west east} | -/no | Форсирует запуск защитного переключения кольца, при этом блокируется указанный порт. |
| no switch forced | | Отмена форсирования переключения кольца. |
| switch manual {west east} | -/no | Ручное блокирование указанного west (east)-порта и разблокирование east (west). |
| no switch manual | | Отмена ручной блокировки. |
| abort | - | Откатить изменения, внесенные с момента входа в режим конфигурации кольца. |

Команды режима EХЕС

Вид запроса командной строки режима EХЕС:

```
console#
```

Таблица 124 – Команды режима EХЕС

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---------------------------------|---------------------------------------|--|
| show erps [vlan vlan_id] | vlan_id: (1..4094) | Запрос информации об общем состоянии ERPS или состоянии указанного кольца. |

5.15.7 Настройка протокола LLDP

Основной функцией протокола **Link Layer Discovery Protocol (LLDP)** является обмен между сетевыми устройствами о своем состоянии и характеристиках. Информация, собранная посредством протокола LLDP, накапливается в устройствах и может быть запрошена управляющим компьютером по протоколу SNMP. Таким образом, на основании собранной информации, на управляющем компьютере может быть смоделирована топология сети.

Коммутаторы поддерживают передачу как стандартных параметров, так и опциональных, таких как:

- имя устройства и его описание;
- имя порта и его описание;
- информация о MAC/PHY;
- и т.д.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console (config) #
```

Таблица 125 – Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---------------------------|---------------------------------------|---|
| lldp run | -/разрешено | Разрешает коммутатору использование протокола LLDP. |
| no lldp run | | Запрещает коммутатору использование протокола LLDP. |
| lldp timer seconds | seconds: (5..32768)/30 сек | Определяет, как часто устройство будет отправлять обновление информации LLDP. |
| no lldp timer | | Устанавливает значение по умолчанию. |

| | | |
|---|--|---|
| <code>lldp hold-multiplier number</code> | number: (2..10)/4 | <p>Задаёт величину времени для принимающего устройства, в течение которого нужно удерживать принимаемые пакеты LLDP перед их сбросом.</p> <p>Данная величина передается на принимаемую сторону в LLDP update пакетах (пакетах обновления), является кратностью для таймера LLDP (lldp timer). Таким образом, время жизни LLDP пакетов рассчитывается по формуле $TTL = \min(65535, LLDP-Timer * LLDP-HoldMultiplier)$.</p> |
| <code>no lldp hold-multiplier</code> | | Устанавливает значение по умолчанию. |
| <code>lldp reinit seconds</code> | seconds: (1..10)/2 сек | Минимальное время, которое LLDP-порт будет ожидать перед повторной инициализацией LLDP. |
| <code>no lldp reinit</code> | | Устанавливает значение по умолчанию. |
| <code>lldp tx-delay seconds</code> | seconds: (1..8192)/2 сек | <p>Устанавливает задержку между последующими передачами пакетов LLDP, инициированными изменениями значений или статуса в локальных базах данных MIB LLDP.</p> <p> Рекомендуется, чтобы данная задержка была меньше, чем значение $0.25 * LLDP-Timer$.</p> |
| <code>no lldp tx-delay</code> | | Устанавливает значение по умолчанию. |
| <code>lldp lldpdu {filtering flooding}</code> | -/filtering | <p>Определяет режим обработки пакетов LLDP, когда протокол LLDP выключен на коммутаторе:</p> <ul style="list-style-type: none"> - <i>filtering</i> – указывает, что LLDP-пакеты фильтруются, если протокол LLDP выключен на коммутаторе; - <i>flooding</i> – указывает, что LLDP-пакеты передаются, если протокол LLDP выключен на коммутаторе. |
| <code>no lldp lldpdu</code> | | Устанавливает значение по умолчанию. |
| <code>lldp med fast-start repeat-count number</code> | number: (1..10)/3 | Устанавливает число повторений PDU LLDP для быстрого запуска, определяемого посредством LLDP-MED. |
| <code>no lldp med fast-start repeat-count</code> | | Устанавливает значение по умолчанию. |
| <code>lldp med network-policy number application [vlan vlan_id] [vlan-type {tagged untagged}] [up priority] [dscp value]</code> | <p>number: (1..32); application: (voice, voice-signaling, guest-voice, guest-voice-signaling, softphone-voice, video-conferencing, streaming-video, video-signaling); vlan_id: (0..4095); priority: (0..7); value: (0..63)</p> | <p>Определяет правило для параметра network-policy (сетевая политика устройства). Данный параметр является опциональным для расширения протокола LLDP MED.</p> <ul style="list-style-type: none"> - <i>number</i> – порядковый номер правила network policy; - <i>application</i> – главная функция, определенная для данного правила network policy. - <i>vlan_id</i> – идентификатор VLAN для данного правила; - tagged/untagged – определяет тегированной или нетегированной будет VLAN, используемая данным правилом. - <i>priority</i> – приоритет данного правила (используется на втором уровне модели OSI); - <i>value</i> – значение DSCP, используемое данным правилом. Если не указывать значение DSCP, по умолчанию коммутатор будет отправлять параметр DSCP 0. <p> Изменение network-policy возможно только после снятия политики со всех интерфейсов, где она применена.</p> |
| <code>no lldp med network-policy number</code> | | Удаляет созданное правило для параметра network-policy. |
| <code>lldp notifications interval seconds</code> | seconds: (5..3600)/5 сек | <p>Устанавливает максимальную скорость передачи уведомлений LLDP.</p> <ul style="list-style-type: none"> - <i>seconds</i> – период времени, в течение которого устройство может отправить не более одного уведомления. |
| <code>no lldp notifications interval</code> | | Устанавливает значение по умолчанию. |

Команды режима конфигурации интерфейсов Ethernet

Вид запроса командной строки в режиме конфигурации интерфейсов Ethernet:

```
console (config-if) #
```

Таблица 126 – Команды режима конфигурации интерфейса Ethernet

| Команда | Значение/Значение по умолчанию | Действие |
|---|--|--|
| lldp transmit | По умолчанию разрешено использование в обоих направлениях. | Разрешает передачу пакетов по протоколу LLDP на интерфейсе. |
| no lldp transmit | | Запрещает передачу пакетов по протоколу LLDP на интерфейсе. |
| lldp receive | | Разрешает прием пакетов по протоколу LLDP на интерфейсе. |
| no lldp receive | | Запрещает прием пакетов по протоколу LLDP на интерфейсе. |
| lldp optional-tlv tlv_list | tlv_list: (port-desc, sys-name, sys-desc, sys-cap, 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size, 802.3-power-via-mdi)/По умолчанию опциональные TLV не включены в пакет. | <p>Определяет, какие опциональные TLV-поля (Type, Length, Value) будут включены устройством в передаваемый LLDP-пакет.</p> <p>В команду можно включить от одного до пяти опциональных TLV.</p> <p> TLV 802.3-power-via-mdi доступна только на устройствах с поддержкой PoE.</p> |
| no lldp optional-tlv | | Устанавливает значение по умолчанию. |
| lldp optional-tlv 802.1 {pvid [enable disable] ppvid {add remove} ppid vlan-name {add remove} vlan_id} | ppvid: (1-4094); vlan_id: (2-4094); По умолчанию опциональные TLV не включены. | Определяет, какие опциональные TLV-поля будут включены устройством в передаваемый LLDP-пакет: |
| lldp optional-tlv 802.1 protocol {add remove} {stp rstp mstp pause 802.1x lacp gvrp} | | <ul style="list-style-type: none"> - pvid – PVID интерфейса; - ppvid – добавить/удалить PPVID; - vlan-name – добавить/удалить номер VLAN; - protocol – добавить/удалить определенный протокол. |
| no lldp optional-tlv 802.1 pvid | | Устанавливает значение по умолчанию. |
| lldp management-address {ip_address none automatic [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port port-channel group vlan vlan_id]} | <p>формат ip-address: A.B.C.D;</p> <p>gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); tve_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128); vlan_id: (1..4094).</p> <p>По умолчанию управляющий адрес определяется автоматически.</p> | <p>Определяет управляющий адрес, объявленный на интерфейсе.</p> <ul style="list-style-type: none"> - ip_address – задается статический IP-адрес; - none – указывает, что адрес не объявлен; - automatic – указывает, что система автоматически выбирает управляющий адрес из всех IP-адресов коммутатора; - automatic – указывает, что система автоматически выбирает управляющий адрес, из сконфигурированных адресов заданного интерфейса. <p>Если интерфейс ethernet или интерфейс группы портов принадлежат VLAN, то данный адрес VLAN не будет включен в список возможных управляющих адресов.</p> <p> В случае наличия нескольких IP-адресов система выбирает начальный IP-адрес из диапазона динамических IP-адресов. Если динамические адреса отсутствуют, то система выбирает начальный IP-адрес из диапазона возможных статических IP-адресов.</p> |
| no lldp management-address | | Удаляет управляющий IP-адрес. |
| lldp notification {enable disable} | По умолчанию отправка уведомлений LLDP запрещена. | Разрешает/запрещает отправку уведомлений LLDP на интерфейсе. |
| no lldp notifications | | Устанавливает значение по умолчанию. |
| lldp med enable [tlv_list] | tlv_list: (network-policy, location, inventory)/запрещено использование расширения протокола LLDP MED. | Разрешает использование расширения протокола LLDP MED. В команду можно включить от одного до трех специальных TLV. |
| lldp med network-policy {add remove} number | number: (1-32) | Назначает правило network-policy данному интерфейсу. |
| no lldp med network-policy | | <ul style="list-style-type: none"> - add – назначает правило; - remove – удаляет правило; - number – номер правила. <p>Удаляет правило network-policy с данного интерфейса.</p> |

| | | |
|---|---|--|
| lldp med location {coordinate <i>coordinate</i> civic-address <i>civic_address_data</i> ecs-elin <i>ecs_elin_data</i> } | coordinate: 16 байт; civic_address_data: (6..160) байт; ecs_elin_data: (10..25) байт. | Задаёт местоположение устройства для протокола LLDP (значение параметра location протокола LLDP MED). - <i>coordinate</i> – адрес в системе координат; - <i>civic_address_data</i> – административный адрес устройства; - <i>ecs-elin_data</i> – адрес в формате, определенном ANSI/TIA 1057. |
| no lldp med location {coordinate civic-address ecs-elin} | | Удаляет настройки параметра местоположения location. |
| lldp med notification topology-change {enable disable} | -/запрещено | Разрешает/запрещает отправку уведомлений LLDP MED об изменении топологии. - enable – разрешает отправку уведомлений; - disable – запрещает отправку уведомлений. |
| no lldp med notifications topology-change | | Устанавливает значение по умолчанию. |



Пакеты LLDP, принятые через группу портов, запоминаются индивидуально портами группы, принявшими сообщения. LLDP отправляет различные сообщения на каждый порт группы.



Работа протокола LLDP не зависит от состояния протокола STP на порту, пакеты LLDP отправляются и принимаются на заблокированных протоколом STP-портах. Если порт контролируется по 802.1X, то LLDP работает с портом только в случае, если он авторизован.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 127 – Команды режима Privileged EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|--|--|--|
| clear lldp table [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> oob] | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32) | Очищает таблицу адресов обнаруженных соседних устройств и начинает новый цикл обмена пакетами по протоколу LLDP MED. |
| show lldp configuration [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> oob detailed] | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32) | Показывает LLDP-конфигурации всех физических интерфейсов устройства либо заданных интерфейсов. |
| show lldp med configuration [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> oob detailed] | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32) | Показывает конфигурации расширения протокола LLDP – MED для всех физических интерфейсов либо заданных интерфейсов. |

| | | |
|---|--|--|
| show lldp local {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port oob} | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Показывает LLDP-информацию, которую анонсирует данный порт. |
| show lldp local tlvs-overloading {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port oob} | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Показывает статус перезагрузки TLVs LLDP. |
| show lldp neighbors {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port oob} | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Показывает информацию о соседних устройствах, на которых работает протокол LLDP. |
| show lldp statistics {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port oob detailed} | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Показывает статистику LLDP. |

Примеры выполнения команд

- Установить для порта te1/0/10 следующие tlv-поля: port-description, system-name, system-description. Для данного интерфейса добавить управляющий адрес 10.10.10.70.

```
console(config)# configure
console(config)# interface tengigabitethernet 1/0/10
console(config-if)# lldp optional-tlv port-desc sys-name sys-desc
console(config-if)# lldp management-address 10.10.10.70
```

- Посмотреть конфигурацию LLDP:

```
console# show lldp configuration
```

| LLDP state: Enabled | | | | |
|-----------------------------------|-----------|---------------|-------------|---------------|
| Timer: 30 Seconds | | | | |
| Hold Multiplier: 4 | | | | |
| Reinit delay: 4 Seconds | | | | |
| Tx delay: 2 Seconds | | | | |
| Notifications Interval: 5 Seconds | | | | |
| LLDP packets handling: Filtering | | | | |
| Chassis ID: mac-address | | | | |
| Port | State | Optional TLVs | Address | Notifications |
| te1/0/7 | Rx and Tx | SN, SC | None | Disabled |
| te1/0/8 | Rx and Tx | SN, SC | None | Disabled |
| te1/0/9 | Rx and Tx | SN, SC | None | Disabled |
| te1/0/10 | Rx and Tx | PD, SD | 10.10.10.70 | Disabled |

Таблица 128 – Описание результатов

| Поле | Описание |
|-------|--|
| Timer | Определяет, как часто устройство шлет LLDP-обновления. |

| | |
|-----------------|---|
| Hold Multiplier | Определяет величину времени (TTL, Time-To-Live) для принимающего устройства, в течение которого нужно удерживать принимаемые пакеты LLDP перед их сбросом: TTL = Timer * Hold Multiplier. |
| Reinit delay | Определяет минимальное время, в течение которого порт будет ожидать перед посылкой следующего LLDP-сообщения. |
| Tx delay | Определяет задержку между последующими передачами LLDP-кадров, инициированных изменениями значений либо статуса. |
| Port | Номер порта. |
| State | Режим работы порта для протокола LLDP. |
| Optional TLVs | TLV-опции, которые передаются Возможные значения: PD – Описание порта; SN – Системное имя; SD – Описание системы; SC – Возможности системы. |
| Address | Адрес устройства, который передается в LLDP-сообщениях. |
| Notifications | Указывает, разрешены или запрещены уведомления LLDP. |

- Показать информацию о соседних устройствах

```
console# show lldp neighbors
```

| Port | Device ID | Port ID | System Name | Capabilities |
|---------|----------------|---------|-------------|--------------|
| Te1/0/1 | 0060.704C.73FE | 1 | ts-7800-2 | B |
| Te1/0/2 | 0060.704C.73FD | 1 | ts-7800-2 | B |
| Te1/0/3 | 0060.704C.73FC | 9 | ts-7900-1 | B, R |
| Te1/0/4 | 0060.704C.73FB | 1 | ts-7900-2 | W |

Таблица 129 – Описание результатов

| <i>Поле</i> | <i>Описание</i> |
|--------------------------|--|
| Port | Номер порта. |
| Device ID | Имя или MAC-адрес соседнего устройства. |
| Port ID | Идентификатор порта соседнего устройства. |
| System name | Системное имя устройства. |
| Capabilities | Данное поле описывает тип устройства: B – Мост (Bridge); R – Маршрутизатор (Router); W – Точка доступа WI-FI (WLAN Access Point); T – Телефон (Telephone); D – DOCSIS-устройство (DOCSIS cable device); H – Сетевое устройство (Host); r – Повторитель (Repeater); O – Тип неизвестен (Other). |
| System description | Описание соседнего устройства. |
| Port description | Описание порта соседнего устройства. |
| Management address | Адрес управления устройством. |
| Auto-negotiation support | Определяет, поддерживается ли автоматическое определение режима порта. |
| Auto-negotiation status | Определяет, включена ли поддержка автоматического определения режима порта. |

| | |
|---|---|
| Auto-negotiation Advertised Capabilities | Определяет режимы, поддерживаемые функцией автоматического определения порта. |
| Operational MAU type | Рабочий MAU-тип устройства. |

5.15.8 Настройка протокола OAM

Ethernet OAM (Operation, Administration, and Maintenance), IEEE 802.3ah — функции уровня канала передачи данных представляют собой протокол мониторинга состояния канала. В этом протоколе для передачи информации о состоянии канала между непосредственно подключенными устройствами Ethernet используются блоки данных протокола OAM (OAMPDU). Оба устройства должны поддерживать стандарт IEEE 802.3ah.

Команды режима конфигурации интерфейсов Ethernet

Вид запроса командной строки в режиме конфигурации интерфейсов Ethernet:

```
console(config-if)#
```

Таблица 130 — Команды режима конфигурации интерфейса Ethernet

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---------------------------------------|---|
| ethernet oam | —/отключено | Включить поддержку Ethernet OAM на порту. |
| no ethernet oam | | Отключить Ethernet OAM на конфигурируемом порту. |
| ethernet oam link-monitor supported | —/отключено | Включить поддержку «link-monitor». |
| no ethernet oam link-monitor supported | | Восстановить значение по умолчанию. |
| ethernet oam link-monitor frame threshold count | count: (1..65535)/1 | Установить порог количества ошибок за указанный период (период устанавливается командой ethernet oam link-monitor frame window). |
| no ethernet oam link-monitor frame threshold | | Восстановить значение по умолчанию. |
| ethernet oam link-monitor frame window window | window: (10..600)/100 мс | Установить временной промежуток для подсчета количества ошибок. |
| no ethernet oam link-monitor frame window | | Восстановить значение по умолчанию. |
| ethernet oam link-monitor frame-period threshold count | count: (1..65535)/1 | Установить порог для события «frame-period» (период устанавливается командой ethernet oam link-monitor frame-period window). |
| no ethernet oam link-monitor frame-period threshold | | Восстановить значение по умолчанию. |
| ethernet oam link-monitor frame-period window window | window: (1..65535)/10000 | Установить временной промежуток для события «frame-period» (в кадрах). |
| no ethernet oam link-monitor frame-period window | | Восстановить значение по умолчанию. |
| ethernet oam link-monitor frame-seconds threshold count | count: (1..900)/1 | Установить порог для события «frame-period» (период устанавливается командой ethernet oam link-monitor frame-seconds window), в секундах. |
| no ethernet oam link-monitor frame-seconds threshold | | Восстановить значение по умолчанию. |
| ethernet oam link-monitor frame-seconds window window | window: (100..9000)/100 мс | Установить временной промежуток для события «frame-period». |
| no ethernet oam link-monitor frame-seconds window | | Восстановить значение по умолчанию. |

| | | |
|---|----------------------|--|
| ethernet oam mode {active passive} | —/active | Установить режим работы протокола OAM: - active — коммутатор постоянно отправляет OAMPDU; - passive — коммутатор начинает отправлять OAMPDU только при наличии OAMPDU со встречной стороны. |
| no ethernet oam mode | | Восстановить значение по умолчанию. |
| ethernet-oam remote-failure | —/включено | Включить поддержку и обработку событий «remote-failure». |
| no ethernet oam remote-failure | | Восстановить значение по умолчанию. |
| ethernet oam remote-loopback supported | —/отключено | Включить поддержку функции заворота трафика. |
| no ethernet oam remote-loopback supported | | Восстановить значение по умолчанию. |
| ethernet oam uni-directional detection | —/отключено | Включить функцию обнаружения однонаправленных связей на базе протокола Ethernet OAM. |
| no ethernet oam uni-directional detection | | Восстановить значение по умолчанию. |
| ethernet oam uni-directional detection action {log error-disable} | —/log | Определить реакцию коммутатора на однонаправленную связь: - log — отправка SNMP trap и запись в журнал; - error-disable — перевод порта в состояние «error-disable», запись в журнал и отправка SNMP trap. |
| no ethernet oam uni-directional detection action | | Восстановить значение по умолчанию. |
| ethernet oam uni-directional detection aggressive | —/отключено | Включить агрессивный режим определения однонаправленной связи. Если от соседнего устройства перестают приходить Ethernet OAM-сообщения — линк помечается как однонаправленный. |
| no ethernet oam uni-directional detection aggressive | | Восстановить значение по умолчанию. |
| ethernet oam uni-directional detection discovery-time time | time: (5..300)/5 сек | Установить временной интервал для определения типа связи на порту. |
| no ethernet oam uni-directional detection discovery-time | | Восстановить значение по умолчанию. |

Команды режима privileged EXEC

Все команды доступны для привилегированного пользователя. Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 131 — Команды режима privileged EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|--|--|
| clear ethernet oam statistics [interface {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port}] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Очистить статистику Ethernet OAM для указанного интерфейса. |
| show ethernet oam discovery [interface {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port}] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Отобразить состояние протокола Ethernet OAM для указанного интерфейса. |

| | | |
|--|--|---|
| show ethernet oam statistics [interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> }] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Отобразить статистику обмена протокольными сообщениями для указанного интерфейса. |
| show ethernet oam status [interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> }] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Отобразить настройки Ethernet OAM для указанного интерфейса. |
| show ethernet oam uni-directional detection [interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> }] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Отобразить состояние механизма определения однонаправленных связей для указанного интерфейса. |
| ethernet oam remote-loopback {start stop} {interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> }} | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Запуск/остановка удаленной петли для указанного интерфейса. |

Примеры выполнения команд

- Отобразить состояние протокола для порта tengigabitethernet 1/0/3:

```
console# show ethernet oam discovery interface TenGigabitEthernet 1/0/3
```

```
tengigabitethernet 1/0/3
Local client
-----

Administrative configurations:
Mode:                active
Unidirection:        not supported
Link monitor:         supported
Remote loopback:     supported
MIB retrieval:        not supported
Mtu size:             1500
Operational status:
Port status:         operational
Loopback status:     no loopback
PDU revision:        3
Remote client
-----

MAC address: a8:f9:4b:0c:00:03
Vendor(oui): a8 f9 4b
Administrative configurations:
PDU revision:        3
Mode:                active
Unidirection:        not supported
Link monitor:         supported
Remote loopback:     supported
MIB retrieval:        not supported
Mtu size:             1500
console#
```

5.15.9 Настройка функции Flex-link

Flex-link — функция резервирования, предназначенная для обеспечения надежности канала передачи данных. В связке flex-link могут находиться интерфейсы Ethernet и Port-channel. Один из этих интерфейсов находится в заблокированном состоянии и начинает пропускать трафик только в случае аварии на втором интерфейсе.

Команды режима конфигурирования интерфейса Ethernet, интерфейса группы портов

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet, интерфейса группы портов:

```
console(config-if) #
```

Таблица 132 – Команды режима конфигурирования интерфейса Ethernet, группы портов

| Команда | Значение/Значение по умолчанию | Действие |
|--|--|---|
| flex-link backup {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel port_channel} | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..4); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); port_channel (1..48)/- | Включает flex-link на интерфейсе и назначает выбранному интерфейсу роль backup-интерфейса в flex-link паре. |
| no flex-link backup {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel port_channel} | | Выключает flex-link на интерфейсе и удаляет выбранный интерфейс из flex-link пары. |
| flex-link preempt mode [forced bandwidth off] | -/off | Задаёт действие при поднятии интерфейса, участвующего во flex-link: - forced — если поднявшийся интерфейс настроен как master, то он станет активным интерфейсом; - bandwidth — при поднятии интерфейса активным станет интерфейс с большей пропускной способностью; - off — поднявшийся интерфейс останется в заблокированном состоянии. |
| no flex-link preempt mode | | Возвращает значение по умолчанию. |
| flex-link preempt delay delay | delay: (1..300)/35 | Задаёт время от перехода отключенного порта в состояние «up», по прошествии которого выполняется действие, установленное командой flex-link preempt mode . - delay — период времени, в секундах. |
| no flex-link preempt delay | | Возвращает значение по умолчанию. |

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 133 – Команды режима EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|---|--------------------------------------|--|
| show interfaces flex-link [detailed] {gigabitethernet | gi_port: (1..8/0/1..48); te_port: | Показывает конфигурацию функции flex-link. |

| | | |
|---|---|--|
| <code>gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel port- channel}</code> | <code>(1..8/0/1..4); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); port_channel: (1..48)</code> | |
|---|---|--|

5.15.10 Настройка функции Layer 2 Protocol Tunneling (L2PT)

Функция Layer 2 Protocol Tunneling (L2PT) позволяет пропускать служебные пакеты различных L2-протоколов (PDU) через сеть провайдера, что позволяет прозрачно связать клиентские сегменты сети.

L2PT инкапсулирует PDU на интерфейсе коммутатора, граничащего с оборудованием, кадры которого необходимо инкапсулировать, и передает их на другой такой же коммутатор, который ожидает инкапсулированные кадры, а затем деинкапсулирует их. Это позволяет пользователям передавать информацию 2-го уровня через сеть провайдера. Коммутаторы предоставляют возможность инкапсулировать служебные пакеты протоколов STP, LACP, LLDP, IS-IS.

Пример

Если включить L2PT для протокола STP, то коммутаторы A, B, C и D будут объединены в одно связующее дерево, несмотря на то, что коммутатор A не соединен напрямую с коммутаторами B, C и D. Информация об изменении топологии сети может быть передана сквозь сеть провайдера.

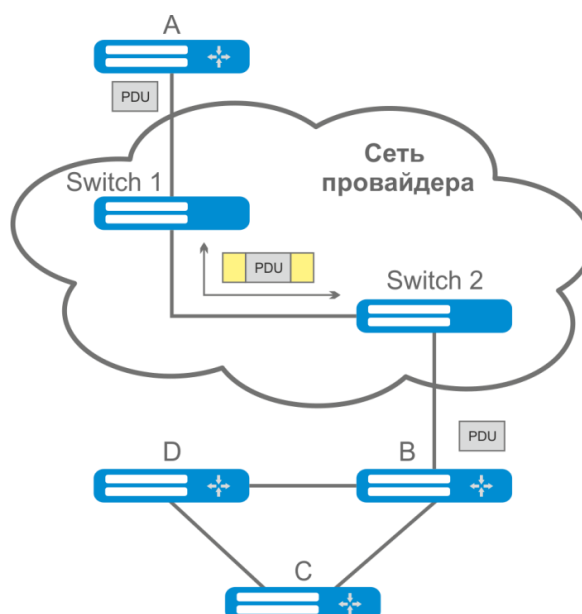


Рисунок 84 — Пример работы функции L2PT

Алгоритм работы функционала следующий:

Инкапсуляция:

1. Все L2 PDU перехватываются на CPU.
2. Подсистема L2PT определяет L2-протокол, которому соответствует принятый PDU, и проверяет, включена ли на порту, с которого принят этот PDU, настройка `l2protocol-tunnel` для данного L2-протокола.

Если настройка включена, то:

- во все порты VLAN, на которых включено туннелирование, отправляется PDU-кадр;
- во все порты VLAN, на которых выключено туннелирование, отправляется инкапсулированный PDU-кадр (исходный кадр с Destination MAC-адресом, измененным на туннельный).

Если настройка выключена, то:

- PDU-кадр передается в обработчик соответствующего протокола.

Декапсуляция:

3. Реализован перехват на CPU Ethernet-кадров с MAC-адресом назначения, заданным при помощи команды `I2protocol-tunnel address xx-xx-xx-xx-xx-xx`. Перехват включается только тогда, когда хотя бы на одном порту включена настройка `I2protocol-tunnel` (независимо от протокола).
4. При перехвате пакета с MAC-адресом назначения `xx-xx-xx-xx-xx-xx`, он сначала попадает в подсистему L2PT, которая определяет L2-протокол для данного PDU по его заголовку, и проверяет, включена ли на порту, с которого принят инкапсулированный PDU, настройка `I2protocol-tunnel` для данного L2-протокола.

Если настройка включена, то:

- порт, с которого был получен инкапсулированный PDU-кадр, блокируется с причиной `I2pt-guard`.

Если настройка выключена:

- во все порты VLAN, на которых включено туннелирование, отправляется декапсулированный PDU-кадр;
- во все порты VLAN, на которых выключено туннелирование, отправляется инкапсулированный PDU-кадр.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 134 – Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---|---|
| <code>I2protocol-tunnel address {mac_address}</code> | mac_address: (01:00:ee:ee:00:00, 01:00:0c:cd:cd:d0, 01:00:0c:cd:cd:d1, 01:00:0c:cd:cd:d2, 01:0f:e2:00:00:03)/ 01:00:ee:ee:00:00 | Задать MAC-адрес назначения для туннелируемых кадров. |
| <code>no I2protocol-tunnel address</code> | | Установить значение по умолчанию. |

Команды режима конфигурации интерфейса Ethernet



На интерфейсе, граничащем с оконечным устройством, не поддерживающим STP, должен быть отключен протокол STP (spanning-tree disable) и включена фильтрация BPDU (spanning-tree bpd filtering).

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet, интерфейса группы портов:

```
console(config-if)#
```

Таблица 135 – Команды режима конфигурации интерфейса Ethernet

| Команда | Значение/Значение по умолчанию | Действие |
|--|-----------------------------------|---|
| <code>l2protocol-tunnel {stp lacp lldp isis-l1 isis-l2 pvst cdp dtp vtp pagp udld}</code> | -/выключено | Включение режима инкапсуляции пакетов STP BPDU. |
| <code>no l2protocol-tunnel {stp lacp lldp isis-l1 isis-l2 pvst cdp dtp vtp pagp udld}</code> | | Выключение режима инкапсуляции пакетов STP BPDU. |
| <code>l2protocol-tunnel cos cos</code> | cos: (0..7)/5 | Задать значение CoS для запакованных PDU-кадров. |
| <code>no l2protocol-tunnel cos</code> | | Установка CoS в значение по умолчанию. |
| <code>l2protocol-tunnel drop-threshold {stp lacp lldp isis-l1 isis-l2 pvst cdp dtp vtp pagp udld} threshold</code> | treshold: (1..4096)/ выключено | Настройка порогового значения скорости входящих PDU-кадров (в пакетах в секунду), полученных и подлежащих инкапсуляции. При превышении порога PDU отбрасываются. |
| <code>no l2protocol-tunnel drop-threshold {stp lacp lldp isis-l1 isis-l2 pvst cdp dtp vtp pagp udld}</code> | | Отключает режим контроля скорости входящих PDU-кадров. |
| <code>l2protocol-tunnel shutdown-threshold {stp lacp lldp isis-l1 isis-l2 pvst cdp dtp vtp pagp udld} threshold</code> | treshold: (1..4096)/ выключено | Настройка порогового значения скорости входящих PDU-кадров (в пакетах в секунду), полученных и подлежащих инкапсуляции. При превышении порога порт будет переведен в состояние Errdisable (отключен). |
| <code>no l2protocol-tunnel shutdown-threshold {stp lacp lldp isis-l1 isis-l2 pvst cdp dtp vtp pagp udld}</code> | | Отключает режим контроля скорости входящих PDU-кадров. |

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 136 – Команды режима Privileged EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|---|--|---|
| <code>show l2protocol-tunnel [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet</code> | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); tve_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..48) | Отображает информацию L2PT для указанного интерфейса или для всех интерфейсов, на которых включен L2PT, если интерфейс не указан. |

| | | |
|---|---|--|
| <code>hu_port port-channel group]</code> | | |
| <code>clear l2protocol-tunnel statistics [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group]</code> | <code>gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..48)</code> | Очистка статистики L2PT для указанного интерфейса или для всех интерфейсов, на которых включен L2PT, если интерфейс не указан. |

Примеры выполнения команд

- Установить туннельный MAC-адрес в значение 01:00:0c:cd:cd:d0, включить отправку SNMP traps от триггера l2protocol-tunnel (триггера на срабатывание drop-threshold и shutdown-threshold).

```
console(config)#l2protocol-tunnel address 01:00:0c:cd:cd:d0
console(config)#snmp-server enable traps l2protocol-tunnel
```

- Включить режим туннелирования STP на интерфейсе, установить значение CoS-пакетов BPDU равным 4, включить контроль скорости входящих пакетов BPDU.

```
console(config)# interface tengigabitEthernet 1/0/1
console(config-if)# spanning-tree disable
console(config-if)# switchport mode customer
console(config-if)# switchport customervlan 100
console(config-if)# l2protocol-tunnel stp
console(config-if)# l2protocol-tunnel cos 4
console(config-if)# l2protocol-tunnel drop-threshold stp 40
console(config-if)# l2protocol-tunnel shutdown-threshold stp 100

console#show l2protocol-tunnel
```

| MAC address for tunneled frames: 01:00:0c:cd:cd:d0 | | | | | | | |
|--|-----|----------|--------------------|----------------|----------------|----------------|--------------|
| Port | CoS | Protocol | Shutdown Threshold | Drop Threshold | Encaps Counter | Decaps Counter | Drop Counter |
| te1/0/1 | 4 | stp | 100 | 40 | 650 | 0 | 450 |

Примеры сообщений о срабатывании триггера:

```
12-Nov-2015 14:32:35 %-I-DROP: Tunnel drop threshold 40 exceeded for interface
te1/0/1
12-Nov-2015 14:32:35 %-I-SHUTDOWN: Tunnel shutdown threshold 100 exceeded for
interface te1/0/1
```

5.16 Voice VLAN

Voice VLAN используется для выделения VoIP-оборудования в отдельную VLAN. Для VoIP-кадров могут быть назначены QoS-атрибуты для приоритизации трафика. Классификация кадров, относящихся к кадрам VoIP-оборудования, базируется на OUI (Organizationally Unique Identifier – первые 24 бита MAC-адреса) отправителя. Назначение Voice VLAN для порта происходит автоматически – когда на порт поступает кадр с OUI из таблицы Voice VLAN. Когда порт определяется, как принадлежащий Voice VLAN – данный порт добавляется во VLAN как tagged.

Voice VLAN применим для следующих схем:

- VoIP-оборудование настраивается, чтобы рассылать тегированные пакеты, с ID Voice VLAN, настроенным на коммутаторе;
- VoIP-оборудование рассылает нетегированные DHCP-запросы. В ответе от DHCP-сервера присутствует опция 132 (VLAN ID), с помощью которой устройство автоматически назначает себе VLAN для маркировки трафика (Voice VLAN).



Для назначения Voice VLAN на стороне оконечного оборудования необходимо использовать lldp-med политики или DHCP.

Список OUI-производителей VoIP-оборудования, доминирующих на рынке:

| OUI | Фирма-производитель |
|----------|---------------------|
| 00:E0:BB | 3COM |
| 00:03:6B | Cisco |
| 00:E0:75 | Veritel |
| 00:D0:1E | Pingtel |
| 00:01:E3 | Siemens |
| 00:60:B9 | NEC/ Philips |
| 00:0F:E2 | Huawei-3COM |
| 00:09:6E | Avaya |



Voice VLAN может быть активирован на портах, работающих в режиме trunk и general.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console (config) #
```

Таблица 137 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--|--------------------------------|--|
| voice vlan aging-timeout <i>timeout</i> | timeout: (1..43200)/1440 | Устанавливает таймаут для порта, принадлежащего к voice-vlan. Если с порта в течение заданного времени не было кадров с OUI VoIP-оборудования, то voice vlan удаляется с данного порта. |
| no voice vlan aging-timeout | | Восстанавливает значение по умолчанию. |
| voice vlan cos <i>cos</i> [<i>remark</i>] | cos: (0-7)/6 | Устанавливает выходную очередь для трафика в Voice VLAN в соответствии с настроенным для Voice VLAN CoS без смены CoS. - <i>remark</i> — включает переназначение CoS на указанный для трафика в Voice VLAN. |
| no voice vlan cos | | Восстанавливает значение по умолчанию. |
| voice vlan id <i>vlan_id</i> | | Устанавливает идентификатор VLAN для Voice VLAN |
| no voice vlan id | vlan_id: (1..4094) | Удаляет идентификатор VLAN для Voice VLAN Для удаления идентификатора VLAN требуется предварительно отключить функцию voice vlan на всех портах. |
| voice vlan oui-table { <i>add oui</i> <i>remove oui</i> } [<i>word</i>] | word: (1..32) символов | Позволяет редактировать таблицу OUI. - <i>oui</i> – первые 3 байта MAC-адреса; - <i>word</i> – описание oui. |
| no voice vlan oui-table | | Удаляет все пользовательские изменения OUI-таблицы. |
| voice vlan state { <i>oui-enabled</i> <i>disabled</i> } | -/выключено | Включить/отключить voice VLAN. |
| no voice vlan state | | Вернуть значение по умолчанию. |

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet, интерфейса группы портов:

```
console(config-if)#
```

Таблица 138 – Команды режима конфигурации интерфейса Ethernet

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---------------------------------------|---|
| voice vlan enable | -/отключено | Включает Voice VLAN для порта. |
| no voice vlan enable | | Отключает Voice VLAN для порта. |
| voice vlan cos mode {src all} | -/src | Включает маркировку трафика для всех кадров, либо только для источника. |
| no voice vlan cos mode | | Восстанавливает значение по умолчанию. |

5.17 Групповая адресация

5.17.1 Функция посредника протокола IGMP (IGMP Snooping)

Функция IGMP Snooping используется в сетях групповой рассылки. Основной задачей IGMP Snooping является предоставление многоадресного трафика только для тех портов, которые запросили его.



IGMP Snooping может использоваться только в статической группе VLAN. Поддерживаются версии протокола IGMP – IGMPv1, IGMPv2, IGMPv3.



Чтобы IGMP Snooping был активным, функция групповой фильтрации “bridge multicast filtering” должна быть включена (см. раздел 5.17.2 Правила групповой адресации (multicast addressing)).

Распознавание портов, к которым подключены многоадресные маршрутизаторы, основано на следующих событиях:

- IGMP-запросы приняты на порту;
- пакеты протокола Protocol Independent Multicast (PIM/PIMv2) приняты на порту;
- пакеты протокола многоадресной маршрутизации Distance Vector Multicast Routing Protocol (DVMRP) приняты на порту;
- пакеты протокола MRDISC приняты на порту;
- пакеты протокола Multicast Open Shortest Path First (MOSPF) приняты на порту.

Команды режима глобальной конфигурации


Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 139 – Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|----------------------------|---------------------------------------|---|
| ip igmp snooping | По умолчанию функция выключена | Разрешает использование функции IGMP Snooping коммутатором. |
| no ip igmp snooping | | Запрещает использование функции IGMP Snooping коммутатором. |

| | | |
|---|---|--|
| <code>ip igmp snooping vlan <i>vlan_id</i></code> | vlan_id: (1..4094) По умолчанию функция выключена | Разрешает использование функции IGMP Snooping коммутатором для данного интерфейса VLAN. - <i>vlan_id</i> – идентификационный номер VLAN. |
| <code>no ip igmp snooping vlan <i>vlan_id</i></code> | | Запрещает использование функции IGMP Snooping коммутатором для данного интерфейса VLAN. |
| <code>ip igmp snooping vlan <i>vlan_id</i> static <i>ip_multicast_address</i> [interface { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group}]</code> | vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Регистрирует групповой IP-адрес в таблице групповой адресации и статически добавляет интерфейсы из группы для текущей VLAN. - <i>vlan_id</i> – идентификационный номер VLAN; - <i>ip_multicast_address</i> – групповой IP-адрес. Перечисление интерфейсов осуществляется через «-» и «,». |
| <code>no ip igmp snooping vlan <i>vlan_id</i> static <i>ip_address</i> [interface { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group}]</code> | | Удаляет групповой IP-адрес из таблицы. |
| <code>ip igmp snooping vlan <i>vlan_id</i> mrouter learn pim-dvmrp</code> | vlan_id: (1..4094) По умолчанию разрешено | Разрешает для данной группы VLAN автоматическое распознавание портов, к которым подключены многоадресные маршрутизаторы. - <i>vlan_id</i> – идентификационный номер VLAN. |
| <code>no ip igmp snooping vlan <i>vlan_id</i> mrouter learn pim-dvmrp</code> | | Запрещает для данной группы VLAN автоматическое распознавание портов, к которым подключены многоадресные маршрутизаторы. |
| <code>ip igmp snooping vlan <i>vlan_id</i> mrouter interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group}</code> | vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Определяет порт, к которому подключен маршрутизатор многоадресной рассылки для заданной VLAN. - <i>vlan_id</i> – идентификационный номер VLAN. |
| <code>no ip igmp snooping vlan <i>vlan_id</i> mrouter interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group}</code> | | Указывает, что к порту не подключен маршрутизатор многоадресной рассылки. |
| <code>ip igmp snooping vlan <i>vlan_id</i> forbidden mrouter interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group}</code> | vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Устанавливает запрет на определение порта (статически, динамически) как порта, к которому подключен маршрутизатор многоадресной рассылки. - <i>vlan_id</i> – идентификационный номер VLAN. |
| <code>no ip igmp snooping vlan <i>vlan_id</i> forbidden mrouter interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group}</code> | | Снимает запрет на определение порта как порта, к которому подключен маршрутизатор многоадресной рассылки. |
| <code>ip igmp snooping vlan <i>vlan_id</i> querier</code> | vlan_id: (1..4094); | Включает поддержку выдачи запросов igmp-query коммутатором в данной VLAN. |

| | | |
|---|---|--|
| <code>no ip igmp snooping vlan <i>vlan_id</i> querier</code> | -/выдача запросов отключена | Отключает поддержку выдачи запросов igmp-query коммутатором в данной VLAN. |
| <code>ip igmp snooping vlan <i>vlan_id</i> querier version {2 3}</code> | -/IGMPv3 | Устанавливает версию IGMP-протокола, на основании которой будут формироваться IGMP-query запросы. |
| <code>no ip igmp snooping vlan <i>vlan_id</i> querier version</code> | | Устанавливает значение по умолчанию. |
| <code>ip igmp snooping vlan <i>vlan_id</i> querier address <i>ip_address</i></code> | vlan_id: (1..4094) | Определяет исходный IP-адрес, который будет использоваться IGMP querier-ом. Querier – устройство, которое отправляет IGMP-запросы. |
| <code>no ip igmp snooping vlan <i>vlan_id</i> querier address</code> | | Устанавливает значение по умолчанию. По умолчанию если IP-адрес настроен для VLAN, он используется в качестве адреса источника IGMP Snooping Querier. |
| <code>ip igmp snooping vlan <i>vlan_id</i> replace source-ip <i>ip_address</i></code> | vlan_id: (1..4094); ip_address: A.B.C.D/0.0.0.0 | Включает замену IP-адреса источника на указанный IP-адрес во всех пакетах IGMP report в заданной VLAN. - <i>vlan_id</i> – идентификационный номер VLAN; - <i>A.B.C.D</i> – IP-адрес, на который будет произведена замена SRC IP.  Значение по умолчанию 0.0.0.0 говорит о том, что замена SRC IP IGMP report производится не будет. |
| <code>no ip igmp snooping vlan <i>vlan_id</i> replace source-ip</code> | | Отключает замену IP-адреса источника в пакетах IGMP report в заданной VLAN. |
| <code>ip igmp snooping vlan <i>vlan_id</i> immediate-leave [host-based]</code> | vlan_id: (1..4094); -/выключено | Включить процесс IGMP Snooping Immediate-Leave на текущей VLAN. Означает, что порт должен быть немедленно удален из группы IGMP после получения сообщения IGMP leave. - host-based – механизм fast-leave срабатывает только в том случае, когда все подключенные к данному порту пользователи отписались от группы (счетчик пользователей ведется на основании Source MAC-адресов в заголовках IGMP-report'ов); |
| <code>no ip igmp snooping vlan <i>vlan_id</i> immediate-leave</code> | | Отключить процесс IGMP Snooping Immediate-Leave на текущей VLAN. |
| <code>ip igmp snooping vlan <i>vlan_id</i> proxy-report [version <i>version</i>]</code> | vlan_id: (1..4094); version: (1..3) | Включить функцию проху report в определенном VLAN. При включении этой функции коммутатор на пришедшие IGMP query будет отвечать от своего имени. Клиентские IGMP report при этом отбрасываются. - version – устанавливает версию IGMP для отправки пакетов. По умолчанию версия определяется по пришедшему на коммутатор пакету IGMP query. |
| <code>no ip igmp snooping vlan <i>vlan_id</i> proxy-report</code> | | Выключить Proxy report в определенном VLAN. |
| <code>ip igmp snooping vlan <i>vlan_id</i> cos <i>cos</i></code> | vlan_id: (1..4094); cos: (0..7)/0 | Устанавливает значение CoS для исходящих в порт mrouter IGMP-сообщений в указанной VLAN. - <i>vlan_id</i> – идентификационный номер VLAN; - <i>cos</i> – класс обслуживания. |
| <code>no ip igmp snooping vlan <i>vlan_id</i> cos <i>cos</i></code> | | Устанавливает значение CoS для исходящих в порт mrouter IGMP-сообщений в указанной VLAN равным нулю. |

Команды режима конфигурации интерфейса VLAN

Вид запроса командной строки режима конфигурации VLAN:

```
console(config-if) #
```

Таблица 140 – Команды режима конфигурации интерфейса VLAN

| Команда | Значение/Значение по умолчанию | Действие |
|---------------------------------------|---------------------------------------|--|
| <code>ip igmp robustness count</code> | count: (1..7)/2 | Устанавливает значение устойчивости для IGMP. Если на канале наблюдается потеря данных, значение устойчивости должно быть увеличено. |
| <code>no ip igmp robustness</code> | | Устанавливает значение по умолчанию. |


| | | |
|--|--|--|
| <code>ip igmp query-interval seconds</code> | seconds: (30..18000)/125 c | Устанавливает таймаут, по которому система отправляет основные запросы всем участникам группы многоадресной передачи для проверки их активности. |
| <code>no ip igmp query-interval</code> | | Устанавливает значение по умолчанию. |
| <code>ip igmp query-max-response-time seconds</code> | seconds: (5..20)/10 c | Устанавливает максимальное время ответа на запрос. |
| <code>no ip igmp query-max-response-time</code> | | Устанавливает значение по умолчанию. |
| <code>ip igmp last-member-query-count count</code> | count: (1..7)/значение переменной robustness | Устанавливает количество запросов, после рассылки которых, коммутатор определяет, что на данном порту нет желающих участвовать в многоадресной рассылке. |
| <code>no ip igmp last-member-query-count</code> | | Устанавливает значение по умолчанию. |
| <code>ip igmp last-member-query-interval milliseconds</code> | milliseconds: (100..25500)/1000 mc | Устанавливает интервал запроса для последнего участника. |
| <code>no ip igmp last-member-query-interval</code> | | Устанавливает значение по умолчанию. |
| <code>ip igmp version version</code> | version: (1-3)/2 | Установить версию протокола IGMP. |
| <code>no ip igmp version</code> | | Установить значение по умолчанию. |

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet

Вид запроса командной строки режима конфигурации интерфейса:

```
console(config-if) #
```

Таблица 141 – Команды режима конфигурации интерфейса Ethernet

| Команда | Значение/Значение по умолчанию | Действие |
|--|---------------------------------------|--|
| <code>switchport access multicast-tv vlan vlan_id</code> | vlan_id: (1..4094) | Включает перенаправление IGMP-запросов с клиентских VLAN в Multicast VLAN для интерфейса в режиме «access».  Для работы данной функции требуется включение ip igmp snooping не только глобально и в Multicast VLAN, но и в клиентских VLAN. |
| <code>no switchport access multicast-tv vlan</code> | | Выключает перенаправление IGMP-запросов с клиентских Vlan в Multicast Vlan для интерфейса в режиме «access». |
| <code>switchport trunk multicast-tv vlan vlan_id [tagged]</code> | vlan_id: (1..4094) | Включает перенаправление IGMP-запросов из VLAN, участником которых является порт, в Multicast VLAN для интерфейса в режиме «trunk». Multicast-трафик передается на порт нетегированным или тегированным в зависимости от параметра tagged. Параметр tagged указывает на то, что Multicast-трафик должен отправляться в порт тегированным в Multicast VLAN. |
| <code>no switchport trunk multicast-tv vlan</code> | | Выключает перенаправление IGMP-запросов в Multicast VLAN. Порт исключается из групп многоадресной рассылки в Multicast VLAN. |
| <code>switchport general multicast-tv vlan vlan_id [tagged]</code> | vlan_id: (1..4094) | Включает перенаправление IGMP-запросов из VLAN, участником которых является порт, в Multicast VLAN для интерфейса в режиме «general». Multicast-трафик передается на порт нетегированным или тегированным в зависимости от параметра tagged. Параметр tagged указывает на то, что Multicast-трафик должен отправляться в порт тегированным в Multicast VLAN. |
| <code>no switchport general multicast-tv vlan</code> | | Выключает перенаправление IGMP-запросов в Multicast VLAN. Порт исключается из групп многоадресной рассылки в Multicast VLAN. |

Команды режима EXEC

Все команды доступны только для привилегированного пользователя.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 142 – Команды режима EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---------------------------------------|---|
| show ip igmp snooping mrouter [interface <i>vlan_id</i>] | vlan_id: (1..4094) | Показывает информацию об изученных многоадресных маршрутизаторах в указанной группе VLAN. |
| show ip igmp snooping interface <i>vlan_id</i> | vlan_id: (1..4094) | Показывает информацию IGMP-snooping для данного интерфейса. |
| show ip igmp snooping groups [vlan <i>vlan_id</i>] [ip-multicast-address <i>ip_multicast_address</i>] [ip-address <i>IP_address</i>] | vlan_id: (1..4094) | Показывает информацию об изученных многоадресных группах, участвующих в групповой рассылке. |
| show ip igmp snooping cpe vlans [vlan <i>vlan_id</i>] | vlan_id: (1..4094) | Показывает таблицу соответствий между VLAN оборудования, установленного у пользователя, и VLAN для телевидения. |

Примеры выполнения команд

Включить функцию IGMP snooping на коммутаторе. Для VLAN 6 разрешить автоматическое распознавание портов, к которым подключены многоадресные маршрутизаторы. Увеличить значение устойчивости до 4. Установить максимальное время ответа на запрос – 15 секунд.

```
console# configure
console (config)# ip igmp snooping
console (config-if)# ip igmp snooping vlan 6 mrouter learn pim-dvmrp
console (config)# interface vlan 6
console (config-if)# ip igmp robustness 4
console (config-if)# ip igmp query-max-response-time 15
```

5.17.2 Правила групповой адресации (multicast addressing)

Данный класс команд предназначен для задания правил групповой адресации в сети на канальном и сетевом уровнях модели OSI.

Команды режима конфигурации интерфейса VLAN

Вид запроса командной строки в режиме конфигурации интерфейса VLAN:

```
console (config-if) #
```

Таблица 143 – Команды режима конфигурации интерфейса VLAN

| Команда | Значение/Значение по умолчанию | Описание |
|--|---|--|
| bridge multicast mode {mac-group ipv4-group ipv4-src-group} | -/mac-group | Задаёт режим групповой передачи данных. - mac-group – многоадресная передача, основанная на VLAN и MAC-адресах; - ipv4-group – многоадресная передача с типом фильтрации, основанной на VLAN и адресе приемника в формате IPv4; - ip-src-group – многоадресная передача с типом фильтрации, основанной на VLAN и адресе отправителя в формате IPv4. |
| no bridge multicast mode | | Устанавливает значение по умолчанию. |
| bridge multicast address {mac_multicast_address ip_multicast_address} [{add remove}] {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port port-channel group} | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); tve_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Добавляет групповой MAC-адрес в таблицу групповой адресации и статически добавляет или удаляет интерфейсы из группы. - mac_multicast_address – групповой MAC-адрес; - ip_multicast_address – IP-адрес многоадресной рассылки; - add – добавляет статическую подписку к групповому MAC-адресу диапазона Ethernet-портов или групп портов. - remove – удаляет статическую подписку к групповому MAC-адресу. Перечисление интерфейсов осуществляется через «-» и «,» |
| no bridge multicast address {mac_multicast_address ip_multicast_address } | | Удаляет групповой MAC-адрес из таблицы. |
| bridge multicast forbidden address {mac_multicast_address ip_multicast_address} [{add remove}] {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port port-channel group} | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); tve_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Запрещает подключение настраиваемого порта/портов к групповому IPv6-адресу (MAC-адресу). - mac_multicast_address – групповой MAC-адрес; - ip_multicast_address – IP-адрес многоадресной рассылки; - add – добавление порта/портов в список запрещенных; - remove – удаление порта/портов из списка запрещенных. Перечисление интерфейсов осуществляется через «-» и «,» |
| no bridge multicast forbidden address {mac_multicast_address ip_multicast_address } | | Удаляет запрещающее правило для группового MAC-адреса. |
| bridge multicast forward-all {add remove} {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port port-channel group} | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); tve_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) По умолчанию передача всех многоадресных пакетов запрещена. | Разрешает передачу всех многоадресных пакетов на порту. - add – добавляет порты/объединенные порты в список портов, для которых разрешена передача всех групповых пакетов; - remove – убирает группу портов/объединенных портов из разрешающего правила. Перечисление интерфейсов осуществляется через «-» и «,». |
| no bridge multicast forward-all | | Восстанавливает значение по умолчанию. |
| bridge multicast forbidden forward-all {add remove} {gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel group} | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); tve_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) По умолчанию портам не запрещено динамически присоединяться к многоадресной группе. | Запрещает порту динамически добавляться к многоадресной группе. - add – добавляет порты/объединенные порты в список портов, для которых запрещена передача всех групповых пакетов; - remove – убирает группу портов/объединенных портов из запрещающего правила. Перечисление интерфейсов осуществляется через «-» и «,». |
| no bridge multicast forbidden forward-all | | Восстанавливает значение по умолчанию. |

| | | |
|--|---|--|
| bridge multicast ip-address <i>ip_multicast_address</i> { add remove } { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group } | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..128) | Регистрирует IP-адрес в таблице групповой адресации и статически добавляет/удаляет интерфейсы из группы. - <i>ip_multicast_address</i> – групповой IP-адрес; - add – добавляет порты к группе; - remove – удаляет порты из группы. Перечисление интерфейсов осуществляется через «-» и «,». |
| no bridge multicast ip-address <i>ip_multicast_address</i> | | Удаляет групповой IP-адрес из таблицы. |
| bridge multicast forbidden ip-address <i>ip_multicast_address</i> { add remove } { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group } | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..128) | Запрещает порту динамически добавляться к многоадресной группе. - <i>ip_multicast_address</i> – групповой IP-адрес; - add – добавление порта/портов к списку запрещенных; - remove – удаление порта/портов из списка запрещенных. Перечисление интерфейсов осуществляется через «-» и «,» <input checked="" type="checkbox"/> Прежде чем определить запрещенные порты, группы многоадресной рассылки должны быть зарегистрированы. |
| no bridge multicast forbidden ip-address <i>ip_multicast_address</i> | | Восстанавливает значение по умолчанию. |
| bridge multicast source ip_address group <i>ip_multicast_address</i> { add remove } { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group } | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..128) | Устанавливает соответствие между IP-адресом пользователя и групповым адресом в таблице групповой адресации, и статически добавляет/удаляет интерфейсы из группы. - <i>ip_address</i> – исходный IP-адрес; - <i>ip_multicast_address</i> – групповой IP-адрес; - add – добавить порты в группу исходного IP-адреса; - remove – удалить порты из группы исходного IP-адреса. |
| no bridge multicast source ip_address group <i>ip_multicast_address</i> | | Восстанавливает значение по умолчанию. |
| bridge multicast forbidden source ip_address group <i>ip_multicast_address</i> { add remove } { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group } | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..128) | Устанавливает запрет на добавление/удаление соответствия между IP-адресом пользователя и групповым адресом в таблице групповой адресации для определенного порта. - <i>ip_address</i> – исходный IP-адрес; - <i>ip_multicast_address</i> – групповой IP-адрес; - add – запрет на добавление порта в группу исходного IP-адреса; - remove – запрет на удаление порта из группы исходного IP-адреса. |
| no bridge multicast forbidden source ip_address group <i>ip_multicast_address</i> | | Восстанавливает значение по умолчанию. |
| bridge multicast ipv6 mode { mac-group ip-group ip-src-group } | -/ mac-group | Задает режим групповой передачи данных для IPv6-пакетов многоадресной рассылки. - mac-group – многоадресная передача, основанная на VLAN и MAC-адресах; - ip-group – многоадресная передача с типом фильтрации, основанной на VLAN и адресе приемника в формате IPv6; - ip-src-group – многоадресная передача с типом фильтрации, основанной на VLAN и адресе отправителя в формате IPv6. |
| no bridge multicast ipv6 mode | | Устанавливает значение по умолчанию. |

| | | |
|---|--|--|
| bridge multicast ipv6 ip-address <i>ipv6_multicast_address</i> { add remove } { gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group } | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Регистрирует групповой IPv6-адрес в таблице групповой адресации, и статически добавляет/удаляет интерфейсы из группы. - <i>ipv6_multicast_address</i> – групповой IP-адрес; - add – добавляет порты к группе; - remove – удаляет порты из группы. Перечисление интерфейсов осуществляется через «-» и «,». |
| no bridge multicast ipv6 ip-address <i>ipv6_multicast_address</i> | | Удаляет групповой IP-адрес из таблицы. |
| bridge multicast ipv6 forbidden ip-address <i>ipv6_multicast_address</i> { add remove } { gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group } | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Запрещает подключение настраиваемого порта/портов к групповому IPv6-адресу. - <i>ipv6_multicast_address</i> – групповой IP-адрес; - add – добавление порта/портов в список запрещенных; - remove – удаление порта/портов из списка запрещенных. Перечисление интерфейсов осуществляется через «-» и «,» |
| no bridge multicast ipv6 forbidden ip-address <i>ipv6_multicast_address</i> | | Восстанавливает значение по умолчанию. |
| bridge multicast ipv6 source ip-address group <i>ipv6_multicast_address</i> { add remove } { gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group } | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Устанавливает соответствие между IPv6-адресом пользователя и групповым адресом в таблице групповой адресации, и статически добавляет/удаляет интерфейсы из группы. - <i>ipv6_address</i> – исходный IP-адрес; - <i>ipv6_multicast_address</i> – групповой IP-адрес; - add – добавить порты в группу исходного IP-адреса; - remove – удалить порты из группы исходного IP-адреса. |
| no bridge multicast ipv6 source ip-address group <i>ipv6_multicast_address</i> | | Восстанавливает значение по умолчанию. |
| bridge multicast ipv6 forbidden source ip-address group <i>ipv6_multicast_address</i> { add remove } { gigabitethernet gi_port tengigabitethernet te_port hundredgigabitethernet hu_port port-channel group } | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Устанавливает запрет на добавление/удаление соответствия между IPv6-адресом пользователя и групповым адресом в таблице групповой адресации для определенного порта. - <i>ipv6_address</i> – исходный IPv6-адрес; - <i>ipv6_multicast_address</i> – групповой IPv6-адрес; - add – запрет на добавление порта в группу исходного IPv6-адреса; - remove – запрет на удаление порта из группы исходного IPv6-адреса. |
| no bridge multicast ipv6 forbidden source ip-address group <i>ipv6_multicast_address</i> | | Восстанавливает значение по умолчанию. |

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet, интерфейса группы портов:

```

console# configure
console(config)# interface {gigabitethernet gi_port | tengigabitethernet te_port | twentyfivegigabitethernet twe_port | hundredgigabitethernet hu_port | port-channel group | range {...}}
console(config-if)#

```

Таблица 144 – Команды режима конфигурации интерфейса Ethernet, VLAN, группы интерфейсов

| Команда | Значение/Значение по умолчанию | Описание |
|---|--------------------------------|--|
| bridge multicast unregistered {forwarding filtering} | -/forwarding | Устанавливает правило передачи пакетов с незарегистрированных групповых адресов. - forwarding – передавать незарегистрированные многоадресные пакеты; - filtering – фильтровать незарегистрированные многоадресные пакеты. |
| no bridge multicast unregistered | | Устанавливает значение по умолчанию. |

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 145 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Описание |
|--|--|---|
| bridge multicast filtering | -/отключено | Включает фильтрацию групповых адресов. |
| no bridge multicast filtering | | Отключает фильтрацию групповых адресов. |
| mac address-table aging-time <i>seconds</i> | seconds: (10..400)/300 секунд | Задаёт время хранения MAC-адреса в таблице глобально. |
| no mac address-table aging-time | | Устанавливает значение по умолчанию. |
| mac address-table learning <i>vlan vlan_id</i> | vlan_id: (1..4094, all)/включено | Включить изучение MAC-адресов в данном VLAN. |
| no mac address-table learning <i>vlan vlan_id</i> | | Отключить изучение MAC-адресов в данном VLAN. |
| mac address-table static <i>mac_address vlan vlan_id</i> interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> } [permanent delete-on-reset delete-on-timeout secure] | vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Добавляет исходный MAC-адрес в таблицу групповой адресации. - <i>mac_address</i> – MAC-адрес; - <i>vlan_id</i> – номер VLAN; - permanent – данный MAC-адрес можно удалить только с помощью команды no bridge address ; - delete-on-reset – данный адрес удалится после перезагрузки устройства; - delete-on-timeout – данный адрес удалится по тайм-ауту; - secure – данный адрес удалится только с помощью команды no bridge address или после возвращения порта в режим обучения (no port security). |
| no mac address-table static [<i>mac_address</i>] <i>vlan vlan_id</i> | | Удаляет MAC-адрес из таблицы групповой адресации. |
| bridge multicast reserved-address <i>mac_multicast_address</i> {ethernet-v2 <i>ethtype</i> llc <i>sap</i> llc-snap <i>pid</i> } {discard bridge} | ethtype: (0x0600..0xFFFF); sap: (0..0xFFFF); pid: (0..0xFFFFFFFF) | Определяет действие для пакетов многоадресной рассылки с зарезервированного адреса. - <i>mac_multicast_address</i> – групповой MAC-адрес; - <i>ethtype</i> – тип пакета Ethernet v2; - <i>sap</i> – тип пакета LLC; - <i>pid</i> – тип пакета LLC-Snap; - discard – сброс пакетов; - bridge – пакеты передаются в режиме bridge. |
| no bridge multicast reserved-address <i>mac_multicast_address</i> [ethernet-v2 <i>ethtype</i> llc <i>sap</i> llc-snap <i>pid</i>] | | Устанавливает значение по умолчанию. |

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 146 – Команды режима Privileged EXEC

| Команда | Значение/Значение по умолчанию | Описание |
|--|--|---|
| clear mac address-table {dynamic secure} [interface {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port port-channel group}] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); tve_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Удаляет статические/динамические записи из таблицы групповой адресации. - dynamic – удаление динамических записей; - secure – удаление статических записей. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 147 – Команды режима EXEC

| Команда | Значение/Значение по умолчанию | Описание |
|---|---|---|
| show mac address-table [dynamic static secure] [vlan vlan_id] [interface {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port port-channel group}] [address mac_address] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); tve_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128); vlan_id: (1..4094) | Показывает таблицу MAC-адресов для указанного интерфейса либо всех интерфейсов. - dynamic – просмотр только динамических записей; - static – просмотр только статических записей; - secure – просмотр только безопасных записей; - vlan_id – идентификационный номер VLAN; - mac-address – MAC-адрес. |
| show mac address-table count [vlan vlan_id] [interface {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port port-channel group}] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); tve_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128); vlan_id: (1..4094) | Показывает количество записей в таблице MAC-адресов для указанного интерфейса либо для всех интерфейсов. - vlan_id – идентификационный номер VLAN. |
| show bridge multicast address-table [vlan vlan_id] [address {mac_multicast_address ipv4_multicast_address ipv6_multicast_address}] [format {ip mac}] [source {ipv4_source_address ipv6_source_address}] | vlan_id: (1..4094) | Показывает таблицу групповых адресов для указанного интерфейса либо всех интерфейсов VLAN (команда доступна только для привилегированного пользователя). - vlan_id – идентификационный номер VLAN; - mac_multicast_address – групповой MAC-адрес; - ipv4_multicast_address – групповой IPv4-адрес; - ipv6_multicast_address – групповой IPv6-адрес; - ip – просмотр по IP-адресам; - mac – просмотр по MAC-адресам; - ipv4_source_address – IPv4-адрес источника; - ipv6_source_address – IPv6-адрес источника. |

| | | |
|---|--|--|
| show bridge multicast address-table static [vlan <i>vlan_id</i>] [address { <i>mac_multicast_address</i> <i>ipv4_multicast_address</i> <i>ipv6_multicast_address</i> } [source <i>ipv4_source_address</i> <i>ipv6_source_address</i>] [all mac ip] | vlan_id: (1..4094) | Показывает таблицу статических групповых адресов для указанного интерфейса либо всех интерфейсов VLAN. - <i>vlan_id</i> – идентификационный номер VLAN; - <i>mac_multicast_address</i> – групповой MAC-адрес; - <i>ipv4_multicast_address</i> – групповой IPv4-адрес; - <i>ipv6_multicast_address</i> – групповой IPv6-адрес; - <i>ipv4_source_address</i> – IPv4-адрес источника; - <i>ipv6_source_address</i> – IPv6-адрес источника; - ip – просмотр по IP-адресам; - mac – просмотр по MAC-адресам; - all – просмотр полной таблицы. |
| show bridge multicast filtering <i>vlan_id</i> | vlan_id: (1..4094) | Показывает конфигурацию фильтра групповых адресов для указанного VLAN. - <i>vlan_id</i> – идентификационный номер VLAN. |
| show bridge multicast unregistered [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i>] | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..128); <i>vlan_id</i> : (1..4094) | Показывает конфигурацию фильтра для незарегистрированных групповых адресов. |
| show bridge multicast mode [vlan <i>vlan_id</i>] | vlan_id: (1..4094) | Показывает режим групповой адресации для указанного интерфейса либо всех интерфейсов VLAN. - <i>vlan_id</i> – идентификационный номер VLAN. |
| show bridge multicast reserved-addresses | - | Отображает правила, установленные для групповых зарезервированных адресов. |

Примеры выполнения команд

- Включить фильтрацию групповых адресов коммутатором. Задать время хранения MAC-адреса 400 секунд, разрешить передачу незарегистрированных многоадресных пакетов на 11 порту коммутатора.

```

console # configure
console(config) # mac address-table aging-time 400
console(config) # bridge multicast filtering
console(config) # interface tengigabitethernet 1/0/11
console(config-if) # bridge multicast unregistered forwarding

console# show bridge multicast address-table format ip

```

| Vlan | IP/MAC Address | type | Ports |
|------|-------------------|---------|--------------|
| 1 | 224-239.130 2.2.3 | dynamic | te0/1, te0/2 |
| 19 | 224-239.130 2.2.8 | static | te0/1-8 |
| 19 | 224-239.130 2.2.8 | dynamic | te0/9-11 |

Forbidden ports for multicast addresses:

| Vlan | IP/MAC Address | Ports |
|------|-------------------|-------|
| 1 | 224-239.130 2.2.3 | te0/8 |
| 19 | 224-239.130 2.2.8 | te0/8 |

5.17.3 MLD Snooping – протокол контроля многоадресного трафика в IPv6

MLD Snooping – механизм многоадресной рассылки сообщений, позволяющий минимизировать многоадресный трафик в IPv6-сетях.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console (config) #
```

Таблица 148 – Команды глобального режима конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|---|--|--|
| <code>ipv6 mld snooping [vlan vlan_id]</code> | vlan_id: (1..4094) -/выключено | Включает MLD snooping. |
| <code>no ipv6 mld snooping [vlan vlan_id]</code> | | Отключает MLD snooping. |
| <code>ipv6 mld snooping vlan vlan_id static ipv6_multicast_address [interface { gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group}]</code> | vlan_id: (1..4094); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Регистрирует групповой IPv6-адрес в таблице групповой адресации и статически добавляет/удаляет интерфейсы из группы для текущей VLAN. - <i>ipv6_multicast_address</i> – групповой IPv6-адрес; Перечисление интерфейсов осуществляется через «-» и «,». |
| <code>no ipv6 mld snooping vlan vlan_id static ipv6_multicast_address [interface { gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group}]</code> | | Удаляет групповой IP-адрес из таблицы. |
| <code>ipv6 mld snooping vlan vlan_id forbidden mrouter interface {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group}</code> | vlan_id: (1..4094); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Добавляет правило, запрещающее портам из списка регистрироваться как MLD-mrouter. |
| <code>no ipv6 mld snooping vlan vlan_id forbidden mrouter interface {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group}</code> | | Удаляет правило, запрещающее портам из списка регистрироваться как MLD-mrouter. |
| <code>ipv6 mld snooping vlan vlan_id mrouter learn pim-dvmrp</code> | vlan_id: (1..4094); -/включено | Изучать порты, подключенные к mrouter по MLD-query-пакетам. |
| <code>no ipv6 mld snooping vlan vlan_id mrouter learn pim-dvmrp</code> | | Не изучать порты, подключенные к mrouter по MLD-query-пакетам. |

| | | |
|--|---|---|
| <code>ipv6 mld snooping vlan <i>vlan_id</i> mrouter interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i>}</code> | vlan_id: (1..4094); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Добавляет список mrouter-портов. |
| <code>no ipv6 mld snooping vlan <i>vlan_id</i> mrouter interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i>}</code> | | Удаляет mrouter-порты. |
| <code>ipv6 mld snooping vlan <i>vlan_id</i> immediate-leave</code> | vlan_id: (1..4094) | Включить процесс MLD Snooping Immediate-Leave на текущей VLAN. |
| <code>no ipv6 mld snooping vlan <i>vlan_id</i> immediate-leave</code> | -/выключено | Отключить процесс MLD Snooping Immediate-Leave на текущей VLAN. |
| <code>ipv6 mld snooping querier</code> | | Включает поддержку выдачи запросов igmp-query. |
| <code>no ipv6 mld snooping querier</code> | -/выключено | Отключает поддержку выдачи запросов igmp-query. |

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов, интерфейса VLAN

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet, интерфейса группы портов и интерфейса VLAN:

```
console(config-if) #
```

Таблица 149 – Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов, интерфейса VLAN

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---|--|
| <code>ipv6 mld last-member-query-interval <i>interval</i></code> | interval: (100..25500)/1000 миллисекунд | Задаёт максимальную задержку ответа последнего члена группы, которая используется для вычисления кода максимальной задержки ответа (Max Response Code). |
| <code>no ipv6 mld last-member-query-interval</code> | | Восстанавливает значение по умолчанию. |
| <code>ipv6 mld last-member-query-count <i>count</i></code> | (1..7)/значение переменной robustness | Устанавливает количество запросов, после рассылки которых, коммутатор определяет, что на данном порту нет желающих участвовать в многоадресной рассылке. |
| <code>no ipv6 mld last-member-query-count</code> | | Устанавливает значение по умолчанию. |
| <code>ipv6 mld query-interval <i>value</i></code> | value: (30..18000)/125 секунд | Задаёт интервал рассылки основных MLD-запросов. |
| <code>no ipv6 mld query-interval</code> | | Восстанавливает значение по умолчанию. |
| <code>ipv6 mld query-max-response-time <i>value</i></code> | value: (5..20)/10 секунд | Задаёт максимальную задержку ответа, которая используется для вычисления кода максимальной задержки ответа. |
| <code>no ipv6 mld query-max-response-time</code> | | Восстанавливает значение по умолчанию. |
| <code>ipv6 mld robustness <i>value</i></code> | value: (1..7)/2 | Устанавливает значение коэффициента отказоустойчивости. Если на канале наблюдается потеря данных, коэффициент отказоустойчивости должен быть увеличен. |
| <code>no ipv6 mld robustness</code> | | Восстанавливает значение по умолчанию. |
| <code>ipv6 mld version <i>version</i></code> | version: (1..2)/2 | Устанавливает версию протокола, действующую на данном интерфейсе. |
| <code>no ipv6 mld version</code> | | Восстанавливает значение по умолчанию. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 150 – Команды режима EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|--|---------------------------------------|---|
| show ipv6 mld snooping groups [vlan <i>vlan_id</i>] [address <i>ipv6_multicast_address</i>] [source <i>ipv6_address</i>] | vlan_id: (1..4094) | Отображает информацию о зарегистрированных группах в соответствии с заданными в команде параметрами фильтрации. - <i>ipv6_multicast_address</i> – групповой адрес IPv6; - <i>ipv6_address</i> – IPv6-адрес источника. |
| show ipv6 mld snooping interface <i>vlan_id</i> | vlan_id: (1..4094) | Отображает информацию о конфигурации MLD-snooping для данной VLAN. |
| show ipv6 mld snooping mrouter [interface <i>vlan_id</i>] | vlan_id: (1..4094) | Отображает информацию о mrouter-портах. |

5.17.4 Функция ограничения multicast-трафика


Функции ограничения multicast-трафика используются для удобной настройки ограничения просмотра определенных групп многоадресной рассылки.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 151 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--|---------------------------------------|---|
| multicast snooping profile <i>profile_name</i> | | Переход в режим конфигурации multicast-профиля. |
| no multicast snooping profile <i>profile_name</i> | profile_name: (1..32) символов | Удалить указанный multicast-профиль.  Multicast-профиль может быть удален только после того, как будет отвязан от всех портов коммутатора. |

Команды режима конфигурации multicast-профиля

Вид запроса командной строки режима конфигурации multicast-профиля:

```
console(config-mc-profile)#
```

Таблица 152 – Команды режима конфигурации multicast-профиля

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|---|
| match ip <i>low_ip</i> [<i>high_ip</i>] | <i>low_ip</i> : валидный multicast-адрес; | Задает соответствие профиля указанному диапазону IPv4 multicast-адресов. |
| no match ip <i>low_ip</i> [<i>high_ip</i>] | <i>high_ip</i> : валидный multicast-адрес | Удаляет соответствие профиля указанному диапазону IPv4 multicast-адресов. |
| match ipv6 <i>low_ipv6</i> [<i>high_ipv6</i>] | | Задает соответствие профиля указанному диапазону IPv6 multicast-адресов. |

| | | |
|--|--|--|
| no match ipv6 <i>low_ipv6</i> [<i>high_ipv6</i>] | low_ipv6: валидный IPv6 multicast-адрес; high_ipv6: валидный IPv6 multicast-адрес | Удаляет соответствие профиля указанному диапазону IPv6 multicast-адресов. |
| permit | -/no permit | В случае несоответствия одному из заданных диапазонов, IGMP-report будут пропускаться. |
| no permit | | В случае несоответствия одному из заданных диапазонов, IGMP-report будут отбрасываться. |

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet

Вид запроса командной строки режима конфигурации интерфейса:

```
console(config-if)#
```

Таблица 153 – Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet

| Команда | Значение/Значение по умолчанию | Действие |
|--|---------------------------------------|--|
| multicast snooping max-groups <i>number</i> | number (1..1000)/- | Ограничивает количество одновременно просматриваемых multicast-групп для интерфейса. |
| no multicast snooping maxgroups | | Снимает ограничение на количество одновременно просматриваемых групп для интерфейса. |
| multicast snooping add <i>profile_name</i> | profile name: (1..32) символов | Привязывает указанный multicast-профиль к интерфейсу. |
| multicast snooping remove { <i>profile_name</i> all} | | Удаляет соответствие multicast-профиля (всех multicast-профилей) интерфейсу. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 154 – Команды режима EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|--|---------------------------------------|---|
| show multicast snooping groups count | - | Отображает информацию для всех портов о текущем количестве зарегистрированных групп, а также максимальное возможное количество. |
| show multicast snooping profile [<i>profile_name</i>] | profile name: (1..32) символов | Отображает информацию о multicast-профилях, которые были сконфигурированы. |

5.17.5 RADIUS-авторизация запросов IGMP

Данный механизм позволяет производить авторизацию запросов протокола IGMP с помощью RADIUS-сервера. Для обеспечения надежности и распределения нагрузки может использоваться несколько RADIUS-серверов. Выбор сервера для отправки очередного запроса авторизации происходит случайным образом. Если сервер не ответил, он помечается как временно нерабочий, и перестает участвовать в механизме опроса на определенный период, а запрос отсылается на следующий сервер.

Полученные авторизационные данные хранятся в кэш-памяти коммутатора в течение заданного периода времени. Это позволяет ускорить повторную обработку IGMP-запросов.

Параметры авторизации включают в себя:

- MAC-адрес клиентского устройства;
- Идентификатор порта коммутатора;
- IP-адрес группы;
- Решение о доступе – deny/permit.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console (config) #
```

Таблица 155 – Команды режима глобального конфигурирования

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---------------------------------------|---|
| ip igmp snooping authorization cache-timeout <i>timeout</i> | timeout: (0..10000) мин/0 | Устанавливает время жизни в кэше. Если значение равно нулю – отсчёт времени жизни отключен (запись не удаляется со временем). |
| no ip igmp snooping authorization cache-timeout | | Установка значения по умолчанию. |

Команды режима конфигурирования интерфейса (диапазона интерфейсов) Ethernet

Вид запроса командной строки режима конфигурирования интерфейса:

```
console (config-if) #
```

Таблица 156 – Команды режима конфигурирования интерфейса Ethernet

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---------------------------------------|--|
| multicast snooping authorization radius [required] | -/отключено | Включает авторизацию через RADIUS-сервер. Если указан параметр required , то в случае недоступности всех RADIUS-серверов IGMP-запросы игнорируются. В противном случае IGMP-запрос будет обработан даже при отсутствии ответа сервера. |
| no multicast snooping authorization | | Отключение авторизации. |
| multicast snooping authorization forwarding-first | -/отключено | Включает предварительную обработку IGMP-запросов на порту до ответа RADIUS-сервера. По получении ответа от сервера в случае положительного ответа подписка остается, в случае отрицательного – удаляется, если дополнительно настроена функция ip igmp snooping immediate-leave . |
| no multicast snooping authorization forwarding-first | | Восстанавливает значение по умолчанию. |

Команды режима EXEC

Все команды доступны только для привилегированного пользователя.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 157 – Команды режима EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|--|---|
| show ip igmp snooping authorization-cache [interface gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..4); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Отображает содержимое кэша авторизации IGMP. Если в команде указан интерфейс – то отображаются только те группы, которые зарегистрированы на указанном интерфейсе. |
| clear ip igmp snooping authorization-cache [interface gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..4); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Очищает кэш авторизации. Если в команде указан интерфейс – кэш-записи очищаются для указанного интерфейса. Если интерфейс не указан – кэш очищается полностью. |

5.18 Маршрутизация многоадресного трафика

5.18.1 Протокол PIM

PIM – протокол многоадресной маршрутизации для IP-сетей, созданный для решения проблем групповой маршрутизации. PIM базируется на традиционных маршрутных протоколах (например, Border Gateway Protocol), вместо того, чтобы создавать собственную сетевую топологию. PIM использует unicast-таблицу маршрутизации для проверки RPF. Эта проверка выполняется маршрутизаторами, чтобы убедиться, что передача многоадресного трафика выполняется по пути без петель.

RP (rendezvous point) – точка randevу, на которой будут регистрироваться источники многоадресных потоков и создавать маршрут от источника S (себя) до группы G: (S, G).

BSR (bootstap router) – механизм сбора информации о RP кандидатах, формировании списка RP для каждой многоадресной группы и отправка списка в пределах домена. Конфигурация многоадресной маршрутизации на базе IPv4.


Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config) #
```

Таблица 158 – Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|------------------------------------|---------------------------------------|--|
| ip multicast-routing pim | -/По умолчанию функция выключена | Включить многоадресную маршрутизацию, протокол PIM на всех интерфейсах. |
| no ip multicast-routing pim | | Отключить многоадресную маршрутизацию и протокол PIM. |
| ipv6 multicast-routing pim | -/По умолчанию функция выключена | Включить для IPv6 многоадресную маршрутизацию, протокол PIM на всех интерфейсах. |

| | | |
|---|--|---|
| no ipv6 multicast-routing pim | | Отключить для IPv6 многоадресную маршрутизацию и протокол PIM. |
| ip pim bsr-candidate <i>ip_address [mask] [priority priority_num]</i> | mask: (8..32)/30; priority_num: (0..192)/0 | Указать устройство как кандидата в BSR (bootstrap router). - <i>ip_address</i> – валидный IP-адрес коммутатора; - <i>mask</i> – маска подсети; - <i>priority_num</i> – приоритет. |
| no ip pim bsr-candidate | | Отключение данного параметра. |
| ipv6 pim bsr-candidate <i>ipv6_address [mask] [priority priority_num]</i> | mask: (8..128)/126; priority_num: (0..192)/0 | Указать устройство как кандидата в BSR (bootstrap router). - <i>ipv6_address</i> – валидный IPv6-адрес коммутатора; - <i>mask</i> – маска подсети; - <i>priority_num</i> – приоритет. |
| no ipv6 pim bsr-candidate | | Отключение данного параметра. |
| ip pim dm {range multicast_subnet default} | - | Включить маршрутизацию заданного диапазона мультикастных групп в режиме PIM-DM. - <i>multicast_subnet</i> – многоадресная подсеть; - <i>default</i> – определяет диапазон в 224.0.1.0/24.  Команду можно ввести несколько раз, задав несколько диапазонов. |
| no ip pim dm {range multicast_subnet default} | | Отключить данный параметр. |
| ip pim rp-address <i>unicast_address [multicast_subnet]</i> | - | Создание статической Rendezvous Point (RP), дополнительно можно указать многоадресную подсеть для данной RP. - <i>unicast_addr</i> – IP-адрес; - <i>multicast_subnet</i> – многоадресная подсеть. |
| no ip pim rp-address <i>unicast_address [multicast_subnet]</i> | | Удаление статической RP или удаление RP для указанной подсети. |
| ipv6 pim rp-address <i>ipv6_unicast_address [ipv6_multicast_subnet]</i> | - | Создание статической Rendezvous Point (RP), дополнительно можно указать многоадресную подсеть для данной RP. - <i>ipv6_unicast_addr</i> – IPv6-адрес; - <i>ipv6_multicast_subnet</i> – многоадресная подсеть. |
| no ipv6 pim rp-address <i>ipv6_unicast_address [ipv6_multicast_subnet]</i> | | Удаление статической RP или удаление RP для указанной подсети. |
| ip pim rp-candidate <i>unicast_address [group-list acc_list] [priority priority] [interval secs]</i> | acc_list: (0..32) символа priority: (0..192)/192; secs: (1..16383)/60 секунд | Создание кандидата для Rendezvous Point (RP) - <i>unicast_addr</i> – IP-адрес; - <i>acc_list</i> – список многоадресных префиксов, задаваемый с помощью стандартного ACL; - <i>priority</i> – приоритетность кандидата; - <i>secs</i> – период отправки сообщений. |
| no ip pim rp-candidate <i>unicast_address</i> | | Отключение данного параметра. |
| ipv6 pim rp-candidate <i>ipv6_unicast_address [group-list acc_list] [priority priority] [interval secs]</i> | acc_list: (0..32) символа priority: (0..192)/192; secs: (1..16383)/60 секунд | Создание кандидата для Rendezvous Point (RP) - <i>ipv6_unicast_addr</i> – IPv6-адрес; - <i>acc_list</i> – список многоадресных префиксов, задаваемый с помощью стандартного ACL; - <i>priority</i> – приоритетность кандидата; - <i>secs</i> – период отправки сообщений. |
| no ipv6 pim rp-candidate <i>ipv6_unicast_address</i> | | Отключение данного параметра. |
| ip pim ssm {range multicast_subnet default} | - | Указать многоадресную подсеть - range – указать многоадресную подсеть; - <i>multicast_subnet</i> – многоадресная подсеть; - default – указать диапазон в 232.0.0.0/8. |
| no ip pim ssm [range multicast_subnet default] | | Отключение данного параметра. |
| ipv6 pim ssm {range ipv6_multicast_subnet default} | - | Указать многоадресную подсеть - range – указать многоадресную подсеть; - <i>ipv6_multicast_subnet</i> – многоадресная подсеть; - default – указать диапазон в FF3E::/32. |
| no ipv6 pim ssm [range ipv6_multicast_subnet default] | | Отключение данного параметра. |

| | | |
|--|-------------|---|
| <code>ipv6 pim rp-embedded</code> | -/включено | Включить расширенный функционал rendezvous point (RP). |
| <code>no ipv6 pim rp-embedded</code> | | Отключить расширенный функционал rendezvous point (RP). |
| <code>ip multicast multipath {group-paths-num group-next-hop}</code> | -/выключено | <p>Включает балансировку пакетов PIM Join в сторону доступных RP.</p> <p>- group-paths-num – метод балансировки, при котором хеш функция, подсчитанная на основе адреса группы, делится по модулю на N, где N – количество доступных RP.</p> <p>! Вышеуказанный метод необходим для корректной работы балансировки при использовании EVPN/VXLAN. На практике он приводит к «синхронизации» VTEP и выбору одного и того же RP для отправки трафика конкретной группы.</p> <p>- group-next-hop – метод балансировки, при котором подсчет хеш функции базируется на адресе группы и адресе next-hop.</p> <p>! По умолчанию в случае наличия в таблице маршрутизации более одного маршрута до RP, PIM Join отправляется в сторону PIM соседа с наибольшим IP.</p> |
| <code>no ip multicast multipath</code> | | Устанавливает значение по умолчанию. |

Команды режима конфигурации интерфейса Ethernet, VLAN, группы портов

Вид запроса командной строки:

```
console (config-if) #
```

Таблица 159 – Команды режима конфигурации интерфейсов Ethernet, VLAN, группы портов

| <i>Команда</i> | <i>Значение/ Значение по умолчанию</i> | <i>Действие</i> |
|---|--|--|
| <code>ip (ipv6) pim</code> | -/включено | Включение PIM на интерфейсе. |
| <code>no ip (ipv6) pim</code> | | Выключение PIM на интерфейсе. |
| <code>ip (ipv6) pim bsr-border</code> | -/отключено | Прекратить передачу BSR-сообщений с интерфейса. |
| <code>no ip pim bsr-border</code> | | Отключение данного параметра. |
| <code>ip (ipv6) pim dr-priority priority</code> | priority: (0..4294967294)/1 | Указание приоритета для выбора DR-роутера. - <i>priority</i> – приоритет DR-роутера определяющий, кто из коммутаторов станет DR-роутером. Коммутатор с наибольшим значением станет DR-роутером. |
| <code>no ip (ipv6) pim dr-priority</code> | | Возвращает значение по умолчанию. |
| <code>ip ip (ipv6) pim hello-interval secs</code> | secs: (1..18000)/30 сек | Указание периода отправки hello-пакетов. - <i>sec</i> – период отправки hello-пакетов. |
| <code>no ip (ipv6) pim hello-interval</code> | | Возвращает значение по умолчанию. |
| <code>ip (ipv6) pim join-prune-interval interval</code> | interval: (1..18000)/60 секунд | Указать интервал, в течение которого коммутатор отправляет join или prune-сообщения. - <i>interval</i> – период времени отправки join, prune сообщений. |
| <code>no ip (ipv6) pim join-prune-interval</code> | | Возвращает значение по умолчанию. |
| <code>ip (ipv6) pim neighbor-filter acc_list</code> | acc_list: (0..32) символа | Фильтрация входящих PIM-сообщений. - <i>acc_list</i> – список адресов, на основе которых производится фильтрация. |
| <code>no ip (ipv6) pim neighbor-filter</code> | | Отключение данного параметра. |
| <code>ip igmp static-group group-address [source source_addr]</code> | - | <p>Включить статический запрос multicast-группы на интерфейсе.</p> <p>- <i>group_address</i> – IP-адрес группы;</p> <p>- <i>source_addr</i> – IP-адрес источника группы.</p> <p>! На интерфейсе должен быть включен PIM.</p> |
| <code>no ip igmp static-group group-address [source source_addr]</code> | | Выключить статический запрос multicast-группы. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 160 – Команды режима EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|---|
| show ip (ipv6) pim rp mapping [<i>RP_addr</i>] | - | Отображает активные RP, связанные с маршрутной информацией. - <i>RP_addr</i> – IP-адрес. |
| show ip (ipv6) pim neighbor [detail] [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group vlan <i>vlan_id</i>] | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..128); <i>vlan_id</i> : (1..4094). | Отображает информацию о PIM-соседах. |
| show ip (ipv6) pim interface [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> port-channel group hundredgigabitethernet <i>hu_port</i> vlan <i>vlan_id</i> state-on state-off] | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..128); <i>vlan_id</i> : (1..4094). | Отображает информацию по PIM-интерфейсам: - state-on – отображает все интерфейсы, где включен PIM; - state-off – отображает все интерфейсы, где выключен PIM. |
| show ip (ipv6) pim group-map [<i>group_address</i>] | - | Отображает таблицу привязки многоадресных групп. - <i>group-address</i> – адрес группы. |
| show ip (ipv6) pim counters | - | Отображает содержимое PIM-счетчиков. |
| show ip (ipv6) pim bsr election | - | Отображает информацию о BSR. |
| show ip (ipv6) pim bsr rp-cache | - | Отображает информацию о изученных кандидатах в RP. |
| show ip (ipv6) pim bsr candidate-rp | - | Отображает состояние кандидатов в RP. |
| clear ip (ipv6) pim counters | - | Обнуляет PIM-счетчики. |

Пример использования команд

- Базовая настройка PIM SM с статическим RP (1.1.1.1). Предварительно должен быть настроен протокол маршрутизации.

```
console# configure
console(config)# ip multicast-routing
console(config)# ip pim rp-address 1.1.1.1
```

5.18.2 Функция PIM Snooping

Функция PIM Snooping используется в сетях, где коммутатор исполняет роль L2-устройства между PIM-маршрутизаторами.

Основной задачей PIM Snooping является предоставление многоадресного трафика только для тех портов, с которых были получен PIM Join, PIM Register.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console (config) #
```

Таблица 161 — Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--|---------------------------------------|---|
| ip pim snooping | —/выключено | Разрешить использование функции PIM Snooping коммутатором. |
| no ip pim snooping | | Запретить использование функции |
| ip pim snooping vlan vlan_id | vlan_id: (1..4094) | Разрешить использование функции PIM Snooping коммутатором для данного интерфейса VLAN. vlan_id — идентификационный номер VLAN. |
| no ip pim snooping vlan vlan_id | | Запретить использование функции PIM Snooping коммутатором для данного интерфейса VLAN. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 162 — Команды режима EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|--|---------------------------------------|--|
| show ip pim snooping | — | Показать общую информацию о настройках. |
| show ip pim snooping vlan vlan_id | vlan_id: (1..4094) | Показать статистику контроля многоадресного трафика в данной vlan. |
| show ip pim snooping groups | — | Показать список зарегистрированных групп. |
| sh ip pim snooping neighbors | — | Показать список зарегистрированных участников PIM. |

5.18.3 Протокол MSDP

Протокол обнаружения источников многоадресной рассылки (MSDP) используется для обмена информацией об источниках Multicast-трафика между разными PIM-доменами. MSDP-соединение обычно устанавливается между RP каждого домена.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console (config) #
```

Таблица 163 — Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--------------------|---------------------------------------|--|
| router msdp | — | Включить протокол MSDP и перейти в режим его конфигурации. |

| | | |
|-----------------------------|--|--|
| <code>no router msdp</code> | | Остановить протокол MSDP и удалить всю его конфигурацию. |
|-----------------------------|--|--|

Команды режима конфигурации протокола MSDP

Вид запроса командной строки в режиме конфигурации протокола MSDP:

```
console(config-msdp) #
```

Таблица 164 — Команды режима конфигурации протокола MSDP

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---------------------------------------|--|
| <code>connect-source ip_address</code> | -/IP-адрес не назначен | Назначить IP-адрес, который будет использован в качестве исходящего при соединении с MSDP-пиром. |
| <code>no connect-source</code> | | Установить значение по умолчанию. |
| <code>cache-sa-holdtime secs</code> | secs: (150..3600)/150 сек | Установить время жизни SA-записи в кэше. |
| <code>no cache-sa-holdtime</code> | | Установить значение по умолчанию. |
| <code>holdtime secs</code> | secs: (3..150)/75 сек | Установить таймер holdtime. Если в течение этого времени не будет принято keepalive-сообщение, то соединение с соседом сбрасывается. |
| <code>no holdtime</code> | | Установить значение по умолчанию. |
| <code>keepalive secs</code> | secs: (1..60)/30 сек | Установить интервал между отправкой keepalive-сообщений. |
| <code>no keepalive</code> | | Установить значение по умолчанию. |
| <code>originator-ip ip_address</code> | -/IP-адрес не назначен | Назначить IP-адрес, используемый в качестве адреса RP в исходящих сообщениях SA. |
| <code>no originator-ip</code> | | Установить значение по умолчанию. |
| <code>peer ip_address</code> | — | Добавить в конфигурацию MSDP-пир и войти в режим его конфигурации. |
| <code>no peer ip_address</code> | | Удалить MSDP-пир. |

Команды режима конфигурации MSDP-пира

Вид запроса командной строки в режиме конфигурации MSDP-пира:

```
console(config-msdp) #
```

Таблица 165 — Команды режима конфигурации MSDP-пира

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---------------------------------------|--|
| <code>connect-source ip_address</code> | —/IP-адрес не назначен | Назначить IP-адрес, который будет использован в качестве исходящего при соединении с MSDP-пиром. |
| <code>no connect-source</code> | | Установить значение по умолчанию. |
| <code>description text</code> | text: (1..160) символа | Задать описание MSDP-пира. |
| <code>no description</code> | | Удалить описание. |
| <code>mesh-group name</code> | name: (1..31) символа | Добавить соседа к MESH-группе. |
| <code>no mesh-group</code> | | Удалить соседа. |

| | | |
|---|------------------------------------|--|
| sa-filter { in out } <i>sec_num { permit deny }</i> [rp-address ip_addr_rp group-address ip_addr_gr source-address <i>ip_addr_src]</i> | <i>sec_num:</i> (0..4294967294) | Создать правило фильтрации SA-сообщений: - permit — разрешающее правило фильтрации; - deny — запрещающее правило фильтрации; - <i>sec_num</i> — номер секции правила; - <i>ip_addr_rp</i> — фильтрация по адресу RP; - <i>ip_addr_gr</i> — фильтрация по адресу группы; - <i>ip_addr_src</i> — фильтрация по адресу источника Multicast-трафика. |
| no sa-filter { in out } <i>sec_num</i> | | Удаляет созданную секцию правила. |
| shutdown | —/выключено | Административно выключить сессию с MSDP-пиром, не удаляя его конфигурации. |
| no shutdown | | Установить значение по умолчанию. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 166 — Команды режима EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---------------------------------------|--|
| show ip msdp peers [ip_addr] | — | Показать информацию о настроенных пирах, статусе соединения, настройках пиров, а также статистику обмена сообщениями протокола MSDP - <i>ip_addr</i> — IP-адрес пира. |
| show ip msdp source-active | — | Показать содержимое кэша SA. |
| show ip msdp summary | — | Показать суммарную информацию протокола MSDP. |
| clear ip msdp counters | — | Обнулить счетчики. |
| clear ip msdp peers [ip_addr] | — | Переустановить соединения с MSDP-пирами - <i>ip_addr</i> — IP-адрес пира. |

5.18.4 Функция IGMP Proxy

Функция многоадресной маршрутизации IGMP Proxy предназначена для реализации упрощенной маршрутизации многоадресных данных между сетями, управляемой на основании протокола IGMP. С помощью IGMP Proxy устройства, не находящиеся в одной сети с сервером многоадресной рассылки, имеют возможность подключаться к многоадресным группам.

Маршрутизация осуществляется между интерфейсом вышестоящей сети (uplink) и интерфейсами нижестоящих сетей (downlink). При этом на uplink-интерфейсе коммутатор ведет себя как обычный получатель многоадресного трафика (multicast client) и формирует собственные сообщения протокола IGMP. На интерфейсах downlink коммутатор выступает в качестве сервера многоадресной рассылки и обрабатывает сообщения протокола IGMP от устройств, подключенных к этим интерфейсам.



Количество поддерживаемых групп многоадресной рассылки протоколом IGMP Proxy указано в таблице 9.



IGMP Proxy поддерживает до 512 downlink-интерфейсов.



Ограничения реализации функции IGMP Proxy:

- IGMP Proxy не поддерживается на группах агрегации LAG;
- может быть определен только один интерфейс вышестоящей сети;
- при использовании версии V3 протокола IGMP на интерфейсах к нижестоящей сети, обрабатываются только запросы типа exclude (*,G) и include (*,G).

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 167 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|------------------------------------|----------------------------------|--|
| ip multicast-routing igmp-proxy | -/По умолчанию функция выключена | Разрешает работу маршрутизации многоадресных данных на сконфигурированных интерфейсах. |
| no ip multicast-routing | | Запрещает работу маршрутизации многоадресных данных на сконфигурированных интерфейсах. |

Команды режима конфигурации интерфейсов Ethernet, VLAN, интерфейса группы портов

Вид запроса командной строки в режиме конфигурации интерфейсов Ethernet, VLAN, интерфейса группы портов:

```
console(config-if)#
```

Таблица 168 – Команды режима конфигурации интерфейсов Ethernet, VLAN, группы портов

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|---|
| ip igmp-proxy { gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group vlan vlan_id} | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128); vlan_id: (1..4094) | Конфигурируемый интерфейс является интерфейсом к нижестоящей сети. Команда назначает связанный uplink-интерфейс, участвующий в маршрутизации. |
| ip igmp-proxy downstream protected interface { enable disable} | - | Включить защиту по нисходящему интерфейсу. IPv4 multicast-трафик, поступающий на интерфейс, не будет перенаправлен. |
| no ip igmp-proxy downstream protected interface | - | Отключить защиту по нисходящему интерфейсу. |
| ip igmp static-group group- address [source source_addr] | - | Включить статический запрос multicast-группы на интерфейсе. - group_address – IP-адрес группы; - source_addr – IP-адрес источника группы. |
| no ip igmp static-group group- address [source source_addr] | - | Выключить статический запрос multicast-группы. |



На интерфейсе должен быть включен IGMP Proxy.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 169 – Команды режима EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|---|---|---|
| show ip mroute [<i>ip_multicast_address</i> [<i>ip_address</i>]] [summary] | - | Команда предназначена для просмотра списков многоадресных групп. Возможен выбор групп по адресу группы или по адресу источника многоадресных данных. - <i>ip_multicast_address</i> – IP-адрес группы; - <i>ip_address</i> – IP-адрес источника; - summary – краткое содержание каждой записи в многоадресной таблице маршрутизации. |
| show ip igmp-proxy interface [vlan <i>vlan_id</i> gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i>] | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); <i>group</i> : (1..128); <i>vlan_id</i> : (1..4094) | Информация о статусе IGMP-проху применительно к интерфейсам. |

Примеры выполнения команд

```
console#show ip igmp-proxy interface
```

```
* - the switch is the Querier on the interface

IP Forwarding is enabled
IP Multicast Routing is enabled
IGMP Proxy is enabled
Global Downstream interfaces protection is enabled
SSM Access List Name: -

Interface  Type          Interface Protection  CoS  DSCP
vlan5      upstream
vlan30     downstream default                -    -
```

5.19 Функции управления

5.19.1 Механизм AAA

Для обеспечения безопасности системы используется механизм AAA (аутентификация, авторизация, учет).

- Authentication (аутентификация) — сопоставление запроса существующей учётной записи в системе безопасности.
- Authorization (авторизация, проверка уровня доступа) — сопоставление учётной записи в системе (прошедшей аутентификацию) и определённых полномочий.
- Accounting (учёт) — слежение за потреблением ресурсов пользователем.






Для шифрования данных используется механизм SSH.





Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console (config) #
```

Таблица 170 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|---|---|---|
| aaa authentication login {authorization default list_name} method_list | list_name: (1..12) символов; method_list: (enable, line, local, none, tacacs, radius); -/По умолчанию осуществляется проверка по локальной базе данных (aaa authentication login authorization default local) | Устанавливает способ аутентификации для входа в систему. - <i>authorization</i> - разрешает прохождение авторизации по описанным ниже методам; - default – использовать для аутентификации описанные ниже методы; - <i>list_name</i> – имя списка аутентификационных методов, активирующегося, когда пользователь входит в систему. Описание методов (method_list): - <i>enable</i> – использовать пароль для аутентификации; - <i>line</i> – использовать пароль терминала для аутентификации; - <i>local</i> – использовать локальную базу имен пользователей для аутентификации; - <i>none</i> – не использовать аутентификацию; - <i>radius</i> – использовать список RADIUS-серверов для аутентификации; - <i>tacacs</i> – использовать список TACACS серверов для аутентификации.  Если метод аутентификации не определен, то доступ к консоли всегда успешный.  Создание списка осуществляется командой: aaa authentication login list_name method_list. Использование списка: aaa authentication login list-name  Во избежание потери доступа следует вводить необходимый минимум настроек для указываемого метода аутентификации. |
| no aaa authentication login {default list_name} | | Устанавливает значение по умолчанию. |
| aaa authentication enable authorization {default list_name} method_list | list_name: (1..12) символов; method_list: (enable, line, local, none, tacacs, radius); -/По умолчанию осуществляется проверка по локальной базе данных (aaa authentication enable authorization default enable) | Устанавливает способ аутентификации при повышении уровня привилегий для входа в систему. - <i>authorization</i> - разрешает прохождение авторизации по описанным ниже методам; - default – использовать для аутентификации описанные ниже методы; - <i>list_name</i> – имя списка аутентификационных методов, активирующегося, когда пользователь входит в систему. Описание методов (method_list): - <i>enable</i> – использовать пароль для аутентификации; - <i>line</i> – использовать пароль терминала для аутентификации; - <i>local</i> – использовать локальную базу имен пользователей для аутентификации; - <i>none</i> – не использовать аутентификацию; - <i>radius</i> – использовать список RADIUS-серверов для аутентификации; - <i>tacacs</i> – использовать список TACACS-серверов для аутентификации.  Если метод аутентификации не определен, то доступ к консоли всегда успешный.  Создание списка осуществляется командой: aaa authentication login list-name method_list. Использование списка: aaa authentication login list-name |

| | | |
|---|---|--|
| | |  <p>Во избежание потери доступа следует вводить необходимый минимум настроек для указываемого метода аутентификации.</p> |
| no aaa authentication enable authorization {default list_name} | | Устанавливает значение по умолчанию. |
| enable password password [encrypted] [level level] | level: (1..15)/1; password: (0..159) символов | Устанавливает пароль для контроля изменения привилегий доступа пользователей. - <i>level</i> – уровень привилегий; - <i>password</i> – пароль; - <i>encrypted</i> – задать зашифрованный пароль (например, пароль в зашифрованном виде, скопированный с другого устройства). |
| no enable password [level level] | | Удаляет пароль для соответствующего уровня привилегий. |
| username name {nopassword password password password encrypted encrypted_password} [privileged level] | name: (1..20) символов; password: (1..64) символов; encrypted_password: (1..64) символов; level: (1..15) | Добавляет пользователя в локальную базу данных. - <i>level</i> – уровень привилегий; - <i>password</i> – пароль; - <i>name</i> – имя пользователя; - <i>encrypted_password</i> – зашифрованный пароль (например, пароль в зашифрованном виде, скопированный с другого устройства). |
| no username name | | Удаляет пользователя из локальной базы данных |
| aaa accounting login start-stop group {radius tacacs+} | -/По умолчанию ведение учета запрещено | <p>Разрешает ведение учета (аккаунта) для сессий управления.</p> <p> Ведение учета разрешено только для пользователей, вошедших в систему по имени и паролю, для пользователей, вошедших по паролю терминала, ведение учета запрещено.</p> <p> Ведение учета активируется и прекращается, когда пользователь входит и отключается от системы, что соответствует значениям start и stop в сообщениях протокола RADIUS (параметры, содержащиеся в сообщениях протокола RADIUS, приведены в таблице 171).</p> |
| no aaa accounting login start-stop | | Запрещает ведение учета (аккаунта) для введенных в CLI команд. |
| aaa accounting dot1x start-stop group radius | -/По умолчанию ведение учета запрещено | <p>Разрешает ведение учета (аккаунта) для сессий 802.1x.</p> <p> Ведение учета активируется и прекращается, когда пользователь входит и отключается от системы, что соответствует значениям start и stop в сообщениях протокола RADIUS (параметры, содержащиеся в сообщениях протокола RADIUS приведены в таблице 171).</p> <p> В режиме Multiple sessions сообщения stat/stop посылаются для каждого пользователя, в режиме Multiple hosts – только для пользователя, прошедшего аутентификацию (см. раздел по 802.1x).</p> |
| no aaa accounting dot1x start-stop group radius | | Устанавливает значение по умолчанию. |
| ip http authentication aaa login-authentication [login-authorization] [http https] method_list | method_list: (local, none, tacacs, radius) | <p>Определяет метод аутентификации при доступе к HTTP-серверу. При установке списка методов дополнительный метод будет применяться только в том случае, когда по основному методу аутентификации возвращена ошибка.</p> <p>- method_list – метод аутентификации: <i>local</i> – по имени из локальной базы данных; <i>none</i> – не используется; <i>tacacs</i> – использование списков всех серверов TACACS+; <i>radius</i> – использование списков всех RADIUS-серверов.</p> |
| no ip http authentication aaa login-authentication | | Устанавливает значение по умолчанию. |
| aaa authentication mode {chain break} | -/chain | <p>Устанавливает алгоритм опроса методов аутентификации.</p> <p>- chain – после неудачной попытки аутентификации по первому методу в списке следует попытка аутентификации по следующему методу в цепочке;</p> |

| | | |
|---|---|---|
| | | - break – после неудачной аутентификации по первому методу процесс аутентификации останавливается. Аутентификация по следующему методу допустима только в случае невозможности аутентификации по предыдущему методу. |
| aaa accounting commands stop-only group tacacs+ | -/По умолчанию ведение учета команд выключено | Включает ведение учета введенных в CLI команд по протоколу Tacacs+. |
| no aaa accounting commands stop-only group | | Устанавливает значение по умолчанию. |
| aaa authorization commands {default list_name} group method_list | list_name: (1..15) символов; method_list: (tacacs, local); -/по умолчанию активен список default и авторизация не осуществляется | Устанавливает способ авторизации вводимых команд. - default — редактировать список с именем default, который по умолчанию есть в системе; - list_name — имя списка методов авторизации, создаваемого и редактируемого пользователем; - tacacs — метод, позволяющий использовать список TACACS-серверов для авторизации; - local — метод, при котором авторизация не осуществляется. |
| no aaa authorization commands {default list_name} | | Устанавливает значение по умолчанию. - default — сброс списка с именем default к значению по умолчанию; - list_name — удаление пользовательского списка с именем list_name. Список с именем default не может быть удален из системы. |
| aaa authorization commands {default list_name} | list_name: (1..15) символов; -/default | Активирует список методов авторизации вводимых команд. - default — сделать активным список с именем default; - list_name — сделать активным соответствующий пользовательский список. |
| no aaa authorization commands | | Устанавливает значение по умолчанию. |



Для того чтобы клиент получил доступ к устройству, даже если все методы аутентификации вернули ошибку, используйте значение последнего метода в команде – none.

Таблица 171 – Атрибуты сообщений ведения учета протокола RADIUS для сессий управления

| Атрибут | Наличие атрибута в сообщении Start | Наличие атрибута в сообщении Stop | Описание |
|---------------------------|------------------------------------|-----------------------------------|--|
| User-Name (1) | Есть | Есть | Идентификация пользователя. |
| NAS-IP-Address (4) | Есть | Есть | IP-адрес коммутатора, который используется для сессий с Radius-сервером. |
| Class (25) | Есть | Есть | Произвольное значение, включенное во все сообщения учета сессий. |
| Called-Station-ID (30) | Есть | Есть | IP-адрес коммутатора, используемый для сессий управления. |
| Calling-Station-ID (31) | Есть | Есть | IP-адрес пользователя. |
| Acct-Session-ID (44) | Есть | Есть | Уникальный идентификатор учета. |
| Acct-Authentic (45) | Есть | Есть | Указывает метод, по которому клиент должен быть аутентифицирован. |
| Acct-Session-Time (46) | Нет | Есть | Показывает, как долго пользователь был подключен к системе. |
| Acct-Terminate-Cause (49) | Нет | Есть | Причина закрытия сессии. |

Таблица 172 – Атрибуты сообщений ведения учета протокола RADIUS для сессий 802.1x

| <i>Атрибут</i> | <i>Наличие атрибута в сообщении Start</i> | <i>Наличие атрибута в сообщении Stop</i> | <i>Описание</i> |
|---------------------------|---|--|--|
| User-Name (1) | Есть | Есть | Идентификация пользователя. |
| NAS-IP-Address (4) | Есть | Есть | IP-адрес коммутатора, который используется для сессий с Radius-сервером. |
| NAS-Port (5) | Есть | Есть | Порт коммутатора, на котором подключился пользователь. |
| Class (25) | Есть | Есть | Произвольное значение, включенное во все сообщения учета сессий. |
| Called-Station-ID (30) | Есть | Есть | IP-адрес коммутатора. |
| Calling-Station-ID (31) | Есть | Есть | IP-адрес пользователя. |
| Acct-Session-ID (44) | Есть | Есть | Уникальный идентификатор учета. |
| Acct-Authentic (45) | Есть | Есть | Указывает метод, по которому клиент должен быть аутентифицирован. |
| Acct-Session-Time (46) | Нет | Есть | Показывает, как долго пользователь был подключен к системе. |
| Acct-Terminate-Cause (49) | Нет | Есть | Причина закрытия сессии. |
| Nas-Port-Type (61) | Есть | Есть | Показывает тип порта клиента. |

Команды режима конфигурации терминала

Вид запроса командной строки в режиме конфигурации терминала:

```
console(config-line)#
```

Таблица 173 – Команды режима конфигурации терминальных сессий

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---------------------------------------|--|
| login authentication {default list_name} | list_name: (1..12) символов | Задает метод аутентификации при входе для консоли, Telnet, SSH. - default – использовать список «по умолчанию», созданный командой aaa authentication login default - list_name – использовать список, созданный командой aaa authentication login list_name . |
| no login authentication | | Устанавливает значение по умолчанию. |
| enable authentication {default list_name} | list_name: (1..12) символов | Задает метод аутентификации пользователя при повышении уровня привилегий для консоли, Telnet, SSH. - default – использовать список «по умолчанию», созданный командой aaa authentication login default - list_name – использовать список, созданный командой aaa authentication login list_name . |
| no enable authentication | | Устанавливает значение по умолчанию. |
| password password [encrypted] | password: (0..159) символов | Задает пароль для терминала. - encrypted – задать зашифрованный пароль (например, пароль в зашифрованном виде, скопированный с другого устройства). |
| no password | | Удаляет пароль для терминала. |

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 174 – Команды режима Privileged EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|------------------------------------|---------------------------------------|---|
| show authentication methods | - | Показывает информацию об аутентификационных методах на коммутаторе. |
| show users accounts | - | Показывает локальную базу данных пользователей и их привилегий. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Все команды данного раздела доступны только для привилегированных пользователей.

Таблица 175 – Команды режима EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|------------------------|---------------------------------------|---|
| show accounting | - | Показывает информацию о настроенных методах ведения учета (аккаунта). |

5.19.2 Протокол RADIUS

Протокол RADIUS используется для аутентификации, авторизации и учета. Сервер RADIUS использует базу данных пользователей, которая содержит данные проверки подлинности для каждого пользователя. Таким образом, использование протокола RADIUS обеспечивает дополнительную защиту при доступе к ресурсам сети, а также при доступе к самому коммутатору.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 176 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|---|---|---|
| radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } [auth-port <i>auth_port</i>] [acct-port <i>acct_port</i>] [timeout <i>timeout</i>] [retransmit <i>retries</i>] [deadtime <i>time</i>] [key <i>secret_key</i>] [priority <i>priority</i>] [usage <i>type</i>] | hostname: (1..158) символов; auth_port: (0..65535)/1812; acct_port: (0..65535)/1813; timeout: (1..30) сек; retries: (1..15); | Добавляет указанный сервер в список используемых RADIUS-серверов. - <i>ip_address</i> – IPv4 или IPv6-адрес RADIUS-сервера; - <i>hostname</i> – сетевое имя RADIUS-сервера; - <i>auth_port</i> – номер порта для передачи аутентификационных данных; - <i>acct_port</i> – номер порта для передачи данных учета; - <i>timeout</i> – интервал ожидания ответа от сервера; |

| | | |
|--|---|--|
| encrypted radius-server host {ipv4-address ipv6-address hostname} [auth-port auth_port] [acct-port acct_port] [timeout timeout] [retransmit retries] [deadtime time] [key secret_key] [priority priority] [usage type] | time (0..2000) мин; secret_key: (0..128) символов; priority: (0..65535)/0; type: (login, dot1.x, all)/all | - <i>retries</i> – количество попыток поиска RADIUS-сервера; - <i>time</i> – время в минутах, в течение которого недоступные сервера не будут опрашиваться RADIUS-клиентом коммутатора; - <i>secret_key</i> – ключ для аутентификации и шифрования всего обмена данными RADIUS; - <i>priority</i> – приоритет использования RADIUS-сервера (чем ниже значение, тем приоритетнее сервер); - <i>type</i> – тип использования RADIUS-сервера; - encrypted – задать ключ в зашифрованном виде. В случае отсутствия в команде параметров <i>timeout</i> , <i>retries</i> , <i>time</i> , <i>secret_key</i> для данного RADIUS-сервера используются значения, настроенные с помощью команд, указанных ниже. |
| no radius-server host {ipv4-address ipv6-address hostname} | | Удаляет указанный сервер из списка используемых RADIUS-серверов. |
| [encrypted] radius-server key [key] | key: (0..128) символов/по умолчанию ключ – пустая строка | Устанавливает ключ, используемый по умолчанию, для аутентификации и шифрования всего обмена данными RADIUS между устройством и окружением RADIUS. - encrypted – задать ключ в зашифрованном виде. |
| no radius-server key | | Устанавливает значение по умолчанию. |
| radius-server timeout <i>timeout</i> | timeout: (1..30)/3 сек | Устанавливает интервал ожидания ответа от сервера, используемый по умолчанию. |
| no radius-server timeout | | Устанавливает значение по умолчанию. |
| radius-server retransmit <i>retries</i> | retries: (1..15)/3 | Определяет количество попыток, используемое по умолчанию, поиска RADIUS-сервера из списка серверов. При отказе осуществляется поиск следующего по приоритету сервера из списка. |
| no radius-server retransmit | | Устанавливает значение по умолчанию. |
| radius-server deadtime <i>deadtime</i> | deadtime: (0..2000)/0 мин | Позволяет оптимизировать время опроса RADIUS-серверов, когда некоторые сервера недоступны. Устанавливает время в минутах, используемое по умолчанию, в течение которого недоступные сервера не будут опрашиваться RADIUS-клиентом коммутатора. |
| no radius-server deadtime | | Устанавливает значение по умолчанию. |
| radius-server host source-interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> loopback <i>loopback_id</i> vlan <i>vlan id</i> } | vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); loopback_id: (1..64); group: (1..128) | Задаёт интерфейс устройства, IP-адрес которого будет использоваться по умолчанию в качестве адреса источника передаваемого в сообщениях протокола RADIUS. |
| no radius-server host source-interface | | Удаляет интерфейс устройства. |
| radius-server host source-interface-ipv6 {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> loopback <i>loopback_id</i> vlan <i>vlan id</i> } | vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); loopback_id: (1..64); group: (1..128) | Задаёт интерфейс устройства, IPv6-адрес которого будет использоваться по умолчанию в качестве адреса источника передаваемого в сообщениях протокола RADIUS. |
| no radius-server host source-interface-ipv6 | | Удаляет интерфейс устройства. |

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 177 – Команды режима Privileged EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|--|--------------------------------|---|
| <code>show radius-servers [key]</code> | - | Отображает параметры настройки RADIUS-серверов (команда доступна только для привилегированных пользователей). |
| <code>show radius server {statistics group accounting configuration nas rejected secret user}</code> | - | Отображает статистику протокола Radius, информацию о пользователях, конфигурацию RADIUS-сервера. |

Примеры использования команд

- Установить глобальные значения для параметров: интервал ожидания ответа от сервера – 5 секунд, количество попыток поиска RADIUS-сервера – 5, время, в течение которого недоступные сервера не будут опрашиваться RADIUS-клиентом коммутатора – 10 минут, секретный ключ – `secret`. Добавить в список RADIUS-сервер, расположенный на узле сети с IP-адресом 192.168.16.3, порт сервера для аутентификации – 1645, количество попыток доступа к серверу – 2.

```
console# configure
console (config)# radius-server timeout 5
console (config)# radius-server retransmit 5
console (config)# radius-server deadtime 10
console (config)# radius-server key secret
console (config)# radius-server host 196.168.16.3 auth-port 1645
retransmit 2
```

- Показать параметры настройки RADIUS-серверов

```
console# show radius-servers
```

| IP address | Port | port | Time- | Ret- | Dead- | Prio. | Usage |
|--------------|------|------|--------|------|--------|-------|-------|
| | Auth | Acct | Out | rans | Time | | |
| 192.168.16.3 | 1645 | 1813 | Global | 2 | Global | 0 | all |

Global values

```
-----
TimeOut : 5
Retransmit : 5
Deadtime : 10
Source IPv4 interface :
Source IPv6 interface :
```

5.19.3 Протокол TACACS+

Протокол TACACS+ обеспечивает централизованную систему безопасности для проверки пользователей, получающих доступ к устройству, при этом поддерживая совместимость с RADIUS и другими процессами проверки подлинности. TACACS+ предоставляет следующие службы:

- *Authentication (проверка подлинности)*. Обеспечивается во время входа в систему по именам пользователей и определенным пользователями паролям;
- *Authorization (авторизация)*. Обеспечивается во время входа в систему. После завершения сеанса проверки подлинности запускается сеанс авторизации с использованием проверенного имени пользователя, также сервером проверяются привилегии пользователя.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console (config) #
```

Таблица 178 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|---|--|--|
| tacacs-server host {ip_address hostname} [single-connection] [port-number port] [timeout timeout] [key secret_key] [priority priority] | hostname: (1..158) символов; port: (0..65535)/49; timeout: (1..30) сек; secret_key: (0..128) символов; priority: (0..65535)/0; | Добавляет указанный сервер в список используемых TACACS серверов. - ip_address – IP-адрес TACACS-сервера; - hostname – сетевое имя TACACS-сервера; - single-connection – в каждый момент времени иметь не больше одного соединения для обмена данными с TACACS-сервером; - port – номер порта для обмена данными с TACACS-сервером; - timeout – интервал ожидания ответа от сервера; - secret_key – ключ для аутентификации и шифрования всего обмена данными TACACS; - priority – приоритет использования TACACS-сервера (чем ниже значение, тем приоритетнее сервер); - encrypted – значение secret_key в зашифрованном виде. В случае отсутствия в команде параметров timeout, secret_key для данного TACACS-сервера используются значения, настроенные с помощью команд, указанных ниже. |
| encrypted tacacs-server host {ip_address hostname} [single-connection] [port-number port] [timeout timeout] [key secret_key] [priority priority] | | Удаляет указанный сервер из списка используемых TACACS-серверов. |
| no tacacs-server host {ip_address hostname} | key: (0..128) символов/по умолчанию ключ – пустая строка | Устанавливает ключ, используемый по умолчанию, для аутентификации и шифрования всего обмена данными TACACS между устройством и окружением TACACS; - encrypted – значение secret_key в зашифрованном виде. |
| tacacs-server key key | | Устанавливает значение по умолчанию. |
| encrypted tacacs-server key key | | Устанавливает интервал ожидания ответа от сервера, используемый по умолчанию. |
| no tacacs-server key | timeout: (1..30)/5 сек | Установить значение по умолчанию. |
| tacacs-server timeout timeout | | Задаёт интерфейс устройства, IP-адрес которого будет использоваться по умолчанию в качестве адреса источника для обмена сообщениями с TACACS-сервером. |
| no tacacs-server timeout | vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); loopback_id (1..64); tunnel (1-16); group: (1..128) | Удаляет интерфейс устройства. |
| tacacs-server host source-interface {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group loopback loopback_id tunnel tunnel vlan vlan id} | | |
| no tacacs-server host source-interface | | |

Команды режима EXEC

Вид запроса командной строки в режиме EXEC:

```
console#
```

Таблица 179 – Команды режима EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|--|--------------------------------|---|
| show tacacs [ip_address hostname] | host_name: (1..158) символов | Отображает настройку и статистику для сервера TACACS+. - ip_address – IP-адрес TACACS+ сервера; - hostname – имя сервера. |

5.19.4 Протокол управления сетью (SNMP)

SNMP – технология, призванная обеспечить управление и контроль над устройствами и приложениями в сети связи путём обмена управляющей информацией между агентами, расположенными на сетевых устройствах, и менеджерами, находящимися на станциях управления. SNMP определяет сеть как совокупность сетевых управляющих станций и элементов сети (главные машины, шлюзы и маршрутизаторы, терминальные серверы), которые совместно обеспечивают административные связи между сетевыми управляющими станциями и сетевыми агентами.

Коммутаторы позволяют настроить работу протокола SNMP для удаленного мониторинга и управления устройством. Устройство поддерживает протоколы версий SNMPv1, SNMPv2, SNMPv3.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 180 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--|--|--|
| snmp-server server | По умолчанию | Включить поддержку протокола SNMP. |
| no snmp-server server | поддержка протокола SNMP отключена | Отключает поддержку протокола SNMP. |
| snmp-server community <i>community [ro rw su]</i> <i>[ipv4_address ipv6_address ipv6z_address] [mask mask prefix prefix_length]] [view view_name]</i> | community: (1..20) символов; encrypted_community: (1..20) символов; формат ipv4_address: A.B.C.D; формат ipv6_address: X:X:X::X; формат ipv6z_address: X:X:X::X%<ID>; mask: - /255.255.255.255; prefix_length: (1..32)/32; view_name: (1..30) символов; group_name: (1..30) символов | Устанавливает значение строки сообщества для обмена данными по протоколу SNMP. - <i>community</i> – строка сообщества (пароль) для доступа по протоколу SNMP; - encrypted – задать строку сообщества в зашифрованном виде; - ro – доступ только для чтения; - rw – доступ для чтения и записи; - su – доступ администратора; - <i>view_name</i> – определяет имя для правила обозрения SNMP, которое должно быть предварительно определено с помощью команды snmp-server view . Определяет объекты, доступные сообществу; - <i>ipv4_address, ipv6_address, ipv6z_address</i> – IP-адрес устройства; - <i>mask</i> – маска адреса IPv4, которая определяет, какие биты адреса источника пакета сравниваются с заданным IP-адресом; - <i>prefix_length</i> – число бит, которые составляют префикс IPv4-адреса; - <i>group_name</i> – определяет имя группы, которое должно быть предварительно определено с помощью команды snmp-server group . Определяет объекты, доступные сообществу. |
| snmp-server view <i>view_name</i> <i>OID {included excluded}</i> | view_name: (1..30) символов | Создает или редактирует правило обозрения для SNMP – разрешающее правило, либо ограничивающее серверу-обозревателю доступ к OID. - <i>OID</i> – идентификатор объекта MIB, представленный в виде дерева ASN.1 (строка вида 1.3.6.2.4, может включать в себя зарезервированные слова, например: system, dod). С помощью символа * можно обозначить семейство поддеревьев: 1.3.*.2); - include – OID включена в правило для обозрения; - exclude – OID исключена из правила для обозрения. |
| no snmp-server view <i>viewname [OID]</i> | | Удаляет правило обозрения для SNMP. |

| | | |
|--|--|---|
| encrypted snmp-server user username groupname {v3 remote host v3 [encrypted] [auth {md5 sha} auth- password] } | username: (1..20) символов groupname: (1..30) символов engineid-string: (5..32) символов password: (1..32) символа md5: 16 или 32 байт sha: 20 или 36 байт формат IPv4: A.B.C.D IPv6: X:X:X::X IPv6z: X:X:X::X%<ID> | Создает SNMPv3- пользователя. - <i>username</i> – имя пользователя; - <i>groupname</i> – имя группы; - <i>engineid-string</i> – идентификатор удаленного SNMP-устройства, которому пользователь принадлежит; - <i>auth-password</i> – пароль для аутентификации и генерации ключа; - <i>md5</i> – ключ md5; - <i>sha</i> – ключ sha; - <i>host</i> – IP-адрес/ имя хоста. |
| no snmp-server user username [remote engineid-string] | | Удаляет SNMP-v3-пользователя. |
| snmp-server group group_name {v1 v2 v3 {noauth auth priv} [notify notify_view]} [read read_view] [write write_view] | group_name: (1..30) символов; notify_view: (1..32) символов; read_view: (1..32) символов; write_view: (1..32) символов | Создает SNMP-группу или таблицу соответствий SNMP-пользователей и правил обозрений SNMP. - v1, v2, v3 – SNMP v1, v2, v3 модель безопасности; - noauth, auth, priv – тип аутентификации, используемый протоколом SNMP v3 (noauth – без аутентификации, auth – аутентификация без шифрования, priv – аутентификация с шифрованием); - <i>notify_view</i> – имя правила обозрения, которому разрешено определять сообщения SNMP-агента – <i>inform</i> и <i>trap</i> ; - <i>read_view</i> – имя правила обозрения, которому разрешено только чтение содержимого SNMP-агента коммутатора; - <i>write_view</i> – имя правила обозрения, которому разрешено вводить данные и конфигурировать содержимое SNMP-агента коммутатора. |
| no snmp-server group groupname {v1 v2 v3 [noauth auth priv]} | | Удаляет SNMP-группу. |
| snmp-server user user_name group_name {v1 v2c v3 [remote {ip_address host}]} | user_name: (1..20) символов; group_name: (1..30) символов | Создает SNMPv3-пользователя. - <i>user_name</i> – имя пользователя; - <i>group_name</i> – имя группы. |
| no snmp-server user user_name {v1 v2c v3 [remote {ip_address host}]} | | Удаляет SNMPv3-пользователя. |
| snmp-server filter filter_name OID {included excluded} | filter_name: (1..30) символов | Создает или редактирует правило SNMP-фильтра, которое позволяет фильтровать <i>inform</i> и <i>trap</i> -сообщения, передаваемые SNMP-серверу. - <i>filter_name</i> – имя SNMP-фильтра; - <i>OID</i> – идентификатор объекта MIB, представленный в виде дерева ASN.1 (строка вида 1.3.6.2.4, может включать в себя зарезервированные слова, например: <i>system</i> , <i>dod</i> . С помощью символа * можно обозначить семейство поддеревьев: 1.3.*.2); - include – OID включена в правило фильтрации; - exclude – OID исключена из правила фильтрации. |
| no snmp-server filter filter_name [OID] | | Удаляет правило SNMP-фильтра. |

| | | |
|--|---|---|
| snmp-server host <i>{ipv4_address ipv6_address hostname}</i> [traps informs] [version {1 2c 3 {noauth auth priv}}] {community username} [udp-port port] [filter filter_name] [timeout seconds] [retries retries] | hostname: (1..158) символов; community: (1..20) символов; username: (1..20) символов port: (1..65535)/162; filter_name: (1..30) символов; seconds: (1..300)/15; retries: (0..255)/3 | Определяет настройки для передачи сообщений уведомления inform и trap SNMP-серверу. - <i>community</i> – строка сообщества SNMPv1/2с для передачи сообщений уведомления; - <i>username</i> – имя пользователя SNMPv3 для аутентификации; - version – определяют тип сообщений trap – trap SNMPv1, trap SNMPv2, trap SNMPv3; - auth – указывает подлинность пакета без шифрования; - noauth – не указывает подлинность пакета; - priv – указывает подлинность пакета с шифрованием; - <i>port</i> – UDP-порт SNMP-сервера; - <i>seconds</i> – период ожидания подтверждений перед повторной передачей сообщений inform; - <i>retries</i> – количество попыток передачи сообщений inform, при отсутствии их подтверждения. |
| no snmp-server host <i>{ipv4_address ipv6_address hostname}</i> [traps informs] | | Удаляет настройки для передачи сообщений уведомления inform и trap SNMPv1/v2/v3-серверу. |
| snmp-server engineid local <i>{engineid_string default}</i> | engineid_string: (5..32) символов | Создает идентификатор локального SNMP-устройства – engineID. - <i>engineid_string</i> – имя SNMP-устройства; - default – при использовании данной настройки engine ID будет автоматически создан на основе MAC-адреса устройства. |
| no snmp-server engineid local | | Удаляет идентификатор локального SNMP-устройства – engine ID |
| snmp-server source-interface {traps informs} { tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group loopback loopback_id vlan vlan id} | te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); loopback_id: (1..64) group: (1..128) | Задает интерфейс устройства, IP-адрес которого будет использоваться по умолчанию в качестве адреса источника для обмена сообщениями с SNMP-сервером. |
| no snmp-server source-interface [traps informs] | | Удаляет интерфейс устройства. |
| snmp-server source-interface-ipv6 {traps informs} { tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group loopback loopback_id vlan vlan id} | te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); loopback_id: (1..64) group: (1..128) | Аналогично для IPv6. |
| no snmp-server source-interface-ipv6 [traps informs] | | Удаляет интерфейс устройства. |
| snmp-server engineid remote <i>{ipv4_address ipv6_address hostname} engineid_string</i> | hostname: (1..158) символов; engineid_string: (5..32) символов | Создает идентификатор удаленного SNMP-устройства – engine ID. - <i>engineid_string</i> – идентификатор SNMP-устройства. |
| no snmp-server engineID remote <i>{ipv4_address ipv6_address hostname}</i> | | Удаляет идентификатор удаленного SNMP-устройства – engine ID. |
| snmp-server enable traps | -/включено | Включает поддержку SNMP trap-сообщений. |
| no snmp-server enable traps | | Отключает поддержку SNMP trap-сообщений. |
| snmp-server enable traps ospf | -/включено | Включает отправку SNMP trap-сообщений протокола OSPF. |
| no snmp-server enable traps ospf | | Отключает отправку SNMP trap-сообщений. |
| snmp-server enable traps ipv6 ospf | -/включено | Включает отправку SNMP trap-сообщений протокола OSPF (IPv6). |
| no snmp-server enable traps ipv6 ospf | | Отключает отправку SNMP trap-сообщений. |
| snmp-server enable traps erps | -/включено | Включает отправку SNMP trap-сообщений протокола ERPS. |

| | | |
|--|--|---|
| no snmp-server enable traps erps | | Отключает отправку SNMP trap-сообщений протокола ERPS. |
| snmp-server trap authentication | -/разрешено | Разрешает передавать сообщения trap-серверу, который не прошел аутентификацию. |
| no snmp-server trap authentication | | Запрещает передавать сообщения trap-серверу, который не прошел аутентификацию. |
| snmp-server contact text | text: (1..160) символов | Определяет контактную информацию устройства. |
| no snmp-server contact | | Удаляет контактную информацию устройства. |
| snmp-server location text | text: (1..160) символов | Определяет информацию о местоположении устройства. |
| no snmp-server location | | Удаляет информацию о местоположении устройства. |
| snmp-server set <i>variable_name name1 value1</i> <i>[name2 value2 [...]]</i> | variable_name, name, value должны задаваться в соответствии со спецификацией | Позволяет установить значения переменных в базе данных MIB коммутатора. - <i>variable_name</i> – имя переменной; - <i>name, value</i> – пары соответствий имя – значение. |
| snmp-server enable traps authentication | -/включено | Включает отправку SNMP trap-сообщений по событиям login/logout/reject. |
| no snmp-server enable traps authentication | | Отключает отправку SNMP trap-сообщений. |
| snmp-server enable traps dhcp-snooping limit clients | -/отключено | Включить отправку SNMP trap-сообщений при достижении предельного количества подключенных DHCP-клиентов. |
| no snmp-server enable traps dhcp-snooping limit clients | | Отключить отправку SNMP trap-сообщений. |

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

```
console(config-if) #
```

Таблица 181 – Команды режима конфигурации интерфейса Ethernet

| Команда | Значение/Значение по умолчанию | Действие |
|---------------------------------|---------------------------------------|--|
| snmp trap link-status | -/включено | Включает отправку SNMP trap-сообщений при изменении состояния настраиваемого порта. |
| no snmp trap link-status | | Выключает отправку SNMP trap-сообщений при изменении состояния настраиваемого порта. |

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console(config) #
```

Таблица 182 – Команды режима Privileged EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|--|---------------------------------------|---|
| show snmp | - | Показывает статус SNMP-соединений. |
| show snmp engineID | - | Показывает идентификатор локального SNMP-устройства – engineID. |
| show snmp views [view_name] | view_name: (1..30) символов | Показывает правила обозрения SNMP. |
| show snmp groups [group_name] | group_name: (1..30) символов | Показывает SNMP-группы. |
| show snmp filters [filter_name] | filter_name: (1..30) символов | Показывает SNMP-фильтры. |
| show snmp users [user_name] | user_name: (1..30) символов | Показывает SNMP-пользователей. |

5.19.5 Протокол удалённого мониторинга сети (RMON)

Протокол мониторинга сети (RMON) является расширением протокола SNMP, позволяя предоставить более широкие возможности контроля сетевого трафика. Отличие RMON от SNMP состоит в характере собираемой информации – данные собираемые RMON в первую очередь характеризуют трафик между узлами сети. Информация, собранная агентом, передается в приложение управления сетью.


Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 183 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--|--|--|
| rmon event <i>index type</i> [community <i>com_text</i>] [description <i>desc_text</i>] [owner name] | index: (1..65535); type: (none, log, trap, log-trap); com_text: (0..127) символов; desc_text: (0..127) символов; name: строка | Настраивает события, используемые в системе удаленного мониторинга. - <i>index</i> – индекс события; - <i>type</i> – тип уведомления, генерируемого устройством по этому событию: none – не генерировать уведомления, log – генерировать запись в таблице, trap – отсылать SNMP trap, log-trap – генерировать запись в таблице и отсылать SNMP trap; - <i>com_text</i> – строка сообщества SNMP для пересылки trap; - <i>desc_text</i> – описание события; - <i>name</i> – имя создателя события. |
| no rmon event <i>index</i> | | Удаляет событие, используемое в системе удаленного мониторинга. |
| rmon alarm <i>index mib_object_id interval rthreshold fthreshold revent fevent [type type] [startup direction] [owner name]</i> | index: (1..65535); mib_object_id: корректный OID; interval: (1..2147483647) сек; rthreshold: (0..2147483647); fthreshold: (0..2147483647); revent: (1..65535); fevent: (0..65535); type: (absolute, delta)/absolute; startup: (rising, falling, rising-falling)/rising-falling; name: строка | Настраивает условия выдачи аварийных сигналов. - <i>index</i> – индекс аварийного события; - <i>mib_object_id</i> – идентификатор переменной части объекта OID; - <i>interval</i> – интервал, в течение которого данные отбираются и сравниваются с восходящей и нисходящей границами; - <i>rthreshold</i> – восходящая граница; - <i>fthreshold</i> – нисходящая граница; - <i>revent</i> – индекс события, которое используется при пересечении восходящей границы; - <i>fevent</i> – индекс события, которое используется при пересечении нисходящей границы; - <i>type</i> – метод отбора указанных переменных и подсчета значения для сравнения с границами: Метод absolute – абсолютное значение выбранной переменной будет сравнено с границей на конце исследуемого интервала; Метод delta – значение выбранной переменной при последнем отборе будет вычтено из текущего значения и разница будет сравнена с границами (разница между значениями переменной в конце и в начале контрольного интервала); - startup – инструкция для генерации событий на первом контрольном интервале. Определяет правила генерации аварийных событий для первого контрольного интервала путем сравнения отобранной переменной с одной, либо обеими границами: - rising – генерировать единичное аварийное событие по восходящей границе, если значение отобранной переменной на первом контрольном интервале больше либо равно этой границе; - falling – генерировать единичное аварийное событие по нисходящей границе, если значение отобранной переменной на |

| | | |
|---|--|---|
| | | <p>первом контрольном интервале меньше либо равно этой границе;</p> <ul style="list-style-type: none"> - rising-falling – генерировать единичное аварийное событие по восходящей и/или нисходящей границе, если значение отобранной переменной на первом контрольном интервале больше либо равно восходящей границе и/или меньше либо равно нисходящей границе; - owner – имя создателя аварийного события. |
| no rmon alarm index | | Удаляет условие выдачи аварийных событий. |
| rmon table-size {history hist_entries log log_entries} | <p>hist_entries: (20..32767)/270; log_entries: (20..32767)/100</p> | <p>Задает максимальный размер RMON-таблиц.</p> <ul style="list-style-type: none"> - history – максимальное количество строк в таблице истории; - log – максимальное количество строк в таблице записей. <p> Значение вступит в силу только после перезагрузки устройства.</p> |
| no rmon table-size {history log} | | Устанавливает значение по умолчанию. |

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet, интерфейса группы портов:

```
console(config-if) #
```

Таблица 184 – Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|--|
| rmon collection stats index [owner name] [buckets bucket_num] [interval interval] | <p>index: (1..65535); name: (0..160) символов; bucket-num: (1..50)/50; interval: (1..3600)/1800 сек</p> | <p>Включает формирование истории по группам статистики для базы данных (MIB) удаленного мониторинга.</p> <ul style="list-style-type: none"> - index – индекс требуемой группы статистики; - name – владелец группы статистики; - bucket_num – значение, ассоциируемое с количеством ячеек для сбора истории по группе статистики; - interval – период опроса для формирования истории. |
| no rmon collection stats index | | Выключает формирование истории по группам статистики для базы данных (MIB) удаленного мониторинга. |

Команды режима EХЕС

Вид запроса командной строки режима EХЕС:

```
console>
```

Таблица 185 – Команды режима EХЕС

| Команда | Значение/Значение по умолчанию | Действие |
|--|--|--|
| show rmon statistics { gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port port-channel group} | <p>gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); tve_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128)</p> | Показывает статистику интерфейса Ethernet либо группы портов, используемую для удаленного мониторинга. |

| | | |
|---|--|---|
| show rmon collection stats [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i>] | | Отображает информацию по запрашиваемым группам статистики. |
| show rmon history index {throughput errors other} [period <i>period</i>] | index: (1..65535); period: (1..2147483647) сек | Показывает историю Ethernet статистики RMON. - <i>index</i> – запрошенная группа статистики; - throughput – показывает счетчики производительности (пропускной способности); - errors – показывает счетчики ошибок; - other – показывает счетчики обрывов и коллизий; - <i>period</i> – показывает историю за запрошенный период времени. |
| show rmon alarm-table | - | Показывает сводную таблицу аварийных событий. |
| show rmon alarm index | index: (1..65535) | Показывает конфигурацию настройки аварийных событий. - <i>index</i> – индекс аварийного события. |
| show rmon events | - | Показывает таблицу событий удаленного мониторинга RMON. |
| show rmon log [index] | index: (0..65535) | Показывает таблицу записей удаленного мониторинга RMON. - <i>index</i> – индекс события. |

Примеры выполнения команд

- Показать статистику 10 интерфейса Ethernet:

```
console# show rmon statistics tengigabitethernet 1/0/10
```

```
Port te0/10
Dropped: 8
Octets: 878128 Packets: 978
Broadcast: 7 Multicast: 1
CRC Align Errors: 0 Collisions: 0
Undersize Pkts: 0 Oversize Pkts: 0
Fragments: 0 Jabbers: 0
64 Octets: 98 65 to 127 Octets: 0
128 to 255 Octets: 0 256 to 511 Octets: 0
512 to 1023 Octets: 491 1024 to 1518 Octets: 389
```

Таблица 186 – Описание результатов

| Параметр | Описание |
|------------------|--|
| Dropped | Количество задетектированных событий, когда пакеты были отброшены. |
| Octets | Количество байт данных (включая байты плохих пакетов), принятых из сети (исключая фреймовые биты, но включая биты контрольной суммы). |
| Packets | Количество принятых пакетов (включая плохие, широковещательные и многоадресные пакеты). |
| Broadcast | Количество принятых широковещательных пакетов (только корректные пакеты). |
| Multicast | Количество принятых многоадресных пакетов (только корректные пакеты). |
| CRC Align Errors | Количество принятых пакетов длиной от 64 до 1518 байт включительно, имеющих неверную контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы – FCS), либо с нецелым числом байт (ошибки выравнивания – Alignment). |
| Collisions | Оценка количества коллизий на данном Ethernet-сегменте. |
| Undersize Pkts | Количество принятых пакетов длиной меньше 64 байт (исключая фреймовые биты, но включая биты контрольной суммы), но в остальном правильно сформированных. |
| Oversize Pkts | Количество принятых пакетов длиной больше 1518 байт (исключая фреймовые биты, но включая биты контрольной суммы), но в остальном правильно сформированных. |

| | |
|---------------------|--|
| Fragments | Количество принятых пакетов длиной меньше 64 байт (исключая фреймовые биты, но включая биты контрольной суммы), имеющих неверную контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы – FCS), либо с нецелым числом байт (ошибки выравнивания – Alignment). |
| Jabbers | Количество принятых пакетов длиной больше 1518 байт (исключая фреймовые биты, но включая биты контрольной суммы), имеющих неверную контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы – FCS), либо с нецелым числом байт (ошибки выравнивания – Alignment). |
| 64 Octet | Количество принятых пакетов (включая плохие пакеты) длиной 64 байта (исключая фреймовые биты, но включая биты контрольной суммы). |
| 65 to 127 Octets | Количество принятых пакетов (включая плохие пакеты) длиной от 65 до 127 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы). |
| 128 to 255 Octets | Количество принятых пакетов (включая плохие пакеты) длиной от 128 до 255 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы). |
| 256 to 511 Octets | Количество принятых пакетов (включая плохие пакеты) длиной от 256 до 511 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы). |
| 512 to 1023 Octets | Количество принятых пакетов (включая плохие пакеты) длиной от 512 до 1023 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы). |
| 1024 to 1518 Octets | Количество принятых пакетов (включая плохие пакеты) длиной от 1024 до 1518 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы). |

- Показать информацию по группам статистики для порта 8:

```
console# show rmon collection stats tengigabitethernet 1/0/8
```

| Index | Interface | Interval | Requested Samples | Granted Samples | Owner |
|-------|-----------|----------|-------------------|-----------------|-------|
| 1 | te0/8 | 300 | 50 | 50 | Eltex |

Таблица 187 – Описание результатов

| Параметр | Описание |
|-------------------|---|
| Index | Индекс, уникально идентифицирующий запись. |
| Interface | Ethernet-интерфейс, на котором запущен опрос. |
| Interval | Интервал в секундах между опросами. |
| Requested Samples | Запрошенное количество отсчетов, которое может быть сохранено. |
| Granted Samples | Разрешенное (оставшееся) количество отсчетов, которое может быть сохранено. |
| Owner | Владелец данной записи. |

- Показать счетчики пропускной способности для группы статистики 1:

```
console# show rmon history 1 throughput
```

| | | | | | |
|-------------------------|---------------------|---------|-----------|-----------|-----|
| Sample set: 1 | Owner: MES | | | | |
| Interface: te1/0/1 | Interval: 1800 | | | | |
| Requested samples: 50 | Granted samples: 50 | | | | |
| Maximum table size: 100 | | | | | |
| Time | Octets | Packets | Broadcast | Multicast | % |
| Nov 10 2009 18:38:00 | 204595549 | 278562 | 2893 | 675218 | 67% |

Таблица 188 – Описание результатов

| <i>Параметр</i> | <i>Описание</i> |
|-----------------|--|
| Time | Дата и время создания записи. |
| Octets | Количество байт данных (включая байты плохих пакетов) принятых из сети (исключая фреймовые биты, но включая биты контрольной суммы). |
| Packets | Количество принятых пакетов (включая плохие пакеты) в течение периода формирования записи. |
| Broadcast | Количество принятых хороших пакетов в течение периода формирования записи направленных на широковещательные адреса. |
| Multicast | Количество принятых хороших пакетов в течение периода формирования записи направленных на многоадресные адреса. |
| Utilization | Оценка средней пропускной способности физического уровня на данном интерфейсе в течение периода формирования записи. Пропускная способность оценивается величиной до тысячной процента. |
| CRC Align | Количество принятых в течение периода формирования записи пакетов длиной от 64 до 1518 байт включительно, имеющих неверную контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы – FCS), либо с нецелым числом байт (ошибки выравнивания – Alignment). |
| Collisions | Оценка количества коллизий на данном Ethernet сегменте в течение периода формирования записи. |
| Undersize Pkts | Количество принятых в течение периода формирования записи пакетов длиной меньше 64 байт (исключая фреймовые биты, но включая биты контрольной суммы), но в остальном правильно сформированных. |
| Oversize Pkts | Количество принятых в течение периода формирования записи пакетов длиной больше 1518 байт (исключая фреймовые биты, но включая биты контрольной суммы), но в остальном правильно сформированных. |
| Fragments | Количество принятых в течение периода формирования записи пакетов длиной меньше 64 байт (исключая фреймовые биты, но включая биты контрольной суммы), имеющих неверную контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы – FCS), либо с нецелым числом байт (ошибки выравнивания – Alignment). |
| Jabbers | Количество принятых в течение периода формирования записи пакетов длиной больше 1518 байт (исключая фреймовые биты, но включая биты контрольной суммы), имеющих неверную контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы – FCS), либо с нецелым числом байт (ошибки выравнивания – Alignment). |
| Dropped | Количество задетектированных событий, когда пакеты были отброшены в течение периода формирования записи. |

- Показать сводную таблицу сигналов тревоги:

```
console# show rmon alarm-table
```

| Index | OID | Owner |
|-------|------------------------|---------|
| 1 | 1.3.6.1.2.1.2.2.1.10.1 | CLI |
| 2 | 1.3.6.1.2.1.2.2.1.10.1 | Manager |

Таблица 189 – Описание результатов

| Параметр | Описание |
|----------|--|
| Index | Индекс, уникально идентифицирующий запись. |
| OID | OID контролируемой переменной. |
| Owner | Пользователь, создавший запись. |

- Показать конфигурацию аварийных событий с индексом 1:

```
console# show rmon alarm 1
```

```
Alarm 1
-----
OID: 1.3.6.1.2.1.2.2.1.10.1
Last sample Value: 878128
Interval: 30
Sample Type: delta
Startup Alarm: rising
Rising Threshold: 8700000
Falling Threshold: 78
Rising Event: 1
Falling Event: 1
Owner: CLI
```

Таблица 190 – Описание результатов

| Параметр | Описание |
|-------------------|--|
| OID | OID контролируемой переменной. |
| Last Sample Value | Значение переменной на последнем контрольном интервале. Если метод отбора переменных absolute – то это абсолютное значение переменной, если delta – то разница между значениями переменной в конце и в начале контрольного интервала. |
| Interval | Интервал в секундах, в течение которого данные отбираются и сравниваются с верхней и нижней границами. |
| Sample Type | Метод отбора указанных переменных и подсчета значения для сравнения с границами. Метод absolute – абсолютное значение выбранной переменной будет сравнено с границей на конце исследуемого интервала. Метод delta – значение выбранной переменной при последнем отборе будет вычтено из текущего значения, и разница будет сравнена с границами (разница между значениями переменной в конце и в начале контрольного интервала). |
| Startup Alarm | Инструкция для генерации событий на первом контрольном интервале. Определяет правила генерации аварийных событий для первого контрольного интервала путем сравнения отобранной переменной с одной, либо обеими границами. rising – генерировать единичное аварийное событие по восходящей границе, если значение отобранной переменной на первом контрольном интервале больше либо равно этой границе. falling – генерировать единичное аварийное событие по нисходящей границе, если значение отобранной переменной на первом контрольном интервале меньше либо равно этой границе. rising-falling – генерировать единичное аварийное событие по восходящей и/или нисходящей границе, если значение отобранной переменной на первом контрольном интервале больше либо равно восходящей границе, и/или меньше либо равно нисходящей границе. |
| Rising Threshold | Значение восходящей границы. Когда значение отобранной переменной на предыдущем контрольном интервале было меньше данной границы, а на текущем контрольном интервале больше либо равно значению границы, тогда единичное событие генерируется. |

| | |
|-------------------|--|
| Falling Threshold | Значение нисходящей границы. Когда значение отобранной переменной на предыдущем контрольном интервале было больше данной границы, а на текущем контрольном интервале меньше либо равно значению границы, тогда единичное событие генерируется. |
| Rising Event | Индекс события используемого, когда восходящая граница пересечена. |
| Falling Event | Индекс события используемого, когда нисходящая граница пересечена. |
| Owner | Пользователь, создавший запись. |

- Показать таблицу событий удаленного мониторинга RMON:

```
console# show rmon events
```

| Index | Description | Type | Community | Owner | Last time sent |
|-------|----------------|----------|-----------|---------|----------------------|
| 1 | Errors | Log | | CLI | Nov 10 2009 18:47:17 |
| 2 | High Broadcast | Log-Trap | router | Manager | Nov 10 2009 18:48:48 |

Таблица 191 – Описание результатов

| Параметр | Описание |
|----------------|---|
| Index | Индекс, уникально идентифицирующий событие. |
| Description | Комментарий, описывающий событие. |
| Type | Тип уведомления, генерируемого устройством по этому событию: - none – не генерировать уведомления; - log – генерировать запись в таблице; - trap – отсылать SNMP trap; - log-trap – генерировать запись в таблице и отсылать SNMP trap. |
| Community | Строка сообщества SNMP для пересылки trap. |
| Owner | Пользователь, создавший событие. |
| Last time sent | Время и дата генерирования последнего события. Если не было сгенерировано событий, то это значение будет равно нулю. |

- Показать таблицу записей удаленного мониторинга RMON:

```
console# show rmon log
```

| | | |
|-------------------------|-------------|----------------------|
| Maximum table size: 100 | | |
| Event | Description | Time |
| 1 | Errors | Nov 10 2009 18:48:33 |

Таблица 192 – Описание результатов

| Параметр | Описание |
|-------------|--|
| Index | Индекс, уникально идентифицирующий запись. |
| Description | Комментарий, описывающий событие. |
| Time | Время создания записи. |

5.19.6 Списки доступа ACL для управления устройством

Программное обеспечение коммутаторов позволяет разрешить либо ограничить доступ к управлению устройством через определенные порты или группы VLAN. Для этой цели создаются списки доступа (Access Control List, ACL) для управления.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console (config) #
```

Таблица 193 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--|---------------------------------------|--|
| management access-list name | name: (1..32) символа | Создает список доступа для управления. Вход в режим конфигурации списка доступа для управления. |
| no management access-list name | | Удаляет список доступа для управления. |
| management access-class {console-only name} | name: (1..32) символа | Ограничивает управление устройством по определенному списку доступа (access list). Активирует указанный список доступа. - console-only – управление устройством доступно только с консоли. |
| no management access-class | | Отменяет ограничение на управление устройством по определенному списку доступа (access list). |

Команды режима конфигурации списка доступа для управления

Вид запроса командной строки в режиме конфигурации списка доступа для управления:

```
console (config) # management access-list eltex_manag
console (config-macl) #
```

Таблица 194 – Команды режима конфигурации списка доступа для управления

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|--|
| permit [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group oob vlan vlan_id] [service service] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128); vlan_id: (1..4094) service: (telnet, snmp, http, https, ssh) | Задаёт разрешающее условие для управляющего списка доступа. - <i>service</i> – тип доступа. |
| permit ip-source {ipv4_address ipv6_address/prefix_length} [mask {mask prefix_length}] [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group oob vlan vlan_id] [service service] | | |
| deny [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group oob vlan vlan_id] [service service] [ace-priority index] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128); vlan_id: (1..4094); | Задаёт запрещающее условие для управляющего списка доступа. - <i>service</i> – тип доступа, |

| | | |
|--|---|--|
| <code>deny ip-source {ipv4_address ipv6_address/prefix_length} [mask {mask prefix_length}] [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port port-channel group oob vlan vlan_id] [service service]</code> | service: (telnet, snmp, http, https, ssh) | |
|--|---|--|

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 195 – Команды режима Privileged EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---------------------------------------|---|
| <code>show management access-list [name]</code> | name: (1..32) символа | Показывает списки доступа (access list) для управления. |
| <code>show management access-class</code> | - | Показывает информацию об активных списках доступа (access list) для управления. |

5.19.7 Настройка доступа

5.19.7.1 Telnet, SSH


Данные команды предназначены для настройки серверов доступа для управления коммутатором. Поддержка серверов Telnet и SSH коммутатором позволяет удаленно подключаться к нему для мониторинга и конфигурации.


Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 196 – Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|----------------------------------|---------------------------------------|---|
| <code>ip telnet server</code> | По умолчанию Telnet сервер включен | Разрешает удаленное конфигурирование устройства через Telnet. |
| <code>no ip telnet server</code> | | Запрещает удаленное конфигурирование устройства через Telnet. |
| <code>ip ssh server</code> | По умолчанию SSH сервер отключен | Разрешает удаленное конфигурирование устройства через SSH.  До тех пор, пока ключ для шифрования не сгенерирован, SSH-сервер будет находиться в резерве. После генерации ключа (используемые команды <code>crypto key generate rsa</code> и <code>crypto key generate dsa</code>) сервер перейдет в рабочее состояние. |
| <code>no ip ssh server</code> | | Запрещает удаленное конфигурирование устройства через SSH. |

| | | |
|--|---|---|
| ip ssh port <i>port_number</i> | port_number: (1..65535)/22 | TCP-порт, используемый SSH-сервером. |
| no ip ssh port | | Устанавливает значение по умолчанию. |
| ip ssh-client source-interface { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> loopback <i>loopback_id</i> vlan <i>vlan_id</i> } | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); <i>loopback_id</i> : (1..64) <i>group</i> : (1..128); <i>vlan_id</i> : (1..4094) | Задает интерфейс для SSH-сессий. |
| no ip ssh-client source-interface | | Удаляет интерфейс. |
| ipv6 ssh-client source-interface { gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> loopback <i>loopback_id</i> vlan <i>vlan_id</i> } | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); <i>loopback_id</i> : (1..64) <i>group</i> : (1..128); <i>vlan_id</i> : (1..4094) | Задает интерфейс для IPv6 SSH-сессий. |
| no ipv6 ssh-client source-interface | | Удаляет интерфейс. |
| ip ssh pubkey-auth | По умолчанию использование публичного ключа запрещено | Разрешает использование публичного ключа для входящих SSH-сессий. |
| no ip ssh pubkey-auth | | Запрещает использование публичного ключа для входящих SSH-сессий. |
| ip ssh cipher <i>algorithms</i> | <i>algorithms</i> : (3des, aes128, aes192, aes256, arcfour, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com aes256-gcm@openssh, chacha20-poly1305@openssh.com) /разрешены все алгоритмы, кроме none | Задает список разрешенных алгоритмов шифрования для сервера. |
| no ip ssh cipher | | Восстанавливает список разрешенных алгоритмов обмена ключами по умолчанию. |
| ip ssh kex <i>methods</i> | <i>methods</i> : (dh-group-exchange-sha1, dh-group1-sha1, curve25519-sha256@libssh.org, diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group14-sha256, diffie-hellman-group14-sha1)/ разрешены все методы | Задает список разрешенных методов обмена ключами для сервера. |
| no ip ssh kex | | Восстанавливает список разрешенных алгоритмов обмена ключами по умолчанию. |
| ip ssh password-auth | По умолчанию включено | Включает режим аутентификации по паролю. |
| no ip ssh password-auth | | Отключает режим аутентификации по паролю. |
| crypto key pubkey-chain <i>ssh</i> | По умолчанию ключ не создан | Входит в режим конфигурации публичного ключа. |
| crypto key generate <i>dsa</i> | - | Генерирует пару ключей DSA – частный и публичный для SSH-сервиса.  Если хотя бы один из пары ключей уже создан, то система предложит перезаписать ключ. |
| crypto key generate <i>rsa</i> | - | Генерирует пару ключей RSA – частный и публичный для SSH-сервиса.  Если хотя бы один из пары ключей уже создан, то система предложит перезаписать ключ. |
| crypto key import <i>dsa</i> | - | Импортирует пару ключей DSA. |
| encrypted crypto key import <i>dsa</i> | - | - encrypted – в зашифрованном виде. |
| crypto key import <i>rsa</i> | - | Импортирует пару ключей RSA. |

| | | |
|--|-----------------------------------|---|
| encrypted crypto key import rsa | | - encrypted – в зашифрованном виде. |
| ip http server | по умолчанию HTTP-сервер включен | Разрешает удаленное конфигурирование устройства через web. |
| no ip http server | | Запрещает удаленное конфигурирование устройства через web. |
| ip http port port | 1..59999/80 | Задает порт HTTP-сервера. |
| no ip http port | | Восстанавливает значение по умолчанию. |
| ip http secure-server | по умолчанию HTTPS-сервер включен | Включает HTTPS-сервер. |
| no ip http secure-server | | Выключает HTTPS-сервер. |
| ip http timeout-policy seconds [http-only https-only] | seconds: (0..86400)/600 | Задает таймаут HTTP-сессии. |
| no ip http timeout-policy | | Восстанавливает значение по умолчанию. |
| crypto certificate {1 2} generate | - | Генерирует SSL-сертификат. |
| crypto certificate {1 2} import | | Импортирует SSL-сертификат, назначенный центром сертификации. |
| no crypto certificate {1 2} | | Восстанавливает SSL-сертификат по умолчанию для указанного сертификата. |



Ключи, сгенерированные командами `crypto key generate rsa` и `crypto key generate dsa`, сохраняются в закрытом для пользователя файле конфигурации.

Команды режима конфигурации публичного ключа

Вид запроса командной строки в режиме конфигурации публичного ключа:

```
console# configure
console(config)# crypto key pubkey-chain ssh
console(config-pubkey-chain)#
```

Таблица 197 – Команды режима конфигурации публичного ключа

| Команда | Значение/Значение по умолчанию | Действие |
|--------------------------------------|---------------------------------------|---|
| user-key username {rsa dsa} | username: (1..48) символов | Вход в режим создания индивидуального публичного ключа. - rsa – создать RSA-ключ; - dsa – создать DSA-ключ. |
| no user-key username | | Удаляет публичный ключ для определенного пользователя. |

Вид запроса командной строки в режиме создания индивидуального публичного ключа:

```
console# configure
console(config)# crypto key pubkey-chain ssh
console(config-pubkey-chain)# user-key eltex rsa
console(config-pubkey-key)#
```

Таблица 198 – Команды режима создания индивидуального публичного ключа

| Команда | Значение/Значение по умолчанию | Действие |
|----------------------------------|---------------------------------------|---|
| key-string | - | Создает публичный ключ для определенного пользователя. |
| key-string row key_string | - | Создает публичный ключ для определенного пользователя. Ввод ключа осуществляется построчно. - key_string – часть ключа. Для того чтобы система поняла, что ключ введен полностью, необходимо ввести команду <code>key-string row</code> без символов. |

Команды режима EXEC

Команды данного раздела доступны только для привилегированных пользователей.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 199 – Команды режима EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|---|---|--|
| <code>show ip ssh</code> | - | Показывает конфигурацию SSH-сервера, а также активные входящие SSH-сессии. |
| <code>show crypto key pubkey-chain ssh [username username] [fingerprint {bubble-babble hex}]</code> | username: (1..48) символов. По умолчанию отпечаток ключа в шестнадцатеричном формате. | Показывает публичные SSH-ключи, сохраненные на коммутаторе. - <i>username</i> – имя удаленного клиента; - bubble-babble – отпечаток ключа в коде Bubble Babble; - hex – отпечаток ключа в шестнадцатеричном коде. |
| <code>show crypto key mypubkey [rsa dsa]</code> | - | Показывает публичные ключи SSH-коммутатора. |
| <code>show crypto certificate [1 2]</code> | - | Отображает SSL-сертификаты для HTTPS-севера. |

Примеры выполнения команд

Включить сервер SSH на коммутаторе. Разрешить использование публичных ключей. Создать RSA-ключ для пользователя **eltex**:

```
console# configure
console(config)# ip ssh server
console(config)# ip ssh pubkey-auth
console(config)# crypto key pubkey-chain ssh
console(config-pubkey-chain)# user-key eltex rsa
console(config-pubkey-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAQACvTnRwPWlA14kpqIw9GBRonZQZxjHKcqKL6rMlQ+ZNXf
ZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+Vu4GRfpSwoQUvV35LqJJk67IOU/zfwO11gkTwm175Q
R9gHujS6KwGN2QWXgh3ub8gDjTSqmuSn/Wd05iDX2IExQWu08licglk02LYciz+Z4TrEU/9FJx
wPiVQOjc+KBXuR0juNg5nFYsY0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA6w9o44t6+AINEICB
CCA4YcF6zMzaT1wefWwX6f+Rmt5nhhqdatN/4oJfcel66DqVX1gWmNzNR4DYDvSzg01DnwCAC8
Qh Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

5.19.7.2 Команды конфигурации терминала

Команды конфигурации терминала служат для настройки параметров локальной и удаленной консоли.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 200 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--|--------------------------------|---|
| <code>line {console telnet ssh}</code> | - | Вход в режим соответствующего терминала (локальная консоль, удаленная консоль – Telnet или удаленная защищенная консоль – SSH). |

Команды режима конфигурации терминала

Вид запроса командной строки в режиме конфигурации терминала

```
console# configure
console(config)# line {console|telnet|ssh}
console(config-line)#
```

Таблица 201 – Команды режима конфигурации терминала

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---|---|
| speed <i>bps</i> | bps: (4800, 9600, 19200, 38400, 57600, 115200)/115200 бод | Устанавливает скорость доступа по локальной консоли (команда доступна только в режиме конфигурации локальной консоли). |
| no speed | | Устанавливает значение по умолчанию. |
| autobaud | -/включено | Включает автоматическое определение скорости доступа по локальной консоли (команда доступна только в режиме конфигурации локальной консоли). |
| no autobaud | | Выключает автоматическое определение скорости доступа по локальной консоли. |
| exec-timeout <i>minutes</i> [<i>seconds</i>] | minutes: (0..65535)/10 мин; seconds: (0..59)/0 сек | Задаёт интервал, в течение которого система ожидает ввода пользователя. Если в течение данного интервала пользователь ничего не вводит, то консоль отключается. |
| no exec-timeout | | Устанавливает значение по умолчанию. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 202 – Команды режима EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---------------------------------------|---------------------------------|
| show line [<i>console</i> <i>telnet</i> <i>ssh</i>] | - | Показывает параметры терминала. |

5.20 Журнал аварий, протокол SYSLOG

Системные журналы позволяют вести историю событий, произошедших на устройстве, а также контролировать произошедшие события в реальном времени. В журнал заносятся события семи типов: чрезвычайные, сигналы тревоги, критические и не критические ошибки, предупреждения, уведомления, информационные и отладочные.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 203 – Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|-------------------|---------------------------------------|---|
| logging on | -/регистрация включена | Включает регистрацию отладочных сообщений и сообщений об ошибках. |

| | | |
|---|--|---|
| no logging on | | <p>Выключает регистрацию отладочных сообщений и сообщений об ошибках.</p> <p><input checked="" type="checkbox"/> При выключенной регистрации отладочные сообщения и сообщения об ошибках будут передаваться на консоль.</p> |
| logging host { <i>ip_address</i> <i>host</i> } [<i>port port</i>] [<i>severity level</i>] [<i>facility facility</i>] [<i>description text</i>] | <p>host: (1..158) символов; port: (1..65535)/514; level: (см. Таблица 204); facility: (local0..7)/local7; text: (1..64) символов</p> | <p>Включает передачу аварийных и отладочных сообщений на удаленный SYSLOG-сервер.</p> <ul style="list-style-type: none"> - <i>ip_address</i>— IPv4 или IPv6-адрес SYSLOG-сервера; - <i>host</i> – сетевое имя SYSLOG-сервера; - <i>port</i> – номер порта для передачи сообщений по протоколу SYSLOG; - <i>level</i> – уровень важности сообщений, передаваемых на SYSLOG-сервер; - <i>facility</i> – услуга, передаваемая в сообщениях; - <i>text</i> – описание SYSLOG-сервера. |
| no logging host { <i>ip_address</i> <i>host</i> } | | Удаляет выбранный сервер из списка используемых SYSLOG-серверов. |
| logging console [<i>level</i>] | level: (см. Таблица 204)/informational | Включает передачу аварийных или отладочных сообщений выбранного уровня важности на консоль. |
| no logging console | | Выключает передачу аварийных или отладочных сообщений на консоль. |
| logging buffered [<i>severity_level</i>] | severity_level: (см. Таблица 204)/informational | Включает передачу аварийных или отладочных сообщений выбранного уровня важности во внутренний буфер. |
| no logging buffered | | Выключает передачу аварийных или отладочных сообщений во внутренний буфер. |
| logging cli-commands | -/отключено | Включает логирование введенных в CLI команд. |
| no logging cli-commands | | Отключает логирование введенных в CLI команд. |
| logging buffered size <i>size</i> | size: (20..1000)/200 | Изменяет количество сообщений, запоминаемых во внутреннем буфере. Новое значение размера буфера применится после перезагрузки устройства. |
| no logging buffered size | | Устанавливает значение по умолчанию. |
| logging file [<i>level</i>] | level: (Таблица 204) /errors | Включает передачу аварийных или отладочных сообщений выбранного уровня важности в файл журнала. |
| no logging file | | Выключает передачу аварийных или отладочных сообщений в файл журнала. |
| aaa logging login | -/включено | Заносить в журналы события аутентификации, авторизации и учета (AAA). |
| no aaa logging login | | Не заносить в журналы события аутентификации, авторизации и учета (AAA). |
| file-system logging { <i>copy</i> <i>delete-rename</i> } | По умолчанию регистрация включена | Включает регистрацию событий файловой системы. |
| no file-system logging { <i>copy</i> <i>delete-rename</i> } | | Выключает регистрацию событий файловой системы. |
| logging aggregation on | -/отключено | Включает контроль агрегации syslog-сообщений. |
| no logging aggregation on | | Отключает агрегацию syslog-сообщений. |
| logging aggregation aging-time <i>sec</i> | sec: (15..3600)/300 секунд | Устанавливает время хранения сгруппированных syslog-сообщений. |
| no logging aggregation aging-time | | Устанавливает значение по умолчанию. |
| logging service cpu-rate-limits <i>traffic</i> | traffic: (http, telnet, ssh, snmp, ip, link-local, arp-switch-mode, arp-inspection, stp-bpdu, other-bpdu, dhcp-snooping, dhcpv6-snooping, igmp-snooping, mld-snooping, sflow, log-deny-aces, vrrp)/- | Включает контроль ограничения скорости входящих кадров для определенного типа трафика. |
| no logging service cpu-rate-limits <i>traffic</i> | | Отключает логирование. |
| logging origin-id { <i>string</i> <i>hostname</i> <i>ip</i> <i>ipv6</i> } | -/нет | Задаёт параметр, который будет использоваться в качестве идентификатора хоста в syslog-сообщениях. |

| | | |
|--|--|---|
| no logging origin-id | | Использовать значение по умолчанию. |
| logging source-interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> loopback <i>loopback_id</i> vlan <i>vlan_id</i> } | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); loopback_id: (1..64) group: (1..128); vlan_id: (1..4094) | Использовать IP-адрес указанного интерфейса в качестве источника в IP-пакетах протокола SYSLOG. |
| no logging source-interface | | Использовать IP-адрес исходящего интерфейса. |
| logging source-interface-ipv6 {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> loopback <i>loopback_id</i> vlan <i>vlan_id</i> } | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); loopback_id: (1..64) group: (1..128); vlan_id: (1..4094) | Использовать IPv6-адрес указанного интерфейса в качестве источника в IP-пакетах протокола SYSLOG. |
| no logging source-interface-ipv6 | | Использовать IPv6-адрес исходящего интерфейса. |

Каждое сообщение имеет свой уровень важности — в таблице 204 приведены типы сообщений в порядке убывания их важности.

Таблица 204 – Типы важности сообщений

| <i>Тип важности сообщений</i> | <i>Описание</i> |
|--------------------------------|---|
| Чрезвычайные (emergencies) | В системе произошла критическая ошибка, система может работать неправильно. |
| Сигналы тревоги (alerts) | Необходимо немедленное вмешательство в систему. |
| Критические (critical) | В системе произошла критическая ошибка. |
| Ошибочные (errors) | В системе произошла ошибка. |
| Предупреждения (warnings) | Предупреждение, неаварийное сообщение. |
| Уведомления (notifications) | Уведомление системы, неаварийное сообщение. |
| Информационные (informational) | Информационные сообщения системы. |
| Отладочные (debugging) | Отладочные сообщения, предоставляют пользователю информацию для корректной настройки системы. |

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 205 – Команда режима Privileged EXEC для просмотра файла журнала

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|----------------------------|---------------------------------------|--|
| clear logging | - | Удаляет все сообщения из внутреннего буфера. |
| clear logging file | - | Удаляет все сообщения из файла журнала. |
| show logging file | - | Отображает состояние журнала, аварийные и отладочные сообщения, записанные в файле журнала. |
| show logging | - | Отображает состояние журнала, аварийные и отладочные сообщения, записанные во внутреннем буфере. |
| show syslog-servers | - | Отображает настройки для удалённых syslog-серверов. |

Примеры использования команд

- Включить регистрацию ошибочных сообщений на консоли:

```
console# configure
console (config)# logging on
console (config)# logging console errors
```

- Очистить файл журнала:

```
console# clear logging file
Clear Logging File [y/n]y
```

5.21 Зеркалирование (мониторинг) портов

Функция зеркалирования портов предназначена для контроля сетевого трафика путем пересылки копий входящих и/или исходящих пакетов с одного или нескольких контролируемых портов на один контролирующий порт.

К контролирующему порту применяются следующие ограничения:

- Порт не может быть контролирующим и контролируемым портом одновременно;
- Порт не может быть членом группы портов;
- IP-интерфейс должен отсутствовать для этого порта;
- Протокол GVRP должен быть выключен на этом порту.

К контролируемым портам применяются следующие ограничения:

- Порт не может быть контролирующим и контролируемым портом одновременно;
- Существует ограничение на 7 сессий зеркалирования: по 8 зеркалируемых интерфейсов (портов или VLAN) в каждой.



Зеркалирование VLAN возможно только в первой сессии

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console (config) #
```

Таблица 206 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|---|
| monitor session <i>session_id</i> destination interface gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> [network] | <i>session_id</i> : (1..7); <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32) | Указывает зеркалирующий порт для выбранной сессии мониторинга. - network – позволяет вести обмен данными. |
| no monitor session <i>session_id</i> destination | | Выключает функцию мониторинга на настраиваемом интерфейсе. |

| | | |
|--|--|---|
| monitor session <i>session_id</i> destination remote vlan <i>vlan_id reflector-port</i> gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port network</i> | vlan_id: (1..4094); session_id: (1..7); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Указывается служебный vlan для зеркалирования трафика с заданного рефлектор-порта для выбранной сессии. - remote vlan – служебный vlan для зеркалирования трафика; - reflector-port – физический порт для передачи зеркалируемого трафика, на этом интерфейсе не должен был прописан remote vlan. |
| no monitor session <i>session_id</i> destination | | Выключает функцию мониторинга на настраиваемом интерфейсе. |
| monitor session <i>session_id</i> source interface gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port [rx tx both]</i> | session_id: (1..7); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Добавляет указанный зеркалируемый порт для выбранной сессии мониторинга. - rx – копировать пакеты, принятые контролируемым портом; - tx – копировать пакеты, переданные контролируемым портом; - both – копировать все пакеты с контролируемого порта. |
| monitor session <i>session_id</i> source interface gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> | | Выключает функцию мониторинга на настраиваемом интерфейсе. |
| monitor session <i>session_id</i> source vlan <i>vlan_id</i> | vlan_id: (1..4094); session_id: (1..7) | Добавляет указанный зеркалируемый vlan для выбранной сессии мониторинга. |
| no monitor session <i>session_id</i> source vlan <i>vlan_id</i> | | Выключает функцию мониторинга на настраиваемом интерфейсе. |
| monitor session <i>session_id</i> source remote vlan <i>vlan_id</i> | vlan_id: (1..4094); session_id: (1..7) | Добавляет в качестве источника vlan с уже ранее зеркалируемым трафиком для выбранной сессии мониторинга. |
| no monitor session <i>session_id</i> source remote vlan <i>vlan_id</i> | | Выключает функцию мониторинга на настраиваемом интерфейсе. |

5.22 Функция sFlow

sFlow – технология, позволяющая осуществлять мониторинг трафика в пакетных сетях передачи данных путем частичной выборки трафика для последующей инкапсуляции в специальные сообщения, передаваемые на сервер сбора статистики.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config) #
```

Таблица 207 – Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|--|--|
| sflow receiver <i>id</i> { <i>ipv4_address</i> <i>ipv6_address</i> <i>ipv6z_address</i> <i>url</i> } [port <i>port</i>] [max-datagram-size <i>byte</i>] | <i>id</i> : (1..8); <i>port</i> : (1.. 65535)/6343; <i>byte</i> : положительное целое число/1400; формат <i>ipv4_address</i> : A.B.C.D; формат <i>ipv6_address</i> : X:X:X:X:X; формат <i>ipv6z_address</i> : X:X:X:X::X%<ID>; <i>url</i> : (1..158) символов | Задаёт адрес сервера сбора статистики sflow. - <i>id</i> – номер sflow-сервера; - <i>ipv4_address</i> , <i>ipv6_address</i> , <i>ipv6z_address</i> – IP-адрес; - <i>url</i> – доменное имя хоста; - <i>port</i> – номер порта; - <i>byte</i> – максимальное количество байт, которое может быть отправлено в один пакет данных. |
| no sflow receiver <i>id</i> | | Удаляет адрес сервера сбора статистики sflow. |
| sflow receiver { <i>sourceinterface</i> <i>sourceinterface-ipv6</i> } { tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel <i>group</i> loopback <i>loopback_id</i> vlan <i>vlan_id</i> oob } | <i>vlan_id</i> : (1..4094); <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32); <i>loopback_id</i> : (1..64) <i>group</i> : (1..128) | Задаёт интерфейс устройства, IP-адрес которого будет использоваться по умолчанию в качестве адреса источника сбора статистики. |
| no sflow receiver source-interface | | Удаляет явное задание интерфейса, с адреса которого будет отправляться статистика sflow. |

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

```
console# configure
console(config)# interface { tengigabitethernet te_port | }
console(config-if)#
```

Таблица 208 – Команды режима конфигурации интерфейса Ethernet

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---|---|
| sflow flow-sampling <i>rate id</i> [max-header-size <i>bytes</i>] | <i>rate</i> : (1024..107374823); <i>id</i> : (1..8); <i>bytes</i> : (20..256)/128 байт | Задаёт среднюю скорость выборки пакетов. Итоговая скорость выборки считается как 1/rate*current_speed (current_speed – текущая средняя скорость). - <i>rate</i> – средняя скорость выборки пакетов; - <i>id</i> – номер sflow-сервера; - <i>bytes</i> – максимальное количество байт, которое будет скопировано из образца пакета. |
| no sflow flow-sampling | | Отключает счетчики выборки на порту. |
| sflow counters-sampling <i>sec id</i> | <i>sec</i> : (15..86400) секунд; <i>id</i> : (0..8) | Определяет максимальный интервал между успешными выборками пакетов. - <i>sec</i> – максимальный интервал между выборками в секундах; - <i>id</i> – номер sflow-сервера (задается командой sflow receiver в глобальном режиме конфигурации). |
| no sflow counters-sampling | | Отключает счетчики выборки на порту. |

Команды режима EХЕС

Запрос командной строки в режиме EХЕС имеет следующий вид:

```
console>
```

Таблица 209 – Команды, доступные в режиме EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|--|--|
| show sflow configuration [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port] | | Выводит настройки sflow. |
| clear sflow statistics [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); tve_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Очищает статистику sFlow. Если интерфейс не указан, команда очищает все счетчики статистики sFlow. |
| show sflow statistics [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port] | | Отображает статистику sFlow. |

Примеры выполнения команд

- Установить IP-адрес 10.0.80.1 сервера 1 для сбора статистики sflow. Для ethernet-интерфейсов te1/0/1-te1/0/24 установить среднюю скорость выборки пакетов – 10240 кбит/с и максимальный интервал между успешными выборками пакетов – 240 с.

```
console# configure
console(config)# sflow receiver 1 10.0.80.1
console(config)# interface range tengigabitethernet 1/0/1-24
console(config-if-range)# sflow flowing-sample 1 10240
console (config-if)# sflow counters-sampling 240 1
```

5.23 Функции диагностики физического уровня

Сетевые коммутаторы содержат аппаратные и программные средства для диагностики физических интерфейсов и линий связи. В перечень тестируемых параметров входят следующие:

Для электрических интерфейсов:

- длина кабеля;
- расстояние до места неисправности – обрыва или замыкания.

Для оптических интерфейсов 1G и 10G:

- параметры питания – напряжение и ток;
- выходная оптическая мощность;
- оптическая мощность на приеме.


5.23.1 Диагностика медного кабеля

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 210 – Команды диагностики медного кабеля

| Команда | Значение/Значение по умолчанию | Действие |
|---|--------------------------------|---|
| test cable-diagnostics tdr [all interface gigabitethernet gi_port] | gi_port: (1..8/0/1..48) | Выполнить виртуальное тестирование кабеля для указанного интерфейса. - all — для всех интерфейсов. |
| show cable-diagnostics tdr [interface gigabitethernet gi_port] | gi_port: (1..8/0/1..48) | Отобразить результаты последнего виртуального тестирования кабеля для указанного интерфейса. |
| show cable-diagnostics cable-length [interface gigabitethernet gi_port] | gi_port: (1..8/0/1..48) | Отобразить предположительную длину кабеля, подключенного к указанному интерфейсу (если номер порта не задан, то команда выполняется для всех портов).  Интерфейс должен быть активным и работать в режиме 1000 Мбит/с или 100 Мбит/с. Диагностика подерживается только на интерфейсах GigabitEthernet. |

Пример выполнения команды

Протестировать порт gi 1/0/1:

```
console# test cable-diagnostics tdr interface gigabitethernet 1/0/1
```

```
5324#test cable-diagnostics tdr interface gi0/1
..
Cable on port gi1/0/1 is good
```

5.23.2 Диагностика оптического трансивера

Функция диагностики позволяет оценить текущее состояние оптического трансивера и оптической линии связи.

Возможен автоматический контроль состояния линий связи. Для этого коммутатор периодически опрашивает параметры оптических интерфейсов и сравнивает их с пороговыми значениями, заданными производителями трансиверов. При выходе параметров за допустимые пределы коммутатор формирует предупреждающие и аварийные сообщения.

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 211 – Команда диагностики оптического трансивера

| Команда | Значение/Значение по умолчанию | Действие |
|--|--|---|
| show fiber-ports optical-transceiver [interface gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port t] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Отображает результаты диагностики оптического трансивера. |

Пример выполнения команды:

```
sw1# show fiber-ports optical-transceiver interface
TengigabitEthernet1/0/5
```

| Port | Temp [C] | Voltage [Volt] | Current [mA] | Output Power [mW / dBm] | Input Power [mW / dBm] | LOS | Transceiver Type |
|---|----------|----------------|--------------|-------------------------|------------------------|-----|------------------|
| te1/0/5 | 33 | 3.28 | 11.45 | 0.28 / -5.52 | 0.24 / -6.11 | No | Fiber |
| Temp - Internally measured transceiver temperature Voltage - Internally measured supply voltage Current - Measured TX bias current Output Power - Measured TX output power in milliWatts/dBm Input Power - Measured RX received power in milliWatts/dBm LOS - Loss of signal N/A - Not Available, N/S - Not Supported, W - Warning, E - Error Transceiver information: Vendor name: OEM Serial number: S1C53253701833 Connector type: SC Type: SFP/SFP+ Compliance code: BaseBX10 Laser wavelength: 1550 nm Transfer distance: 20000 m Diagnostic: supported | | | | | | | |

Таблица 212 – Параметры диагностики оптического трансивера

| Параметр | Значение |
|--------------|--------------------------------------|
| Temp | Температура трансивера. |
| Voltage | Напряжение питания трансивера. |
| Current | Отклонение тока на передаче. |
| Output Power | Выходная мощность на передаче (мВт). |
| Input Power | Входная мощность на приеме (мВт). |
| LOS | Потеря сигнала. |

Значения результатов диагностики:

- N/A – недоступно;
- N/S – не поддерживается.

5.24 IP Service Level Agreements (IP SLA)

IP SLA (соглашения об уровне обслуживания в IP-сетях) — технология активного мониторинга, используемая для измерения параметров быстродействия компьютерных сетей и качества передачи данных. Активный мониторинг представляет собой продолжительную циклическую генерацию трафика, сбор информации о его прохождении по сети и ведение статистики.

На данный момент измерение параметров сети может осуществляться с использованием протокола ICMP.

При каждом выполнении операции ICMP Echo устройство отправляет *ICMP Echo request* сообщение на адрес назначения, ожидает получения сообщения *ICMP Echo reply* в течение заданного интервала времени.

С одной IP SLA операцией можно связать несколько объектов TRACK. Состояние объекта TRACK изменяется в момент изменения состояния IP SLA операции, либо с заданной задержкой.

При изменении состояния трека возможно выполнение макрокоманд. Макрокоманды выполняются в режиме глобального конфигурирования. Для выполнения команд режима privileged EXEC команды необходимо дополнить префиксом *do*. Команды создания набора макрокоманд приведены в таблице 36.

Для использования функции IP SLA необходимо выполнить следующие действия:

- Создать операцию *icmp-echo* и сконфигурировать её.
- Запустить выполнение операции.
- Создать TRACK-объект, связанный с конкретной IP SLA операцией и сконфигурировать его.
- При необходимости, создать макросы, выполняемые при изменении состояния объекта TRACK.
- Просмотреть статистику, при необходимости, очистить её.
- При необходимости, прекратить выполнение операции.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console (config) #
```

Таблица 213 — Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--|--|---|
| <i>ip sla operation</i> | operation: (1..64) | Переходит в режим конфигурирования IP SLA операции. - <i>operation</i> — номер операции. |
| <i>no ip sla operation</i> | | Удаляет IP SLA операцию. |
| <i>ip sla schedule operation life life start-time start-time</i> | operation: (1..64); life: (forever); start-time: (now) | Запускает на выполнение IP SLA операцию. - <i>operation</i> — номер операции. - <i>life</i> — время, в течение которого операция будет выполняться. - <i>start-time</i> — время запуска. |
| <i>no ip sla schedule operation</i> | | Прекращает выполнение IP SLA операции. - <i>operation</i> — номер операции. |
| <i>track object ip sla operation state</i> | object: (1..64); operation: (1..64) | Создает TRACK-объект, который будет отслеживать состояние IP SLA операции. - <i>object</i> — номер TRACK-объекта. - <i>operation</i> — номер IP SLA операции. |
| <i>no track object ip sla</i> | | Удаляет TRACK объект. - <i>object</i> — номер TRACK-объекта. |

Таблица 214 — Команды режима создания операций IP SLA

| Команда | Значение/Значение по умолчанию | Действие |
|---|---------------------------------------|---|
| icmp-echo {A.B.C.D / host } [source-ip A.B.C.D] | host: (1..158) символов | Переходит в режим конфигурирования ICMP ECHO операции. - A.B.C.D — IPv4-адрес узла сети; - host — доменное имя узла сети. |

Команды режима конфигурирования IP SLA ICMP ECHO операции

Вид запроса командной строки в режиме конфигурирования IP SLA ICMP ECHO:

```
console (config-ip-sla-icmp-echo) #
```

Таблица 215 — Команды режима конфигурирования операции ICMP Echo

| Команда | Значение/Значение по умолчанию | Действие |
|--------------------------------|---------------------------------------|---|
| frequency secs | secs: (10..500)/10 сек | Устанавливает частоту повторения ICMP ECHO операции. - secs — частота, в секундах. |
| no frequency | | Устанавливает значение частоты повторений по умолчанию. |
| timeout msec | msecs: (50..5000)/2000 мс | Устанавливает длину таймаута, по истечении которого, если не пришел ICMP-ответ, операция будет считаться неудачной. - msec — таймаут, в миллисекундах. |
| no timeout | | Устанавливает значение таймаута по умолчанию. |
| request-data-size bytes | bytes: (28..1472)/28 байт | Установить количество байт, передаваемых в ICMP-пакете в качестве данных (payload). - bytes — количество байт. |
| no request-data-size | | Установить значение количества байт по умолчанию. |



Для нормального выполнения операции ICMP Echo рекомендуется устанавливать значение частоты выполнения операции большим, чем значение таймаута операции.

Команды режима конфигурирования трека

Вид запроса командной строки режима конфигурирования трека:

```
console (config-track) #
```

Таблица 216 — Команды режима конфигурации трека

| Команда | Значение/Значение по умолчанию | Действие |
|--|--------------------------------|--|
| <code>delay {up secs down secs up secs down secs}</code> | <code>secs: (1..180)/0</code> | Устанавливает задержку для смены состояния TRACK-объекта, при изменении состояния IP SLA операции. - <code>secs</code> — задержка, в секундах. - <code>up</code> — задержка изменения состояния, при изменении операции в состояние OK; - <code>down</code> — задержка изменения состояния, при изменении операции в состояние Error. |
| <code>delay {up secs down secs up secs down secs}</code> | | Удаляет задержку. |

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 217 — Команды режима privileged EXEC

| Команда | Значение | Действие |
|--|---------------------------------|---|
| <code>show ip sla operation [operation]</code> | <code>operation: (1..64)</code> | Отображает информацию о настроенных IP SLA операциях. - <code>operation</code> — номер операции. |
| <code>show track [object]</code> | <code>object: (1..64)</code> | Отображает информацию о настроенных TRACK-объектах. - <code>object</code> — номер объекта. |
| <code>clear ip sla counters [operation]</code> | <code>operation: (1..64)</code> | Обнуляет счетчики IP SLA операции. - <code>operation</code> — номер операции. |

Пример настройки, предназначенной для контроля узла сети с адресом 10.9.2.65 с отправкой ICMP-запроса каждые 20 секунд, временем ответа на ICMP-запрос не превышающим 500 мс и размером данных 92 байта; задержка смены состояния TRACK-объекта — 3 секунды; при изменении состояния TRACK-объекта выполняются макросы TEST_DOWN и TEST_UP:

```
console# configure
console(config)# interface vlan 1
console(config-if)# ip address 10.9.2.80 255.255.255.192
console(config-if)# exit
console(config)# macro name TEST_DOWN track 1 state down
Enter macro commands one per line. End with the character '@'.
int gil/0/11
no shutdown
@
console(config)#
console(config)# macro name TEST_UP track 1 state up
Enter macro commands one per line. End with the character '@'.
int gil/0/11
shutdown
@
console(config)#
console(config)# ip sla 1
console(config-ip-sla)# icmp-echo 10.9.2.65
console(config-ip-sla-icmp-echo)# timeout 500
console(config-ip-sla-icmp-echo)# frequency 20
console(config-ip-sla-icmp-echo)# request-data-size 92
console(config-ip-sla-icmp-echo)# exit
console(config-ip-sla)# exit
console(config)# ip sla schedule 1 life forever start-time now
console(config)# track 1 ip sla 1 state
```

```
console(config-track)# delay up 3 down 3
console(config-track)# exit
console(config)# exit
console#
```

Пример вывода статистики для операции ICMP Echo:

```
IP SLA Operational Number: 1
Type of operation: icmp-echo
Target address: 10.9.2.65
Source Address: 10.9.2.80
Request size (ICMP data portion): 92
Operation frequency: 20
Operation timeout: 500
Operation state: scheduled
Operation return code: OK
Operation Success counter: 254
Operation Failure counter: 38
ICMP Echo Request counter: 292
ICMP Echo Reply counter: 254
ICMP Error counter: 0
```

где

- *Operation state* — текущее состояние операции:
 - *scheduled* — операция выполняется;
 - *pending* — выполнение операции остановлено.
- *Operation return code* — код завершения последней выполненной операции:
 - *OK* — успешное завершение предыдущей операции;
 - *Error* — неудачное завершение последней попытки измерения.
- *Operation Success counter* — количество успешно законченных операций.
- *Operation Failure counter* — количество неудачно законченных операций.
- *ICMP Echo Request counter* — количество проведённых запусков операции.
- *ICMP Echo Reply counter* — количество полученных ответов на ICMP-запрос.

ICMP Error counter — счётчик, отображающий количество измерительных операций, закончившихся с соответствующим кодом ошибки.

5.24 Функции обеспечения безопасности

5.24.1 Функции обеспечения защиты портов

С целью повышения безопасности в коммутаторе существует возможность настроить какой-либо порт так, чтобы доступ к коммутатору через этот порт предоставлялся только заданным устройствам. Функция защиты портов основана на определении MAC-адресов, которым разрешается доступ. MAC-адреса могут быть настроены вручную или изучены коммутатором. После изучения необходимых адресов порт следует заблокировать, защитив его от поступления пакетов с неизученными MAC-адресами. Таким образом, когда заблокированный порт получает пакет, и MAC-адрес источника пакета не связан с этим портом, активизируется механизм защиты, в зависимости от которого могут быть приняты следующие меры: несанкционированные пакеты, поступающие на заблокированный порт, пересылаются, отбрасываются, либо же порт, принявший пакет, отключается. Функция безопасности Locked Port позволяет сохранить список изученных MAC-адресов в файле конфигурации, таким образом, этот список можно восстановить после перезагрузки устройства.



Существует ограничение на количество MAC-адресов, которое может изучить порт, использующий функцию защиты.

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet, интерфейса группы портов:

```
console (config-if) #
```

Таблица 218 – Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|--|--|
| port security | -/выключено | Включает функцию защиты на интерфейсе. Блокирует функцию изучения новых адресов для интерфейса. Пакеты с неизученными MAC-адресами источника отбрасываются. Команда аналогична команде port security discard . |
| no port security | | Отключает функцию защиты на интерфейсе. |
| port security max num | num: (0..32768)/1 | Задаёт максимальное количество адресов, которое может изучить порт. |
| no port security max | | Устанавливает значение по умолчанию. |
| port security routed secure-address mac_address | Формат MAC-адреса: H.H.H, H:H:H:H:H:H, H-H-H-H-H-H | Устанавливает защищённый MAC-адрес. |
| no port security routed secure-address mac_address | | Удаляет защищённый MAC-адрес. |
| port security {forward discard discard-shutdown} [trap freq] | freq: (1..1000000) сек | Включает функцию защиты на интерфейсе. Блокирует функцию изучения новых адресов для интерфейса. - forward – пакеты с неизученными MAC-адресами источника пересылаются; - discard – пакеты с неизученными MAC-адресами источника отбрасываются; - discard-shutdown – пакеты с неизученными MAC-адресами источника отбрасываются, порт отключается; - freq – частота генерируемых сообщений протокола SNMP trap при поступлении несанкционированных пакетов. |
| port security trap freq | freq: (1..1000000) сек | Задаёт частоту генерируемых сообщений протокола SNMP trap при поступлении несанкционированных пакетов. |
| port security mode {secure {permanent delete-on-reset} max-addresses lock} | -/lock | Задаёт режим ограничения изучения MAC-адресов для настраиваемого интерфейса. - secure – настраивает статическое ограничение изучения MAC-адресов на порту; - permanent – данный MAC-адрес сохранится в таблице даже после перезагрузки устройства; - delete-on-reset – данный адрес удалится после перезагрузки устройства; - max-addresses – удаляет текущие динамически изученные адреса, связанные с интерфейсом. Разрешено изучение максимального количества адресов на порту. Повторное изучение и старение разрешены; - lock – сохраняет в конфигурацию текущие динамически изученные адреса, связанные с интерфейсом и запрещает обучение новым адресам и старение уже изученных адресов. |
| no port security mode | | Устанавливает значение по умолчанию. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 219 – Команды режима EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|--|--|
| show ports security { gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group detailed } | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Показывает настройки функции безопасности на выбранном интерфейсе. |
| show ports security addresses { gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group detailed } | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Показывает текущие динамические адреса для заблокированных портов. |
| set interface active { gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group } | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Активирует интерфейс, отключенный функцией защиты порта (команда доступна только для привилегированного пользователя). |

Примеры выполнения команд

- Включить функцию защиты на 15 интерфейсе Ethernet. Установить ограничение на изучение адресов – 1 адрес. После изучения MAC-адреса заблокировать функцию изучения новых адресов для интерфейса с целью отбросить пакеты с неизученными MAC-адресами источника. Сохранить в файл изученный адрес.

```
console# configure
console(config)# interface tengigabitethernet 1/0/15
console(config-if)# port security mode secure permanent
console(config-if)# port security max 1
console(config-if)# port security
```

- Подключить клиента к порту и изучить MAC-адрес.

```
console(config-if)# port security discard
console(config-if)# port security mode lock
```

5.24.2 Проверка подлинности клиента на основе порта (стандарт 802.1x)

5.24.2.1 Базовая проверка подлинности


Аутентификация на основе стандарта 802.1x обеспечивает проверку подлинности пользователей коммутатора через внешний сервер на основе порта, к которому подключен клиент. Только аутентифицированные и авторизованные пользователи смогут передавать и принимать данные. Проверка подлинности пользователей портов выполняется сервером RADIUS посредством протокола EAP (Extensible Authentication Protocol).

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console (config) #
```

Таблица 220 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|---|--------------------------------|---|
| dot1x system-auth-control | -/выключено | Включает режим аутентификации 802.1X на коммутаторе. |
| no dot1x system-auth-control | | Выключает режим аутентификации 802.1X на коммутаторе. |
| aaa authentication dot1x default {none radius} [none radius] | -/radius | <p>Задаёт один или два метода проверки подлинности, авторизации и учёта (AAA), для использования на интерфейсах IEEE 802.1X.</p> <ul style="list-style-type: none"> - none – не выполнять аутентификацию; - radius – использовать список RADIUS-серверов для аутентификации пользователя. <p> Второй метод аутентификации используется только в случае, если по первому аутентификация была неуспешной.</p> |
| no aaa authentication dot1x default | | Устанавливает значение по умолчанию. |

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

```
console (config-if) #
```



Протокол EAP (Extensible Authentication Protocol) выполняет задачи для аутентификации удаленного клиента, при этом определяя механизм аутентификации.

Таблица 221 – Команды режима конфигурации интерфейса Ethernet

| Команда | Значение/Значение по умолчанию | Действие |
|--|--|---|
| dot1x port-control {auto force-authorized force-unauthorized} [time-range time] | -/force-authorized; time: (1..32) | <p>Настраивает аутентификацию 802.1X на интерфейсе. Разрешает ручной контроль за состоянием авторизации порта.</p> <ul style="list-style-type: none"> - auto – использовать 802.1X для изменения состояния клиента между авторизованным и неавторизованным; - force-authorized – выключает аутентификацию 802.1X на интерфейсе. Порт переходит в авторизованное состояние без аутентификации; - force-unauthorized – переводит порт в неавторизованное состояние. Игнорируются все попытки аутентификации клиента, коммутатор не предоставляет сервис аутентификации для этого порта; - time – интервал времени. Если данный параметр не определен, то порт не авторизован. |
| no dot1x port-control | | Устанавливает значение по умолчанию. |
| dot1x reauthentication | -/периодические повторные проверки подлинности выключены | Включает периодические повторные проверки подлинности (переаутентификацию) клиента. |
| no dot1x reauthentication | | Выключает периодические повторные проверки подлинности (переаутентификацию) клиента. |

| | | |
|--|---|---|
| dot1x timeout eap-timeout <i>period</i> | period: (1..65535) /30 | Задает интервал времени в секундах, в течение которого сервер EAP ожидает ответа от клиента EAP до повторной передачи запроса. |
| no dot1x timeout eap-timeout | | Установить значение по умолчанию. |
| dot1x timeout supplicant-held-period <i>period</i> | period: (1..65535) /60 | Задает период времени, в течение которого запрашивающий ждет до перезапуска аутентификации после получения ответа FAIL от сервера Radius. |
| no dot1x timeout supplicant-held-period | | Установить значение по умолчанию. |
| dot1x timeout reauth-period <i>period</i> | period: (300..4294967295)/ 3600 сек | Устанавливает период между повторными проверками подлинности. |
| no dot1x timeout reauth-period | | Устанавливает значение по умолчанию. |
| dot1x timeout quiet-period <i>period</i> | period: (10..65535)/60 сек | Устанавливает период, в течение которого коммутатор остается в состоянии молчания после неудачной проверки подлинности. В течение периода молчания коммутатор не принимает и не инициирует никаких аутентификационных сообщений. |
| no dot1x timeout quiet-period | | Устанавливает значение по умолчанию |
| dot1x timeout tx-period <i>period</i> | period: (30..65535)/30 сек | Устанавливает период, в течение которого коммутатор ожидает ответ на запрос либо идентификацию по протоколу EAP от клиента, перед повторной отправкой запроса. |
| no dot1x timeout tx-period | | Устанавливает значение по умолчанию. |
| dot1x max-req <i>count</i> | count: (1..10)/2 | Устанавливает максимальное число попыток передачи запросов протокола EAP-клиенту перед новым запуском процесса проверки подлинности. |
| no dot1x max-req | | Устанавливает значение по умолчанию. |
| dot1x timeout supp-timeout <i>period</i> | period: (1..65535)/30 секунд | Устанавливает период между повторными передачами запросов протокола EAP-клиенту. |
| no dot1x timeout supp-timeout | | Устанавливает значение по умолчанию. |
| dot1x timeout server-timeout <i>period</i> | period: (1..65535)/30 секунд | Устанавливает период, в течение которого коммутатор ожидает ответа от сервера аутентификации. |
| no dot1x timeout server-timeout | | Устанавливает значение по умолчанию. |
| dot1x timeout silence-period <i>period</i> | period: (60..65535) сек/не задано | Устанавливает период времени неактивности клиента, по истечении которого клиент становится неавторизованным. |
| no dot1x timeout silence-period | | Устанавливает значение по умолчанию |

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 222 – Команды режима Privileged EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|---|--|--|
| dot1x re-authenticate [gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> oob] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Вручную осуществляет повторную проверку подлинности указанного порта в команде, либо всех портов, поддерживающих 802.1X. |

| | | |
|--|--|--|
| dot1x unlock client gigabitethernet gi_port tengigabitethernet te_port <i>mac_address</i> | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Заблокировать клиента с указанным MAC-адресом на порту при достижении порога максимально возможных попыток аутентификации. |
| show dot1x interface { gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port oob} | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Показывает состояние 802.1X для коммутатора либо для указанного интерфейса. |
| show dot1x users [username <i>username]</i> | username: (1..160) символов | Показывает активных аутентифицированных пользователей 802.1X коммутатора. |
| show dot1x statistics interface { gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port oob} | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Показывает статистику по 802.1X для выбранного интерфейса. |

Примеры выполнения команд

- Включить режим аутентификации 802.1x на коммутаторе. Использовать RADIUS-сервер для проверки подлинности клиентов на интерфейсах IEEE 802.1X. Для 8 интерфейса Ethernet использовать режим аутентификации 802.1x.

```
console# configure
console(config)# dot1x system-auth-control
console(config)# aaa authentication dot1x default radius
console(config)# interface tengigabitethernet 1/0/8
console(config-if)# dot1x port-control auto
```

- Показать состояние 802.1x для коммутатора, для 8 интерфейса Ethernet.

```
console# show dot1x interface tengigabitethernet 1/0/8
```

```
Authentication is enabled
Authenticating Servers: Radius
Unauthenticated VLANs:
Authentication failure traps are disabled
Authentication success traps are disabled
Authentication quiet traps are disabled

te1/0/8
Host mode: multi-host
Port Administrated Status: auto
Guest VLAN: disabled
Open access: disabled
Server timeout: 30 sec
Port Operational Status: unauthorized*
* Port is down or not present
Reauthentication is disabled
Reauthentication period: 3600 sec
Silence period: 0 sec
Quiet period: 60 sec
Interfaces 802.1X-Based Parameters
Tx period: 30 sec
Supplicant timeout: 30 sec
Max req: 2
Authentication success: 0
Authentication fails: 0
```

Таблица 223 – Описание результатов выполнения команд

| <i>Параметр</i> | <i>Описание</i> |
|-------------------------------|--|
| <i>Port</i> | Номер порта. |
| <i>Admin mode</i> | Режим аутентификации 802.1X: Force-auth, Force-unauth, Auto. |
| <i>Oper mode</i> | Операционный режим порта: авторизованный, неавторизованный, либо выключенный (Authorized, Unauthorized, Down). |
| <i>Reauth Control</i> | Контроль переаутентификации. |
| <i>Reauth Period</i> | Период между повторными проверками подлинности. |
| <i>Username</i> | Имя пользователя при использовании 802.1X. Если порт авторизован, то отображается имя текущего пользователя. Если порт не авторизован, то отображается имя последнего успешно авторизованного пользователя на порту. |
| <i>Quiet period</i> | Период, в течение которого коммутатор остается в состоянии молчания после неудачной проверки подлинности. |
| <i>Tx period</i> | Период, в течение которого коммутатор ожидает ответ на запрос либо идентификацию по протоколу EAP от клиента, перед повторной отправкой запроса. |
| <i>Max req</i> | Максимальное число попыток передачи запросов протокола EAP клиенту перед новым запуском процесса проверки подлинности. |
| <i>Supplicant timeout</i> | Период между повторными передачами запросов протокола EAP клиенту. |
| <i>Server timeout</i> | Период, в течение которого коммутатор ожидает ответа от сервера аутентификации. |
| <i>Session Time</i> | Время подключения пользователя к устройству. |
| <i>Mac address</i> | MAC-адрес пользователя. |
| <i>Authentication Method</i> | Метод аутентификации установленной сессии. |
| <i>Termination Cause</i> | Причина закрытия сессии. |
| <i>State</i> | Текущее значение автомата состояний определителя подлинности и выходного автомата состояний. |
| <i>Authentication success</i> | Количество полученных сообщений об успешной аутентификации от сервера. |
| <i>Authentication fails</i> | Количество полученных сообщений о неуспешной аутентификации от сервера. |
| <i>VLAN</i> | Группа VLAN назначенная пользователю. |
| <i>Filter ID</i> | Идентификатор группы фильтрации. |

- Показать статистику по 802.1x для интерфейса Ethernet 8.

```
console# show dot1x statistics interface tengigabitethernet 1/0/8
```

```
EapolFramesRx: 12
EapolFramesTx: 8
EapolStartFramesRx: 1
EapolLogoffFramesRx: 1
EapolRespIdFramesRx: 4
EapolRespFramesRx: 6
EapolReqIdFramesTx: 3
EapolReqFramesTx: 5
InvalidEapolFramesRx: 0
EapLengthErrorFramesRx: 0
LastEapolFrameVersion: 1
LastEapolFrameSource: 00:00:02:56:54:38
```

Таблица 224 – Описание результатов выполнения команд

| <i>Параметр</i> | <i>Описание</i> |
|-------------------------------|---|
| <i>EapolFramesRx</i> | Количество корректных пакетов любого типа протокола EAPOL (Extensible Authentication Protocol over LAN), принятых данным определителем подлинности. |
| <i>EapolFramesTx</i> | Количество корректных пакетов любого типа протокола EAPOL, переданных данным определителем подлинности. |
| <i>EapolStartFramesRx</i> | Количество пакетов Start протокола EAPOL, принятых данным определителем подлинности. |
| <i>EapolLogoffFramesRx</i> | Количество пакетов Logoff протокола EAPOL, принятых данным определителем подлинности. |
| <i>EapolRespIdFramesRx</i> | Количество пакетов Resp/Id протокола EAPOL, принятых данным определителем подлинности. |
| <i>EapolRespFramesRx</i> | Количество пакетов ответов (кроме Resp/Id) протокола EAPOL, принятых данным определителем подлинности. |
| <i>EapolReqIdFramesTx</i> | Количество пакетов Resp/Id протокола EAPOL, переданных данным определителем подлинности. |
| <i>EapolReqFramesTx</i> | Количество пакетов запросов (кроме Resp/Id) протокола EAPOL, переданных данным определителем подлинности. |
| <i>InvalidEapolFramesRx</i> | Количество пакетов протокола EAPOL с нераспознанным типом, принятых данным определителем подлинности. |
| <i>EapLengthErrorFramesRx</i> | Количество пакетов протокола EAPOL с некорректной длиной, принятых данным определителем подлинности. |
| <i>LastEapolFrameVersion</i> | Версия протокола EAPOL, принятая в самом последнем на данный момент пакете. |
| <i>LastEapolFrameSource</i> | MAC-адрес источника, принятый в самом последнем на данный момент пакете. |

5.24.2.2 Расширенная проверка подлинности

Расширенные настройки dot1x позволяют проводить проверку подлинности для нескольких клиентов, подключенных к порту. Существует два варианта аутентификации: первый, когда проверка подлинности на основе порта требует аутентификации только одного клиента, чтобы доступ к системе имели все клиенты (режим Multiple hosts), второй, когда проверка подлинности требует аутентификации всех подключенных к порту клиентов (режим Multiple sessions). Если порт в режиме Multiple hosts не проходит аутентификацию, то всем подключенным хостам будет отказано в доступе к ресурсам сети.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 225 – Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---------------------------------------|--|
| dot1x traps authentication success [802.1x mac web] | -/выключено | Разрешает отправку trap-сообщений, когда клиент успешно проходит аутентификацию. |
| no dot1x traps authentication success | | Устанавливает значение по умолчанию. |
| dot1x traps authentication failure [802.1x mac web] | -/выключено | Разрешает отправку trap-сообщений, когда клиент не прошел аутентификацию. |
| no dot1x traps authentication failure | | Устанавливает значение по умолчанию. |

| | | |
|--|-------------|--|
| dot1x traps authentication quiet | -/выключено | Включает отправку trap-сообщений при превышении пользователем максимально допустимого количества безуспешных попыток аутентификации. |
| no dot1x traps authentication quiet | | Устанавливает значение по умолчанию. |

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

```
console (config-if) #
```

Таблица 226 – Команды режима конфигурации интерфейса Ethernet

| Команда | Значение/Значение по умолчанию | Действие |
|---|--|--|
| dot1x host-mode {multi-host single-host multi-sessions} | -/multi-host | Разрешает наличие одного/нескольких клиентов на авторизованном порту 802.1X. - multi-host – несколько клиентов; - single-host – один клиент; - multi-sessions – несколько сессий. |
| dot1x violation-mode {restrict protect shutdown} [trap freq] | -/protect; freq: (1..1000000)/1 сек | Задает действие, которое необходимо выполнить, когда устройство, MAC-адрес которого отличается от MAC-адреса клиента, осуществляет попытку доступа к интерфейсу. - restrict – пакеты с MAC-адресом, отличным от MAC-адреса клиента, пересылаются, при этом адрес источника не изучается; - protect – пакеты с MAC-адресом, отличным от MAC-адреса клиента, отбрасываются; - shutdown – порт выключается, пакеты с MAC-адресом, отличным от MAC-адреса клиента, отбрасываются; - freq – частота генерируемых сообщений протокола SNMP trap при поступлении несанкционированных пакетов.  Команда игнорируется в режиме Multiple hosts. |
| no dot1x single-host-violation | | Устанавливает значение по умолчанию. |
| dot1x authentication [mac 802.1x web] | -/выключена | Включает аутентификацию - mac – включает аутентификацию, основанную на MAC-адресах; - 802.1x – включает аутентификацию, основанную на 802.1x; - web -включает механизм Web-based аутентификации.  - Не должно быть статических привязок MAC-адресов. - Функция повторной аутентификации должна быть включена. |
| no dot1x authentication | | Выключает аутентификацию, основанную на MAC-адресах пользователей. |
| dot1x max-hosts hosts | hosts: (1..4294967295) | Задает максимальное количество хостов, прошедших аутентификацию. |
| no dot1x max-hosts | | Возвращает значение по умолчанию. |
| dot1x max-login-attempts num | num: (0, 3..10)/0 | Задает количество неудачных попыток ввода логина, после которых клиент блокируется. - 0 – бесконечное число попыток. |
| no dot1x max-login-attempts | | Возвращает значение по умолчанию. |
| dot1x guest-vlan enable | -/выключена | Включает функцию гостевой VLAN на текущем интерфейсе. |
| no dot1x guest-vlan enable | | Выключает функцию гостевой VLAN на текущем интерфейсе. |

Команды режима конфигурации интерфейса VLAN

Вид запроса командной строки в режиме конфигурации интерфейса VLAN:

```
console# configure  
console (config)# interface vlan vlan id
```

Таблица 227 – Команды режима конфигурации интерфейса VLAN

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|----------------------------|--|---|
| dot1x guest-vlan | по умолчанию VLAN не определена как гостевая | Определить гостевую VLAN. Открывает неавторизованным пользователям интерфейса доступ к гостевой VLAN. Если гостевая VLAN определена и разрешена, порт будет автоматически присоединяться к ней, когда не авторизован, и покидать, когда пройдет авторизацию. Чтобы использовать данный функционал, порт не должен быть статическим членом гостевой VLAN. |
| no dot1x guest-vlan | | Установить значение по умолчанию. |

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 228 — Команды режима Privileged EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|--|---|
| show dot1x interface { gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port oob} | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Настройки протокола 802.1x на интерфейсе (команда доступна только для привилегированного пользователя). |
| show dot1x detailed | - | Показывает расширенные настройки протокола 802.1x. |
| show dot1x credentials | - | Структура учета данных отображает параметры авторизованных клиентов. |
| show dot1x users [username] | username: строка | Показывает авторизованных клиентов. |
| show dot1x locked clients | - | Показывает неавторизованных клиентов, заблокированных по тайм-ауту. |
| show dot1x statistics interface {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port oob} | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Показывает статистику 802.1X на интерфейсах. |

5.24.3 Настройка функции MAC Address Notification

Функция MAC Address Notification позволяет отслеживать появление и исчезновение активного оборудования на сети путем сохранения истории изучения MAC-адресов. При обнаружении изменений в составе изученных MAC-адресов коммутатор сохраняет информацию в таблице и извещает об этом с помощью сообщений протокола SNMP. Функция имеет настраиваемые параметры — глубина истории о событиях и минимальный интервал отправки сообщений. Сервис MAC Address Notification отключен по умолчанию и может быть настроен выборочно для отдельных портов коммутатора.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 229 – Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---------------------------------------|--|
| mac address-table notification change | -/выключена | Команда предназначена для глобального управления функцией MAC notification. Команда разрешает регистрацию событий добавления и удаления MAC-адресов в/из таблиц коммутатора и отправку уведомления о событиях. Для работы функции необходимо дополнительно разрешать генерацию уведомлений на интерфейсах (см. ниже). |
| no mac address-table notification change | | Выключить функцию MAC notification глобально и отменить соответствующие настройки на всех интерфейсах. |
| mac address-table notification flapping | -/выключена | Включить функцию обнаружения флаппинга MAC-адресов. |
| no mac address-table notification flapping | | Выключить функцию обнаружения флаппинга MAC-адресов. |
| mac address-table notification change interval value | value: (0..4294967295)/1 | Максимальный промежуток времени между отправками SNMP-уведомлений. Если значение интервала времени равно 0, то генерация уведомлений и сохранение событий в историю будет осуществляться немедленно по мере возникновения событий об изменении состояния таблицы MAC-адресов. Если значение интервала времени больше 0, то устройство будет накапливать события об изменении состояния таблицы MAC-адресов в течение этого времени, а затем отправлять уведомления протокола SNMP и сохранять события в истории. |
| no mac address-table notification change interval | | Установить значение по умолчанию. |
| mac address-table notification change history value | value: (0..500)/1 | Задать максимальное количество событий об изменении состояния таблицы MAC-адресов, которое сохраняется в истории. Если установлен размер истории равный 0, то события не сохраняются. При переполнении буфера истории новое событие помещается на место самого старого. |
| no mac address-table notification change history | | Установить значение по умолчанию. |
| snmp-server enable traps mac-notification change | -/выключена | Включить отправку SNMP-уведомлений об изменении состояния таблицы MAC-адресов. Для отключения используется отрицательная форма команды. Если отправка уведомлений включена, то устройство будет информировать о событиях сообщениями протокола SNMP и сохранять соответствующие события в истории. Если отправка SNMP-уведомлений выключена, то устройство будет только сохранять события в истории. |
| no snmp-server enable traps mac-notification change | | Отключить отправку SNMP-уведомлений об изменении состояния таблицы MAC-адресов. |
| snmp-server enable traps mac-notification flapping | -/выключена | Включить отправку трапов о флаппинге MAC-адресов. |
| no snmp-server enable traps mac-notification flapping | | Отключить отправку трапов о флаппинге MAC-адресов. |

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки:

```
console(config-if) #
```

Таблица 230 – Команды режима конфигурации интерфейса Ethernet

| Команда | Значение/Значение по умолчанию | Действие |
|--|--------------------------------|--|
| snmp trap mac-notification change [added removed] | -/выключена | Включить генерацию уведомлений на интерфейсе о событиях изменения состояния MAC-адресов. Отдельно можно разрешить генерацию уведомлений только об изучении MAC-адресов либо только об их удалении. |
| no snmp trap mac-notification change | | Отключить генерацию уведомлений на интерфейсе. |

Команды режима privileged EXEC

Вид запроса командной строки:

```
console#
```

Таблица 231 – Команды режима конфигурации интерфейса Ethernet

| Команда | Значение/Значение по умолчанию | Действие |
|---|--|--|
| show mac address-table notification change history [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigaethernet twe_port hundredgigabitethernet hu_port port-channel group vlan vlan_id] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) group: (1..128); vlan_id: (1..4094) | Отобразить все уведомления об изменении состояния MAC-адресов, сохраненных в истории. |
| show mac address-table notification change statistics | - | Отобразить статистику сервиса: общее количество событий об изучении MAC-адресов, общее количество событий об удалении MAC-адресов, общее количество отправленных SNMP-сообщений. |

Пример использования команд

- В примере показано, как настроить передачу сообщений SNMP MAC Notification на сервер с адресом 172.16.1.5. При настройке задается общее разрешение работы сервиса, настраивается минимальный интервал отправки сообщений, задается размер истории событий и настраивается сервис на выбранном порту.

```
console(config)# snmp-server host 172.16.1.5 traps private
console(config)# snmp-server enable traps mac-notification change
console(config)# mac address-table notification change
console(config)# mac address-table notification change interval 60
console(config)# mac address-table notification change history 100
console(config)# interface gigabitethernet 0/7
console(config-if)# snmp trap mac-notification change
console(config-if)# exit
console(config)#
```

5.24.4 Контроль протокола DHCP и опция 82

DHCP (Dynamic Host Configuration Protocol) – сетевой протокол, позволяющий клиенту по запросу получать IP-адрес и другие требуемые параметры, необходимые для работы в сети TCP/IP.

Протокол DHCP может использоваться злоумышленниками для совершения атак на устройство, как со стороны клиента, заставляя DHCP-сервер выдать все доступные адреса, так и со стороны сервера путем его подмены. Программное обеспечение коммутатора позволяет обеспечить защиту устройства от атак с использованием протокола DHCP, для чего применяется функция контроля протокола DHCP – DHCP snooping.

Устройство способно отслеживать появление DHCP-серверов в сети, разрешая их использование только на «доверенных» интерфейсах, а также контролировать доступ клиентов к DHCP-серверам по таблице соответствий.

Опция 82 протокола DHCP (option 82) используется для того, чтобы проинформировать DHCP-сервер о том, от какого DHCP-ретранслятора (Relay Agent) и через какой его порт был получен запрос. Применяется для установления соответствий IP-адресов и портов коммутатора, а также для защиты от атак с использованием протокола DHCP. Опция 82 представляет собой дополнительную информацию (имя устройства, номер порта), добавляемую коммутатором, который работает в режиме DHCP relay агента (без добавления IP-адреса на клиентский интерфейс) или функции DHCP Snooping (при условии включения команды ip dhcp information option). На основании данной опции, DHCP-сервер выделяет IP-адрес (диапазон IP-адресов) и другие параметры порту коммутатора. Получив необходимые данные от сервера, DHCP Relay агент выделяет IP-адрес клиенту, а также передает ему другие необходимые параметры.

Таблица 232 – Формат полей опции 82

| <i>Поле</i> | <i>Передаваемая информация</i> |
|-----------------|---|
| Circuit ID | Имя хоста устройства. Строка вида eth <stacked/slotid/interfaceid>:<vlan> Последний байт – номер порта, к которому подключено устройство, отправляющее dhcp-запрос. |
| Remote agent ID | Enterprise number – 0089c1 MAC-адрес устройства. |



Для использования опции 82 на устройстве должна быть включена функция DHCP relay агента (без добавления IP-адреса на клиентский интерфейс) или функция DHCP Snooping (при условии включения команды ip dhcp information option).



Для корректной работы функции DHCP Snooping все используемые DHCP-серверы должны быть подключены к «доверенным» портам коммутатора. Для добавления порта в список «доверенных» используется команда IP dhcp snooping trust в режиме конфигурации интерфейса. Для обеспечения безопасности все остальные порты коммутатора должны быть «недоверенными».

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console (config) #
```

Таблица 233 – Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|------------------|---------------------------------------|---|
| ip dhcp snooping | -/выключено | Включает контроль протокола DHCP путем ведения таблицы DHCP snooping и отправки клиентских широковещательных DHCP-запросов на «доверенные» порты. |

| | | |
|--|---|--|
| no ip dhcp snooping | | Выключает контроль протокола DHCP. |
| ip dhcp snooping vlan <i>vlan_id</i> | vlan_id: (1..4094)/выключено | Разрешает контроль протокола DHCP в пределах указанной VLAN. |
| no ip dhcp snooping vlan <i>vlan_id</i> | | Запрещает контроль протокола DHCP в пределах указанной VLAN. |
| ip dhcp snooping information option allowed-untrusted | По умолчанию прием DHCP-пакетов с опцией 82 от «ненадежных» портов запрещен | Разрешает принимать DHCP-пакеты с опцией 82 от «ненадежных» портов. |
| no ip dhcp snooping information option allowed-untrusted | | Запрещает принимать DHCP-пакеты с опцией 82 от «ненадежных» портов. |
| ip dhcp snooping verify | По умолчанию верификация включена | Включает верификацию MAC-адреса клиента и MAC-адреса источника, принятого в DHCP-пакете на «недоверенных» портах. |
| no ip dhcp snooping verify | | Выключает верификацию MAC-адреса клиента и MAC-адреса источника, принятого в DHCP-пакете на «недоверенных» портах. |
| ip dhcp snooping database | Резервный файл не используется | Разрешает использование резервного файла (базы) контроля протокола DHCP. |
| no ip dhcp snooping database | | Запрещает использование резервного файла (базы) контроля протокола DHCP. |
| ip dhcp information option | -/выключено | Разрешает устройству добавление опции 82 при работе протокола DHCP. |
| no ip dhcp information option | | Запрещает устройству добавление опции 82 при работе протокола DHCP. |
| ip dhcp information option format-type access-node-id node_id | node_id: (1..48) символов/system description | Устанавливает идентификатор Access Node ID опции 82. |
| no ip dhcp information option format-type access-node-id | | Устанавливает значение по умолчанию |

| | | |
|--|--|--|
| ip dhcp information option format-type circuit-id <i>format [delimiter delimiter]</i> | format: (sp, sv, pv, spv, bin,user-defined); delimiter: (.,;#)/пробел | Настраивает формат DHCP опции 82. Формат: - sp — номер слота и порта; - sv — номер слота и VLAN; - pv — номер порта и VLAN; - spv — номер слота, порта и VLAN; - bin — бинарный формат: VLAN, слот, порт; - user-defined — формат определяется пользователем. Возможно настроить шаблоны в ASCII и HEX. При определении используются следующие шаблоны: %h: hostname в ASCII; %p: короткое имя порта, например, gi1/0/1 в ASCII; %P: длинное имя порта, например, gigabitethernet 1/0/1 в ASCII; %t: тип порта (значение поля ifTable::ifType в шестнадцатеричном виде) в ASCII; %m: мак-адрес порта в формате H-H-H-H-H-H в ASCII; %M: мак-адрес системы в формате H-H-H-H-H-H в ASCII; %u: номер юнита в ASCII; %s: номер слота в ASCII; %n: номер порта (как на лицевой панели) в ASCII; %i: ifIndex порта в ASCII; %v: идентификатор VLAN в ASCII; %V: имя VLAN в ASCII; %c: мак-адрес клиента в формате H-H-H-H-H-H в ASCII; %a: IP адрес системы в формате A.B.C.D в ASCII. (%a10 – адрес с interface vlan 10); %%: одиночный символ % в ASCII. \$\$: одиночный символ \$ в ASCII \$t: тип порта (значение поля ifTable::ifType в шестнадцатеричном виде) в HEX; \$m: мак-адрес порта в формате H-H-H-H-H-H в HEX; \$M: мак-адрес системы в формате H-H-H-H-H-H в HEX; \$u: номер юнита в HEX; \$s: номер слота в HEX; \$n: номер порта (как на лицевой панели) в HEX; \$i: ifIndex порта в HEX; \$v: идентификатор VLAN в HEX; \$c: мак-адрес клиента в формате H-H-H-H-H-H в HEX; \$b[XY]: добавляются произвольные байты XY в HEX (\$b13) |
| no ip dhcp information option format-type circuit-id | | Запрещает устройству добавление опции 82 при работе протокола DHCP. |
| ip dhcp information option format-type remote-id <i>remote-id</i> | remote_id: (1..128)/mac address в hex | Устанавливает идентификатор Remote agentID опции 82. Для настройки возможно использовать шаблоны, определенные в circuit-id user-defined. |
| no ip dhcp information option format-type remote-id <i>remote-id</i> | | Устанавливает значение по умолчанию. |
| ip dhcp information option suboption-type | -/выключено | Добавляет в начало circuit id/remote id дополнительные 2 байта (Type и length). |
| no ip dhcp information option suboption-type | | Устанавливает значение по умолчанию. |

Таблица 234 – Формат полей опции 82 согласно рекомендациям TR-101

| Поле | Передаваемая информация |
|-----------------|--|
| Circuit ID | Имя хоста устройства. строка вида eth <stacked/slotid/interfaceid>: <vlan> Последний байт – номер порта, к которому подключено устройство, отправляющее запрос DHCP. |
| Remote agent ID | Enterprise number – 0089c1 MAC-адрес устройства. |

Таблица 235 – Формат полей опции 82 режима custom

| <i>Поле</i> | <i>Передаваемая информация</i> |
|-----------------|---|
| Circuit ID | Длина (1 байт) Тип Circuit ID Длина (1 байт) VLAN (2 байта) Номер модуля (1 байт) Номер порта (1 байт) |
| Remote agent ID | Длина (1 байт) Тип Remote ID (1 байт) Длина (1 байт) MAC-адрес коммутатора |

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов


Существует возможность включить добавление опции 82 для отдельных интерфейсов и портов. Приоритет применения команды от низкого уровня к высокому: глобальная настройка, настройка на интерфейсе, настройка на порту.

Формат опции 82 при этом определяется только в глобальном режиме.

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet, интерфейса группы портов:

```
console(config-if)#
```

Таблица 236 – Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---|--|
| ip dhcp snooping trust | По умолчанию интерфейс не является доверенным | Добавляет интерфейс в список «доверенных» при использовании контроля протокола DHCP. DHCP-трафик «доверенного» интерфейса считается безопасным и не контролируется. |
| no ip dhcp snooping trust | | Удаляет интерфейс из списка «доверенных» при использовании контроля протокола DHCP. |
| ip dhcp information option [global] | -/global | Разрешает добавление опции 82 на выбранном интерфейсе при работе протокола DHCP. global – глобальная настройка для применения опции 82.  Приоритет работы команды ip dhcp information optional – порт, interface vlan, глобальная конфигурация. |
| no ip dhcp information option | | Запрещает добавление опции 82 на выбранном интерфейсе при работе протокола DHCP. |
| ip source-guard | По умолчанию функция выключена | Включает функцию защиты IP-адреса клиента для настраиваемого интерфейса. - mac-check - добавляет проверку MAC-адреса источника для входящего трафика. |
| no ip source-guard | | Выключает функцию защиты IP-адреса клиента для настраиваемого интерфейса. |
| ip dhcp snooping limit clients value | value: (1..2048)/ не задан | Устанавливает предельное количество подключенных клиентов. |
| no ip dhcp snooping limit clients | | Устанавливает значение по умолчанию. |

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 237 – Команды режима Privileged EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|--|
| ip dhcp snooping binding <i>mac_address vlan_id</i> <i>ip_address {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group}</i> <i>expiry {seconds infinite}</i> | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128); seconds: (10..4294967295) сек | Добавляет в файл (базу) контроля протокола DHCP соответствие MAC-адреса клиента, группе VLAN и IP-адресу для указанного интерфейса. Данная запись будет действительна в течение указанного в команде времени жизни записи, если клиент не отправит запрос на DHCP-сервер на обновление. Таймер обнуляется в случае получения от клиента запроса на обновление (команда доступна только для привилегированного пользователя). - <i>seconds</i> – время жизни записи; - infinity – время жизни записи не ограничено. |
| no ip dhcp snooping binding <i>mac_address vlan_id</i> | | Удаляет из файла (базы) контроля протокола DHCP соответствие MAC-адреса клиента и группы VLAN. |
| clear ip dhcp snooping database | - | Очищает файл (базу) контроля протокола DHCP. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 238 – Команды режима EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|--|
| show ip dhcp information option | - | Показывает информацию об использовании опции 82 протокола DHCP. |
| show ip dhcp information option vlan vlan_id interface <i>[gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port portchannel group]</i> | gi_port: (1..8/0/1..48) te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..48); vlan:(1..4094) | Показывает информацию по опции 82 на конкретном порту. |
| show ip dhcp information option tokens [brief] | - | Показывает информацию о возможных вариантах настройки шаблонов в опции 82. |
| show ip dhcp snooping <i>[gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port portchannel group]</i> | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Показывает конфигурацию функции контроля протокола DHCP. |

| | | |
|---|--|---|
| <pre>show ip dhcp snooping binding [macaddress mac_address] [ip- address ip_address] [vlan vlan_id] [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port portchannel group]</pre> | <pre>gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128); vlan_id: (1..4094)</pre> | <p>Показывает соответствия из файла (базы) контроля протокола DHCP.</p> |
|---|--|---|

Примеры выполнения команд

- Разрешить использование DHCP опции 82 в 10 VLAN:

```
console# configure
console(config)# ip dhcp snooping
console(config)# ip dhcp snooping vlan 10
console(config)# ip dhcp information option
console(config)# interface tengigabitethernet 1/0/24
console(config)# ip dhcp snooping trust
```

- Показать все соответствия из таблицы контроля протокола DHCP:

```
console# show ip dhcp snooping binding
```

5.24.5 Защита IP-адреса клиента (IP source Guard)

Функция защиты IP-адреса (IP Source Guard) предназначена для фильтрации трафика, принятого с интерфейса, на основании таблицы соответствий DHCP snooping и статических соответствий IP Source Guard. Таким образом, IP Source Guard позволяет бороться с подменой IP-адресов в пакетах.



Поскольку функция контроля защиты IP-адреса использует таблицы соответствий DHCP snooping, имеет смысл использовать данную функцию, предварительно настроив и включив DHCP snooping.



Функцию защиты IP-адреса (IP Source Guard) необходимо включить глобально и для интерфейса.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 239 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--------------------|--------------------------------|---|
| ip source-guard | По умолчанию функция выключена | Включает функцию защиты IP-адреса клиента для всего коммутатора. |
| no ip source-guard | | Выключает функцию защиты IP-адреса клиента для всего коммутатора. |

| | | |
|---|---|---|
| ip source-guard binding <i>mac_address vlan_id</i> <i>ip_address {gigabitethernet</i> <i>gi_port tengigabitethernet</i> <i>te_port </i> twentyfivegigabitethernet <i>twe_port </i> hundredgigabitethernet <i>hu_port port-channel group}</i> | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128); vlan_id: (1..4094) | Создание статической записи в таблице соответствия между IP-адресом клиента, его MAC-адресом и группой VLAN для указанного в команде интерфейса. |
| no ip source-guard binding <i>mac_address vlan_id</i> | | Удаление статической записи в таблице соответствия. |
| ip source-guard tcam retries-freq {seconds never} | seconds: (10..600)/60 сек | Задает частоту обращения устройства к внутренним ресурсам с целью записи в память неактивных защищенных IP-адресов. - never – запрещает запись в память неактивных защищенных IP-адресов. |
| no ip source-guard tcam retries-freq | | Устанавливает значение по умолчанию. |

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet, интерфейса группы портов:

```
console(config-if)#
```

Таблица 240 – Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

| Команда | Значение/Значение по умолчанию | Действие |
|---------------------------|---------------------------------------|---|
| ip source-guard | По умолчанию | Включает функцию защиты IP-адреса клиента для настраиваемого интерфейса. |
| no ip source-guard | функция выключена. | Выключает функцию защиты IP-адреса клиента для настраиваемого интерфейса. |

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 241 – Команды режима Privileged EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|------------------------------------|---------------------------------------|---|
| ip source-guard tcam locate | - | Вручную запускает процесс обращения устройства к внутренним ресурсам с целью записи в память неактивных защищенных IP-адресов. Команда доступна только для привилегированного пользователя. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 242 – Команды режима EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---|--|
| <code>show ip source-guard configuration [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port ort-channel group]</code> | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); tve_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Команда отображает настройку функции защиты IP-адреса на заданном либо на всех интерфейсах устройства. |
| <code>show ip source-guard statistics [vlan vlan_id]</code> | vlan_id: (1..4094) | Команда отображает статистику функции защиты IP-адреса на заданном либо на всех VLAN. |
| <code>show ip source-guard status [mac-address mac_address] [ip-address ip_address] [vlan vlan_id] [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port port-channel group]</code> | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); tve_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128); vlan_id: (1..4094) | Команда отображает статус функции защиты IP-адреса для указанного интерфейса, IP-адреса, MAC-адреса или группы VLAN. |
| <code>show ip source-guard inactive</code> | - | Команда отображает не активные IP-адреса отправителя. |

Примеры выполнения команд

- Показать настройку функции защиты IP-адреса для всех интерфейсов:

```
console# show ip source-guard configuration
```

```
IP source guard is globally enabled.

Interface      State
-----      -
te0/4          Enabled
te0/21         Enabled
te0/22         Enabled
```

- Включить функцию защиты IP-адреса для фильтрации трафика на основании таблицы соответствий DHCP snooping и статических соответствий IP Source Guard. Создать статическую запись в таблице соответствия для интерфейса Ethernet 12: IP-адрес клиента – 192.168.16.14, его MAC-адрес – 00:60:70:4A:AB:AF. Интерфейс в третьей группе VLAN:

```
console# configure
console(config)# ip dhcp snooping
console(config)# ip source-guard
console(config)# ip source-guard binding 0060.704A.ABAF 3 192.168.16.14
1/0/12
```

5.24.6 Контроль протокола ARP (ARP Inspection)

Функция контроля протокола **ARP (ARP Inspection)** предназначена для защиты от атак с использованием протокола ARP (например, ARP-spoofing – перехват ARP-трафика). Контроль протокола ARP осуществляется на основе статических соответствий IP- и MAC-адресов, заданных для группы VLAN.



Порт, сконфигурированный «недоверенным» для функции ARP Inspection, должен также быть «недоверенным» для функции DHCP snooping или соответствие MAC-адреса и IP-адреса для этого порта должно быть сконфигурировано статически. Иначе данный порт не будет отвечать на запросы ARP.



Для ненадёжных портов выполняются проверки соответствий IP- и MAC-адресов.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console (config) #
```

Таблица 243 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|---|---|---|
| ip arp inspection | По умолчанию | Включает контроль протокола ARP (функцию ARP Inspection). |
| no ip arp inspection | функция выключена | Выключает контроль протокола ARP (функцию ARP Inspection). |
| ip arp inspection vlan <i>vlan_id</i> | <i>vlan_id</i> : (1..4094); По умолчанию | Разрешает проверку протокола ARP, основанную на базе соответствий DHCP snooping, в выбранной группе VLAN. |
| no ip arp inspection vlan <i>vlan_id</i> | функция выключена | Запрещает проверку протокола ARP, основанную на базе соответствий DHCP snooping, в выбранной группе VLAN. |
| ip arp inspection validate | - | Предоставляет специфичные проверки для контроля протокола ARP. MAC-адрес источника: Для ARP-запросов и ответов проверяется соответствие MAC-адреса в заголовке Ethernet MAC-адресу источника в содержимом протокола ARP. MAC-адрес назначения: Для ARP-ответов проверяется соответствие MAC-адреса в заголовке Ethernet MAC-адресу назначения в содержимом протокола ARP. IP-адрес: Проверяется содержимое ARP-сообщения на наличие некорректных IP-адресов. |
| no ip arp inspection validate | | Запрещает специфичные проверки для контроля протокола ARP. |
| ip arp inspection list create <i>name</i> | <i>name</i> : (1..32) символа | 1. Создание списка статических ARP-соответствий. |
| no ip arp inspection list create <i>name</i> | | 2. Вход в режим конфигурации ARP-списков. Удаление списка статических ARP-соответствий. |
| ip arp inspection list assign <i>vlan_id</i> | <i>vlan_id</i> : (1..4094) | Назначает список статических ARP-соответствий для указанной VLAN. |
| no ip arp inspection list assign <i>vlan_id</i> | | Отменяет назначение списка статических ARP-соответствий для указанной VLAN. |
| ip arp inspection logging interval {<i>seconds</i> infinite} | <i>seconds</i> : (0..86400)/ 5 сек | Задаёт минимальный интервал между сообщениями, содержащими информацию протокола ARP, передаваемыми в журнал. - значение 0 указывает на то, что сообщения будут генерироваться незамедлительно; - infinite – не генерировать сообщений в журнал. |
| no ip arp inspection logging interval | | Устанавливает значение по умолчанию. |

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet, интерфейса группы портов:

```
console (config-if) #
```

Таблица 244 – Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

| Команда | Значение/Значение по умолчанию | Действие |
|-----------------------------------|---|---|
| ip arp inspection trust | По умолчанию интерфейс не является доверенным | Добавляет интерфейс в список «доверенных» при использовании контроля протокола ARP. ARP-трафик «доверенного» интерфейса считается безопасным и не контролируется. |
| no ip arp inspection trust | | Удаляет интерфейс из списка «доверенных» при использовании контроля протокола ARP. |

Команды режима конфигурации ARP-списков

Вид запроса командной строки в режиме конфигурации ARP-списков:

```
console# configure
console(config)# ip arp inspection list create spisok
console(config-arp-list)#
```

Таблица 245 – Команды режима конфигурации ARP-списков

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---------------------------------------|---|
| ip ip_address mac-address mac_address | - | Добавляет статическое соответствие IP- и MAC-адресов. |
| no ip ip_address mac-address mac_address | - | Удаляет статическое соответствие IP- и MAC-адресов. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 246 – Команды режима EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|--|--|
| show ip arp inspection [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128) | Показывает конфигурацию функции контроля протокола ARP Inspection на выбранном интерфейсе/всех интерфейсах. |
| show ip arp inspection list | - | Показывает списки статических соответствий IP- и MAC-адресов (команда доступна только для привилегированного пользователя). |
| show ip arp inspection statistics [vlan vlan_id] | vlan_id: (1..4094) | Показывает статистику для следующих типов пакетов, которые были обработаны при помощи функции ARP: - переданные пакеты (forwarded); - потерянные пакеты (dropped); - ошибки в IP/MAC (IP/MAC Failures). |
| clear ip arp inspection statistics [vlan vlan_id] | vlan_id: (1..4094) | Очищает статистику контроля протокола ARP Inspection. |

Примеры выполнения команд

- Включить контроль протокола ARP и добавить в список spisok статическое соответствие: MAC-адрес: 00:60:70:AB:CC:CD, IP-адрес: 192.168.16.98. Назначить список spisok статических ARP-соответствий для VLAN 11:

```
console# configure
console(config)# ip arp inspection list create spisok
console(config-arp-list)# ip 192.168.16.98 mac-address 0060.70AB.CCCD
console(config-arp-list)# exit
console(config)# ip arp inspection list assign 11 spisok
```

- Показать списки статических соответствий IP- и MAC-адресов:

```
console# show ip arp inspection list
```

```
List name: servers
Assigned to VLANs: 11
IP                ARP
-----
192.168.16.98    0060.70AB.CCCD
```

5.24.7 Функционал First Hop Security

Пакет функций First Hop Security включает в себя анализатор DHCPv6-пакетов, IPv6 Source Guard, ND Inspection и RA Guard. Данный набор функций предназначен для обеспечения контроля и фильтрации IPv6 трафика в сети.

Анализатор DHCPv6 пакетов позволяет добавлять соседей в таблицу привязок IPv6 binding table при получении адреса по DHCP, а также позволяет бороться с недоверенными DHCPv6 серверами.

IPv6 Source Guard позволяет устройству отклонять трафик, если он исходит от адреса, который не сохранен в IPv6 binding table. Таблица привязок соседей IPv6 binding table, подключенных к устройству, создается из таких источников информации, как отслеживание по протоколу обнаружения соседей (NDP).

С помощью функции ND Inspection коммутатор проверяет сообщения NS (Neighbor Solicitation) и NA (Neighbor Advertisement) и сохраняет их в IPv6 binding table. На основании таблицы коммутатор отбрасывает любые поддельные сообщения NS / NA.

Функционал RA Guard позволяет блокировать или отклонять нежелательные или посторонние сообщения Router Advertisement (RA), поступающие на коммутатор от маршрутизатора.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 247 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--|---------------------------------------|---|
| ipv6 neighbor binding policy <i>policy_name</i> | policy_name: (1..32) символа | Создать политику привязки соседей (neighbor binding) и перейти в режим её конфигурирования. |
| no ipv6 neighbor binding policy <i>policy_name</i> | | Удалить политику привязки соседей. |
| ipv6 first hop security policy <i>policy_name</i> | policy_name: (1..32) символа | Создать политику First Hop Security. |
| no ipv6 first hop security policy <i>policy_name</i> | | Удалить политику привязки соседей. |
| ipv6 first hop security logging packet drop | -/выключено | Активировать логирование дропа пакетов при несоответствии политикам безопасности служб RA Guard, ND Inspection, DHCPv6 Guard и IPv6 Source Guard. |
| no ipv6 first hop security logging packet drop | | Установить значение по умолчанию. |
| ipv6 neighbor binding address-config {stateless any dhcp} | -/выключено | Включить добавление записей в таблицу привязки соседей на основании: <ul style="list-style-type: none"> - dhcp-пакета DHCPv6 Reply. При этом все Link-local IPv6-адреса вносятся в таблицу привязки соседей по умолчанию в результате анализа ICMPv6-пакетов; - any — добавлять все адреса; - stateless — на основе IPv6 RA сообщений. |

| | | |
|--|--|---|
| no ipv6 neighbor binding address-config | | Установить значение по умолчанию. |
| ipv6 neighbor binding address-prefix {vlan X:X:X:X::X/<0-128>} | - | Добавить статическую запись с префиксом в таблицу Neighbor Prefix Table: vlan — привязать запись к определенному VLAN. |
| no ipv6 neighbor binding address-prefix {vlan X:X:X:X::X/<0-128>} | | Удалить статическую запись с префиксом из таблицы Neighbor Prefix Table. |
| ipv6 neighbor binding address-prefix-validation | -/выключено | Включить проверку адресов в таблице привязки соседей |
| no ipv6 neighbor binding address-prefix-validation | | Установить значение по умолчанию. |
| ipv6 neighbor binding lifetime minutes | minutes: 1..60 / 5 | Установить время жизни таблицы привязки соседей для записи в минутах. |
| no ipv6 neighbor binding lifetime | | Установить значение по умолчанию. |
| ipv6 neighbor binding logging | -/выключено | Включить логирование основных событий по изменению таблицы привязки. |
| no ipv6 neighbor binding logging | | Установить значение по умолчанию. |
| ipv6 neighbor binding max-entries {interface-limit vlan-limit mac-limit} {limit disable} | limit: (0..65535)/ выключено | Определить максимальное количество записей в таблице привязки соседей. - interface-limit — определить лимит для интерфейса; - vlan-limit — определить лимит VLAN; - mac-limit — определить лимит MAC-адресов; - disable — разрешить максимальное количество записей. Максимальное значение = 4294967294. |
| no ipv6 neighbor binding max-entries | | Установить значение по умолчанию. |
| ipv6 neighbor binding static ipv6 {X:X:X:X::X} vlan vlan_id interface interface mac mac-address | - | Добавить статическую запись без префикса в таблицу Neighbor Prefix Table: - vlan — привязать запись к определенному VLAN; - interface — привязать запись к определенному интерфейсу; - mac — привязать запись к определенному MAC-адресу. |
| no ipv6 neighbor binding static ipv6 {X:X:X:X::X} vlan vlan_id | | Удалить статическую запись. |
| ipv6 source guard policy policy_name | policy_name: (1..32) символа | Создать политику Source Guard и перейти в режим её конфигурирования. |
| no ipv6 source guard policy policy_name | | Удалить политику Source Guard. |
| ipv6 dhcp guard policy policy_name | policy_name: (1..32) символа | Создать политику DHCP Guard и перейти в режим её конфигурирования. |
| no ipv6 dhcp guard policy policy_name | | Удалить политику DHCP Guard. |
| ipv6 dhcp guard preference {minimum minimum_value maximum maximum_value} | minimum_value; maximum_value: (0..255)/выключено | Установить максимальный и минимальный пределы предпочтения для DHCPv6-сервера. |
| ipv6 dhcp guard preference | | Установить значение по умолчанию. |
| ipv6 nd inspection policy policy_name | policy_name: (1..32) символа | Создать политику ND Inspection и перейти в режим её конфигурирования. |
| no ipv6 nd inspection policy policy_name | | Удалить политику ND Inspection. |
| ipv6 nd inspection drop-unsecure | -/выключено | Включить отбрасывание пакетов с отсутствующими или недопустимыми параметрами или подписью. |
| no ipv6 nd inspection drop-unsecure | | Установить значение по умолчанию. |
| ipv6 nd inspection sec-level minimum | minimum: (0..7)/ выключено | Установить минимальное значение параметра уровня безопасности при использовании опций криптографически сгенерированного адреса (CGA). |
| no ipv6 nd inspection sec-level minimum | | Установить значение по умолчанию. |
| ipv6 nd inspection validate source-mac | -/выключено | Включить проверку MAC-адреса пакета по его адресу link-layer. |

| | | |
|--|--|--|
| <code>no ipv6 nd inspection validate source-mac</code> | | Установить значение по умолчанию. |
| <code>ipv6 nd raguard policy</code> | policy_name: (1..32) символа | Создать политику ND RA Guard и перейти в режим её конфигурирования. |
| <code>no ipv6 nd raguard policy</code> | | Удалить политику ND RA Guard. |
| <code>ipv6 nd raguard hop-limit {minimum minimum_value maximum maximum_value}</code> | minimum_value; maximum_value: (1..255)/выключено | Установить пределы значения Cur Hop Limit в сообщениях Router Advertisement. |
| <code>no ipv6 nd raguard hop-limit</code> | | Установить значение по умолчанию. |
| <code>ipv6 nd raguard managed-config-flag {off on}</code> | -/выключено | Включить проверку флага managed-config в сообщениях Router Advertisement: - off — значение флага должно быть 0; - on — значение флага должно быть 1. |
| <code>no ipv6 nd raguard managed-config-flag</code> | | Установить значение по умолчанию. |
| <code>ipv6 nd raguard other-config-flag {off on}</code> | -/выключено | Включить проверку флага other-config в сообщениях Router Advertisement: - off — значение флага должно быть 0; - on — значение флага должно быть 1. |
| <code>no ipv6 nd raguard other-config-flag</code> | | Установить значение по умолчанию. |
| <code>ipv6 nd raguard router-preference minimum {low medium high}</code> | -/выключено | Установить минимальное объявляемое значение Default Router Preference в сообщениях Router Advertisement: - low — низкое значение; - medium — среднее значение; - high — высокое значение. |
| <code>no ipv6 nd raguard router-preference minimum</code> | | Установить значение по умолчанию. |
| <code>ipv6 nd raguard router-preference maximum {low medium high}</code> | -/выключено | Установить максимальное объявляемое значение Default Router Preference в сообщениях Router Advertisement: - low — низкое значение; - medium — среднее значение; - high — высокое значение. |
| <code>no ipv6 nd raguard router-preference maximum</code> | | Установить значение по умолчанию. |

Команды режима конфигурации политики привязки соседей

Вид запроса командной строки:

```
console(config-nbr-binding) #
```

Таблица 248 – Команды режима политики привязки соседей

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---------------------------------------|--|
| <code>logging binding enable</code> | -/выключено | Включить логирование добавления/удаления IPv6 в таблицу привязки соседей. |
| <code>logging binding disable</code> | | Выключить логирование добавления/удаления IPv6 в таблицу привязки соседей. |
| <code>max-entries {interface-limit vlan-limit mac-limit} {limit disable}</code> | limit: (0..65535)/ выключено | Определить максимальное количество записей в таблице привязки соседей. - interface-limit — определить лимит для интерфейса; - vlan-limit — определить лимит VLAN; - mac-limit — определить лимит MAC-адресов; - disable — разрешить максимальное количество записей. Максимальное значение = 4294967294. |
| <code>no max-entries</code> | | Установить значение по умолчанию. |

| | | |
|---|-------------|---|
| address-config {dhcp any stateless} | -/выключено | Включить добавление записей в таблицу привязки соседей на основании: - dhcp-пакета DHCPv6 Reply. При этом все Link-local IPv6-адреса вносятся в таблицу привязки соседей по умолчанию в результате анализа ICMPv6-пакетов; - any — добавлять все адреса; - stateless — на основе IPv6 RA сообщений. |
| no address-config | | Установить значение по умолчанию. |
| address-prefix-validation {enable disable} | -/выключено | Включить проверку адресов в таблице привязки соседей. |
| no address-prefix-validation | | Установить значение по умолчанию. |
| device-role {permitter internal} | -/выключено | Указать роль устройства, подключенного к интерфейсу: - permitter — устройство периметра; - internal — внутреннее устройство. |
| no device-role | | Убрать роль с устройства, подключенного к интерфейсу. |

Команды режима конфигурации политики Source Guard

Вид запроса командной строки:

```
console (config-ipv6-srcgrd) #
```

Таблица 249 – Команды режима IPv6 Source Guard политики

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|------------------------|---------------------------------------|--|
| trusted-port | -/выключено | Определить доверенный порт. Данная политика назначается на порт, на котором не должна применяться политика Source Guard. |
| no trusted-port | | Установить значение по умолчанию. |

Команды режима конфигурации политики DHCP Guard

Вид запроса командной строки:

```
console (config-dhcp-guard) #
```

Таблица 250 – Команды режима ipv6 DHCP Guard политики

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---|---|
| device-role {client server} | -/выключено | Указать роль устройства, подключенного к интерфейсу: - server — установить роль сервера; - client — установить роль клиента. |
| no device-role | | Убрать роль с устройства, подключенного к интерфейсу. |
| match reply {disable prefix-list prefix_list} | prefix_list: (0..32) символа/ выключено | Включить проверку анонсируемых адресов, полученных в сообщениях DHCPv6: - disable — отключить проверку по DHCPv6-сообщениям; - prefix-list — префикс-маска, по которой будет осуществляться проверка. |
| no match reply | | Установить значение по умолчанию. |
| match server address {disable prefix-list prefix_list} | prefix_list: (0..32) символа/ выключено | Включить проверку адреса источника сервера: - disable — отключить проверку адреса источника сервера; - prefix-list — префикс-маска, по которой будет осуществляться проверка. |
| no match server address | | Установить значение по умолчанию. |
| preference minimum {preference_value disable} | preference_value: (0..255)/выключено | Установить минимальный предел анонсируемых DHCPv6-сервером опций: - disable — выключить проверку опций. |
| no preference minimum | | Установить значение по умолчанию. |

| | | |
|---|---|--|
| preference maximum {preference_value disable} | preference_value: (0..255)/выключено | Установить максимальный предел анонсируемых DHCPv6-сервером опций: - disable — выключить проверку опций. |
| no preference maximum | | Установить значение по умолчанию. |

Команды режима конфигурации политики ND Inspection

Вид запроса командной строки:

```
console(config-nd-inspection) #
```

Таблица 251 – Команды режима IPv6 ND Inspection политики

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|--|---|
| device-role {host router} | -/выключено | Указать роль устройства, подключенного к интерфейсу: - host — установить роль хоста - router — установить роль маршрутизатора |
| no device-role | | Установить значение по умолчанию. |
| drop-unsecure {enable disable} | -/выключено | Включить отбрасывание пакетов с отсутствующими или недопустимыми параметрами или подписью. |
| no drop-unsecure | | Установить значение по умолчанию. |
| sec-level minimum {sec_level_minimum disable} | sec_level_minimum: (0..7)/выключено | Указать минимальное значение параметра уровня безопасности при использовании опций криптографически сгенерированного адреса (CGA). |
| no sec-level minimum | | Установить значение по умолчанию. |
| validate source-mac {enable disable} | -/выключено | Включить проверку MAC-адреса пакета по его link-layer адресу: - enable — включить - disable — выключить |
| no validate source-mac | | Установить значение по умолчанию. |

Команды режима конфигурации политики RA Guard

Вид запроса командной строки:

```
console(config-ra-guard) #
```

Таблица 252 – Команды режима IPv6 RA Guard политики

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|--|--|
| device-role {host router} | -/выключено | Указать роль устройства, подключенного к интерфейсу: - host — установить роль хоста; - router — установить роль маршрутизатора. |
| no device-role | | Установить значение по умолчанию. |
| hop-limit {minimum value_limit maximum value_limit} | value_limit: (1..255)/выключено | Установить пределы значения Cur Hop Limit в сообщениях Router Advertisement. |
| no hop-limit | | Установить значение по умолчанию. |
| managed-config-flag {off on} | -/выключено | Включить проверку флага managed-config в сообщениях Router Advertisement: - off — значение флага должно быть 0; - on — значение флага должно быть 1. |
| no managed-config-flag | | Установить значение по умолчанию. |
| match ra address {disable prefix-list prefix_list} | prefix_list: (1-32) символа/ выключено | Включить проверку адресов в сообщениях Router Advertisement: - disable — отключить проверку адресов - prefix-list — префикс маска, по которой будет осуществляться проверка. |
| no match ra address | | Установить значение по умолчанию. |

| | | |
|--|--|--|
| match ra prefixes {disable prefix-list prefix_list} | prefix_list: (1-32) символа/ выключено | Включить проверку префиксов в сообщениях Router Advertisement: - disable — отключить проверку префиксов; - prefix-list — префикс-маска, по которой будет осуществляться проверка. |
| no match ra address | | Установить значение по умолчанию. |
| other-config-flag {off on} | -/выключено | Включить проверку флага other-config в сообщениях Router Advertisement: - off — значение флага должно быть 0; - on — значение флага должно быть 1. |
| no other-config-flag | | Установить значение по умолчанию. |
| router-preference minimum {low medium high} | -/выключено | Установить минимальное объявляемое значение Default Router Preference в сообщениях Router Advertisement: - low — низкое значение; - medium — среднее значение; - high — высокое значение. |
| no router-preference minimum | | Установить значение по умолчанию. |
| router-preference maximum {low medium high} | -/выключено | Установить максимальное объявляемое значение Default Router Preference в Router Advertisement сообщениях: - low — низкое значение; - medium — среднее значение; - high — высокое значение. |
| no router-preference maximum | | Установить значение по умолчанию. |

Команды режима конфигурации политики First Hop Security

Вид запроса командной строки:

```
console (config-ipv6-fhs) #
```

Таблица 253 – Команды режима IPv6 First Hop Security политики

| Команда | Значение/Значение по умолчанию | Действие |
|---|---------------------------------------|---|
| logging packet drop {enable disable} | -/выключено | Активировать логирование дропа пакетов при несоответствии политикам безопасности служб RA Guard, ND Inspection, DHCPv6 Guard и IPv6 Source Guard: - enable — включить логирование дропа пакетов для данной политики; - disable — отключить логирование дропа пакетов для данной политики. |
| no logging packet drop | | Установить значение по умолчанию. |

Команды режима конфигурации интерфейса VLAN

Вид запроса командной строки:

```
console (config-if) #
```

Таблица 254 – Команды режима конфигурации интерфейса VLAN

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|---|
| ipv6 first hop security | -/выключено | Включить функционал First Hop Security во VLAN. |
| no ipv6 first hop security | | Выключить функционал First Hop Security во VLAN. |
| ipv6 first hop security attach-policy policy_name | policy_name: (1..32) символа/ выключено | Добавить политику First Hop Security на интерфейс. |
| no ipv6 first hop security attach-policy | | Удалить политику First Hop Security с интерфейса. |
| ipv6 neighbor binding | -/выключено | Включить привязку соседей и добавление записей в таблицу. |

| | | |
|---|---|--|
| no ipv6 neighbor binding | | Выключить привязку соседей и добавление записей в таблицу. |
| ipv6 neighbor binding attach-policy policy_name | policy_name: (1..32) символа/ выключено | Добавить политику Neighbor Binding на интерфейс. |
| no ipv6 neighbor binding attach-policy | | Удалить политику Neighbor Binding с интерфейса. |
| ipv6 source guard | -/выключено | Включить IPv6 Source Guard. |
| no ipv6 source guard | | Выключить IPv6 Source Guard. |
| ipv6 dhcp guard | -/выключено | Включить DHCP Guard. |
| no ipv6 dhcp guard | | Выключить DHCP Guard. |
| ipv6 dhcp guard attach-policy policy_name | policy_name: (1..32) символа/ выключено | Добавить политику DHCP Guard на интерфейс. |
| no ipv6 dhcp guard attach-policy | | Удалить политики DHCP Guard с интерфейса. |
| ipv6 nd inspection | -/выключено | Включить IPv6 ND Inspection. |
| no ipv6 nd inspection | | Выключить IPv6 ND Inspection. |
| ipv6 nd inspection attach-policy policy_name | policy_name: (1..32) символа/ выключено | Добавить политику ND Inspection на интерфейс. |
| no ipv6 nd inspection attach-policy | | Удалить политику ND Inspection с интерфейса. |
| ipv6 nd rguard | -/выключено | Включить IPv6 ND RA Guard. |
| no ipv6 nd rguard | | Выключить IPv6 ND RA Guard. |
| ipv6 nd rguard attach-policy policy_name | policy_name: (1..32) символа/ выключено | Добавить политику ND RA Guard на интерфейс. |
| no ipv6 nd rguard attach-policy | | Удалить политику ND RA Guard с интерфейса. |

Команды режима EXEC

Вид запроса командной строки:

```
console#
```

Таблица 255 – Команды режима EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|---|---------------------------------------|---|
| show ipv6 first hop security | - | Отобразить настройки функций IPv6 First Hop Security. |
| show ipv6 source guard | - | Отобразить состояние функции IPv6 source guard. |
| show ipv6 neighbor binding table | - | Отобразить таблицу привязок соседей. |
| show ipv6 dhcp guard | - | Отобразить состояние и настройки функции DHCP Guard. |
| show ipv6 nd inspection | - | Отобразить состояние и настройки функции ND Inspection. |
| show ipv6 nd rguard | - | Отобразить состояние и настройки функции RA Guard. |

5.25 Функции DHCP Relay агента

Коммутаторы поддерживают функции DHCP Relay агента. Задачей DHCP Relay агента является передача DHCP-пакетов от клиента к серверу и обратно в случае, если DHCP-сервер находится в одной сети, а клиент в другой. Другой функцией является добавление дополнительных опций в DHCP-запросы клиента (например, опции 82).

Принцип работы DHCP Relay агента на коммутаторе: коммутатор принимает от клиента DHCP-запросы, передает эти запросы серверу от имени клиента (оставляя в запросе опции с требуемыми клиентом параметрами и, в зависимости от конфигурации, добавляя свои опции). Получив ответ от сервера, коммутатор передает его клиенту.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console (config) #
```

Таблица 256 – Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---------------------------------------|---|
| ip dhcp relay enable | По умолчанию агент выключен | Включение функций DHCP Relay агента на коммутаторе. |
| no ip dhcp relay enable | | Выключение функций DHCP Relay агента на коммутаторе. |
| ip dhcp relay address <i>ip_address [vlan vlan_id]</i> | vlan_id: (1..4094) | Задаёт IP-адрес доступного DHCP-сервера для DHCP Relay агента. - <i>vlan</i> — клиентский VLAN, запросы из которого будут направлены на IP-адрес конкретного DHCP-сервера. |
| no ip dhcp relay address <i>[ip_address]</i> | | Удаляет IP-адрес из списка DHCP-серверов для DHCP Relay агента. Может быть задано до восьми серверов в виде диапазона или перечислением. |

Команды режима конфигурации интерфейса VLAN

Вид запроса командной строки в режиме конфигурации интерфейса VLAN:

```
console# configure
console (config) # interface vlan vlan_id
console (config-if) #
```

Таблица 257 – Команды режима конфигурации интерфейса VLAN, интерфейса Ethernet

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---------------------------------------|--|
| ip dhcp relay enable | По умолчанию агент выключен | Включение функций DHCP Relay агента на настраиваемом интерфейсе. |
| no ip dhcp relay enable | | Выключение функций DHCP Relay агента на настраиваемом интерфейсе. |
| ip dhcp relay gateway-address <i>ip_addr</i> | По умолчанию адрес не выбран | Позволяет настроить конкретный адрес источника для dhcp пакетов из клиентского Vlan. |
| no ip dhcp relay gateway-address | | Возвращает в режим работы по умолчанию. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 258 – Команды режима EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---------------------------|---------------------------------------|--|
| show ip dhcp relay | - | Отображает конфигурацию настроенной функции DHCP Relay агента для коммутатора и отдельно для интерфейсов, а также список доступных серверов. |

Примеры выполнения команд

- Показать состояние функции DHCP Relay агента:

```
console# show ip dhcp relay
```

```
DHCP relay is Enabled
DHCP relay is not configured on any vlan.
Servers: 192.168.16.38
Relay agent Information option is Enabled
```

5.26 Конфигурация DHCP-сервера

DHCP-сервер осуществляет централизованное управление сетевыми адресами и соответствующими конфигурационными параметрами, автоматически предоставляя их клиентам. Это позволяет избежать ручной настройки устройств сети и уменьшает количество ошибок.



Ethernet-коммутаторы могут работать как DHCP-клиент (получение собственного IP-адреса от сервера DHCP), так и как DHCP-сервер. В случае если DHCP-сервер отключен, то коммутатор может работать с DHCP Relay.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console (config) #
```

Таблица 259 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|---|--------------------------------|--|
| <code>ip dhcp server</code> | -/выключено | Включение функции DHCP-сервера на коммутаторе.  Перед включением DHCP-сервера предварительно должны быть отключены DHCP-клиенты во всех VLAN. В том числе включенный по умолчанию DHCP-клиент в VLAN 1. |
| <code>no ip dhcp server</code> | | Выключение функции DHCP-сервера на коммутаторе. |
| <code>ip dhcp pool host name</code> | name: (1..32) символов | Вход в режим конфигурации статических адресов DHCP-сервера. |
| <code>no ip dhcp pool host name</code> | | Удаляет конфигурацию DHCP-клиента с заданным именем. |
| <code>ip dhcp pool network name</code> | name: (1..32) символов | Вход в режим конфигурации DHCP-пула адресов DHCP-сервера. - name – имя DHCP-пула адресов.  Максимально допустимое количество DHCP pool указано в таблице 9. |
| <code>no ip dhcp pool network name</code> | | Удаляет DHCP-пул с заданным именем. |
| <code>ip dhcp excluded-address low_address [high_address]</code> | - | Указывает IP-адреса, которые DHCP-сервер не будет назначать для DHCP-клиентов. - low-address – начальный IP-адрес диапазона; - high-address – конечный IP-адрес диапазона. |
| <code>no ip dhcp excluded-address low_address [high_address]</code> | | Удаление IP-адреса из списка исключений для назначения его DHCP-клиентам. |

Команды режима конфигурации статических адресов DHCP-сервера

Вид запроса командной строки в режиме конфигурации статических адресов DHCP-сервера:

```
console# configure
console (config) # ip dhcp pool host name
console (config-dhcp) #
```

Таблица 260 – Команды режима конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|---|--------------------------------|--|
| address <i>ip_address</i> { <i>mask</i> <i>prefix_length</i> } { <i>client-identifier id</i> <i>hardware-address mac_address</i> } | - | Ручное резервирование IP-адресов для DHCP-клиента. - <i>ip_address</i> – IP-адрес, который будет сопоставлен с физическим адресом клиента; - <i>mask/prefix_length</i> – маска подсети/длина префикса; - <i>id</i> – физический адрес (идентификатор) сетевой карты; - <i>mac_address</i> – MAC-адрес. |
| no address | | Удаляет зарезервированные IP-адреса. |
| client-name <i>name</i> | name: (1..32) символов | Определяет имя DHCP-клиента. |
| no client-name | | Удаляет имя DHCP-клиента. |

Команды режима конфигурации пула DHCP-сервера

Вид запроса командной строки в режиме конфигурации пула DHCP-сервера:

```
console# configure
console(config)# ip dhcp pool network name
console(config-dhcp)#
```

Таблица 261 – Команды режима конфигурации


| Команда | Значение/Значение по умолчанию | Действие |
|---|--------------------------------|---|
| address { <i>network_number</i> low <i>low_address</i> high <i>high_address</i> } { <i>mask</i> <i>prefix_length</i> } | - | Устанавливает номер подсети и маску подсети для пула адресов DHCP-сервера. - <i>network_number</i> – IP-адрес номера подсети; - <i>low_address</i> – начальный IP-адрес диапазона адресов; - <i>high_address</i> – конечный IP-адрес диапазона адресов. - <i>mask/prefix_length</i> – маска подсети/длина префикса. |
| no address | | Удаляет конфигурацию DHCP - пула адресов |
| lease { <i>days</i> [<i>hours</i> [<i>minutes</i>]] infinite } | -/1 день | Время аренды IP-адреса, который назначен от DHCP. - infinite – время аренды не ограничено; - <i>days</i> – количество дней; - <i>hours</i> – количество часов; - <i>minutes</i> – количество минут. |
| no lease | | Установить значение по умолчанию. |

Команды режима конфигурации пула DHCP-сервера и статических адресов DHCP-сервера

Вид запроса командной строки:

```
console(config-dhcp)#
```

Таблица 262 – Команды режима конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|---|
| default-router <i>ip_address_list</i> | По умолчанию список маршрутизаторов не определен. | Определяет список маршрутизаторов по умолчанию для DHCP-клиента: - <i>ip_address_list</i> – список IP-адресов маршрутизаторов, может содержать до 8 записей, разделенных пробелом.  IP-адрес маршрутизатора должен быть в той же подсети, что и клиент. |
| no default-router | | Устанавливает значение по умолчанию. |
| dns-server <i>ip_address_list</i> | По умолчанию список DNS-серверов не определен. | Определяет список DNS-серверов, доступных для клиентов DHCP. - <i>ip_address_list</i> – список IP-адресов DNS-серверов, может содержать до 8 записей, разделенных пробелом. |
| no dns-server | | Устанавливает значение по умолчанию. |

| | | |
|--|---|--|
| domain-name <i>domain</i> | domain: (1..32) символов | Определяет доменное имя для DHCP-клиентов. |
| no domain-name | | Устанавливает значение по умолчанию. |
| netbios-name-server <i>ip_address_list</i> | По умолчанию список WINS-серверов не определен. | Определяет список WINS-серверов, доступных для клиентов DHCP. - <i>ip_address_list</i> – список IP-адресов WINS-серверов, может содержать до 8 записей, разделенных пробелом. |
| no netbios-name-server | | Устанавливает значение по умолчанию. |
| netbios-node-type { <i>b-node</i> <i>p-node</i> <i>m-node</i> <i>h-node</i> } | По умолчанию тип узла NetBIOS не определен. | Определяет тип узла NetBIOS Microsoft для клиентов DHCP: - <i>b-node</i> – широковещательный; - <i>p-node</i> – точка-точка; - <i>m-node</i> – комбинированный; - <i>h-node</i> – гибридный. |
| no netbios-node-type | | Устанавливает значение по умолчанию. |
| next-server <i>ip_address</i> | | Используется для указания DHCP-клиенту адреса сервера (как правило, TFTP-сервера), с которого должен быть получен загрузочный файл. |
| no next-server | | Устанавливает значение по умолчанию. |
| next-server-name <i>name</i> | name: (1..64) символов | Используется для указания DHCP-клиенту имя сервера, с которого должен быть получен загрузочный файл. |
| no next-server-name | | Устанавливает значение по умолчанию. |
| bootfile <i>filename</i> | filename: (1..128) символов | Указывает имя файла, используемого для начальной загрузки DHCP-клиента. |
| no bootfile | | Устанавливает значение по умолчанию. |
| time-server <i>ip_address_list</i> | По умолчанию список серверов не определен. | Определяет список серверов времени, доступных для клиентов DHCP. - <i>ip_address_list</i> – список IP-адресов серверов времени, может содержать до 8 записей, разделенных пробелом. |
| no time-server | | Устанавливает значение по умолчанию. |
| option <i>code</i> { boolean <i>bool_val</i> integer <i>int_val</i> ascii <i>ascii_string</i> ip[-list] <i>ip_address_list</i> hex { <i>hex_string</i> none } [description <i>desc</i>] | code: (0..255); bool_val: (true, false); int_val: (0..4294967295); ascii_string: (1..160) символов; desc: (1..160) символов | Настраивает опции DHCP-сервера. - <i>code</i> – код опции DHCP-сервера; - <i>bool_val</i> – логическое значение; - <i>integer</i> – целое положительное число; - <i>ascii_string</i> – строка в формате ASCII; - <i>ip_address_list</i> – список IP-адресов; - <i>hex_string</i> – строка в 16-ом формате. |
| no option <i>code</i> | | Удаляет опции для DHCP-сервера. |

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 263 – Команды режима Privileged EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|---|---------------------------------------|--|
| clear ip dhcp binding { <i>ip_address</i> *} | - | Удаление записей из таблицы соответствия физических адресов и адресов, выданных с пула DHCP-сервером: - <i>ip_address</i> – IP-адрес, назначенный DHCP-сервером; - * – удалить все записи. |
| show ip dhcp | - | Просмотр конфигурации DHCP-сервера. |
| show ip dhcp excluded-addresses | - | Просмотр IP-адресов, которые DHCP-сервер не будет назначать для DHCP-клиентов. |
| show ip dhcp pool host [<i>ip_address</i> <i>name</i>] | name: (1..32) символов | Просмотр конфигурации для статических адресов DHCP-сервера: - <i>ip_address</i> – IP-адрес клиента; - <i>name</i> – имя DHCP-пула адресов. |
| show ip dhcp pool network [<i>name</i>] | name: (1..32) символов | Просмотр конфигурации DHCP-пула адресов DHCP-сервера: - <i>name</i> – имя DHCP-пула адресов. |

| | | |
|--|---|--|
| <code>show ip dhcp binding</code> <i>[ip_address]</i> | - | Просмотр IP-адресов, которые сопоставлены с физическими адресами клиентов, а также время аренды, способ назначения и состояние IP-адресов. |
| <code>show ip dhcp server statistics</code> | - | Просмотр статистики DHCP-сервера. |
| <code>show ip dhcp allocated</code> | - | Просмотр активных IP-адресов, выданных DHCP-сервером. |

Примеры выполнения команд

- Настроить DHCP-пул с именем *test* и указать для DHCP-клиентов: имя домена – *test.ru*, шлюз по умолчанию – *192.168.45.1* и DNS-сервер – *192.168.45.112*.

```
console#
console# configure
console(config)# ip dhcp pool network test
console(config-dhcp)# address 192.168.45.0 255.255.255.0
console(config-dhcp)# domain-name test.ru
console(config-dhcp)# dns-server 192.168.45.112
console(config-dhcp)# default-router 192.168.45.1
```

5.27 Конфигурация ACL (списки контроля доступа)

ACL (Access Control List – список контроля доступа) – таблица, которая определяет правила фильтрации входящего и исходящего трафика на основании передаваемых в пакетах протоколов, TCP/UDP портов, IP-адресов или MAC-адресов.



ACL-списки на базе IPv6, IPv4 и MAC-адресов не должны иметь одинаковые названия.



IPv6- и IPv4-списки могут работать вместе на одном физическом интерфейсе. IPv4-списки и ACL на базе MAC-адресации могут работать вместе на одном физическом интерфейсе. Список ACL на базе MAC-адресации не может совмещаться со списками для IPv6. Два списка одинакового типа не могут работать вместе на интерфейсе.

Команды для создания и редактирования списков ACL доступны в режиме глобальной конфигурации.

Команды режима глобальной конфигурации

Командная строка в режиме глобальной конфигурации имеет вид:

```
console(config)#
```

Таблица 264 – Команды для создания и конфигурации списков ACL

| Команда | Значение/Значение по умолчанию | Действие |
|--|---------------------------------------|--|
| <code>ip access-list <i>access_list</i></code> <code>{deny permit} {any <i>ip_address [ip_address_mask]</i>}</code> | | Создание стандартного списка ACL. - deny – запретить прохождение пакетов с указанными параметрами; - permit – разрешить прохождение пакетов с указанными параметрами. |
| <code>no ip access-list <i>access_list</i></code> | <i>access_list</i> : (0..32) | Удалить стандартный список ACL. |
| <code>ip access-list extended <i>access_list</i></code> | символа | Создание нового расширенного списка ACL для адресации IPv4 и вход в режим его конфигурации (если список с данным именем еще не создан) либо вход в режим конфигурации ранее созданного списка. |
| <code>no ip access-list extended <i>access_list</i></code> | | Удаление расширенного списка ACL для адресации IPv4. |

| | | |
|--|---------------------------------------|---|
| ipv6 access-list <i>access_list</i> {deny permit} {any <i>ipv6_address</i> [<i>ipv6_address_prefix</i>]} | | Создание нового стандартного списка ACL для адресации IPv6. - deny – запретить прохождение пакетов с указанными параметрами; - permit – разрешить прохождение пакетов с указанными параметрами. |
| no ipv6 access-list <i>access_list</i> | | Удаление стандартного списка ACL для адресации IPv6. |
| ipv6 access-list extended <i>access_list</i> | | Создание нового расширенного списка ACL для адресации IPv6 и вход в режим его конфигурации (если список с данным именем еще не создан) либо вход в режим конфигурации ранее созданного списка. |
| no ipv6 access-list extended <i>access_list</i> | | Удаление расширенного списка ACL для адресации IPv6. |
| mac access-list extended <i>access_list</i> | | Создание нового списка ACL на базе MAC-адресации и вход в режим его конфигурации (если список с данным именем еще не создан) либо вход в режим конфигурации ранее созданного списка. |
| no mac access-list extended <i>access_list</i> | | Удаление списка ACL на базе MAC-адресации. |
| time-range <i>time_name</i> | <i>time_name</i> : (0..32) символа | Вход в режим конфигурации time-range и определение временных интервалов для списка доступа. - <i>time_name</i> – имя профиля настроек time-range. |
| no time-range <i>time_name</i> | | Удаление заданной конфигурации time-range. |

Для того чтобы активизировать список ACL, необходимо связать его с интерфейсом. Интерфейсом, использующим список, может быть либо интерфейс Ethernet, либо группа портов.

Команды режима конфигурации интерфейса Ethernet, VLAN, группы портов

Командная строка в режиме конфигурации интерфейса Ethernet, VLAN, группы портов имеет вид:

```
console(config-if) #
```

Таблица 265 – Команда назначения списка ACL-интерфейсу

| Команда | Значение/Значение по умолчанию | Действие |
|---|---|---|
| service-acl input <i>access_list</i> | <i>access_list</i> : (0..32) символа | В настройках определённого физического интерфейса команда привязывает указанный список к данному интерфейсу. – глобальная настройка для применения опции 82. <input checked="" type="checkbox"/> Под действие ACL, назначаемого на interface vlan, попадает не только маршрутизируемый трафик, но и трафик внутри сети. <input checked="" type="checkbox"/> Под действие ACL, назначаемого на interface vlan, попадает весь входящий в порты трафик в данной VLAN. |
| no service-acl input | | Удаление списка с интерфейса. |

Команды режима Privileged EXEC

Командная строка в режиме Privileged EXEC имеет вид:

```
console#
```

Таблица 266 – Команды для просмотра списков ACL

| Команда | Значение/Значение по умолчанию | Действие |
|---|---|--|
| show access-lists [<i>access_list</i>] | <i>access_list</i> : (0..32) символа | Показывает списки ACL, созданные на коммутаторе. |
| show access-lists time-range-active [<i>access_list</i>] | | Показывает списки ACL, созданные на коммутаторе, которые в настоящее время являются активными. |

| | | |
|--|---|---|
| show interfaces access-lists [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group vlan vlan_id] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128); vlan_id: (1..4094) | Показывает списки ACL, назначенные интерфейсам. |
| clear access-lists counters [tengigabitethernet te_port hundredgigabitethernet hu_port port-channel group vlan vlan_id] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128); vlan_id: (1..4094) | Обнулить все счетчики списков ACL либо счетчики для списков ACL заданного интерфейса. |
| show interfaces access-lists trapped packets [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group vlan vlan_id] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128); vlan_id: (1..4094) | Показывает счетчики списков доступа. |

Команды режима EXEC

Командная строка в режиме EXEC имеет вид:

```
console#
```

Таблица 267 – Команды для просмотра списков ACL

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|------------------------------------|---------------------------------------|-------------------------------------|
| show time-range [time_name] | - | Показывает конфигурацию time-range. |

5.27.1 Конфигурация ACL на базе IPv4

В данном разделе приведены значения и описания основных параметров, используемых в составе команд настройки списков ACL, основанных на адресации IPv4. Создание и вход в режим редактирования списков ACL, основанных на адресации IPv4, осуществляется по команде: **ip access-list extended access-list**. Например, для создания списка ACL под названием EltexAL необходимо выполнить следующие команды:

```
console#
console# configure
console(config)# ip access-list extended EltexAL
console(config-ip-al)#
```

Таблица 268 – Основные параметры, используемые в командах

| <i>Параметр</i> | <i>Значение</i> | <i>Действие</i> |
|-----------------|----------------------|--|
| permit | Действие 'разрешить' | Создает разрешающее правило фильтрации в списке ACL. |
| deny | Действие 'запретить' | Создает запрещающее правило фильтрации в списке ACL. |

| | | |
|-----------------------------|-------------------------------------|---|
| <i>protocol</i> | Протокол | Поле предназначено для указания протокола (или всех протоколов), на основе которого будет осуществляется фильтрация. При выборе протокола возможны следующие варианты: icmp, igmp, ip, tcp, egr, igr, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis, ipip, либо числовое значение протокола, в диапазоне (0 – 255). Для соответствия любому протоколу используется значение IP . |
| <i>source</i> | Адрес источника | Определяет IP-адрес источника пакета. |
| <i>source_wildcard</i> | Wildcard-маска адреса источника | Битовая маска, применяемая к IP-адресу источника пакета. Маска определяет биты IP-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Например, используя маску, можно определить для правила фильтрации IP-сеть. Чтобы добавить в правило фильтрации IP-сеть 195.165.0.0, необходимо задать значение маски 0.0.255.255, то есть согласно данной маске последние 16 бит IP-адреса будут игнорироваться. |
| <i>destination</i> | Адрес назначения | Определяет IP-адрес назначения пакета. |
| <i>destination_wildcard</i> | Wildcard-маска адреса назначения | Битовая маска, применяемая к IP-адресу назначения пакета. Маска определяет биты IP-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Маска используется аналогично маске <i>source_wildcard</i> . |
| <i>vlan</i> | Идентификатор Vlan | Определяет Vlan, для которого будет применяться правило. |
| <i>dscp</i> | Поле DSCP в заголовке L3 | Определяет значение DSCP-поля diffserv. Возможные коды сообщений поля dscp : (0 – 63). |
| <i>precedence</i> | Приоритет IP | Определяет приоритет IP-трафика: (0-7). |
| <i>time_name</i> | Имя профиля конфигурации time-range | Определяет конфигурацию временных интервалов. |
| <i>icmp_type</i> | - | Тип сообщений протокола ICMP, используемый для фильтрации ICMP-пакетов. Возможные типы сообщений поля <i>icmp_type</i> : echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain_name-request, domain_name-reply, skip, photuris, либо числовое значение типа сообщения, в диапазоне (0 – 255). |
| <i>icmp_code</i> | Код сообщения протокола ICMP | Код сообщений протокола ICMP, используемый для фильтрации ICMP-пакетов. Возможные коды сообщений поля <i>icmp_code</i> : (0 – 255). |
| <i>igmp_type</i> | Тип сообщения протокола IGMP | Тип сообщений протокола IGMP, используемый для фильтрации пакетов IGMP. Возможные типы сообщений поля <i>igmp_type</i> : host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3, либо числовое значение типа сообщения, в диапазоне (0 – 255). |
| <i>destination_port</i> | UDP/TCP-порт назначения | Возможные значения поля TCP-порта: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110), syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80); Для UDP-порта: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). Либо числовое значение (0 – 65535). |
| <i>source_port</i> | UDP/TCP-порт источника | |

| | | |
|-------------------------|---|--|
| <i>list_of_flags</i> | Флаги протокола TCP | Если для условия фильтрации флаг должен быть установлен, то перед ним ставится знак «+», если не должен быть установлен, то «-». Возможные варианты флагов: +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn и -fin . При использовании нескольких флагов в условии фильтрации, флаги объединяются в одну строку без пробелов, например: +fin-ack . |
| disable_port | Отключение порта | Выключает порт, с которого был принят пакет, удовлетворяющий условиям любой из команд запрета deny , в составе которой было описано поле. |
| log_input | Отправка сообщений | Включает отправку информационных сообщений в системный журнал при получении пакета, который соответствует записи. |
| <i>offset_list_name</i> | Наименование списка шаблонов пользователя | Задаёт использование списка шаблонов пользователя для распознавания пакетов. Для каждого списка ACL может быть определен свой список шаблонов. |
| <i>ace-priority</i> | Приоритет записи | Индекс задаёт положение правила в списке и его приоритет. Чем меньше индекс – тем приоритетнее правило. Диапазон допустимых значений (1..2147483647). |



Для выбора всего диапазона параметров, кроме **dscp** и **IP-precedence**, используется параметр «**any**».



Если пакет попадает под критерий правила в ACL, то над ним выполняется действие этого правила (**permit/deny**). Дальнейшая проверка не производится.



Если на интерфейс назначены IP и MAC ACL, то первоначально пакет будет проверен на соответствие правилам IP ACL, потом MAC ACL (в случае, если не попадёт под действие ни одного из правил IP ACL).



Если после проверки на соответствие правилам IP или MAC ACL (когда 1 ACL назначен на интерфейс) или IP и MAC ACL (когда 2 ACL назначены на интерфейс) пакет не попал под действие ни одного из правил, то над данным пакетом будет применено действие "deny any any".

Таблица 269 – Команды, используемые для настройки ACL-списков на основе IP-адресации

| Команда | Действие |
|---|--|
| permit protocol {any source source_wildcard} {any destination destination_wildcard} [dscp dscp precedence precedence] [time-range time_name] [ace-priority index] | Добавляет разрешающую запись фильтрации для протокола. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором. |
| no permit protocol {any source source_wildcard} {any destination destination_wildcard} [dscp dscp precedence precedence] [time-range time_name] | Удаляет созданную ранее запись. |
| permit ip {any source_ip source_ip_wildcard} {any destination_ip destination_ip_wildcard} [dscp dscp precedence precedence] [time-range range_name] [ace priority index] | Добавляет разрешающую запись фильтрации для протокола IP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором. |
| no permit ip {any source_ip source_ip_wildcard} {any destination_ip destination_ip_wildcard} [dscp dscp precedence precedence] [time-range range_name] | Удаляет созданную ранее запись. |
| permit icmp {any source source_wildcard} {any destination destination_wildcard} {any icmp_type} {any icmp_code} [dscp dscp ip-precedence precedence] [time-range time_name] [ace-priority index] [offset-list offset_list_name] [vlan vlan_id] | Добавляет разрешающую запись фильтрации для протокола ICMP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором. |
| no permit icmp {any source source_wildcard} {any destination destination_wildcard} {any icmp_type} {any icmp_code} [dscp dscp ip-precedence precedence] [time-range time_name] [offset-list offset_list_name] [vlan vlan_id] | Удаляет созданную ранее запись. |

| | |
|--|--|
| permit igmp {any source source_wildcard} {any destination destination_wildcard} [igmp_type] [dscp dscp precedence precedence] [time-range time_name] [ace-priority index] | Добавляет разрешающую запись фильтрации для протокола IGMP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором. |
| no permit igmp {any source source_wildcard} {any destination destination_wildcard} [igmp_type] [dscp dscp precedence precedence] [time-range time_name] | Удаляет созданную ранее запись. |
| permit tcp {any source source_wildcard} {any source_port} {any destination destination_wildcard} {any destination_port} [dscp dscp precedence precedence] [match-all list_of_flags] [time-range time_name] [ace-priority index] | Добавляет разрешающую запись фильтрации для протокола TCP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором. |
| no permit tcp {any source source_wildcard} {any source_port} {any destination destination_wildcard} {any destination_port} [dscp dscp precedence precedence] [match-all list_of_flags] [time-range time_name] | Удаляет созданную ранее запись. |
| permit udp {any source source_wildcard} {any source_port} {any destination destination_wildcard} {any destination_port} [dscp dscp precedence precedence] [time-range time_name] [ace-priority index] | Добавляет разрешающую запись фильтрации для протокола UDP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором. |
| no permit udp {any source source_wildcard} {any source_port} {any destination destination_wildcard} {any destination_port} [dscp dscp precedence precedence] [time-range time_name] | Удаляет созданную ранее запись. |
| deny protocol {any source source_wildcard} {any destination destination_wildcard} [dscp dscp precedence precedence] [time-range time_name] [disable-port log-input] [ace-priority index] | Добавляет запрещающую запись фильтрации для протокола. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова disable-port физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова log-input будет отправлено сообщение в системный журнал. |
| no deny protocol {any source source_wildcard} {any destination destination_wildcard} [dscp dscp precedence precedence] [time-range time_name] [disable-port log-input] | Удаляет созданную ранее запись. |
| deny ip {any source_ip source_ip_wildcard} {any destination_ip destination_ip_wildcard} [dscp dscp precedence precedence] [time-range range_name] [disable-port log-input] [ace-priority index] | Добавляет запрещающую запись фильтрации для протокола IP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова disable-port физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова log-input будет отправлено сообщение в системный журнал. |
| no deny ip {any source_ip source_ip_wildcard} {any destination_ip destination_ip_wildcard} [dscp dscp precedence precedence] [time-range range_name] [disable-port log-input] | Удаляет созданную ранее запись. |
| deny icmp {any source source_wildcard} {any destination destination_wildcard} {any icmp_type} {any icmp_code} [dscp dscp precedence precedence] [time-range time_name] [disable-port log-input] [ace-priority index] | Добавляет запрещающую запись фильтрации для протокола ICMP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова disable-port физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова log-input будет отправлено сообщение в системный журнал. |
| no deny icmp {any source source_wildcard} {any destination destination_wildcard} {any icmp_type} {any icmp_code} [dscp dscp precedence precedence] [time-range time_name] [disable-port log-input] | Удаляет созданную ранее запись. |
| deny igmp {any source source_wildcard} {any destination destination_wildcard} [igmp_type] [dscp dscp precedence precedence] [time-range time_name] [ace-priority index] [disable-port log-input] | Добавляет запрещающую запись фильтрации для протокола IGMP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова disable-port физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова log-input будет отправлено сообщение в системный журнал. |

| | |
|---|--|
| no deny igmp {any source source_wildcard} {any destination destination_wildcard} [igmp_type] [dscp dscp precedence precedence] [time-range time_name] [disable-port log-input] | Удаляет созданную ранее запись. |
| deny tcp {any source source_wildcard} {any source_port} {any destination destination_wildcard} {any destination_port} [dscp dscp precedence precedence] [match-all list_of_flags] [time-range time_name] [ace-priority index] [disable-port log-input] | Добавляет запрещающую запись фильтрации для протокола TCP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова disable-port физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова log-input будет отправлено сообщение в системный журнал. |
| no deny tcp {any source source_wildcard} {any source_port} {any destination destination_wildcard} {any destination_port} [dscp dscp precedence precedence] [match-all list_of_flags] [time-range time_name] [disable-port log-input] | Удаляет созданную ранее запись. |
| deny udp {any source source_wildcard} {any source_port} {any destination destination_wildcard} {any destination_port} [dscp dscp precedence precedence] [time-range time_name] [ace-priority index] [disable-port log-input] | Добавляет запрещающую запись фильтрации для протокола UDP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова disable-port физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова log-input будет отправлено сообщение в системный журнал. |
| no deny udp {any source source_wildcard} {any source_port} {any destination destination_wildcard} {any destination_port} [dscp dscp precedence precedence] [time-range time_name] [disable-port log-input] | Удаляет созданную ранее запись. |
| offset-list offset_list_name {offset_base offset mask value} ... | Создаёт список шаблонов пользователя с именем <i>name</i> . Имя может включать от 1 до 32 символов. В одной команде может содержаться до тринадцати шаблонов в зависимости от выбранного режима настройки списков доступа (команда set system mode), включающих следующие параметры: - <i>offset_base</i> – базовое смещение. Возможные значения: I3 – начало смещения с начала IP-заголовка; I4 – начало смещения с конца IP-заголовка. - <i>offset</i> – смещение байта данных в пределах пакета. Базовое смещение принимается за начало отсчета; - <i>mask</i> – маска. В анализе пакета принимают участие только те разряды байта, для которых в соответствующих разрядах маски задана '0'; - <i>value</i> – искомое значение. |
| no offset-list offset_list_name | Удаляет созданный ранее список. |

5.27.2 Конфигурация ACL на базе IPv6

В данном разделе приведены значения и описания основных параметров, используемых в составе команд настройки списков ACL, основанных на адресации IPv6.

Создание и вход в режим редактирования списков ACL, основанных на адресации IPv6, осуществляется по команде: **ipv6 access-list** *access-list*. Например, для создания списка ACL под названием MESipv6 необходимо выполнить следующие команды:

```
console#
console# configure
console(config)# ipv6 access-list MESipv6
console(config-ipv6-al)#
```

Таблица 270 – Основные параметры, используемые в командах

| Параметр | Значение | Действие |
|---------------|--------------------|--|
| permit | Действие разрешить | Создает разрешающее правило фильтрации в списке ACL. |
| deny | Действие запретить | Создает запрещающее правило фильтрации в списке ACL. |

| | | |
|---|---|---|
| <i>protocol</i> | Протокол | Поле предназначено для указания протокола (или всех протоколов), на основе которого будет осуществляется фильтрация. При выборе протокола возможны следующие варианты: icmp , tcp , udp либо числовое значение протокола – icmp (58), tcp (6), udp (17). Для соответствия любому протоколу используется значение IPv6 . |
| <i>source_prefix/length</i> | Адрес отправителя и его длина | Определяет IPv6-адрес и длину префикса сети (0-128) (количество старших бит адреса) источника пакета. |
| <i>destination_prefix/length</i> | Адрес назначения и его длина | Определяет IPv6-адрес и длину префикса сети (0-128) (количество старших бит адреса) назначения пакета. |
| <i>dscp</i> | Поле DSCP в заголовке L3 | Определяет значение DSCP-поля diffserv. Возможные коды сообщений поля dscp : (0 – 63). |
| <i>precedence</i> | Приоритет IP | Определяет приоритет IP-трафика:(0-7). |
| <i>time_name</i> | Имя профиля конфигурации time-range | Определяет конфигурацию временных интервалов. |
| <i>icmp_type</i> | Тип сообщения протокола ICMP | Используется для фильтрации ICMP-пакетов. Возможные типы и числовые значения сообщений поля icmp_type : destination-unreachable (1), packet-too-big (2), time-exceeded (3), parameter-problem (4), echo-request (128), echo-reply (129), mld-query (130), mld-report (131), mldv2-report (143), mld-done (132), router-solicitation (133), router-advertisement (134), nd-ns (135), nd-na (136). |
| <i>icmp_code</i> | Код сообщений протокола ICMP | Используется для фильтрации ICMP-пакетов. Возможные значения поля (0 – 255). |
| <i>destination_port</i> <i>source_port</i> | UDP/TCP-порт назначения UDP/TCP-порт источника | Возможные значения поля TCP-порта: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110), syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80); Для UDP-порта: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). Либо числовое значение (0 – 65535). |
| <i>list_of_flags</i> | Флаги протокола TCP | Если для условия фильтрации флаг должен быть установлен, то перед ним ставится знак «+», если не должен быть установлен, то «-». Возможные варианты флагов: +urg , +ack , +psh , +rst , +syn , +fin , -urg , -ack , -psh , -rst , -syn и -fin . |
| <i>disable-port</i> | Отключение порта | Выключает порт, с которого был принят пакет, удовлетворяющий условиям любой из команд запрета deny , в составе которой, было описано поле. |
| <i>log-input</i> | Отправка сообщений | Включает отправку информационных сообщений в системный журнал при получении пакета, который соответствует записи. |
| <i>ace-priority</i> | Индекс правила | Индекс правила в таблице, чем меньше индекс – тем приоритетнее правило: (1..2147483647). |



Для выбора всего диапазона параметров, кроме **dscp** и **IP-precedence** используется параметр «**any**».



После того, как хотя бы одна запись добавлена в список ACL, последними в список добавляются записи

permit-icmp any any nd-ns any

permit-icmp any any nd-na any

deny ipv6 any any

Две первые из них разрешают поиск соседних IPv6-устройств с помощью протокола ICMPv6, а последняя означает игнорирование всех пакетов, не удовлетворяющих условиям ACL.

Таблица 271 – Команды, используемые для настройки ACL списков на основе IPv6-адресации

| <i>Команда</i> | <i>Действие</i> |
|--|--|
| permit protocol {any source_prefix/length} {any destination_prefix/length} [dscp dscp precedence precedence] [time-range time_name] [ace-priority index] | Добавляет разрешающую запись фильтрации для протокола. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором. |
| no permit protocol {any source_prefix/length} {any destination_prefix/length} [dscp dscp precedence precedence] [time-range time_name] | Удаляет созданную ранее запись. |
| permit icmp {any source_prefix/length} {any destination_prefix/length} {any icmp_type} {any icmp_code} [dscp dscp precedence precedence] [time-range time_name] [ace-priority index] | Добавляет разрешающую запись фильтрации для протокола ICMP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором. |
| no permit icmp {any source_prefix/length} {any destination_prefix/length} {any icmp_type} {any icmp_code} [dscp dscp precedence precedence] [time-range time_name] | Удаляет созданную ранее запись. |
| permit tcp {any source_prefix/length} {any source_port} {any destination_prefix/length} {any destination_port} [dscp dscp precedence precedence] [time-range time_name] [match-all list_of_flags] [ace-priority index] | Добавляет разрешающую запись фильтрации для протокола TCP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором. |
| no permit tcp {any source_prefix/length} {any source_port} {any destination_prefix/length} {any destination_port} [dscp dscp precedence precedence] [time-range time_name] [match-all list_of_flags] | Удаляет созданную ранее запись. |
| permit udp {any source_prefix/length} {any source_port} {any destination_prefix/length} {any destination_port} [dscp dscp precedence precedence] [time-range time_name] [ace-priority index] | Добавляет разрешающую запись фильтрации для протокола UDP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором. |
| no permit udp {any source_prefix/length} {any source_port} {any destination_prefix/length} {any destination_port} [dscp dscp precedence precedence] [time-range time_name] | Удаляет созданную ранее запись. |
| deny protocol {any source_prefix/length} {any destination_prefix/length} [dscp dscp precedence precedence] [time-range time_name] [disable-port log-input] [ace-priority index] | Добавляет запрещающую запись фильтрации для протокола. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова disable-port физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова log-input будет отправлено сообщение в системный журнал. |
| no deny protocol {any source_prefix/length} {any destination_prefix/length} [dscp dscp precedence precedence] [time-range time_name] [disable-port log-input] | Удаляет созданную ранее запись. |
| deny icmp {any source_prefix/length} {any destination_prefix/length} {any icmp_type} {any icmp_code} [dscp dscp precedence precedence] [time-range time_name] [disable-port log-input] [ace-priority index] | Добавляет запрещающую запись фильтрации для протокола ICMP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова disable-port физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова log-input будет отправлено сообщение в системный журнал. |
| no deny icmp {any source_prefix/length} {any destination_prefix/length} {any icmp_type} {any icmp_code} [dscp dscp precedence precedence] [time-range time_name] [disable-port log-input] | Удаляет созданную ранее запись. |
| deny tcp {any source_prefix/length} {any source_port} {any destination_prefix/length} {any destination_port} [dscp dscp precedence precedence] [match-all list_of_flags] [time-range time_name] [disable-port log-input] [ace-priority index] | Добавляет запрещающую запись фильтрации для протокола TCP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова disable-port физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова log-input будет отправлено сообщение в системный журнал. |

| | |
|--|--|
| no deny tcp {any source_prefix/length} {any source_port} {any destination_prefix/length} {any destination_port} [dscp dscp precedence precedence] [match-all list_of_flags] [time-range time_name] [disable-port log-input] | Удаляет созданную ранее запись. |
| deny udp {any source_prefix/length} {any source_port} {any destination_prefix/length} {any destination_port} [dscp dscp precedence precedence] [match-all list_of_flags] [time-range time_name] [disable-port log-input] [ace-priority index] | Добавляет запрещающую запись фильтрации для протокола UDP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова disable-port физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова log-input будет отправлено сообщение в системный журнал. |
| no deny udp {any source_prefix/length} {any source_port} {any destination_prefix/length} {any destination_port} [dscp dscp precedence precedence] [match-all list_of_flags] [time-range time_name] [disable-port log-input] | Удаляет созданную ранее запись. |
| offset-list offset_list_name {offset_base offset mask value} ... | Создаёт список шаблонов пользователя с именем <i>name</i> . Имя может включать от 1 до 32 символов. В одной команде может содержаться до тринадцати шаблонов в зависимости от выбранного режима настройки списков доступа (команда set system mode), включающих следующие параметры: - <i>offset_base</i> – базовое смещение. Возможные значения: I3 – начало смещения с начала IPv6-заголовка; I4 – начало смещения с конца IPv6-заголовка. - <i>offset</i> – смещение байта данных в пределах пакета. Базовое смещение принимается за начало отсчета; - <i>mask</i> – маска. В анализе пакета принимают участие только те разряды байта, для которых в соответствующих разрядах маски задана '0'; - <i>value</i> – искомое значение. |
| no offset-list offset_list_name | Удаляет созданный ранее список. |

5.27.3 Конфигурация ACL на базе MAC

В данном разделе приведены значения и описания основных параметров, используемых в составе команд настройки списков ACL, основанных на MAC-адресации.

Создание и вход в режим редактирования списков ACL, основанных на MAC-адресации, осуществляется по команде: **mac access-list extended** *access-list*.

Например, для создания списка ACL под названием MESmac необходимо выполнить следующие команды:

```
console#
console# configure
console(config)# mac access-list extended MESmac
console(config-mac-al)#
```

Таблица 272 – Основные параметры, используемые в командах

| Параметр | Значение | Действие |
|---------------|--------------------|--|
| permit | Действие разрешить | Создает разрешающее правило фильтрации в списке ACL. |
| deny | Действие запретить | Создает запрещающее правило фильтрации в списке ACL. |
| <i>source</i> | Адрес отправителя | Определяет MAC-адрес источника пакета. |

| | | |
|-----------------------------|--|--|
| <i>source_wildcard</i> | wildcard-маска адреса источника | Маска определяет биты MAC-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Например, используя маску, можно определить для правила фильтрации диапазона MAC-адресов. Чтобы добавить в правило фильтрации все MAC-адреса, начинающиеся на 00:00:02:AA.xx.xx, необходимо задать значение маски 0.0.0.0.FF.FF, то есть, согласно данной маске, последние 32 бита MAC-адреса будут не важны для анализа. |
| <i>destination</i> | Адрес назначения | Определяет MAC-адрес назначения пакета. |
| <i>destination_wildcard</i> | wildcard-маска адреса назначения | Маска определяет биты MAC-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Маска используется аналогично маске <i>source_wildcard</i> . |
| <i>vlan_id</i> | <i>vlan_id</i> : (0..4095) | Подсеть VLAN фильтруемых пакетов. |
| <i>cos</i> | <i>cos</i> : (0..7) | Класс обслуживания (CoS) фильтруемых пакетов. |
| <i>cos_wildcard</i> | wildcard-маска адреса обслуживания (CoS) фильтруемых пакетов | Маска определяет биты CoS, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Например, чтобы использовать в правиле фильтрации CoS 6 и 7, необходимо в поле CoS указать значение 6, либо 7, а в поле маски значение 1 (7 в двоичном представлении – 111, 1 – 001, получается, что последний бит будет игнорироваться, то есть CoS может быть либо 110 (6), либо 111 (7)). |
| <i>eth_type</i> | <i>eth_type</i> : (0..0xFFFF) | Ethernet-тип фильтруемых пакетов в шестнадцатеричной записи. |
| disable-port | - | Выключает порт, с которого был принят пакет, удовлетворяющий условиям команды запрета deny . |
| log-input | Отправка сообщений | Включает отправку информационных сообщений в системный журнал при получении пакета, который соответствует записи. |
| <i>time_name</i> | Имя профиля конфигурации <i>time-range</i> | Определяет конфигурацию временных интервалов. |
| <i>offset_list_name</i> | Побайтовое смещение от ключевой точки | Задаёт использование списка шаблонов пользователя для распознавания пакетов. Для каждого списка ACL может быть определен свой список шаблонов. |
| <i>ace-priority</i> | Индекс правила | Индекс правила в таблице, чем меньше индекс – тем приоритетнее правило 1-2147483647. |



Для выбора всего диапазона параметров, кроме **dscp** и **IP-precedence**, используется параметр «**any**».



Если пакет попадает под критерий правила в ACL, то над ним выполняется действие этого правила (**permit/deny**). Дальнейшая проверка не производится.

Если на интерфейс назначены IP и MAC ACL, то первоначально пакет будет проверен на соответствие правилам IP ACL, потом MAC ACL (в случае, если не попадет под действие ни одного из правил IP ACL).

Если после проверки на соответствие правилам IP или MAC ACL (когда 1 ACL назначен на интерфейс) или IP и MAC ACL (когда 2 ACL назначены на интерфейс) пакет не попал под действие ни одного из правил, то над данным пакетом будет применено действие "deny any any".

Таблица 273 – Команды, используемые для настройки ACL-списков на основе MAC-адресации

| Команда | Действие |
|--|---|
| permit { any <i>source source-wildcard</i> } { any <i>destination destination_wildcard</i> } [vlan <i>vlan_id</i>] [cos <i>cos cos_wildcard</i>] [<i>eth_type</i>] [time-range <i>time_name</i>] [ace-priority <i>index</i>] [offset-list <i>offset_list_name</i>] | Добавляет разрешающую запись фильтрации. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором. |

| | |
|---|---|
| no permit {any source source-wildcard} {any destination destination_wildcard} [vlan vlan_id] [cos cos cos_wildcard] [eth_type] [time-range time_name] [offset-list offset_list_name] | Удаляет созданную ранее запись. |
| deny {any source source-wildcard} {any destination destination_wildcard} [vlan vlan_id] [cos cos cos_wildcard] [eth_type] [time-range time_name] [disable-port log-input] [ace-priorityindex] [offset-list offset_list_name] | Добавляет запрещающую запись фильтрации. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова disable-port , физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова <i>log-input</i> будет отправлено сообщение в системный журнал. |
| no deny {any source source-wildcard} {any destination destination_wildcard} [vlan vlan_id] [cos cos cos_wildcard] [eth_type] [time-range time_name] [disable-port log-input] [offset-list offset_list_name] | Удаляет созданную ранее запись. |
| offset-list offset_list_name {offset_base offset mask value} ... | Создаёт список шаблонов пользователя с именем <i>name</i> . Имя может включать от 1 до 32 символов. В одной команде может содержаться до тринадцати шаблонов в зависимости от выбранного режима настройки списков доступа (команда set system mode), включающих следующие параметры: - <i>offset_base</i> – базовое смещение. Возможные значения: I2 – начало смещения от EtherType; outer-tag – начало смещения от STAG; inner-tag – начало смещения от STAG; src-mac – начало смещения с MAC-адреса источника; dst-mac – начало смещения с MAC-адреса назначения. - <i>offset</i> – смещение байта данных в пределах пакета. Базовое смещение принимается за начало отсчета; - <i>mask</i> – маска. В анализе пакета принимают участие только те разряды байта, для которых в соответствующих разрядах маски задана '0'; - <i>value</i> – искомое значение. |
| no offset-list offset_list_name | Удаляет созданный ранее список. |

5.28 Конфигурация защиты от DoS-атак

Данный класс команд позволяет блокировать некоторые распространенные классы DoS-атак.

Команды режима глобальной конфигурации

Командная строка в режиме глобальной конфигурации имеет вид:

```
console (config)#
```

Таблица 274 – Команды для настройки защиты от DoS-атак

| Команда | Значение/Значение по умолчанию | Действие |
|---|--------------------------------|---|
| security-suite deny martian-addresses [reserved] {add remove} ip_address | ip_address: ip-адрес | Запрещает прохождение кадров с недопустимыми («марсианскими») IP-адресами источника (loopback, broadcast, multicast). |
| security-suite deny syn-fin | -/включено | Отбрасывает пакеты TCP с одновременно установленными SYN- и FIN- флагами. |
| no security-suite deny syn-fin | | Выключает функцию отбрасывания пакетов TCP с одновременно установленными SYN- и FIN- флагами. |

| | | |
|---|----------------------|--|
| security-suite dos protect {add remove} {stacheldraht invasor-trojan back-orifice-trojan} | - | Запрещает/разрешает прохождение определенных типов трафика, характерных для вредоносных программ: - stacheldraht – отбрасывает TCP-пакеты с портом источника равным 16660; - invasor-trojan – отбрасывает TCP-пакеты с портом назначения равным 2140 и портом источника 1024; - back-orifice-trojan – отбрасывает UDP-пакеты с портом назначения 31337 и портом источника равным 1024. |
| security-suite enable [global-rules-only] | -/выключено | Включает класс команд security-suite. - global-rules-only — отключает класс команд security-suite на интерфейсах. Не влияет на работу команды security-suite deny syn-fin. |
| no security-suite enable | | Отключает класс команд security-suite. |
| security-suite syn protection mode {block report disabled} | -/block | Настраивает режим защиты от SYN-атак: - block — отбрасывает предназначенные устройству TCP-пакеты с установленным флагом SYN и формирует предупреждающее сообщение; - report — формирует предупреждающее сообщение при приходе предназначенного устройству TCP-пакета с установленным флагом SYN; - disable — отключает защиту. |
| no security-suite syn protection mode | | Настраивает режим по умолчанию. |
| security-suite syn protection recovery sec | sec: (10..600) / 60 | Определяет интервал, по истечении которого будет разблокирован ранее заблокированный источник SYN-атаки. |
| no security-suite syn protection recovery | | Устанавливает значение по умолчанию. |
| security-suite syn protection threshold rate | rate: (20..200) / 80 | Определяет скорость (количество пакетов в секунду) от конкретного источника, при которой этот источник будет идентифицирован как атакующий. |
| no security-suite syn protection threshold | | Устанавливает значение по умолчанию. |
| security-suite syn protection statistics | -/выключено | Включает ведение статистики SYN-атак. |
| no security-suite syn protection statistics | | Выключает ведение статистики SYN-атак. |

Команды режима конфигурации интерфейса Ethernet, группы портов

Командная строка в режиме конфигурации интерфейса Ethernet, группы портов имеет вид:

```
console (config-if)#
```

Таблица 275 – Команда конфигурации защиты от DoS-атак для интерфейсов


| Команда | Значение/Значение по умолчанию | Действие |
|---|---|--|
| security-suite deny {fragmented icmp syn} {add remove} {any ip_address [mask]} | ip_address: IP-адрес; mask: маска в формате IP-адреса или префикса | Создает правило, запрещающее прохождение трафика, соответствующего критериям. - fragmented – фрагментированные пакеты; - icmp – ICMP-трафик; - syn – syn-пакеты. |
| no security-suite deny {fragmented icmp syn} | | Удаляет запрещающее правило. |
| security-suite dos syn-attack rate {any ip_address [mask]} | rate: (199..2000) пакетов в секунду; ip_address: – IP-адрес; | Задает порог syn-запросов на определенный IP-адрес/сеть, при превышении которого лишние кадры будут отбрасываться. |
| no security-suite dos syn-attack {any ip_address [mask]} | mask: маска в формате IP-адреса или префикса | Восстанавливает значение по умолчанию. |

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 276 – Команда режима Privileged EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---|--|
| show security-suite configuration | - | Отображает настройки защиты от DoS-атак. |
| show security-suite syn protection {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group} | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); hu_port: (1..8/0/1..32); group: (1..48) | Отображает настройки защиты от SYN-атак и оперативное состояние интерфейсов. |
| show security-suite syn protection statistics [detailed] [source-ip ip_address interface {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group}] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..48) | Отображает настройки статистики защиты от SYN-атак и информацию об источниках атаки. - detailed — отображает дополнительную информацию об источнике атаки; - source-ip — отображает информацию для указанного ip-адреса источника; - interface — отображает информацию для указанного интерфейса.  В статистике сохраняется информация о 512 последних источниках атак. |
| clear security-suite syn protection statistics | - | Очищает статистику об источниках SYN-атак. |

5.29 Качество обслуживания – QoS

По умолчанию на всех портах коммутатора используется организация очереди пакетов по методу FIFO: первый пришел – первый ушел (First In – First Out). Во время интенсивной передачи трафика при использовании данного метода могут возникнуть проблемы, поскольку устройством игнорируются все пакеты, не вошедшие в буфер очереди FIFO, и соответственно теряются безвозвратно. Решает данную проблему метод, организующий очереди по приоритету трафика. Механизм QoS (Quality of service – качество обслуживания), реализованный в коммутаторах, позволяет организовать восемь очередей приоритета пакетов в зависимости от типа передаваемых данных.



5.29.1 Настройка QoS

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 277 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|---|--|--|
| <i>ip tx-dscp value</i> | value: (0..63)/56 | Установить значение поля DSCP для IP-пакетов, формируемых центральным процессором. |
| no ip tx-dscp | | Установить значение по умолчанию. |
| <i>ipv6 tx-user-priority value</i> | value: (0..7)/7 | Установить значение поля DSCP для пакетов, формируемых центральным процессором. |
| no ipv6 tx-user-priority | | Установить значение по умолчанию. |
| <i>ip tx-user-priority value</i> | value: (0..7)/7 | Установить значение поля CoS для тегированных пакетов, формируемых центральным процессором. |
| no ip tx-user-priority | | Установить значение по умолчанию. |
| qos [basic advanced [ports-trusted ports-not-trusted]] | -/basic | Разрешает коммутатору использовать QoS. - basic – базовый режим QoS; - advanced – расширенный режим конфигурации QoS, включающий полный перечень команд настройки QoS; - ports-trusted – в данном подрежиме пакеты направляются в выходную очередь на основании полей в этих пакетах; - ports-not-trusted – в данном подрежиме все пакеты направляются в очередь, которой соответствует cos=0 (соответствие можно посмотреть командой «show qos interface queuing»), для отправки в другие очереди требуется назначить на входной интерфейс стратегию классификации трафика (policy-map). Значения dscp не учитываются при выборе выходной очереди в этом подрежиме. |
| qos advanced-mode trust {cos dscp cos-dscp} | -/отключен | Установить метод доверия на портах при работе в режиме расширенного конфигурации QoS и подрежиме ports-trusted. - cos – порт доверяет значению 802.1p User priority; - dscp – порт доверяет значению DSCP в IPv4/IPv6-пакетах; - cos-dscp – порт доверяет обоим уровням, однако DSCP имеет приоритет над 802.1p. |
| no qos advanced-mode trust | | Устанавливает метод по умолчанию. |
| class-map class_map_name [match-all match-any] | class_map_name: (1..32) символов; По умолчанию используется опция match-all | 1. Создает список критериев классификации трафика. 2. Входит в режим редактирования списка критериев классификации трафика. - match-all – все критерии данного списка должны быть выполнены; - match-any – один, любой критерий данного списка должен быть выполнен.  В списке критериев может быть одно или два правила. Если правила два, и оба они указывают на разные типы ACL (IP, MAC), то классификация будет осуществляться по первому в списке верному правилу.  Действует только для режима qos advanced. |
| no class-map class_map_name | | Удаляет список критериев классификации трафика. |
| policy-map policy_map_name | policy_map_name: (1..32) символов | 1. Создает стратегию классификации трафика. 2. Входит в режим редактирования стратегии классификации трафика.  В одном направлении поддерживается только одна стратегия классификации трафика. По умолчанию policy-map устанавливает DSCP = 0 для IP-пакетов и CoS = 0 для тегированных пакетов.  Действует только для режима qos advanced. |
| no policy-map policy_map_name | | Удаляет правило классификации трафика. |

| | | |
|--|--|--|
| <p>qos aggregate-policer <i>aggregate_policer_name</i> <i>committed_rate_kbps</i> <i>excess_burst_byte</i> [exceed-action {drop policed-dscp-transmit [peak peak_rate_kbps <i>peak_burst_byte</i> [violateaction {drop policed-dscp-transmit}]}}]</p> | <p>aggregate_policer_name: (1..32) символа; committed_rate_kbps: (3..100000000) кбит/с; excess_burst_byte: (3000..268431360) байт; peak_rate_kbps: (3..100000000) кбит/с; peak_burst_byte: (3000..268431360) байт</p> | <p>Определяет шаблон настроек, который позволяет ограничить полосу пропускания канала. При работе с полосой пропускания используется алгоритм маркированной «корзины». Задачей алгоритма является принятие решения: передать пакет или отбросить. Параметрами алгоритма являются скорость поступления (CIR) маркеров в «корзину» и объём (CBS) «корзины».</p> <ul style="list-style-type: none"> - <i>committed-rate-kbps</i> – среднее значение скорости трафика. Данная скорость гарантируется при передаче информации; - <i>committed-burst-byte</i> – размер сдерживающего порога в байтах; - drop – пакет будет отброшен, когда «корзина» переполнится; - policed-dscp-transmit – при переполнении «корзины» значение DSCP будет переопределено; - peak – установить пороговое значение скорости трафика с переопределёнными значениями DSCP; - violate-action – установить действие над пакетом после превышения порогового значения. <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Нельзя удалить шаблон настроек, если он используется в стратегии policy map, перед удалением следует удалить назначение шаблона стратегии: по police aggregate aggregate-policer-name. <input checked="" type="checkbox"/> Действует только для режима qos advanced. <input checked="" type="checkbox"/> Параметр policed-dscp-transmit позволяет при превышении значения committed_rate или peak_rate передать пакет дальше, изменив в нем метку dscp, которая настраивается командой qos map policed-dscp с дополнительным аргументом violation в случае с peak_rate. При этом при превышении committed_rate и peak_rate можно настраивать разные значения dscp. |
| <p>no qos aggregate-policer <i>aggregate_policer_name</i></p> | | <p>Удаляет шаблон настроек регулирования скорости канала.</p> |
| <p>qos aggregate-policer <i>aggregate_policer_name pps</i> <i>committed_rate_pps</i> <i>committed_burst_packet</i> [exceedaction {drop policed-dscp-transmit [peak <i>peak_rate_pps</i> <i>peak_burst_packet</i> [violateaction {drop policed-dscp-transmit}]}}]</p> | <p>committed_rate_pps: (125..195312500) pps; committed_burst_packet: (1..195312500) пакетов; aggregate_policer_name: (1..32) символов; peak_rate_pps: (125..195312500) pps; peak_burst_packet: (1..195312500) пакетов</p> | <p>Определяет шаблон настроек, который позволяет ограничить полосу пропускания канала и в то же время гарантировать определенную скорость передачи данных. При работе с полосой пропускания используется алгоритм маркированной «корзины». Задачей алгоритма является принятие решения: передать пакет или отбросить. Параметрами алгоритма являются скорость поступления (CIR) маркеров в «корзину» и объём (CBS) «корзины».</p> <ul style="list-style-type: none"> - <i>committed-rate-pps</i> – среднее значение скорости трафика в pps; - <i>excess_burst_packet</i> – размер сдерживающего порога в пакетах; - drop – пакет будет отброшен, когда «корзина» переполнится; - policed-dscp-transmit – при переполнении «корзины» значение DSCP будет переопределено. <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Нельзя удалить шаблон настроек, если он используется в стратегии policy map, перед удалением следует удалить назначение шаблона стратегии: по police aggregate aggregate-policer-name. <input checked="" type="checkbox"/> Действует только для режима qos advanced. <input checked="" type="checkbox"/> Параметр policed-dscp-transmit позволяет при превышении значения committed_rate или peak_rate передать пакет дальше, изменив в нем метку dscp, которая настраивается командой qos map policed-dscp с дополнительным аргументом violation в случае с peak_rate. При этом при превышении committed_rate и peak_rate можно настраивать разные значения dscp. |

| | | |
|--|--|--|
| no qos aggregate-policer <i>aggregate_policer_name</i> | | Удаляет шаблон настроек регулирования скорости канала. |
| qos map policed-dscp <i>[dscp_list]</i> | dscp_list: (0..63) dscp_mark_down: (0..63) По умолчанию таблица повторной маркировки является пустой, то есть значения DSCP для всех входящих пакетов остаются неизменными | Заполняет таблицу перемаркировки DSCP. Для входящих пакетов с указанными значениями DSCP задает новое значение DSCP. - <i>dscp_list</i> – определяет до 8 значений DSCP, значения разделяются знаком пробела; - <i>dscp_mark_down</i> – определяет новое значение dscp; - violation – задать новое значение DSCP в пакете при превышении значения <i>peak_rate</i> . |
| no qos map policed-dscp <i>[dscp_list]</i> | | Устанавливает значения по умолчанию. |
| wrr-queue cos-map <i>queue_id</i> <i>cos1...cos8</i> | <i>queue_id</i> : (1..8); <i>cos1...cos8</i> : (0..7); Значения CoS по умолчанию для очередей: CoS = 1 – очередь 1 CoS = 2 – очередь 2 CoS = 0 – очередь 3 CoS = 3 – очередь 4 CoS = 4 – очередь 5 CoS = 5 – очередь 6 CoS = 6 – очередь 7 CoS = 7 – очередь 8 | Определяет значения CoS для очередей исходящего трафика. |
| no wrr-queue cos-map <i>[queue_id]</i> | | Устанавливает значения по умолчанию. |
| wrr-queue bandwidth <i>weight1..weight8</i> | <i>weight</i> : (0..255)/1 По умолчанию вес каждой очереди равен 1 | Присваивает вес исходящим очередям, используемый механизмом WRR (Weighted Round Robin – весовой механизм распределения нагрузки). |
| no wrr-queue bandwidth | | Устанавливает значение по умолчанию. |
| priority-queue out num-of-queues <i>number_of_queues</i> | <i>number_of_queues</i> : (0..8) По умолчанию все очереди обрабатываются по алгоритму «strict priority». | Задаёт количество приоритетных очередей. Для приоритетной очереди вес WRR будет игнорироваться. Если задается отличное от «0» значение N, то старшие N очередей будут приоритетными (не будут участвовать в WRR). Пример: 0: все очереди равноправны; 1: семь младших очередей участвуют в WRR, 8-ая не участвует; 2: шесть младших очередей участвуют в WRR, 7, 8 не участвуют. |
| no priority-queue out num-of-queues | | Устанавливает значение по умолчанию. |
| qos map enable {cos-dscp dscp-cos} | -/выключено | Использовать заданную таблицу перемаркировки для доверенных портов коммутатора. |
| no qos map enable {cos-dscp dscp-cos} | | Не использовать таблицу перемаркировки. |
| qos map dscp-cos <i>dscp_list to cos</i> | <i>dscp_list</i> : (0..63); <i>cos</i> : (0..7) | Заполнить таблицу перемаркировки DSCP. Заменяет значение DSCP на CoS. |
| no qos map dscp-cos [<i>dscp_list</i>] | | Устанавливает значение по умолчанию. |
| qos map cos-dscp <i>cos to dscp_list</i> | <i>dscp_list</i> : (0..63); <i>cos</i> : (0..7) | Заполнить таблицу перемаркировки CoS. Заменяет значение CoS на DSCP. |
| no qos map cos-dscp [<i>cos</i>] | | Устанавливает значение по умолчанию. |

| | | |
|---|---|---|
| qos map policed-dscp <i>dscp_list to dscp_mark_down</i> | dscp_list: (0..63) dscp_mark_down: (0..63) По умолчанию таблица повторной маркировки является пустой, то есть значения DSCP для всех входящих пакетов остаются неизменными | Заполняет таблицу перемаркировки DSCP. Для входящих пакетов с указанными значениями DSCP задает новое значение DSCP. - <i>dscp_list</i> – определяет до 8 значений DSCP, значения разделяются знаком пробела; - <i>dscp_mark_down</i> – определяет новое значение dscp. <input checked="" type="checkbox"/> Действует только для режима qos advanced. |
| no qos map policed-dscp <i>[dscp_list]</i> | | Устанавливает значение по умолчанию. |
| qos map dscp-queue <i>dscp_list to queue_id</i> | dscp_list: (0..63) queue_id: (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 | Устанавливает соответствие между значениями DSCP входящих пакетов и очередями. - <i>dscp_list</i> – определяет до 8 значений DSCP, значения разделяются знаком пробела. |
| no qos map dscp-queue <i>[dscp_list]</i> | | Устанавливает значения по умолчанию. |
| qos trust {cos dscp cos-dscp} | -/cos | Устанавливает режим доверия коммутатора в базовом режиме QoS (CoS или DSCP). - cos – устанавливает классификацию входящих пакетов по значениям CoS. Для нетегированных пакетов используется значение CoS по умолчанию; - dscp – устанавливает классификацию входящих пакетов по значениям DSCP. - cos-dscp – устанавливает классификацию входящих пакетов по значениям DSCP для IP-пакетов и по значениям CoS для не IP-пакетов. <input checked="" type="checkbox"/> Действует только для режима qos basic. |
| no qos trust | | Устанавливает значения по умолчанию. |
| qos dscp-mutation | - | Позволяет применить таблицу изменений dscp к совокупности dscp-доверенных портов. Использование таблицы изменений позволяет перезаписать значения dscp в IP-пакетах на новые значения. <input checked="" type="checkbox"/> Применить таблицу изменений DSCP возможно только для входящего трафика доверенных портов. <input checked="" type="checkbox"/> Действует только для режима qos basic. |
| no qos dscp-mutation | | Отменяет использование карты изменений dscp. |
| qos map dscp-mutation <i>in_dscp to out_dscp</i> | in_dscp: (0..63), out_dscp: (0..63) По умолчанию карта изменений является пустой, то есть значения DSCP для всех входящих пакетов остаются неизменными | Заполняет таблицу перемаркировки DSCP. Для входящих пакетов с указанными значениями DSCP задает новые значения DSCP. - <i>in-dscp</i> – определяет до 8 значений DSCP, значения разделяются знаком пробела; - <i>out-dscp</i> – определяет до 8 новых значений DSCP, значения разделяются знаком пробела. |
| no qos map dscp-mutation <i>[in_dscp]</i> | | Устанавливает значения по умолчанию. |
| rate-limit vlan <i>vlan_id rate burst</i> | vlan_id: (1..4094); rate: (3..100000000) кбит/с; burst: (3000..268431360) байт/128 кбайт | Устанавливает ограничение скорости для входящего трафика для заданной VLAN. - <i>vlan_id</i> – номер VLAN; - <i>rate</i> – средняя скорость трафика (CIR); - <i>burst</i> – размер сдерживающего порога (ограничение скорости) в байтах. |
| no rate-limit vlan <i>vlan_id</i> | | Снимает ограничение скорости входящего трафика. |

| | | |
|---|---|--|
| rate-limit vlan <i>vlan_id</i> pps <i>rate_pps</i> <i>burst_packet</i> | <i>vlan_id</i> : (1..4094); <i>rate_pps</i> : (125.. 195312500) pps <i>burst_pps</i> : (1..195312500) пакетов | Установить ограничение скорости для входящего трафика для заданной VLAN. - <i>vlan_id</i> – номер VLAN; - <i>rate_pps</i> – количество пакетов в секунду. - <i>burst_packet</i> – размер сдерживающего порога (ограничение скорости) в пакетах. |
| no rate-limit vlan <i>vlan_id</i> | | Снимает ограничение скорости входящего трафика. |
| traffic-limiter mode { kbps pps } | /kbps | Установить режим работы ограничения трафика. - kbps — ограничение входящих килобит в секунду; - pps — ограничение входящих пакетов в секунду; Данная команда изменяет режим работы для следующего функционала: storm-control, rate-limit, rate-limit vlan, police, qos aggregate-policer. Выбранный режим должен соответствовать настройкам ограничения трафика иначе ограничения трафика не произойдет. Например: команда storm-control unicast kbps не будет ограничивать трафик, если введена команда traffic-limiter mode pps. |

Команды режима редактирования списка критериев классификации трафика

Вид запроса командной строки режима редактирования списка критериев классификации трафика:

```
console# configure
console(config)# class-map class-map-name [match-all | match-any]
console(config-cmap)#
```

Таблица 278 – Команды режима редактирования списка критериев классификации трафика

| Команда | Значение/Значение по умолчанию | Действие |
|---|---------------------------------------|--|
| match access-group <i>acl_name</i> | <i>acl_name</i> : (1..32) символов | Добавляет критерий классификации трафика. Определяет правила фильтрации трафика по списку ACL для классификации. Действует только для режима qos advanced. |
| no match access-group <i>acl_name</i> | | Удаляет критерий классификации трафика. |

Команды режима редактирования стратегии классификации трафика

Вид запроса командной строки режима редактирования стратегии классификации трафика:

```
console# configure
console(config)# policy-map policy-map-name
console(config-pmap)#
```

Таблица 279 – Команды режима редактирования стратегии классификации трафика

| Команда | Значение/Значение по умолчанию | Действие |
|---|---|---|
| <code>class class_map_name</code> <code>[access-group acl_name]</code> | <code>class_map_name:</code> (1..32) символов; <code>acl_name:</code> (1..32) символов | <p>Определяет правило классификации трафика и входит в режим конфигурации правила классификации – <code>policy-map class</code>.</p> <p>- <code>acl_name</code> – определяет правила фильтрации трафика по списку ACL для классификации. При создании нового правила классификации опциональный параметр <code>access-group</code> обязателен.</p> <p><input checked="" type="checkbox"/> Для того чтобы использовать настройки стратегии <code>policy-map</code> для интерфейса, используйте команду <code>service-policy</code> в режиме конфигурации интерфейса.</p> <p><input checked="" type="checkbox"/> Действует только для режима <code>qos advanced</code>.</p> |
| <code>no class class_map_name</code> | | Удаляет правило классификации трафика <code>class-map</code> из стратегии <code>policy-map</code> . |

Команды режима конфигурации правила классификации

Вид запроса командной строки режима конфигурации правила классификации:

```
console# configure
console(config)# policy-map policy-map-name
console(config-pmap)# class class-map-name [access-group acl-name]
console(config-pmap-c)#
```

Таблица 280 – Команды режима конфигурации правила классификации

| Команда | Значение/Значение по умолчанию | Действие |
|---|--|--|
| <code>trust</code> | По умолчанию режим доверия не установлен | Определяет режим доверия к определенному типу трафика согласно глобальному режиму доверия. |
| <code>no trust</code> | | Устанавливает значение по умолчанию. |
| <code>set {dscp new_dscp queue queue_id cos new_cos vlan vlan_id}</code> | <code>new_dscp:</code> (0..63); <code>queue_id:</code> (1..8); <code>new_cos:</code> (0..7); <code>vlan_id:</code> (1..4094) | <p>Устанавливает новые значения для IP-пакета.</p> <p><input checked="" type="checkbox"/> Команда <code>set</code> является взаимоисключающей с командой <code>trust</code> для одной и той же стратегии <code>policy-map</code>.</p> <p><input checked="" type="checkbox"/> Стратегии <code>policy-map</code>, использующие команды <code>set</code>, <code>trust</code> или имеющий классификацию ACL, назначаются только для исходящих интерфейсов.</p> <p><input checked="" type="checkbox"/> Действует только для режима <code>qos advanced</code>.</p> |
| <code>no set</code> | | Удаляет новые значения для IP-пакета. |
| <code>redirect {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port port-channel group}</code> | <code>gi_port:</code> (1..8/0/1..48); <code>te_port:</code> (1..8/0/1..48); <code>tve_port:</code> (1..8/0/1..120); <code>hu_port:</code> (1..8/0/1..32); <code>group:</code> (1..128) | Направляет пакеты, удовлетворяющие правилу классификации трафика, в указанный порт. |
| <code>no redirect</code> | | Устанавливает значение по умолчанию. |

| | | |
|--|--|---|
| <p>police committed_rate_kbps committed_burst_byte [exceed-action {drop policed-dscp-transmit [peak peak_rate_kbps peak_burst_byte [violate-action {drop policed-dscp-transmit}]}}]</p> | <p>committed_rate_kbps: (3..12582912) кбит/с; committed_burst_byte: (3000..19173960) байт; peak_rate_kbps: (3..57982058) кбит/с; peak_burst_byte: (3000..19173960) байт</p> | <p>Позволяет ограничить полосу пропускания канала. При работе с полосой пропускания используется алгоритм маркированной «корзины». Задачей алгоритма является принятие решения: передать пакет или отбросить. Параметрами алгоритма являются скорость поступления (CIR) маркеров в «корзину» и объём (CBS) «корзины».</p> <ul style="list-style-type: none"> - <i>committed_rate_kbps</i> – среднее значение скорости трафика; - <i>committed_burst_byte</i> – размер сдерживающего порога в байтах; - drop – пакет будет отброшен, когда «корзина» переполнится; - policed-dscp-transmit – при переполнении «корзины», значение DSCP будет переопределено. - peak – установить пороговое значение скорости трафика с переопределенными значениями DSCP; - violate-action – установить действие над пакетом после превышения порогового значения. <p><input checked="" type="checkbox"/> Действует только для режима qos advanced.</p> <p><input checked="" type="checkbox"/> Параметр policed-dscp-transmit позволяет при превышении значения <i>committed-rate</i> или <i>peak_rate</i> передать пакет дальше, изменив в нем метку dscp, которая настраивается командой qos map policed-dscp с дополнительным аргументом violation в случае с <i>peak_rate</i>. При этом при превышении <i>committed_rate</i> и <i>peak_rate</i> можно настраивать разные значения dscp.</p> |
| <p>police aggregate <i>aggregate_policer_name</i></p> | | <p>Назначает правилу классификации трафика шаблон настроек, который позволяет ограничить полосу пропускания канала.</p> <p><input checked="" type="checkbox"/> Действует только для режима qos advanced.</p> |
| <p>no police</p> | | <p>Удаляет шаблон настроек регулирования скорости канала из правила классификации трафика.</p> |
| <p>police pps committed_rate_pps committed_burst_packet [exceed-action {drop policed-dscp-transmit [peak peak_rate_pps peak_burst_packet [violate-action {drop policed-dscp-transmit}]}}]</p> | <p>committed_rate_pps: (125.. 19531250) pps; committed_burst_packet: (1.. 19531250) пакетов; peak_rate_pps: (125..19531250) pps; peak_burst_packet: (1..19531250) пакетов</p> | <p>Позволяет ограничить полосу пропускания канала. При работе с полосой пропускания используется алгоритм маркированной «корзины». Задачей алгоритма является принятие решения: передать пакет или отбросить. Параметрами алгоритма являются скорость поступления (CIR) маркеров в «корзину» и объём (CBS) «корзины».</p> <ul style="list-style-type: none"> - <i>committed_rate_pps</i> – среднее значение скорости трафика в pps; - <i>committed_burst_packet</i> – размер сдерживающего порога в байтах; - drop – пакет будет отброшен, когда «корзина» переполнится; - policed-dscp-transmit – при переполнении «корзины», значение DSCP будет переопределено. - peak – установить пороговое значение скорости трафика с переопределенными значениями DSCP; - violate-action – установить действие над пакетом после превышения порогового значения. <p><input checked="" type="checkbox"/> Действует только для режима qos advanced.</p> <p><input checked="" type="checkbox"/> Параметр policed-dscp-transmit позволяет при превышении значения <i>committed-rate</i> или <i>peak_rate</i> передать пакет дальше, изменив в нем метку dscp, которая настраивается командой qos map policed-dscp с дополнительным аргументом violation в случае с <i>peak_rate</i>. При этом при превышении <i>committed_rate</i> и <i>peak_rate</i> можно настраивать разные значения dscp.</p> |

| | | |
|---|--------------------|---|
| no police | | Удаляет шаблон настроек регулирования скорости канала из правила классификации трафика. |
| mirror { <i>monitor_session</i> } | monitor_session: 1 | Указать номер monitor-сессии для зеркалирования трафика. |
| no mirror { <i>monitor_session</i> } | | Отменить зеркалирование. |

Команды режима конфигурации профиля qos tail-drop

Вид запроса командной строки режима конфигурации профиля qos tail-drop:

```
console# configure
console(config)# qos tail-drop profile profile_id
console(config-tdprofile)#
```

Таблица 281 – Команды режима конфигурации профиля qos tail-drop

| Команда | Значение/Значение по умолчанию | Действие |
|--|--|--|
| port-limit <i>limit</i> | limit: (0..7576)/25 | Задать размер пакетного разделяемого пула для порта. |
| no port-limit | | Установить значение по умолчанию. |
| queue <i>queue_id</i> [limit <i>limit</i>] [without-sharing withsharing] | limit: (0..7576)/12; queue_id: (1..8) | Изменить параметры очереди: - <i>queue_id</i> – номер очереди; - <i>limit</i> – количество пакетов в очереди; - without-sharing – запретить доступ к общему пулу; - with-sharing – разрешить доступ к общему пулу. |
| no queue <i>queue_id</i> | | Установить значение по умолчанию. |

Команды режима конфигурации интерфейса Ethernet, группы портов

Вид запроса командной строки режима конфигурации интерфейса Ethernet, группы портов:

```
console(config-if)#
```

Таблица 282 – Команды режима конфигурации интерфейса Ethernet, группы портов

| Команда | Значение/Значение по умолчанию | Действие |
|---|---|---|
| service-policy { <i>input</i> <i>output</i> } <i>policy_map_name</i> [default-action { deny-any permit-any }] | policy_map_name: (1..32) символов | Назначает интерфейсу стратегию классификации трафика. - deny-any – отбросить трафик, не попадающий под действие политики; - permit-any – разрешить прохождение трафика, не попадающего под действие политики. |
| no service-policy { <i>input</i> <i>output</i> } | | Удаляет стратегию классификации трафика с интерфейса. |
| traffic-shape <i>committed_rate</i> [<i>committed_burst</i>] | committed_rate: (64..100000000) кбит/с; committed_burst: (4096..12578880) байт | Устанавливает ограничение скорости для исходящего трафика через интерфейс. - <i>committed_rate</i> – средняя скорость трафика, кбит/с; - <i>committed_burst</i> – размер сдерживающего порога (ограничение скорости) в байтах. |
| no traffic-shape | | Снимает ограничение скорости исходящего трафика через интерфейс. |
| traffic-shape queue <i>queue_id</i> <i>committed_rate</i> [<i>committed_burst</i>] | queue_id: (0..8); committed_rate: (64..100000000) кбит/с; committed_burst: (4096..12578880) байт | Устанавливает ограничение скорости трафика через интерфейс для исходящей очереди. - <i>committed_rate</i> – средняя скорость трафика, кбит/с; - <i>committed_burst</i> – размер сдерживающего порога (ограничение скорости) в байтах. |
| no traffic-shape queue <i>queue_id</i> | | Снимает ограничение скорости трафика через интерфейс для исходящей очереди. |

| | | |
|---|---|--|
| qos trust [cos dscp cos-dscp] | -/включено | Включает базовый механизм qos для интерфейса. - cos – порт доверяет значению 802.1p User priority; - dscp – порт доверяет значению DSCP в IPv4/IPv6-пакетах; - cos-dscp – порт доверяет обоим уровням, однако DSCP имеет приоритет над 802.1p. |
| no qos trust | | Выключает базовый механизм qos для интерфейса. |
| rate-limit rate [burst burst] | rate: (64..100000000) кбит/с; burst: (3000..268431360) байт/128 кбайт | Устанавливает ограничение скорости для входящего трафика. |
| no rate-limit | | Снимает ограничение скорости входящего трафика. |
| rate-limit pps rate_pps [burst burst_packet] | rate_pps: (125..195312500) pps; burst_pps: (1..195312500) пакетов | Устанавливает ограничение скорости для входящего трафика в pps. |
| no rate-limit | | Снимает ограничение скорости входящего трафика. |
| qos cos default_cos | default_cos: (0..7)/0 | Устанавливает значение CoS по умолчанию для порта (CoS, применяемый для всего нетегированного трафика, проходящего через интерфейс). |
| no qos cos | | Устанавливает значение по умолчанию. |
| qos tail-drop profile profile_id | profile_id: (1..8) | Привязать указанный профиль к интерфейсу. |
| no qos tail-drop profile | | Убрать привязку. |

Команды режима конфигурации интерфейса VLAN

Вид запроса командной строки режима конфигурации интерфейса VLAN:

```
console (config-if) #
```

Таблица 283 – Команды режима конфигурации интерфейса VLAN

| Команда | Значение/значение по умолчанию | Действие |
|---------------------------|---------------------------------------|--|
| qos cos egress cos | cos: (0..7) | Устанавливает значение параметра поля приоритета 802.1p для исходящего тегированного трафика, формируемого центральным процессором. <input checked="" type="checkbox"/> При отсутствии команды значение cos будет получено из настроек команд ip tx-user-priority value или ipv6 tx-user-priority value. |
| no qos cos egress | | Установить значение по умолчанию. |


Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 284 – Команды режима EXEC

| Команда | Значение/значение по умолчанию | Действие |
|--|---------------------------------------|---|
| show qos | - | Показывает режим QOS, настроенный на устройстве. В базовом режиме показывает «доверенный» режим (trust mode). |
| show class-map [class_map_name] | class_map_name: (1..32) символа | <input checked="" type="checkbox"/> Действует только для режима qos advanced. |
| show policy-map [policy_map_name] | policy_map_name: (1..32) символа | <input checked="" type="checkbox"/> Действует только для режима qos advanced. |

| | | |
|---|---|--|
| show qos aggregate-policer <i>[aggregate_policer_name]</i> | aggregate_policer_name: (1..32) символа | Показывает настройки средней скорости и ограничения полосы пропускания для правил классификации трафика.  Действует только для режима qos advanced. |
| show qos interface [buffers queuing policers shapers] [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port port-channel group vlan vlan_id] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); tve_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128); vlan_id: (1..4094) | Показывает QoS-параметры для интерфейса. - <i>vlan_id</i> – номер VLAN; - <i>te_port</i> – номер интерфейсов Ethernet XG1-XG12; - <i>group</i> – номер группы портов; - buffers – настройки буфера для очередей интерфейса; - queuing – алгоритм обработки очередей (WRR или EF), вес для WRR-очередей, классы обслуживания для очередей и приоритет для EF; - policers – сконфигурированные стратегии классификации трафика для интерфейса; - shapers – ограничение скорости для исходящего трафика. |
| show qos map [dscp-queue dscp-dp policed-dscp dscp-mutation dscp-cos cos-dscp] | - | Показывает информацию о замене полей в пакетах, используемых QoS. - dscp-queue – таблица соответствия DSCP и очередей; - dscp-dp – таблица соответствия меток DSCP и приоритета сброса (DP); - policed-dscp – таблица перемаркировки DSCP; - dscp-mutation – таблица изменения DSCP-to-DSCP; - dscp-cos – таблица изменений dscp-cos; - cos-dscp – таблица изменений cos-dscp. |
| show qos tail-drop | - | Просмотр параметров tail-drop. |
| show qos tail-drop gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet tve_port hundredgigabitethernet hu_port | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); tve_port: (1..8/0/1..120); hu_port: (1..8/0/1..32) | Просмотр tail-drop информации по конкретному порту (всем портам). |
| show qos tail-drop unit unit_id | unit_id: (1..8) | Просмотр tail-drop информации по конкретному устройству в стеке. |

Примеры выполнения команд

- Включить режим QoS advanced. Распределить трафик по очередям, пакеты с DSCP 12 в первую очередь, пакеты с DSCP 16 во вторую. Восьмая очередь – приоритетная. Создать стратегию классификации трафика по списку ACL, разрешающему передачу TCP-пакетов с DSCP 12 и 16 и ограничивающую скорость – средняя скорость 1000 Кбит/с, порог ограничения 200000 байт. Использовать данную стратегию на интерфейсах Ethernet 14 и 16.

```

console#
console# configure
console(config)# ip access-list tcp_ena
console(config-ip-acl)# permit tcp any any any any dscp 12
console(config-ip-acl)# permit tcp any any any any dscp 16
console(config-ip-acl)# exit
console(config)# qos advanced
console(config)# qos map dscp-queue 12 to 1
console(config)# qos map dscp-queue 16 to 2
console(config)# priority-queue out num-of-queues 1
console(config)# policy-map traffic
console(config-pmap)# class class1 access-group tcp_ena
console(config-pmap-c)# police 1000 200000 exceed-action drop
console(config-pmap-c)# exit
console(config-pmap)# exit
console(config)# interface tengigabitethernet 1/0/14
console(config-if)# service-policy input traffic
console(config-if)# exit
console(config)# interface tengigabitethernet 1/0/16

```

```
console(config-if) # service-policy input traffic
console(config-if) # exit
console(config) #
```

5.29.2 Статистика QoS

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config) #
```

Таблица 285 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|---|--|--|
| qos statistics aggregate-policer <i>aggregate_policer_name</i> | aggregate_policer_name: (1..32) символов/выключено | Включает QoS-статистику по ограничению полос пропускания. |
| no qos statistics aggregate-policer <i>aggregate_policer_name</i> | | Отключает QoS-статистику по ограничению полос пропускания. |
| qos statistics interface | -/выключено | Включает сбор QoS-статистики на всех интерфейсах. |
| no qos statistics interface | | Выключает сбор QoS-статистики на всех интерфейсах. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 286 – Команды режима EXEC

| Команда | Значение/ Значение по умолчанию | Действие |
|--|--|--|
| clear qos statistics | - | Очищает статистику QoS по всем интерфейсам. |
| clear qos statistics interface gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32) | Очищает статистику QoS указанного интерфейса. |
| show qos statistics | - | Показывает статистику QoS по всем интерфейсам. |
| show qos statistics interface gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> | <i>gi_port</i> : (1..8/0/1..48); <i>te_port</i> : (1..8/0/1..48); <i>twe_port</i> : (1..8/0/1..120); <i>hu_port</i> : (1..8/0/1..32) | Показывает статистику QoS указанного интерфейса. |

5.30 Конфигурация протоколов маршрутизации

5.30.1 Конфигурация статической маршрутизации

Статическая маршрутизация – вид маршрутизации, при которой маршруты указываются в явном виде при конфигурации маршрутизатора. Вся маршрутизация при этом происходит без участия каких-либо протоколов маршрутизации.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console (config) #
```

Таблица 287 – Команды режима глобальной конфигурации

| Команда | Значение/ Значение по умолчанию | Действие |
|--|---|---|
| ip route <i>prefix prefix_length</i> { reject-route <i>gateway</i> [metric <i>metric</i>] [track <i>track</i>] [vrf <i>vrf_name</i>] [distance <i>distance</i>]} | <p>prefix: (A.B.C.D); prefix_length: (A.B.C.D или /n); gateway: (A.B.C.D) metric (1..255)/1; vrf_name: (1..32) символа; track: (1..64); distance (1..255)/1</p> | <p>Создает статическое правило маршрутизации.</p> <ul style="list-style-type: none"> - <i>prefix</i> – IP-адрес сети назначения; - <i>prefix_length</i> – маска префикса назначения или её длина; - reject-route – запрещает маршрутизацию к сети назначения через все шлюзы; - <i>gateway</i> – IP-адрес шлюза для доступа к сети назначения; - <i>metric</i> – метрика для данного маршрута; - <i>vrf_name</i> – имя экземпляра VRF; - <i>track</i> – номер объекта отслеживания; - <i>distance</i> – административная дистанция маршрута. |
| no ip route <i>prefix prefix_length</i> { rejectroute <i>gateway</i> } [vrf <i>vrf_name</i>] | | Удаляет правило из таблицы статической маршрутизации. |
| distance { ospf { inter-as intra-as } static } <i>distance</i> | <p>distance (1..255)/static:1, OSPF intra-as:30, OSPF inter-as:110</p> | <p>Устанавливает значение административной дистанции (AD) для всех маршрутов указанного типа.</p> <ul style="list-style-type: none"> - ospf inter-as – устанавливает значение AD для межзональных маршрутов, принятых по протоколу OSPF; - ospf intra-as – устанавливает значение AD для внутризональных маршрутов, принятых по протоколу OSPF; - static – устанавливает значение AD для статических маршрутов. |
| no distance { ospf { inter-as intra-as } static } | | Устанавливает значение по умолчанию. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 288 – Команды режима EXEC

| Команда | Значение/ Значение по умолчанию | Действие |
|--|---------------------------------|---|
| show ip route [connected static <i>address ip_address</i> [<i>mask</i> <i>prefix_length</i>] [longer-prefixes]] | - | <p>Показывает таблицу маршрутизации, удовлетворяющую заданным критериям.</p> <ul style="list-style-type: none"> - connected – подключенный маршрут, то есть маршрут, взятый с непосредственно подключенного и функционирующего интерфейса; - static – статический маршрут, прописанный в таблице маршрутизации. |

| | | |
|---------------|---|---|
| show distance | - | Показать значение административной дистанции для различных источников маршрута. |
|---------------|---|---|

Пример выполнения команды

- Показать таблицу маршрутизации:

```
console# show ip route
```

```
Maximum Parallel Paths: 2 (4 after reset)
Codes: C - connected, S - static
C 10.0.1.0/24 is directly connected, Vlan 1
S 10.9.1.0/24 [5/2] via 10.0.1.2, 17:19:18, Vlan 12
S 10.9.1.0/24 [5/3] via 10.0.2.2, Backup Not Active
S 172.1.1.1/32 [5/3] via 10.0.3.1, 19:51:18, Vlan 12
```

Таблица 289 – Описание результата выполнения команды

| Поле | Описание |
|--------------|--|
| C | Показывает происхождение маршрута: C – Connected (маршрут взят из непосредственно подключенного и функционирующего интерфейса), S – Static (статический маршрут, прописанный в таблице маршрутизации). |
| 10.9.1.0/24 | Адрес сети. |
| [5/2] | Первое значение в скобках – административная дистанция (степень доверия маршрутизатору, чем число выше, тем меньше доверие к источнику), второе число – метрика маршрута. |
| via 10.0.1.2 | Определяет IP-адрес следующего маршрутизатора, через который проходит маршрут до сети. |
| 00:39:08 | Определяет время последнего обновления маршрута (часы, минуты, секунды). |
| Vlan 1 | Определяет интерфейс, через который проходит маршрут до сети. |

Команды режима конфигурации VRF

Вид запроса командной строки режима конфигурации VRF:

```
console(config-vrf) #
```

Таблица 290 – Команды режима конфигурации VRF

| Команда | Значение/ Значение по умолчанию | Действие |
|---|--|--|
| <code>ip route prefix {mask prefix_length} {gateway [metric distance]}</code> | prefix_length: (0..32); distance (1..255)/1 | Создать статическое правило маршрутизации. - <i>prefix</i> — сеть назначения (например, 172.7.0.0); - <i>mask</i> — маска сети (в формате десятичной системы исчисления); - <i>prefix_length</i> — префикс маски сети (количество единиц в маске); - <i>gateway</i> — шлюз для доступа к сети назначения; - <i>distance</i> — вес маршрута. |
| <code>no ip route prefix {mask prefix_length} {gateway}</code> | | Удалить правило из таблицы статической маршрутизации. |
| <code>ip default-gateway {gateway}</code> | —/шлюз по умолчанию | Задать для коммутатора адрес шлюза по умолчанию через VRF. |
| <code>no ip default-gateway {gateway}</code> | ни не задан | Удалить назначенный адрес шлюза по умолчанию. |

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 291 – Команды режима EXEC

| Команда | Значение/ Значение по умолчанию | Действие |
|--|--|---|
| show ip route [connected vrf vrf_name static address ip_address [mask prefix_length] [longer-prefixes]] | — | Показать таблицу маршрутизации, удовлетворяющую заданным критериям. - connected — подключенный маршрут, то есть маршрут, взятый с непосредственно подключенного и функционирующего интерфейса; - static — статический маршрут, прописанный в таблице маршрутизации; - vrf — область виртуальной маршрутизации, в которой находится маршрут. |

5.30.2 Настройка протокола RIP

Протокол RIP (англ. Routing Information Protocol) — внутренний протокол, который позволяет маршрутизаторам динамически обновлять маршрутную информацию, получая ее от соседних маршрутизаторов. Это очень простой протокол, основанный на применении дистанционного вектора маршрутизации. Как дистанционно-векторный протокол, RIP периодически посылает обновления между соседями, строя, таким образом, топологию сети. В каждом обновлении передается информация о дистанции до всех сетей на соседний маршрутизатор. Коммутатор поддерживает протокол RIP версии 2.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 292 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|----------------------|---------------------------------------|---|
| router rip | - | Вход в режим конфигурации протокола RIP. |
| no router rip | | Удаление глобальной конфигурации протокола RIP. |

Команды режима конфигурации протокола RIP

Вид запроса командной строки:

```
console(config-rip)#
```

Таблица 293 – Команды режима конфигурации протокола RIP

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|--|--|
| default-metric [<i>metric</i>] | metric: (1..15)/1 | Устанавливает значение метрики, с которой будут анонсироваться маршруты, полученные другими протоколами маршрутизации. Без параметра устанавливает значение по умолчанию. |
| no default-metric | | Устанавливает значение по умолчанию. |
| network <i>A.B.C.D</i> | A.B.C.D: IP-адрес интерфейса | Устанавливает IP-адрес интерфейса, который будет участвовать в процессе маршрутизации. |
| no network <i>A.B.C.D</i> | | Удаляет IP-адрес интерфейса, который будет участвовать в процессе маршрутизации. |
| redistribute { static connected } [metric transparent] | - | Разрешает анонсирование маршрутов через RIP. - без параметров – означает, что будет использоваться default-metric при анонсировании маршрутов; - metric transparent – означает, что будет использоваться метрика из таблицы маршрутизации. |
| no redistribute { static connected } [metric transparent] | | Запрещает анонсирование статических маршрутов через RIP. - metric transparent – запрещает использовать метрику из таблицы маршрутизации. |
| redistribute ospf [metric <i>metric</i> match type route-map <i>route_map_name</i>] | metric: (1..15, transparent)/1; match: (internal, external-1, external-2); route_map_name: (1..32) символа | Разрешает анонсирование OSPF-маршрутов через RIP. - <i>type</i> – производить анонсирование только для указанных типов OSPF-маршрутов; - <i>route-map_name</i> – производить анонсирование маршрутов после их фильтрации через указанную route-map; |
| redistribute bgp metric [<i>metric</i> transparent] | metric: (1..15, transparent)/1 | Разрешает анонсирование BGP-маршрутов через RIP. - <i>metric</i> – значение метрики для импортируемых маршрутов; - metric transparent – означает, что будет использоваться метрика из таблицы маршрутизации. |
| no redistribute bgp metric [<i>metric</i> transparent] | | Без параметров запрещает анонсирование маршрутов BGP через RIP. В случае указания параметра возвращает его дефолтное значение. |
| redistribute isis [<i>level</i>] [match <i>match</i>] [metric <i>metric</i>] [transparent] | level: (level-1, level-2, level-1-2)/level-2; match: (internal, external); metric: (1..15, transparent)/1 | Разрешает анонсирование IS-IS маршрутов через RIP. - <i>level</i> – установить, из какого уровня IS-IS будут анонсироваться маршруты; - <i>match</i> – производить анонсирование только для указанных типов IS-IS маршрутов. |
| no redistribute isis [<i>level</i>] [match <i>match</i>] [metric <i>metric</i>] [transparent] | | Без параметров запрещает анонсирование маршрутов IS-IS через RIP. В случае указания параметра возвращает его дефолтное значение. |
| shutdown | -/включено | Выключают процесс маршрутизации по протоколу RIP. |
| no shutdown | | Включают процесс маршрутизации по протоколу RIP. |
| passive-interface | -/включено | Отключить обновления маршрутизации. |
| no passive-interface | | Включить обновления маршрутизации. |
| default-information originate | -/маршрут не генерируется | Генерировать маршрут по умолчанию. |
| no default-information originate | | Восстановить значение по умолчанию. |

Команды режима конфигурации интерфейса IP

Вид запроса командной строки:

```
console(config-ip) #
```

Таблица 294 – Команды режима конфигурации интерфейса IP

| <i>Команда</i> | <i>Значение/ Значение по умолчанию</i> | <i>Действие</i> |
|---|--|--|
| ip rip shutdown | -/включено | Выключают процесс маршрутизации по протоколу RIP на данном интерфейсе. |
| no ip rip shutdown | | Включают процесс маршрутизации по протоколу RIP на данном интерфейсе. |
| ip rip passive-interface | По умолчанию отправка обновлений включена | Выключает отправку обновлений на интерфейсе. |
| no ip rip passive-interface | | Устанавливает значение по умолчанию. |
| ip rip offset <i>offset</i> | offset: (1..15)/1 | Добавляет смещение к метрике. |
| no ip rip offset | | Устанавливает значение по умолчанию. |
| ip rip default-information originate <i>metric</i> | metric: (1..15)/1; По умолчанию функция отключена | Устанавливает метрику для маршрута по умолчанию транслируемого через RIP. |
| no ip rip default-information originate | | Устанавливает значение по умолчанию. |
| ip rip authentication mode {text md5} | По умолчанию аутентификация отключена. | Включает аутентификацию в RIP и определяет ее тип: - text – аутентификация открытым текстом; - md5 – аутентификации MD5. |
| no ip rip authentication mode | | Устанавливает значение по умолчанию. |
| ip rip authentication key-chain <i>key_chain</i> | key_chain: (1..32) символов | Определяет набор ключей, который может использоваться для аутентификации. |
| no ip rip authentication key-chain | | Устанавливает значение по умолчанию. |
| ip rip authentication-key <i>clear_text</i> | clear_text: (1..16) символов | Определяет ключ для аутентификации открытым текстом. |
| no ip rip authentication-key | | Устанавливает значение по умолчанию. |
| ip rip distribute-list access <i>acl_name</i> | acl_name: (1..32) символов | Устанавливает стандартный IP ACL для фильтрации анонсируемых маршрутов. |
| no ip rip distribute-list | | Устанавливает значение по умолчанию. |

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 295 – Команды режима Privileged EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---------------------------------------|---|
| show ip rip [database statistics peers] | - | Просмотр информации о RIP-маршрутизации: - database – информация о настройках RIP; - statistics – статистические данные; - peers – информация участника сети. |

Примеры использования команд

Включить протокол RIP для подсети 172.16.23.0 (IP-адрес на коммутаторе **172.16.23.1**) и аутентификацию MD5 через набор ключей **mykeys**:

```
console#
console# configure
console(config)# router rip
console(config-rip)# network 172.16.23.1
console(config-rip)# interface ip 172.16.23.1
console(config-if)# ip rip authentication mode md5
console(config-if)# ip rip authentication key-chain mykeys
```

5.30.3 Настройка протокола OSPF, OSPFv3

OSPF (*Open Shortest Path First*) — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути алгоритм Дейкстры. Протокол OSPF представляет собой протокол внутреннего шлюза (IGP). Протокол OSPF распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы.

Устройство поддерживает одновременную работу нескольких независимых экземпляров процессов OSPF. Настройка параметров экземпляра OSPF производится путем указания идентификатора экземпляра (**process_id**).

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console (config) #
```

Таблица 296 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--|---------------------------------------|---|
| router ospf [<i>process_id</i>] [vrf vrf_name] | process_id: (1..65535)/1 | Включает маршрутизацию по протоколу OSPF. Задаёт идентификатор процесса. |
| no router ospf [<i>process_id</i>] [vrf vrf_name] | vrf_name: (1..32) символа | Выключает маршрутизацию по протоколу OSPF. |
| ipv6 router ospf [<i>process_id</i>] | process_id: (1..65535)/1 | Включает маршрутизацию по протоколу OSPFv3. Задаёт идентификатор процесса. |
| no ipv6 router ospf [process_id] | | Выключает маршрутизацию по протоколу OSPFv3. |
| ipv6 distance ospf { <i>inter-as</i> <i>intra-as</i> } <i>distance</i> | distance: (1..255) | Задаёт административную дистанцию для маршрутов OSPF, OSPFv3. - inter-as – для внешних автономных систем; - intra-as – внутри автономной системы. |
| no ipv6 distance ospf {inter-as intra-as} | | Возвращает значения по умолчанию. |

Команды режима процесса OSPF

Вид запроса командной строки в режиме конфигурации процесса OSPF:

```
console (router_ospf_process) #  
console (ipv6 router_ospf_process) #
```

Таблица 297 – Команды режима конфигурации процесса OSPF

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|---|
| redistribute connected [<i>metric metric</i>] [route-map name] [filter-list acl_name] [subnets] | metric: (1..65535); name: (1..255) символов | Разрешает анонсирование connected маршрутов: - metric – значение метрики для импортируемых маршрутов; - name – имя политики импорта, позволяющей фильтровать и вносить изменения в импортируемые маршруты; - acl_name – имя стандартного IP ACL, который будет использоваться для фильтрации импортируемых маршрутов; - subnets – позволяет импортировать подсети. |
| no redistribute connected [metric metric] [route-map name] [filter-list acl_name] [subnets] | | Запрещает указанную функцию. |

| | | |
|---|--|--|
| redistribute static [<i>metric metric</i>] [<i>route-map name</i>] [<i>filter-list acl_name</i>] [<i>subnets</i>] | metric: (1..65535); name: (1..255) символов | Импорт статических маршрутов в OSPF. - <i>metric</i> – устанавливает значение метрики для импортируемых маршрутов; - <i>name</i> – применяет политику импорта, позволяющую фильтровать и вносить изменения в импортируемые маршруты; - <i>acl_name</i> – имя стандартного IP ACL, который будет использован для фильтрации импортируемых маршрутов; - subnets – позволяет импортировать подсети. |
| no redistribute static [<i>metric metric</i>] [<i>route-map name</i>] [<i>filter-list acl_name</i>] [<i>subnets</i>] | | Запрещает указанную функцию. |
| redistribute ospf id [<i>nssa-only</i>] [<i>metric metric</i>] [<i>metric-type {type-1 type-2}</i>] [<i>route-map name</i>] [<i>match {internal external-1 external-2}</i>] [<i>subnets</i>] | id: (1..65535); metric: (1..65535); name: (0..32) символа. | Импорт маршрутов из процесса OSPF в процесс OSPF: - nssa-only – устанавливает значение nssa-only для всех импортируемых маршрутов; - metric-type type-1 – импортирует с пометкой как OSPF external 1; - metric-type type-2 – импортирует с пометкой как OSPF external 2; - match internal – импортирует маршруты в пределах area; - match external-1 – импортирует маршруты типа OSPF external 1; - match external-2 – импортирует маршруты типа OSPF external 2; - subnets – позволяет импортировать подсети; - <i>name</i> – применяет указанную политику импорта, позволяющую фильтровать и вносить изменения в импортируемые маршруты; - <i>metric</i> – устанавливает значение метрики для импортируемых маршрутов. |
| no redistribute ospf [<i>id</i>] [<i>nssa-only</i>] [<i>metric metric</i>] [<i>metric-type {type-1 type-2}</i>] [<i>route-map name</i>] [<i>match {internal external-1 external-2}</i>] [<i>subnets</i>] | | Запрещает указанную функцию. |
| redistribute rip [<i>metric metric</i>] [<i>route-map name</i>] [<i>filter-list acl_name</i>] [<i>subnets</i>] | metric: (1..65535); name: (1..255) символа | Импорт маршрутов из RIP в OSPF. - <i>metric</i> – значение метрики для импортируемых маршрутов; - <i>name</i> – имя политики импорта, позволяющей фильтровать и вносить изменения в импортируемые маршруты; - <i>acl_name</i> – имя стандартного IP ACL, который будет использован для фильтрации импортируемых маршрутов; - subnets – позволяет импортировать подсети. |
| no redistribute rip [<i>metric metric</i>] [<i>route-map name</i>] [<i>filter-list acl_name</i>] [<i>subnets</i>] | | Запрещает указанную функцию. |
| redistribute isis [<i>level</i>] [<i>match match</i>] [<i>metric metric</i>] [<i>route-map name</i>] [<i>filter-list acl_name</i>] [<i>subnets</i>] | level: (level-1, level-2, level-1-2)/level-2; match: (internal, external); metric: (1-65535); acl_name: (1..32) символа | Импорт маршрутов из IS-IS в OSPF. - <i>level</i> – установить из какого уровня IS-IS будут анонсироваться маршруты; - <i>match</i> – производить анонсирование только для указанных типов IS-IS маршрутов; - <i>metric</i> – значение метрики для импортируемых маршрутов; - <i>name</i> – имя политики импорта, позволяющей фильтровать и вносить изменения в импортируемые маршруты; - <i>acl_name</i> – имя стандартного IP ACL, который будет использован для фильтрации импортируемых маршрутов; - subnets – позволяет импортировать подсети. |
| no redistribute isis [<i>level</i>] [<i>match match</i>] [<i>metric metric</i>] [<i>route-map name_policy</i>] [<i>filter-list name_acl</i>] [<i>subnets</i>] | | Без параметров запрещает импорт маршрутов из IS-IS в OSPF. В случае указания параметра возвращает его значение по умолчанию. |

| | | |
|--|--|---|
| redistribute bgp [<i>metric metric</i>] [<i>route-map name</i>] [<i>filter-list acl_name</i>] [<i>subnets</i>] | metric: (1..65535); name: (1..255) символа; acl_name: (1..32) символа | Импорт маршрутов из BGP в OSPF. - <i>metric</i> – значение метрики для импортируемых маршрутов; - <i>name</i> – имя политики импорта, позволяющей фильтровать и вносить изменения в импортируемые маршруты; - <i>acl_name</i> – имя стандартного IP ACL, который будет использован для фильтрации импортируемых маршрутов; - subnets – позволяет импортировать подсети. |
| no redistribute bgp [<i>metric metric</i>] [<i>route-map name</i>] [<i>filter-list acl_name</i>] [<i>subnets</i>] | | Без параметров запрещает импорт маршрутов из BGP в OSPF. В случае указания параметра возвращает его значение по умолчанию. |
| router-id <i>A.B.C.D</i> | A.B.C.D: идентификатор маршрутизатора в формате ipv4-адреса | Устанавливает идентификатор маршрутизатора, который уникально идентифицирует маршрутизатор в пределах одной автономной системы. |
| no router-id <i>A.B.C.D</i> | | Устанавливает значение по умолчанию. |
| network <i>ip_addr</i> area <i>A.B.C.D</i> [shutdown] | ip_addr: A.B.C.D | Включить (отключить) экземпляр OSPF на IP-интерфейсе (для IPv4). |
| no network <i>ip_addr</i> | | Удаляет IP-адрес интерфейса. |
| default-metric <i>metric</i> | metric: (1..65535) | Устанавливает метрику OSPF-маршрута. |
| no default-metric | | Отключение функции. |
| area <i>A.B.C.D</i> stub [no-summary] | A.B.C.D: идентификатор маршрутизатора в формате IPv4-адреса | Устанавливает для указанной зоны тип stub. Зона – совокупность сетей и маршрутизаторов, имеющих один и тот же идентификатор. - no-summary – не отправлять информацию о суммированных внешних маршрутах. |
| no area <i>A.B.C.D</i> stub | | Устанавливает значение по умолчанию. |
| area <i>A.B.C.D</i> nssa [no-summary] [<i>translator-stability-interval interval</i>] [<i>translator-role {always candidate}</i>] | A.B.C.D: идентификатор маршрутизатора в формате IPv4-адреса; interval: целое положительное число | Устанавливает для указанной зоны тип NSSA. - no-summary – не принимать информацию о суммированных внешних маршрутах внутри NSSA-зоны; - <i>interval</i> – определяет промежуток времени (в секундах), в течение которого транслятор будет выполнять свои функции после того, как обнаружит, что транслятором стал другой граничный маршрутизатор; - translator-role – определяет, каким образом на маршрутизаторе будет функционировать режим транслятора (трансляции Type-7 LSA в Type-5 LSA); - always – в принудительном постоянном режиме; - candidate – в режиме участия в выборах транслятора. |
| no area <i>A.B.C.D</i> nssa | | Устанавливает значение по умолчанию. |
| area <i>A.B.C.D</i> virtual-link <i>A.B.C.D</i> [<i>hello-interval secs</i>] [<i>retransmit-interval secs</i>] [<i>transmit-delay secs</i>] [<i>dead-interval secs</i>] [null <i>message-digest</i>] [<i>key-chain word</i>] | A.B.C.D: идентификатор маршрутизатора в формате IPv4-адреса; secs: (1..65535) секунд; word: (1..256) символов | Создание виртуального соединения между основной и другими удаленными областями, которые имеют между ними области. - hello-interval – указать hello-интервал; - retransmit-interval – указать интервал между повторными передачами; - transmit-delay – указать время задержки; - dead-interval – указать dead-интервал; - null – без аутентификации; - message-digest – аутентификация с шифрованием; - <i>word</i> – пароль для аутентификации. |
| no area <i>A.B.C.D</i> virtual-link <i>A.B.C.D</i> [<i>hello-interval secs</i>] [<i>retransmit-interval secs</i>] [<i>transmit-delay secs</i>] [<i>dead-interval secs</i>] [null <i>message-digest</i>] [<i>key-chain word</i>] | | Удаляет виртуальное соединение. |
| area <i>A.B.C.D</i> default-cost <i>cost</i> | A.B.C.D: идентификатор маршрутизатора в формате IPv4-адреса; cost: целое положительное число | Устанавливает значение стоимости суммарного маршрута, используемого для stub- и NSSA-зон (для IPv4). |
| no area <i>A.B.C.D</i> default-cost | | Устанавливает значение по умолчанию. |


| | | |
|--|--|---|
| area A.B.C.D authentication [message-digest] | A.B.C.D: идентификатор маршрутизатора в формате IPv4-адреса; -/выключено | Включает аутентификацию для всех интерфейсов данной зоны (для IPv4): - message-digest – с шифрованием MD5. |
| no area A.B.C.D authentication [message-digest] | | Отключает аутентификацию. |
| area A.B.C.D range network_address mask [advertise not-advertise] | A.B.C.D: идентификатор маршрутизатора в формате IPv4-адреса; network_address: A.B.C.D; mask: E.F.G.H | Создает суммарный маршрут на границе зоны (для IPv4). - advertise – анонсировать созданный маршрут; - not-advertise – не анонсировать созданный маршрут. |
| no area A.B.C.D range network_address mask | | Удаляет суммарный маршрут. |
| area A.B.C.D filter-list prefix prefix_list in | A.B.C.D: идентификатор маршрутизатора в формате IPv4-адреса; prefix_list: (1..32) символа | Устанавливает фильтр на маршруты, анонсируемые в указанную зону из других зон (для IPv4). |
| no area A.B.C.D filter-list prefix prefix_list in | | Удаляет фильтр на маршруты, анонсируемые в указанную зону из других зон (для IPv4). |
| area A.B.C.D filter-list prefix prefix_list out | A.B.C.D: идентификатор маршрутизатора в формате IPv4-адреса; prefix_list: (1..32) символа | Устанавливает фильтр на маршруты, анонсируемые из указанной зоны в другие зоны (для IPv4). |
| no area A.B.C.D filter-list prefix prefix_list out | | Удаляет фильтр на маршруты, анонсируемые из указанной зоны в другие зоны (для IPv4). |
| area A.B.C.D shutdown | A.B.C.D: идентификатор маршрутизатора в формате IPv4-адреса; -/выключено | Отключает процесс OSPF для зоны. |
| no area A.B.C.D shutdown | | Включает процесс OSPF для зоны. |
| passive-interface | -/выключено | Запрещает всем IP-интерфейсам, участвующим в процессе OSPF, обмениваться протокольными сообщениями с соседями (включает пассивный режим).  При применении данной команды настройка ip ospf passive-interface удаляется со всех ip интерфейсов и становится для них значением по умолчанию. |
| no passive-interface | | Устанавливает значение по умолчанию. |
| shutdown | -/выключено | Отключает процесс OSPF. |
| no shutdown | | Включает процесс OSPF. |
| timers spf delay delay | delay: (0..600000)/5000 мс | Устанавливает величину задержки, производимой перед очередным последовательным расчетом SPF. |
| no timers spf delay | | Устанавливает значение по умолчанию. |
| timers lsa throttle min_interval hold_interval max_interval | min_interval: (0..60000)/5000 мс; hold_interval: (0..60000)/0 мс; max_interval: (0..60000)/0 мс | Задаёт временные параметры LSA-троттлинга. Троттлинг действует только на LSA, источником которых является локальное устройство. - <i>min_interval</i> — минимальный временной интервал между двумя последовательно отправляющимися одинаковыми LSA. - <i>hold_interval</i> — интервал, определяющий текущее время задержки. С каждой новой последовательной LSA этот интервал умножается на два, пока не достигнет значения <i>max_interval</i> . - <i>max_interval</i> — максимальный временной интервал между двумя последовательно отправляющимися одинаковыми LSA. |
| no timers lsa throttle | | Устанавливает значение по умолчанию. |
| timers lsa arrival min_arrival | min_arrival: (0..60000)/1000 мс | Установить минимальный временной интервал, с которым маршрутизатор обрабатывает принимаемые LSA. |
| no timers lsa arrival min_arrival | | Устанавливает значение по умолчанию. |

Вид запроса командной строки:

```
console (config-ip) #
```

Таблица 298 – Команды режима конфигурации интерфейса IP

| Команда | Значение/Значение по умолчанию | Действие |
|---|---|---|
| ip ospf shutdown | -/включено | Выключает маршрутизацию по протоколу OSPF на интерфейсе. |
| no ip ospf shutdown | | Включает маршрутизацию по протоколу OSPF на интерфейсе. |
| ip ospf network {broadcast point-to-point} | -/broadcast | Выбрать тип сети: - broadcast — широковещательная сеть с множественным доступом; - point-to-point — сеть «точка-точка». |
| no ip ospf network | | Устанавливает значение по умолчанию. |
| ip ospf authentication [message-digest] | -/выключено | Включает аутентификацию в OSPF с использованием заданного пароля в нешифрованном виде. - message-digest — включает аутентификацию в OSPF с использованием заданного набора ключей и алгоритма MD5. |
| no ip ospf authentication | | Устанавливает значение по умолчанию. |
| ip ospf authentication-key key | key: (1..8) символов/пароль не задан | Назначает пароль для аутентификации соседей, доступных через текущий интерфейс. Пароль задается в нешифрованном виде. Пароль, указанный таким образом, будет внедрен в заголовок каждого уходящего в эту сеть пакета OSPF в качестве ключа аутентификации. |
| no ip ospf authenticationkey | | Устанавливает значение по умолчанию. |
| encrypted ip ospf authentication-key EncryptedWord | EncryptedWord: (1..8) байт/пароль не задан | Назначает пароль для аутентификации соседей, доступных через текущий интерфейс. Пароль задается в зашифрованном виде. Пароль, указанный таким образом, будет внедрен в заголовок каждого уходящего в эту сеть пакета OSPF в качестве ключа аутентификации. |
| no encrypted ip ospf authentication-key | | Устанавливает значение по умолчанию. |
| ip ospf authentication key-chain key_chain | key_chain: (1..32) символов/не задано | Задаёт имя набора ключей, который будет использоваться при аутентификации. |
| no ip ospf authentication key-chain | | Устанавливает значение по умолчанию. |
| ip ospf authentication null | -/не используется | Отключает использование аутентификации на текущем интерфейсе. |
| ip ospf cost cost | cost: (1..65535)/10 | Устанавливает метрику состояния канала, которая является основным показателем "стоимости" пересылки данных по каналу. |
| no ip ospf cost | | Устанавливает значение по умолчанию. |
| ip ospf dead-interval {interval minimal} | interval: (1..65535) секунд; minimal – 1 сек | Устанавливает интервал времени в секундах, по истечении которого сосед будет считаться неактивным. Этот интервал должен быть кратным значению hello-interval. Как правило, dead-interval равен 4 интервалам отправки hello-пакетов. |
| no ip ospf dead-interval | | Устанавливает значение по умолчанию. |
| ip ospf hello-interval interval | interval: (1..65535)/10 секунд | Устанавливает интервал времени в секундах, по истечении которого маршрутизатор отправляет следующий hello-пакет с интерфейса. |
| no ip ospf hello-interval | | Устанавливает значение по умолчанию. |
| ip ospf mtu-ignore | -/включено | Отключение проверки MTU. |
| no ip ospf mtu-ignore | | Устанавливает значение по умолчанию. |

| | | |
|---|------------------------------|---|
| <code>ip ospf passive-interface</code> | | Запрещает IP-интерфейсу обмениваться протокольными сообщениями с соседями (включает пассивный режим). |
| <code>no ip ospf passive-interface</code> | -/выключено | Устанавливает значение по умолчанию.  Если применена настройка <code>passive-interface</code> в режиме конфигурации процесса OSPF, то данная команда выводит данный IP-интерфейс из пассивного режима. |
| <code>ip ospf priority <i>priority</i></code> | <i>priority</i> : (0..255)/1 | Устанавливает приоритет маршрутизатора, который используется для выбора DR и BDR. |
| <code>no ip ospf priority</code> | | Устанавливает значение по умолчанию. |

Команды режима конфигурации интерфейса Ethernet, VLAN:

Вид запроса командной строки:

```
console(config-if) #
```

Таблица 299 – Команды режима конфигурации интерфейса Ethernet, VLAN

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|--|--|
| <code>ipv6 ospf shutdown</code> | -/включено | Выключает маршрутизацию по протоколу OSPFv3 на интерфейсе. |
| <code>no ipv6 ospf shutdown</code> | | Включает маршрутизацию по протоколу OSPFv3 на интерфейсе. |
| <code>ipv6 ospf process area <i>area</i> [shutdown]</code> | <i>process</i> : (1..65536); <i>area</i> : идентификатор маршрутизатора в формате IPv4-адреса | Включает (отключает) OSPF процесс для определенной зоны. |
| <code>ipv6 ospf cost <i>cost</i></code> | <i>cost</i> : (1..65535)/10 | Устанавливает метрику состояния канала, которая является условным показателем "стоимости" пересылки данных по каналу. |
| <code>no ipv6 ospf cost</code> | | Устанавливает значение по умолчанию. |
| <code>ipv6 ospf dead-interval <i>interval</i></code> | <i>interval</i> : (1..65535) секунд | Устанавливает интервал времени в секундах, по истечении которого сосед будет считаться неактивным. Этот интервал должен быть кратным значению <code>hello-interval</code> . Как правило, <code>dead-interval</code> равен 4 интервалам отправки <code>hello</code> -пакетов. |
| <code>no ipv6 ospf dead-interval</code> | | Устанавливает значение по умолчанию. |
| <code>ipv6 ospf hello-interval <i>interval</i></code> | <i>interval</i> : (1..65535)/10 секунд | Устанавливает интервал времени в секундах, по истечении которого маршрутизатор отправляет следующий <code>hello</code> -пакет с интерфейса. |
| <code>no ipv6 ospf hello-interval</code> | | Устанавливает значение по умолчанию. |
| <code>ipv6 ospf mtu-ignore</code> | -/disabled | Отключает проверки MTU. |
| <code>no ipv6 ospf mtu-ignore</code> | | Устанавливает значение по умолчанию. |
| <code>ipv6 ospf neighbor {<i>ipv6_address</i>}</code> | - | Задаёт IPv6 адрес соседа. |
| <code>ipv6 ospf neighbor {<i>ipv6_address</i>}</code> | | Удаляет IPv6 адрес соседа. |
| <code>ipv6 ospf priority <i>priority</i></code> | <i>priority</i> : (0..255)/1 | Устанавливает приоритет маршрутизатора, который используется для выбора DR и BDR. |
| <code>no ipv6 ospf priority</code> | | Устанавливает значение по умолчанию. |
| <code>ipv6 ospf retransmit-interval <i>interval</i></code> | <i>interval</i> : (1..65535)/5 секунд | Устанавливает интервал времени в секундах, по истечении которого маршрутизатор повторно отправит пакет, на который не получил подтверждения о получении (например, Database Description пакет или Link State Request пакеты). |
| <code>no ipv6 ospf retransmit-interval</code> | | Устанавливает значение по умолчанию. |
| <code>ipv6 ospf transmit-delay <i>delay</i></code> | <i>delay</i> : (1..65535)/1 секунд | Устанавливает примерное время в секундах, необходимое для передачи пакета состояния канала. |
| <code>no ip ospf transmit-delay</code> | | Устанавливает значение по умолчанию. |

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 300 – Команды режима Privileged EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|---|--|--|
| show {ip ipv6} ospf [process_id] [vrf vrf_name] | process_id: (1..65536) vrf_name: (1..32) символа | Отображает конфигурации OSPF. |
| show {ip ipv6} ospf [process_id] neighbor [vrf vrf_name] | process_id: (1..65536) vrf_name: (1..32) символа | Отображает информации об OSPF-соседах. |
| show ip ospf [process_id] neighbor A.B.C.D [vrf vrf_name] | process_id: (1..65536); A.B.C.D: IP-адрес соседа vrf_name: (1..32) символа | Отображает информации об OSPF-соседе с указанным адресом. |
| show {ip ipv6} ospf [process_id] interface [vrf vrf_name] | process_id: (1..65536) vrf_name: (1..32) символа | Отображает конфигурации всех OSPF-интерфейсов. |
| show {ip ipv6} ospf [process_id] interface {gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group vlan vlan_id tunnel tunnel_id A.B.C.D [vrf vrf_name] [brief]} | process_id: (1..65535); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..48); vlan_id: (1..4094); tunnel_id: (1..16) A.B.C.D: IP-адрес vrf_name: (1..32) символа | Отображает конфигурации конкретного OSPF-интерфейса. |
| show {ip ipv6} ospf [process_id] database [vrf vrf_name] [router [vrf vrf_name] summary [vrf vrf_name] as-summary [vrf vrf_name]] | process_id: (1..65535) vrf_name: (1..32) символа | Отображает состояние базы данных протокола OSPF. |
| show {ip ipv6} ospf virtual-links [process_id] [vrf vrf_name] | process_id: (1..65535) vrf_name: (1..32) символа | Отображает параметры и текущее состояние виртуальных линков. |
| clear ip ospf {process_id vrf vrf_name process} | process_id: (1..65535) vrf_name: (1..32) символа | Разрывает соседства и удаляет соответствующие маршруты. |

Примеры использования команд

- Показать OSPF-соседей для определенного VRF (vrf1):

```
console# show ip ospf neighbor vrf vrf1
```

- Перезапустить OSPF-соседей для определенного VRF (vrf1):

```
console# clear ip ospf vrf vrf1 process
```

5.30.4 Настройка протокола BGP (Border Gateway Protocol)

BGP (Border Gateway Protocol – протокол граничного шлюза) является протоколом маршрутизации между автономными системами (AS). Основной функцией BGP-системы является обмен информацией о доступности сетей с другими системами BGP. Информация о доступности сетей включает список автономных систем (AS), через которые проходит эта информация.

BGP является протоколом прикладного уровня и функционирует поверх протокола транспортного уровня TCP (порт 179). После установки соединения передаётся информация обо всех маршрутах, предназначенных для экспорта. В дальнейшем передаётся только информация об изменениях в таблицах маршрутизации.



Поддержка протокола BGP предоставляется по лицензии.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console (config) #
```

Таблица 301 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|---|
| router bgp [<i>as_plain_id</i> <i>as_dot_id</i>] | <i>as_plain_id</i> : (1..4294967295)/1 <i>as_dot_id</i> : (1.0..65535.65535) | Включает маршрутизацию по протоколу BGP. Задаёт идентификатор AS и переходит в режим её конфигурирования. - <i>as_plain_id</i> – идентификатор автономной системы, используемый маршрутизатором при установлении соседства и обмене маршрутной информацией; - <i>as_dot_id</i> – идентификатор автономной системы в 32-битном формате. |
| no router bgp [<i>as_plain_id</i> <i>as_dot_id</i>] | | Останавливает BGP-маршрутизатор, удаляет всю конфигурацию протокола BGP. |

Команды режима конфигурации AS

Вид запроса командной строки в режиме конфигурации AS:

```
console (router-bgp) #
```

Таблица 302 – Команды режима конфигурации AS

| Команда | Значение/Значение по умолчанию | Действие |
|---|--------------------------------|--|
| bgp router-id <i>ip_add</i> | - | Задать идентификатор BGP-маршрутизатора. |
| no bgp router-id | | Удалить идентификатор BGP-маршрутизатора. |
| bgp asnotation dot | -/asplain | Задействует систему обозначение номеров AS в формате asdot. |
| no bgp asnotation | | Устанавливает значение по умолчанию. |
| bgp client-to-client reflection | -/включено | Включает пересылку маршрутов, полученных от reflector-клиента, другим reflector-клиентам. |
| no bgp client-to-client reflection | | Выключает пересылку маршрутов, полученных от reflector-клиента, другим reflector-клиентам. |

| | | |
|--|-----------------------|---|
| bgp cluster-id <i>ip_add</i> | - | <p>Задаёт идентификатор кластера BGP-маршрутизатора.</p> <p><input checked="" type="checkbox"/> В случае если идентификатор кластера не настроен, в качестве идентификатора будет использоваться глобальный идентификатор BGP-маршрутизатора.</p> |
| no bgp cluster-id | - | Удалить идентификатор кластера BGP-маршрутизатора. |
| shutdown | -/no shutdown | <p>Административно выключает протокол BGP, не удаляя его конфигурацию.</p> <p><input checked="" type="checkbox"/> Это действие влечёт за собой разрыв всех сессий с BGP-соседями и очистку таблицы маршрутизации протокола BGP.</p> |
| no shutdown | | Включить работу AS. |
| neighbor <i>ip_add</i> | - | Задать IP-адрес для BGP-соседа или перейти в режим конфигурирования существующего соседа. |
| no neighbor <i>ip_add</i> | | Удалить конфигурацию для BGP-соседа с указанным IPv4 или IPv6-адресом. |
| peer-group <i>name</i> | name: (0..32) символа | Создает Peer-группу. - <i>name</i> – имя группы. |
| no peer-group <i>name</i> | | Удаляет созданную Peer-группу. |
| address-family <i>ipv4</i> {unicast multicast} | -/unicast | Указывает тип IPv4 Address Family и переводит коммутатор в режим конфигурации соответствующей Address Family. |
| no address-family <i>ipv4</i> {unicast multicast} | | Выключает соответствующую Address-Family. |
| address-family <i>l2vpn evpn</i> | -/выключено | Указывает тип l2vpn Address Family и переводит коммутатор в режим конфигурации соответствующей address-family. |
| no address-family <i>l2vpn evpn</i> | | Выключает соответствующую address-family. |

Команды режима конфигурации Address-Family

Вид запроса командной строки в режиме конфигурации Address-Family:

```
console (router-bgp-af) #
```

Таблица 303 – Команды режима конфигурации Address-Family

| Команда | Значение/Значение по умолчанию | Действие |
|--|--|---|
| network <i>ip_add</i> [mask <i>mask</i>] | - | <p>Задает подсеть, которая анонсируется BGP-соседям.</p> <p>- <i>ip-add</i> – адрес подсети; - <i>mask</i> – маска подсети.</p> <p><input checked="" type="checkbox"/> Если маска не указана, по умолчанию она задается классовым методом адресации. mask – маска IP-подсети или длина префикса.</p> |
| no network <i>ip_add</i> [mask <i>mask</i>] | | Удаляет анонс данной подсети. - <i>ip-add</i> – адрес подсети; - <i>mask</i> – маска подсети. |
| redistribute connected [metric <i>metric</i> filter-list <i>name</i>] | metric: (1-4294967295); name: (0..32) символа | <p>Разрешает анонсирование connected-маршрутов.</p> <p>- <i>metric</i> – значение атрибута MED, которое будет присвоено импортированным маршрутам; - <i>name</i> – название access-list, который будет применен к маршрутам.</p> |
| no redistribute connected | | Запрещает анонсирование connected-маршрутов. |
| redistribute rip [metric <i>metric</i> filter-list <i>name</i>] | metric: (1-4294967295); name: (0..32) символа | <p>Импортирует маршруты RIP в BGP.</p> <p>- <i>metric</i> – значение атрибута MED, которое будет присвоено импортированным маршрутам; - <i>name</i> – название access-list, который будет применен к маршрутам.</p> |
| no redistribute rip | | Запрещает импорт маршрутов из протокола RIP. |


| | | |
|---|---|--|
| redistribute static [<i>metric metric</i> <i>filter-list name</i>] | metric: (1-4294967295); name: (0..32) символа | Разрешает анонсирование статических маршрутов. - <i>metric</i> – значение атрибута MED, которое будет присвоено импортированным маршрутам; - <i>name</i> – название access-list, который будет применен к маршрутам. |
| no redistribute static | | Запрещает анонсирование статических маршрутов. |
| redistribute ospf <i>id</i> [<i>metric metric</i> <i>match type</i> <i>metric-type mtype</i> <i>nssa-only</i> <i>filter-list name</i>] | id: (1..65535); metric: (1-4294967295); type: (internal, external-1, external-2); name: (1..32) символов; mtype: (type-1, type-2); name: (0..32) символа | Импортирует маршруты OSPF в BGP. - <i>id</i> – идентификатор процесса OSPF; - <i>metric</i> – значение атрибута MED, которое будет присвоено импортированным маршрутам; - <i>type</i> – тип OSPF-маршрутов, анонсируемых в BGP; - <i>name</i> – название access-list, который будет применен к маршрутам; - <i>mtype</i> – тип метрики Ex1 или Ex2. |
| no redistribute ospf | | Запрещает импорт маршрутов из протокола OSPF. |
| redistribute isis [<i>level</i>] [<i>match match</i>] [<i>metric metric</i>] [<i>filter-list acl_name</i>] | level: (level-1, level-2, level-1-2)/level-2; match: (internal, external); metric: (1-65535); acl_name: (1..32) символа | Импортирует маршруты из IS-IS в BGP. - <i>level</i> – установить из какого уровня IS-IS будут анонсироваться маршруты; - <i>match</i> – производить анонсирование только для указанных типов IS-IS маршрутов; - <i>metric</i> – значение метрики для импортируемых маршрутов; - <i>acl_name</i> – имя стандартного IP ACL, который будет использован для фильтрации импортируемых маршрутов. |
| no redistribute isis | | Запрещает импорт маршрутов из протокола IS-IS. |
| redistribute bgp [<i>metric metric</i> / <i>filter-list name</i>] | metric: (1-4294967295); name: (0..32) символа | Импортирует маршруты, полученные в none default VRF по протоколу BGP, в BGP AF I2vpn evpn - <i>metric</i> – значение атрибута MED, которое будет присвоено импортированным маршрутам; - <i>name</i> – название access-list, который будет применен к маршрутам. |
| no redistribute bgp | | Запрещает анонсирование маршрутов. |
| aggregate-address <i>ipv4_add mask</i> [summary-only / as-set / advertise-map <i>route_map_name</i> / attribute-map <i>route_map_name</i> / suppress-map <i>route_map_name</i>] | | Включает агрегацию более специфичных маршрутов, входящих в указанный префикс: - <i>ipv4_add</i> – IPv4-адрес подсети; - <i>mask</i> – маска подсети - <i>route_map_name</i> – имя route-map; - <i>summary-only</i> – запретить отправку соседям маршрутов, которые попадают под суммирующий маршрут; - <i>as-set</i> – включить добавление в суммирующий маршрут as-path, полученный из префиксов, попадающих под суммирующий маршрут; - <i>suppress-map</i> – запретить отправку соседям маршрутов, попадающих под route-map (параметр summary-only игнорируется); - <i>advertise-map</i> – маршруты, попадающие под route-map, не будут попадать под суммирующий; - <i>attribute-map</i> – включить установку для суммирующего маршрута атрибутов, указанных в действии set в route-map. |
| no aggregate-address <i>ipv4_add mask</i> | | Удалить агрегацию более специфичных маршрутов, входящих в указанный префикс. |

Команды режима конфигурации BGP-соседа

Вид запроса командной строки в режиме конфигурации BGP-соседа:

```
console (router-bgp-nbr) #
```

Таблица 304 – Команды режима конфигурации BGP-соседа

| | | |
|---|---|---|
| <p>maximum-prefix value [threshold percent hold-timer second action type]</p> | <p>value: (0-4294967295); percent: (0-100); second: (30-86400); type: (restart, warning-only)</p> | <p>Включает ограничение количества принимаемых маршрутов от BGP-соседа.</p> <ul style="list-style-type: none"> - <i>value</i> – максимальное количество принимаемых маршрутов; - <i>percent</i> – процент от максимального количества маршрутов, по достижении которого отправляется предупреждение; - <i>second</i> – временной промежуток (в секундах), по истечению которого происходит переподключение, если сессия была разорвана из-за превышения количества маршрутов; - <i>type</i> – назначает действие, выполняемое при достижении максимального значения (разрыв сессии <restart> или отправка предупреждения <warning-only>). |
| <p>no maximum-prefix</p> | | <p>Выключает ограничение количества принимаемых маршрутов от BGP-соседа.</p> |
| <p>advertisement-interval <i>adv_sec withdraw with_sec</i></p> | <p>adv-sec: (0-65535)/30 секунд; with-sec: (0-65535)/30 секунд</p> | <p>Задаёт временные интервалы.</p> <ul style="list-style-type: none"> - <i>adv-sec</i> – минимальный интервал между отправкой UPDATE сообщений одного и того же маршрута; - <i>with-sec</i> – минимальный интервал между анонсированием маршрута и его последующим де-анонсированием. <p> – Advertisement-interval должен быть больше или равен withdraw-interval;</p> <ul style="list-style-type: none"> – Маршруты, которые должны быть анонсированы соседним BGP-маршрутизаторам, распределяются по нескольким UPDATE-сообщениям. Между отправкой этих UPDATE-сообщений выдерживается случайный временной интервал таким образом, чтобы общее время между обновлением маршрутов в локальной таблице BGP и отправкой последнего UPDATE-сообщения не превышало advertisement-interval или as-origination-interval в случае отправки локальных (маршруты из локальной AS) маршрутов в eBGP-соединении. Таким образом, каждый из маршрутов может иметь случайную величину задержки анонсирования; – Точность работы таймеров advertisement-interval, withdraw-interval и as-origination-interval зависит от максимального значения любого из этих трёх таймеров, настроенных на BGP-маршрутизаторе (учитываются таймеры, настроенные для всех BGP-соседей). Все значения таймеров анонсирования и де-анонсирования маршрутов, сконфигурированных на устройстве, дискретизируются интервалом в 1/255 от наибольшего настроенного значения. Увеличение максимального значения будет приводить к увеличению частоты дискретизации таймеров и, соответственно, к понижению точности их работы. |
| <p>no advertisement-interval</p> | | <p>Устанавливает значение по умолчанию.</p> |
| <p>as-origination-interval <i>seconds</i></p> | <p>seconds: (0-65535)/15 секунд</p> | <p>Задаёт временной интервал между отправкой UPDATE сообщений одного и того же маршрута, используется для анонса локальных (маршруты из локальной AS) маршрутов eBGP соседям.</p> |
| <p>no as-origination-interval</p> | | <p>Устанавливает значение по умолчанию.</p> |
| <p>connect-retry-interval <i>seconds</i></p> | <p>seconds: (1-65535)/120 секунд</p> | <p>Задаёт временной интервал, по истечению которого возобновляется попытка создать BGP-сессию с соседом.</p> |
| <p>no connect-retry-interval</p> | | <p>Устанавливает значение по умолчанию.</p> |
| <p>next-hop-self</p> | <p>-/выключено</p> | <p>Включает подмену значения атрибута NEXT_HOP на локальный адрес маршрутизатора.</p> |

| | | |
|--|---|--|
| no next-hop-self | | Отключить подмену атрибута NEXT_HOP. |
| remote-as [<i>as_plain_id</i> <i>as_dot_id</i>] | as_plain_id: (1..4294967295)/1 as_dot_id: (1.0..65535.65535) | Задаёт номер автономной системы, в которой находится BGP-сосед. Установление соседства невозможно, пока соседу не назначен номер AS. <input checked="" type="checkbox"/> Это действие влечёт разрыв сессии с соседом и очистку всех принятых от него маршрутов. |
| no remote-as | | Удалить идентификатор соседней автономной системы. |
| timers <i>holdtime keepalive</i> | holdtime: (0 3-65535)/90 секунд; keepalive: (0-21845)/30 секунд | Задаёт временные интервалы. - <i>holdtime</i> – если в течение этого времени не будет принято keepalive-сообщение, то соединение с соседом сбрасывается; - <i>keepalive</i> – интервал между отправкой keepalive-сообщений. <input checked="" type="checkbox"/> Значения holdtime и keepalive должны быть либо оба равны нулю, либо оба больше нуля. holdtime должен быть больше или равен keepalive. – Если был выбран таймер hold, который настроен на локальном маршрутизаторе, то используется локальное значение таймера keepalive; – Если был выбран таймер hold, который настроен на соседнем маршрутизаторе и значение локально настроенного таймера keepalive меньше чем 1/3 выбранного таймера hold, то используется локальное значение таймера keepalive; – Если был выбран таймер hold, который настроен на соседнем маршрутизаторе и значение локально настроенного таймера keepalive больше чем 1/3 выбранного таймера hold, то используется целое число, которое меньше чем 1/3 выбранного таймера hold. |
| no timers | | Устанавливает значение по умолчанию. |
| timers idle-hold <i>seconds</i> | seconds: (1..32747)/15 | Задаёт временной интервал удержания соседа в состоянии Idle после того, как он был сброшен в это состояние. За этот интервал все попытки переустановить соединение с соседом будут отклонены. |
| no timers idle-hold | | Устанавливает значение по умолчанию. |
| timers open-delay <i>seconds</i> | seconds: (0-240)/0 секунд | Задаёт временной интервал между установкой TCP-соединения и отправкой первого OPEN-сообщения. |
| no timers open-delay | | Устанавливает значение по умолчанию. |
| shutdown | -/no shutdown | Административно выключает сессию с BGP-соседом и очищает принятые от него маршруты, не удаляя его конфигурации. |
| no shutdown | | Административно включает сессию с BGP-соседом. |
| update-source [<i>gigabitethernet gi_port</i> <i>tengigabitethernet te_port</i> <i>twentyfivegigabitethernet twe_port</i> <i>hundredgigabitethernet hu_port</i> <i>Port-Channel group</i> <i>Loopback loopback</i> <i>Vlan vlan_id</i>] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..48); loopback: (1-64); vlan-id: (1-4094) | Назначает интерфейс, который будет использован в качестве исходящего при соединении с соседом. |
| no update-source | | Отменяет ручную настройку исходящего интерфейса, включает автоматический выбор интерфейса. |

| | | |
|---|---|--|
| route-reflector-client [meshed] | -/disabled | <p>Назначить BGP-соседа Route-Reflector клиентом.</p> <ul style="list-style-type: none"> - meshed – параметр выставляется если используется mesh-топология. При получении от такого клиента BGP-маршрутов они не будут пересылаться другим клиентам. <input checked="" type="checkbox"/> BGP-маршрутизатор является route-reflector-ом, если хотя бы один его сосед сконфигурирован как route-reflector клиент. <input checked="" type="checkbox"/> Для применения данной команды необходим перезапуск BGP-сессии с соседом. |
| no route-reflector-client | | Устанавливает значение по умолчанию. |
| soft-reconfiguration in-bound | -/disabled | <p>Команда сохраняет полученные от соседа маршруты в отдельной области памяти. Метод позволяет применить входящую политику «route-map in» для соседа без сброса соседства и запроса маршрутов.</p> <input checked="" type="checkbox"/> По умолчанию работает механизм Route Refresh. |
| no soft-reconfiguration in-bound | | Отключить механизм сохранения маршрутов. |
| prefix-list name {in out} | name: (0..32) символа | - <i>name</i> – название IP prefix-list, который будет применен к анонсируемым или принимаемым маршрутам. |
| no prefix-list name {in out} | | Отвязать IP prefix-list. |
| peer-group name | name: (0..32) символа | <p>- <i>name</i> – имя Peer-группы, которая будет применена к соседу.</p> <input checked="" type="checkbox"/> Настройки на Peer-группе имеют более высокий приоритет, чем настройки на самом соседе. |
| no peer-group | | Удалить соседа из группы. |
| address-family ipv4 {unicast multicast} | -/unicast | Указывает тип IPv4 address family и переводит коммутатор в режим конфигурации соответствующей address family для этого BGP-соседа. |
| no address-family ipv4 {unicast multicast} | | Выключить соответствующую IPv4 address-family. |
| address-family l2vpn evpn | -/выключено | Указывает тип l2vpn address family и переводит коммутатор в режим конфигурации соответствующей Address Family для этого BGP-соседа. |
| no address-family l2vpn evpn | | Выключает соответствующую Address-Family. |
| fall-over bfd | -/выключено | Включить протокол BFD на соседе. |
| no fall-over bfd | | Выключить протокол BFD на соседе. |
| password word | word: (1..128) символов; По умолчанию аутентификация отключена | Включает аутентификацию всех TCP-сегментов, принятых от BGP-соседа. Задает ключ аутентификации в текстовом виде. Данная настройка игнорируется, если для аутентификации указана key-chain. - <i>word</i> – ключ в текстовом виде. |
| no password | | Устанавливает значение по умолчанию. |
| password encrypted encryptedword | encryptedword: (1..128); По умолчанию аутентификация отключена | Включает аутентификацию всех TCP-сегментов, принятых от BGP-соседа. Задает ключ аутентификации в зашифрованном виде (например, пароль в зашифрованном виде, скопированный с другого устройства). Данная настройка игнорируется, если для аутентификации указана key-chain. - <i>encryptedword</i> – ключ в зашифрованном виде. |
| no password encrypted | | Устанавливает значение по умолчанию. |
| password key-chain word | word: (1..32) символов; По умолчанию аутентификация отключена | Задать имя связки ключей, которая будет использоваться для аутентификации всех TCP сегментов, принятых от BGP-соседа. - <i>word</i> – имя связки ключей. |
| no password key-chain | | Устанавливает значение по умолчанию. |


| | | |
|-------------------------------|---------------|---|
| <code>ebgp-multihop</code> | -/TTL равен 1 | Устанавливает TTL равный 64 для EBGp-подключений. |
| <code>no ebgp-multihop</code> | | Устанавливает значение по умолчанию. |

Команды режима конфигурации Address Family BGP-соседа

Вид запроса командной строки в режиме конфигурации Address Family BGP-соседа:

```
console (router-bgp-nbr-af) #
```

Таблица 305 – Команды режима конфигурации Address Family BGP-соседа

| Команда | Значение/Значение по умолчанию | Действие |
|---|---|--|
| <code>maximum-prefix value [threshold percent hold-timer second action type]</code> | value: (0-4294967295); percent: (0-100); second: (30-86400); type: (restart, warning-only) | Включает ограничение количества принимаемых маршрутов от BGP-соседа. - <i>value</i> – максимальное количество принимаемых маршрутов; - <i>percent</i> – процент от максимального количества маршрутов, по достижении которого отправляется предупреждение; - <i>second</i> – временной промежуток (в секундах), по истечению которого происходит переподключение, если сессия была разорвана из-за превышения количества маршрутов; - <i>type</i> – назначает действие, выполняемое при достижении максимального значения (разрыв сессии <restart> или отправка предупреждения <warning-only>). |
| <code>no maximum-prefix</code> | | Выключает ограничение количества принимаемых маршрутов от BGP-соседа. |
| <code>advertisement-interval adv_sec withdraw with_sec</code> | adv-sec: (0-65535)/30 секунд; with-sec: (0-65535)/30 секунд | <p>Задаёт временные интервалы.</p> <ul style="list-style-type: none"> - <i>adv-sec</i> – минимальный интервал между отправкой UPDATE сообщений одного и того же маршрута; - <i>with-sec</i> – минимальный интервал между анонсированием маршрута и его последующим де-анонсированием. <p> – Advertisement-interval должен быть больше или равен withdraw-interval;</p> <ul style="list-style-type: none"> – Маршруты, которые должны быть анонсированы соседним BGP-маршрутизаторам, распределяются по нескольким UPDATE-сообщениям. Между отправкой этих UPDATE-сообщений выдерживается случайный временной интервал таким образом, чтобы общее время между обновлением маршрутов в локальной таблице BGP и отправкой последнего UPDATE-сообщения не превышало <i>advertisement-interval</i> или <i>as-origination-interval</i> в случае отправки локальных (маршруты из локальной AS) маршрутов в eBGP-соединении. Таким образом, каждый из маршрутов может иметь случайную величину задержки анонсирования; – Точность работы таймеров <i>advertisement-interval</i>, <i>withdraw-interval</i> и <i>as-origination-interval</i> зависит от максимального значения любого из этих трёх таймеров, настроенных на BGP-маршрутизаторе (учитываются таймеры, настроенные для всех BGP-соседей). Все значения таймеров анонсирования и де-анонсирования маршрутов, сконфигурированных на устройстве, дискретизируются интервалом в 1/255 от наибольшего настроенного значения. Увеличение максимального значения будет приводить к увеличению частоты дискретизации таймеров и, соответственно, к понижению точности их работы. |

| | | |
|--|------------------------------|--|
| no advertisement-interval | | Устанавливает значение по умолчанию. |
| as-origination-interval <i>seconds</i> | seconds: (0-65535)/15 секунд | Задаёт временной интервал между отправкой UPDATE сообщений одного и того же маршрута, используется для анонса локальных (маршруты из локальной AS) маршрутов eBGP-соседам. |
| no as-origination-interval | | Устанавливает значение по умолчанию. |
| default-originate [<i>route-map name</i>] | name: (0..32) символа/- | <p>Анонсирует BGP-соседу маршрут по умолчанию вне зависимости от его наличия в локальной таблице маршрутизации. В качестве nexthop в таком маршруте будет указан интерфейс, с которого установлена BGP-сессия.</p> <ul style="list-style-type: none"> - route-map – параметр позволяет анонсировать маршрут по умолчанию, только если он присутствует в локальной таблице маршрутизации и его источником не является протокол BGP. - <i>name</i> — имя политики route-map, которая будет применена к операции анонсирования маршрута по умолчанию. <p><input checked="" type="checkbox"/> Route-map должна содержать в себе только секцию match ip address с указанием на prefix-list, под который попадает маршрут по умолчанию. Пример настройки такой route-map и prefix-list приведен под таблицей.</p> <p><input checked="" type="checkbox"/> Если в prefix-list находится указание на какой-либо маршрут, отличный от дефолтного, то именно этот маршрут должен присутствовать в локальной таблице маршрутизации, чтобы анонсировался маршрут по умолчанию. Ограничений на источник этого маршрута нет.</p> |
| no default-originate | | Отменяет настройку default-originate . |
| route-map <i>name</i> {in out} | name: (0..32) символа | - <i>name</i> – имя политики route-map, которая будет применена к соседу в данной Address Family. Позволяет фильтровать и вносить изменения в анонсируемые и принимаемые маршруты. |
| no route-map <i>name</i> {in out} | | Удаление политики с данной Address Family. |
| next-hop-self | -/включено | Включает подмену значения атрибута NEXT_HOP на локальный адрес маршрутизатора. |
| no next-hop-self | | Отключить подмену атрибута NEXT_HOP. |
| route-reflector-client [<i>meshed</i>] | -/disabled | <p>Назначить BGP-соседа Route-Reflector клиентом.</p> <ul style="list-style-type: none"> - meshed – параметр выставляется если используется mesh-топология. При получении от такого клиента BGP-маршрутов они не будут пересылаться другим клиентам. <p><input checked="" type="checkbox"/> BGP-маршрутизатор является route-reflector-ом, если хотя бы один его сосед сконфигурирован как route-reflector клиент.</p> <p><input checked="" type="checkbox"/> Для применения данной команды необходим перезапуск BGP-сессии с соседом.</p> |
| no route-reflector-client | | Устанавливает значение по умолчанию. |

Пример настройки route-map, используемой в команде default-originate

```

console#configure
console(config)#route-map RM_DEFAULT_ROUTE 10 permit
console(config-route-map)#match ip address prefix-list PL_DEFAULT_ROUTE
console(config-route-map)#exit
console(config)#ip prefix-list PL_DEFAULT_ROUTE seq 5 permit 0.0.0.0/0

```

Команды режима конфигурации Peer-групп

Вид запроса командной строки в режиме конфигурации Peer-групп:

```
console(router-bgp-nbrgrp) #
```

Таблица 306 – Команды режима конфигурации Peer-групп

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|--|
| maximum-prefix <i>value [threshold percent hold-timer second action type]</i> | value: (0-4294967295); percent: (0-100); second: (30-86400); type: (restart, warning-only) | Включает ограничение количества принимаемых маршрутов от BGP-соседа. - <i>value</i> – максимальное количество принимаемых маршрутов; - <i>percent</i> – процент от максимального количества маршрутов, по достижении которого отправляется предупреждение; - <i>second</i> – временной промежуток (в секундах), по истечению которого происходит переподключение, если сессия была разорвана из-за превышения количества маршрутов; - <i>type</i> – назначает действие, выполняемое при достижении максимального значения (разрыв сессии <restart> или отправка предупреждения <warning-only>). |
| no maximum-prefix | | Выключает ограничение количества принимаемых маршрутов от BGP-соседа. |
| advertisement-interval <i>adv_sec withdraw with_sec</i> | adv-sec: (0-65535)/30 секунд; with-sec: (0-65535)/30 секунд | Задаёт временные интервалы. - <i>adv-sec</i> – минимальный интервал между отправкой UPDATE сообщений одного и того же маршрута; - <i>with-sec</i> – минимальный интервал между анонсированием маршрута и его последующим де-анонсированием.  <ul style="list-style-type: none"> – Advertisement-interval должен быть больше или равен withdraw-interval; – Маршруты, которые должны быть анонсированы соседним BGP-маршрутизаторам, распределяются по нескольким UPDATE-сообщениям. Между отправкой этих UPDATE-сообщений выдерживается случайный временной интервал таким образом, чтобы общее время между обновлением маршрутов в локальной таблице BGP и отправкой последнего UPDATE-сообщения не превышало advertisement-interval или as-origination-interval в случае отправки локальных (маршруты из локальной AS) маршрутов в eBGP-соединении. Таким образом, каждый из маршрутов может иметь случайную величину задержки анонсирования; – Точность работы таймеров advertisement-interval, withdraw-interval и as-origination-interval зависит от максимального значения любого из этих трёх таймеров, настроенных на BGP-маршрутизаторе (учитываются таймеры, настроенные для всех BGP-соседей). Все значения таймеров анонсирования и де-анонсирования маршрутов, сконфигурированных на устройстве, дискретизируются интервалом в 1/255 от наибольшего настроенного значения. Увеличение максимального значения будет приводить к увеличению частоты дискретизации таймеров и, соответственно, к понижению точности их работы. |
| no advertisement-interval | | Устанавливает значение по умолчанию. |
| as-origination-interval <i>seconds</i> | seconds: (0-65535)/15 секунд | Задаёт временной интервал между отправкой UPDATE сообщений одного и того же маршрута, используется для анонса локальных (маршруты из локальной AS) маршрутов eBGP соседям. |
| no as-origination-interval | | Устанавливает значение по умолчанию. |
| connect-retry-interval <i>seconds</i> | seconds: (1-65535)/120 секунд | Задаёт временной интервал, по истечению которого возобновляется попытка создать BGP-сессию с соседом. |
| no connect-retry-interval | | Устанавливает значение по умолчанию. |

| | | |
|--|---|--|
| next-hop-self | -/выключено | Включает подмену значения атрибута NEXT_HOP на локальный адрес маршрутизатора. |
| no next-hop-self | | Отключить подмену атрибута NEXT_HOP. |
| remote-as [<i>as_plain_id</i> <i>as_dot_id</i>] | as_plain_id: (1..4294967295)/1 as_dot_id: (1.0..65535.65535) | Задаёт номер автономной системы, в которой находится BGP-сосед. Установление соседства невозможно, пока соседу не назначен номер AS. <input checked="" type="checkbox"/> Это действие влечёт разрыв сессии с соседом и очистку всех принятых от него маршрутов. |
| no remote-as | | Удалить идентификатор соседней автономной системы. |
| timers <i>holdtime keepalive</i> | holdtime: (0 3-65535)/90 секунд; keepalive: (0-21845)/30 секунд | Задаёт временные интервалы. - <i>holdtime</i> – если в течение этого времени не будет принято keepalive-сообщение, то соединение с соседом сбрасывается; - <i>keepalive</i> – интервал между отправкой keepalive-сообщений. <input checked="" type="checkbox"/> Значения holdtime и keepalive должны быть либо оба равны нулю, либо оба больше нуля. holdtime должен быть больше или равен keepalive. – Если был выбран таймер hold, который настроен на локальном маршрутизаторе, то используется локальное значение таймера keepalive; – Если был выбран таймер hold, который настроен на соседнем маршрутизаторе и значение локально настроенного таймера keepalive меньше чем 1/3 выбранного таймера hold, то используется локальное значение таймера keepalive; Если был выбран таймер hold, который настроен на соседнем маршрутизаторе и значение локально настроенного таймера keepalive больше чем 1/3 выбранного таймера hold, то используется целое число, которое меньше чем 1/3 выбранного таймера hold. |
| no timers | | Устанавливает значение по умолчанию. |
| timers idle-hold <i>seconds</i> | seconds: (1..32747)/15 | Задаёт временной интервал удержания соседа в состоянии Idle после того, как он был сброшен в это состояние. За этот интервал все попытки переустановить соединение с соседом будут отклонены. |
| no timers idle-hold | | Устанавливает значение по умолчанию. |
| timers open-delay <i>seconds</i> | seconds: (0-240)/0 секунд | Задаёт временной интервал между установкой TCP-соединения и отправкой первого OPEN-сообщения. |
| no timers open-delay | | Устанавливает значение по умолчанию. |
| shutdown | -/no shutdown | Административно выключает сессии со всеми BGP-соседями, входящими в состав peer-группы, и очищает принятые от них маршруты, не удаляя их конфигурации. В конфигурацию каждого соседа, входящего в peer-группу, в контекст (router-bgp-nbr) добавляется команда shutdown. |
| no shutdown | | Административно включает сессии со всеми BGP-соседями, входящими в состав peer-группы. Удаляет команду shutdown из конфигурации каждого соседа, входящего в peer-группу. |
| update-source [<i>gigabitethernet gi_port</i> <i>tengigabitethernet te_port</i> <i>twentyfivegigabitethernet twe_port</i> <i>hundredgigabitethernet hu_port</i> Port-Channel group Loopback loopback Vlan vlan_id] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..48); loopback: (1-64); vlan-id: (1-4094) | Назначает интерфейс, который будет использован в качестве исходящего при соединении с соседом. |
| no update-source | | Отменяет ручную настройку исходящего интерфейса, включает автоматический выбор интерфейса. |

| | | |
|---|---|---|
| route-reflector-client [meshed] | -/disabled | <p>Назначить BGP-соседа Route-Reflector клиентом.</p> <p>- meshed — параметр выставляется если используется mesh-топология. При получении от такого клиента BGP-маршрутов они не будут пересылаться другим клиентам.</p> <p><input checked="" type="checkbox"/> BGP-маршрутизатор является route-reflector-ом, если хотя бы один его сосед сконфигурирован как route-reflector клиент.</p> <p><input checked="" type="checkbox"/> Для применения данной команды необходим перезапуск BGP-сессии с соседом.</p> |
| no route-reflector-client | | Устанавливает значение по умолчанию. |
| soft-reconfiguration inbound | -/disabled | <p>Команда сохраняет полученные от соседа маршруты в отдельной области памяти. Метод позволяет применить входящую политику «route-map in» для соседа без сброса соседства и запроса маршрутов.</p> <p><input checked="" type="checkbox"/> По умолчанию работает механизм Route Refresh.</p> |
| no soft-reconfiguration inbound | | Отключить механизм сохранения маршрутов. |
| prefix-list name {in out} | name: (0..32) символа | - <i>name</i> – название IP prefix-list, который будет применен к анонсируемым или принимаемым маршрутам. |
| no prefix-list name {in out} | | Отвязать IP prefix-list. |
| fall-over bfd | -/выключено | Включить протокол BFD на peer-группе. |
| no fall-over bfd | | Выключить протокол BFD на peer-группе. |
| password word | word: (1..128) символов; По умолчанию аутентификация отключена | <p>Включает аутентификацию всех TCP-сегментов, принятых от BGP-соседа. Задает ключ аутентификации в текстовом виде. Данная настройка игнорируется, если для аутентификации указана key-chain.</p> <p>Данная настройка игнорируется для пиров, входящих в настраиваемую группу, для которых присутствуют собственные настройки аутентификации.</p> <p>- <i>word</i> – ключ в текстовом виде.</p> |
| no password | | Устанавливает значение по умолчанию. |
| password encrypted encryptedword | encryptedword: (1..128); По умолчанию аутентификация отключена | <p>Включает аутентификацию всех TCP-сегментов, принятых от BGP-соседа. Задает ключ аутентификации в зашифрованном виде (например, пароль в зашифрованном виде, скопированный с другого устройства).</p> <p>Данная настройка игнорируется, если для аутентификации указана key-chain.</p> <p>Данная настройка игнорируется для пиров, входящих в настраиваемую группу, для которых присутствуют собственные настройки аутентификации.</p> <p>- <i>encryptedword</i> – ключ в зашифрованном виде.</p> |
| no password encrypted | | Устанавливает значение по умолчанию. |
| password key-chain word | word: (1..32) символов; По умолчанию аутентификация отключена | <p>Задать имя связки ключей, которая будет использоваться для аутентификации всех TCP сегментов, принятых от BGP-соседа. Данная настройка игнорируется для пиров, входящих в настраиваемую группу, для которых присутствуют собственные настройки аутентификации.</p> <p>- <i>word</i> — имя связки ключей.</p> |
| no password key-chain | | Устанавливает значение по умолчанию. |

Команды режима Privileged EXEC

Все команды доступны для привилегированного пользователя.

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 307 – Команды режима Privileged EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|---|--|--|
| <code>clear ip bgp [ip_add]</code> | - | Переустанавливает соединения с BGP-соседями, очищая принятые от них маршруты; - <i>ip_add</i> – адрес соседнего BGP-спикера, с которым будет переустановлена сессия. |
| <code>show ip bgp afi safi</code> | afi: (all, ipv4, l2vpn); safi (all, unicast, multicast, evpn) | Отобразить таблицу BGP-маршрутов (Loc-RIB) указанных AFI/SAFI. - <i>afi</i> — идентификатор Address Family; - <i>safi</i> — идентификатор Sub-Address Family. |
| <code>show ip bgp [ip_add]</code> | - | Отобразить таблицу BGP-маршрутов (Loc-RIB). - <i>ip_add</i> – префикс подсети назначения, по которому будет отображена подробная информация о маршрутах до неё. |
| <code>show ip bgp neighbor [ip-add [detail advertised-routes received-routes]]</code> | - | Отобразить информацию о настроенных BGP-соседах. - <i>ip_add</i> – адрес соседнего BGP-спикера, по которому будет отфильтрована информация; - <i>detail</i> – отобразить подробную информацию; - <i>advertised-routes</i> – отобразить таблицу маршрутов, анонсированных соседу; - <i>received-routes</i> – отобразить таблицу принимаемых маршрутов до применения к ним входящей политики. Для отображения принимаемых маршрутов с ключом <i>received-routes</i> в контексте настройки соответствующего соседа должна быть задействована команда <i>soft-reconfiguration inbound</i>. |
| <code>show ip bgp peer-group name</code> | - | Отобразить созданные Peer-группы и их настройки. - <i>name</i> – отобразить настройки группы с именем <i>name</i> . |
| <code>show ip bgp peer-group name neighbors</code> | - | Отобразить состоящих в peer-группе соседей. |

5.30.5 Настройка протокола IS-IS

IS-IS (*Intermediate System to Intermediate System*) — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link state technology) и использующий для нахождения кратчайшего пути алгоритм Дейкстры. Протокол IS-IS представляет собой протокол внутреннего шлюза (IGP). Протокол IS-IS распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 308 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|-----------------------------|--------------------------------|---|
| <code>router isis</code> | -/ISIS маршрутизатор отключен | Запускает IS-IS маршрутизатор. Входит в режим конфигурации протокола IS-IS. |
| <code>no router isis</code> | | Останавливает IS-IS маршрутизатор. Удаляет конфигурацию протокола IS-IS. |

Команды режима конфигурации протокола IS-IS

Вид запроса командной строки в режиме конфигурации протокола IS-IS:

```
console(router-isis)#
```

Таблица 309 – Команды режима конфигурации протокола IS-IS

| Команда | Значение/Значение по умолчанию | Действие |
|---|--|--|
| address-family ipv4 unicast | - | Переходит в режим конфигурации Address-Family. |
| authentication key word [level] | word: (1..20) символов; level: (level-1, level-2)/level-1-2 | Задать ключ аутентификации в виде текста. Используется для аутентификации LSP, CSNP, PSNP PDU. Данная настройка игнорируется, если для аутентификации указана key-chain. - <i>word</i> – ключ в текстовом виде; - <i>level</i> – уровень IS-IS, для которого применится настройка. |
| no authentication key | | Удаляет ключ аутентификации. |
| authentication key encrypted encryptedword [level] | encryptedword: (1..128) символов; level: (level-1, level-2)/level-1-2 | Задаёт ключ аутентификации в зашифрованном виде (например, пароль в зашифрованном виде, скопированный с другого устройства). Используется для аутентификации LSP, CSNP, PSNP PDU. Данная настройка игнорируется, если для аутентификации указана key-chain. - <i>encryptedword</i> – ключ в зашифрованном виде; - <i>level</i> – уровень IS-IS, для которого применится настройка. |
| no authentication key | | Удаляет ключ аутентификации. |
| authentication key-chain word [level] | word: (1..32) символа; level: (level-1, level-2)/level-1-2 | Задать имя связки ключей, которая будет использоваться для аутентификации LSP, CSNP, PSNP PDU. - <i>word</i> – имя связки ключей; - <i>level</i> – уровень IS-IS, для которого применится настройка. |
| no authentication key-chain | | Отключает режим использования связки ключей для аутентификации. |
| authentication mode {text md5} [level] | level: (level-1, level-2)/level-1-2; По умолчанию аутентификация отключена. | Включает аутентификацию в IS-IS и определяет ее тип: - text – аутентификация открытым текстом; - md5 – аутентификация MD5; - <i>level</i> – уровень IS-IS, для которого применится настройка. |
| no authentication mode | | Устанавливает значение по умолчанию. |
| hostname dynamic | -/включено | Включить поддержку динамических hostname. |
| no hostname dynamic | | Выключить поддержку динамических hostname. |
| is-type {level-1 level-2-only level-1-2} | -/level-1-2 | Задаёт тип маршрутизатора в IS-IS домене: - level-1 – все взаимодействия с другими маршрутизаторами происходят на 1 уровне; - level-2-only – все взаимодействия с другими маршрутизаторами происходят на 2 уровне; - level-1-2 – устройство поддерживает взаимодействия обоих уровней. |
| no is-type | | Устанавливает значение по умолчанию. |
| lsp-buff-size size | size (512-9000)/1500 байт | Устанавливает максимально возможный размер отправляемых LSP и SNP. Значение lsp buffer size не должно превышать значение pdu buffer size. |
| no lsp-buff-size | | Устанавливает значение по умолчанию. |
| lsp-gen-interval second [level] | second: (1-65535000)/30000 миллисекунд; level: (level-1, level-2)/level-1-2 | Задаёт минимальный интервал в мс, между генерацией одной и той же LSP. - <i>second</i> – значение интервала в миллисекундах, по истечении которого LSP может быть заново сгенерировано; - <i>level</i> – уровень для которого применим данный интервал. Если не указывать, интервал применится к обоим уровням. |
| no lsp-gen-interval | | Устанавливает значение по умолчанию. |
| lsp-refresh-interval second | second: (1-65235)/900 секунд | Задаёт максимальный интервал в секундах, между генерацией LSP. - <i>second</i> – значение интервала в секундах, по истечении которого LSP будет заново сгенерировано. |
| no lsp-refresh-interval | | Устанавливает значение по умолчанию. |
| max-lsp-lifetime second | second: (350-65535)/1200 секунд | Задаёт время жизни LSP. Значение должно быть хотя бы на 300 секунд больше, чем lsp-refresh-interval. - <i>second</i> – значение в секундах. |
| no max-lsp-lifetime | | Устанавливает значение по умолчанию. |

| | | |
|---|---|--|
| metric-style style [level] | style: (narrow, wide, both)/both level: (level-1, level-2)/level-1-2 | Задает используемый стиль метрики. - <i>narrow</i> – поддерживать только стандартную (узкую) метрику; - <i>wide</i> – поддерживать только расширенную метрику; - <i>both</i> – поддерживать оба стиля метрики; - <i>level</i> – уровень, для которого применим указанный стиль метрики. Если не указывать, метрика применится к обоим уровням. |
| no metric-style | | Устанавливает значение по умолчанию. |
| net XX.XXXX.XXXX.XX | - | Устанавливает так называемый NET (Network Entity Title) адрес – уникальный идентификатор маршрутизатора в пределах IS-IS домена. При записи NET используется шестнадцатичная система счисления. |
| no net | | Удаляет идентификатор маршрутизатора. |
| shutdown | -/включено | Отключает процесс ISIS. |
| no shutdown | | Включает процесс ISIS. |
| spf interval maximum-wait second | second: (0-4294967295)/5000 | Устанавливает интервал между двумя последовательными пересчетами алгоритма SPF в миллисекундах. |
| no spf interval maximum-wait | | Устанавливает значение по умолчанию. |
| spf threshold restart-limit number | number: (1-4294967295)/10 | Устанавливает сколько раз алгоритм SPF может быть прерван обновлением LSDB. |
| no spf threshold restart-limit | | Устанавливает значение по умолчанию. |
| spf threshold updates-restart number | number: (1-4294967295)/4294967295 | Задает количество обновлений LSDB, при которых алгоритм SPF останавливается и перезапускается. |
| no spf threshold updates-restart | | Устанавливает значение по умолчанию. |
| spf threshold updates-start number | number: (1-4294967295)/4294967295 | Количество обновлений LSDB, необходимое для немедленного запуска алгоритма SPF (spf interval maximum-wait при этом игнорируется). |
| no spf threshold updates-start | | Устанавливает значение по умолчанию. |

Команды режима конфигурации Address-Family

Вид запроса командной строки в режиме конфигурации Address-Family:

```
console(router-isis-af) #
```

Таблица 310 – Команды режима конфигурации Address-Family

| Команда | Значение/Значение по умолчанию | Действие |
|--|--|--|
| redistribute connected [level level] [metric-type type] [metric metric] [filter-list name] | level: (level-1, level-2); type: (internal, external); metric: (1-16777215); name: (1-32) символа | Разрешает импорт connected маршрутов: - <i>level</i> – уровень IS-IS, в который будет выполняться перераспределение маршрутов; - <i>type</i> – установить импортируемым маршрутам тип метрики; - <i>metric</i> – значение метрики для импортируемых маршрутов; - <i>name</i> – имя стандартного IP ACL, который будет использован для фильтрации импортируемых маршрутов. Если глобально включен стандартный (narrow) стиль метрики, все значения метрики больше 63 будут указаны в TLV как 63. |
| no redistribute connected [level level] [metric-type type] [metric metric] [filter-list name] | | Без параметров запрещает импорт connected маршрутов в IS-IS. В случае указания параметра возвращает его дефолтное значение. |

| | | |
|--|---|---|
| redistribute static [<i>level level</i>] [<i>metric-type type</i>] [metric metric] [<i>filter-list name</i>] | level: (level-1, level-2); type: (internal, external); metric: (1-16777215); name: (1-32) символа | Разрешает импорт статических маршрутов в IS-IS. - <i>level</i> – уровень IS-IS, в который будет выполняться перераспределение маршрутов; - <i>type</i> – установить импортируемым маршрутам тип метрики; - <i>metric</i> – значение метрики для импортируемых маршрутов; - <i>name</i> – имя стандартного IP ACL, который будет использован для фильтрации импортируемых маршрутов. Если глобально включен стандартный (narrow) стиль метрики, все значения метрики больше 63 будут указаны в TLV как 63. |
| no redistribute static [<i>level level</i>] [<i>metric-type type</i>] [metric metric] [<i>filter-list name</i>] | | Без параметров запрещает импорт статических маршрутов в IS-IS. В случае указания параметра возвращает его дефолтное значение. |
| redistribute rip [<i>level level</i>] [metric-type type] [<i>metric metric</i>] [filter-list name] | level: (level-1, level-2); type: (internal, external); metric: (1-16777215); name: (1-32) символа | Разрешает импорт маршрутов из RIP в IS-IS. - <i>level</i> – уровень IS-IS, в который будет выполняться перераспределение маршрутов; - <i>type</i> – установить импортируемым маршрутам тип метрики; - <i>metric</i> – значение метрики для импортируемых маршрутов; - <i>name</i> – имя стандартного IP ACL, который будет использован для фильтрации импортируемых маршрутов. Если глобально включен стандартный (narrow) стиль метрики, все значения метрики больше 63 будут указаны в TLV как 63. |
| no redistribute rip [<i>level level</i>] [metric-type type] [<i>metric metric</i>] [filter-list name] | | Без параметров запрещает импорт маршрутов из RIP в IS-IS. В случае указания параметра возвращает его дефолтное значение. |
| redistribute bgp [<i>level level</i>] [metric-type type] [<i>metric metric</i>] [filter-list name] | level: (level-1, level-2); type: (internal, external); metric: (1-16777215); name: (1-32) символа | Разрешает импорт маршрутов из BGP в IS-IS. - <i>level</i> – уровень IS-IS, в который будет выполняться перераспределение маршрутов; - <i>type</i> – установить импортируемым маршрутам тип метрики; - <i>metric</i> – значение метрики для импортируемых маршрутов; - <i>name</i> – имя стандартного IP ACL, который будет использован для фильтрации импортируемых маршрутов. Если глобально включен стандартный (narrow) стиль метрики, все значения метрики больше 63 будут указаны в TLV как 63. |
| no redistribute bgp [<i>level level</i>] [metric-type type] [<i>metric metric</i>] [filter-list name] | | Без параметров запрещает импорт маршрутов из BGP в IS-IS. В случае указания параметра возвращает его дефолтное значение. |
| redistribute ospf [<i>id id</i>] [<i>level level</i>] [metric-type type] [<i>match match</i>] [metric metric] [<i>filter-list name</i>] | Id: (1-65536) level: (level-1, level-2); type: (internal, external); match: (internal, external-1, external-2); metric: (1-16777215); name: (1-32) символа | Разрешает импорт маршрутов из OSPF в IS-IS. - <i>id</i> – идентификатор процесса OSPF; - <i>level</i> – уровень IS-IS, в который будет выполняться перераспределение маршрутов; - <i>type</i> – установить импортируемым маршрутам тип метрики; - <i>match</i> – тип маршрута OSPF, подлежащий импорту. - <i>metric</i> – значение метрики для импортируемых маршрутов; - <i>name</i> – имя стандартного IP ACL, который будет использован для фильтрации импортируемых маршрутов. Если глобально включен стандартный (narrow) стиль метрики, все значения метрики больше 63 будут указаны в TLV как 63. |

| | | |
|---|--|---|
| no redistribute ospf [<i>id</i>] [level <i>level</i>] [metric-type <i>type</i>] [match <i>match</i>] [metric <i>metric</i>] [filter-list <i>name</i>] | | Без параметров запрещает импорт маршрутов из OSPF в IS-IS. В случае указания параметра возвращает его дефолтное значение. |
|---|--|---|

Команды режима конфигурации интерфейса Ethernet, VLAN:

Вид запроса командной строки:

```
console (config-if) #
```

Таблица 311 – Команды режима конфигурации интерфейса Ethernet, VLAN

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|--|
| ip router isis | -/выключено | Включает протокол маршрутизации IS-IS на текущем интерфейсе. |
| no ip router isis | | Выключает протокол маршрутизации IS-IS на текущем интерфейсе. |
| isis authentication key word [<i>level</i>] | word: (1..20) символов; level: (level-1, level-2)/ level-1-2 | Задать ключ аутентификации в виде текста. Используются для аутентификации HELLO PDU. Данная настройка игнорируется, если для аутентификации указан key-chain. - <i>word</i> – ключ в текстовом виде; - <i>level</i> – уровень IS-IS. |
| no isis authentication key | | Удаляет ключ аутентификации. |
| isis authentication key encrypted <i>encryptedword</i> [<i>level</i>] | encryptedword: (1..128) символов; level: (level-1, level-2)/ level-1-2 | Задает ключ аутентификации в зашифрованном виде (например, пароль в зашифрованном виде, скопированный с другого устройства). Используются для аутентификации HELLO PDU. Данная настройка игнорируется, если для аутентификации указан key-chain. - <i>encryptedword</i> – ключ в зашифрованном виде; - <i>level</i> – уровень IS-IS. |
| no isis authentication key | | Удаляет ключ аутентификации. |
| isis authentication key-chain word [<i>level</i>] | word: (1..32) символа; level: (level-1, level-2)/ level-1-2 | Задать имя связки ключей, которая будет использоваться для аутентификации HELLO PDU. - <i>word</i> – имя связки ключей; - <i>level</i> – уровень IS-IS. |
| no isis authentication key-chain | | Отключает режим использования связки ключей для аутентификации. |
| isis authentication mode {text md5} [<i>level</i>] | level: (level-1, level-2)/level-1-2; По умолчанию аутентификация отключена | Включает аутентификацию в HELLO PDU на текущем интерфейсе и определяет ее тип: - text – аутентификация открытым текстом; - md5 – аутентификация MD5; - <i>level</i> – уровень IS-IS. |
| no isis authentication mode | | Устанавливает значение по умолчанию. |
| isis circuit-type {level-1 level-2-only level-1-2} | -/level-1-2 | Указывает, соседства какого уровня можно формировать на данном интерфейсе. |
| no isis circuit-type | | Устанавливает значение по умолчанию. |
| isis metric <i>metric</i> [<i>level</i>] | metric: (1-16777215)/10; level: (level-1, level-2)/ level-1-2 | Устанавливает метрику для данного интерфейса. - <i>metric</i> – значение метрики. Если глобально включен стандартный (narrow) стиль метрики, все значения метрики больше 63 будут указаны в TLV как 63; - <i>level</i> – уровень IS-IS, для которого будет применяться метрика. |
| no isis metric | | Устанавливает значение по умолчанию. |
| isis passive-interface | -/пассивный режим отключен | Переводит интерфейс в пассивный режим. В этом режиме интерфейс не отправляет и не принимает HELLO PDU. |
| no isis passive-interface | | Устанавливает значение по умолчанию. |
| isis network point-to-point | -/broadcast | Устанавливает тип интерфейса point-to-point. |
| no isis network point-to-point | | Устанавливает значение по умолчанию. |

| | | |
|--|---|---|
| isis hello-padding <i>value</i> | value: (disable, enable, adaptive)/enable | Устанавливает режим работы паддинга hello-сообщений. - <i>disable</i> – отключить паддинг во всех сообщениях hello; - <i>enable</i> – включить паддинг во всех сообщениях hello; - <i>adaptive</i> – включить паддинг до установления соседства. |
| no isis hello-padding | | Устанавливает значение по умолчанию. |
| isis pdu-buff-size <i>size</i> | size (512-9000)/1500 байт | Устанавливает максимальный размер PDU, отправляемых и получаемых на этом интерфейсе. Значение pdu-buff-size должно быть больше значения isp-buff-size. |
| no isis pdu-buff-size | | Устанавливает значение по умолчанию. |

Команды режима конфигурации интерфейса Loopback:

Вид запроса командной строки:

```
console (config-if) #
```

Таблица 312 – Команды режима конфигурации интерфейса Loopback

| Команда | Значение/Значение по умолчанию | Действие |
|---|---|---|
| ip router isis | -/выключено | Включает протокол маршрутизации IS-IS на текущем интерфейсе. |
| no ip router isis | | Выключает протокол маршрутизации IS-IS на текущем интерфейсе. |
| isis circuit-type {level-1 level-2-only level-1-2} | -/level-1-2 | Указывает, соседства какого уровня можно формировать на данном интерфейсе. |
| no isis circuit-type | | Устанавливает значение по умолчанию. |
| isis metric <i>metric</i> [<i>level</i>] | metric: (1-16777215)/10; level: (level-1, level-2)/level-1-2 | Устанавливает метрику для данного интерфейса. - <i>metric</i> – значение метрики. Если глобально включен стандартный (narrow) стиль метрики, все значения метрики больше 63 будут указаны в TLV как 63; - <i>level</i> – уровень IS-IS, для которого будет применяться метрика. |
| no isis metric | | Устанавливает значение по умолчанию. |
| isis passive-interface | -/пассивный режим отключен | Переводит интерфейс в пассивный режим. В этом режиме интерфейс не отправляет и не принимает HELLO PDU. |
| no isis passive-interface | | Устанавливает значение по умолчанию. |

Команды режима Privileged EXEC

Вид запроса командной строки имеет вид:

```
console#
```

Таблица 313 – Команды режима Privileged EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|--|--|--|
| show isis database [<i>level</i>] | level: (level-1, level-2) | Отображает базу данных топологии протокола IS-IS. - <i>level</i> – указывает уровень протокола IS-IS, базу данных которого необходимо отобразить. |
| show isis hostname | - | Отображает известные соответствия SystemID и Hostname. |
| show isis interfaces [<i>gigabitethernet gi_port</i> <i>tengigabitethernet te_port</i> <i>twentyfivegigabitethernet twe_port</i> <i>hundredgigabitethernet hu_port</i> <i>port-channel group</i> <i>loopback loopback</i> <i>vlan vlan_id</i>] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..48); loopback: (1-64); vlan-id: (1-4094) | Отображает информацию об интерфейсах, участвующих в IS-IS. |

| | | |
|--|--|--|
| show isis neighbors [detail] [gigabitethernet gi_port tengigabitethernet te_port twentyfivegigabitethernet twe_port hundredgigabitethernet hu_port port-channel group loopback loopback vlan vlan_id] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..48); loopback: (1-64); vlan-id: (1-4094) | Отображает информацию о соседях. - detail – использование данного параметра позволяет отобразить детальную информацию о соседях. |
| clear isis | - | Сбросить все соседства и очистить таблицу маршрутизации IS-IS. |

5.30.6 Настройка Route-Map

Применение route-map позволяет изменять атрибуты у анонсируемых и принимаемых маршрутов BGP.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console (config) #
```

Таблица 314 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|---|
| system router resources <i>policy-ip-routes [number of IPv4 policy routes]</i> <i>policy-ipv6-routes [number of IPv6 policy routes]</i> | number of IPv4 policy routes: (0..32)/0; number of IPv6 policy routes: (0..32)/0 | Выделяет ресурсы маршрутизации для изменения next-hop у транзитного маршрутизируемого трафика. Команда применяется после перезагрузки. <input checked="" type="checkbox"/> В текущей версии ПО поддерживается работа только IPv4 policy routes. |
| no system router resources | | Устанавливает значение по умолчанию. |
| route-map name [section_id] [permit deny] | name: (0..32) символа; section_id: (1..4294967295) | Создает запись route-map. Переводит командную строку в режим конфигурирования route-map. - name – название route-map; - section_id – номер записи в этой route-map; - permit – применить set команды к маршрутам; - deny – отбросить маршруты. <input checked="" type="checkbox"/> Максимальное количество route-map = 32 (включая секции одного route-map). |
| no route-map name [section_id] [permit deny] | | Удаляет route-map. - name – название route-map; - section_id – удаляет запись с номером section_id. |

Команды режима конфигурации интерфейсов Ethernet, VLAN, интерфейса группы портов

Вид запроса командной строки в режиме конфигурации секции route-map:

```
console (config-route-map) #
```

Таблица 315 – Команды режима конфигурации интерфейса Ethernet, VLAN, интерфейса группы портов

| Команда | Значение/Значение по умолчанию | Действие |
|-----------------------------------|--------------------------------|---|
| ip policy route-map name | name: (0..32) символа | Применяет route-map с именем name для заданного интерфейса. |
| no system router resources | | Удаляет route-map с интерфейса.. |

Команды режима конфигурации секции route-map

Вид запроса командной строки в режиме конфигурации секции route-map:

```
console (config-route-map) #
```

Таблица 316 – Команды режима конфигурации секции route-map

| Команда | Значение/Значение по умолчанию | Действие |
|--|---|--|
| continue <i>section_id</i> [and] | <i>section_id</i> : (1..4294967295). | <p>Задать номер следующей секции route-map, которая будет применена к маршрутам, после применения текущей.</p> <ul style="list-style-type: none"> - <i>section_id</i> – номер записи в этой route-map; - and – указывает, что match установки в этой route-map должны быть логически объединены (AND) с match установками в route-map, обозначенных параметром <i>section_id</i>. <p><input checked="" type="checkbox"/> Создание цепочек route-map (без параметра and) возможно, если тип route-map выставлен в permit.</p> <p><input checked="" type="checkbox"/> Если при создании цепочки применяется параметр and, то все set установки должны находиться в последней секции этой цепочки.</p> |
| no continue | | Сбрасывает установку. |
| match ip [address next-hop route-source] prefix-list <i>name</i> | <i>name</i> : (0..32) символа | <p>Задает соответствие prefix-list и адреса маршрута.</p> <ul style="list-style-type: none"> - address – соответствие prefix-list и ip-адреса маршрута; - next-hop – соответствие prefix-list и next-hop ip-адреса маршрута; - route-source – соответствие prefix-list и ip-адреса источника маршрута; - <i>name</i> – название route-map; <p><input checked="" type="checkbox"/> Чтобы не отбрасывались остальные маршруты, не указанные в prefix-list, необходимо создать пустой route-map и привязать его к текущему через continue.</p> |
| no match ip [address next-hop route-source] prefix-list <i>name</i> | | Сбрасывает соответствие. |
| match local-preference <i>value</i> | <i>value</i> : (1..4294967295). | Задает соответствие маршрута с атрибутом local-preference. |
| no match local-preference | | Сбрасывает соответствие. |
| match metric <i>value</i> | <i>value</i> : (1..4294967295). | Задает соответствие маршрута с атрибутом metric. |
| no match metric | | Сбрасывает соответствие. |
| match origin [igp egp incomplete] | - | <p>Задает соответствие маршрута с атрибутом origin.</p> <ul style="list-style-type: none"> - igp – маршрут был получен из протокола внутренней маршрутизации (например, командой network); - egp – маршрут был выучен по протоколу EGP; - incomplete – маршрут был выучен каким-то иным образом (например, командой redistribute). |
| no match origin | | Сбрасывает соответствие. |
| set as-path path-limit <i>value</i> | <i>value</i> : (0-255) | <p>Добавить к маршруту атрибут AS_PATHLIMIT.</p> <p>Нулевое значение ограничивает анонсирование локально сгенерированных маршрутов, только между iBGP соседями (не будут видны для eBGP).</p> <p>Значение больше 0 означает, что если AS_PATH атрибут имеет больше AS-номеров, чем значение AS_PATHLIMIT, то нужно его отбросить при выходе в eBGP.</p> |
| no set as-path path-limit | | Сбрасывает path-limit. |
| set as-path prepend <i>as_number</i> | <i>as_number</i> : (1-4294967295) | Добавить к атрибуту AS-Path введенные AS номера. |
| no set as-path prepend | | Сбрасывает добавление к AS-Path. |
| set as-path prepend local-as <i>value</i> | <i>value</i> : (0-10) | Добавить к атрибуту AS-Path <i>value</i> номеров Local AS (на выход eBGP-соседу). |

| | | |
|---|---------------------------------------|--|
| no set as-path prepend local-as | | Сбрасывает добавление к AS-Path. |
| set as-path remove <i>as_number</i> | <i>as_number</i> : (0..127) символа | Удалить из атрибута AS-Path указанную AS. |
| no set as-path remove | | Сбрасывает удаление. |
| set ip next-hop <i>ip_address</i> | - | Установить next-hop атрибут маршрута. - <i>ip_address</i> – IP-адрес next-hop. |
| no set ip next-hop | | Сбрасывает установку атрибута next-hop. |
| set local-preference <i>value</i> | value: (1-4294967295) | Установить значение атрибута local-preference. |
| no set local-preference | | Сбрасывает установку атрибута local-preference. |
| set metric <i>value</i> | value: (1-4294967295) | Установить значение атрибута metric. |
| no set metric | | Сбрасывает установку атрибута metric. |
| set next-hop-peer | Атрибут не установлен | Установить значение атрибута next-hop, как адрес соседа. |
| no set next-hop-peer | | Сбрасывает установку атрибута. |
| set origin [<i>igp</i> <i>egp</i> <i>incomplete</i>] | - | Установить значение атрибута origin. - igp – маршрут был получен из протокола внутренней маршрутизации (например, командой network); - egp – маршрут был выучен по протоколу EGP; - incomplete – маршрут был выучен каким-то иным образом (например, командой redistribute). |
| no set origin | | Сбрасывает установку атрибута origin. |
| set weight <i>value</i> | | value: (1-4294967295) |
| no set weight | Сбрасывает установку атрибута weight. | |

Команды режима Privileged EXEC

Все команды доступны для привилегированного пользователя.

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 317 – Команды режима Privileged EXEC

| Команда | Значение/Значение по умолчанию | Действие |
|---------------------------------------|---------------------------------------|--|
| show route-map [<i>name</i>] | name: (0..32) символа | Просмотр информации о созданных route-map. - <i>name</i> – имя route-map. |

5.30.7 Настройка Prefix-List


Prefix-листы позволяют фильтровать принимаемые и анонсируемые маршруты протоколов динамической маршрутизации.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console (config) #
```

Таблица 318 – Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|---|--|
| <code>ip prefix-list list-name [seq seq_value] [description text] {deny permit} ip_address [mask] [ge ge_value] [le le_value]</code> | list-name: (1..32); seq_value: (1..4294967294); text: (0..80) символа; ge_value: (1..32); le_value: (1..32) | Создать Prefix-list. - list-name – имя создаваемого prefix-листа; - seq_value – номер записи в списке префиксов; - text – описание списка префиксов; - deny – запрещающее действие для маршрута; - permit – разрешающее действие для маршрута; - ge_value – соответствие длине префикса, равной или большей, чем настроенная длина префикса; - le_value – соответствие длине префикса, которая равна или меньше настроенной длины префикса.  Если не нашлось ни одного соответствия, то будет применена неявная политика по умолчанию deny any. |
| <code>no ip prefix-list list-name [seq seq_value]</code> | | Удалить созданный Prefix-List. |

Команды режима Privileged EXEC

Все команды доступны для привилегированного пользователя.

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 319 – Команды режима Privileged EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---------------------------------------|---|
| <code>show ip prefix-list [name]</code> | name: (0..32) символа | Просмотр информации о созданных prefix-list. - name – имя prefix-list. |

5.30.8 Настройка связки ключей

Связка ключей позволяет создать набор паролей (ключей) с последующей возможностью настройки времени действия каждого пароля. Созданные пароли могут использоваться протоколами RIP, OSPF, IS-IS для аутентификации.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 320 – Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--------------------------------|---------------------------------------|--|
| <code>key chain word</code> | word: (1..32) символа/- | Создает связку ключей с именем word и входит в режим конфигурации связки ключей. |
| <code>no key chain word</code> | | Удаляет связку ключей с именем word. |

Команды режима конфигурации связки ключей

Вид запроса командной строки в режиме конфигурации связки ключей:

```
console (config-keychain) #
```

Таблица 321 – Команды режима конфигурации связки ключей

| Команда | Значение/Значение по умолчанию | Действие |
|-----------------------------|---------------------------------------|---|
| key <i>key_id</i> | key_id: (1..255)/- | Создает ключ с идентификатором <i>key_id</i> и входит в режим конфигурации ключа. |
| no key <i>key_id</i> | | Удаляет ключ с идентификатором <i>key_id</i> . |

Команды режима конфигурации ключа

Вид запроса командной строки в режиме конфигурации ключа:

```
console (config-keychain-key) #
```

Данный режим доступен из режима конфигурации связки ключей и предназначен для задания самого ключа и его параметров.

Таблица 322 – Команды режима конфигурации ключа

| Команда | Значение/Значение по умолчанию | Действие |
|---|---------------------------------------|--|
| key-string <i>word</i> | <i>word</i> : (1..16) символов/- | Задаёт значение ключа. |
| no key-string | | Удаляет значение ключа. |
| encrypted key-string <i>encryptedword</i> | encryptedword/- | Задаёт значение ключа в зашифрованном виде. - <i>encryptedword</i> – зашифрованный пароль (например, пароль в зашифрованном виде, скопированный с другого устройства). |
| no encrypted key-string | | Удаляет значение ключа. |
| accept-lifetime <i>time_to_start</i> { <i>time_to_stop</i> <i>duration</i> <i>infinite</i> } | -/всегда действителен | Задаёт время жизни ключа, в течение которого ключ будет действителен для сверки с ключом в принимаемых сообщениях. - <i>time_to_start</i> – время и дата начала действия ключа. Задаётся в формате <i>hh:mm:ss month day year</i> ; - <i>time_to_stop</i> – время и дата прекращения действия ключа. Задаётся в формате <i>hh:mm:ss month day year</i> ; - <i>duration</i> – задаёт продолжительность действия ключа в секундах; - <i>infinite</i> – устанавливает бесконечное время действия ключа. |
| no accept-lifetime | | Удалить время жизни ключа. |
| send-lifetime <i>time_to_start</i> { <i>time_to_stop</i> <i>duration</i> <i>infinite</i> } | -/всегда действителен | Задаёт время жизни ключа, в течение которого ключ будет действителен для отправки сообщений. - <i>time_to_start</i> – время и дата начала действия ключа. Задаётся в формате <i>hh:mm:ss month day year</i> . - <i>time_to_stop</i> – время и дата прекращения действия ключа. Задаётся в формате <i>hh:mm:ss month day year</i> . - <i>duration</i> – задаёт продолжительность действия ключа в секундах. - <i>infinite</i> – устанавливает бесконечное время действия ключа. |
| no send-lifetime | | Удалить время жизни ключа. |



Если в какой-то момент времени сразу несколько ключей будут являться действительными, то фактически использоваться будет ключ с наименьшим идентификатором.

Команды режима Privileged EXEC

Вид запроса командной строки имеет вид:

```
console#
```

Таблица 323 – Команды режима Privileged EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|----------------------------|---------------------------------------|--|
| show key chain word | word: (1..32) символа/- | Отображает информацию о связке ключей с именем word. |

Примеры выполнения команд

Создать связку ключей с именем name1 и поместить в неё два ключа. На ключе key 2 настроить временной интервал, в течение которого этот ключ может быть использован для сверки с ключом в принятых пакетах.

```
console(config)#key chain name1
console(config-keychain)#key 1
console(config-keychain-key)#key-string testkey1
console(config-keychain-key)#exit
console(config-keychain)#key 2
console(config-keychain-key)#key-string testkey2
console(config-keychain-key)#accept-lifetime 12:00:00 feb 20 2020
12:00:00 mar 20 2020
```

Показать информацию о созданной связке ключей:

```
console# show key chain name1
```

```
Key-chain name1:
  key 1 -- text (Encrypted) "y9nRgqddPOa7W3O4gfrNBeGhigRuwwp6mWCy69nLuQk="
    accept lifetime (always valid) - (always valid) [valid now]
    send lifetime (always valid) - (always valid) [valid now]
  key 2 -- text (Encrypted) "G7sTS+v5oGJwHBL6UxZyWVPzbqZ/6fIOF3h3NB6wYMM="
    accept lifetime (12:00:00 Feb 20 2020) - (12:00:00 Mar 20 2020)
    send lifetime (always valid) - (always valid) [valid now]
```

5.30.9 *Балансировка нагрузки Equal-Cost Multi-Path (ECMP)*

Балансировка нагрузки ECMP позволяет передавать пакеты одному получателю по нескольким «лучшим маршрутам». Данный функционал предназначен для распределения нагрузки и оптимизации пропускной способности сети. ECMP может работать как со статическими маршрутами, так и с протоколами динамической маршрутизации.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 324 – Команды режима глобальной конфигурации

| Команда | Значение/Значение по умолчанию | Действие |
|---|--------------------------------|---|
| <code>ip maximum-paths maximum_paths</code> | maximum_paths: (1..64)/1 | Задать максимальное количество путей, которые могут быть установлены в FIB для каждого маршрута. <input checked="" type="checkbox"/> Настройка вступит в силу только после сохранения конфигурации и перезагрузки устройства. |
| <code>no ip maximum-paths</code> | | Установить значение по умолчанию. |

5.30.10 Настройка Virtual Router Redundancy Protocol (VRRP)

Протокол VRRP предназначен для резервирования маршрутизаторов, выполняющих роль шлюза по умолчанию. Это достигается путём объединения IP-интерфейсов группы маршрутизаторов в один виртуальный, который будет использоваться как шлюз по умолчанию для компьютеров в сети. На канальном уровне резервируемые интерфейсы имеют MAC-адрес 00:00:5E:00:01:XX, где XX – номер группы VRRP (VRID).

Только один из физических маршрутизаторов может выполнять маршрутизацию трафика на виртуальном IP-интерфейсе (VRRP master), остальные маршрутизаторы в группе предназначены для резервирования (VRRP backup). Выбор VRRP master происходит в соответствии с RFC 5798. Если текущий master становится недоступным – выбор повторяется. Наивысший приоритет имеет маршрутизатор с собственным IP-адресом, совпадающим с виртуальным. В случае доступности он всегда становится VRRP master. Максимальное количество VRRP-процессов для коммутаторов MES2300-xx, MES3300-xx – 255, для коммутаторов MES5312, MES5316A, MES5324A, MES5332A, MES5400-24, MES5400-48, MES5410-48, MES5500-32 – 127.

Команды режима конфигурации интерфейсов Ethernet, VLAN, интерфейса группы портов

Вид запроса командной строки в режиме конфигурации интерфейсов Ethernet, VLAN, интерфейса группы портов:

```
console(config-if)#
```

Таблица 325 – Команды режима конфигурации интерфейса Ethernet, VLAN, интерфейса группы портов

| Команда | Значение/Значение по умолчанию | Действие |
|---|--|--|
| <code>vrrp vrid description text</code> | vrid: (1..255); text: (1..160 символов) | Добавление описания цели или использования для VRRP маршрутизатора с идентификатором vrid. |
| <code>no vrrp vrid description</code> | | Удаление описания VRRP-маршрутизатора. |
| <code>vrrp vrid ip ip_address</code> | | Определение IP-адреса VRRP-маршрутизатора |
| <code>no vrrp vrid ip [ip_address]</code> | vrid: (1..255) | Удаление IP-адреса VRRP с маршрутизатора. Если в качестве параметра не указан IP-адрес, то удалятся все IP-адреса виртуального маршрутизатора, вследствие чего удалится и сам виртуальный маршрутизатор vrid на данном устройстве. |
| <code>vrrp vrid preempt</code> | vrid: (1..255); По умолчанию включено | Включение режима, при котором backup-маршрутизатор с более высоким приоритетом будет пытаться перехватить на себя роль master у текущего master-маршрутизатора с более низким приоритетом. <input checked="" type="checkbox"/> Маршрутизатор, который является владельцем IP-адреса маршрутизатора, будет перехватывать на себя роль master независимо от настроек данной команды. |
| <code>no vrrp vrid preempt</code> | | Установка значения по умолчанию. |
| <code>vrrp vrid priority priority</code> | vrid: (1..255); | Назначение приоритета VRRP-маршрутизатора. |

| | | |
|--|---|--|
| no vrrp vrid priority | priority: (1..254); По умолчанию: 255 для владельца IP-адреса, 100 для остальных | Установка значения по умолчанию. |
| vrrp vrid shutdown | vrid: (1..255); | Выключение VRRP-протокола на данном интерфейсе. |
| no vrrp vrid shutdown | По умолчанию: выключен | Включение VRRP-протокола на данном интерфейсе. |
| vrrp vrid source-ip ip_address | vrid: (1..255); По умолчанию: 0.0.0.0 | Определение реального VRRP-адреса, который будет использоваться в качестве IP-адреса отправителя для VRRP-сообщений. |
| no vrrp vrid source-ip | | Установка значения по умолчанию. |
| vrrp vrid track track_number [decrement decrement_priority] | vrid: (1..255); track_number: (1..64); decrement: (1..253) | Изменяет приоритет VRRP-маршрутизатора при изменении состояния трека. При переходе трека в состояние down приоритет VRRP-маршрутизатора понижается на значение <i>decrement_priority</i> или на 10, если значение <i>decrement_priority</i> не указано. |
| no vrrp vrid track | | Отменяет изменение приоритета VRRP-маршрутизатора. |
| vrrp vrid timers advertise {seconds msec milliseconds} | seconds: (1..40); milliseconds: (50..40950); По умолчанию: 1 сек | Определение интервала между анонсами master-маршрутизатора. Если интервал задан в миллисекундах, то происходит округление вниз до ближайшей секунды для VRRP Version 2 и до ближайших сотых долей секунды (10 миллисекунд) для VRRP Version 3. |
| no vrrp vrid timers advertise [msec] | | Установка значения по умолчанию. |
| vrrp vrid version {2 3 2&3} | -/2 | Определение поддерживаемой версии VRRP протокола. - 2 – поддерживается VRRPv2, определенный в RFC3768. Получаемые VRRPv3-сообщения отбрасываются маршрутизатором. Отправляются только VRRPv2-анонсы; - 3 – поддерживается VRRPv3, определенный в RFC5798, без совместимости с VRRPv2 (8.4, RFC5798). Получаемые VRRPv2-сообщения отбрасываются маршрутизатором. Отправляются только VRRPv3-анонсы; - 2&3 – поддерживается VRRPv3, определенный в RFC5798 с обратной совместимостью с VRRPv2. Получаемые VRRPv2-сообщения обрабатываются маршрутизатором. Отправляются VRRPv2- и VRRPv3-анонсы. |
| no vrrp vrid version | | Установка значения по умолчанию. |
| vrrp vrid checksum exclude pseudo-header | По умолчанию: используется метод расчета контрольной суммы с псевдозаголовком | Включить метод расчета контрольной суммы в заголовке VRRP без учета псевдозаголовка. RFC 3768. |
| no vrrp vrid checksum exclude pseudo-header | | Установить метод расчета контрольной суммы, определенный в RFC5798, по умолчанию. |
| vrrp vrid accept mode [accept drop] | -/drop; vrid: (1..255) | Устанавливает режим работы обработки пакетов, адресованных на виртуальный адрес: - accept – VRRP-маршрутизатор в состоянии Master будет принимать пакеты, адресованные на виртуальный адрес, даже если он не является владельцем этого адреса; - drop – VRRP-маршрутизатор в состоянии Master будет отбрасывать пакеты, адресованные на виртуальный адрес, если он не является владельцем этого адреса. |
| no vrrp vrid accept mode | | Установка значения по умолчанию. |
| vrrp vrid authentication {text word md5 key-chain key md5 key-string { string encrypted md5-string }} | word: (1-8) символов; key: (1-32) символов; string: (1-80) символов; md5-string: (1-128) символов; vrid: (1..255); По умолчанию: аутентификация отключена | Устанавливает режим аутентификации для пакетов VRRP: - text – подстановка в VRRP-пакеты пароля для аутентификации в не зашифрованном виде; - md5 key-chain – подстановка в VRRP-пакеты пароля для аутентификации в зашифрованном виде с помощью сконфигурированного ключа шифрования; - key – сконфигурированный ключ шифрования; - md5 key-string – подстановка в VRRP-пакеты пароля для аутентификации в зашифрованном виде с помощью задания пароля; - string – пароль задается в открытом виде (хранится в зашифрованном виде); - md5-string – пароль задается в зашифрованном виде. |
| no vrrp vrid authentication | | Установка значения по умолчанию. |

Команды режима Privileged EXEC

Все команды доступны для привилегированного пользователя.

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 326 – Команды режима Privileged EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---|--|
| show vrrp [all brief counters interface {gigabitethernet <i>gi_port</i> tengigabitethernet <i>te_port</i> twentyfivegigabitethernet <i>twe_port</i> hundredgigabitethernet <i>hu_port</i> port-channel group vlan <i>vlan_id</i>}] | gi_port: (1..8/0/1..48); te_port: (1..8/0/1..48); twe_port: (1..8/0/1..120); hu_port: (1..8/0/1..32); group: (1..128); vlan_id: (1..4094) | Просмотр краткой или детальной информации для всех или одного настроенного виртуального маршрутизатора VRRP. - all — просмотр информации о всех виртуальных маршрутизаторах, включая отключенные; - brief — просмотр краткой информации о всех виртуальных маршрутизаторах; - counters - отображает счетчики для VRRP. |

Примеры выполнения команд

- Настроить IP-адрес 10.10.10.1 на VLAN 10, использовать этот адрес в качестве адреса виртуального маршрутизатора. Включить VRRP-протокол на интерфейсе VLAN.

```
console(config-vlan)# interface vlan 10  
console(config-if)# ip address 10.10.10.1 /24  
console(config-if)# vrrp 1 ip 10.10.10.1  
console(config-if)# no vrrp 1 shutdown
```

- Посмотреть конфигурацию VRRP:

```
console# show vrrp
```

```
Interface: vlan 10  
Virtual Router 1  
Virtual Router name  
Supported version VRRPv3  
State is Initializing  
Virtual IP addresses are 10.10.10.1(down)  
Source IP address is 0.0.0.0(default)  
Virtual MAC address is 00:00:5e:00:01:01  
Advertisement interval is 1.000 sec  
Preemption enabled  
Priority is 255
```

5.30.11 Настройка протокола Bidirectional Forwarding Detection (BFD)

Протокол BFD позволяет быстро обнаружить неисправности линков. BFD может работать как со статическими маршрутами, так и с протоколами динамической маршрутизации RIP, OSPF, BGP.

В текущей версии ПО реализована работа только с протоколом BGP.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 327 — Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|--|--|
| bfd neighbor ip_addr [interval int] [min-rx min] [multiplier mult_num] | int: (150..1000)/150 min: (150..1000)/150 mult_num: (1..255)/3 | Задать BFD-соседа. - int — минимальный интервал передачи для обнаружения ошибки; - min — минимальный интервал приёма для обнаружения ошибки; - mult_num — количество потерянных пакетов до разрыва сессии. |
| no bfd neighbor ip_addr | | Установить значение по умолчанию. |

Команды режима Privileged EXEC

Все команды доступны для привилегированного пользователя.

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 328 — Команды режима Privileged EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---------------------------------------|--|
| show ip bfd neighbors [ip_addr] [detail] | - | Просмотр информации об активных BFD-соседах. |

5.30.12 Конфигурация виртуальной области маршрутизации (VRF lite)

VRF (Virtual Routing and Forwarding) — это технология, которая позволяет нескольким экземплярам таблицы маршрутизации сосуществовать в одном маршрутизаторе одновременно.

Список поддерживаемых в VRF функций доступен в таблице 332.

Таблица 329 — Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|-----------------------------|---------------------------------------|---|
| ip vrf [vrf_name] | vrf_name: (1..32) символа | Создание виртуальной области маршрутизации. |
| no ip vrf [vrf_name] | | Удаление виртуальной области маршрутизации. |

Таблица 330 — Команды режима конфигурации интерфейса

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--------------------------|---------------------------------------|---|
| ip vrf [vrf_name] | vrf_name: (1..32) символа | Привязка интерфейса к области виртуальной маршрутизации. После ввода команды все созданные в дальнейшем IP-адреса будут ассоциироваться с VRF, к которому был привязан интерфейс. |
| no ip vrf | | Отвязка интерфейса от области виртуальной маршрутизации. |

Таблица 331 — Команды режима EXEC

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|------------------------------------|---------------------------------------|---|
| show ip vrf [all /vrf_name] | vrf_name: (1..32) символа | Вывод информации о созданных виртуальных областях маршрутизации и об L3-интерфейсах, которые в них находятся. |

| <i>Функции</i> | <i>Навигация</i> |
|-----------------------------|--|
| Команды управления системой | 5.4 Команды управления системой |
| Статическая маршрутизация | 5.30 Конфигурация протоколов маршрутизации |
| OSPF | 5.30.3 Настройка протокола OSPF, OSPFv3 |
| BGP | 5.30.4 Настройка протокола BGP (Border Gateway Protocol) |

5.31 Конфигурация VXLAN

VXLAN — это виртуальная расширенная частная сеть (Virtual eXtensible Local Area Network). Данная технология позволяет упаковывать Ethernet-кадры в UDP-сегменты и транспортировать их по IP-сети.

VTEP — Virtual Tunnel End Point, устройство, на котором начинается или заканчивается VXLAN-тоннель. Модели, описываемые в данном руководстве, могут действовать в качестве VTEP.

В качестве control plane для VXLAN используется EVPN. Это расширение протокола BGP, которое позволяет сети передавать информацию о доступности конечного устройства, такую как MAC-адреса уровня 2 и IP-адреса уровня 3. Эта технология плоскости управления использует MP-BGP для распределения MAC-адресов и IP-адресов конечных устройств, где MAC-адреса рассматриваются как маршруты. EVPN позволяет устройствам действовать в качестве VTEP для обмена информацией между собой о доступности своих конечных устройств.



Поддержка VXLAN предоставляется по лицензии.



Для коммутаторов серий MES2300-xx и MES3300-xx технология EVPN/VXLAN не поддерживается.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console (config) #
```

Таблица 333 — Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|--|--|---|
| vxlan word | word: (1..64) символа | Создать VXLAN-инстанс с именем word и перейти в режим его конфигурации. Если VXLAN-инстанс с таким именем уже создан, то перейти в режим его конфигурации. |
| no vxlan word | | Удалить VXLAN с именем word. |
| anycast-gateway mac-address mac_address | mac_address: H.H.H или H:H:H:H:H:H или H-H-H-H-H-H/ не задано | Задать виртуальный MAC-адрес, который заменяет базовый MAC-адрес коммутатора в ARP-сообщениях, исходящих с интерфейсов, на которых данная функция активна. |
| no anycast-gateway mac-address | | Установить значение по умолчанию. |

Команды режима конфигурации VXLAN

Вид запроса командной строки в режиме конфигурации VXLAN:

```
console (config-vxlan) #
```

Таблица 334 — Команды режима конфигурации VXLAN

| Команда | Значение/Значение по умолчанию | Действие |
|---|--|--|
| shutdown | -/no shutdown | Установить административный статус DOWN для VXLAN-инстанса. |
| no shutdown | | Устанавливает значение по умолчанию. |
| vlan vlan-id | vlan-id: (1-4094) | Задать vlan id, который будет связан с VXLAN-инстансом. |
| no vlan | | Удалить связку vlan id с VXLAN-инстансом |
| vni vni-id [ip-routing] | vni-id: (1-16777214) | Задать Virtual Network Identifier (VNI), который будет использоваться в рамках данного VXLAN. - ip-routing — указывает, что данный VNI будет использоваться для инкапсуляции в VXLAN IP-пакетов, маршрутизируемых в VRF. |
| no vni | | Удалить заданный VNI. |
| route-target { export import both } community | community: (ASN2:NN, IPV4:NN, ASN4:NN) | Создает списки импорта и экспорта Route Target Community: - export — добавить Route Target Community к экспортируемой маршрутной информации; - import — импортировать маршрутную информацию с указанным Route Target; - both — указать импорт и экспорт. |
| no route-target { export import both } community | | Удаляет списки импорта и экспорта Route Target Community. |
| mcast-group ip_multicast_address | -/выключено | Включает в текущей VXLAN режим репликации BUM трафика с помощью PIM Multicast и привязывает групповой адрес к данной VXLAN. Этот адрес будет использоваться как адрес назначения в VXLAN пакетах. - ip_multicast_address – групповой IP-адрес. <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"><input checked="" type="checkbox"/></div> <div> <p>Для получения трафика указанной в команде выше группы необходимо включение протокола PIM на интерфейсе loopback с указанием данной группы как статической. Описание соответствующих команд в следующей таблице.</p> </div> </div> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"><input checked="" type="checkbox"/></div> <div> <p>Все VTEP в одном VNI должны использовать один и тот же метод репликации. В случае multicast на всех VTEP в одном VNI должен использоваться один и тот же адрес группы.</p> </div> </div> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"><input checked="" type="checkbox"/></div> <div> <p>Максимальное количество уникальных multicast VXLAN туннелей (multicast групп) 256. Одна multicast группа может быть назначена на несколько VXLAN туннелей.</p> </div> </div> |
| no mcast-group | | Устанавливает значение по умолчанию. |



Для корректной работы VXLAN необходимо установление сессии BGP между loopback-интерфейсами устройств с указанием адреса loopback в качестве bgp router-id.

Команды режима конфигурации интерфейса loopback

Вид запроса командной строки в режиме конфигурации интерфейса loopback имеет вид:

```
Console (config-if) #
```

Таблица 335 — Команды режима конфигурации интерфейса loopback

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---------------------------------------|--|
| <code>ip pim</code> | -/выключено | Включить протокол PIM на интерфейсе. |
| <code>no ip pim</code> | /- | Устанавливает значение по умолчанию. |
| <code>ip igmp static-group ip_multicast_address</code> | | Создает запись (*, G) с указанной мультикастовой группой и добавляет интерфейс loopback в OIL. Отправляет на RP PIM Join с указанным адресом мультикастовой группы. - ip_multicast_address – групповой IP-адрес. |
| <code>no ip igmp static-group ip_multicast_address</code> | | Удаляет запись (*, G) с указанной мультикастовой группой. Отправляет на RP PIM Prune с указанным адресом мультикастовой группы. |

Команды режима конфигурации интерфейса VLAN

Вид запроса командной строки в режиме конфигурации интерфейса VLAN:

```
console (config-if) #
```

Таблица 336 — Команды режима конфигурации интерфейса VLAN

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---------------------------------|---------------------------------------|--|
| <code>anycast-gateway</code> | -/выключено | Включает функцию anycast-gateway на данном интерфейсе. |
| <code>no anycast-gateway</code> | | Устанавливает значение по умолчанию. |

Команды режима конфигурации VRF

Вид запроса командной строки в режиме конфигурации VRF:

```
Console (config-vrf) #
```

Таблица 337 — Команды режима конфигурации VRF

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---------------------------------------|--|
| <code>vni vni-id</code> | vni-id: (1-16777214) | Задать Virtual network Identifier (VNI), который будет использоваться для инкапсуляции в VXLAN IP пакетов, маршрутизируемых в VRF. |
| <code>no vni</code> | | Удалить заданный VNI. |
| <code>route-target {import export both}</code> | ASN2:NN or IPv4:NN or ASN4:NN/- | Задать значение расширенного BGP-комьюнити route-target. - import – импортировать комьюнити; - export – экспортировать комьюнити; - both – экспортировать и импортировать комьюнити. Формат записи комьюнити: ASN2 – 16-битное значение AS; ASN4 – 32-битное значение AS; IPv4 – IPv4-адрес; NN – числовое значение route target. |
| <code>no route-target {import export both}</code> | | Удалить значение комьюнити. |

Команды режима Privileged EXEC

Вид запроса командной строки имеет вид:

```
console#
```

Таблица 338 — Команды режима глобальной конфигурации

| <i>Команда</i> | <i>Значение/Значение по умолчанию</i> | <i>Действие</i> |
|---|---|--|
| show evpn Ethernet-segment {port-channel group es_number mac-address esi} [detailed] | group: (1..48); es_number: (1..16777214); mac_address: Н.Н.Н или Н:Н:Н:Н:Н:Н или Н-Н-Н- Н-Н-Н; esi: Н:Н:Н:Н:Н:Н:Н:Н:Н:Н | Отображает информацию об Ethernet Segment Identifier. |
| show evpn inclusive-multicast [word] | word: (1..64) символа | Отображает информацию о маршрутах типа 3, которые используются для передачи широковещательного, неизвестного одноадресного и многоадресного (BUM) трафика. |
| show evpn mac-ip [word] | word: (1..64) символа | Отображает информацию о маршрутах типа 2, которые используются для передачи информации о MAC-/IP-адресах. |
| show vxlan tunnels [word] | word: (1..64) символа | Отображает информацию обо всех установленных VXLAN-туннелях: - word – имя VXLAN. Отображает информацию об установленных туннелях указанной VXLAN. |
| show vxlan [word] | word: (1..64) символа | Отображает краткую информацию по всем созданным VXLAN-туннелям: - word – имя VXLAN. Отображает детальную информацию по указанной VXLAN. |
| show ip anycast-gateway | - | Выводит информацию об anycast-gateway. |

Пример конфигурации для двух устройств

Между двумя устройствами R1 и R2 установлена BGP-сессия между loopback-интерфейсами.

Включена AF I2vpn evpn для обеспечения установления VXLAN-туннелей и передачи информации об изученных MAC-адресах.

Создан VXLAN-инстанс с именем test_vxlan. К нему привязана VLAN 1000, задан VNI 1000.

Конфигурация 1:

```
no spanning-tree
!
vlan database
vlan 1000
exit
!
vxlan test_vxlan
vni 1000
vlan 1000
exit
!
hostname R1
!
interface TenGigabitEthernet1/0/1
description To_R2
ip address 172.16.1.1 255.255.255.252
exit
!
interface TenGigabitEthernet1/0/3
switchport access vlan 1000
exit
!
interface loopback1
ip address 10.0.0.1 255.255.255.255
exit
```

```
!  
!  
ip route 10.0.0.2 /32 172.16.1.2  
!  
router bgp 65500  
bgp router-id 10.0.0.1  
address-family ipv4 unicast  
exit  
!  
address-family l2vpn evpn  
exit  
!  
neighbor 10.0.0.2  
remote-as 65500  
update-source loopback 1  
address-family ipv4 unicast  
exit  
!  
address-family l2vpn evpn  
exit  
exit  
exit  
!  
!  
end
```

Конфигурация 2:

```
no spanning-tree  
!  
vlan database  
vlan 1000  
exit  
!  
vxlan test_vxlan  
vni 1000  
vlan 1000  
exit  
!  
hostname R2  
!  
interface TenGigabitEthernet1/0/1  
description To_R1  
ip address 172.16.1.2 255.255.255.252  
exit  
!  
interface TenGigabitEthernet1/0/3  
switchport access vlan 1000  
exit  
!  
interface loopback1  
ip address 10.0.0.2 255.255.255.255  
exit  
!  
!  
ip route 10.0.0.1 /32 172.16.1.1  
!  
router bgp 65500  
bgp router-id 10.0.0.2  
address-family ipv4 unicast  
exit  
!  
address-family l2vpn evpn
```

```

exit
!
neighbor 10.0.0.1
remote-as 65500
update-source loopback 1
address-family ipv4 unicast
exit
!
address-family l2vpn evpn
exit
exit
exit
!
!
end

```

Если изучить MAC-адрес на интерфейсе TenGigabitEthernet1/0/3 на R1, то можно проконтролировать его наличие в таблице MAC-адресов на R2.

Посмотреть MAC-адреса, изученные в VXLAN, можно в выводе команды `show mac address-table`. Тип данных адресов указывается как `evpn-vxlan`. Пример вывода:

| Flags: I - Internal usage VLAN | | | |
|--------------------------------|-------------------|-----------|------------|
| Aging time is 300 sec | | | |
| Vlan | Mac Address | Interface | Type |
| 1 | e0:d9:e3:26:d6:00 | 0 | self |
| 1000 | 00:00:00:00:00:10 | 10.0.0.1 | evpn-vxlan |
| 1000 | 0c:9d:92:61:9f:c4 | 10.0.0.1 | evpn-vxlan |
| te1/0/1(I) | e0:d9:e3:17:6b:40 | te1/0/1 | dynamic |
| te1/0/1(I) | e0:d9:e3:17:6b:41 | te1/0/1 | dynamic |

Команды режима конфигурации интерфейса Port-Channel

Вид запроса командной строки режима конфигурации интерфейса:

```
console(config-if)#
```

Таблица 339 — Команды режима конфигурации интерфейса Port-Channel

| Команда | Значение/Значение по умолчанию | Действие |
|--------------------------------------|--------------------------------|---|
| <code>ethernet-segment esi</code> | esi: (1-16777214) | Создать Ethernet Segment Identifier (ESI) с номером esi и перейти в режим конфигурирования. |
| <code>no ethernet-segment esi</code> | | Удалить Ethernet Segment Identifier с номером esi. |

Команды режима конфигурирования ESI

Вид запроса командной строки режима конфигурации ESI:

```
console(config-es)#
```

Таблица 340 — Команды режима конфигурации ESI

| Команда | Значение/Значение по умолчанию | Действие |
|------------------------------------|--|---|
| <code>system-mac system_mac</code> | mac_address: H.H.H или H:H:H:H:H или H-H-H-H-H-H | Задать MAC-адрес, используемый в качестве System ID протокола LACP. |
| <code>no system-mac</code> | | Удалить MAC-адрес. |

6 СЕРВИСНОЕ МЕНЮ, СМЕНА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

6.1 Меню Startup

Меню **Startup** используется для выполнения специальных процедур, таких как восстановление заводских настроек и восстановление пароля.

Для входа в меню **Startup** необходимо прервать загрузку нажатием клавиши **<Esc>** или **<Enter>** в течение первых двух секунд после появления сообщения автозагрузки (по окончании выполнения процедуры POST).

```

Startup Menu
[1] Image menu
[2] Restore Factory Defaults
[3] Boot password
[4] Password Recovery Procedure
[5] Back
Enter your choice or press 'ESC' to exit:
    
```

Для выхода из меню и загрузки устройства нажмите клавишу **<5>**, либо **<Esc>**.



Если в течение 15 секунд (значение по умолчанию) не выбран ни один из пунктов меню, то загрузка устройства продолжится. Время ожидания можно увеличить с помощью команд консоли.

Таблица 341 – Описание меню Startup

| № | Название | Описание |
|-----|--|---|
| <1> | Image menu Выбор активного файла системного ПО | Данная процедура используется для выбора активного файла системного ПО . Если не выбран новый загруженный файл системного ПО активным, то устройство выполнит загрузку с использованием текущего активного образа Image menu. [1] Show current image — просмотр данных о версиях ПО на устройстве; [2] Set current image — выбор активного файла системного ПО; [3] Back. |
| <2> | Restore Factory Defaults Восстановление заводских настроек | Данная процедура используется для удаления конфигурации устройства. Восстановление конфигурации по умолчанию. |
| <3> | Boot password Установка/удаление пароля на начальный загрузчик | Данная процедура используется для установки/удаления пароля на начальный загрузчик . |
| <4> | Password Recovery Procedure Восстановление пароля | Данная процедура используется для восстановления утраченного пароля, она позволяет подключиться к устройству без пароля. Для восстановления пароля нажать клавишу <2> , при последующем подключении к устройству пароль будет проигнорирован. Current password will be ignored! Для возврата в меню Startup нажмите клавишу [enter] . ==== Press Enter To Continue ==== |
| <5> | Back Выход из меню | Для выхода из меню и загрузки устройства нажмите клавишу <Enter> либо <Esc> . |

6.2 Обновление программного обеспечения с сервера TFTP



Сервер TFTP должен быть запущен и настроен на компьютере, с которого будет загружаться программное обеспечение. Сервер должен иметь разрешение на чтение файлов начального загрузчика и/или системного ПО. Компьютер с запущенным TFTP-сервером должен быть доступен для коммутатора (можно проконтролировать, выполнив на коммутаторе команду `ping A.B.C.D`, где A.B.C.D – IP-адрес компьютера).



Обновление программного обеспечения может осуществляться только привилегированным пользователем.

6.2.1 Обновление системного программного обеспечения

Загрузка устройства осуществляется из файла системного программного обеспечения (ПО), который хранится во Flash-памяти. При обновлении новый файл системного ПО сохраняется в специально выделенной области памяти. При загрузке устройство запускает активный файл системного ПО.



Процедура обновления стека коммутаторов не отличается от процедуры обновления одиночного коммутатора. Сначала будет обновлён Master юнит, затем ПО будет загружено на остальные юниты стека.



Если текущая версия ПО 5.5.x.x, то при переходе на актуальную версию ПО 6.x.x рекомендуется воспользоваться инструкцией по обновлению версии ПО в сетевых коммутаторах MES5312 и MES53xxA при переходе с версии 5.5.x.x на 6.0.2 и более поздние, которая находится в разделе "Центр Загрузки".

Для просмотра текущей версии системного программного обеспечения, работающего на устройстве, введите команду `show version`:

```
console# show version
```

```
Active-image: flash://system/images/image1.ros
Version: 5.5.4
Commit: 25503143
MD5 Digest: 6f3757fab5b6ae3d20418e4d20a68c4c
Date: 03-Jun-2016
Time: 19:54:26
Inactive-image: flash://system/images/_image1.ros
Version: 5.5.4
Commit: 16738956
MD5 Digest: d907f3b075e88e6a512cf730e2ad22f7
Date: 10-Jun-2016
Time: 11:05:50
```

Процедура обновления ПО:

Скопировать новый файл программного обеспечения на устройство в выделенную область памяти. Формат команды:

```
boot system tftp://tftp_ip_address/[directory/]filename
```

Пример выполнения команды:

```
console# boot system tftp://10.10.10.1/image1.ros
```

```
26-Feb-2016 11:07:54 %COPY-I-FILECPY: Files Copy - source URL
tftp://10.10.10.1/image.ros destination URL flash://
system/images/mes5324-401.ros
26-Feb-2016 11:08:53 %COPY-N-TRAP: The copy operation was completed successfully

Copy: 20644469 bytes copied in 00:00:59 [hh:mm:ss]
```

Новая версия программного обеспечения станет активной после перезагрузки коммутатора.

Для просмотра данных о версиях программного обеспечения и их активности введите команду **show bootvar**:

```
console#show bootvar
```

```
Active-image: flash://system/images/image1.ros
Version: 5.5.4
MD5 Digest: 0534f43d80df854179f5b2b9007ca886
Date: 01-Mar-2016
Time: 17:17:31
Inactive-image: flash://system/images/_image1.ros
Version: 5.5.4
MD5 Digest: b66fd2211e4ff7790308bafa45d92572
Date: 26-Feb-2016
Time: 11:08:56
```

```
console# reload
```

```
This command will reset the whole system and disconnect your current
session. Do you want to continue (y/n) [n]?
```

Подтвердите перезагрузку вводом **y**.

ПРИЛОЖЕНИЕ А. ПРИМЕРЫ ПРИМЕНЕНИЯ И КОНФИГУРАЦИИ УСТРОЙСТВА

Настройка протокола множества связующих деревьев (MSTP)

Протокол MSTP позволяет строить множество связующих деревьев для отдельных групп VLAN на коммутаторах локальной сети, что позволяет балансировать нагрузку. Для простоты рассмотрим случай с тремя коммутаторами, объединенными в кольцевую топологию.

Пусть VLAN 10, 20, 30 объединяются в первом экземпляре MSTP, VLAN 40, 50, 60 объединяются во втором экземпляре. Необходимо, чтобы трафик VLAN-ов 10, 20, 30 между первым и вторым коммутаторами передавался напрямую, а трафик VLAN-ов 40, 50, 60 передавался транзитом через коммутатор 3. Коммутатор 2 назначим корневым для внутреннего связующего дерева (IST – Internal Spanning Tree) в котором передается служебная информация. Коммутаторы объединяются в кольцо, используя порты te1 и te2. Ниже приведена схема, изображающая логическую топологию сети.



Рисунок А.1 – Настройка протокола множества связующих деревьев

Когда один из коммутаторов выходит из строя либо обрывается канал, множество деревьев MSTP перестраивается, что позволяет минимизировать последствия аварии. Ниже приведен процесс конфигурации коммутаторов. Для более быстрой настройки создается общий конфигурационный шаблон, который загружается на TFTP-сервер и используется впоследствии для настройки всех коммутаторов.

1. Создание шаблона и конфигурация первого коммутатора

```

console# configure
console(config)# vlan database
console(config-vlan)# vlan 10,20,30,40,50,60
console(config-vlan)# exit
console(config)# interface vlan 1
console(config-if)# ip address 192.168.16.1 /24
console(config-if)# exit
console(config)# spanning-tree mode mst
console(config)# interface range TengigabitEthernet 1/0/1-2
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk allowed vlan add 10,20,30,40,50,60
console(config-if)# exit
console(config)# spanning-tree mst configuration
console(config-mst)# name sandbox
console(config-mst)# instance 1 vlan 10,20,30

```

```
console(config-mst)# instance 2 vlan 40,50,60
console(config-mst)# exit
console(config)# do write
console(config)# spanning-tree mst 1 priority 0
console(config)# exit
console#copy running-config tftp://10.10.10.1/mstp.conf
```

Настройка selective-qinq

Добавление SVLAN

Приведенный здесь пример конфигурации коммутатора демонстрирует как добавлять метку SVLAN 20 ко всему входящему трафику за исключением VLAN 27.

```
console# show running-config
```

```
vlan database
vlan 20,27
exit
!
interface tengigabitethernet1/0/5
 switchport mode general
 switchport general allowed vlan add 27 tagged
 switchport general allowed vlan add 20 untagged
 switchport general ingress-filtering disable
 selective-qinq list ingress permit ingress_vlan 27
 selective-qinq list ingress add_vlan 20
exit
!
!
end
```

Подмена CVLAN

В сетях передачи данных довольно часто возникают задачи, связанные с подменой VLAN (например, для коммутаторов уровня доступа существует типовая конфигурация, но пользовательский трафик, VOIP и трафик для управления требуется передавать в разных VLAN на различных направлениях). В этом случае было бы удобно воспользоваться функцией подмены CVLAN для замены типизированных VLAN на VLAN для требуемого направления. Ниже приведена конфигурация коммутатора, в котором осуществляется подмена VLAN 100, 101 и 102 на 200, 201 и 202. Обратная подмена должна осуществляться на этом же интерфейсе:

```
console# show running-config
```

```
vlan database
vlan 100-102,200-202
exit
!
interface tengigabitethernet 1/0/1
 switchport mode trunk
 switchport trunk allowed vlan add 200-202
 selective-qinq list egress override_vlan 100 ingress_vlan 200
 selective-qinq list egress override_vlan 101 ingress_vlan 201
 selective-qinq list egress override_vlan 102 ingress_vlan 202
 selective-qinq list ingress override_vlan 200 ingress_vlan 100
 selective-qinq list ingress override_vlan 201 ingress_vlan 101
 selective-qinq list ingress override_vlan 202 ingress_vlan 102
exit!end
```

ПРИЛОЖЕНИЕ Б. КОНСОЛЬНЫЙ КАБЕЛЬ

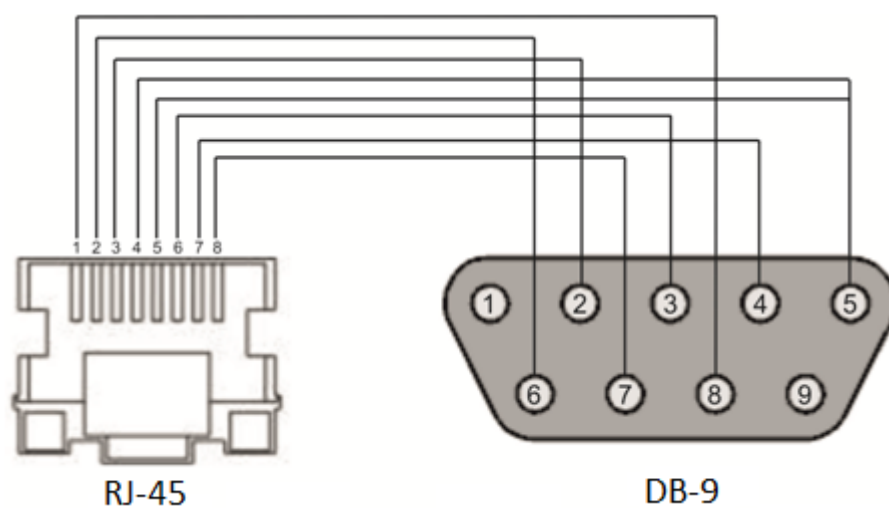


Рисунок Б.1 – Подключение консольного кабеля

ПРИЛОЖЕНИЕ В. ПОДДЕРЖИВАЕМЫЕ ЗНАЧЕНИЯ ETHERTYPE

Таблица В.1 – Поддерживаемые значения EtherType

| | | | | | | | | | |
|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| 0x22DF | 0x8145 | 0x889e | 0x88cb | 0x88e0 | 0x88f4 | 0x8808 | 0x881d | 0x8832 | 0x8847 |
| 0x22E0 | 0x8146 | 0x88a8 | 0x88cc | 0x88e1 | 0x88f5 | 0x8809 | 0x881e | 0x8833 | 0x8848 |
| 0x22E1 | 0x8147 | 0x88ab | 0x88cd | 0x88e2 | 0x88f6 | 0x880a | 0x881f | 0x8834 | 0x8849 |
| 0x22E2 | 0x8203 | 0x88ad | 0x88ce | 0x88e3 | 0x88f7 | 0x880b | 0x8820 | 0x8835 | 0x884A |
| 0x22E3 | 0x8204 | 0x88af | 0x88cf | 0x88e4 | 0x88f8 | 0x880c | 0x8822 | 0x8836 | 0x884B |
| 0x22E6 | 0x8205 | 0x88b4 | 0x88d0 | 0x88e5 | 0x88f9 | 0x880d | 0x8824 | 0x8837 | 0x884C |
| 0x22E8 | 0x86DD | 0x88b5 | 0x88d1 | 0x88e6 | 0x88fa | 0x880f | 0x8825 | 0x8838 | 0x884D |
| 0x22EC | 0x86DF | 0x88b6 | 0x88d2 | 0x88e7 | 0x88fb | 0x8810 | 0x8826 | 0x8839 | 0x884E |
| 0x22ED | 0x885b | 0x88b7 | 0x88d3 | 0x88e8 | 0x88fc | 0x8811 | 0x8827 | 0x883A | 0x884F |
| 0x22EE | 0x885c | 0x88b8 | 0x88d4 | 0x88e9 | 0x88fd | 0x8812 | 0x8828 | 0x883B | 0x8850 |
| 0x22EF | 0x8869 | 0x88b9 | 0x88d5 | 0x88ea | 0x88fe | 0x8813 | 0x8829 | 0x883C | 0x8851 |
| 0x22F0 | 0x886b | 0x88ba | 0x88d6 | 0x88eb | 0x88ff | 0x8814 | 0x882A | 0x883D | 0x8852 |
| 0x22F1 | 0x8881 | 0x88bf | 0x88d7 | 0x88ec | 0x8800 | 0x8815 | 0x882B | 0x883E | 0x9999 |
| 0x22F2 | 0x888b | 0x88c4 | 0x88d8 | 0x88ed | 0x8801 | 0x8816 | 0x882C | 0x883F | 0x9c40 |
| 0x22F3 | 0x888d | 0x88c6 | 0x88d9 | 0x88ee | 0x8803 | 0x8817 | 0x882D | 0x8840 | |
| 0x22F4 | 0x888e | 0x88c7 | 0x88db | 0x88ef | 0x8804 | 0x8819 | 0x882E | 0x8841 | |
| 0x0800 | 0x8895 | 0x88c8 | 0x88dc | 0x88f0 | 0x8805 | 0x881a | 0x882F | 0x8842 | |
| 0x8086 | 0x8896 | 0x88c9 | 0x88dd | 0x88f1 | 0x8806 | 0x881b | 0x8830 | 0x8844 | |
| 0x8100 | 0x889b | 0x88ca | 0x88de | 0x88f2 | 0x8807 | 0x881c | 0x8831 | 0x8846 | |

ПРИЛОЖЕНИЕ Г. ОПИСАНИЕ ПРОЦЕССОВ КОММУТАТОРА

Таблица Г.1 – Описание процессов коммутатора

| Имя процесса | Описание процесса |
|--------------|---|
| 3SMA | Aging для IP-multicast |
| 3SWF | Передача пакетов между уровнем 2 и сетевым уровнем |
| 3SWQ | Программная обработка ACL перехваченных пакетов |
| AAAT | Управление и обработка методов AAA |
| AATT | Симулятор AAA для проверки методов AAA |
| ARPG | Реализация протокола ARP |
| B_RS | Управление перезагрузкой устройств в стеке |
| BFD | Реализация протокола BFD |
| BOXM | Дополнительные действия в стеке (получение сведений о стеке, индикация, обмен сообщениями, смена Unit ID) |
| BOXS | Обработка команд состояния стека: добавление Master/Slave, изучение топологии, обновление версии ПО ведомого устройства (slave) |
| BRGS | Bridge Security – ARP Inspection, DHCP Snooping, DHCP Relay Agent, IP Source Guard |
| BRMN | Bridge Management: STP, операции с FDB (добавление, удаление записей), зеркалирование, конфигурация портов/VLAN, GVRP, GARP, LLDP, IGMP Snooping, IP multicast |
| BSNC | Автомат синхронизации ведущего и ведомого устройств в стеке |
| BTPC | Клиент BOOTP |
| CDB_ | Копирование конфигурационных файлов |
| CNLD | Загрузка/выгрузка конфигурации |
| COPY | Управление копированием файлов |
| CPUT | Утилизация CPU |
| D_LM | Link Manager – отслеживание состояния стек-линков |
| D_SP | Stacking Protocol |
| DDFG | Работа с файловой системой |
| DFST | Распределенная файловая система (DFS). Используется в работе стека |
| DH6C | DHCPv6-клиент |
| DHCP | Сервер и Relay Agent DHCP |
| DHCp | Ping |
| DMNG | Distant Manager – получение информации с удаленных юнитов (версия ПО, uptime, установка активного образа ПО) |
| DNSC | Клиент DNS |
| DNSS | Сервер DNS |
| DSND | Data Set Delays Report |
| DSPT | Dispatcher – обработка событий от удаленных юнитов об изменении состояния вентиляторов, источников питания, термодатчиков, SFP-трансиверов. Получение сообщений от удаленных юнитов об их версии ПО, серийном номере, MD5 сумме ПО. |
| DSYN | Stack application |
| DTSA | Stack application |
| ECHO | Протокол ECHO |
| EPOE | PoE (взаимодействие с пользователем) |
| ESTC | Логирование событий о превышении порогов трафика на CPU (cpu input-rate detailed) |
| EVAP | TRX Training – автоматическая настройка параметров SERDES |
| EVAU | Обработка событий Address Update, нижний уровень, передача выше |
| EVFB | Опрос состояния SFP |
| EVLC | Обработка событий о смене состояния порта, нижний уровень, передача выше |
| EVRT | RX Training |

| | |
|------|--|
| EVRX | Обработка событий приёма пакета из коммутатора в CPU, нижний уровень, передача пакета на уровень 2 |
| EVTX | Обработка событий окончания отправки пакета из CPU в коммутатор, нижний уровень |
| exRX | Обработка выхода пакетов с нижнего уровня 2 |
| FFTT | Управление таблицей маршрутизации и маршрутизация пакетов |
| FHSF | IPv6 First Hop Security (Обработка таймеров) |
| GOAH | Реализация web-сервера GoAhead |
| GRN_ | Реализация Green Ethernet |
| HCLT | Получение и обработка команд настройки устройства нижнего уровня |
| HCPT | PoE (взаимодействие с контроллером) |
| HLTX | Отправка пакетов из CPU в коммутатор |
| HOST | Основной host-поток, холостой ход |
| HSCS | Stack Config – настройка функций коммутатора на удаленном юните |
| HSES | Stack Events – обработка событий link changed, address update с удаленных юнитов на мастере |
| HSEU | Обработка событий стека |
| ICMP | Реализация протокола ICMP |
| IOTG | Управление терминалами ввода-вывода |
| IOTM | Управление терминалами ввода-вывода |
| IOUR | Управление терминалами ввода-вывода |
| IP6C | Счётчики IPv4 и IPv6 |
| IP6M | Маршрутизация IPv4 и IPv6 |
| IPAT | Управление базой данных IP-адресов |
| IPG | Обработка перехваченных фрагментированных IP-пакетов |
| IPRD | Вспомогательная задача для ARP, RIP, OSPF |
| IPMT | Управление IP multicast маршрутизацией и IGMP Proxy |
| IT60 | Задачи для работы с прерываниями |
| IT61 | |
| IT64 | |
| IT99 | |
| IV11 | Задача для работы с виртуальными прерываниями |
| L2HU | Передача пакетов на уровень 3 |
| L2PS | Обработка событий смены состояния/настроек интерфейсов и передача сообщений зарегистрированным службам |
| L2UT | Утилизация портов (show interfaces utilization) |
| LBDR | Реализация функции Loopback Detection |
| LBDT | Отправка пакетов Loopback Detection |
| LTMR | Общая задача для всех таймеров |
| MACT | Обработка события об окончании действия в FDB (aging MAC-адресов) |
| MLDP | Marvell Link Layer Reliable Datagram Protocol, stack transport |
| MNGT | Автотесты |
| MRDP | Marvell Reliable Datagram Protocol, stack transport |
| MROR | Резервирование конфигурационного файла в энергонезависимой памяти |
| MSCm | Менеджер для работы с терминальными сессиями |
| MSRP | Передача событий в стеке пользовательским задачам |
| MSSS | Прослушивание IP-сокетов |
| MUXT | Отслеживание изменений структуры стека |
| NACT | Виртуальное тестирование кабеля (VCT) |
| NBBT | N-Base |
| NINP | Работа с комбо-портами |
| NSCT | Настройка ограничения скорости перехвата пакетов на CPU, ведение статистики по перехваченным пакетам |

| | |
|------|--|
| NSFP | Отслеживание событий, связанных с SFP, на сетевом уровне |
| NSTM | Storm Control |
| NTPL | Периодическая генерация сигнала для опроса таблиц MAC, VLAN, портов, мультикаста, маршрутизации, приоритизации |
| NTST | Добавление и удаление юнитов в стеке, сброс на дефолт состояния юнита, на сетевом уровне |
| NVCT | Вспомогательная задача для VCT. Запуск теста и отслеживание изменения состояния порта. |
| OBSR | Задача для отслеживания и уведомления об изменениях специфических параметров интерфейсов, необходимых для LLDP, CDP и других протоколов. |
| PLCR | Обработка событий смены состояния портов устройств стека |
| PLCT | Обработка событий смены состояния портов |
| PNGA | Реализация ping |
| POLI | Policy Management |
| PTPT | Precise Time Protocol |
| RADS | RADIUS-сервер |
| RCDS | Клиент Remote CLI |
| RCLA | Сервер Remote CLI |
| RCLB | |
| RELY | DHCPv6 Relay |
| ROOT | Родительский таск для всех задач |
| RPTS | Routing protocol |
| SCLC | Отслеживание состояния OOB-порта |
| SCPT | Автообновление и автоконфигурация |
| SCRX | Получение трафика с OOB-порта |
| SEAU | Получение событий Address Update, нижний уровень |
| SELC | Получение событий о смене состояния порта, нижний уровень |
| SERT | Отслеживание событий на порту для начала процедуры RX Training |
| SERX | Получение событий приёма пакета из коммутатора в CPU, нижний уровень |
| SETX | Получение событий окончания отправки пакета из CPU в коммутатор, нижний уровень |
| SFMG | sFlow Manager – обработка событий изменения IP-адреса, запросов CLI/SNMP, таймеров |
| SFSM | sFlow Sampler |
| SFTR | Протокол Sflow |
| SNAD | База данных SNA |
| SNAE | Обработка событий SNA |
| SNAS | Сохранение базы данных SNA в ПЗУ |
| SNMP | Реализация протокола SNMP |
| SNTP | Реализация протокола SNTP |
| SOCK | Управление работой сокетов |
| SQIN | Настройка Selective QinQ |
| SS2M | Slave To Master – передача сообщений с ведомого устройства (slave) на ведущее (master) |
| SSHP | Сервер SSH – настройка, обработка команд, таймер |
| SSHU | Сервер SSH – протокол |
| SSLP | Реализация SSL |
| SSTC | Логирование событий о превышении порогов трафика на CPU (cpu input-rate detailed) |
| STMB | Обработка SNMP-запросов о статусе стека |
| STSA | CLI-сессия через COM-порт |
| STSB | CLI-сессия через VLAN |
| STSC | CLI-сессия через VLAN |
| STSD | CLI-сессия через VLAN |

| | |
|------|---|
| STSE | CLI-сессия через VLAN |
| SW2M | Обработка событий Address Update от FDB, блокировка порта при возникновении ошибки на порту |
| SYLG | Вывод сообщений в syslog |
| TBI_ | Таблица временных промежутков для ACL |
| TCP | Реализация протокола TCP |
| TFTP | Реализация протокола TFTP |
| TMNG | Управление приоритетами задач |
| TNSL | Клиент Telnet |
| TNSR | Сервер Telnet |
| TRCE | Реализация traceroute |
| TRIG | Запуск действия в FDB (aging MAC-адресов) |
| TRMT | Управление юнитами в стеке с поддержкой транзакций |
| TRNS | File Transfer – копирование файлов между юнитами стека (ПО) |
| UDPR | UDP Relay |
| URGN | Обработка критических событий (например, перезагрузки) |
| VRRP | Реализация протокола VRRP |
| WBAM | Web-based Authentication |
| WBSO | Взаимодействие с web-клиентами, нижний уровень |
| WBSR | Управление и таймеры web-сервера |
| WNTT | Поддержка NAT для WBA |
| XMOD | Реализация протокола X-modem |

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения технической консультации по вопросам эксплуатации оборудования ООО «Предприятие «ЭЛТЕКС» вы можете обратиться в Сервисный центр компании:

Форма обратной связи на сайте: <https://eltex-co.ru/support/>

Servicedesk: <https://servicedesk.eltex-co.ru/>

На официальном сайте компании вы можете найти техническую документацию и программное обеспечение для продукции ООО «Предприятие «ЭЛТЕКС», обратиться к базе знаний или оставить интерактивную заявку:

Официальный сайт компании: <https://eltex-co.ru/>

База знаний: <https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base>

Центр загрузок: <https://eltex-co.ru/support/downloads>