Комплексные решения для построения сетей

MES3000

MES3108, MES3108F, MES3116, MES3116F, MES3124, MES3124F, MES3224, MES3224F

Руководство по эксплуатации, версия ПО 2.5.46

Коммутаторы магистрального уровня, коммутаторы уровня агрегации

Версия документа	Дата выпуска	Содержание изменений
Версия 1.31		Добавлены разделы: - 5.8.3 Функция Private vlan - 5.26 Функции Lightweight DHCPv6 Relay Agent (LDRA) Изменения в разделах: - 5.6.2 Команды для работы с файлами - 5.8 Конфигурирование интерфейсов и VLAN - 5.11 Группы агрегации каналов – Link Agregation Group (LAG) - 5.15.8 Настройка протокола G.8032v2 (ERPS) - 5.15.5.1 Настройка протокола STP, RSTP - 5.15.12 Настройка функции Layer 2 Protocol Tunneling (L2PT) - 5.17.1 Правила групповой адресации (multicast addressing) - 5.17.2 Функция посредника протокола IGMP (IGMP Snooping) - 5.19 Журнал аварий, протокол SYSLOG - 5.24.3 Контроль протокола DHCP и опции 82 - 5.25 Функции DHCP Relay посредника - 5.27 Конфигурирование PPPoE Intermediate Agent - 5.29 Конфигурирование ACL (списки контроля доступа) - 5.31.1 Настройка QoS
Версия 1.30	23.06.2016	Изменения в разделах: - 5.4 Команды управления системой - 5.8.2 Настройка VLAN и режимов коммутации интерфейсов - 5.8.3 Настройка интерфейса IP - 5.14.1 Протокол ipv6 - 5.15.5 Семейство протоколов STP (STP, RSTP, MSTP) - 5.19 Журнал аварий, протокол SYSLOG - 5.27 Конфигурирование DHCP-сервера - 5.28.1 Конфигурирование ACL на базе IPv4 - 5.30 Качество обслуживания QoS
Версия 1.29	10.02.2016	Изменения в разделах: - 5.8 Конфигурирование интерфейсов - 5.10 Контроль широковещательного «шторма» - 5.17 Групповая адресация - 5.18.4 Протокол управления сетью (SNMP) - 5.24.2 Проверка подлинности клиента на основе порта (стандарт 802.1x) - 5.24.3 Контроль протокола DHCP и опция 82 - 5.24.4 Защита IP-адреса клиента (IP-source Guard) - 5.24.5 Контроль протокола ARP (ARP Inspection) - 5.24.6 Настройка функции MAC Address Notification - 5.28.1 Конфигурирование ACL (списки контроля доступа) - 6.2 Обновление программного обеспечения с сервера TFTP Добавлено: - 2.2.3 Функция Layer 2 Protocol Tunneling (L2PT)
Версия 1.28	15.10.2015	Изменения в разделах: - 5.17.5 Функция многоадресной маршрутизации IGMP Proxy - 5.31.3 Настройка протокола OSPF
Версия 1.27	1.09.2015	Изменения в разделах: - 2.2.8 Дополнительные функции - 5.4 Команды управления системой - 5.8 Конфигурирование интерфейсов - 5.10 Контроль широковещательного «шторма» - 5.11 Группы агрегации каналов – Link Agregation Group (LAG) - 5.15.2 Настройка протокола ARP - 5.15.6 Настройка функции flex-link - 5.17.5 Функция многоадресной маршрутизации IGMP Proxy - 5.18.1 Механизм AAA - 5.20 Зеркалирование (мониторинг) портов - 5.30.5 Настройка Virtual Router Redundancy Protocol (VRRP) - 5.30.1 Настройка QoS Добавлен раздел: - 5.23 IP Service Level Agreements (IP SLA)
Версия 1.26	03.06.2015	Изменения в разделах: - 5.15.4 Механизм обнаружения петель (loopback-detection) - 5.15.5 Семейство протоколов STP

		- 5.18.2 Протокол RADIUS - 5.23.2. Проверка подлинности клиента на основе порта (стандарт 802.1x) - 5.23.3 Контроль протокола DHCP и опция 82 - 5.24 Функции DHCP Relay посредника
Версия 1.25	11.03.2015	Изменения в разделах: - 5.8.2 Настройка интерфейса VLAN - 5.10 Контроль широковещательного «шторма» - 5.17.2 Функция посредника протокола IGMP (IGMP Snooping) - 5.18.4 Протокол управления сетью (SNMP) - 5.23.2.2 Расширенная проверка подлинности
Версия 1.24	26.01.2015	Изменения в разделах: -5.6.3 Команды для резервирования конфигурации -5.24 Функции DHCP Relay посредника Добавлены разделы: -5.15.6 Настройка функции flex-link
Версия 1.23	25.11.2014	Изменения в разделах: - 5.18.1 Механизм AAA - 5.30.5 Настройка протокола Virtual Router Redundancy Protocol (VRRP) Добавлены разделы: - 5.14.3 Настройка функции IPv6 RA guard - 5.14.4 Настройка функции DHCPv6 guard
Версия 1.22	21.10.2014	Изменения в разделах: - 5.8.2 Настройка интерфейса Vlan - 5.10 Контроль широковещательного «шторма»
Версия 1.21	13.10.2014	Изменения в разделах: - 5.11 Группы агрегации каналов - 5.15.6 Протокол EAPS
Версия 1.20	26.08.2014	Изменения в разделах: - 5.4 Команды управления системой - 5.15.6 Протокол EAPS - 5.24 Функции DHCP Relay посредника - 5.30.3 Настройка протокола OSPF - Приложение А: Настройка Multicast-tv
Версия 1.19	28.07.2014	Изменения в разделах: - 5.12Настройка IPv4-адресации - 5.18.7.1 Telnet, SSH, HTTP и FTP Добавлены разделы: - 5.8.3 Настройка IP-интерфейса
Версия 1.18	29.05.2014	Изменения в разделах: - 5.8.2 Настройка интерфейса VLAN - 5.9 Selective Q-in-Q - 5.30.3 Настройка протокола OSPF Добавлены разделы: - 5.30.4 Настройка протокола BFD
Версия 1.17	29.04.2014	Изменение раздела: - 5.8.1 Параметры Ethernet-интерфейсов и интерфейсов Port-Channel
Версия 1.16	01.04.2014	Изменения в раздела: - 5.22.1 Диагностика медного кабеля
Версия 1.15	29.01.2014	Изменения в разделах: - 5.17.2 Функция посредника протокола IGMP (IGMP Snooping)
Версия 1.14	05.12.2013	Изменения в разделах: - 2.2 Функции коммутатора Добавлены разделы: - 5.30.4 Настройка Virtual Router Redundancy Protocol (VRRP)
Версия 1.13	22.11.2013	Изменения в разделах: - 5.15.5 Семейство протоколов STP (STP, RSTP, MSTP) - 5.8.1 Параметры Ethernet-интерфейсов и интерфейсов Port-Channel - 5.18.2 Протокол RADIUS - 5.20 Зеркалирование (мониторинг) портов Добавлены разделы: - 5.2 Фильтрация сообщений командной строки

Версия 1.12	02.10.2013	Изменения в разделах: - 4.4.2 Работа коммутатора в режиме стекирования - 5.6 Настройки системного времени - 5.16.2 Функция посредника протокола IGMP (IGMP Snooping) - 5.29.3 Настройка протокола OSPF
Версия 1.11	15.08.2013	Изменения в разделах: - 5.26.1 Конфигурирование ACL на базе IPv4 - 5.26.2 Конфигурирование ACL на базе IPv6 - 5.26.3 Конфигурирование ACL на базе MAC
Версия 1.10	18.06.2013	Добавлены разделы: - 5.5.3 Команды для резервирования конфигурации - 5.14.7 Настройка протокола G.8032v2 (ERPS) - 5.14.9 Настройка протокола OAM - 5.14.10 Настройка протокола CFM Изменения в разделах: - 4.1 Настройка терминала - 5.9 Контроль широковещательного «шторма» - 5.17.2 Протокол RADIUS - 5.17.3 Протокол TACACS+ - 5.17.4 Протокол управления сетью (SNMP) - 5.17.1 Механизм AAA - 5.17.7.1Telnet, SSH, HTTP и FTP - 5.17.7.2 Команды конфигурирования терминала - 5.21.2 Диагностика оптического трансивера
Версия 1.9	20.03.2013	Добавлены разделы: - 5.17.4 Функции ограничения multicast-трафика Изменения в разделах: - 5.17.2 Функция посредника протокола IGMP (IGMP Snooping) - 5.18.1 Механизм AAA - 5.18.7 Настройка доступа - 5.23.3 Контроль протокола DHCP и опция 82 - 5.25 Конфигурирование PPPoE Intermediate Agent
Версия 1.8	06.03.2013	Изменения в разделах: - 5.3. Добавлено описание конфигурирования функций мониторинга и защиты CPU. - 5.7.1. Добавлено описание конфигурирования функций мониторинга нагрузки на интерфейсах. - 5.7.2. Добавлено описание конфигурирования MAC-based vlan, EtherType для исходящих пакетов. - 5.16.1. Добавлено описание конфигурирования изучения MAC-адресов во VLAN. - 5.16.2 Функция посредника протокола IGMP (IGMP Snooping). - 5.17.4. Добавлено описание конфигурирования SNMP trap-сообщений на портах. - 5.19. Добавлено описание конфигурирования удаленного зеркалирования. - 5.22.3. Добавлено описание конфигурирования формата DHCP опции 82. Добавлены разделы: - 5.24 Конфигурирование PPPoE Intermediate Agent. - 5.28.3 Настройка протокола OSPF. - Приложение Б Типовые схемы построения сетей на базе протокола EAPS -Приложение В Описание процессов коммутатора
Версия 1.7	27.11.2012	Изменения в разделе: - 2.3 Основные технические характеристики - 4.4.2 Работа коммутатора в режиме стекирования - 5.10 Группы агрегации каналов – Link Agregation Group (LAG)
Версия 1.6	10.09.2012	Изменения в разделе: - 5.21 Функции диагностики физического уровня
Версия 1.5	24.08.2012	Добавлено описание функции MAC Address Notification. Изменения в разделах: - 5.5.2 Команды для работы с файлами - 7.2.1 Добавление SVLAN - 7.2.2 Подмена CVLAN

Версия 1.4	04.07.2012	Поддержка работы устройств в режиме стекирования. Добавлено описание MES3224, MES3224F.
Версия 1.3	20.12.2011	Изменения в разделах: - 5.8 Selective Q-in-Q - 7.2 Настройка selective-qinq
Версия 1.2	01.12.2011	Добавлено описание конфигурирования протокола EAPS. Поддержка протокола – начиная с версии 2.1.12
Версия 1.1	30.08.2011	Добавлено описание функции IGMP Proxy. Функция поддержана в ПО начиная с версии 2.1.8
Версия 1.0	10.06.2011	Первая публикация.
Версия программного обеспечения	**2.5.46**	

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ 10
2 ОПИСАНИЕ ИЗДЕЛИЯ 11
2.1 Назначение 11
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 15
2.2.6 Функции обеспечения безопасности 15
2.2.7 Функции управления коммутатором 16
2.2.8 Дополнительные функции 18
2.3 Основные технические характеристики 18
2.4 Конструктивное исполнение 21
2.4.1 Передняя панель устройства 21
2.4.2 Задняя панель устройства 23
2.4.3 Боковые панели устройства 24
2.4.4 Световая индикация 24
2.5 Комплект поставки 26
3 УСТАНОВКА И ПОДКЛЮЧЕНИЕ 27
3.1 Крепление кронштейнов 27
3.2 Установка устройства в стойку 27
3.3 Установка модулей питания 29
3.4 Подключение питающей сети 29
3.5 Установка и удаление SFP-трансиверов 30
4 НАЧАЛЬНАЯ НАСТРОЙКА КОММУТАТОРА 31
4.1 Настройка терминала 31
4.2 Включение устройства 31
4.3 Загрузочное меню 32
4.4 Режимы работы коммутатора 33
4.4.1 Выбор режима работы коммутатора 33
4.4.2 Работа коммутатора в режиме стекирования 33
4.5 Настройка функций коммутатора 35
4.5.1 Базовая настройка коммутатора 35
4.5.2 Настройка параметров системы безопасности 38
4.5.3 Настройка баннера 40
5 УПРАВЛЕНИЕ УСТРОЙСТВОМ. ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ 41
5.1 Базовые команды 42
5.2 Фильтрация сообщений командной строки 44
5.3 Настройка макрокоманд 44
5.4 Команды управления системой 45
5.5 Команды для настройки параметров для задания паролей 50
5.6 Работа с файлами 51
5.6.1 Описание аргументов команд 51
5.6.2 Команды для работы с файлами 51
5.6.3 Команды для резервирования конфигурации 54
5.6.4 Команды для автоматического обновления и конфигурирования 55
5.7 Настройка системного времени 56
5.8 Конфигурирование интерфейсов и VLAN 60
5.8.1 Настройка параметров Ethernet-интерфейсов и интерфейсов Port-Channel 61
5.8.2 Настройка VLAN и режимов коммутации интерфейсов 68
5.8.3 Настройка Private VLAN 76

5.8.4 Настройка интерфейса IP 79
5.9 Selective Q-in-Q 80
5.10 Контроль широковещательного «шторма» 81
5.11 Группы агрегации каналов – Link Agregation Group (LAG) 83
5.11.1 Статические группы агрегации каналов 84
5.11.2 Протокол агрегации каналов LACP 84
5.12 Настройка IPv4-адресации 86
5.13 Настройка Green Ethernet 88
5.14 Настройка IPv6-адресации 89
5.14.1 Протокол IPv6 89
5.14.2 Туннелирование протокола IPv6 (ISATAP) 93
5.14.3 Настройка функции IPv6 RA guard 94
5.14.4 Настройка функции DHCPv6 guard 95
5.15 Настройка протоколов 96
5.15.1 Настройка протокола DNS – системы доменных имен 96
5.15.2 Настройка протокола ARP 97
5.15.3 Настройка протокола GVRP 98
5.15.4 Механизм обнаружения петель (loopback-detection) 100
5.15.5 Семейство протоколов STP (STP, RSTP, MSTP) 102
5.15.6 Настройка функции flex-link 108
5.15.7 Протокол EAPS 109
5.15.8 Настройка протокола G.8032v2 (ERPS) 111
5.15.9 Настройка протокола LLDP 112
5.15.10 Настройка протокола OAM 118
5.15.11 Настройка протокола CFM 120
5.15.12 Настройка функции Layer 2 Protocol Tunneling (L2PT) 123
5.16 Voice VLAN 127
5.17 Групповая адресация 128
5.17.1 Правила групповой адресации (multicast addressing) 128
5.17.2 Функция посредника протокола IGMP (IGMP Snooping) 134
5.17.3 MLD snooping – протокол контроля многоадресного трафика в IPv6 138
5.17.4 Функции ограничения multicast-трафика 140
5.17.5 Функция многоадресной маршрутизации IGMP Proxy 142
5.18 Функции управления 144
5.18.1 Механизм AAA 144
5.18.2 Протокол RADIUS 148
5.18.3 Протокол TACACS+ 151
5.18.4 Протокол управления сетью (SNMP) 152
5.18.5 Протокол удалённого мониторинга сети (RMON) 157
5.18.6 Списки доступа ACL для управления устройством 164
5.18.7 Настройка доступа 165
5.19 Журнал аварий, протокол SYSLOG 169
5.20 Зеркалирование (мониторинг) портов 171
5.21 Функция sFlow 173
5.22 Функции диагностики физического уровня 174
5.22.1 Диагностика медного кабеля 175
5.22.2 Диагностика оптического трансивера 177
5.23 IP Service Level Agreements (IP SLA) 179
5.23.1 Операция ICMP Echo 180
5.23.2 Операция UDP Jitter 182
5.24 Функции обеспечения безопасности 185
5.24.1 Функции обеспечения защиты портов 185
5.24.2 Проверка подлинности клиента на основе порта (стандарт 802.1x) 186
5.24.3 Контроль протокола DHCP и опции 82 194

5.24.4 Защита IP-адреса клиента (IP-source Guard) ... 199
5.24.5 Контроль протокола ARP (ARP Inspection) ... 201
5.24.6 Настройка функции MAC Address Notification ... 204
5.25 Функции DHCP Relay посредника ... 205
5.26 Функции Lightweight DHCPv6 Relay Agent (LDRA) ... 207
5.27 Конфигурирование PPPoE Intermediate Agent ... 208
5.28 Конфигурирование DHCP-сервера ... 211
5.29 Конфигурирование ACL (списки контроля доступа) ... 214
5.29.1 Конфигурирование ACL на базе IPv4 ... 216
5.29.2 Конфигурирование ACL на базе IPv6 ... 220
5.29.3 Конфигурирование ACL на базе MAC ... 223
5.30 Конфигурирование защиты от DoS-атак ... 224
5.31 Качество обслуживания - QOS ... 225
5.31.1 Настройка QoS ... 226
5.31.2 Статистика QoS ... 234
5.32 Конфигурация протоколов маршрутизации ... 235
5.32.1 Конфигурация статической маршрутизации ... 235
5.32.2 Настройка протокола RIP ... 237
5.32.3 Настройка протокола OSPF ... 239
5.32.4 Настройка протокола BFD ... 242
5.32.5 Настройка Virtual Router Redundancy Protocol (VRRP) ... 242
6 СЕРВИСНОЕ МЕНЮ, СМЕНА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ... 245
6.1 Меню Startup ... 245
6.2 Обновление программного обеспечения с сервера TFTP ... 247
6.2.1 Обновление системного программного обеспечения ... 247
6.2.2 Обновление загрузочного файла устройства (начального загрузчика) ... 248
ПРИЛОЖЕНИЕ А ПРИМЕРЫ ПРИМЕНЕНИЯ И КОНФИГУРИРОВАНИЯ УСТРОЙСТВА ... 250
Настройка протокола множества связующих деревьев (MSTP) ... 250
Настройка selective-qinq ... 252
Добавление SVLAN ... 252
Подмена CVLAN ... 252
Настройка функции IGMP Proxy ... 253
Настройка multicast-TV VLAN ... 253
ПРИЛОЖЕНИЕ Б ТИПОВЫЕ СХЕМЫ ПОСТРОЕНИЯ СЕТЕЙ НА БАЗЕ ПРОТОКОЛА EAPS ... 256
ПРИЛОЖЕНИЕ В ОПИСАНИЕ ПРОЦЕССОВ КОММУТАТОРА ... 258

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

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.

Для достижения высоких скоростей широко применяются технологии передачи информации Gigabit Ethernet (GE) и 10Gigabit Ethernet (10GE). Передача информации на больших скоростях, особенно в сетях крупного масштаба, подразумевает выбор такой топологии сети, которая позволяет гибко осуществлять распределение высокоскоростных потоков.

Коммутаторы серии MES3000 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) в сочетании с высокой надежностью за счет резервирования узлов, определяющих бесперебойность функционирования – модулей питания и модулей вентиляции.

Варианты исполнения коммутаторов серии MES3000:

- MES3124: 24 порта 10/100/1000Base-T, 4 порта 10GBaseX(SFP+) или 1000Base-X(SFP);
- MES3124F: 20 портов 1000Base-X(SFP), 4 комбинированных порта 10/100/1000Base-T/ 1000Base-X(SFP), 4 порта 10GBase-X(SFP+) или 1000Base-X(SFP);
- MES3116: 16 портов 10/100/1000Base-T, 2 порта 10GBaseX(SFP+) или 1000Base-X(SFP);
- MES3116F: 12 портов 1000Base-X(SFP), 4 комбинированных порта 10/100/1000Base-T/ 1000Base-X(SFP), 2 порта 10GBase-X(SFP+) или 1000Base-X(SFP);
- MES3108: 8 портов 10/100/1000Base-T, 2 порта 10GBaseX(SFP+) или 1000Base-X(SFP);
- MES3108F: 4 порта 1000Base-X(SFP), 4 комбинированых порта 10/100/1000Base-T/ 1000Base-X(SFP), 2 порта 10GBase-X(SFP+) или 1000Base-X(SFP);
- MES3224: 24 порта 10/100/1000 Base-T, 2 порта 10GBaseX(SFP+) или 1000Base-X(SFP), 2 порта 10GBase-LR/ER/ZR (XFP);
- MES3224F: 20 портов 1000 Base-X(SFP), 4 комбинированных порта 10/100/1000Base-T/ 1000Base-X(SFP), 2 порта 10GBase-X(SFP+) или 1000Base-X(SFP), 2 порта 10GBase-LR/ER/ZR (XFP).

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

2 ОПИСАНИЕ ИЗДЕЛИЯ

2.1 Назначение

Устройства серии MES3000 являются мощными многоцелевыми сетевыми коммутаторами, выполняющими свои коммутационные функции на канальном и сетевом уровнях модели OSI. Коммутаторы серии MES3000 обеспечивают высокую плотность электрических/оптических гигабитных портов, позволяют совмещать на одном устройстве оптические и электрические соединения за счет наличия комбинированных интерфейсов, имеют высокоскоростные порты, способные работать на скоростях 1Гбит/с и 10Гбит/с, что позволяет постепенно наращивать производительность сети переходя от скоростей 1Гбит/с к скоростям 10Гбит/с по мере необходимости.

2.2 Функции коммутатора

2.2.1 Базовые функции

В таблице 2.1 приведен список базовых функций устройств серии MES3000, доступных для администрирования.

Таблица 2.1 – 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 обратного давления (Back pressure)	Метод обратного давления используется на полудуплексных соединениях для регулирования потока данных от встречного устройства путем создания коллизий. Метод позволяет избежать переполнения буферной памяти устройства и потери данных.
Поддержка MDI/MDIX	Автоматическое определение типа кабеля - перекрестный кабель или кабель прямого подключения. – MDI (Media-Dependent Interface – прямой) – стандарт кабелей для подключения оконечных устройств; – MDIX (Media-Dependent Interface with Crossover – перекрестный) - стандарт кабелей для подключения концентраторов и коммутаторов.
Поддержка 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 2.2 приведены функции устройств серии MES3000 при работе с MAC–адресами.

Таблица 2.2 – 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 маршрутизации. 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 маршрутизации.
Функция 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.

2.2.3 Функции второго уровня сетевой модели OSI

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

Таблица 2.3 – Описание функций второго уровня (уровень 2 OSI)

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.
Функция MVR	Функция, позволяющая перенаправлять многоадресный трафик из одной VLAN в другую на основании IGMP-сообщений, что позволяет уменьшить нагрузку на uplink-порту. Применяется в решениях III-play.
Защита от широковещательного «шторма» (Broadcast Storm Control)	Широковещательный шторм – это размножение широковещательных сообщений в каждом узле, которое приводит к лавинообразному росту их числа и парализует работу сети. Устройства MES3000 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), находящимися 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	Обеспечивает изоляцию между устройствами, находящимися в одном широковещательном домене, в пределах всей L2-сети. Реализованы режимы работы порта: Promiscious, Isolated (Isolated-порты не могут обмениваться друг с другом) и Community (порты могут обмениваться между собой и Promiscious-портом)
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.
Поддержка протокола RSTP (IEEE 802.1w Rapid spanning tree protocol)	Rapid (быстрый) STP (RSTP) – является усовершенствованием протокола STP, характеризуется меньшим временем приведения сети к древовидной топологии и имеет более высокую устойчивость.
Поддержка функционала Layer 2 Protocol Tunneling (L2PT)	Layer 2 Protocol Tunneling (L2PT) позволяет пропускать служебные пакеты (PDU) L2-протоколов через сеть провайдера, что обеспечивает «прозрачную» связь клиентских сегментов сети.
Протокол EAPS	EAPS (Ethernet Automatic Protection Switching) – протокол, обеспечивающий исключение зацикливания трафика в сетях с кольцевой топологией, а также предназначенный для быстрого восстановления прохождения трафика в случае аварии на отдельном участке сети. EAPS обеспечивает время восстановления существенно меньше, чем протоколы Spanning Tree.
Протокол ERPS (Ethernet Ring Protection Switching)	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.
Поддержка VLAN	VLAN – это группа портов коммутатора, образующих одну широковещательную область (домен). Коммутатор поддерживает различные средства классификации пакетов для определения их принадлежности к определенной VLAN.

Поддержка GVRP (GARP VLAN)	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.
Поддержка VLAN на базе портов (Port-Based VLAN)	Распределение по группам VLAN выполняется по входящим портам. Данное решение позволяет использовать на каждом порту только одну группу VLAN.
Поддержка 802.1Q	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.
Объединение каналов с использованием LACP	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.
Создание групп LAG	В устройствах MES3000 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.
Поддержка Auto Voice VLAN	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)
Selective Q-in-Q	Позволяет назначать внешний VLAN SPVLAN (Service Provider's VLAN) на основе сконфигурированных правил фильтрации по номерам внутренних VLAN (Customer VLAN). Применение Selective Q-in-Q позволяет разобрать трафик абонента на несколько VLAN, изменить метку SPVLAN у пакета в отдельном участке сети

2.2.4 Функции третьего уровня сетевой модели OSI

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

Таблица 2.4 – Описание функций третьего уровня (Layer 3)

Клиенты BootP и DHCP (Dynamic Host Configuration Protocol)	Устройства MES3000 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 Proxy	IGMP Proxy - 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 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.

2.2.5 Функции QoS

В таблице 2.5 приведены основные функции качества обслуживания (Quality of Service)

Таблица 2.5 – Основные функции качества обслуживания

Поддержка приоритетных очередей	Устройство поддерживает приоритезацию исходящего трафика по очередям на каждом порту. Распределение пакетов по очередям может производиться в результате классификации пакетов по различным полям в заголовках пакетов.
Поддержка класса обслуживания 802.1p	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 MES3000 могут использовать значение приоритета 802.1p для распределения кадров по приоритетным очередям.

2.2.6 Функции обеспечения безопасности

Таблица 2.6 – Функции обеспечения безопасности

DHCP snooping	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.

Опция 82 протокола DHCP	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 ненадёжный (untrusted) порт.
UDP relay	Перенаправление широковещательного UDP-трафика на указанный IP-адрес
Функции DHCP-сервера	DHCP-сервер осуществляет централизованное управление сетевыми адресами и соответствующими конфигурационными параметрами, автоматически предоставляя их клиентам.
IP Source address guard	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.
Dynamic ARP Inspection (Protection)	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-пакета IP-адресу отправителя. Если адреса не совпадают, то коммутатор отбрасывает пакет.
L2 – L3 – L4 ACL (Access Control List)	На основе информации, содержащейся в заголовках уровней 2, 3 и 4, у администратора есть возможность настроить до 1024 правил, согласно которым пакет будет обработан, либо отброшен.
Time-Based ACL	Позволяет сконфигурировать временные рамки, в течение которых данный ACL будет действовать
Поддержка заблокированных портов	Основная функция блокировки – повысить безопасность сети, предоставляя доступ к порту коммутатора только для устройств имеющих MAC – адреса, закрепленные за этим портом.
Проверка подлинности на основе порта (802.1x)	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.

2.2.7 Функции управления коммутатором

Таблица 2.7 – 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 MES3000 поддерживает 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 MES3000 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 *SNTP* - 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 MES3000 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 так же 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 2.8 приведены дополнительные функции устройства.

Таблица 2.8 – Дополнительные функции устройства

Виртуальное тестирование кабеля (VCT)	Сетевые коммутаторы MES3000 имеют в своём составе программные и аппаратные средства, позволяющие выполнять функции виртуального тестера кабеля – VCT. Тестер позволяет определить состояние медного кабеля связи (исправен/обрыв/замыкание) и измерить длину исправного кабеля. По результатам тестирования формируется отчет.
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
IP SLA	Технология активного мониторинга, используемая для измерения параметров быстродействия компьютерных сетей и качества передачи данных. Поддерживаемые операции – ICMP Echo, UDP Jitter.

2.3 Основные технические характеристики

Основные технические параметры коммутатора приведены в таблице 2.9

Таблица 2.9 – Основные технические характеристики

Общие параметры		
Пакетный процессор		Marvell 98DX4122
Интерфейсы	MES3108	8x 10/100/1000Base-T 2x (10GBase-X(SFP+)/1000Base-X (SFP)
	MES3108F	4x 1000 Base-X (SFP) 4xCombo (10/100/1000Base-T/1000Base-X) 2x (10G Base-X (SFP+)/1000Base-X (SFP))
	MES3116	16x 10/100/1000Base-T 2x (10GBase-X(SFP+)/1000Base-X (SFP)
	MES3116F	12x 1000 Base-X (SFP) 4xCombo (10/100/1000Base-T/1000Base-X) 2x (10G Base-X (SFP+)/1000Base-X (SFP))
	MES3124	24x 10/100/1000Base-T 4x (10GBase-X(SFP+)/1000Base-X (SFP)
	MES3124F	20x 1000 Base-X (SFP) 4xCombo (10/100/1000Base-T/1000Base-X) 4x (10G Base-X (SFP+)/1000Base-X (SFP))

	MES3224	24x 10/100/1000 Base-T, 2x(10GBase-X(SFP+)/1000Base-X (SFP)), 2 x(10GBase-LR/ER/ZR (XFP))
	MES3224F	20 x1000 Base-X(SFP), 4 Combo (10/100/1000 Base-T/1000 Base-X), 2 (10GBase-X(SFP+)/1000Base-X (SFP), 2 x(10GBase-LR/ER/ZR (XFP))
Оптические трансиверы	MES3100	SFP, SFP+
	MES3200	SFP, SFP+, XFP
Дуплексный/Полудуплексный режим		дуплексный/полудуплексный режим для электрических портов, дуплексный режим для оптических портов
Производительность коммутатора		128 Гбит/с
Объем буферной памяти		12 Mb
Скорость передачи данных		электрические интерфейсы 10/100/1000 Мбит/с оптические интерфейсы 1/10 Гбит/с
Таблица MAC-адресов		16К записей (часть MAC-адресов резервируется для использования системой)
Объем TCAM		для маршрутизации: 3272x24B для задач обработки трафика: 2048x24B
Количество правил SQinQ		Ingress: 980 Egress: 140
Количество правил ACL		1012
Поддержка VLAN		согласно 802.1Q до 4К активных VLAN
Качество обслуживания QoS		приоритезация трафика, 8 уровней 8 выходных очередей с разными приоритетами для каждого порта
Multicast		до 1024 статических multicast-групп
Количество ACL		1024
Общее количество правил в ACL		до 2048
Количество L3 интерфейсов		512
Агрегация каналов (LAG)		12 групп, до 8 портов в каждой
Количество экземпляров MSTP		64
Сверхдлинные кадры (jumbo frames)		максимальный размер пакетов 10К
Стекирование		до 8 устройств

Соответствие стандартам	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-T Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z Fiber Gigabit Ethernet ANSI/IEEE 802.3 автоопределение скорости IEEE 802.3x контроль потоков данных IEEE 802.3ad объединение каналов LACP IEEE 802.1p приоритезация трафика IEEE 802.1q виртуальные локальные сети VLAN IEEE 802.1v IEEE 802.3 ac IEEE 802.1d связующее дерево STP IEEE 802.1w быстрое связующее дерево RSTP IEEE 802.1s множество связующих деревьев MSTP IEEE 802.1x аутентификация пользователей
Управление	
Локальное управление	SNMP, CLI
Удаленное управление	TELNET, SSH, WEB
Физические характеристики и условия окружающей среды	
Источники питания	сеть переменного тока: 220В+-20%, 50 Гц сеть постоянного тока: -36 .. - 72В варианты питания: - один источник питания постоянного или переменного тока; - два источника питания постоянного или переменного тока, с возможностью горячей замены.
Потребляемая мощность	не более 50Вт
Масса	не более 3,6 кг
Габаритные размеры	430x44x265 мм
Интервал рабочих температур	от -10 до +45 ^{o}C
Интервал температуры хранения	от -40 до +70 ^{o}C
Относительная влажность при эксплуатации (без образования конденсата)	не более 80%
Относительная влажность при хранении (без образования конденсата)	от 10% до 95%
Средний срок службы	20 лет

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 серии MES3000 выполнены в металлическом корпусе с возможностью установки в 19” каркас, высота корпуса 1U.

В комбинированных портах может быть активным только один из интерфейсов. При одновременном подключении будет активен интерфейс с SFP-трансивером.

2.4.1 Передняя панель устройства

Внешний вид передней панели MES3108, MES3108F, MES3116, MES3116F, MES3124, MES3124F, MES3224, MES3224F показан на рисунках 1-8.

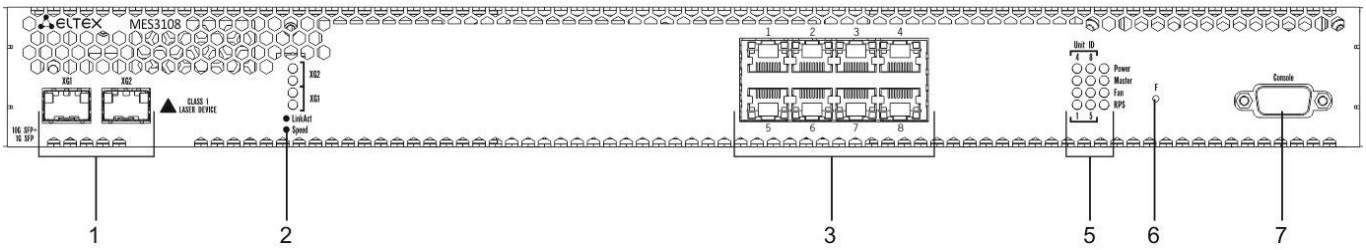


Рисунок 1 – MES3108, передняя панель

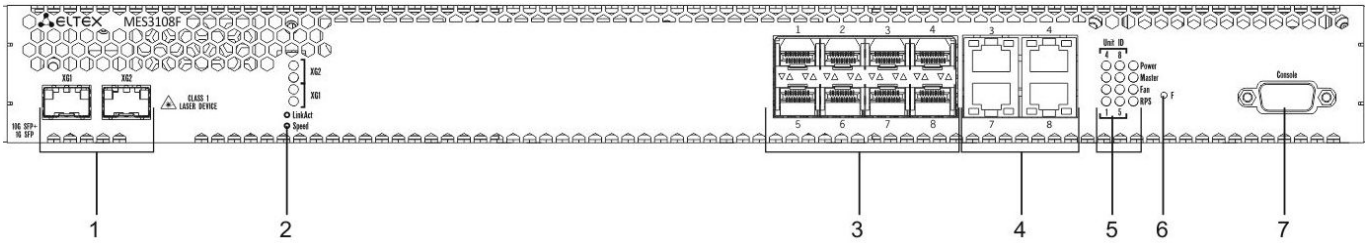


Рисунок 2 – MES3108F, передняя панель

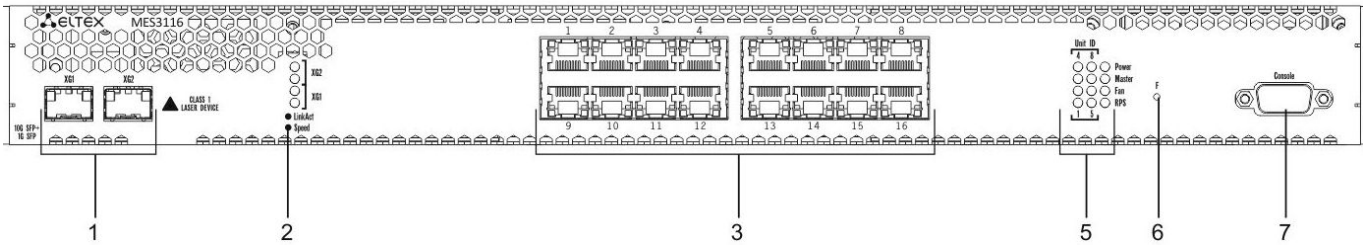


Рисунок 3 – MES3116, передняя панель

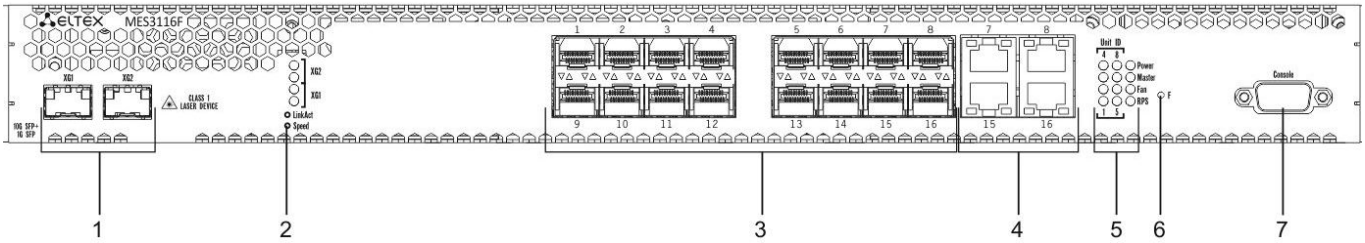


Рисунок 4 – MES3116F, передняя панель

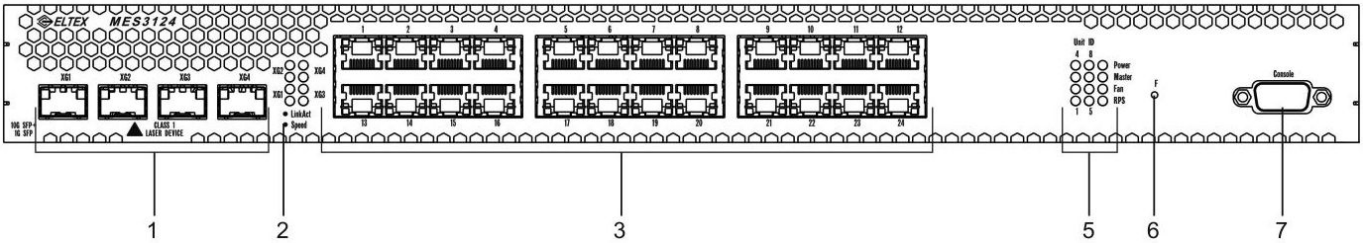


Рисунок 5 – MES3124, передняя панель

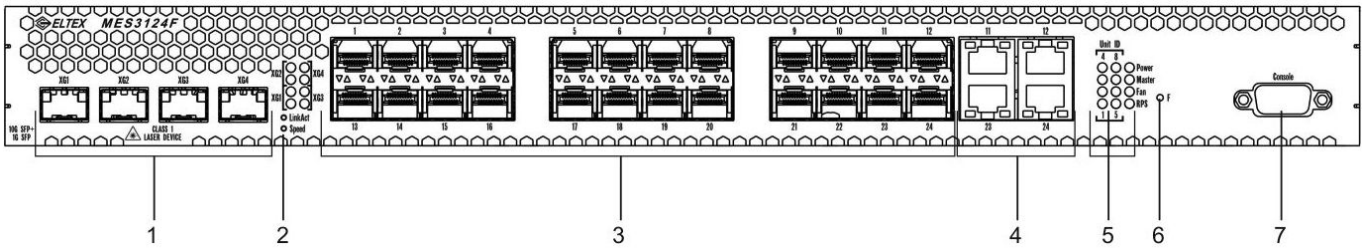


Рисунок 6 – MES3124F, передняя панель

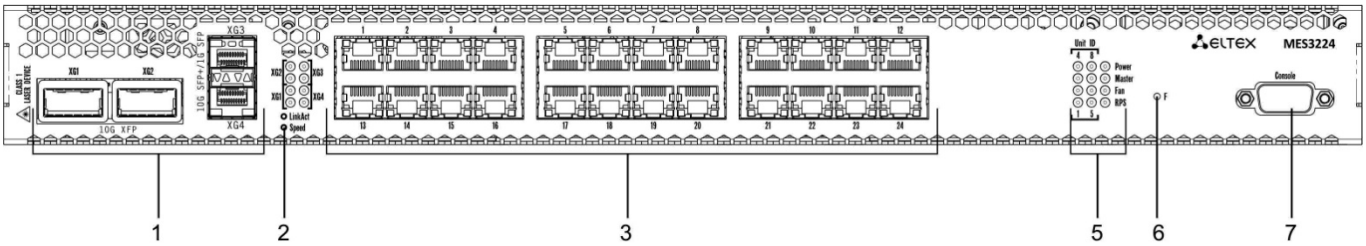


Рисунок 7 – MES3224, передняя панель

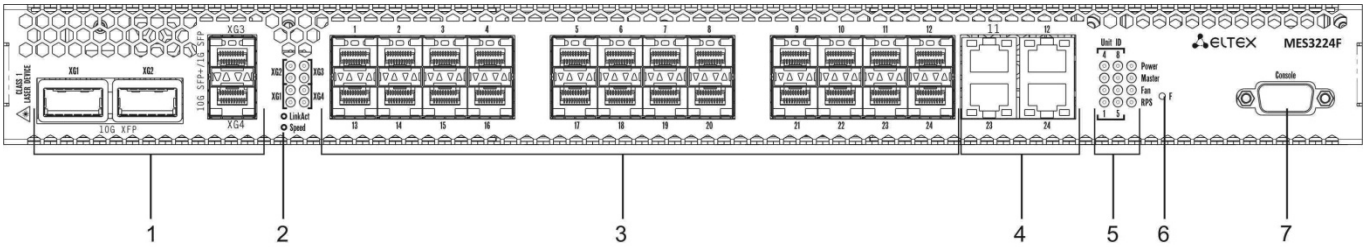


Рисунок 8 – MES3224F, передняя панель

В таблице 2.10 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели коммутатора.

Таблица 2.10 – Описание разъемов, индикаторов и органов управления передней панели

№	Элемент панели		Описание
1	XG1, XG2 XG3, XG4		Слоты для установки трансиверов. Для устройств серии MES3100 трансиверы SFP+/SFP. Для устройств серии MES3224: - слоты XG1, XG2 для установки трансиверов 10G XFP; - слоты XG3, XG4 для установки трансиверов 10G SFP+/ 1G SFP.
2	XG1, XG2 XG3, XG4		Индикаторы работы оптических интерфейсов XG.
3	[1..8/16/24]		8/16/24 порта Gigabit Ethernet. Для устройств MES3108, MES3116, MES3124, MES3224: 10/100/1000 Base-T (RJ-45). Для устройств MES3108F, MES3116F, MES3124F, MES3224F: 1000 Base-X (SFP).
4	MES3108F	3, 4, 7, 8	Комбинированные порты 10/100/1000 Base-T (RJ-45).
	MES3116F	7, 8, 15, 16	
	MES3124F MES3224F	11, 12, 23, 24	
5	Unit ID		Индикаторы номера устройства в стеке.
	Power		Индикатор питания устройства.
	Master		Индикатор режима работы устройства (ведущий/ведомый).
	Fan		Индикатор работы вентиляторов.
	RPS		Индикатор резервного электропитания.
6	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 устройства до заводской конфигурации.
7	Console		Консольный порт RS-232 для локального управления устройством.

2.4.2 Задняя панель устройства

Внешний вид задней панели коммутаторов серии MES3000 приведен на рисунке 9[1].

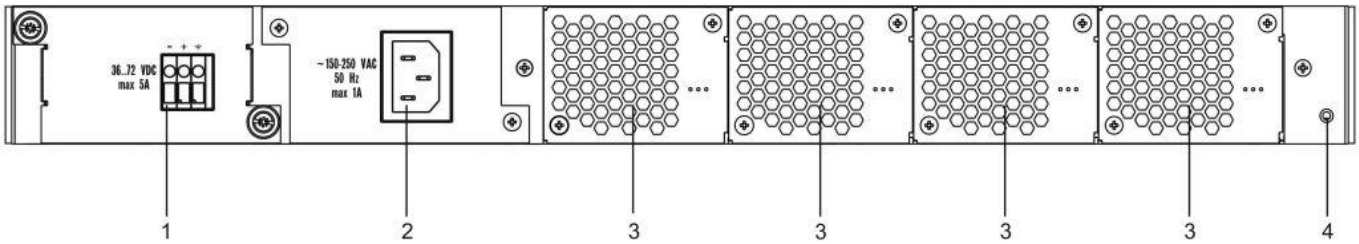


Рисунок 9 – MES3000 задняя панель

[1] На рисунке показана комплектация коммутатора с 1 источником питания постоянного тока и с 1 источником питания переменного тока.

В таблице 2.11 приведен перечень разъемов, расположенных на задней панели коммутатора.

Таблица 2.11 – Описание разъемов задней панели коммутатора

№	Элемент задней панели	Описание
1		Разъем для подключения к источнику электропитания постоянного тока
2		Разъем для подключения к источнику электропитания переменного тока
3	Съемные вентиляторы	Съемные вентиляционные модули с возможностью горячей замены.
4	Клемма заземления ⏚	Клемма для заземления устройства.

2.4.3 Боковые панели устройства

Рисунок 10 – Правая боковая панель Ethernet-коммутаторов серии MES3000

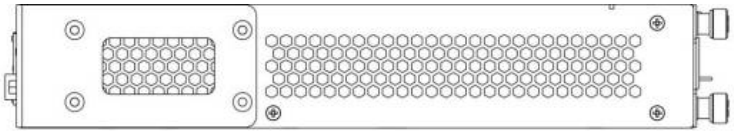


Рисунок 11 – Левая боковая панель Ethernet-коммутаторов серии MES3000

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 индицируется двумя светодиодными индикаторами, *LINK/ACT* зеленого цвета и *SPEED* янтарного цвета. Расположение светодиодов показано на рисунках 12,13.

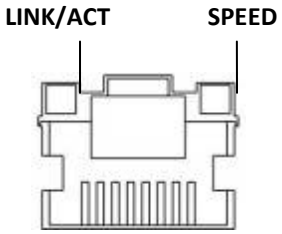


Рисунок 12 – Внешний вид разъема RJ-45

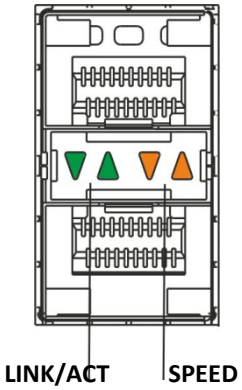


Рисунок 13– Внешний вид разъема с SFP-трансиверами

Таблица 2.12 – Световая индикация состояния интерфейсов Ethernet

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

Состояние интерфейсов XG отображается индикаторами, расположенными рядом с разъемами интерфейсов, рисунок 14. С каждым интерфейсом XG связана пара индикаторов. Верхний янтарный индикатор отображает активность передающей части порта, нижний зеленый – активность приемной части порта. Передача данных отображается мерцанием индикатора соответствующего направления.

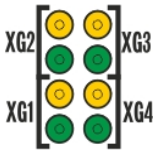


Рисунок 14 – Внешний вид индикаторов интерфейсов XG

Индикаторы *Unit ID* (1-8) служат для обозначения номера устройства в стеке.

Системные индикаторы (Power, Master, Fan, RPS) служат для определения состояния работы узлов коммутаторов серии MES3000.

Таблица 2.13 – Световая индикация системных индикаторов и индикаторов XG портов

Название индикатора	*Функция индикатора*	*Состояние индикатора*	*Состояние устройства*
XG1-XG4	Режим работы порта	Активны (мерцают) оба индикатора (нижний – зеленый, верхний – янтарный)	скорость работы порта – 1000Мбит/с
		Активны (мерцают) оба индикатора (нижний – зеленый, верхний – янтарный)	передача данных на скорости 10 Гбит/с
Power	Состояние источников питания	Выключен	Питание выключено
		Зеленый, горит постоянно	Питание включено, нормальная работа устройства
		Зеленый, мерцает	Самотестирование устройства при старте (POST)
		Оранжевый	Отсутствие первичного питания основного источника (при питании устройства от резервного источника) или авария основного источника питания
Master	Признак ведущего устройства при работе в стеке	Зеленый, горит постоянно	Устройство является «мастером» стека
		Выключен	Устройство не является «мастером» в стеке или не задан режим стекирования
Fan	Состояние вентилятора охлаждения	Выключен	Все вентиляторы исправны
		Красный	Отказ одного или более вентиляторов
RPS	Режим работы резервного источника питания	Зеленый, горит постоянно	Резервный источник подключен и работает нормально
		Выключен	Резервный источник не подключен
		Красный	Отсутствие первичного питания резервного источника или его неисправность

В том случае, когда коммутатор работает в автономном режиме без стекирования, индикаторы *Master* и *Unit ID* выключены.

2.5 Комплект поставки

В базовый комплект поставки входят:

- Ethernet-коммутатор;
- Модуль питания PM75-48/12 или PM-150-220/12 (опционально);
- Шнур питания (в случае комплектации модулем питания на 220В);
- Комплект крепежа в стойку;
- Документация.

По заказу покупателя в комплект поставки могут быть включены SFP/SFP+-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. Для установки кронштейнов:

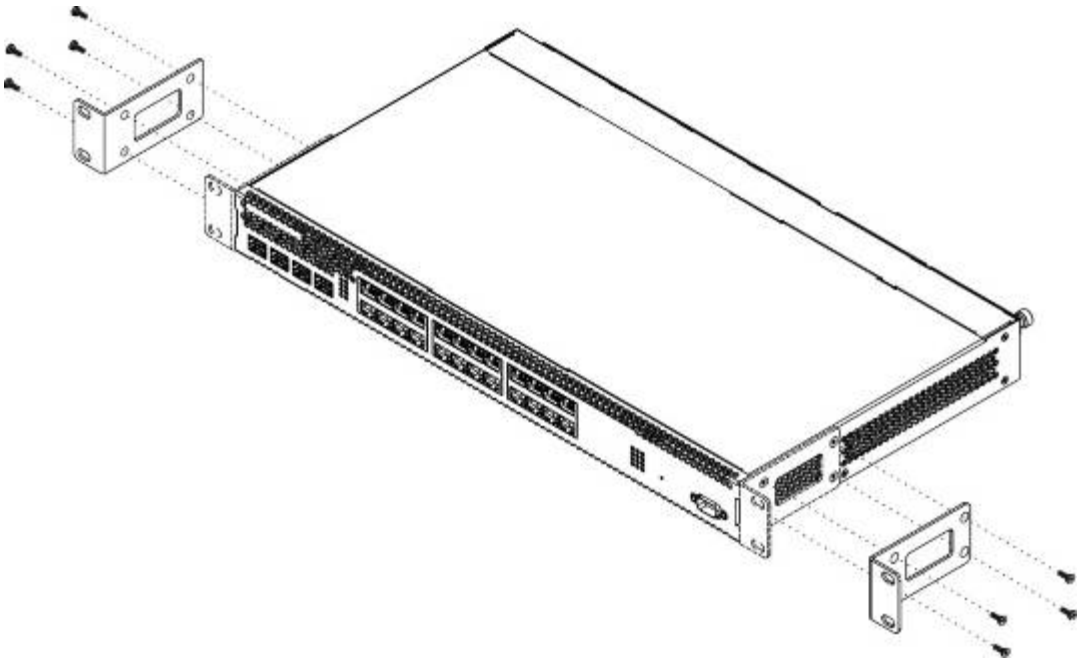


Рисунок 15 – Крепление кронштейнов

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

3.2 Установка устройства в стойку

Для установки устройства в стойку:

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

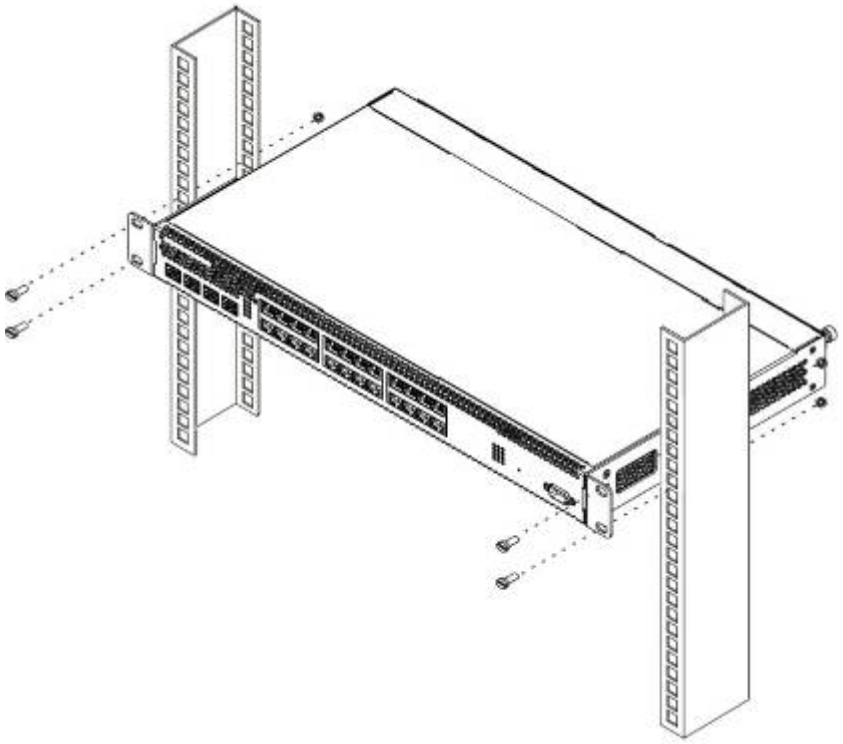


Рисунок 16 – Установка устройства в стойку

На рисунке 17 приведен пример размещения коммутаторов MES3000 в стойке.

Рисунок 17 – Размещение коммутаторов MES-3000 в стойке

Устройство имеет фронтальную вентиляцию. На передней панели устройства расположены вентиляционные отверстия. Не закрывайте вентиляционные отверстия, а также вентиляторы, расположенные на задней панели, посторонними предметами во избежание перегрева компонентов коммутатора и нарушения его работы.

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.

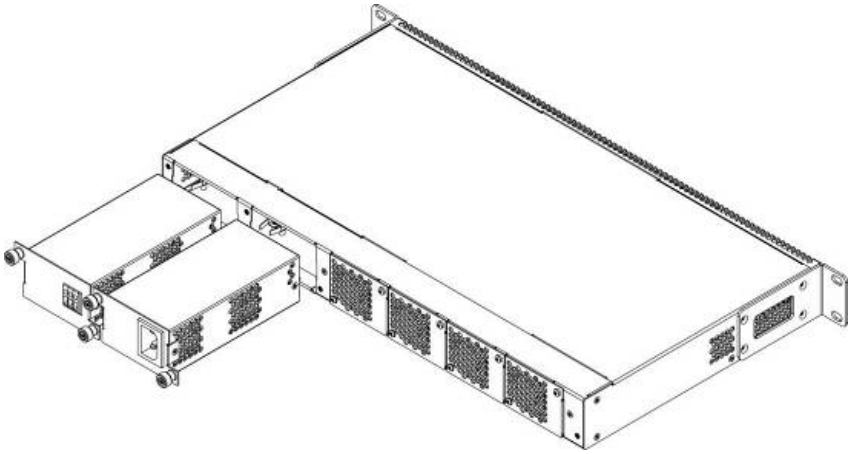


Рисунок 18 – Установка модулей питания.

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 требованиями ПУЭ.
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. Для подключения к сети постоянного тока используйте провод сечением не менее 1 мм^2.
4. Включите питание устройства и убедитесь в отсутствии аварий по состоянию индикаторов на передней панели.

3.5 Установка и удаление SFP-трансиверов

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

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

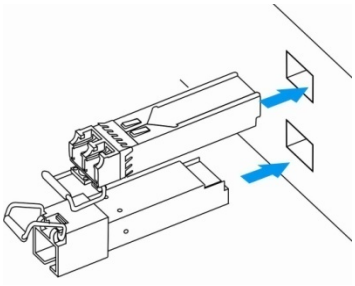


Рисунок 19 – Установка SFP-трансиверов

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

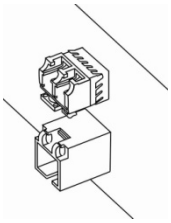


Рисунок 20 – Установленные SFP-трансиверы

Для удаления трансивера:

1. Откройте защелку модуля.

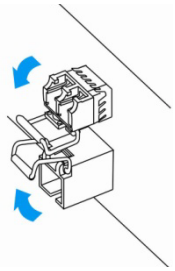


Рисунок 21 – Открытие защелки SFP-трансиверов

2. Извлеките модуль из слота.

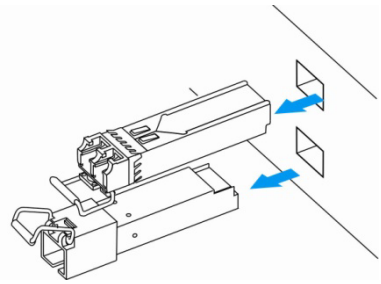


Рисунок 22 – Извлечение SFP-трансиверов

4 НАЧАЛЬНАЯ НАСТРОЙКА КОММУТАТОРА

4.1 Настройка терминала

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

1. Выбрать соответствующий последовательный порт.
2. Установить скорость передачи данных – 115200 бод.
3. Задать формат данных: 8 бит данных, 1 стоповый бит, без контроля четности.
4. Отключить аппаратное и программное управление потоком данных.
5. 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 серии MES3000:

```
Boot1 Checksum Test.............................PASS
Boot2 Checksum Test.............................PASS
Flash Image Validation Test.....................PASS

BOOT Software Version 0.0.0.3 Built  17-Aug-2010  23:18:59

Networking device with CPU based on arm926ejs core. 256 MByte SDRAM.
I-Cache 16 KB. D-Cache 16 KB. L2 Cache 256 KB. Cache Enabled.

MAC Address   :  a8:f9:4b:a3:a4:a6.
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.

Пример дальнейшей загрузки устройства.

```
Preparing to decompress...
 100%
Decompressing SW from image-1
 100%

OK
Running from RAM...

*****************************************************************
*** Running  SW  Ver. 2.1.6  Date  05-Jun-2011  Time  16:14:03 ***
*****************************************************************

HW version is V01
Base Mac address is: a8:f9:4b:80:b0:80
Dram size is  : 256M bytes
```

```
Dram first block size is  : 229376K bytes Dram first PTR is  : 0x1C00000 Dram
second block size is  : 4096K bytes Dram second PTR is  : 0xFC00000 Flash size
is: 16M
05-Jun-2011 16:14:09 %CDB-I-LOADCONFIG: Loading running configuration.
05-Jun-2011 16:14:09 %CDB-I-LOADCONFIG: Loading startup configuration.
Device configuration:
Slot 1 - 28 ports
Device 0: GT_98DX4122 (BobCat)

------------------------------------
-- Unit Standalone                --
------------------------------------

Tapi Version: v1.9.3.2
Core Version: v1.9.3.2
```

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

```
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”:

```
Boot1 Checksum Test...............................PASS
Boot2 Checksum Test...............................PASS
Flash Image Validation Test.......................PASS

BOOT Software Version 0.0.0.3 Built  17-Aug-2010  23:18:59

Networking device with CPU based on arm926ejs core. 256 MByte SDRAM.
I-Cache 16 KB. D-Cache 16 KB. L2 Cache 256 KB. Cache Enabled.

MAC Address   :  a8:f9:4b:a3:a4:a6.
Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.
```

Вид загрузочного меню:

```
          Startup Menu

[1]  Download Software
[2]  Erase Flash File
[3]  Password Recovery Procedure
[4]  Set Terminal Baud-Rate
[5]  Stack menu
[6]  Back
 Enter your choice or press 'ESC' to exit:
```

Таблица 4.1 – Функции интерфейса загрузочного меню

Функция	***Описание***
Download Software	Загрузить новую версию программного обеспечения коммутатора, используя XMODEM
Erase Flash File	Стереть информацию с Flash
Password Recovery	Сбросить настройки аутентификации

Procedure	
Set Terminal Baud-Rate	Установить скорость работы терминального режима
Stack Menu	Вход в меню управления стеком
Back	Продолжить загрузку

4.4 Режимы работы коммутатора

Устройство может работать в двух режимах – автономном и режиме стекирования. В режиме стекирования несколько коммутаторов могут быть объединены в стек и функционировать как единое устройство. По умолчанию коммутаторы MES3000 работают в режиме автономного устройства.

Стекирование может производиться только с помощью SFP+ модулей.

4.4.1 Выбор режима работы коммутатора

Выбор режима работы коммутатора доступен в меню управления стеком (пункт [5] загрузочного меню):

```
          Startup Menu

[1]  Download Software
[2]  Erase Flash File
[3]  Password Recovery Procedure
[4]  Set Terminal Baud-Rate
[5]  Stack menu
[6]  Back
 Enter your choice or press 'ESC' to exit:
```

Пункт [3] – выбор режима работы коммутатора ([1] – автономный режим, [2] – режим стекирования):

```
     Stack menu

[1]  Show unit stack id
[2]  Set unit stack id
[3]  Set unit working mode
[4]  Back
 Enter your choice or press 'ESC' to exit:
```

4.4.2 Работа коммутатора в режиме стекирования

Стек MES3000 функционирует как единое устройство и может состоять из 8 устройств, 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, берущее на себя функции управления стеком.
- *Slave* (UID устройств от 3 до 8) – устройства, подчиняющееся master. Не может работать в автономном режиме (если отсутствует master).

В режиме стекирования MES3124/MES3124F и MES3224/MES3224F используют XG3 и XG4 порты для синхронизации, при этом эти порты не участвуют в передаче данных. MES3108/MES3108F и MES3116/MES3116F используют для синхронизации только один порт - XG2, при этом этот порт не участвует в передаче данных. Возможны две топологии синхронизирующихся устройств – кольцевая и линейная. Рекомендуется использовать кольцевую топологию для повышения отказоустойчивости стека.

Команды режима privileged EXEC

Запрос командной строки имеет следующий вид:

console#

Таблица 4.2 – Базовые команды, доступные в режиме privileged EXEC

Команда	***Значение/ значение по умолчанию***	***Действие***
unit mode {standalone|stackable}	-	Определяет режим работы коммутатора: - **standalone** – коммутатор может работать как самостоятельное устройство; - **stackable** – коммутатор может работать в режиме стека. Смена режима происходит после перезагрузки коммутатора.
unit renumber local after-reset *unit_id*	unit_id: (1..8)/1	Назначает номер устройства «unit-id» локальному устройству (на котором выполнена команда). Команда может быть использована в режиме «standalone» или в режиме «stackable» на ведущем устройстве. Смена номера устройства произойдёт после перезагрузки коммутатора.
unit renumber *current_id* **after-reset** *new_id*	current_id: (1..8) new_id: (1..8)	Назначает новый номер устройства «new-id» коммутатору с номером «current-id». Команда может быть использована только на ведущем устройстве стека. Смена номера устройства произойдёт после перезагрузки этого устройства.
show unit [*unit_id*]	unit_id: (1..8)	Отображает информацию об устройствах, входящих в стек. При вводе команды без параметра отображается краткая информация обо всех устройствах стека. При указании «unit-id» отображается подробная информация о выбранном устройстве.

- Пример использования команды **show unit**:

console# **show unit** 1

```
Unit:                    1
MAC address:             a8:f9:4b:80:bf:40
Master:                  Enabled.
Product:                 MES-3124F 28-port Fiber 1G/10G Stackable Managed Switch.
Software:                2.5.14
Uplink unit:             2
Downlink unit:           0
Status:                  master
Active image:            image-2
Selected for next boot: image-2
Topology is Chain
Stack image auto synchronization is enabled
Unit Mode After Reset:  stacking
Unit Num After Reset:   1
```

Таблица 4.3 – Описание результатов выполнения команды «show unit»

Поле	*Описание*
Unit:	Идентификатор выбранного устройства
MAC address:	MAC-адрес коммутатора
Master:	Разрешение стать ведущим устройством в стеке
Product:	Описание модели коммутатора
Uplink unit:	Идентификатор коммутатора, подключенного к порту Uplink (для MES3124 – XG3, для MES3116,3108 – XG1)
Downlink unit:	Идентификатор коммутатора, подключенного к порту Downlink (для MES3124 – XG4, для MES3116,3108 – XG2)
Status:	Текущая роль коммутатора в стеке
Active image:	Активный образ ПО
Selected for next boot:	Образ ПО, который будет активным после перезагрузки
Topology is	Текущая топология стека - chain (цепочка) или ring (кольцо)
Unit Mode After Reset:	Режим работы коммутатора после перезагрузки – standalone/stacking
Unit Num After Reset:	Идентификатор коммутатора, который применится после перезагрузки

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 конфигурирования 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 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.

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
```

```
Gateway IP Address         Activity status       Type
---------------------      ------------------  --------
192.168.16.1              Active              static


IP Address                Type
---------------------      ------------------
192.168.16.144 /24         Static
```

4.5.1.3 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
```

```
Gateway IP Address   Activity status            Type
---------------------      ------------------   --------
192.168.16.1        Active              DHCP

IP Address                 Type
-------------------  ------------
192.168.16.149 /24        DHCP
```

4.5.1.4 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 MES3000 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.

  Community-String    Community-Access    View name     IP address
-------------------- ------------------ -------------- ------------
      private            read write        Default     192.168.16.44

 Community-String      Group name          IP address       Type
------------------   ------------------ ---------------    ------

Traps are enabled.
Authentication-failure trap is enabled.

Version 1,2 notifications
 Target Address    Type    Community   Version   Udp   Filter   To    Retries
                                                 Port  name     Sec
---------------- -------- ----------- ---------- ----- ------- ----- ---------

Version 3 notifications
 Target Address    Type    Username   Security Udp   Filter   To    Retries
                                      Level    Port  name     Sec
---------------- -------- ----------- -------- ----- ------- ----- ---------

System Contact:
System Location:
```

4.5.2 Настройка параметров системы безопасности

Для обеспечения безопасности системы используется механизм AAA (аутентификация, авторизация, учет). 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 не задан. 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 ([3] Password Recovery Procedure).

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, которое будет выводиться при попытке получения доступа к устройству.

console(config)# **banner motd ;**

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

5 УПРАВЛЕНИЕ УСТРОЙСТВОМ. ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ

Для конфигурирования настроек коммутатора используется четыре основных режима. 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. Приглашение системы в этом режиме состоит из имени устройства (host name) и символа “>”.

```
console>
```

Если имя устройства не назначено, то вместо него используется слово “console”.

Привилегированный командный режим (privileged EXEC), этот режим доступен при входе привилегированного пользователя. Вход в режим должен быть обязательно защищен паролем. Только в привилегированном режиме доступны команды изменения системных параметров коммутатора. В привилегированном режиме в строке приглашения системы используется символ «#». Для перехода из режима EXEC в привилегированный режим может быть использована команда enable.

```
console> enable
enter password:
console#
```

Режим глобального конфигурирования (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 конфигурирования интерфейса (interface configuration), данный режим предназначен для конфигурирования интерфейсов (порт, группа портов, интерфейс VLAN) коммутатора. Вход в режим осуществляется из режима глобального конфигурирования, для каждого интерфейса своей командой (в примере ниже команда для входа в режим конфигурирования интерфейса VLAN с VID=1).

```
console(config)# interface vlan 1
console (config-if)#
```

Режим конфигурирования терминала (line configuration), данный режим предназначен для конфигурирования, связанного с работой терминала. Вход в режим осуществляется из режима глобального конфигурирования.

```
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 5.1 – 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	-	Закрыть 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.
no terminal history		Выключить функцию сохранения истории введенных команд для текущей терминальной сессии.
terminal history size *size*	size: (10..216)/10	Изменить размер буфера истории введенных команд для текущей терминальной сессии.
no terminal 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, One line: <return>)..
no terminal datadump		Установить значение по умолчанию.
show banner [motd | login | exec]	-	Отображает конфигурацию баннеров.

Команды режима privileged EXEC

Запрос командной строки имеет следующий вид:

```
console#
```

Таблица 5.2 – Базовые команды, доступные в режиме privileged EXEC

Команда	*Значение/ значение по умолчанию*	*Действие*
disable [*priv***]**	priv: (1..15)/1	Вернуться в нормальный режим из привилегированного (если значение не указано – то уровень привилегий 1).
configure[*terminal***]**	-	Перейти в режим конфигурирования.
debug-mode	-	Перейти в режим отладки (команда доступна только для привилегированного пользователя).

Команды, доступные во всех режимах конфигурирования

Запрос командной строки имеет один из следующих видов:

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

Таблица 5.3 – Базовые команды, доступные во всех режимах конфигурирования

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

Команды режима глобального конфигурирования

Запрос командной строки имеет следующий вид:

`console(config)#`

Таблица 5.4 – Базовые команды, доступные в режиме конфигурирования

Команда	*Значение*	*Действие*
banner motd *d message-text d* **no banner motd**	-	Задать текст сообщения motd (сообщения текущего дня), и включить вывод на экран. - *d* - разделитель; - *message-text* – текст сообщения (в строке до 510 символов, общее 2000 символов).
banner exec *d message-text d* **no banner exec**	-	Задать текст сообщения exec (пример: пользователь успешно вошел в систему), и включить вывод на экран. - *d* - разделитель; - *message-text* – текст сообщения (в строке до 510 символов, общее 2000 символов).
banner login *d message-text d* **no banner login**	-	Задать текст сообщения login (информационное сообщение, которое отображается перед вводом имени пользователя и пароля), и включить вывод на экран. - *d* - разделитель; - *message-text* – текст сообщения (в строке до 510 символов, общее 2000 символов).

Команды режима конфигурирования терминала

Запрос командной строки в режиме конфигурирования терминала имеет следующий вид:

`console(config-line)#`

Таблица 5.5 – Базовые команды, доступные в режиме конфигурирования 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*}	(0..216)/10	Изменить размер буфера истории введенных команд.
no history sie		Установить значение по умолчанию.
motd-banner	-/включен	Включить вывод приветственных сообщений типа «motd» (сообщения текущего дня).
no motd-banner		Выключить вывод информационных сообщений типа «motd».
login-banner	-/ включен	Включить вывод приветственных сообщений login.
no login-banner		Выключить вывод приветственных сообщений login.
exec-banner	-/ включен	Включить вывод приветственных сообщений exec.
no exec-banner		Выключить вывод приветственных сообщений exec.

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 5.6 – Команды режима глобального конфигурирования

Метод	*Значение/Значение по умолчанию*	*Действие*
begin *pattern*	-	Показывает строки, первые символы которых соответствуют шаблону *pattern*
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 глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

`console(config)#`

Таблица 5.7 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
macro name [*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 *word*		Удаляет указанный макрос.
macro global apply *word*	(1..32) символов	Применяет указанный макрос.
macro global trace *word*	(1..32) символов	Проверяет указанный макрос на валидность.
macro global description *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 5.8 – Команды режима EXEC

Команда	*Действие*	
macro apply *word*	(1..32) символов	Применяет указанный макрос
macro trace *word*		Проверяет указанный макрос на валидность
show parser macro [description [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***}] | name** *macro-name***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12); macro-name: (1..32) символов	Отображает параметры настроенных макросов на устройстве.

Команды режима конфигурации интерфейса

Вид запроса командной строки режима конфигурации интерфейса:

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

Таблица 5.9 – Команды режима конфигурации интерфейса

Команда	***Действие***	
macro apply *word*	(1..32) символов	Применяет указанный макрос.
macro trace *word*	(1..32) символов	Проверяет указанный макрос на валидность.
macro description *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 5.10 – Команды управления системой в режиме EXEC

Команда	***Значение/ Значение по умолчанию***	***Действие***
ping [ip] {*A.B.C.D*|*host*} [**size** *size*] [**count** *count*] [**timeout** *timeout*]	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 так же для контроля поступающих ответов (ICMP Echo-Reply). - *A.B.C.D* - IPv4-адрес узла сети; - *host* – доменное имя узла сети; - *size* – размер пакета для отправки, количество байт в пакете; - *count* – количество пакетов для передачи; - *timeout* – время ожидания ответа на запрос.
ping ipv6 {*A.B.C.D.E.F*|*host*} [**size** *size*] [**count** *count*] [**timeout** *timeout*]	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 так же, для контроля поступающих ответов (ICMP Echo-Reply). - *A.B.C.D.E.F* - IPv6-адрес узла сети; - *host* – доменное имя узла сети; - *size* – размер пакета для отправки, количество байт в пакете; - *count* – количество пакетов для передачи; - *timeout* – время ожидания ответа на запрос.
traceroute ip {*A.B.C.D* |*host***}** **[size** *size***]** **[ttl** *ttl***]** **[count** *count***] [timeout** *timeout***] [source** *ip_address***]** **[tos** *tos***]**	host (1..158) символов; size (64..1518)/64 Байт; ttl (1..255)/30; count (1..10)/3; timeout (1..60) /3 с; tos(0..255)/0	Определение маршрута трафика до узла назначения. - *A.B.C.D* - IPv4-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; - *tos* – тип сервиса, передаваемый в заголовке протокола IP. **Описание ошибок при выполнении команд и результатов приведено в таблицах 5.12, 5.13**
traceroute ipv6 **{***A.B.C.D.E.F*|*host***} [size** *size***]** **[ttl** *ttl***]**	host (1..158) символов; size (66..1518)/66 Байт; ttl (1..255)/30; count (1..10)/3;	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

[count *count***]** **[timeout** *timeout***]** **[source** *ip_address***]** **[tos** *tos***]**	timeout (1..60) /3 с; tos(0..255)/0	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; - *tos* – тип сервиса, передаваемый в заголовке протокола IP. **Описание ошибок при выполнении команд и результатов приведено в таблицах 5.12, 5.13.**
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 5.14 , 5.15**
ssh {*A.B.C.D* **|** *host*} **[port** *port*] **[username** *username*] **[cipher** *cipher*]	host (1..158) символов; port (1..65535)/22; username (1..70) символов	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; - *username* – имя пользователя, под которым необходимо выполнить вход; - *cipher* – выбор метода шифрования. Поддерживаются следующие методы: 3des, aes128, aes192, aes256, arcfour. По умолчанию предлагаются все методы.
resume [*connection*]	(1..4)/последняя установленная сессия	Переключение на другую установленную TELNET-сессию. - *connection* – номер установленной telnet-сессии.
show unit [*number*]	number: (1 .. 8)	Отображает информацию о состоянии стека. - *number* – номер стека.
show cpu counters	-	Просмотр счетчиков пакетов центрального процессора.
show users	-	Отображение информации о пользователях, использующих ресурсы устройства.
show sessions	-	Отображение информации об открытых TELNET-сессиях к удаленным устройствам.
show system [**unit** *unit*]	(1..8)/-	Отображение системной информации коммутатора. - *unit* – номер устройства в стеке (для коммутатора, работающего в автономном режиме, параметр не используется). **Параметр «unit» при выполнении команды доступен только в режиме стекирования.**
show version	-	Отображение текущей версии системного программного обеспечения, работающего на устройстве.
show system tcam utilization **[unit** unit**]**	(1..8)/-	Отображение загрузки ресурсов памяти TCAM (определенно адресуемая память). - *unit* – номер устройства в стеке (для коммутатора, работающего в автономном режиме, параметр не используется). **Параметр [unit unit] при выполнении команды доступен только в режиме стекирования.**

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 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».

Команды режима privileged EXEC

Запрос командной строки в режиме privileged EXEC имеет следующий вид:

console#

Таблица 5.11 – Команды управления системой в режиме privileged EXEC

Команда	*Значение/ Значение по умолчанию*	*Действие*
reload [unit *unit_id***]**	unit_id: (1..8)	Команда служит для перезапуска устройства. - *unit_id* – номер устройства в стеке.
reload in [*minutes* **|** *hh:mm***]**	minutes: (1..999); hh (0..23), mm (0..59).	Установка промежутка времени, через который произойдет отложенная перезагрузка устройства.
reload cancel	-	Отмена отложенного перезапуска.
show cpu utilization	-	Отображение статистики по уровню загрузки ресурсов центрального процессора.
show cpu input-rate	-	Отображение статистики по скорости входящих фреймов, обрабатываемых процессором.
show cpu input-rate detailed	-	Отображение статистики по скорости входящих фреймов, обрабатываемых процессором по типу трафика.
show cpu rate-limits	-	Отображение ограничений по скорости для входящих фреймов, обрабатываемых процессором.
clear cpu counters	-	Обнуление счетчиков пакетов центрального процессора.
show system id [unit unit**]**	(1..8)/-	Отображение информации системной идентификации устройства. - *unit* – номер устройства в стеке (для коммутатора, работающего в автономном режиме, параметр не используется). **Параметр [unit unit] при выполнении команды доступен только в режиме стекирования.**
show system defaults [{management|ipv6|802.1x |port|fdb|multicast| port-mirroring| spanning-tree|vlan| voice-vlan| network-security| dos-attacks | ip-addressing| qos-acl }]	-	Отображение заводских настроек устройства.
show system resources routing	-	Отображение информации об использовании ресурсов таблицы маршрутизации.
show system resources tcam		Отображение подробной информации об использовании ресурсов TCAM (Ternary Content Addressable Memory).
show system tcam utilization	-	Отображение краткой информации об использовании ресурсов TCAM (Ternary Content Addressable Memory).

- Пример использования команды **traceroute**:

console# **traceroute** *eltex.com*

```
Type Esc to abort.
Tracing the route to eltex.com (148.21.11.69)
   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 5.12 – 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.

Таблица 5.13 – Ошибки при выполнении команды traceroute

Символ ошибки	*Описание*
*	Таймаут 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 MES3000 поддерживает специальные команды – функции контроля терминала. Для входа в режим специальных команд во время активной Telnet-сессии используется комбинация клавиш Ctrl-shift-6.

Таблица 5.14 – 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-сессии:

Таблица 5.15 – Ключевые слова, используемые при открытии Telnet-сессии

Опция	***Описание***
/echo	Локально включает функцию *echo* (подавление вывода на консоль).
/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. Потоковое 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.

Команды режима глобального конфигурирования

Запрос командной строки в режиме глобального конфигурирования имеет следующий вид:

```
console(config)#
```

Таблица 5.16 – Команды управления системой в режиме глобального конфигурирования

Команда	***Значение/ Значение по умолчанию***	***Действие***
hostname *name*	(1..160) символов/-	Команда служит для задания сетевого имени устройства.
no hostname		Вернуть сетевое имя устройства в значение по умолчанию.
stack master unit *unit*	(1..2)/ нет ведущего устройства	Назначение ведущего устройства в стеке. Данная команда доступна только в режиме стекирования.
no stack master unit		Установить значение по умолчанию.
service cpu-utilization	-/enabled	Разрешить устройству программно измерять уровень загрузки ресурсов центрального процессора коммутатора.
no service cpu-utilization		Запретить устройству программно измерять уровень загрузки ресурсов центрального процессора коммутатора.
service cpu-input-rate	-/disabled	Разрешить устройству программно измерять скорость входящих фреймов, обрабатываемых центральным процессором коммутатора.
no service cpu-input-rate		Запретить устройству программно измерять скорость входящих фреймов, обрабатываемых центральным процессором коммутатора.
service cpu-rate-limits *traffic* **limit** *pps*	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, ptp, other pps: 8..1024	Установка ограничений скорости входящих фреймов для определенного типа трафика. - *pps* - пакетов в секунду.
service tasks-utilization	-/disabled	Разрешить устройству программно измерять уровень загрузки ресурсов центрального процессора коммутатора для каждого системного процесса.
no service tasks-utilization		Запретить устройству программно измерять уровень загрузки ресурсов центрального процессора коммутатора для каждого системного процесса.
system resources routing *routes hosts interfaces*	routes: (20..11136) hosts:(20..2800) interfaces: (2..1024)	Установка размера таблицы маршрутизации. - *routes* – максимальное количество удаленных сетей; - *hosts* – максимальное количество подключенных хостов; - *interfaces* – максимальное количество IP-интерфейсов.
reset-button {enable |	**-/enable**	Настройка реакции коммутатора на нажатие кнопки F.

disable| reset-only}		**- enable –** при нажатии на кнопку длительностью менее 10 с происходит перезагрузка устройства; при нажатии на кнопку длительностью более 10 с происходит сброс устройства до заводской конфигурации; **- disable –** не реагировать (отключена)**;** - **reset-only** – только перезагрузка**.**

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 глобального конфигурирования

Запрос командной строки в режиме глобального конфигурирования имеет следующий вид:

```
console(config)#
```

Таблица 5.17 – Команды управления системой в режиме глобального конфигурирования

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

Таблица 5.18 – Команды управления системой в режиме Privileged EXEC

Команда	***Действие***
show passwords configuration	Отображает информацию об ограничениях на пароли.

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 5.19.

Таблица 5.19 – Список ключевых слов и их описание

Ключевое слово	*Описание*
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.
startup-config	Файл первоначальной конфигурации.
image	Если исходный файл – данный образ активный. Если удаленный файл – данный образ не активный.
boot	Загрузочный файл.
tftp://	Исходный адрес или адрес места назначения для TFTP-сервера. Синтаксис: **tftp://host/[directory/] filename.** - *host* – IPv4-адрес или сетевое имя устройства; - *directory* – каталог; - *filename* – имя файла.
scp://	Исходный адрес или адрес места назначения для SSH-сервера. Синтаксис: **scp://[username[:password]@]host/[directory/] filename** - *username* – имя пользователя; - *password* – пароль пользователя; - *host* – IPv4-адрес или сетевое имя устройства; - *directory* – каталог; - *filename* – имя файла.
xmodem:	Исходный адрес файла при использовании протокола X-modem по последовательному соединению.
unit://*member***/ startup-config**	Конфигурационный файл, используемый при запуске устройства. *member* – может быть IP-адресом или сетевым именем устройства в стеке.
unit://*member***/ image**	Файл системного ПО на устройстве или на одном из устройств стека. Для копирования с ведущего устройства на все остальные модули можно в элементе *member* использовать «*». *member* – может быть IP-адресом или сетевым именем устройства в стеке.
unit://*member***/ boot**	Загрузочный файл на устройстве или на одном из устройств стека. Для копирования с ведущего устройства на все остальные модули можно в элементе *member* использовать «*». *member* – может быть IP-адресом или сетевым именем устройства в стеке.
null:	Пустое место назначения для копий или файлов. Можно копировать удаленный файл к пустому указателю, чтобы определить его размер.
logging	Файл с историей команд.
unit://*member***/ backup-config**	Резервный файл конфигурации на устройстве или на одном из устройств стека. *member* – может быть IP-адресом или сетевым именем устройства в стеке.

5.6.2 Команды для работы с файлами

Команды для работы с файлами доступны только привилегированному пользователю.

Запрос командной строки в режиме Privileged EXEC имеет следующий вид:

```
console#
```

Таблица 5.20 – Команды для работы с файлами в режиме Privileged EXEC

Команда	***Значение***	***Действие***
copy *source-url destination-url* **[snmp]**	source-url: (1..160) символов; destination-url: (1..160) символов;	Копирование файла из местоположения источника в местоположение назначения. - **snmp** – используется только когда копирование осуществляется из/в startup-config. Специфицирует использование исходного адреса или адреса места назначения в формате SNMP; - *source-url* – местоположение копируемого файла; - *destination-url* – адрес места назначения, куда файл будет скопирован.
copy *source_url* **image**		Копирование файла системного ПО с сервера в энергонезависимую память.
copy *source_url* **boot**		Копирование загрузочного файла с сервера в энергонезависимую память.
copy *source_url* **running-config**		Копирование файла конфигурации с сервера в текущую конфигурацию.
copy *source_url* **startup-config**		Копирование файла конфигурации с сервера в первоначальную конфигурацию.
copy running-config *destination_url*		Сохранение текущей конфигурации на сервере.
copy startup-config *destination_url*		Сохранение первоначальной конфигурации на сервере.
copy running-config startup-config	-	Сохранение текущей конфигурации в первоначальную конфигурацию.
copy running-config *file*	-	Сохранение текущей конфигурации в заданный резервный файл конфигурации. Поддерживается два файла конфигурации.
copy startup-config *file*	-	Сохранение первоначальной конфигурации в заданный резервный файл конфигурации.
copy running-config backup-config	-	Сохранение текущей конфигурации в резервный файл конфигурации.
copy startup-config backup-config	-	Сохранение первоначальной конфигурации в резервный файл конфигурации.
dir	-	Отображает список файлов во флэш-памяти
more {flash://<*file*> | **startup-config | running-config | mirror-config |** <*file*>}	<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 USB flash-накопителей; - **mirror-config** – отображает содержимое файла текущей конфигурации с зеркала; - <*file*> – имя файла. **Файлы отображаются в формате ASCII, за исключением image, которые отображаются в шестнадцатеричном формате.** ***.prv файлы не отображаются.**
delete url	-	Удаление файла с флэш-памяти устройства. Файлы *.prv, image-1 и image-2 не могут быть удалены.
delete startup-config	-	Удаления файла первоначальной конфигурации.
boot system [unit *unit*] **{image-1| image-2}**	unit (1..8)	Определяет файл системного ПО, который будет загружен при запуске. - *unit* – номер устройства в стеке (для коммутатора, работающего в автономном режиме, параметр не используется).

show { startup-config |running-config} [aaa| acl| dhcp| eaps| ip-address| channel-group| multicast| management| selective-qinq| qos| routing| snmp| sntp| syslog| spanning-tree| vlan| interfaces [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***| vlan** *vlan_id***]]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12); vlan_id (1..4094)	Отображает содержимое файла первоначальной конфигурации (startup-config) или текущей конфигурации (running-config). Для уменьшения объема отображаемых данных возможен выбор одного из разделов конфигурации. Перечень существующих разделов конфигурации: - **aaa** – настройки параметров авторизации, аутентификации и учета (AAA); - **acl** – конфигурация списков доступа; - **dhcp** – конфигурация DHCP-сервера, функции DHCP relay; - **eaps** – конфигурация протокола EAPS; - **ip-address** – конфигурация IP-интерфейсов; - **channel-group** – конфигурация групп портов (port-channel); - **multicast** – конфигурация многоадресной маршрутизации - IGMP-proxy, IGMP snooping; - **management** – конфигурация управления и доступа к устройству - сервисов web, ssh, telnet; - **selective-qinq** – конфигурация функции Selective Q-in-Q; - **qos** – конфигурация параметров качества облуживания QoS; - **routing** – конфигурация статической маршрутизации, протоколов RIP, OSPF; - **snmp** – конфигурация протокола SNMP; - **sntp** – конфигурация протокола SNTP; - **syslog** – конфигурация syslog; - **spanning-tree** – конфигурация протоколов семейства Spanning Tree; - **vlan** – конфигурация VLAN; - **interfaces** – конфигурация интерфейсов коммутатора - физических интерфейсов, групп интерфейсов (port-channel), VLAN-интерфейсов.
show bootvar [**unit** *unit*]	unit (1..8)	Показывает активный файл системного ПО, который устройство загружает при запуске. - *unit* – номер устройства в стеке (для коммутатора, работающего в автономном режиме, параметр не используется). **Параметр [unit *unit*] при выполнении команды доступен только в режиме стекирования**
write [memory|terminal]		Сохранение текущей конфигурации в файл первоначальной конфигурации.
rename *url new_url*	url: (1 .. 160)	Изменение имени файла. - *url* – текущее имя файла; - *new-url* – новое имя файла.

Существуют некоторые недопустимые комбинации местоположения и места назначения. Нельзя копировать в следующих случаях:

- **если исходный файл и файл назначения – один и тот же файл;**
- **xmodem не может быть адресом назначения. По X-modem с адреса источника файл может быть скопирован только в файл системного ПО, в загрузочный файл или в null;**
- **сервер TFTP не может быть адресом источником и адресом назначения для одной команды копирования;**
- ***.prv файлы не могут быть скопированы;**
- **копирование к/от устройств стека, работающих в ведомом режиме, возможно только для файла системного ПО и загрузочного файла.**

Таблица 5.21 - Описание признаков копирования

Признак	*Описание*
!	Восклицательный знак означает, что процесс копирования идет успешно. Каждый восклицательный знак указывает на успешную передачу десяти пакетов (512 байтов каждый).

.	Точка означает, что процесс копирования прерван. Несколько точек подряд означает, что в процессе копирования возникла ошибка.

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 глобального конфигурирования

Запрос командной строки в режиме глобального конфигурирования имеет следующий вид:

```
console(config)#
```

Таблица 5.22 – Команды управления системой в режиме глобального конфигурирования

Команда	***Значение/ Значение по умолчанию***	***Действие***
backup server *server*	server: 1..22 символов	Указание TFTP-сервера, на который будет производиться резервирование конфигурации. Строка в формате «tftp://XXX.XXX.XXX.XXX».
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 мин/720мин	Указание промежутка времени, по истечении которого будет осуществляться автоматическое резервирование конфигурации.
no backup time-period		Восстанавливает значение по умолчанию
backup auto	disabled	Включение автоматического резервирования конфигурации.
no backup auto		Установка значения по умолчанию.
backup write-memory	disabled	Включение резервирования конфигурации при сохранении пользователем конфигурации на flash-накопитель.
no backup write-memory		Установка значения по умолчанию.

Таблица 5.23 – Команды управления системой в режиме Privileged EXEC

Команда	***Действие***
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 конфигурирования

Процесс автоматического обновления

Коммутатор запускает процесс автоматического обновления, базирующийся на DHCP (до процесса автоматической конфигурации), если он включен и имя текстового файла (DHCP-опция 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.

Если пользователь включил автоматическое сохранение (команда boot host auto-save), то текущая (running) конфигурация будет скопирована в первоначальную конфигурацию (startup).

Команды режима глобального конфигурирования

Запрос командной строки в режиме глобального конфигурирования имеет следующий вид:

```
console(config)#
```

Таблица 5.24 – Команды управления системой в режиме глобального конфигурирования

Команда	*Значение/ Значение по умолчанию*	*Действие*
boot host auto-config	-/включено	Включение автоматического конфигурирования, базирующегося на DHCP.
no boot host auto-config		Установка значения по умолчанию.
boot host auto-save	-/выключено	Включение автоматического сохранения текущей конфигурации в первоначальную после получения ее по TFTP.
no boot host auto-save		Установка значения по умолчанию.
boot host auto-update	-/включено	Включение автоматического обновления ПО, базирующегося на DHCP.
no boot host auto-update		Установка значения по умолчанию.

boot host dhcp	-/выключено	Включение принудительной загрузки конфигурации при следующем включении коммутатора.
no boot host dhcp		Установка значения по умолчанию.

Команды режима privileged EXEC

Запрос командной строки в режиме privileged EXEC имеет следующий вид:

console#

Таблица 5.25 – Команды управления системой в режиме privileged EXEC

Команда	*Значение/ Значение по умолчанию*	*Действие*
show boot	-	Просмотр настроек автоматического обновления и конфигурирования.

- 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 mes3124-test {
         hardware ethernet a8:f9:4b:85:a2:00;  #mac-адрес коммутатора
         filename "mes3124-test.cfg";          #имя конфигурации коммутатора
         option image-filename 35265 18 1 16 "mes3000-2544.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 5.26 - Команды настройки системного времени в режиме Privileged EXEC

Команда	*Значение*	*Действие*
clock set *hh:mm:ss day month year* **clock set** *hh:mm:ss month day year*	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). - *hh* – часы, *mm* – минуты, *ss* – секунды; - *day* – день; *month* – месяц; *year* – год.
show sntp configuration	-	Показывает конфигурацию протокола SNTP.

show sntp status	-	Показывает статус протокола SNTP.

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

console>

Таблица 5.27 - Команды настройки системного времени в режиме «EXEC»

Команда	***Значение***	***Действие***
show clock	-	Показывает системное время и дату.
show clock detail		Дополнительно отображает параметры часового пояса и перехода на летнее время.

Команды режима глобального конфигурирования

Запрос командной строки в режиме глобального конфигурирования имеет следующий вид:

console(config)#

Таблица 5.28 – Список команд для настройки системного времени в режиме глобального конфигурирования

Команда	***Значение/Значение по умолчанию***	***Действие***
clock source sntp	-/внешний источник не используется	Использование внешнего источника для установки системного времени.
no clock source		Запрещает использование внешнего источника для установки системного времени.
clock timezone *zone hours-offset* **[minutes** *minutes-offset***]**	zone описание до 4 символов/ нет описания зоны hours-offset -12..+13/0; minutes-offset (0..59)/0;	Устанавливает значение часового пояса. - *zone* – слово, сформированное из первых букв словосочетания, которое оно заменяет (описание зоны); - *hours-offset* – часовое смещение относительно нулевого меридиана UTC; - *minutes-offset* – минутное смещение относительно нулевого меридиана UTC.
no clock timezone		Устанавливает значение по умолчанию.
clock summer-time *zone* **date** *date month year hh:mm date month year hh:mm* **[***offset***]**	zone (1..4) символа/ нет описания зоны week (1..4, first, last); day (mon..sun); date(1..31); month (Jan..Dec); year (2000 ..2097); hh (0..23), mm (0..59); offset(1..1440)/60 мин; По умолчанию переход на летнее время выключен	Задает дату и время для автоматического перехода на летнее время и возврата обратно (для определенного года). Первым в команде указывается описание зоны, вторым время для перехода на летнее время и третьим время для возврата. - *zone* – слово, сформированное из первых букв словосочетания, которое оно заменяет (описание зоны); - *date* – число; - *month* – месяц; - *year* – год; - *hh* – часы, *mm* – минуты; - *offset* – количество минут, добавляемых при переходе на летнее время.
clock summer-time *zone* **date** *month date year hh:mm month date year hh:mm* **[***offset***]**		

clock summer-time *zone* **recurring {usa|eu|** **{***week day month hh:mm week day month hh:mm***}}** **[***offset***]**		Задает дату и время для автоматического перехода на летнее время и возврата обратно в режиме ежегодно. - *zone* – слово, сформированное из первых букв словосочетания, которое оно заменяет (описание зоны); - *usa* – 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); - *eu* – установить правила перехода на летнее время, используемые Евросоюзом (переход в последнее воскресенье марта, обратно в последнее воскресенье октября, в 1 час утра по Гринвичу); - *hh* – часы, *mm* – минуты; - *week* – неделя месяца (может принимать значения: 1-4, первая, последняя); - *day* – день недели; - *month* – месяц; - *offset* – количество добавляемых минут при переходе на летнее время.
no clock summer-time		Отключает автоматический переход на летнее время.
sntp authentication-key *number* **md5** *value*	number (1..4294967295); value (1..8) символов; По умолчанию проверка подлинности отключена	Устанавливает ключ проверки подлинности для протокола SNTP. - *number* – номер ключа; - *value* – значение ключа.
no sntp authentication-key *number*		Удаляет ключ проверки подлинности для протокола SNTP.
sntp authenticate	-/проверка подлинности не требуется	Требует проверку подлинности для получения информации от NTP-серверов.
no sntp authenticate		Устанавливает значение по умолчанию.
sntp trusted-key *key-number*	key-number (1..4294967295); По умолчанию проверка подлинности отключена	Осуществляет проверку подлинности системы, от которой синхронизируется с помощью SNTP по заданному ключу. - *key-number* – номер ключа.
no sntp trusted-key *key-number*		Устанавливает значение по умолчанию.
sntp client poll timer *seconds*	seconds (60 .. 86400) /1024	Устанавливает время опроса для SNTP-клиента.
no sntp client poll timer		Устанавливает значение по умолчанию.
sntp broadcast client enable	-/запрещено	Разрешает работу широковещательных SNTP-клиентов.
no sntp broadcast client enable		Устанавливает значение по умолчанию.
sntp anycast client enable	-/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 *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***| vlan** *vlan_id***}**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12); vlan_id (1..4094) /запрещено	Разрешает работу SNTP-клиентам, поддерживающим метод рассылки пакетов, позволяющий посылать данные ближайшему устройству из группы получателей, а также широковещательным SNTP-клиентам для выбранного интерфейса. - подробное описание интерфейсов изложено в разделе «Конфигурирование интерфейсов».
no sntp client enable { gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***| vlan** *vlan_id***}**		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 **{***ipv4_address* | *ipv6_address* |{ ipv6-link-local-address} *%{vlan {integer} | ch {integer} | isatap {integer} | {physical-port-name}}| hostname***}** **[poll]** **[key** *keyid***]**	hostname: (1..158) символов; keyid: (1..4294967295)	Задает адрес SNTP-сервера. - *ipv4_address* - Ipv4-адрес узла сети; - *ipv6_address* - Ipv6-адрес узла сети; - *ipv6z-address* - Ipv6z-адрес узла сети для ping. Формат адреса {ipv6-link-local-address}%{interface-name}; ipv6-link-local-address – локальный IPv6 адрес канала; interface-name –имя исходящего интерфейса задается в следующем формате: vlan {integer} | ch {integer} | isatap {integer} | {physical-port-name} - *hostname* – доменное имя узла сети; - **poll** – включает опрос; - *keyid* – идентификатор ключа.
no sntp server {*ipv4_address | ipv6_address | { ipv6-link-local-address}% {vlan {integer} | ch {integer} | isatap {integer} | {physical-port-name} }| hostname***}**		Удаление сервера из списка NTP-серверов.
sntp port *port-number*	port-number: (1..65535)/123	Определяет UDP-порт SNTP сервера.
no sntp port		Устанавливает значение по умолчанию.
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 конфигурирования интерфейса

Запрос командной строки в режиме конфигурирования интерфейса имеет следующий вид:

console(config-if)#

Таблица 5.29 – Список команд для настройки системного времени в режиме конфигурирования 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 широковещательному 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;
- отсутсвие 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 0, reference is 192.168.16.1, unicast
Reference time is cec866d5.8a20cccb 05:47:01.0 UTC Dec 8 2009
Unicast servers:
    Server       Status      Last Response     Offset   Delay
                                               [mSec]   [mSec]
--------------- --------- ------------------- --------- -------
 192.168.16.1      up     05:47:01.0 UTC Dec     7230  -1000
                          8 2009
Anycast server:
    Server      Interface  Status        Last Response       Offset   Delay
                                                             [mSec]   [mSe
--------------- --------- --------- ----------------------- --------- -------
Broadcast:
 Interface     IP address         Last Response
```

В примере выше системное время синхронизировано от сервера 192.168.16.1, последний ответ получен в 05:47:01, несовпадение системного времени с временем на сервере составило 7.23с.

5.8 Конфигурирование интерфейсов и VLAN

В зависимости от того в каком режиме работает коммутатор – автономно или в составе стека, изменяется вид записи для интерфейса Ethernet. При автономной работе запись для интерфейса имеет вид: 1/0/N, где N – номер интерфейса; при работе в составе стека запись для интерфейса имеет вид: K/0/N, где K – номер устройства в стеке, N – номер интерфейса. Выбор режима работы коммутатора описан в пункте *4.4 Режимы работы коммутатора.*

Значение маски может быть записано либо в формате X.X.X.X, либо в формате /N, где N – количество единиц в двоичном представлении маски.

Сброс настроек интерфейса на значения по умолчанию выполняется следующей командой:

console(config)# **default interface** {**gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **| port-channel** *group* **| ip** *ip* **| vlan** *vlan_id* | **tunnel** *tunnel_id* | **range** *{…}*}

5.8.1 Настройка параметров Ethernet-интерфейсов и интерфейсов Port-Channel

Команды режима конфигурирования интерфейса (диапазона интерфейсов)

console# **configure**
console(config)# **interface** { **gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **| port-channel** *group* **| range** *{…}*}
console(config-if)#

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

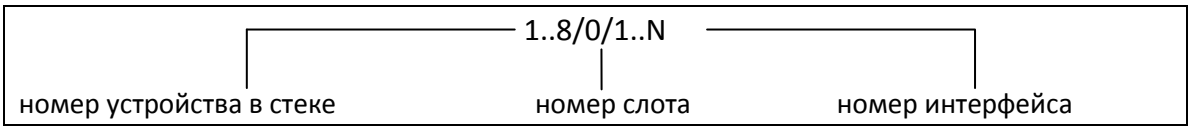
Выбор интерфейса осуществляется при помощи команд:

- **interface gigabitethernet** *gi_port* – для настройки интерфейсов Ethernet g1-g24;
- **interface tengigabitethernet** *te_port* – для настройки интерфейсов Ethernet XG1-XG4;
- **interface port-channel** *group* – для настройки группы каналов,

где

- group – порядковый номер группы каналов принимает значения (1..12);
- gi_port – порядковый номер интерфейса Ethernet g1-g24
  задается в виде: 1..8/0/1..24;
- te_port – порядковый номер интерфейса Ethernet XG1-XG4
  задается в виде: 1..8/0/1..4.

Запись интерфейса



Команды, введенные в режиме конфигурирования 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 gigabitethernet** *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 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 и для входа в режим настройки всех групп портов.

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

console# configure
console(config)# interface range port-channel 1-8
console(config-if)#
```

Таблица 5.30 – Команды режима конфигурирования интерфейса Ethernet и Port-Channel

Команда	***Значение/Значение по умолчанию***	***Действие***
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, port-channel). **Для портов XG1-XG4 возможно переключение скорости (1000-10000)**
no speed		Установить значение по умолчанию.
media-type {force-fiber | force-copper | prefer-fiber | prefer-copper}	-/prefer-fiber	**- force-fiber** – разрешена активность только оптической части комбо-порта; **- force-copper –** разрешена активность только медной части комбо-порта; **- prefer-fiber –** преимущество оптического линка**;** **- prefer-copper –** преимущество медного линка. **Только для комбо-портов**.
no media-type		Установить значение по умолчанию.
duplex *mode*	mode: (full, half)/full	Задать режим дуплекса интерфейса (полнодуплексное соединение, полудуплексное соединение, Ethernet). **Данная команда недоступна для портов XG1-XG4**
no duplex		Установить значение по умолчанию.
negotiation [*cap1* [*cap2… cap5*]]	cap: (10f, 10h, 100f, 100h, 1000f)	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). **Данная команда недоступна для портов XG1-XG4**
no negotiation		Выключает автосогласование для скорости и дуплекса на настраиваемом интерфейсе.
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.

mdix *mode*	mode: (on, auto)/auto	Позволяет использование «перекрещенного» кабеля на настраиваемом интерфейсе (Ethernet). **Данная команда недоступна для портов XG1-XG4**
no mdix		Запрещает использование «перекрещенного» кабеля на настраиваемом интерфейсе.
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.

Команды режима глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

```
console(config)#
```

Таблица 5.31 – Команды режима общих настроек интерфейса Ethernet и Port-Channel

Команда	***Значение/Значение по умолчанию***	***Действие***
port jumbo-frame	-/запрещено	Разрешает коммутатору работать с фреймами большого размера. **Значение maximum transmission unit (MTU) по умолчанию 1500 байт.** **Настройка вступит в силу только после перезагрузки устройства.** **Значение maximum transmission unit (MTU) при настройке port jumbo-frame 10200 байт.**
no port jumbo-frame		Запрещает коммутатору работать с фреймами большого размера.
errdisable recovery cause {loopack-detection | port-security | dot1x-src-address | acl-deny | stp-bpdu-guard | stp-loopback-guard}	-/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 (приём несанкционированного пакета BPDU на интерфейсе); - **stp-loopback-guard** — обнаружение петель протоколом STP.
no errdisable recovery cause {loopack-detection | port-security | dot1x-src-address | acl-deny | stp-bpdu-guard | stp-loopback-guard}		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.
default interface [range] { gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group* **}**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Сброс настроек интерфейса или группы интерфейсов на значения по умолчанию.

Команды режима EXEC

Вид запроса командной строки в режиме EXEC:

`console#`

Таблица 5.32 – Команды режима EXEC

Команда	*Значение*	*Действие*
clear counters	-	Сброс статистики для всех интерфейсов.
clear counters { gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group* }	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Сброс статистики для Ethernet-порта, группы портов.
set interface active { gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group* }	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Активирует порт или группу портов, выключенных командой **shutdown**.
show interfaces configuration {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group*}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Показать конфигурацию интерфейсов.
show interfaces status	-	Показать состояние всех интерфейсов.
show interfaces status { gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group* }	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Показать состояние Ethernet-порта, группы портов.
show interfaces { gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group* }	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Показать сводную информацию о состоянии, настройке и статистике Ethernet-порта, группы портов.
show interfaces advertise	-	Показать параметры автосогласования, объявленные для всех интерфейсов.
show interfaces advertise { gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group* }	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Показать параметры автосогласования, объявленные для Ethernet-порта, группы портов.
show interfaces description	-	Показать описания всех интерфейсов.
show interfaces description { gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group* }	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Показать описание Ethernet-порта, группы портов.
show interfaces counters	-	Показать статистику для всех интерфейсов.
show interfaces counters { gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group* }	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Показать статистику для Ethernet-порта.
show interfaces utilization	-	Показать статистику по нагрузке для всех интерфейсов.
show interfaces utilization {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Показать статистику по нагрузке для Ethernet-интерфейса.
show interfaces mtu {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group*}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Показать настройки MTU на интерфейсе.
show ports jumbo-frame	-	Показать настройку jumbo-frames в коммутаторе.
show errdisable recovery	-	Показать настройки для автоматической повторной активации порта.
show errdisable interfaces	gi_port: (1..8/0/1..24);	Показать причину отключения порта, группы портов и

{gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group*}	te_port: (1..8/0/1..4); group: (1..12)	состояние автоматической активации.

Примеры выполнения команд.

- Показать состояние интерфейсов:

console# **show interfaces status**

```
                                                Flow Link          Up Time     Back   Mdix
Port     Type         Duplex  Speed Neg      ctrl State        (d,h:m:s)  Pressure Mode    Port Mode
-------- ------------ ------  ----- -------- ---- ----------- ----------- -------- ------- ---------
gi1/0/1  1G-Copper    Full    1000  Enabled  Off  Up          01,00:54:25 Disabled Off     Trunk
gi1/0/2  1G-Copper      --      --     --     --  Down            --         --     --     Access
gi1/0/3  1G-Copper      --      --     --     --  Down            --         --     --     Access
gi1/0/4  1G-Copper      --      --     --     --  Down            --         --     --     Access
gi1/0/5  1G-Copper      --      --     --     --  Down            --         --     --     Access
gi1/0/6  1G-Copper      --      --     --     --  Down            --         --     --     Access
gi1/0/7  1G-Copper      --      --     --     --  Down            --         --     --     Access
gi1/0/8  1G-Copper      --      --     --     --  Down            --         --     --     Access
gi1/0/9  1G-Copper      --      --     --     --  Down            --         --     --     Access
gi1/0/10 1G-Copper      --      --     --     --  Down            --         --     --     Access
gi1/0/11 1G-Copper      --      --     --     --  Down            --         --     --     Access
gi1/0/12 1G-Copper      --      --     --     --  Down            --         --     --     Access
gi1/0/13 1G-Copper      --      --     --     --  Down            --         --     --     Access
gi1/0/14 1G-Copper      --      --     --     --  Down            --         --     --     Access
gi1/0/15 1G-Copper      --      --     --     --  Down            --         --     --     Access
gi1/0/16 1G-Copper      --      --     --     --  Down            --         --     --     Access
gi1/0/17 1G-Copper      --      --     --     --  Down            --         --     --     Access
gi1/0/18 1G-Copper      --      --     --     --  Down            --         --     --     Access
gi1/0/19 1G-Copper      --      --     --     --  Down            --         --     --     Access
gi1/0/20 1G-Copper      --      --     --     --  Down            --         --     --     Access
gi1/0/21 1G-Copper      --      --     --     --  Down            --         --     --     Access
gi1/0/22 1G-Copper      --      --     --     --  Down            --         --     --     Access
gi1/0/23 1G-Copper      --      --     --     --  Down            --         --     --     Access
gi1/0/24 1G-Copper      --      --     --     --  Down            --         --     --     General
gi1/0/25 1G-Combo-C     --      --     --     --  Down            --         --     --     Access
gi1/0/26 1G-Combo-C   Full    1000  Enabled  Off  Up          01,00:25:56 Disabled Off     Access
gi1/0/27 1G-Combo-C     --      --     --     --  Down            --         --     --     Trunk
gi1/0/28 1G-Combo-C   Full    1000  Enabled  Off  Up          01,00:54:25 Disabled On      General

                                  Flow     Link
Ch       Duplex  BW     Neg      control  State        Port Mode
-------- ------  -----  -------- -------  -----------  ---------
Po1      Full    1000   Enabled  Off      Up           Trunk
Po2        --      --      --       --    Not Present  Access
Po3        --      --      --       --    Not Present  Access
Po4        --      --      --       --    Not Present  Access
Po5        --      --      --       --    Not Present  Access
Po6        --      --      --       --    Not Present  Access
Po7        --      --      --       --    Not Present  Access
Po8        --      --      --       --    Not Present  Access
```

- Вывести информацию об интерфейсах:

console# **show interfaces GigabitEthernet 1/0/11**

```
gigabitethernet 1/0/11 is up (connected)
  Interface index is 59
  Hardware is gigabitethernet, MAC address is a8:f9:4b:f1:1d:0b
  Interface MTU is 1500
  Full-duplex, 100Mbps, link type is auto, media type is 1G-Combo-C
  Link is up for 0 days, 22 hours, 12 minutes and 35 seconds
  Advertised link modes: 1000baseT/Full 100baseT/Full
                         100baseT/Half 10baseT/Full
                         10baseT/Half
  Flow control is off, MDIX mode is off
  15 second input rate is 0 Kbit/s
  15 second output rate is 0 Kbit/s
      111594 packets input, 7142016 bytes received
```

```
       3 broadcasts, 42367 multicasts
       0 input errors, 0 FCS, 0 alignment
       0 oversize, 0 internal MAC
       0 pause frames received
       9652 packets output, 2456440 bytes sent
       6665 broadcasts, 2987 multicasts
       0 output errors, 0 collisions
       0 excessive collisions, 0 late collisions
       0 pause frames transmitted
       0 symbol errors, 0 carrier, 0 SQE test error
```

- Показать параметры авто-согласования:

console# **show interfaces advertise**

```
Port      Type         Neg      Operational Link Advertisement
--------- ------------ -------- ---------------------------------
gi0/1     1G-Fiber     Disabled                 --
gi0/2     1G-Fiber     Disabled                 --
gi0/3     1G-Fiber     Disabled                 --
…
gi0/22    1G-Fiber     Disabled                 --
gi0/23    1G-Combo-C   Enabled                  --
gi0/24    1G-Combo-C   Enabled  1000f, 100f, 100h, 10f, 10h
te0/1     10G-Fiber    Disabled                 --
te0/2     10G-Fiber    Disabled                 --
te0/3     10G-Fiber    Disabled                 --
te0/4     10G-Fiber    Disabled                 --

Ch        Type         Neg      Operational Link Advertisement
--------- ------------ -------- ---------------------------------
Po1            --      Enabled                  --
…
Po7            --      Enabled                  --
Po8            --      Enabled                  --
```

- Показать статистику по интерфейсам:

console# **show interfaces counters**

```
       Port       InUcastPkts  InMcastPkts  InBcastPkts    InOctets
---------------- ------------ ------------ ------------ ------------
     gi0/1            0            0            0            0
     gi0/2            0            0            0            0
     gi0/3            0            0            0            0
     gi0/4            0            0            0            0
     gi0/5            0            0            0            0
     gi0/6            0            0            0            0
     gi0/7            0            0            0            0
     gi0/8            0            0            0            0
     gi0/9            0            0            0            0
     gi0/10           0            0            0            0
     gi0/11           0            0            0            0
     gi0/12           0            0            0            0
     gi0/13           0            0            0            0
     gi0/14           0            0            0            0
     gi0/15           0            0            0            0
     gi0/16           0            0            0            0
     gi0/17           0            0            0            0
     gi0/18           0            0            0            0
     gi0/19           0            0            0            0
     gi0/20           0            0            0            0
More: <space>,  Quit: q, One line: <return>
```

- 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
```

Таблица 5.33 - Описание счетчиков

Счетчик	***Описание***
InOctets	Количество принятых байтов.
InUcastPkts	Количество принятых одноадресных пакетов.
InMcastPkts	Количество принятых многоадресных пакетов.
InBcastPkts	Количество принятых широковещательных пакетов.
OutOctets	Количество переданных байтов.
OutUcastPkts	Количество переданных одноадресных пакетов.
OutMcastPkts	Количество переданных многоадресных пакетов.
OutBcastPkts	Количество переданных широковещательных пакетов.
Alignment Errors	Количество принятых фреймов с нарушенной целостностью (с количеством байт не соответствующим длине) и не прошедших проверку контрольной суммы (FCS).
FCS Errors	Количество принятых фреймов с количеством байт, соответствующим длине, но не прошедших проверку контрольной суммы (FCS).
Single Collision Frames	Количество фреймов, вовлеченных в единичную коллизию, но впоследствии переданных успешно.
Multiple Collision Frames	Количество фреймов, вовлеченных более чем в одну коллизию, но впоследствии переданных успешно.
Deferred Transmissions	Количество фреймов, для которых первая попытка передачи отложена из-за занятости среды передачи.

Late Collisions	Количество случаев, когда коллизия зафиксирована после того, как в канал связи уже были переданы первые 64 байт (slotTime) пакета.
Excessive Collisions	Количество фреймов, которые не были переданы из-за избыточного количества коллизий.
Carrier Sense Errors	Количество случаев, когда состояние контроля несущей было потеряно, либо не утверждено при попытке передачи фрейма.
Oversize Packets	Количество принятых пакетов, размер которых превышает максимальный разрешенный размер фрейма.
Internal MAC Rx Errors	Количество фреймов, которые не были приняты успешно из-за внутренней ошибки приема на уровне MAC.
Symbol Errors	Для интерфейса, работающего в режиме 100Мб/с – количество случаев, когда имелся недопустимый символ данных, в то время как правильная несущая была представлена. Для интерфейса, работающего в полудуплексном режиме 1000Мб/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. Для интерфейса, работающего в полном дуплексном режиме 1000Мб/с – количество случаев, когда средства приема заняты в течение времени, равному или большему чем минимальный размер фрейма (minFrameSize), и в течение которого имелось хотя бы одно событие, которое заставляет PHY выдавать ошибку приема данных (Data reception error) на GMII.
Received Pause Frames	Количество принятых управляющих MAC-фреймов с кодом операции PAUSE.
Transmitted Pause Frames	Количество переданных управляющих MAC-фреймов с кодом операции PAUSE.

5.8.2 Настройка VLAN и режимов коммутации интерфейсов

Команды режима конфигурирования VLAN

Вид запроса командной строки в режиме конфигурирования VLAN:

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

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

Таблица 5.34 – Команды режима конфигурирования VLAN

Команда	***Значение/Значение по умолчанию***	***Действие***
vlan *VLANlist*	*VLANlist*: (2 .. 4094)	Добавить VLAN, или несколько VLAN.
no vlan *VLANlist*		Удалить VLAN, или несколько VLAN.
map protocol *protocol* [*encaps*] **protocols-group** *group*	protocol (ip, ipx, ipv6, arp, (0600-ffff (hex)}*) encaps (ethernet, rfc1042, llcOther) ethernet group (1.. 2147483647)	Привязать протокол к группе протоколов ассоциированных вместе.
no map protocol *protocol* [*encaps*]		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.
no map subnet *ip_address mask*		Удалить привязку.

Команды режима конфигурирования интерфейса (диапазона интерфейсов) VLAN

Вид запроса командной строки в режиме конфигурирования интерфейса VLAN:

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

Данный режим доступен из режима конфигурирования 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 5.35 – Команды режима конфигурирования интерфейса VLAN

Команда	***Значение/Значение по умолчанию***	***Действие***
name *name*	(1-64) символов/ имя соответствует номеру VLAN	Добавить имя VLAN.
no name		Установить значение по умолчанию.

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

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

```
console# configure
console(config)# interface {tengigabitethernet te_port | gigabitethernet
gi_port |port-channel group | range {…}}
console(config-if)#
```

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

Порт может работать в следующих 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* – 802.1 Q-in-Q интерфейс;
- *promiscuous* – принимающий и передающий трафик private vlan
- *host* – интерфейс принадлежащий к isolated или community vlan

Таблица 5.36 – Команды режима конфигурирования интерфейса Ethernet

Команда	***Значение/Значение по умолчанию***	***Действие***
switchport mode *mode*	access, trunk, general, customer/ access	Задать режим работы порта в VLAN. - *mode* – 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. - *vlan_id* – идентификационный номер VLAN.
no switchport access vlan		Установить значение по умолчанию.
switchport general acceptable-frame-type { untagged-only|tagged-only | all}	-/принимать все типы фреймов	Принимать на интерфейсе только фреймы определенного типа: - **untagged-only** – только нетегированные; - **tagged-only** – только тегированные; - **all** – все фреймы.
switchport trunk allowed vlan add *vlan_list*	vlan_list: (2..4094, all)	Добавить список VLAN для интерфейса. - *vlan_list* – 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. - *vlan_id* – идентификационный номер VLAN.
no switchport trunk native vlan		Установить значение по умолчанию.
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. - *vlan_list* – 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 *vlan_id*	vlan_id: (1..4094)/ 1 – если установлен VLAN по умолчанию	Добавить идентификатор VLAN порта (PVID) для основного интерфейса. - *vlan_id* – 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 фреймов	Принимать на основном интерфейсе только фреймы определенного типа: - **tagged-only** – только тегированные; - **untagged-only** – только не тегированные; - **all** – все фреймы.
no switchport general acceptable-frame-type		Принимать на основном интерфейсе все типы фреймов.
switchport general map protocols-group *group* **vlan** *vlan_id*	vlan_id: (1..4094) group: (1.. 2147483647)	Установить правило классификации VLAN для интерфейса, основанное на привязке к протоколу. - *group* – идентификационный номер группы; - *vlan_id* – идентификационный номер VLAN.
no switchport general map protocols-group *group*		Удалить правило классификации.
switchport general map macs-group *group* **vlan** *vlan_id*	vlan_id: (1..4094) group: (1.. 2147483647)	Установить правило классификации VLAN для интерфейса, основанное на привязке к MAC-адресу. - *group* – идентификационный номер группы; - *vlan_id* – идентификационный номер VLAN.
no switchport general map macs-group *group*		Удалить правило классификации.
switchport general map subnets-group *group* **vlan** *vlan_id*	vlan_id: (1..4094) group: (1.. 2147483647)	Установить правило классификации VLAN для интерфейса, основанное на привязке к IP-адресу. - *group* – идентификационный номер группы; - *vlan_id* – идентификационный номер VLAN.
no switchport general map subnets-group *group*		Удалить правило классификации.
switchport dot1q ethertype egress stag *ethertype*	ethertype: **(**0..ffff) (hex)	Заменить EtherType в исходящих с данного интерфейса пакетах. **Значение Ethertype не должно совпадать с зарезервированными номерами протоколов или быть меньше максимального размера. Основные зарезервированные номера протоколов приведены в таблице 5.37.**
no switchport dot1q ethertype egress stag		Установить значение по умолчанию.
switchport dot1q ethertype ingress stag add *ethertype*	ethertype: (0..ffff) (hex)	Добавить EtherType в таблицу идентификаторов VLAN. **Значение Ethertype не должно совпадать с зарезервированными номерами протоколов или быть меньше максимального размера. Основные зарезервированные номера протоколов приведены в таблице 5.37.**
switchport dot1q ethertype ingress stag remove *ethertype*		Удалить EtherType из таблицы идентификаторов VLAN.
switchport customer vlan *vlan_id*	vlan_id: (1..4094)/1	Добавить VLAN для пользовательского интерфейса. - *vlan_id* – идентификационный номер VLAN.
no switchport customer vlan		Установить значение по умолчанию.
switchport customer multicast-tv vlan *vlan_id*	vlan_id: (1..4094)	Разрешает принимать многоадресный трафик из указанной VLAN (не являющейся VLAN пользовательского интерфейса) на настраиваемом интерфейсе, совместно с пользователями других пользовательских портов, принимающих многоадресный трафик из данной VLAN. - *vlan_id* – идентификационный номер VLAN.
no switchport customer multicast-tv vlan		Запрещает принимать многоадресный трафик на настраиваемом интерфейсе.
switchport forbidden vlan add *vlan_list*	vlan_list: (2..4094, all)/ все VLAN разрешены порту	Запретить добавление указанных VLAN порту. - *vlan_list* – список VLAN ID. Диапазон VLAN можно задать перечислением через запятую или указать начальное и конечное значения диапазона через дефис "-".
switchport forbidden vlan remove *vlan_list*		Разрешить добавление указанных VLAN порту.

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 protected-port	-	Переводит порт в режим изоляции внутри группы портов.
no switchport-protected-port		Восстанавливает значение по умолчанию.
switchport community *community*	community: (1..30)	Добавляет порт в сообщество (группа изоляции портов). Порты внутри сообщества могут обмениваться трафиком только между собой, а также с другими незащищенными портами (на которых нет настройки **switchport protected-port**) - *community* – имя сообщества.
no switchport community		Восстанавливает значение по умолчанию. В этом случае защищенный порт является изолированным портом (не состоящим ни в одном сообществе), и он может обмениваться трафиком только с незащищенными портами (на которых нет настройки **switchport protected-port**).
switchport protected {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12); По умолчанию используется маршрутизация по базе данных изученных MAC-адресов (FDB)	Переводит порт в режим Private VLAN Edge. Отменяет маршрутизацию по базе данных изученных MAC-адресов (FDB) и направляет весь одноадресный, многоадресный и широковещательный трафик на uplink-порт.
no switchport protected		Отключает отмену маршрутизации по базе данных изученных MAC-адресов (FDB).
ip internal-usage-vlan *vlan_id*	vlan_id: (1..4094)/ нет резерва	Зарезервировать VLAN для внутреннего использования на интерфейсе. - *vlan_id* – идентификационный номер VLAN.
no ip internal-usage-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.

Таблица 5.37 – Основные зарезервированные номера протоколов

Номер протокола	***Описание***
0x0800	Internet Protocol Version 4 (IPv4)
0x0806	Address Resolution Protocol (ARP)
0x86DD	Internet Protocol Version 6 (IPv6)
0x8808	Ethernet flow control
0x8809	Slow Protocols (IEEE 802.3)
0x8847	MPLS unicast
0x8848	MPLS multicast
0x8863	PPPoE Discovery stage
0x8864	PPPoE Session Stage
0x8870	Jumbo Frames
0x888E	EAP over LAN (IEEE 802.1X)
0x88CC	LLDP
0x8902	IEEE 802.1ag CFM / Y.1731 OAM

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

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

Таблица 5.38 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
vlan database	-	Вход в режим конфигурирования VLAN.
default interface {vlan *vlan_id* **| range vlan** *vlan_list* **}**	vlan_id: (1..4094); vlan_list: (1..4094)	Сброс настроек интерфейса VLAN или диапазона интерфейсов VLAN на настройки по умолчанию. - *vlan_id* – идентификационный номер VLAN; - *vlan_list* – список VLAN ID. Диапазон VLAN можно задать перечислением через запятую или указать начальное и конечное значения диапазона через дефис "-".
vlan statistics ingress low	-/disable	Включение счётчиков входящего трафика для VLAN 1..2047
no vlan statistics ingress low		Отключение счётчиков входящего трафика для VLAN 1..2047.
vlan statistics ingress high	-/disable	Включение счётчиков входящего трафика для VLAN 2048..4094.
no vlan statistics ingress high		Отключение счётчиков входящего трафика для VLAN 2048..4094.
vlan statistics egress low	-/disable	Включение счётчиков исходящего трафика для VLAN 1..2047 (только для режима standalone).
no vlan statistics egress low		Отключение счётчиков исходящего трафика для VLAN 1..2047 (только для режима standalone).
vlan statistics egress high	-/disable	Включение счётчиков исходящего трафика для VLAN 2048..4094 (только для режима standalone).
no vlan statistics egress high		Отключение счётчиков исходящего трафика для VLAN 2048..4094 (только для режима standalone).

Счётчики разбиты на 4 блока:
Ingress 1..2047
Ingress 2048..4094
Egress 1..2047
Egress 2048..4094

Одновременно можно включить не более двух блоков .Если включен режим qos statistics (qos statistics interface), то только один.

На каждый VLAN в одном направлении (rx или tx) только 2 счётчика: фреймы и пакеты, без разделения на мультикастные/юникастные/бродкастные.

Пример использования команды:

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

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 5.39 – Команды режима Privileged EXEC

Команда	*Значение*	*Действие*
show vlan	-	Показать информацию по всем VLAN.
show vlan name *name*	1..32 символов	Показать информацию по VLAN, поиск по имени.

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.
show default-vlan-membership [**gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* | **port-channel** *group* **]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Показать состав группы дефолтной VLAN.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 5.40 – Команды режима EXEC

Команда	***Значение***	***Действие***
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 counters vlan *vlan_id*	vlan_id: (1..4094)	Показать статистику для VLAN.
show interfaces switchport {gigabitethernet *gi_port* **|** **tengigabitethernet** *te_port* | **port-channel** *group***}**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Показать конфигурацию порта, группы портов.
show interfaces protected-ports [gigabitethernet *gi_port* **|** **tengigabitethernet** *te_port* | **port-channel** *group***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Показать состояние портов: в режиме Private VLAN Edge, в private-vlan-edge-сообществе.

Примеры выполнения команд

- Показать информацию о всех VLAN:

```
console# show vlan
```

```
Vlan mode: Basic

Vlan   Name        Tagged ports        Untagged ports          Type      Authorization----------------------
-----

 1       -                          gi1/0/4-24,te1/0/1-4,Po1-12     Default     Required
 5     test1       gi1/0/16-18          gi1/0/1-3                 permanent   Required
 6     test2       gi1/0/16-18          -                         permanent   Required
 7       -         gi1/0/16-18          -                         permanent   Required
```

- Показать порты источники и приемники многоадресного трафика в VLAN 4:

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

```
Source ports  : gi0/1
Receiver ports: gi0/2,gi0/4,gi0/8
```

- 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 информацию о группах подсетей:

console# **show vlan subnets-groups**

```
Ip Subnet Address    Mask          Group Id
----------------- -----------   -------------
192.168.16.44     255.255.255.0       1
192.168.16.44     255.255.255.0       2
```

- Показать список VLAN для внутреннего использования коммутатором:

console# **show vlan internal usage**

```
Usage   VLAN   Reserved   IP address
------ ------ ---------- ------------
gi0/22    9       Yes       Inactive
```

- **Показать статистику по VLAN 103**

console>**show interfaces counters vlan** 103

```
Vlan    InPkts       InOctets       OutPkts      OutOctets
---- ------------- ------------- ------------- -------------
 103             -             -            23          1612
```

- **Показать статистику по интерфейсам при включенных счетчиках трафика для VLAN**

console>**show interfaces counters**

```
      Port       InUcastPkts  InMcastPkts  InBcastPkts    InOctets
---------------- ------------ ------------ ------------ ------------
    gi1/0/1           0            0            0            0
    gi1/0/2           0            0            0            0
…………………………………………………………………………………………………………………………………………………………………………………………………………
    gi1/0/12          16           14          636         213840
…………………………………………………………………………………………………………………………………………………………………………………………
    gi1/0/23          0           337           0           57884
    gi1/0/24          0            0            0            0
    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
       Ch         InUcastPkts  InMcastPkts  InBcastPkts    InOctets
---------------- ------------ ------------ ------------ ------------
      Po1             0            0            0            0
      Po2             0            0            0            0
      Po3             0            0            0            0
      Po4             0            0            0            0
      Po5             0            0            0            0
      Po6             0            0            0            0
      Po7             0            0            0            0
      Po8             0            0            0            0
      Po9             0            0            0            0
      Po10            0            0            0            0
      Po11            0            0            0            0
      Po12            0            0            0            0

       Ch        OutUcastPkts OutMcastPkts OutBcastPkts  OutOctets
---------------- ------------ ------------ ------------ ------------
      Po1             0            0            0            0
      Po2             0            0            0            0
      Po3             0            0            0            0
```

```
      Po4             0            0            0            0
      Po5             0            0            0            0
      Po6             0            0            0            0
      Po7             0            0            0            0
      Po8             0            0            0            0
      Po9             0            0            0            0
      Po10            0            0            0            0
      Po11            0            0            0            0
      Po12            0            0            0            0

Vlan    InPkts       InOctets       OutPkts      OutOctets
---- ------------- ------------- ------------- -------------
   1             -             -          1102        362938
   5             -             -             0             0
  50             -             -             0             0
 100             -             -             0             0
 101             -             -             0             0
 102             -             -             0             0
 103             -             -            24          1684
 104             -             -             0             0
 105             -             -             0             0
 106             -             -             0             0
 107             -             -             0             0
 108             -             -             0             0
 122             -             -             0             0
```

- Показать конфигурацию порта GigabitEthernet 22:

console# **show interfaces switchport gigabitethernet** 1/0/22

```
Port : gi0/22
Port Mode: Access
Gvrp Status: disabled
Ingress Filtering: true
Acceptable Frame Type: admitAll
Ingress UnTagged VLAN ( NATIVE ): 1
Protected: Disabled
 Port is member in:

Vlan               Name                Egress rule Port Membership Type
---- -------------------------------- ----------- --------------------
 1                  1                   Untagged          System

Forbidden VLANS:
Vlan               Name
---- --------------------------------

Classification rules:
 Protocol based VLANs:
Group ID Vlan ID
-------- -------
Subnet based VLANs:
Group ID Vlan ID
```

5.8.3 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 23.

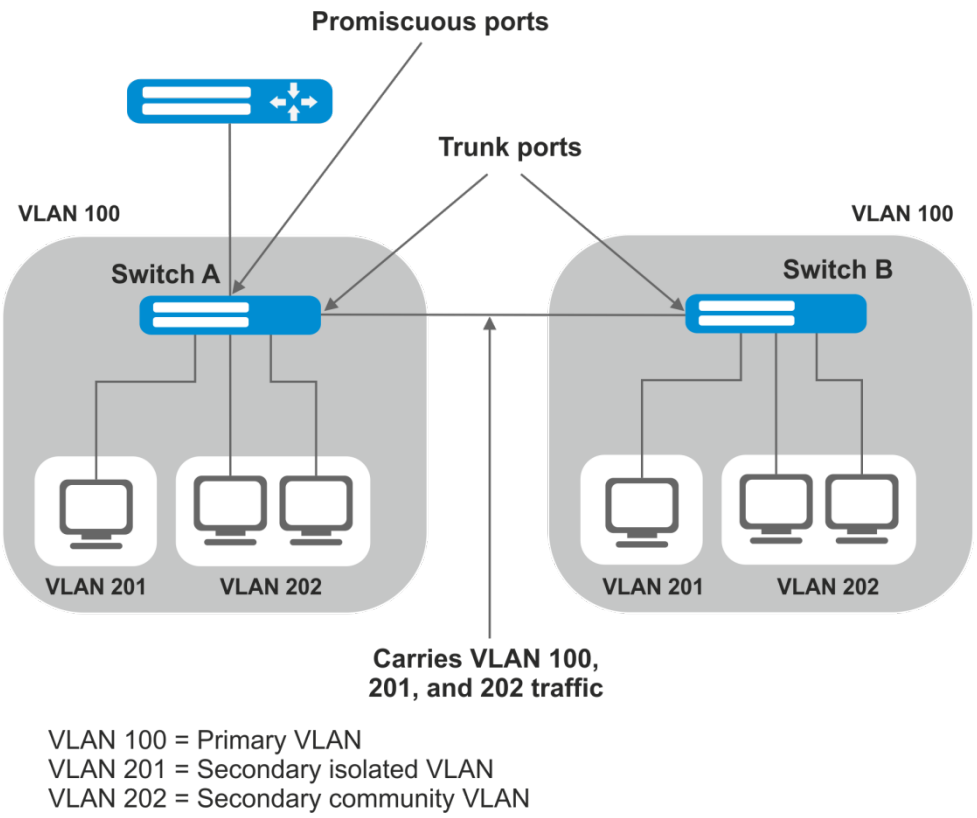


Рисунок 23 – Пример работы технологии Private VLAN

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

```
console# configure
console(config)# interface {tengigabitethernet te_port | gigabitethernet
gi_port |port-channel group | range {…}| vlan vlan_id}
console(config-if)#
```

Таблица 5.41 - Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
switchport mode *mode*	mode: (promiscuous, host)	Задать режим работы порта в VLAN. - *mode* – режим работы порта в VLAN.
no switchport mode		Установить значение по умолчанию.

switchport private-vlan mapping *primary_vlan* **[add | remove** *secondary_vlan]*	primary_vlan: (1..4094); secondary_vlan: (1..4094)	Добавить (удалить) основную и второстепенные VLAN на promiscuous интерфейс . **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 . **На один host интерфейс нельзя добавить больше одного secondary vlan.**
no switchport private-vlan host-association		Удалить основную и второстепенные VLAN.

Таблица 5.42 – Команды режима конфигурирования 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 SW1 (рис.23)

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 host
 description Isolate
 switchport forbidden default-vlan
 switchport private-vlan host-association 100 201
exit
!
interface gigabitethernet 1/0/2
 switchport mode host
 description Community-1
 switchport forbidden default-vlan
 switchport private-vlan host-association 100 202
exit
!
interface gigabitethernet 1/0/3
 switchport mode host
 description Community-2
 switchport forbidden default-vlan
 switchport private-vlan host-association 100 202
exit
!
interface gigabitethernet 1/0/4
 switchport mode 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
 private-vlan community
exit
```

5.8.4 Настройка интерфейса IP

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

Вид запроса командной строки в режиме конфигурирования интерфейса IP.

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

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

Таблица 5.43 – Команды режима конфигурирования интерфейса IP

Команда	*Значение/Значение по умолчанию*	*Действие*
broadcast-address *{255.255.255.255 | 0.0.0.0}*	/255.255.255.255	Назначает шировещательный адрес для интерфейса.
no broadcast-address		Восстанавливает значение по умолчанию.
directed-broadcast	-/disabled	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.
source-precedence	-/disabled	Назначает текущий IP-интерфейс предпочтительным для использования его функцией DHCP Relay. IP-адрес интерфейса будет использован в качестве адреса источника сообщений DHCP Relay. Если на интерфейсе коммутатора создано несколько IP-интерфейсов, то для работы DHCP Relay будет выбран интерфейс с признаком предпочтения (если такой имеется) и наименьшим IP-адресом.
no source-precedence		Отменяет настройку предпочтения.
ip irdp	-/enabled	Разрешает рассылку анонсов протокола IRDP (ICMP Router Discovery Protocol)
no ip irdp		Отключает рассылку анонсов.

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 Selective Q-in-Q

Данная функция 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 прохождения трафика.

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

Наличие хотя бы одного правила Selective Q-in-Q на интерфейсе запрещает включение функции логирования широковещательного шторма на этом интерфейсе.

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

Вид запроса командной строки режима конфигурирования интерфейса конфигурирования:

```
console# configure
console(config)# interface { gigabitethernet gi_port |
tengigabitethernet te_port | port-channel group | range {…}}
console(config-if)#
```

Таблица 5.44 – Команды режима конфигурирования интерфейса (диапазона интерфейсов) Ethernet

Команда	*Значение*	*Действие*
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.
selective-qinq list egress override_vlan *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

[ingress_vlan *ingress_vlan_id***]**		vlan_id. Если *ingress_vlan_id* не указывать – правило будет применяться как правило по умолчанию.
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.
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 5.45 – Команды режима EXEC

Команда	***Значение***	***Действие***
show selective-qinq	-	Отображает список правил selective qinq.
show selective-qinq interface {**gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group* }	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group:(1..12)	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 gigabitethernet 1/0/1
console(config-if)# selective-qinq list ingress override vlan 10
ingress-vlan 11
console(config-if)# end
```

- Отобразить список созданных правил selective qinq:

```
console# show selective-qinq
```

```
Direction Interface Rule type       Vlan ID   Classification     by Parameter
--------- --------- --------------- -------- ---------------- ------------------
ingress   gi0/1     override_vlan   10       ingress_vlan     11
```

5.10 Контроль широковещательного «шторма»

Широковещательный «шторм» возникает вследствие чрезмерного количества широковещательных 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 конфигурирования интерфейса Ethernet

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

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

Таблица 5.46 – Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
storm-control include-multicast	- / функция выключена	Добавляет контроль многоадресного трафика к контролю широковещательного.
no storm-control include-multicast		Выключает контроль многоадресного трафика.
storm-control include-unknown-unicast	- / функция выключена	Добавляет контроль неизвестного одноадресного трафика к контролю широковещательного.
no storm-control include-unknown-unicast		Выключает контроль неизвестного одноадресного трафика.
storm-control include-multicast unknown-unicast	- / функция выключена	Добавляет контроль многоадресного и неизвестного одноадресного трафика к контролю широковещательного.
no storm-control include-multicast unknown-unicast		Выключает контроль многоадресного и неизвестного одноадресного трафика трафика.
storm-control broadcast enable	- / функция выключена	Включает контроль широковещательного трафика.
no storm-control broadcast enable		Выключает контроль широковещательного трафика.
storm-control broadcast logging	- /функция выключена	Включает логирование широковещательного шторма. Логирование многоадресного и одноадресного трафика не осуществляется. **Включение логирования шторма запрещает конфигурирование правил SQinQ на этом интерфейсе.**
no storm-control broadcast logging		Выключает логирование широковещательного шторма.
storm-control broadcast shutdown	- /функция выключена	**Отключает интерфейс при обнаружении широковещательного шторма.** **Функция выключения интерфейса при обнаружении шторма запрещает конфигурирование правил SQinQ на этом интерфейсе.**
no storm-control broadcast shutdown		**Устанавливает значение по умолчанию.**
storm-control broadcast level kbps *rate*	rate: (1..1000000)/ 3500 Кбит/с	Задает максимальную скорость для широковещательного, многоадресного и неизвестного одноадресного трафика.
no port storm-control broadcast level		Устанавливает значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.47 – Команды режима EXEC

Команда	*Значение*	*Действие*
show storm-control [**gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port*]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4)	Показывает конфигурацию функции контроля широковещательного «шторма» для указанного порта, либо всех портов.

Примеры выполнения команд

Включить контроль широковещательного, многоадресного и неизвестного одноадресного трафика на 15 интерфейсе Ethernet. Установить максимальную скорость для контролируемого трафика – 5000 Кб/с:

```
console# configure
console(config)# interface gigabitethernet 1/0/15
console(config-if)# storm-control broadcast enable
console(config-if)# storm-control include-multicast
console(config-if)# storm-control include-multicast unknown-unicast
console(config-if)# storm-control broadcast level kbps 5000
```

5.11 Группы агрегации каналов – Link Agregation Group (LAG)

Коммутаторы MES3000 обеспечивает поддержку до двенадцати интерфейсов Ethernet в одной группе портов LAG и до восьми групп LAG на устройстве или стеке устройств. 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 конфигурирования интерфейса Ethernet.

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet:

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

Таблица 5.48 – Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение*	*Действие*
channel-group *group* **mode** *mode*	group (1..12) mode (on, passive, auto)	Добавить ethernet-интерфейс в группу портов. - *on* – добавить порт в канал без LACP; - *passive* - добавить порт в канал с LACP в режиме «passive»; - *auto* – добавить порт в канал с LACP в режиме «active».
no channel-group		Удалить Ethernet-интерфейс из группы портов.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

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

Таблица 5.49 – Команды режима глобального конфигурирования

Команда	*Значение*	*Действие*
port-channel load-balance {srcdst-mac-ip |	-/src-dst-mac	Задает механизм балансировки нагрузки для группы агрегированных портов.

src-dst-mac | src-dst-ip | src-dst-mac-ip-port | dst-mac | dst-ip | srcmac | srcip} [mpls-aware]		- **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 порте назначения; - **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. Опциональный параметр, актуален только с режимами балансировки по L3/L4-заголовкам пакета.

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 5.50 – Команды режима EXEC

Команда	*Значение*	*Действие*
show interfaces channel-group [group**]**	group: (1..12)	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 конфигурирования 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 конфигурирования соответствующего интерфейса.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

console(config)#

Таблица 5.51 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
lacp system-priority *value*	value: (1..65535/1)	Устанавливает приоритет системы.
no lacp system-priority		Устанавливает значение по умолчанию.

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet:

console(config-if)#

Таблица 5.52 – Команды режима конфигурирования 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 5.53 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show lacp **{ gigabitethernet** *gi_port* **| tengigabitethernet** *te_port***}** **[parameters | statistics | protocol-state]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4);	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..12)	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 1000
console(config-if)# exit
console(config)# interface gigabitethernet 1/0/3
console(config-if)# speed 1000
console(config-if)# channel-group 1 mode auto
console(config-if)# lacp port-priority 12
console(config-if)# exit
console(config)# interface gigabitethernet 1/0/4
console(config-if)# speed 1000
console(config-if)# channel-group 1 mode auto
```

```
console(config-if)# lacp port-priority 13
console(config-if)# exit
```

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 конфигурирования интерфейса Ethernet, интерфейса группы портов, VLAN

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

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

Таблица 5.54 – Команды режима конфигурирования интерфейса Ethernet

Команда	***Значение***	***Действие***
ip address *ip_address mask* [*gateway*| *prefix_length*]	prefix_length: (8 .. 30)	Назначение заданному интерфейсу IP-адреса, маски подсети и адреса шлюза по умолчанию.
no ip address [*ip_address*]		Удаление IP-адреса интерфейса.
ip address dhcp	(1..20) символов	Получение IP-адреса для настраиваемого интерфейса от DHCP-сервера.
no ip address dhcp		Запрет использования протокола DHCP для получения IP-адреса выбранным интерфейсом.
ip unnumbered vlan *vlan_id*	vlan_id: (1..4094)	Разрешает конфигурируемому интерфейсу заимствовать IP-адреса интерфейса VLAN *vlan_id*. Функция применима только для VLAN интерфейсов.
no ip unnumbered vlan		Отключает функцию заимствования адреса.

Команды режима глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

```
console(config)#
```

Таблица 5.55 - Команды режима глобального конфигурирования

Команда	***Значение***	***Действие***
ip default-gateway *ip_address*	-/шлюз по умолчанию не задан	Задает для коммутатора адрес шлюза по умолчанию.
no ip default-gateway		Удаляет назначенный адрес шлюза по умолчанию.
ip helper-address {*ip_interface* | **all**} *ip_address* [*udp_port_list*]	-/disabled	Включает переадресацию широковещательных UDP-пакетов на определенный адрес. - *ip_interface* – IP-адрес интерфейса, для которого выполняется настройка; - **all** – позволяет выбрать все IP-интерфейсы устройства; - *ip_address* – IP-адрес назначения, на который будут перенаправляться пакеты. Значение 0.0.0.0 отключает переадресацию; - *udp_port_list* – 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 {*ip_interface* | **all**} *ip_address*		Отменяет переадресацию на заданных интерфейсах.

ip unnumbered proxy-arp	-/disabled	Включает ретрансляцию сообщений протокола ARP между интерфейсами, которые используют технологию ip unnumbered.
no ip unnumbered proxy-arp		Отключает функцию ARP proxy.

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

console#

Таблица 5.56 - Команды режима Privileged EXEC

Команда	***Значение***	***Действие***
clear host dhcp {*name* **| *}**	(1..158) символов	Удаляет из памяти полученные по протоколу DHCP записи соответствий имен интерфейсов и их IP-адресов. * - удалить все соответствия.
renew dhcp {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***| vlan** *vlan_id***} [force-autoconfig]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12); vlan_id: (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 [*ip_interface* **]**	-	Отображает таблицу переадресации широковещательных UDP-пакетов.

Команды режима EXEC

Вид запроса командной строки в режиме Exec:

console>

Таблица 5.57 - Команды режима EXEC

Команда	***Значение***	***Действие***
show ip interface [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***| vlan** *vlan_id***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12); vlan_id: (1..4094)	Показывает конфигурацию IP-адресации для указанного интерфейса.

Примеры выполнения команд

- Установить IP-адрес шлюза по умолчанию - 192.168.16.2:

console (config)# **ip default-gateway** 192.168.16.2

- Использовать технологию IP unnumbered (позволяет сократить количество используемых IP адресов)

console (config)# **interface vlan** 100
console (config)# **ip address** 100.0.0.1 /24
console (config)# **interface vlan** 1001
console (config)# **ip unnumbered vlan** 100
console (config)# **interface vlan** 1002
console (config)# **ip unnumbered vlan** 100

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 глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

```
console(config)#
```

Таблица 5.58 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
green-ethernet energy-detect	-/включен	Включает энергосберегающий режим для неактивных портов.
no green-ethernet energy-detect		Отключает энергосберегающий режим для неактивных портов.
green-ethernet short-reach	-/включен	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.
green-ethernet short-reach threshold *value*	value: (0..70/40) метров	Устанавливает пороговое значение для энергосберегающего режима short-reach.
no green-ethernet short-reach threshold		Возвращает настройки по умолчанию.

Команды режима конфигурирования интерфейса

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet:

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

Таблица 5.59 – Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
green-ethernet energy-detect	-/ключен	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.
green-ethernet short-reach force	-/Отключен	Перманентно включает энергосберегающий режим для порта.
no green-ethernet short-reach force		Перманентно включает энергосберегающий режим для порта.

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 5.60 - Команды режима Privileged EXEC

Команда	*Значение*	*Действие*
show green-ethernet [gigabitethernet *gi_port* **| tengigabitethernet** *te_port***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4)	Отображает статистику green-ethernet.
green-ethernet power-meter reset	-	Сбрасывает счетчик измерителя мощности.

Примеры выполнения команд

- Отобразить статистику green-ethernet:

console# **show green-ethernet**

```
Energy-Detect mode: Enabled
Short-Reach mode: Enabled
Power Consumption: 83% (5.57W out of maximum 6.69W)
Cumulative Energy Saved: 0 [Watt*Hour]
Short-Reach cable length threshold: 10m

Port      Energy-Detect       Short-Reach           VCT Cable
       Admin Oper Reason   Admin Force Oper Reason   Length
----   ----- ---- -------  ----- ----- ---- -------  ------
gi0/1     on   off  LU        on   off   off  LL       < 50
gi0/2     on   off  LU        on   off   off  LL       < 50
gi0/3     on   off  LU        on   off   on            < 50
gi0/4     on   on             on   off   off  LD
…
gi0/22    on   off  LU        on   off   on            < 50
gi0/23    on   off  LU        on   off   off  LL       50 - 80
gi0/24    on   off  LU        on   off   off  LL       50 - 80
te0/1     on   off  LT        on   off   off  LT
te0/2     on   off  LT        on   off   off  LT
te0/3     on   off  LT        on   off   off  LT
te0/4     on   off  LT        on   off   off  LT
```

- *LU* – интерфейс находится в состоянии UP;
- *LD* – интерфейс находится в состоянии DOWN;
- *LL* – длина кабеля, подключенного к интерфейсу превышает пороговое значение;
- *LT* – интерфейс является оптическим.

5.14 Настройка IPv6-адресации

5.14.1 Протокол IPv6

Коммутаторы MES3000 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 = **gigabitethernet** (1..8/0/1..24)| **tengigabitethernet** (1..8/0/1..4)

Если значение группы или нескольких групп подряд в адресе протокола IPv6 равно нулю - 0000, то данные группы могут быть опущены. Например, адрес FE40:0000:0000:0000:0000:0000: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 глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.61 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
ipv6 default-gateway *ipv6_address*	-	Задает значение локального адреса IPv6-шлюза по умолчанию.
no ipv6 default-gateway		Удаляет настройки IPv6-шлюза по умолчанию
ipv6 host *name ipv6_address1* [*ipv6_address2... ipv6_address4*]	name: (1..158) символов	Создает статическую запись, ставящую в соответствие сетевому имени устройства IPv6-адрес.
no ipv6 host *name*		Удаляет статическую запись соответствия IPv6-адреса и сетевого имени устройства.
ipv6 neighbor *ipv6_address* { **gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **port-channel** *group*| **vlan** *vlan_id*} *mac_address*	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12); vlan_id: (1..4094)	Создает статическое соответствие между MAC-адресом соседнего устройства и его IPv6-адресом. - *ipv6_address* – IPv6-адрес; - *mac_address* – MAC-адрес.
no ipv6 neighbor		Удаляет статическое соответствие между MAC-адресом соседнего устройства и его IPv6-адресом.
ipv6 icmp error-interval *milliseconds* [*bucketsize*]	milliseconds: (0 .. 2147483647)/100 bucketsize: (1..200)/10	Задает ограничение скорости для ICMPv6 сообщений об ошибках.
no ipv6 icmp error-interval		Устанавливает значение по умолчанию.

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

Вид запроса командной строки режима конфигурирования интерфейса:

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

Таблица 5.62 – Команды режима конфигурирования интерфейса (Ethernet, VLAN, Port-channel)

Команда	*Значение/Значение по умолчанию*	*Действие*
ipv6 enable [no-autoconfig]	-	Включает поддержку IPv6 на интерфейсе.
no ipv6 enable		Отключает поддержку IPv6 на интерфейсе.
ipv6 address *ipv6_address/prefix_length* [**eui-64**] **[anycast]**	prefix-length: (3..128) (64 если используется параметр eui-64)	Задает IPv6-адрес на интерфейсе. - *ipv6_address* – IPv6-сеть, назначенная интерфейсу (8 блоков разделенных двоеточием, в каждом блоке 16 бит, записанных в виде четырех шестнадцатеричных чисел); - *prefix_length* – длина префикса IPv6 – десятичное число – количество старших бит адреса составляющих префикс; - **eui-64** – идентификатор, созданный на базе MAC-адреса интерфейса, записывается в 64 младших бита IPv6 адреса; - **anycast** – указывает, что заданный адрес anycast-адрес (до 64 интерфейсов IPv6) .
no ipv6 address [*ipv6_address/ prefix_length*] [**eui-64**]		Удаляет IPv6-адрес с интерфейса.
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 *ipv6_address/ prefix_length* **link-local**	По умолчанию значение локального адреса: (FE80::EUI64)	Задает локальный IPv6-адрес интерфейса. Старшие биты локальных IP-адресов в IPv6 – FE80::
no ipv6 address [*ipv6_address/prefix-length* **link-local]**		Удаляет локальный IPv6-адрес.
ipv6 nd dad attempts *attempts_number*	(0..600)/1	Задает количество сообщений-требований, передаваемых интерфейсом взаимодействующему устройству в случае обнаружения дубликации (коллизии) IPv6-адреса.
ipv6 unreachables	-/enabled	Включение ICMPv6 сообщений о недостижимости адресата при передаче пакетов на определенный интерфейс.
no ipv6 unreachables		Устанавливает значение по умолчанию.
ipv6 mld version {1 | 2}	(1,2)/2	Определение версии протокола MLD для интерфейса.
no ipv6 mld version		Устанавливает значение по умолчанию.
ipv6 mld join-group *group_address*	-	Задает MLD-сообщения для определенной группы. - *group-address* – IPv6-адрес группы многоадресной рассылки.
no ipv6 mld join-group *group_address*		Отменяет отчетность и удаляет IP-адрес из группы многоадресной рассылки.

Команды режима Privileged EXEC

Вид запроса командной строки режима PrivilegedEXEC:

console#

Таблица 5.63 – Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
ipv6 set mtu { gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group* **}** **{** *bytes* **| default}**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12) bytes: (1280 .. 65535) /1500	Задает значение MTU для IPV6 пакетов.
show ipv6 neighbors {**static** | **dynamic**} [**ipv6-address** *ipv6_address*]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12);	Показывает информацию о соседних IPv6 устройствах, содержащуюся в кэше. - **static** – показывает статические записи;

[**mac-address** *mac_address*] [**gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **|** **port-channel** *group* **|** **vlan** *vlan_id*]	vlan_id: (1..4094)	- **dynamic** – показывает динамические записи.
clear ipv6 neighbors	-	Очищает кэш, содержащий информацию о соседних устройствах, работающих по протоколу IPv6. Информация о статических записях сохраняется.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.64 – Команды режима EXEC

Команда	***Значение***	***Действие***
show ipv6 interface [**gigabitethernet** *gi_port* **|** **tengigabitethernet** *te_port* **|** **port-channel** *group* **|** **vlan** *vlan_id*]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12); vlan_id: (1..4094)	Показывает настройки протокола IPv6 для указанного интерфейса.
show ipv6 route	-	Показывает таблицу IPv6-маршрутов.
show ipv6 icmp error-interval	-	Показывает настройки ICMPv6 сообщений об ошибках.

Примеры выполнения команд

Показать динамические записи в таблице маршрутизации о соседних IPv6 устройствах.

```
console# show ipv6 neighbors dynamic
```

```
Interface      IPv6 address                      HW address   State        Router
---------      -----------------------------------    -----------------   -----
VLAN 1      5629:78:13::6782:B588:1AB5    00:00:03:08:D8:98  REACH
```

Возможные состояния:

- *INCMP (Incomplete)* – Процедура разрешения адреса выполняется на входе. Это означает, что запрос о соседстве был отправлен на групповой адрес, но соответствующее подтверждение о соседстве еще не было получено.
- *REACH (Reachable)* – Положительное подтверждение о том, что путь до соседнего устройства функционирует верно, было получено в течение периода «достижимости» (ReachableTime, мс). Пока соседнее устройство достижимо, и обмен пакетами идет нормально, никаких специальных действий не предпринимается.
- *STALE* – Положительное подтверждение о том, что путь до соседнего устройства функционирует верно, было получено в течение времени большего, чем период «достижимости» (ReachableTime, мс). Пока соседнее устройство достижимо, и обмен пакетами идет нормально, никаких специальных действий не предпринимается.
- *DELAY* – Положительное подтверждение о том, что путь до соседнего устройства функционирует верно, было получено в течение времени большего, чем период «достижимости» (ReachableTime, мс) и повторный запрос был передан в течение интервала времени отведенного на попытку (DELAY_FIRST_PROBE_TIME, сек). Если положительный ответ не придет в течение интервала времени, отведенного на попытку (DELAY_FIRST_PROBE_TIME, сек), то состояние пути до соседнего устройства изменится на PROBE.

– *PROBE* – Запросы о соседстве периодически передаются с интервалом «ретрансляции» (RetransTimer, мс) до тех пор, пока не будет получено положительное подтверждение.

5.14.2 Туннелирование протокола IPv6 (ISATAP)

Функция туннелирования трафика IPv6 на базе протокола ISATAP *(Intra-Site Automatic Tunnel Addressing Protocol)* позволяет осуществлять передачу трафика IPv6 через сети с адресацией IPv4. Таким образом, узлы с адресацией IPv6, поддерживающие туннелирование ISATAP, могут сообщаться, инкапсулируя трафик в пакеты с заголовком IPv4.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.65 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
interface tunnel *number*	1	1. Создает интерфейс туннелирования. 2. Осуществляет вход в режим конфигурирования интерфейса туннелирования.
tunnel isatap query-interval *seconds*	(10..3600)/10 сек	Устанавливает период между DNS запросами, отправляемыми для автоматического определения IP-адреса маршрутизатора ISATAP.
no tunnel isatap query-interval		Устанавливает значение по умолчанию.
tunnel isatap solicitation-interval *seconds*	(10..3600)/10 сек	Устанавливает период передачи запросов, требующих подтверждения от маршрутизатора ISATAP (в случае отсутствия активного маршрутизатора).
no tunnel isatap solicitation-interval		Устанавливает значение по умолчанию
tunnel isatap robustness *number*	(1..20)/3	Задает количество DNS-query запросов и количество запросов, передаваемых маршрутизатору ISATAP в течение времени жизни установленного соединения. Периоды запросов определяется формулами: - для DNS: (время жизни принятое в ответе от сервера DNS)/(number+1); - для запросов к маршрутизатору ISATAP: (минимальное время жизни принятое в ответе от ISATAP маршрутизатора)/(number+1).
no tunnel isatap robustness		Устанавливает значение по умолчанию.

Команды режима туннелирования

Вид запроса командной строки режима туннелирования:

```
console# configure
console(config)# interface tunnel 1
console (config-tunnel)#
```

Таблица 5.66 – Команды режима туннелирования

Команда	*Значение/Значение по умолчанию*	*Действие*
tunnel mode ipv6ip isatap	-/ туннелирование отключено	Включает поддержку туннелирования протокола IPv6 через IPv4 при помощи ISATAP. **Для одного и того же интерфейса (например Ethernet/VLAN) поддержка IPv6-адресации и туннелирования могут сосуществовать вместе. Выбор использования IPv6-адресации или**

		туннелирования будет осуществлен на основании информации об IP-адресе назначения.
no tunnel mode ipv6ip isatap		Выключает поддержку туннелирования протокола IPv6.
tunnel isatap router *router_name*	-/доменным именем является строка 'isatap'	Задаёт доменное имя для туннеля IPv6. Пользователи с адресацией IPv4 будут иметь возможность доступа к устройству (устройство туннелирования) при выполнении стандартной процедуры DNS.
no tunnel isatap router		Устанавливает значение по умолчанию
tunnel source { auto | ip-address *ipv4_address* **}**	-/IP-адрес не назначен	Команда назначает локальный IP-адрес туннелю, который будет использоваться, в качестве адреса источника, при отправке пакетов. - **auto –** IP-адрес будет автоматически назначен системой.
no tunnel source		Удаляет локальный IP-адрес туннеля.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.67 – Команды режима EXEC

Команда	*Действие*
show ipv6 tunnel	Показывает информацию о настройках туннеля.

Примеры выполнения команд

Включить интерфейс туннелирования, назначить доменное имя туннеля – ABCD, установить локальный ip-адрес – 192.168.16.88.

```
console# configure
console(config)# interface tunnel 1
console(config-tunnel)# tunnel mode ipv6ip isatap
console(config-tunnel)# tunnel isatap router ABCD
console(config-tunnel)# tunnel source ip-address 192.168.16.88
```

5.14.3 Настройка функции IPv6 RA guard

Функция IPv6 RA guard предоставляет защиту от атак, основанных на рассылке поддельных пакетов Router Advertisement, разрешая отсылку сообщений только с доверенных портов.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.68 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
ipv6 nd raguard	/Выключено	Разрешает коммутатору контролирование функции IPv6 RA guard.
no ipv6 nd raguard		Выключение функции IPv6 RA guard.
ipv6 nd raguard vlan *vlan*	(1..4094)	Разрешает контролирование функции IPv6 RA guard в пределах указанной VLAN. - *vlan* – номер VLAN.

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки режима конфигурирования интерфейса:

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

Таблица 5.69 – Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
ipv6 nd raguard device-role { host | router }	-/host	Выбор режима работы порта. - **host** – блокировка всех входящих RA-сообщений; - **router** – фильтрация RA-сообщений в соответствии с настроенными правилами.
ipv6 nd raguard match access-list *acl*	(1..32) символа	Включение ACL для фильтрации RA-сообщений в режиме router. - *acl* – имя ACL.
ipv6 nd raguard match prefix-list *prefix_list*	(1..32) символа	Включение prefix-list для фильтрации RA-сообщений в режиме router. - *prefix_list* – имя prefix-list.
ipv6 nd raguard trusted-port	По умолчанию все порты являются untrusted	Добавляет порт в список доверенных.

5.14.4 Настройка функции DHCPv6 guard

DHCPv6 guard – функция, позволяющая предотвращать появление сторонних DHCPv6-серверов в сети, разрешая их использование только на доверенных интерфейсах.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.70 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
ipv6 dhcp guard	/Выключено	Разрешает коммутатору контролирование функции DHCPv6 guard.
no ipv6 dhcp guard		Выключение функции DHCPv6 guard.
ipv6 dhcp guard vlan *vlan*	(1..4094)	Разрешает контролирование функции DHCPv6 guard в пределах указанной VLAN. - *vlan* – номер VLAN.

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки режима конфигурирования интерфейса:

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

Таблица 5.71 – Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
ipv6 dhcp guard device-role { client | server }	-/client	Выбор режима работы порта: - **client** – сообщения типа «advertise» и «relpy» отбрасываются; - **server** – сообщения типа «advertise» и «reply» фильтруются по установленным правилам.
ipv6 dhcp guard match server accsess-list *acl*	(1..32) символа	Включение ACL для фильтрации DHCPv6-сообщений. - *acl* – имя ACL.

ipv6 dhcp guard match reply prefix-list *prefix-list*	(1..32) символа	Включение prefix-list для фильтрации DHCPv6-сообщений. - *prefix-list* – имя prefix-list.
ipv6 dhcp guard trusted-port	По умолчанию все порты являются untrusted	Добавляет порт в список доверенных. Для доверенных портов разрешены все типы сообщений.
no ipv6 dhcp guard trusted-port		Удаляет порт из списка доверенных.

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 глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

`console(config)#`

Таблица 5.72 - Команды режима глобального конфигурирования

Команда	***Действие***
ip domain lookup	Разрешает использование протокола DNS.
no ip domain lookup	Запрещает использование протокола DNS.
ip name-server *{server1_ipv4_address| server1_ipv6_address} [server-address2 … ..server-address8]*	Определяет IPv4/IPv6-адреса для доступных DNS-серверов. Можно определить IP-адреса для восьми серверов.
no ip name-server *[server-address1 … …. server-address8]*	Удаляет IP-адрес DNS-сервера из списка доступных.
ip domain name name	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. Имя должно содержать 1 до 158 символов.
no ip domain name	Удаляет доменное имя по умолчанию.
ip host *name address1 [address2 … address4]*	Определяет статические соответствия имен узлов сети IP-адресам, добавляет установленное соответствие в кэш. Функция локального DNS. Имя должно содержать от 1 до 158 символов. Можно определить до четырех IP-адресов.
no ip host *name*	Удаляет статические соответствия имен узлов сети IP-адресам. Имя должно содержать от 1 до 158 символов.

Команды режима EXEC

Вид запроса командной строки в режиме EXEC:

`console#`

Таблица 5.73 - Команды режима EXEC

Команда	***Действие***
clear host {*name*|**}**	Удаляет запись соответствия имени узла сети IP-адресу кэша либо все записи (*). Имя должно содержать от 1 до 158 символов.

show hosts [*name*]	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. Имя должно содержать от 1 до 158 символов.

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 глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

```
console(config)#
```

Таблица 5.74 - Команды режима глобального конфигурирования

Команда	***Значение/Значение по умолчанию***	***Действие***
arp *ip_address hw_ address* **[gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***| vlan** *vlan_id***]**	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; gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12); vlan_id: (1..4094)	Добавляет статическую запись соответствия IP и MAC-адресов в таблицу ARP для указанного в команде интерфейса. - *ip*_address – IP-адрес; - *hw_address* – MAC-адрес.
no arp **ip_address** *[gigabitethernet* **gi_port** *| tengigabitethernet* **te_port** *| port-channel* **group***| vlan* **vlan_id***]*		Удаляет статическую запись соответствия IP и MAC-адресов из таблицы ARP для указанного в команде интерфейса.
arp timeout *sec*	(1-40000000)/ 60000 сек	Настраивает время жизни динамических записей в таблице ARP (сек).
no arp timeout		Устанавливает значение по умолчанию.

Команды режима privileged EXEC

Вид запроса командной строки в режиме privileged EXEC:

```
console#
```

Таблица 5.75 - 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 [**ip-address** *ip_address* | **mac-address** *mac_addres* | **gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **port-channel** *group*]	формат *ip_address*: A.B.C.D формат *mac_address*: H.H.H или H:H:H:H:H:H или H-H-H-H-H-H; gi_port: {1..8/0/1..24); te_port: {1..8/0/1..4); group: (1..12).	Показывает записи ARP-таблицы: все записи, фильтр по IP-адресу; фильтр по MAC-адресу; фильтр по интерфейсу. - *ip_address* – IP-адрес; - *mac_address* – MAC-адрес; - *gi_port* – номер интерфейса Ethernet g1-g4; - *te_port* – номер интерфейса Ethernet XG1-XG4; - *group* – группа каналов.
show arp configuration	-	Показывает глобальную конфигурацию ARP и конфигурацию ARP для интерфейсов.
ip arp proxy disable	-/отключён	Отключает режим проксирования ARP-запросов для коммутатора.
no ip arp proxy disable		Включает режим проксирования ARP-запросов для коммутатора.

Команды режима конфигурирование интерфейса

Вид запроса командной строки в режиме interface configuration:

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

Таблица 5.76 - Команды режима interface configuration

Команда	***Значение/Значение по умолчанию***	***Действие***
ip proxy-arp	-/отключён	Включает режим проксирования ARP-запросов на настраиваемом интерфейсе.
no ip proxy-arp		Отключает режим проксирования ARP-запросов на настраиваемом интерфейсе.
arp timeout *sec*	(1-40000000)	Настраивает время жизни динамических записей в таблице ARP (сек) для настраиваемого интерфейса.
no arp timeout		Устанавливает значение по умолчанию (устанавливается глобально).

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 gigabitethernet
1/0/2
console(config)# exit
console# arp timeout 12000
```

▪ Показать содержимое ARP таблицы:

```
console# show arp
```

```
  VLAN    Interface     IP address        HW address          status
--------------------- --------------- ------------------- ---------------
vlan 1     gi0/12     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 глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.77 – Команды режима глобального конфигурирования

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

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

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

console# **configure**
console(config)# **interface** {**gigabitethernet** *gi_port*| **tengigabitethernet** *te_port*|**port-channel** *group*}
console(config-if)#

Таблица 5.78 – Команды режима конфигурирования 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.
garp timer {join | leave | leaveall} *timer_value*	(10-2147483640) мс Значения по умолчанию: join: 200 мс; leave: 600 мс; leaveall: 10000 мс	Устанавливает значения таймеров протокола GARP (описание таймеров приведено в таблице 5.79). - *timer_value* – значение таймера (должно быть кратно 10).
no garp timer		Установить значения по умолчанию.
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.

Таблица 5.79 – Описание таймеров GARP

Таймер GARP	*Значение*
Join Timer	Определяет интервал передачи запросов на присоединение в группу VLAN (диапазон значений от 10 до 2147483640 миллисекунд, значение по умолчанию – 200 миллисекунд).
Leave Timer	Определяет интервал, который интерфейс будет ожидать перед выходом из группы VLAN (диапазон значений от 10 до 2147483640 миллисекунд, значение по умолчанию – 600 миллисекунд). **Значение Leave таймера должно быть больше или равно трем значениям Join таймера.**
LeaveAll Timer	Определяет интервал, который интерфейс будет ожидать перед отправкой запроса LeaveAll на полное отключение от группы VLAN (диапазон значений от 10 до 2147483640 миллисекунд, значение по умолчанию – 10000

	миллисекунд). **Значение LeaveAll таймера должно быть намного больше значения Leave таймера.**

Значения GARP таймеров должно быть одинаковым для всех взаимодействующих устройств. Если значения таймеров будут отличаться, то коммутатор может некорректно работать по протоколу GVRP.

Взаимодействие нетегированного порта с тегированным может быть административно определено путем установки значения PVID на нетегированном порту.

Интерфейс, настроенный в режиме порта доступа (Access port), не может работать по протоколу GVRP, поскольку он всегда является членом только одной группы VLAN.

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 5.80 – Команды режима privileged EXEC

Команда	*Значение*	*Действие*
clear gvrp statistics [**gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **port-channel** *group*]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Очищает накопленную статистику протокола GVRP.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 5.81 – Команды режима EXEC

Команда	*Значение*	*Действие*
show gvrp configuration [**gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **port-channel** *group*]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12).	Показывает конфигурацию протокола GVRP для указанного интерфейса, либо для всех интерфейсов.
show gvrp statistics [**gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **port-channel** *group*]		Показывает накопленную статистику по протоколу GVRP для указанного интерфейса, либо для всех интерфейсов.
show gvrp error-statistics [**gigabitethernet** *gi_port* | **tengigabitethernet** *te_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 фрейма с адресом назначения, совпадающим с одним из MAC-адресов устройства.

Команды режима глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

console(config)#

Таблица 5.82 - Команды режима глобального конфигурирования

Команда	***Значение/Значение по умолчанию***	***Действие***
loopback-detection enable	-/disabled	Включает механизм обнаружения петель для коммутатора.
no loopback-detection enable		Восстанавливает значение по умолчанию.
loopback-detection interval *seconds*	(1-60)/30 секунд	Устанавливает интервал между loopback-фреймами. - *seconds* – интервал времени между LBD фреймами.
no loopback-detection interval		Восстанавливает значение по умолчанию
loopback-detection mode {src-mac-addr|base-mac-addr}	-	Устанавливает режим обнаружения петель: - **src-mac-addr –** определяет, что MAC-адрес назначения – MAC-адрес интерфейса; - **base-mac-addr –** определяет, что MAC-адрес назначения – MAC-адрес устройства.
loopback-detection vlan-based	- / disabled	Включает режим обнаружения петли во VLAN. При наличии петли во VLAN данная VLAN будет заблокирована на порту, на котором была обнаружена петля.
no loopback-detection vlan-based		Отключает режим обнаружения петли во VLAN.
loopback-detection vlan-based recovery-time *time*	(30-1000000) / disabled	Задает время в секундах, в течение которого VLAN на порту будет находиться в заблокированном состоянии.
no loopback-detection vlan-based recovery-time		VLAN на порту, в котором была обнаружена петля, не будет разблокирована автоматически.

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

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

console# **configure**
console(config)# **interface** {**gigabitethernet** *gi_port*| **tengigabitethernet** *te_port*|**port-channel** *group*}
console(config-if)#

Таблица 5.83 – Команды режима конфигурирования интерфейса Ethernet, группы интерфейсов

Команда	***Значение/Значение по умолчанию***	***Действие***
loopback-detection enable	-/disabled	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 5.84 – Команды режима EXEC

Команда	***Значение***	***Действие***
show loopback-detection [**gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group*]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12).	Отображает состояние механизма loopback-detection. - *gi_port* – номер интерфейса Ethernet g1-g24; - *te_port* – номер интерфейса Ethernet XG1-XG4; - *group* – группа каналов.

5.15.5 Семейство протоколов STP (STP, RSTP, MSTP)

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 конфигурирование 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.

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 глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.85 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
spanning-tree	-	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: - **stp** – IEEE 802.1D Spanning Tree Protocol; - **rstp** – IEEE 802.1W Rapid Spanning Tree Protocol; - **mstp** – IEEE 802.1S Multiple Spanning Tree Protocol.
no spanning-tree mode		Устанавливает значение по умолчанию.
spanning-tree forward-time *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*	(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	-	Разрешает защиту, выключающую любой интерфейс при приеме пакетов BPDU.
no spanning-tree loopback-guard		Запрещает защиту, выключающую интерфейс при приёме пакетов BPDU.
spanning-tree max-age *seconds*	(6..40)/20 сек	Устанавливает время жизни связующего дерева STP.
no spanning-tree max-age		Устанавливает значение по умолчанию.

spanning-tree priority	(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**}	-/short	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 | bridging}	-/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; - **bridging –** на интерфейсе с выключенным протоколом STP BPDU пакеты передаются.
no spanning-tree bpdu		Устанавливает значение по умолчанию.
spanning-tree process *id*	(1-31)/0	Команда создает отдельный процесс и переводит командный интерфейс в режим его конфигурирования.
no spanning-tree process *id*		Удаляет указанный процесс.

При задании STP параметров forward-time, hello-time, max-age необходимо выполнение условия:
2*(Forward-Delay - 1) >= Max-Age >= 2*(Hello-Time + 1).

Команды режима конфигурирования интерфейса Ethernet, интерфейса группы портов

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

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

Таблица 5.86 – Команды режима конфигурирования 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*	(1..200000000)/ см. таблицу 5.87	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, таблица 5.87.
spanning-tree port-priority	(0..240)/128	Устанавливает приоритет интерфейса в связующем дереве STP. **Значение приоритета должно быть кратно 16.**
no spanning-tree port-priority		Устанавливает значение по умолчанию.
spanning-tree portfast [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	-/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 bpduguard	-/защита выключена	Разрешает защиту, выключающую интерфейс при приёме пакетов BPDU.
no spanning-tree bpduguard		Запрещает защиту, выключающую интерфейс при приёме 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 –** разветвлённый.
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 binding-process *id*	(1-31)/0	Привязывает порт к указанному процессу. По умолчанию, все порты управляются нулевым процессом. - *id* – номер процесса.
no spanning-tree binding-process		Восстанавливает привязку порта по умолчанию

Таблица 5.87 – Ценность пути, установленная по умолчанию (spanning-tree cost)

Интерфейс	***Метод определения ценности пути***	
	Long	***Short***
Port-channel	20000	4
TenGigabit Ethernet (10000 Mbps)	2000	2
Gigabit Ethernet (1000 Mbps)	20000	4

Команды режима конфигурирования процесса

Вид запроса командной строки режима конфигурирования процесса:

```
console(config-mstp-process)#
```

Таблица 5.88 – Команды режима privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
spanning-tree forward-time *seconds*	(4..30)/15 сек.	Устанавливает для конфигурируемого процесса интервал времени (*seconds*), затрачиваемый на прослушивание и изучение состояний перед переключением в состояние коммутации.
no spanning-tree forward-time		Устанавливает значение по умолчанию.
spanning-tree hello-time *seconds*	(1..10)/2 сек.	Устанавливает интервал времени (*seconds*) между передачами широковещательных сообщений «Hello» к взаимодействующим коммутаторам.
no spanning-tree hello-time		Устанавливает значение по умолчанию.
spanning-tree max-age *seconds*	(6..40)/20 сек.	Устанавливает время жизни (*seconds*) связующего дерева STP.
no spanning-tree max-age		Устанавливает значение по умолчанию.
spanning-tree mst *instance_id* **priority** *priority*	instance_id: (1..4094); priority: (0..61440)/32768	Устанавливает значение приоритета коммутатора в выбранном экземпляре MST. - *instance_id* – экземпляр MST; - *priority* – приоритет коммутатора. **Значение приоритета должно быть кратно 4096.**

no spanning-tree mst *instance_id* **priority**		Устанавливает значение приоритета по умолчанию.

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

console#

Таблица 5.89 – Команды режима privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show spanning-tree [**process** *process_id*] [**gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group*]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12). process_id: (1..31)/0	Показывает конфигурацию протокола STP для выбранного процесса. - *process_id* – номер процесса.
show spanning-tree [detail] [active | blockedports] [**process** *process_id*]	process_id: (1..31)/0	Показывает подробную информацию о настройках протокола STP, информацию об активных или заблокированных портах. - *process_id* – номер процесса.
clear spanning-tree detected-protocols [**gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group*]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12).	Перезапускает процесс миграции протокола. Заново происходит пересчёт дерева STP.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

console#

Таблица 5.90 – Команды режима EXEC

Команда	***Значение***	***Действие***
show spanning-tree bpdu [**gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group*]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12).	Показывает режим обработки пакетов BPDU на интерфейсах.

5.15.5.2 Настройка протокола MSTP

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

console(config)#

Таблица 5.91 – Команды режима глобального конфигурирования

Команда	***Значение/Значение по умолчанию***	***Действие***
spanning-tree	-	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**}	-/short	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..4094); priority: (0..61440)/32768	Устанавливает приоритет для данного коммутатора перед остальными, использующими общий экземпляр MSTP.

		- *instance_id* – экземпляр MST; - *priority* – 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*	(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. - *hop_count* – максимальное количество транзитных участков для пакета BPDU.
no spanning-tree mst max-hops		Устанавливает значение по умолчанию.
spanning-tree mst configuration	-	Вход в режим конфигурирования протокола MSTP.

Команды режима конфигурирования протокола MSTP

Вид запроса командной строки в режиме конфигурирования протокола MSTP:

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

Таблица 5.92 – Команды режима конфигурирования протокола MSTP

Команда	***Значение/Значение по умолчанию***	***Действие***
instance *instance_id* **vlan** *vlan_range*	instance_id:(1..4094); vlan_range: (1..4094)	Создает соответствие между экземпляром протокола MSTP и группами VLAN. - *instance-id* – идентификатор экземпляра протокола MSTP; - *vlan-range* – номер группы VLAN.
no instance *instance_id* **vlan** *vlan_range*		Удаляет соответствие между экземпляром протокола MSTP и группами VLAN.
name *string*	(1..32) символа	Задает имя конфигурации MST. - *string* – имя конфигурации MST.
no name		Удаляет имя конфигурации MST.
revision *value*	(0..65535)/0	Задает номер ревизии конфигурации MST. - *value* – номер ревизии конфигурации MST.
no revision		Устанавливает значение по умолчанию (*value*).
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 конфигурирования интерфейса Ethernet, интерфейса группы портов

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

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

Таблица 5.93 – Команды режима конфигурирования 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* **port-priority** *priority*	instance_id: (1..4094); priority:(0..240)/128	Устанавливает приоритет интерфейса в экземпляре MSTP. - *instance-id* – идентификатор экземпляра протокола MSTP;

		- *priority* – приоритета коммутатора. **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..4094); 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, таблица 5.87.
spanning-tree port-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.

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

console#

Таблица 5.94 – Команды режима EXEC

Команда	***Значение***	***Действие***
show spanning-tree [**gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group*] [**instance** *instance_id*] [**process** *process_id*]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12); instance_id: (1..64); process_id: 0..31	Показывает конфигурацию протокола STP. - *instance_id* – идентификатор экземпляра протокола MSTP. - *process_id* – номер процесса.
show spanning-tree [detail] [active | blockedports] [**instance** *instance_id*] [**process** *process_id*]	instance_id: (1..4094) ; process_id: 0..31	Показывает подробную информацию о настройке протокола STP, информацию об активных или заблокированных портах. - **detail** – просмотр подробной информации; - **active** – просмотр информации об активных портах; - **blockedports** – просмотр информации о заблокированных портах; - *instance_id* – идентификатор экземпляра протокола MSTP. - *process_id* – номер процесса.
show spanning-tree mst-configuration	-	Показывает информацию о сконфигурированных экземплярах MSTP
clear spanning-tree detected-protocols [**gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group*]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12).	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 широковещательных 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:  long
Loopback guard:   Disabled



  Root ID    Priority    12288
             Address     a8:f9:4b:f1:1d:00
             This switch is the root
             Hello Time  5 sec  Max Age 38 sec  Forward Delay 20 sec

  Number of topology changes 3 last change occurred 00:00:10 ago
      from gi1/0/11
  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
--------- -------- -------- -------- ------ ---- -------- -----------------
 gi1/0/1  enabled   128.49  2000000   Dsbl  Dsbl    No            -
gi1/0/2   enabled   128.50  2000000   Frw   Desg    No       P2P (RSTP
 gi1/0/3  enabled   128.51  2000000   Dsbl  Dsbl    No            -
 gi1/0/4  enabled   128.52  2000000   Dsbl  Dsbl    No            -
 gi1/0/5  enabled   128.53  2000000   Dsbl  Dsbl    No            -
 gi1/0/6  enabled   128.54  2000000   Dsbl  Dsbl    No            -
 gi1/0/7  enabled   128.55  2000000   Dsbl  Dsbl    No            -
 gi1/0/8  enabled   128.56  2000000   Dsbl  Dsbl    No            -
 gi1/0/9  enabled   128.57  2000000   Dsbl  Dsbl    No            -
```

В MSTP информация о последней смене топологии выводится только с помощью команды show spanning-tree detail.

5.15.6 Настройка функции flex-link

Flex-link – функция резервирования, предназначенная для обеспечения надежности канала передачи данных. В связке flex-link могут находиться ethernet и port-channel интерфейсы. 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 5.95 – Команды режима конфигурирования интерфейса Ethernet, группы портов

Команда	*Значение/Значение по умолчанию*	*Действие*
flex-link backup { **tengigabitethernet** *te_port* | **gigabitethernet** *gi_port* | **port-channel** *port_channel}*	te_port: (1..8/0/1..4); gi_port: (1..8/0/1..24); port_channel (1..12)/-	Включает flex-link на интерфейсе и назначает выбранному интерфейсу роль backup-интерфейса в flex-link паре.
no flex-link backup { **tengigabitethernet** *te_port* | **gigabitethernet** *gi_port* | **port-channel** *port_channel}*		Выключает flex-link на интерфейсе и удаляет выбранный интерфейс из flex-link пары.

flex-link preemption mode [**forced | bandwidth| off**]	-/off	Задает 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 preemption mode		Возвращает значение по умолчанию.
flex-link preemption delay *delay*	delay: (1..300)/35	Задает время от перехода отключенного порта в состояние «up», по прошествии которого выполняется действие, установленное командой **flex-link preemption mode**. - delay – период времени, в секундах.
no flex-link preemption delay		Возвращает значение по умолчанию.

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

console#

Таблица 5.96 – Команды режима EXEC

Команда	***Значение***	***Действие***
show interfaces flex-link [detailed] { tengigabitethernet *te_port* **| gigabitethernet** *gi_port* **| port-channel** *port-channel* **}**	te_port: (1..8/0/1..4); gi_port: (1..8/0/1..24); port_channel: (1..12)	Показывает конфигурацию функции flex-link.

5.15.7 Протокол EAPS

Протокол EAPS (Ethernet Automatic 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 глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

console(config)#

Таблица 5.97 – Команды режима глобального конфигурирования

Команда	***Значение/Значение по умолчанию***	***Действие***
eaps	-	Разрешает работу протокола EAPS.
no eaps		Запрещает работу протокола EAPS.
eaps fail-timer *seconds*	seconds: (1..10)/3 сек.	Задает время отсутствия тестовых пакетов, по истечении которого будет зафиксирована авария кольца. - *seconds* – период времени, в секундах.
no eaps fail-timer		Устанавливает значение таймера по умолчанию.
eaps hello-timer *seconds*	seconds: (1..10)/1 сек.	Таймер периодичности отправки hello-пакетов. - *seconds* – период времени отправки hello-пакетов, в секундах.
no eaps hello-timer		Устанавливает значение таймера по умолчанию.
eaps domain *domain_id*	domain_id: (0..63)	Создание EAPS-региона с идентификатором *domain-id* и переход в режим конфигурирования региона.

no eaps domain *domain_id*		Удаление EAPS-региона с идентификатором *domain_id*.

Команды режима конфигурирования домена

Вид запроса командной строки в режиме конфигурирования домена:

`console(config-eaps-domain)#`

Таблица 5.98 – Команды режима конфигурирования EAPS домена

Команда	***Значение/Значение по умолчанию***	***Действие***
control-vlan *vlan_id*	vlan_id: (1..4093)	Идентификатор VLAN, используемой для управления EAPS. Кроме того, для работы протокола должна существовать следующая после управляющей VLAN (control-vlan +1), используемая для управления вторичными кольцами. Управляющая VLAN EAPS не должна использоваться для передачи любого иного трафика. - *vlan_id* – номер VLAN, управляющей EAPS.
no control-vlan		Отмена назначения VLAN.
ring *ring_id*	ring_id: (0..15)	Создание кольца с идентификатором *ring_id* и переход в режим конфигурирования кольца.
no ring *ring_id*		Удаление кольца с идентификатором *ring_id.*
set ring *ring_id* {**enable** | **disable**}	ring_id: (0..15)	Разрешение или запрет работы кольца с идентификатором *ring_id.*

Команды режима конфигурирования кольца

Вид запроса командной строки в режиме конфигурирования:

`console(config-eaps-domain-ring)#`

Таблица 5.99 – Команды режима конфигурирования EAPS кольца

Команда	***Значение/Значение по умолчанию***	***Действие***
primary-port {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* | **port-channel** *group* **}**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12).	Выбор первичного порта коммутатора, включенного в кольцо.
secondary-port {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* | **port-channel** *group* **}**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12).	Выбор вторичного порта коммутатора, включенного в кольцо.
role {master | transit} level *level-id*	level-id: 0..1	Выбор роли коммутатора в конфигурируемом домене и кольце. Возможные роли: - **master** – устройство является ведущим узлом; - **transit** – устройство является транзитным узлом; - **edge** – смежный узел, принадлежащий основному и вторичному кольцам; - **sub-edge** – вспомогательный смежный узел, принадлежащий основному и вторичному кольцам.
role {edge | sub-edge}	-	

Команды режима EXEC

Вид запроса командной строки режима EXEC:

`console#`

Таблица 5.100 – Команды режима EXEC

Команда	***Значение***	***Действие***
show eaps [domain *domain_id* **[ring** *ring_id* **]]**	domain_id: 0..63; ring_id: 1..15.	Запрос информации о состоянии доменов и колец EAPS. - *domain_id* – идентификатор домена EAPS; - *ring_id* – идентификатор кольца EAPS.

5.15.8 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 глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.101 – Команды режима глобального конфигурирования

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

Команды режима конфигурирования кольца

Вид запроса командной строки в режиме конфигурирования кольца:

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

Таблица 5.102 – Команды режима конфигурирования ERPS кольца

Команда	*Значение/Значение по умолчанию*	*Действие*
protected vlan add *vlan_list*	vlan_list:(2..4094, all)	Добавляет диапазон VLAN в список защищенных VLAN. - *vlan_list* – список VLAN. Диапазон VLAN можно задать перечислением через запятую или указать начальное и конечное значения диапазона через дефис "-".
protected vlan remove *vlan_list*	vlan_list:(2..4094, all)	Удаляет диапазон VLAN из списка защищенных VLAN. - *vlan_list* – список VLAN для удаления.
port {west | east} {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* | **port-channel** *group* **}**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12).	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 west порт; - **owner** – коммутатор будет являться владельцем RPL-порта; - **neighbor** – коммутатор будет являться соседом владельца RPL-порта.
no rpl		Удаление RPL-порта коммутатора.
level *level*	level: (0..7)/1	Настройка уровня сообщений R-APS. Необходимо для прохождения сообщений через CFM MEP. - *level* – уровень сообщений R-APS.
no level		Установка значения по умолчанию.
ring enable	-	Включение функционирования кольца.
no ring enable		Выключение функционирования кольца.
version *version*	version: (1..2)/2	Выбор режима совместимости с другими версиями протокола G.8032.

		- *version* – 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 *vlan_id* **[tc-propogation]**	vlan_id: (1..4094)	Указание подкольца для данного кольца. - **tc-propogation** – включает распространение TC в подкольце.
no sub-ring vlan		Удаление подкольца.
timer guard *value*	value:(10-2000) мс, кратное 10/500 мс	Установка таймера блокирующего устаревшие R-APS сообщения.
no timer guard		Установка значения по умолчанию.
timer holdoff *value*	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 флапинге 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 EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.103 – Команды режима EXEC

Команда	***Значение***	***Действие***
show erps [vlan *vlan_id***]**	vlan_id: (1..4094)	Запрос информации об общем состоянии ERPS или состоянии указанного кольца.

5.15.9 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 MES3000 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 глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.104 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
lldp run	enabled	Разрешает коммутатору использование протокола LLDP.
no lldp run		Запрещает коммутатору использование протокола LLDP.
lldp timer *seconds*	(5..32768)/30 сек	Определяет, как часто устройство будет отправлять обновление информации LLDP.
no lldp timer		Устанавливает значение по умолчанию.
lldp hold-multiplier *number*	(2..10)/4	Задает величину времени для принимающего устройства, в течение которого нужно удерживать принимаемые пакеты LLDP перед их сбросом. 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)
no lldp hold-multiplier		Устанавливает значение по умолчанию.
lldp reinit *seconds*	(1..10)/2 сек	Минимальное время, которое LLDP-порт будет ожидать перед повторной инициализацией LLDP.
no lldp reinit		Устанавливает значение по умолчанию.
lldp tx-delay *seconds*	(1..8192)/2 сек	Устанавливает задержку между последующими передачами пакетов LLDP, инициированными изменениями значений или статуса в локальных базах данных MIB LLDP. **Рекомендуется, чтобы данная задержка была меньше, чем значение 0.25* LLDP-Timer.**
no lldp tx-delay		Устанавливает значение по умолчанию.
lldp lldpdu **{filtering | flooding}**	*filtering*	Определяет режим обработки пакетов LLDP, когда протокол LLDP выключен на коммутаторе: - *filtering* – указывает, что LLDP-пакеты фильтруются, если протокол LLDP выключен на коммутаторе; - *flooding* – указывает, что LLDP-пакеты передаются, если протокол LLDP выключен на коммутаторе.
no lldp lldpdu		Устанавливает значение по умолчанию.
lldp med fast-start repeat-count *number*	(1..10)/3	Устанавливает число повторений PDU LLDP для быстрого запуска, определяемого посредством LLDP-MED.
no lldp med fast-start repeat-count		Устанавливает значение по умолчанию.
lldp med network-policy *number application* [**vlan** *vlan_id*] [**vlan-type** {**tagged** | **untagged**}] [**up** *priority*] [**dscp** *value*]	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).	Определяет правило для параметра network-policy (сетевая политика устройства). Данный параметр является опциональным для расширения протокола LLDP MED. - *number* – порядковый номер правила network policy; - *application* – главная функция, определенная для данного правила network policy. Используемые имена: voice, voice-signaling, guest-voice, guest-voice-signaling, softphone-voice, video-conferencing, streaming-video, video-signaling. - *vlan_id* – идентификатор VLAN для данного правила; - **tagged/ untagged** – определяет тегированной или нетегированной будет VLAN, используемая данным правилом. - *priority* – приоритет данного правила (используется на втором уровне модели OSI); - *value* – значение DSCP, используемое данным правилом.
no lldp med network-policy *number*		Удаляет созданное правило для параметра network-policy.
lldp med network-policy voice auto	/enabled	Передавать в сообщениях LLDP-MED параметры voice-vlan
no lldp med network-policy voice auto		Запрещает передачу параметров voice-vlan в LLDP-MED
lldp notifications interval	seconds: (5..3600)/5	Устанавливает максимальную скорость передачи

seconds		уведомлений LLDP. - *seconds* – период времени, в течение которого устройство может отправить не более одного уведомления.
no lldp notifications interval		Устанавливает значение по умолчанию.

Команды режима конфигурирования интерфейсов Ethernet:

Вид запроса командной строки в режиме конфигурирования интерфейсов Ethernet:

`console(config-if)#`

Таблица 5.105 – Команды режима конфигурирования 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*	port-desc, sys-name, sys-desc, sys-cap, 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size По умолчанию опциональные TLV не включены в пакет.	Определяет, какие опциональные TLV-поля (Type, Length, Value) будут включены устройством в передаваемый LLDP-пакет. В команду можно включить от одного до пяти опциональных TLV: port-desc, sys-name, sys-desc, sys-cap, 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size.
no lldp optional-tlv		Устанавливает значение по умолчанию.
lldp optional-tlv 802.1 {pvid [enable|disable] |ppvid {add|remove} *ppv_id* **| vlan-name {add|remove}** *vlan_id***}**	ppvid: (0-4094); vlan_id: (1-4094); По умолчанию опциональные TLV не включены.	Определяет, какие опциональные TLV-поля будут включены устройством в передаваемый LLDP-пакет: - **pvid** – PVID интерфейса; - **ppvid** – добавить/удалить PPVID; - **vlan-name** – добавить/удалить номер VLAN; - **protocol** – добавить/удалить определенный протокол.
lldp optional-tlv 802.1 protocol {add|remove} {stp | rstp | mstp | pause | 802.1x | lacp | gvrp}		
no lldp optional-tlv 802.1 pvid		Устанавливает значение по умолчанию.
lldp management-address {*ip_address* **| none | automatic [gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***| vlan** *vlan_id***] }**	формат ip-address: A.B.C.D gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12); vlan_id: (1 .. 4094) По умолчанию управляющий адрес определяется автоматически.	Определяет управляющий адрес, объявленный на интерфейсе. - *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** *{gigabitethernet|tengigabitethernet|port-channel|vlan}* – указывает, что система автоматически выбирает управляющий адрес, из сконфигурированных адресов заданного интерфейса. Если интерфейс ethernet или интерфейс группы портов принадлежат VLAN, то данный адрес VLAN не будет включен в список возможных управляющих адресов. **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.**
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. - **enable** – разрешает; - **disable** – запрещает.
no lldp notifications		Устанавливает значение по умолчанию.
lldp med enable [*tlv_list*]	network-policy, location, poe-pse, inventory/	Разрешает использование расширения протокола LLDP MED.

	запрещено использование расширения протокола LLDP MED.	В команду можно включить от одного до четырёх специальных TLV: network-policy, location, poe-pse, inventory.
no lldp med enable		Устанавливает значение по умолчанию.
lldp med network-policy {add|remove} *number*	number: (1-32)	Назначает правило network-policy данному интерфейсу. - **add** – назначает правило; - **remove** – удаляет правило; - *number* – номер правила.
no lldp med network-policy *number*		Удаляет правило network-policy с данного интерфейса.
lldp med location {coordinate *coordinate*| **civic-address** *civic_address_data* | **ecs-elin** *ecs_elin_data***}**	coordinate: 16 байт; civic_address_data: (6..160) байт; ecs_elin_data: (10 – 25) байт.	Задает местоположение устройства для протокола LLDP (значение параметра location протокола LLDP MED). - *coordinate* – адрес в системе координат; - *civic_address_data* – административный адрес устройства; - *ecs-elin_data* – адрес в формате, определенном ANSI/TIA 1057.
no lldp med location		Удаляет настройки параметра местоположения location.
lldp med notification topology-change {enable | disable}	-	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

Все команды доступны для привилегированного пользователя.

Вид запроса командной строки режима privileged EXEC:

console#

Таблица 5.106 – Команды режима privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
clear lldp table	-	Очищает таблицу адресов обнаруженных соседних устройств и начинает новый цикл обмена пакетами по протоколу LLDP MED.
show lldp configuration [gigabitethernet *gi_port* **| tengigabitethernet** *te_port***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Показывает LLDP конфигурации всех физических интерфейсов устройства, либо заданных интерфейсов.
show lldp med configuration [gigabitethernet *gi_port* **| tengigabitethernet** *te_port***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Показывает конфигурации расширения протокола LLDP - MED для всех физических интерфейсов, либо заданных интерфейсов.
show lldp local {gigabitethernet *gi_port* **| tengigabitethernet** *te_port***}**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Показывает LLDP-информацию, которую анонсирует данный порт.
show lldp local tlvs-overloading [gigabitethernet *gi_port* **| tengigabitethernet** *te_port***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Показывает статус перезагрузки TLVs LLDP.
show lldp neighbors [gigabitethernet *gi_port* **| tengigabitethernet** *te_port***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Показывает информацию о соседних устройствах, на которых работает протокол LLDP.

show lldp statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Показывает статистику LLDP.

Примеры выполнения команд

Установить для порта g1 следующие tlv-поля: port-description, sytem-name, system-description. Для данного интерфейса добавить управляющий адрес 192.168.17.55

```
console(config)# configure
console(config-if)# lldp optional-tlv port-desc sys-name sys-desc
console(config-if)# lldp management-address 192.168.17.55
```

Посмотреть конфигурацию lldp:

```
console# show lldp configuration
```

```
LLDP state: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
   Port         State            Optional TLVs           Address
---------- --------------- ------------------------ ---------------
gi0/1          Rx and Tx            PD, SN, SD         192.168.16.55
gi0/2          Rx and Tx
…
gi0/22         Rx and Tx
More: <space>,  Quit: q, One line: <return>
```

Таблица 5.107 - 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-фреймов, 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
---------      ----------------  -------- ----------    -------------
gi0/1          0060.704C.73FE      1      ts-7800-2           B
gi0/2          0060.704C.73FD      1      ts-7800-2          B
gi0/3          0060.704C.73FC      9      ts-7900-1          B, R
gi0/4          0060.704C.73FB      1      ts-7900-2           W

show lldp neighbors gigabitethernet 1/0/20

Device ID: 02:10:11:12:13:00
Port ID: gi0/23
Capabilities: B
System Name: sandbox2
System description: 24-port 10/100/1000 Ethernet Switch
Port description: Ethernet Interface
Time To Live: 112

802.3 MAC/PHY Configuration/Status
Auto-negotiation support: Supported
Auto-negotiation status: Enabled
Auto-negotiation Advertised Capabilities: 1000BASE-T full duplex, 100BASE-TX
full duplex mode, 100BASE-TX half duplex mode, 10BASE-T  full duplex mode,
10BASE-T  half duplex mode
Operational MAU type: Unknown
```

Таблица 5.108 - Описание результатов

Поле	***Описание***
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.

5.15.10 Настройка протокола OAM

Ethernet OAM (Operation, Administration, and Maintenance), IEEE 802.3 ah – 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 конфигурирования интерфейсов Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейсов Ethernet:

`console(config-if)#`

Таблица 5.109 – Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
ethernet oam	-/отключено	Включить поддержку Ethernet OAM на порту.
no ethernet oam		Отключить Ethernet OAM на конфигурируемом порту.
ethernet oam link-monitor frame threshold *count*	1..65535/1	Устанавливает порог количества ошибок за указанный период (период устанавливается командой **ethernet oam link-monitor frame window**).
no ethernet oam link-monitor frame threshold		Восстанавливает значение по умолчанию.
ethernet oam link-monitor frame window *window*	10..600/100 мс	Устанавливает временной промежуток для подсчета количества ошибок.
no ethernet oam link-monitor frame window		Восстанавливает значение по умолчанию.
ethernet oam link-monitor frame-period threshold *count*	1..65535/1	Устанавливает порог для события «frame-period» (период устанавливается командой **ethernet oam link-monitor frame-period window**).
no ethernet oam link-monitor frame-period threshold		Восстанавливает значение по умолчанию.
ethernet oam link-monitor frame-period window *window*	1..65535/10000	Устанавливает временной промежуток для события «frame-period» (в фреймах).
no ethernet oam link-monitor frame-period window		Восстанавливает значение по умолчанию.
ethernet oam link-monitor frame-seconds threshold *count*	1..900/1	Устанавливает 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		Восстанавливает значение по умолчанию.
ethernet oam link-monitor frame-seconds window *window*	100..9000/100 мс	Устанавливает временной промежуток для события «frame-period».
no ethernet oam link-monitor frame-seconds window		Восстанавливает значение по умолчанию.
ethernet oam mode {active|passive}	-/active	Устанавливает 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		Восстанавливает значение по умолчанию.
ethernet-oam remote-failure	-/включено	Включает поддержку и обработку событий «remote-failure».
no ethernet oam remote-failure		Восстанавливает значение по умолчанию.
ethernet oam remote-loopback supported	-/отключено	Включает поддержку функции заворота трафика.

no ethernet oam remote-loopback supported		Восстанавливает значение по умолчанию.
ethernet oam uni-directional detection	-/отключено	Включает функцию обнаружения однонаправленных связей на базе протокола Ethernet OAM.
no ethernet oam uni-directional detection		Восстанавливает значение по умолчанию.
ethernet oam uni-directional detection action {log|error-disable}	-/log	Определяет 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		Восстанавливает значение по умолчанию.
ethernet oam uni-directional detection agressive	-/отключено	Включает 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		Восстанавливает значение по умолчанию.
ethernet oam uni-directional detection discovery time *time*	5..300/5 сек	Устанавливает временной интервал для определения типа связи на порту.
no ethernet oam uni-directional detection discovery-time		Восстанавливает значение по умолчанию.

Команды режима privileged EXEC

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

console#

Таблица 5.110 – Команды режима privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
clear ethernet oam statistics [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port***}]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Очищает статистику Ethernet OAM для указанного интерфейса.
show ethernet oam discovery [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port***}]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Отображает состояние протокола Ethernet OAM для указанного интерфейса.
show ethernet oam statistics [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port***}]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Отображает статистику обмена протокольными сообщениями для указанного интерфейса.
show ethernet oam status [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port***}]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Отображает настройки Ethernet OAM для указанного интерфейса.
show ethernet oam uni-directional detection [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port***}]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Отображает состояние механизма определения однонаправленных связей для указанного интерфейса.

Примеры выполнения команд

Отобразить состояние протокола для порта gigabitethernet 1/0/3:

console#**show ethernet oam discovery interface GigabitEthernet** 0/3

```
gigabitethernet 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#
```

5.15.11 Настройка протокола CFM

Ethernet CFM (Connectivity Fault Management), IEEE802.1ag – предоставляет функции наблюдения, поиска и устранения неисправностей в сетях Ethernet, позволяя контролировать соединение, изолировать проблемные участки сети и идентифицировать клиентов, к которым применялись ограничения в сети.

Протокол оперирует следующими понятиями:

- Maintenance Domain (MD) – участок сети, принадлежащий и управляемый одним оператором;
- Maintenance Association (MA) – совокупность конечных точек (MEP), каждая из которых имеет одинаковый идентификатор MAID (Maintenance Association Identifier), определящий тип сервиса;
- Maintenance association End Point (MEP) – конечная точка сервиса, расположенная на его границе;
- Maintenance domain Intermediate Point (MIP) – промежуточная точка домена.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

`console(config)#`

Таблица 5.111 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
ethernet cfm domain *name* **[level** *level***]**	name: (1..32) символов level: (0..7)/0	Создание (или смена уровня) CFM домена (MD) с именем *«name»* и переход в режим конфигурирования домена. - *level* – уровень CFM домена.
no ethernet cfm domain *name*		Удаление CFM домена (MD) с именем «*name».*

Команды режима конфигурирования домена

Вид запроса командной строки в режиме конфигурирования домена:

`console(config-cfm-md)#`

Таблица 5.112 – Команды режима конфигурирования CFM домена (MD)

Команда	*Значение/Значение по умолчанию*	*Действие*
id { dns *dns* **| name** *name* **| id mac** *mac_address number* **| id null }**	name: (1..43) символов dns: (1..43) символов mac_address: H.H.H или H:H:H:H:H:H или H-H-H-H-H-H number: (0-65535) По умолчанию: id name соответствует имени домена	Указание идентификатора CFM домена (MD). Именем домена может быть: - *dns* – dns-имя; - *name* – текстовая строка; - *mac_address number* – MAC-адрес и числовой идентификатор домена; - **null** – NULL идентификатор.
no id		Установка значения по умолчанию.
service port { vlan-id *vlan_id* **| name** *name* **| number** *number* **}**	vlan: (1..4094) vlan_id: (1..4094) name: (1..45) символов number: (0..65535)	Создание CFM-сервиса (MA) без привязки к VLAN и переход в режим конфигурирования сервиса.
no service port		Удаление CFM-сервиса (MA).
service vlan *vlan* **{ vlan-id** *vlan_id* **| name** *name* **| number** *number*		Создание CFM-сервиса (MA) привязанного к VLAN с номером «*vlan*» и переход в режим конфигурирования сервиса. Именем сервиса может быть: - *vlan_id* – номер VLAN; - *name* – текстовая строка; - *number* – числовой идентификатор.
no service vlan *vlan_id* **}**		Удаление CFM-сервиса (MA) привязанного к VLAN с номером «*vlan*».
mip auto-create [lower-mep-only]	-/автоматическое создание отключено	Включение автоматического создания промежуточных точек сервиса (MIP). Промежуточные точки сервиса (MIP) создаются на всех портах, на которых прописан VLAN сервиса. Необязательный параметр «lower-mep-only» исключает из списка порты, на которых уже создана конечная точка сервиса.
no mip auto-create		Устанавливает значение по умолчанию.

Команды режима конфигурирования сервиса

Вид запроса командной строки в режиме конфигурирования домена:

`console(config-cfm-ma)#`

Таблица 5.113 – Команды режима конфигурирования CFM сервиса (MA)

Команда	*Значение/Значение по умолчанию*	*Действие*
continuty-check interval *interval*	interval: (1, 10, 100, 600) секунд/1 секунда	Установка интервала отправки Continuty Check сообщений**.**
no continuty-check interval		Установка значения по умолчанию
direction down	-	Устанавливает направление конечной точки сервиса (MEP) в нисходящее.
no direction down		Устанавливает направление конечной точки сервиса (MEP) в восходящее.
mep *id*	id: (1..8191)	Добавление конечной точки сервиса (MEP) с идентификатором «id» к данному сервису. **Данной командой осуществляется только привязка MEP к сервису. MEP создается в режиме конфигурирования интерфейса.**
no mep *id*		Удаление конечной точки сервиса (MEP).
mip auto-create [{ lower-mep-only | none }]	-/По умолчанию используется режим, сконфигурированный для	Включение автоматического создания промежуточных точек сервиса (MIP). Промежуточные точки сервиса (MIP) создаются на всех портах, на которых прописан VLAN

	домена, в котором находится сервис	сервиса. Необязательные параметры: - **lower-mep-only** – исключает из списка порты, на которых уже создана конечная точка сервиса (MEP); - **none** – не создавать автоматически промежуточные точки сервиса (MIP).
no mip auto-create		Установка значения по умолчанию.

Команды режима конфигурирования интерфейса Ethernet

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

`console(config-if)#`

Таблица 5.114 – Команды режима конфигурирования интерфейса Ethernet

Команда	***Значение/Значение по умолчанию***	***Действие***
ethernet cfm mep *id* **domain** *domain_name* **service { vlan-id** *vlan_id* **| name** *name* **| number** *number* **}**	id: (1..8191) domain_name: (0..32) символов vlan_id: (1..4094) name: (0..45) символов number: (0..65535)	Создание на интерфейсе конечной точки сервиса (MEP) с идентификатором *«id»* для указанного сервиса в указанном домене и переход в режим конфигурирования MEP.
no ethernet cfm mep *id* **domain** *domain_name* **service { vlan-id** *vlan_id* **| name** *name* **| number** *number* **}**		Удаление конечной точки сервиса (MEP) с интерфейса.

Команды режима конфигурирования конечной точки сервиса

Вид запроса командной строки в режиме конфигурирования домена:

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

Таблица 5.115 – Команды режима конфигурирования CFM конечной точки (MEP)

Команда	***Значение/Значение по умолчанию***	***Действие***
Active	-/Выключена	Включение конечной точки сервиса (MEP).
no active		Установка значения по умолчанию.
continuty-check enable	-/Выключена	Включение отправки Continuty Check сообщений.
no continuty-check enable		Установка значения по умолчанию.
cos *cos*	cos: (0..7)/7	Установка значения приоритета CoS, с которым будут отправляться Continuty Check сообщения.
no cos		Установка значения по умолчанию.
alarm delay *delay*	delay: (2500..10000) мс/2500 мс	Указание интервала задержки, по истечении которого будет генерироваться авария.
no alarm delay		Установка значения по умолчанию.
alarm reset *interval*	interval: (2500..10000) мс/10000 мс	Указание промежутка времени, по истечении которого произойдет сброс аварии.
no alarm reset		Установка значения по умолчанию.
alarm notification { all | error-xcon | remote-error-xcon | mac-remote-error-xcon | xcon | none }	-/mac-remote-error-xcon	Включение уведомлений для определенных типов событий. Типы событий: - **all** – все события DefRDI, DefMACStatus, DefRemote, DefError, DefXcon; - **error-xcon** – только события DefError и DefXcon; - **remote-error-xcon** – только события DefRemote, DefError и DefXcon; - **mac-remote-error-xcon** - только события DefMACStatus, DefRemote, DefError и DefXcon; - **xcon** – только событие DefXcon; - **none** – уведомления отключены.
no alarm notification		Установка значения по умолчанию.

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

console#

Таблица 5.116 – Команды режима privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ethernet cfm domain [*name*]	name: (1..32) символов	Отображает информацию об указанном домене или обо всех.
show ethernet cfm errors	-	Отображает информацию об ошибках Continuity Check протокола.
show ethernet cfm maintenance-points { local | remote }	-	Отображает информацию о локальных или удаленных конечных точках сервиса (MEP).
show ethernet cfm mpdb [domain-id { dns *name* **| name** *name***| mac** *mac_address number* **| null}]**	name: (1..43) символов mac_address: H.H.H или H:H:H:H:H:H или H-H-H-H-H-H number: (0-65535)	Отображает информацию о промежуточных точках сервиса (MIP) для указанного домена или для всех.
show ethernet cfm statistics	-	Отображает CFM-статистику для всех доменов.
show ethernet cfm statistics domain *domain_name* **service { vlan-id** *vlan_id* **| name** *name* **| number** *number* **}**	domain_name: (0..32) символов vlan_id: (1..4094) name: (0..45) символов number: (0..65535)	Отображает CFM-статистику для указанного домена.
show ethernet cfm statistics mpid *id*	id: (1..8191)	Отображает CFM-статистику для указанной конечной точки сервиса (MEP).

5.15.12 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 граничном коммутаторе, передает их на другой граничный коммутатор, который ожидает специальные инкапсулированные кадры, а затем декапсулирует их, что позволяет пользователям передавать информацию 2-го уровня через сеть провайдера.

Коммутаторы MES3000 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 (рисунок 24). Информация об изменении топологии сети может быть передана сквозь сеть провайдера.

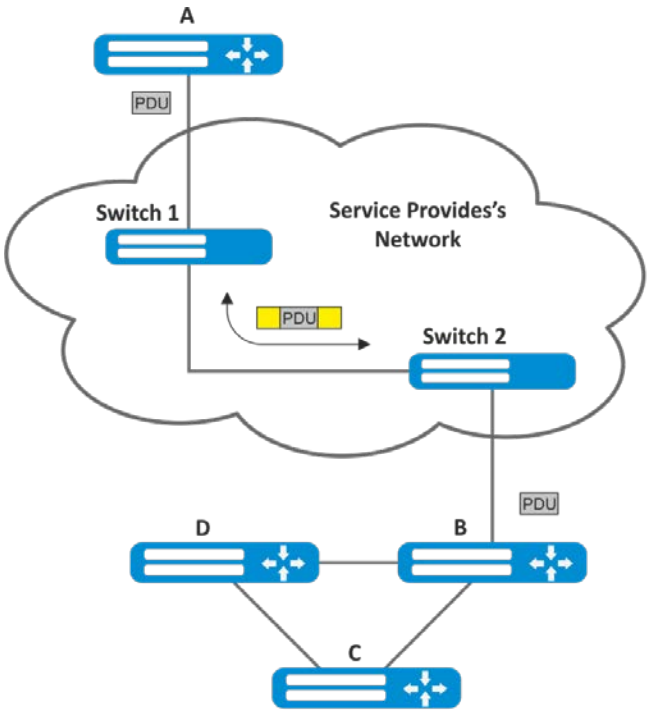


Рисунок 24 - Пример

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

Если настройка выключена, то:

- PDU-фрейм передается в обработчик соответствующего протокола.

Декапсуляция:

1. Реализован перехват на CPU Ethernet-фреймов с Destination MAC-адресом, заданным при помощи команды l2protocol-tunnel address xx-xx-xx-xx-xx-xx. Перехват включается только тогда, когда хотя бы на одном порту включена настройка l2protocol-tunnel (независимо от протокола).

2. При перехвате пакета с Destination MAC адресом 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 l2protocol-tunnel для данного L2-протокола.

Если настройка включена, то:

- порт, с которого был получен инкапсулированный PDU-фрейм, блокируется с причиной l2pt-guard.

Если настройка выключена:

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

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.117 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
l2protocol-tunnel address {*mac-address***}**	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 фреймов..
no l2protocol-tunnel address		Установить значение по умолчанию.

Команды режима конфигурирования интерфейса Ethernet

На граничном интерфейсе должен быть отключен протокол STP (spanning-tree disable).

Граничный интерфейс должен быть настроен в режиме access или customer.

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

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

Таблица 5.118 – Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
l2protocol-tunnel {stp | lacp | lldp | isis-l1 | isis-l2 | eth-fc}	/выключено	Включение режима инкапсуляции пакетов STP BPDU.
no l2protocol-tunnel {stp | lacp | lldp| isis-l1 | isis-l2 | eth-fc}		Выключение режима инкапсуляции пакетов STP BPDU.
l2protocol-tunnel cos *cos*	cos : (0..7)/5	Задать значение CoS для запакованных PDU-фреймов.
no l2protocol-tunnel cos		Установка CoS в значение по умолчанию.
l2protocol-tunnel drop-threshold {stp | lacp | lldp | isis-l1 | isis-l2 | eth-fc} *threshold*	treshold: (1..4096)/выключено	Настройка порогового значения скорости входящих PDU-фреймов (в пакетах в секунду), полученных и подлежащих инкапсуляции. При превышении порога PDU отбрасываются.
no l2protocol-tunnel drop-threshold {stp | lacp | lldp | isis-l1 | isis-l2 | eth-fc}		Отключает режим контроля скорости входящих PDU-фреймов.
l2protocol-tunnel	treshold:	Настройка порогового значения скорости входящих PDU-

shutdown-threshold {stp | lacp | lldp | isis-l1 | isis-l2 | eth-fc} *threshold*	(1..4096)/выключено	фреймов (в пакетах в секунду), полученных и подлежащих инкапсуляции. При превышении порога порт будет переведен в состояние Errdisable (отключен).
no l2protocol-tunnel shutdown-threshold {stp | lacp | lldp | isis-l1 | isis-l2 | eth-fc}		Отключает режим контроля скорости входящих PDU-фреймов.

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

console#

Таблица 5.119 – Команды режима privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show l2protocol-tunnel [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Отображает информацию L2PT для указанного интерфейса или для всех интерфейсов, на которых включен L2PT, если интерфейс не указан.
clear l2protocol-tunnel statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	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-treshold и shutdown-treshold).

```
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 gigabitEthernet 1/0/1
console(config-if)# spanning-tree disable
console(config-if)# switchport mode customer
console(config-if)# switchport customer vlan 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  Drop     Encaps   Decaps   Drop
                 Threshold Threshold Counter  Counter  Counter
-------- --- -------- --------- --------- --------- --------- ---------
gi1/0/1  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 gi1/0/1
12-Nov-2015 14:32:35 %-I-SHUTDOWN: Tunnel shutdown threshold 100 exceeded for interface gi1/0/1

5.16 Voice VLAN

Voice VLAN используется для выделения VoIP-оборудования в отдельную VLAN. Для VoIP-фреймов могут быть назначены QoS-атрибуты для приоритезации трафика. Классификация фреймов, относящихся к фреймам 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 фрейм 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 Voice VLAN ID, настроенным на MES2124;
- VoIP-оборудование рассылает нетегированные DHCP-запросы. В ответе от DHCP-сервера присутствует опция 132, содержащая VLAN ID, который VoIP-устройство автоматически назначает себе в качестве VLAN для маркировки VoIP-трафика (Voice VLAN ID);
- VoIP оборудование получает Voice VLAN ID в lldp-med сообщениях.

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 глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.120 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
voice vlan aging-timeout *timeout*	timeout: (1..43200/1440)	Устанавливает таймаут для порта, принадлежащего к voice-vlan. Если с порта в течение заданного времени не было фреймов с OUI VoIP-оборудования, то voice vlan удаляется с данного порта.
no voice vlan aging-timeout		Восстанавливает значение по умолчанию.
voice vlan cos *cos* **[remark]**	(0-7)/6	Устанавливает COS, которым маркируются фреймы, принадлежащие Voice VLAN.
no voice vlan cos		Восстанавливает значение по умолчанию.
voice vlan id *vlan_id*	vlan_id:(2 .. 4094)	Устанавливает идентификатор VLAN для Voice VLAN
no voice vlan id		Удаляет идентификатор VLAN для Voice VLAN **Для удаления идентификатора VLAN требуется предварительно отключить функцию voice vlan на всех портах.**

voice vlan oui-table {add *oui***|remove** *oui***}** [*word*]	word: (1..32) символов	Позволяет редактировать таблицу OUI. - *oui* – первые 3 байта MAC-адреса; - *word* – описание oui.
no voice vlan oui-table		Удаляет все пользовательские изменения OUI-таблицы.

Команды режима конфигурирования интерфейса Ethernet

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

`console(config-if)#`

Таблица 5.121 – Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
voice vlan enable	Отключена	Включает Voice VLAN для порта.
no voice vlan enable		Отключает Voice VLAN для порта.
voice vlan cos mode {src|all}	-	Включает маркировку трафика для всех фреймов, либо только для источника.
no voice vlan cos mode		Восстанавливает значение по умолчанию.
voice vlan secure	Отключен	Включает безопасный режим для VLAN. Команда применяется только к портам, которые были добавлены к Voice VLAN автоматически.
no voice vlan secure		Восстанавливает значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

`console#`

Таблица 5.122 – Команды режима конфигурирования EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show voice vlan [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Отображает состояние Voice VLAN.

5.17 Групповая адресация

5.17.1 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 конфигурирования интерфейса VLAN

Вид запроса командной строки в режиме конфигурирования интерфейса VLAN:

`console(config-if)#`

Таблица 5.123 – Команды режима конфигурирования интерфейса VLAN

Команда	*Значение/Значение по умолчанию*	*Описание*
bridge multicast mode {mac-group | ipv4-group | ipv4-src-group}	-/mac-group	Задает режим групповой передачи данных. **- mac-group** – многоадресная передача, основанная на VLAN и MAC-адресах; - **ipv4-group** – многоадресная передача с типом фильтрации, основанным на VLAN и адресе приемника в формате IPv4; - **ip-src-group** – многоадресная передача с типом

		фильтрации, основанным 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* |**port-channel** *group*}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12).	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 диапазон 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* |**port-channel** *group*}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12).	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* |**port-channel** *group*}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12). По умолчанию передача всех многоадресных пакетов запрещена.	Разрешает передачу всех многоадресных пакетов на порту. - *mac_multicast_address* – групповой MAC-адрес; - **add** – добавляет порты/объединённые 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* |**port-channel** *group*}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12). По умолчанию портам не запрещено динамически присоединяться к многоадресной группе.	Запрещает порту динамически добавляться к многоадресной группе. - *interface-list* – список интерфейсов Ethernet; - *port-channel-number-list* – список групп портов; - **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 *ip_multicast_address* [[**add** | **remove**] {**gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* |**port-channel** *group*}	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Регистрирует IP-адрес в таблице групповой адресации, и статически добавляет/удаляет интерфейсы из группы. - *ip_multicast_address* – групповой IP-адрес; - **add** – добавляет порты к группе; - **remove** – удаляет порты из группы; Перечисление интерфейсов осуществляется через «–» и «,».
no bridge multicast ip-address *ip_multicast_address*		Удаляет групповой IP-адрес из таблицы.

bridge multicast forbidden ip-address {*ip_multicast_address*} **{add | remove}** **{gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***}**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Запрещает порту динамически добавляться к многоадресной группе. - *ip_multicast_address* – групповой IP-адрес; - **add** – добавление порта/портов к списку запрещенных; - **remove** – удаление порта/портов из списка запрещенных. Перечисление интерфейсов осуществляется через «–» и «,» **Прежде чем определить запрещенные порты, группы многоадресной рассылки должны быть зарегистрированы.**
no bridge multicast forbidden ip-address {*ip_multicast_address*}		Восстанавливает значение по умолчанию.
bridge multicast source *ip-address* **group** *ip_multicast_address* **[[add | remove]** **{gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***}]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Устанавливает соответствие между IP-адресом пользователя и групповым адресом в таблице групповой адресации, и статически добавляет/удаляет интерфейсы из группы. - *ip_address* – исходный IP-адрес; - ip_multicast_address – 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** *ip_multicast_address*		Восстанавливает значение по умолчанию.
bridge multicast forbidden source *ip_address* **group** *ip_multicast_address* **{add | remove}** **{gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***}**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Устанавливает запрет на добавление/удаление соответствия между IP-адресом пользователя и групповым адресом в таблице групповой адресации для определенного порта. - *ip_address* – исходный IP-адрес; - ip_multicast_address – 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** *ip_multicast_address*		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, основанным на VLAN и адресе приемника в формате IPv6; - **ip-src-group** – многоадресная передача с типом фильтрации, основанным на VLAN и адресе отправителя в формате IPv6.
no bridge multicast ipv6 mode		Устанавливает значение по умолчанию.
bridge multicast ipv6 ip-address *ipv6_multicast_address* **[[add | remove]** **{gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***}]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Регистрирует групповой IPv6-адрес в таблице групповой адресации, и статически добавляет/удаляет интерфейсы из группы. - *ip_multicast_address* – групповой IP-адрес; - **add** – добавляет порты к группе; - **remove** – удаляет порты из группы; Перечисление интерфейсов осуществляется через «–» и «,»
no bridge multicast ipv6 ip-address *ip_multicast_address*		Удаляет групповой IP-адрес из таблицы.
bridge multicast ipv6 forbidden ip-address *ipv6_multicast_address* **{add | remove}**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Запрещает подключение настраиваемого порта/портов к групповому IPv6-адресу. - *ipv6_multicast_address* – групповой IP-адрес; - **add** – добавление порта/портов в список запрещенных;

{ gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***}**		- **remove** – удаление порта/портов из списка запрещенных. Перечисление интерфейсов осуществляется через «–» и «,»
no bridge multicast ipv6 forbidden ip-address *ipv6_multicast_address*		Восстанавливает значение по умолчанию.
bridge multicast ipv6 source *ipv6_address* **group** *ipv6_multicast_address* **[[add | remove] { gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***}]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Устанавливает соответствие между IPv6-адресом пользователя и групповым адресом в таблице групповой адресации, и статически добавляет/удаляет интерфейсы из группы. - *ipv6_address* – исходный IP-адрес; - *ipv6_multicast_address* – групповой IP-адрес; - **add** – добавить порты в группу исходного IP-адреса; - **remove** – удалить порты из группы исходного IP-адреса.
no bridge multicast ipv6 source *ipv6_address* **group** *ipv6_multicast_address*		Восстанавливает значение по умолчанию.
bridge multicast ipv6 forbidden source *ipv6_address* **group** *ipv6_multicast_address* **{add | remove} { gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***}**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Устанавливает запрет на добавление/удаление соответствия между IPv6-адресом пользователя и групповым адресом в таблице групповой адресации для определенного порта. - *ipv6_address* – исходный IPv6-адрес; - *ipv6_multicast_address* – 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 *ipv6_address* **group** *ipv6_multicast_address*		Восстанавливает значение по умолчанию.
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 конфигурирования интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов

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

console# **configure**
console(config)# **interface** {**tengigabitethernet** *te_port* | **gigabitethernet** *gi_port* |**port-channel** *group* | ***range*** {…}}
console(config-if)#

Таблица 5.124 – Команды режима конфигурирования интерфейса Ethernet, 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 глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.125 – Команды режима глобального конфигурирования

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 *seconds*	seconds: (10..86400)/300 секунд	Задает время хранения MAC-адреса в таблице глобально. Время хранения MAC-адреса, начиная с 600 секунд, может быть задано только с интервалом в 300 секунд. (900, 1200, 1500 и т.д) При малых значениях aging-time (до 600 секунд) допустима погрешность, соизмеримая с его значением. С увеличением значения aging-time погрешность нивелируется.
no mac address-table aging-time		Устанавливает значение по умолчанию.
mac address-table aging-time *seconds* **vlan** *vlan_id*	seconds: (10..86400)/300 секунд; vlan_id: (1..4094)	Задает время хранения MAC-адреса в таблице для VLAN.
no mac address-table aging-time *seconds* **vlan** *vlan_id*		Устанавливает значение по умолчанию.
mac address-table learning vlan *vlan_id*	vlan_id: (1..4094)/По умолчанию включено	Включить изучение MAC-адресов в данном VLAN.
no mac address-table learning vlan *vlan_id*		Отключить изучение MAC-адресов в данном VLAN.
mac address-table static *mac_address* **vlan** *vlan_id* **interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***} [permanent | delete-on-reset | delete-on-timeout | secure]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Добавляет исходный MAC-адрес в таблицу групповой адресации. - *mac-address* – MAC-адрес; - *vlan_id* – номер VLAN; - **permanent** – данный MAC-адрес можно удалить только с помощью команды **no mac 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 mac address** или после возвращения порта в режим обучения (**no port security**).
no mac address-table static [*mac_address***] vlan** *vlan_id*		Удаляет MAC-адрес из таблицы групповой адресации.
bridge multicast reserved-address *mac_multicast_address* **[ethernet-v2** *ethtype* **| llc** *sap* **| llc-snap** *pid* **] {discard | bridge}**	ethtype: (0x0600..0xFFFF) sap: (0..0xFFFF) pid: (0..0xFFFFFFFFFF)	Определяет действие для пакетов многоадресной рассылки с зарезервированного адреса. - *mac_multicast_address* – групповой MAC-адрес; - *ethtype* – тип пакета Ethernet v2; - *sap* – тип пакета LLC; - *pid* – тип пакета LLC-Snap; - **discard** - сброс пакетов; - **bridge** – пакеты передаются в режиме bridge.
no bridge multicast reserved-address *mac_multicast_address* **[ethernet-v2** *ethtype* **| llc** *sap* **| llc-snap** *pid* **]**		Устанавливает значение по умолчанию.
mac address-table lookup-length *length*	length: (1..8)/3	Задает размер области MAC-адресов в алгоритме хеширования. Изменения вступают в действие после рестарта коммутатора.
no mac address-table lookup-length		Устанавливает значение по умолчанию. Изменения вступают в действие после рестарта коммутатора.
mac address-table notification flapping	-/включено	Включить функцию обнаружения флаппинга MAC-адресов. Флаппинг обнаруживается, если выполняется следующее условие: динамическая запись в MAC-таблице меняет порт

		четыре раза, при этом между каждой сменой проходит не более 2 секунд (точность измерения - одна секунда).
no mac address-table notification flapping		Выключить функцию обнаружения флаппинга MAC-адресов.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

console#

Таблица 5.126 – Команды режима Privileged EXEC

Команда	***Значение***	***Описание***
clear mac address-table {dynamic| secure} [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***}]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	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 5.127 – Команды режима EXEC

Команда	***Значение***	***Описание***
show mac address-table [dynamic | static| secure] [**vlan** *vlan_id*] [**interface** {**gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group*] [**address** *mac_address*]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12); 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* **|port-channel** *group***}]**]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12); 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 *vlan_id*] [**address** *mac_multicast_address* | *ipv4_multicast_address* | *ipv6_multicast_address*] [**source** *ipv4_source_address* |	vlan_id: (1..4094)	Показывает таблицу статических групповых адресов для указанного интерфейса либо всех интерфейсов VLAN. - *vlan_id* – идентификационный номер VLAN; - mac_multicast_address – групповой MAC-адрес; - ipv4_multicast_address – групповой IPv4-адрес; - ipv6_multicast_address – групповой IPv6-адрес; - ipv4_source_address – IPv4-адрес источника; - ipv6_source_address – IPv6-адрес источника;

ipv6_source_address] **[all | mac | ip]**		- **ip** – просмотр по IP-адресам; - **mac** – просмотр по MAC-адресам; - **all** – просмотр полной таблицы.
show bridge multicast filtering *vlan_id*	vlan_id: (1..4094)	Показывает конфигурацию фильтра групповых адресов для указанного VLAN. - *vlan_id* – идентификационный номер VLAN.
show bridge multicast unregistered [**gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group*]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Показывает конфигурацию фильтра для незарегистрированных групповых адресов.
show bridge multicast mode [vlan *vlan_id***]**	vlan_id: [1..4094]	Показывает режим групповой адресации для указанного интерфейса либо всех интерфейсов VLAN. - *vlan_id* – идентификационный номер VLAN.
show bridge multicast reserved-addresses	-	Отображает правила, установленные для групповых зарезервированных адресов.
show mac address-table mode	-	Показывает текущий режим работы таблицы MAC-адресов и режим, который будет применен после рестарта коммутатора.

Примеры выполнения команд

- Включить фильтрацию групповых адресов коммутатором. Задать время хранения MAC-адреса 450 секунд, разрешить передачу незарегистрированных многоадресных пакетов на 11 порту коммутатора.

```
console # configure
console(config) # bridge aging-time 450
console(config) # bridge multicast filtering
console(config) # interface gigabitethernet 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            gi0/1, gi0/2
19   224-239.130|2.2.8            static              gi0/1-8
19   224-239.130|2.2.8            dynamic             gi0/9-11

Forbidden ports for multicast addresses:

Vlan IP/MAC Address         Ports
---- -------------------    -------------------
1    224-239.130|2.2.3              gi0/8
19   224-239.130|2.2.8              gi0/8
```

5.17.2 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 «Правила групповой адресации»).

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 глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

`console(config)#`

Таблица 5.128 – Команды режима глобального конфигурирования

Команда	***Значение***	***Действие***
ip igmp snooping	По умолчанию функция выключена	Разрешает использование функции IGMP Snooping коммутатором.
no ip igmp snooping		Запрещает использование функции IGMP Snooping коммутатором.
ip igmp snooping vlan *vlan_id*	По умолчанию функция выключена	Разрешает использование функции IGMP Snooping коммутатором для данного интерфейса VLAN. - *vlan_id* – идентификационный номер VLAN.
no ip igmp snooping vlan *vlan_id*		Запрещает использование функции IGMP Snooping коммутатором для данного интерфейса VLAN.
ip igmp snooping vlan *vlan_id* **static** *ip_multicast_address* **[interface { gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***}]**	vlan_id: (1..4094); gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Регистрирует групповой IP-адрес в таблице групповой адресации, и статически добавляет интерфейсы из группы для текущей VLAN. - *vlan_id* – идентификационный номер VLAN; - *ip_multicast_address* – групповой IP-адрес. Перечисление интерфейсов осуществляется через «–» и «,».
no ip igmp snooping vlan *vlan_id* **static** *ip_address* **[interface { gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***}]**		Удаляет групповой IP-адрес из таблицы.
ip igmp snooping vlan *vlan_id* **cos** *cos*	vlan_id: (1..4094); cos: (0..7)/0	Устанавливает значение CoS для исходящих в порт mrouter IGMP-сообщений в указанной VLAN. - *vlan_id* – идентификационный номер VLAN; - *cos* – класс обслуживания.
no ip igmp snooping vlan *vlan_id* **cos** *cos*		Устанавливает значение CoS для исходящих в порт mrouter IGMP-сообщений в указанной VLAN равным нулю.
ip igmp snooping vlan *vlan_id* **mrouter learn pim-dvmrp**	vlan_id: (1..4094)/ разрешено	Разрешает для данной группы VLAN автоматическое распознавание портов, к которым подключены многоадресные маршрутизаторы. - *vlan_id* – идентификационный номер VLAN.
no ip igmp snooping vlan *vlan_id* **mrouter learn pim-dvmrp**		Запрещает для данной группы VLAN автоматическое распознавание портов, к которым подключены многоадресные маршрутизаторы.
ip igmp snooping vlan *vlan_id* **mrouter interface { gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***}**	vlan_id: (1..4094); gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Определяет порт, к которому подключен маршрутизатор многоадресной рассылки для заданной VLAN. - *vlan_id* – идентификационный номер VLAN.
no ip igmp snooping vlan *vlan_id* **mrouter interface { gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***}**		Указывает, что к порту не подключен маршрутизатор многоадресной рассылки.

ip igmp snooping vlan *vlan_id* **forbidden mrouter interface** **{ gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***}**	vlan_id: (1..4094); gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Устанавливает запрет на определение порта (статически, динамически) как порта, к которому подключен маршрутизатор многоадресной рассылки. - *vlan_id* – идентификационный номер VLAN.
no ip igmp snooping vlan *vlan_id* **forbidden mrouter interface** **{ gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***}**		Снимает запрет на определение порта как порта, к которому подключен маршрутизатор многоадресной рассылки.
ip igmp snooping vlan *vlan_id* **replace source-ip** *ip_address*	vlan_id: (1..4094)	Включает замену IP-адреса источника на указанный IP-адрес во всех пакетах IGMP report в заданной VLAN. - *vlan_id* – идентификационный номер VLAN.
no ip igmp snooping vlan *vlan_id* **replace source-ip**		Отключает замену IP-адреса источника в пакетах IGMP report в заданной VLAN.
ip igmp snooping map cpe vlan *vlan_id* **multicast-tv vlan** *vlan_id*	vlan_id:(1..4094)	Добавляет соответствие между VLAN пользователя (CPE-VLAN) и VLAN телевещания (multicast-tv-vlan). Если IGMP-сообщение приходит на порт с тегом CPE-vlan и существует соответствие CPE-vlan – multicast-tv-vlan, то IGMP-сообщение будет ассоциировано с VLAN для телевещания.
no ip igmp snooping map cpe vlan *vlan_id*		Удаляет соответствие между VLAN пользователя и VLAN телевещания
ip igmp snooping vlan *vlan_id* **querier**	vlan_id: (1..4094) -/выдача запросов отключена	Включает поддержку выдачи запросов igmp-query коммутатором в данной VLAN.
no ip igmp snooping vlan *vlan_id* **querier**		Отключает поддержку выдачи запросов igmp-query коммутатором в данной VLAN.
ip igmp snooping vlan *vlan_id* **querier version** {**2** | **3**}	-/IGMPv3	Устанавливает версию IGMP-протокола, на основании которой будут формироваться IGMP-query запросы.
no ip igmp snooping vlan *vlan_id* **querier version**		Устанавливает значение по умолчанию
ip igmp snooping vlan *vlan_id* **querier address** *ip_address*	vlan_id: (1-4094)	Определяет исходный IP-адрес, который будет использоваться IGMP querier-ом. Querier – устройство, которое отправляет IGMP-запросы.
no ip igmp snooping vlan *vlan_id* **querier address**		Устанавливает значение по умолчанию. По умолчанию если IP-адрес настроен для VLAN, он используется в качестве адреса источника IGMP Snooping Querier.
ip igmp snooping vlan *vlan_id* **immediate-leave**	vlan_id: (1..4094)/disable	Включить процесс IGMP Snooping Immediate-Leave на текущей VLAN. Означает, что порт должен быть немедленно удален из группы IGMP после получения сообщения IGMP leave. При добавлении опции host-based – механизм fast-leave срабатывает только в том случае, когда все пользователи, подключенные к данному порту отписались от группы (счетчик пользователей ведется на основании src-MAC-адресов в заголовках IGMP-report'ов).
no ip igmp snooping vlan *vlan_id* **immediate-leave [host-based]**		Отключить процесс IGMP Snooping Immediate-Leave на текущей VLAN.
ip igmp snooping vlan *vlan_id* **immediate-leave host-based**	vlan_id: (1..4094)/disable	Включить процесс IGMP Snooping Immediate-Leave на текущей VLAN. Означает, что порт должен быть немедленно удален из группы IGMP после получения сообщения IGMP leave, если больше нет клиентов, которым необходима данная группа.
no ip igmp snooping vlan *vlan_id* **immediate-leave**		Отключить процесс IGMP Snooping Immediate-Leave на текущей VLAN.
ip igmp snooping vlan *vlan_id* **proxy-report** [**version** *version*]	vlan_id: (1..4094); version: (1..3)	Включает режим, при котором коммутатор отправляет report на query запросы статических групп, настроенных на нем. При этому сообщения IGMP-report/leave на эти группы игнорируются.

		- **version** – фиксирует версию report/leave сообщений, отправляемых proxy-report'ером. По умолчанию все IGMP-сообщения, созданные proxy-report'ером – IGMPv3, а ответы на query сообщения будут в той версии, в которой был прислан IGMP-query.
no ip igmp snooping vlan *vlan_id* **proxy-report**		Восстанавливает настройки по умолчанию.
ip igmp snooping vlan *vlan_id* **cos** *cos*	cos: (0..7)	Устанавливает значение параметра поля приоритета 802.1p.
no ip igmp snooping vlan *vlan_id* **cos**		Восстанавливает настройки по умолчанию.

Команды режима конфигурирования интерфейса VLAN

Вид запроса командной строки режима конфигурирования VLAN:

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

Таблица 5.129 – Команды режима конфигурирования интерфейса VLAN

Команда	***Значение/Значение по умолчанию***	***Действие***
ip igmp robustness *count*	(1-7)/2	Устанавливает значение устойчивости для IGMP. Если на канале наблюдается потеря данных, значение устойчивости должно быть увеличено.
no ip igmp robustness		Устанавливает значение по умолчанию.
ip igmp query-interval *seconds*	(30–18000)/125 с	Устанавливает таймаут, по которому система отправляет основные запросы всем участникам группы многоадресной передачи для проверки их активности.
no ip igmp query-interval		Устанавливает значение по умолчанию.
ip igmp query-max-response-time *seconds*	(5-20)/10 с	Устанавливает максимальное время ответа на запрос.
no ip igmp query-max-response-time		Устанавливает значение по умолчанию.
ip igmp last-member-query-count *count*	(1-7)/значение переменной robustness	Устанавливает количество запросов, после рассылки которых, коммутатор определяет, что на данном порту нет желающих участвовать в многоадресной рассылке.
no ip igmp last-member-query-count		Устанавливает значение по умолчанию.
ip igmp last-member-query-interval *milliseconds*	milliseconds: (100..25500)/1000 мс	Устанавливает интервал запроса для последнего участника.
no ip igmp last-member-query-interval		Устанавливает значение по умолчанию.

Команды режима конфигурирования интерфейса (диапазона интерфейсов) Ethernet

Вид запроса командной строки режима конфигурирования интерфейса:

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

Таблица 5.130 – Команды режима конфигурирования интерфейса Ethernet

Команда	***Значение/Значение по умолчанию***	***Действие***
switchport access multicast-tv vlan *vlan_id*	vlan_id: (1-4094)	Включает перенаправление IGMP-запросов с клиентских Vlan в Multicast Vlan и мультикастового трафика в клиентские Vlan для интерфейса в режиме «access».
no switchport access multicast-tv vlan		Выключает перенаправление IGMP-запросов с клиентских Vlan в Multicast Vlan и мультикастового трафика в клиентские Vlan для интерфейса в режиме «access».
switchport trunk multicast-tv vlan *vlan_id* **[tagged]**	vlan_id: (1-4094)	Включает перенаправление IGMP-запросов из VLAN, участником которых является порт, в Multicast VLAN для интерфейса в режиме «trunk». Мультикастовый трафик передается на порт

		нетегированным или тегированным в зависимости от параметра *tagged*. Параметр *tagged* указывает на то, что мультикастовый трафик должен отправляться в порт *тегированным в Multicast VLAN*.
no switchport trunk multicast-tv vlan		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 5.131 – Команды режима EXEC

Команда	*Действие*
show ip igmp snooping mrouter [**interface** *vlan_id*]	Показывает информацию об изученных многоадресных маршрутизаторах в указанной группе VLAN.
show ip igmp snooping interface *vlan_id*	Показывает информацию IGMP-snooping для данного интерфейса.
show ip igmp snooping groups [vlan *vlan_id*] [**ip-multicast-address** *ip_multicast_address*] [**ip-address** *ip_address*]	Показывает информацию об изученных многоадресных группах, участвующих в групповой рассылке.
show ip igmp snooping cpe vlans [**vlan** *vlan_id*]	Показывает таблицу соответствий между VLAN оборудования, установленного у пользователя, и VLAN для телевещания.

Примеры выполнения команд

Включить функцию IGMP snooping на коммутаторе. Для VLAN 6 разрешить автоматическое распознавание портов, к которым подключены многоадресные маршрутизаторы. Установить интервал между IGMP-запросами – 100 сек. Увеличить значение устойчивости до 4. Установить максимальное время ответа на запрос – 15 сек.

```
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 snooping query-interval 100
console (config-if)# ip igmp robustness 4
console (config-if)# ip igmp query-max-response-time 15
```

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 глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

console(config)#

Таблица 5.132 – Команды глобального режима конфигурирования

Команда	*Значение*	*Действие*
ipv6 mld snooping [vlan *vlan_id***]**	vlan_id: 1..4094/ disable	Включает MLD snooipng.

no ipv6 mld snooping [vlan *vlan_id***]**		Отключает MLD snooping.
ipv6 mld snooping vlan *vlan_id* **static** *ipv6_multicast_address* **[interface { gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***}]**	vlan_id: (1-4094); gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Регистрирует групповой IPv6-адрес в таблице групповой адресации, и статически добавляет/удаляет интерфейсы из группы для текущей VLAN. - *ipv6_multicast_address* – групповой IPv6-адрес; Перечисление интерфейсов осуществляется через «–» и «,».
no ipv6 mld snooping vlan *vlan_id* **static** *ipv6_multicast_address* **[interface { gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***}]**		Удаляет групповой IP-адрес из таблицы.
ipv6 mld snooping vlan *vlan_id* **forbidden mrouter interface {gigabitethernet** *gi_port***| tengigabitethernet** *te_port* **|port-channel** *group***}**	vlan_id: (1..4094); gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Добавляет правило, запрещающее портам из списка регистрироваться как MLD-mrouter.
no ipv6 mld snooping vlan *vlan_id* **forbidden mrouter interface {gigabitethernet** *gi_port***| tengigabitethernet** *te_port* **|port-channel** *group***}**		Удаляет правило, запрещающее портам из списка регистрироваться как MLD-mrouter.
ipv6 mld snooping vlan *vlan_id* **mrouter learn pim-dvmrp**	-/включено	Изучать порты, подключенные к mrouter'у по MLD-query-пакетам.
no ipv6 mld snooping vlan *vlan_id* **mrouter learn pim-dvmrp**		Не изучать порты, подключенные к mrouter'у по MLD-query-пакетам.
ipv6 mld snooping vlan ***vlan_id*** **mrouter interface { gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***}**	vlan_id: (1 .. 4094); gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Добавляет список mrouter-портов.
no ipv6 mld snooping vlan *vlan_id* **mrouter interface { gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***}**		Удаляет mrouter-порты.
Ipv6 mld snooping vlan *vlan_id* **immediate-leave**	vlan_id: 1..4094/disable	Включить процесс MLD Snooping Immediate-Leave на текущей VLAN.
no ipv6 mld snooping vlan *vlan_id* **immediate-leave**		Отключить процесс MLD Snooping Immediate-Leave на текущей VLAN.

Команды режима конфигурирования интерфейса VLAN

Вид запроса командной строки режима глобального конфигурирования:

`console(config-if)#`

Таблица 5.133 – Команды режима конфигурирования интерфейса VLAN

Команда	***Значение/Значение по умолчанию***	***Действие***
ipv6 mld join-group *ipv6_multicast_address*	-	Создает статическую группу многоадресной IPv6-рассылки. - *multicast_ipv6_address* – групповой адрес IPv6.
no ipv6 mld join-group *ipv6_multicast_address*		Удаляет статическую группу многоадресной IPv6-рассылки

ipv6 mld last-member-query-count *count*	count: (1..7)	Устанавливает количество MLD-запросов, после рассылки которых коммутатор определяет, что на данном порту нет желающих участвовать в многоадресной IPv6-рассылке
no pv6 mld last-member-query-count		Восстанавливает значение по умолчанию
ipv6 mld last-member-query-interval *interval*	interval: (100..25500)/1000 миллисекунд	Задает максимальную задержку ответа последнего члена группы, которая используется для вычисления кода максимальной задержки ответа (Max Response Code)
no ipv6 mld last-member-query-interval		Восстанавливает значение по умолчанию
ipv6 mld query-interval *value*	value: (30..18000)/125 секунд	Задает интервал рассылки основных MLD-запросов.
no ipv6 mld query-interval		Восстанавливает значение по умолчанию
ipv6 mld query-max-response-time *value*	value: (5..20)/10 секунд	Задает максимальную задержку ответа, которая используется для вычислений кода максимальной задержки ответа
no ipv6 mld query-max-response-time		Восстанавливает значение по умолчанию
ipv6 mld robustness *value*	value: (1..7)	Устанавливает значение коэффициента отказоустойчивости. Если на канале наблюдается потеря данных, коэффициент отказоустойчивости должен быть увеличен.
no ipv6 mld robustness		Восстанавливает значение по умолчанию

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

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

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

Таблица 5.134 – Команды режима конфигурирования интерфейса Ethernet, группы интерфейсов

Команда	***Значение/Значение по умолчанию***	***Описание***
ipv6 mld join-group *ipv6_multicast_address*	-	Дает указание рассылать MLD-report сообщения на присоединение к *ipv6_address* группы с данного порта. - *ipv6_multicast_address* – групповой адрес IPv6.
no ipv6 mld join-group *ipv6_multicast_address*		Удаляет указание рассылать MLD-report сообщения на присоединение к *ipv6_multicast_address* группы с данного порта.
ipv6 mld version *version*	version: (1..2)/2	Устанавливает версию протокола, действующую на данном интерфейсе.
no ipv6 mld version		Восстанавливает значение по умолчанию

Таблица 5.135 – Команды режима EXEC

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

5.17.4 Функции ограничения multicast-трафика

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

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

`console(config)#`

Таблица 5.136 – Команды режима глобального конфигурирования

Команда	*Значение*	*Действие*
multicast snooping profile *name*	*name* : (1..32) символов	Переход в режим конфигурирования multicast-профиля.
no multicast snooping profile *name*		Удалить указанный multicast-профиль. **Multicast-профиль может быть удален только после того, как будет отвязан от всех портов коммутатора.**

Команды режима конфигурирования multicast-профиля

Вид запроса командной строки режима конфигурирования multicast-профиля:

`console(config-mc-profile)#`

Таблица 5.137 – Команды режима конфигурирования multicast-профиля

Команда	*Значение*	*Действие*
match ip *low_ip [high_ip]*	*low_ip:* валидный multicast-адрес *high_ip:* валидный multicast-адрес	Задает соответствие профиля указанному диапазону IPv4 multicast-адресов.
no match ip *low_ip [high_ip]*		Удаляет соответствие профиля указанному диапазону IPv4 multicast-адресов.
match ipv6 *low_ipv6 [high_ipv6]*	*low_ipv6:* валидный IPv6 multicast-адрес *high_ipv6:* валидный IPv6 multicast-адрес	Задает соответствие профиля указанному диапазону IPv6 multicast-адресов.
no match ipv6 *low_ipv6 [high_ipv6]*		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 конфигурирования интерфейса (диапазона интерфейсов) Ethernet

Вид запроса командной строки режима конфигурирования интерфейса:

`console(config-if)#`

Таблица 5.138 – Команды режима конфигурирования интерфейса (диапазона интерфейсов) Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
multicast snooping max-groups *number*	number: (1..1000)/-	Ограничивает количество одновременно просматриваемых multicast-групп для порта.
no multicast snooping max-groups		Снимает ограничение на количество одновременно просматриваемых групп для порта.
multicast snooping profile *name*	*name*: (1..32) символов	Привязывает указанный multicast-профиль к порту.
no multicast snooping profile		Удаляет соответствие multicast-профиля с портом.

Команды режима EXEC

Все команды доступны только для привилегированного пользователя.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.139 – Команды режима EXEC

Команда	*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 [*name***]**	Отображает информацию о сконфигурированных multicast-профилях.

5.17.5 Функция многоадресной маршрутизации 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.

IGMP Proxy поддерживает до 1024 групп многоадресной рассылки.

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 глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.140 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
ip multicast-routing igmp-proxy	По умолчанию функция выключена	Разрешает работу маршрутизации многоадресных данных на сконфигурированных интерфейсах.
ip igmp-proxy version *version*	version: (1..3)/2	Устанавливает версию протокола IGMP для использования коммутатором на uplink-интерфейсе. - *version* – версия IGMP-протокола.
ip igmp-proxy cos *cos*	cos: (0..7)/0	Устанавливает значение 802.1p для пакетов протокола

		IGMP, которое будет использоваться коммутатором на uplink-интерфейсе.
ip igmp-proxy dscp *dscp*	dscp: (0..63)/0	Устанавливает значение DSCP в IP заголовке для пакетов протокола IGMP, которое будет использоваться коммутатором на uplink-интерфейсе.

Команды режима конфигурирования интерфейса VLAN

Вид запроса командной строки режима конфигурирования VLAN:

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

Таблица 5.141 – Команды режима конфигурирования интерфейса VLAN

Команда	***Значение/Значение по умолчанию***	***Действие***
ip igmp-proxy vlan *vlan_id* **[version** *version***] [cos** *cos***] [dscp** *dscp***]**	vlan_id: (1..4094); version: (1..3)/2; cos: (0..7)/0; dscp: (0..63)/0	Конфигурируемая VLAN является интерфейсом к нижестоящей сети. Команда назначает связанный uplink-интерфейс, участвующий в маршрутизации. - *version* – версия протокола IGMP, которая будет использоваться коммутатором на этом интерфейсе; - *cos* – значение 802.1p для пакетов протокола IGMP, которое будет использоваться коммутатором на этом интерфейсе;. - dscp - значение DSCP в IP заголовке для пакетов протокола IGMP, которое будет использоваться коммутатором на этом интерфейсе.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.142 – Команды режима EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show ip mroute-next-hop [group *group* **| source** *source***]**	-	Команда предназначена для просмотра списков многоадресных групп. Возможен выбор групп по адресу группы или по адресу источника многоадресных данных. - *group* – IP-адрес группы; - *source* – IP-адрес источника многоадресных данных.
show ip igmp-proxy	-	Отображение информации об интерфейсе к вышестоящим сетям.
show ip igmp-proxy interface	-	Отображение информации об интерфейсах к нижестоящим сетям.

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

```
Interface Version No of Groups CoS DSCP
--------- ------- ------------ --- ----
 vlan 1      2         0        2   37
 vlan 30     2         0        5   12
```

Пример использования команд

Настроить на устройстве работу функции IGMP Proxy, использовать VLAN 100 в качестве интерфейса к вышестоящей сети 10.1.0.0, а VLAN 101 и 102 в качестве интерфейсов к

нижестоящим сетям 10.2.0.0 и 10.3.0.0 соответственно. На uplink-интерфейсе использовать версию v2 протокола IGMP.

```
console# configure
console (config)# vlan database
console (config)# vlan 100-102
console (config)# exit
console (config)# ip multicast-routing igmp-proxy
console (config)# ip igmp-proxy version 2
console (config)# interface vlan 100
console (config-if)# ip address 10.1.0.1 /24
console (config-if)# exit
console (config)# interface vlan 101
console (config-if)# ip igmp-proxy vlan 100
console (config-if)# ip address 10.2.0.1 /24
console (config-if)# exit
console (config)# interface vlan 102
console (config-if)# ip igmp-proxy vlan 100
console (config-if)# ip address 10.3.0.1 /24
console (config-if)# exit
console (config)#
```

5.18 Функции управления

5.18.1 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 глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.143 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
aaa authentication login {**default** | *list_name*} *method_list*	По умолчанию осуществляется проверка по локальной базе данных (**aaa authentication login default local**) list_name: (1..12) символов	Устанавливает способ аутентификации для входа в систему. - **default** – использовать для аутентификации описанные ниже методы; - *list_name* - имя списка аутентификационных методов, активизирующегося, когда пользователь входит в систему. Описание методов (method_list): - *enable* – использовать пароль для аутентификации; - *line* – использовать пароль терминала для аутентификации; - *local* – использовать локальную базу имен пользователей для аутентификации; - *none* – не использовать аутентификацию; - *radius* – использовать список RADIUS серверов для

		аутентификации; - *tacacs* – 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 mode {chain | break}	-/chain	Устанавливает алгоритм опроса методов аутентификации. - *chain* – после неудачной попытки аутентификации по первому методу в списке следует попытка аутентификации по следующему методу в цепочке. - *break* – после неудачной аутентификации по первому методу процесс аутентификации останавливается.
aaa authentication enable {**default** | *list_name*} *method_list*	По умолчанию осуществляется проверка пароля (**aaa authentication enable default enable**) list_name: 1..12 символов	Устанавливает способ аутентификации при повышении уровня привилегий для входа в систему. - **default** – использовать для аутентификации описанные ниже методы; - *list_name*- имя списка аутентификационных методов активизирующийся, когда пользователь входит в систему. Описание методов (method_list): - *enable* – использовать пароль для аутентификации; - *line* - использовать пароль терминала для аутентификации; - *none* – не использовать аутентификацию; - *radius* – использовать список RADIUS серверов для аутентификации; - *tacacs* – использовать список TACACS серверов для аутентификации. **Если для консоли пароль не определен, то доступ к консоли всегда успешный (aaa authentication enable default enable none).** **Создание списка осуществляется командой aaa authentication enable** list_name method_list**. Использование списка: aaa authentication enable** list_name **Все запросы, передаваемые к Radius и TACACS серверам, включают имя пользователя "$enabx$", где x – уровень привилегий.**
no aaa authentication enable {default | *list_name***}**		Устанавливает значение по умолчанию.
enable password [level *level***]** *password* **[encrypted]**	level: [1..15] password: [1..159] символов	Устанавливает пароль для контроля изменения привилегий доступа пользователей. - *level* – уровень привилегий; - *password* – пароль; - *encrypted* – 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* **} [priveliged** *level***]**	level: [1..15] password: [1..159] символов name: 1..20 символов	Добавляет пользователя в локальную базу данных. - *level* – уровень привилегий; - *password* – пароль; - *name* – имя пользователя; - *encrypted password* –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	По умолчанию ведение учета запрещено	Разрешает ведение учета (аккаунта) для сессий управления. **Ведение учета разрешено только для пользователей, вошедших в систему по имени и паролю, для пользователей, вошедших по паролю терминала, ведение учета запрещено.** **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 5.**144**).**
no aaa accounting login start-stop group radius		Устанавливает значение по умолчанию.
aaa accounting dot1x start-stop group radius	По умолчанию ведение учета запрещено	Разрешает ведение учета (аккаунта) для сессий 802.1x. **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 5.**144**).** **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).**
no aaa accounting dot1x start-stop group radius		Устанавливает значение по умолчанию.
ip http authentication aaa login-authentication *method_list*	method_list: local, none, tacacs, radius/local	Определяет метод аутентификации при доступе к HTTP-серверу. При установке списка методов, дополнительный метод будет применяться, только когда по основному методу аутентификации возвращена ошибка. - *method_list* – метод аутентификации: *local* –по имени из локальной базы данных; *none* – не используется; *tacacs* – использование списков всех серверов TACACS+; *radius* – использование списков всех RADIUS-серверов.
no ip http authentication aaa login-authentication		Устанавливает значение по умолчанию.
ip ftp authentication aaa login-authentication *method_list*	method_list: local, none, tacacs, radius/local	Определяет метод аутентификации при доступе к FTP-серверу. При установке списка методов, дополнительный метод будет применяться, только когда по основному методу аутентификации возвращена ошибка. - *method_list* – метод аутентификации: *local* –по имени из локальной базы данных; *none* – не используется; *tacacs* – использование списков всех серверов TACACS+; *radius* – использование списков всех RADIUS-серверов.
no ip ftp authentication aaa login-authentication		Устанавливает значение по умолчанию
aaa accounting commands stop-only default tacacs	По умолчанию ведение учета запрещено	Разрешает ведение учета (аккаунта) для введенных в CLI команд.
no aaa accounting commands stop-only default tacacs		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 5.144 – 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 5.145– Атрибуты сообщений ведения учета протокола RADIUS для сессий 802.1x

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.
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 конфигурирования терминала

Вид запроса командной строки в режиме конфигурирования терминала:

`console(config-line)#`

Таблица 5.146 – Команды режима конфигурирования терминальных сессий

Команда	*Значение/Значение по умолчанию*	*Действие*
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]**	1..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 5.147 – 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.
clear line *line*	line: (0..8)	Закрывает сессию удаленного управления. - *line* – номер сессии удаленного управления.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Все команды данного раздела доступны только для привилегированных пользователей.

Таблица 5.148 – Команды режима EXEC

Команда	*Действие*
show accounting	Показывает информацию о настроенных методах ведения учета (аккаунта).

5.18.2 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 глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

console(config)#

Таблица 5.149 - Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
radius-server host {*ip_address*| *hostname*} [**auth-port** *auth_port*] [**acct-port** *acct_port*] [**timeout** *timeout*] [**retransmit** *retries*] [**deadtime** *time*] [**key** *secret_key*] [**encrypted key** *encrypted_key*] [**source** *source_ip_address*] [**priority** *priority*] [**usage** *type*]	hostname: (1..158) символов; auth_port: (0..65535)/1812; acct_port: (0..65535)/1813; timeout: (1..30) сек; retries: (1..10); time (0..2000) мин; secret_key: (0..128) символов; encrypted key: (0..128) символов; priority: (0..65535)/0; type: (login, 802.1x, all)/ all В случае отсутствия в команде параметров timeout, retries, time, secret_key, source_ip_address для данного RADIUS-сервера используются значения настроенные с помощью команд указанных ниже (значения по умолчанию)	Добавляет указанный сервер в список используемых RADIUS серверов. - *ip_address* – IPv4 или IPv6-адрес RADIUS-сервера; - *hostname* – сетевое имя RADIUS-сервера; - *auth_port* – номер порта для передачи аутентификационных данных; - *acct_port* – номер порта для передачи данных учета; - *timeout* - интервал ожидания ответа от сервера; - *retries* - количество попыток поиска RADIUS-сервера; - *time* - время в минутах, в течение которого недоступные сервера не будут опрашиваться RADIUS-клиентом коммутатора; - *secret_key* – ключ для аутентификации и шифрования всего обмена данными RADIUS; - *encrypted key* – ключ для аутентификации и шифрования всего обмена данными RADIUS;- source ip-addr - IPv4 или IPv6-адрес, используемый в качестве адреса источника, передаваемого в сообщениях протокола RADIUS; - *priority* – приоритет использования RADIUS-сервера (чем ниже значение, тем приоритетнее сервер); - *type* – тип использования RADIUS-сервера.
no radius-server host {*ip_address*|*hostname*}		Удаляет указанный сервер из списка используемых RADIUS-серверов.
radius-server 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.
no radius-server key		Устанавливает значение по умолчанию.
radius-server timeout *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 *retries*	(1..10)/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 *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 *deadtime*		Устанавливает значение по умолчанию.
radius-server source-ip *ip_address*	-	Задает определенный IPv4-адрес, используемый по умолчанию в качестве адреса источника передаваемого в сообщениях протокола RADIUS.
no radius-server source-ip [*ip_address*]		Удаляет определенный IPv4-адрес, используемый по умолчанию в качестве адреса источника передаваемого в сообщениях протокола RADIUS. Устанавливает IPv4-адрес интерфейса коммутатора в качестве адреса источника для использования в сообщениях протокола RADIUS.
radius-server source-ipv6 *ip_address*	-	Задает определенный IPv6-адрес, используемый по умолчанию в качестве адреса источника передаваемого в сообщениях протокола RADIUS
no radius-server source-ipv6 [*ip_address*]		Удаляет определенный IPv6-адрес, используемый по умолчанию в качестве адреса источника передаваемого в сообщениях протокола RADIUS. Устанавливает IPv6-адрес интерфейса коммутатора в качестве адреса источника для использования в сообщениях протокола RADIUS.
radius-server attributes nas-id include-in-access-req format *nas_id*	nas_id: (1..32)/ атрибут 32 отсутствует в запросах	Добавление атрибута 32 (NAS-ID) в пакеты Radius-request. - *nas_id* – формат опции, макрос *%h* подставляет имя хоста коммутатора.
no radius-server attributes nas-id include-in-access-req format		Возвращает значение по умолчанию.

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 5.150 - Команды режима Privileged EXEC

Команда	***Действие***
show radius-servers	Отображает параметры настройки RADIUS серверов (Команда доступна только для привилегированных пользователей).
show radius statistics	Отображает статистику протокола Radius.

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
```

```
start

  IP address   Port  port   Tim    Ret-  Dead-   source IP  Prio.  Usage
```

```
                Auth  Acct   Out    rans  Time
------------- ----- -----  ------ ----- ------   ---------- -----  ----
 192.168.16.3  1645  1813  Global   2    Global    Global     0     all
 196.168.16.3  1645  1813  Global   2    Global    Global     0     all


Global values
--------------

TimeOut : 5
Retransmit : 5
Deadtime : 10
Source IP : 0.0.0.0
Source IPv6 : ::
```

5.18.3 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 глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

console(config)#

Таблица 5.151 - Команды режима глобального конфигурирования

Команда	***Значение/Значение по умолчанию***	***Действие***
tacacs-server host {*ip_address*|*hostname*} **[single-connection]** **[port** *port***]** **[timeout** *timeout***]** **[key** *secret_key***]** **[encrypted key** *encrypted_key***]** **[source** *source_ip_address***]** **[priority** *priority***]**	hostname: (1..158) символов; port: (0..65535)/49; timeout: (1..30) сек; retries: (1..10); time (0..2000) мин; key: (0..128) символов; encrypted_key: [0..128] символов; priority: (0..65535)/0; (значения по умолчанию)	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; - *key* – ключ для аутентификации и шифрования всего обмена данными TACACS; - *encrypted_key* – ключ в шифрованном виде для аутентификации и шифрования всего обмена данными TACACS; - *source ip_address* – IP-адрес, используемый в качестве адреса источника, передаваемого в сообщениях протокола TACACS; - *priority* – приоритет использования TACACS-сервера (чем ниже значение, тем приоритетнее сервер). В случае отсутствия в команде параметров *timeout, key, source_ip_address* для данного TACACS-сервера используются значения, настроенные с помощью команд, указанных ниже.

no tacacs-server host {*ip_address* | *hostname*}		Удаляет указанный сервер из списка используемых TACACS-серверов.
tacacs-server key [*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.
no tacacs-server key		Устанавливает значение по умолчанию.
tacacs-server timeout *timeout*	(1..30)/5 сек	Устанавливает интервал ожидания ответа от сервера, используемый по умолчанию.
no tacacs-server timeout		Установить значение по умолчанию.
tacacs-server source-ip *source_ip_address*	-	Задает IP-адрес коммутатора, используемый по умолчанию для обмена сообщениями с TACACS-сервером
no tacacs-server source-ip *source_ip_address*		Устанавливает использование IP-адреса интерфейса коммутатора для обмена сообщениями с TACACS-сервером.

Команды режима EXEC

Вид запроса командной строки в режиме EXEC:

```
console#
```

Таблица 5.152 - Команды режима EXEC

Команда	***Значение***	***Действие***
show tacacs [*ip_address*]	-	Отображает настройку и статистику для сервера TACACS+. - *ip_address* – IP-адрес TACACS+ сервера, либо имя сервера.
show tacacs statistics	-	Отображает статистику протокола TACACS+.

Примеры использования команд

Добавить в список серверов TACACS-сервер, расположенный на узле сети с IP-адресом 192.168.16.34, таймаут ожидания ответа от сервера – 4 секунды, секретный ключ для обмена данными с сервером – secret, IP-адрес коммутатора, используемый для обмена с этим сервером – 192.168.16.38, приоритет сервера – 8.

```
console# configure
console(config)# tacacs-server host 192.168.16.34 timeout 4 key secret
source 192.168.16.38 priority 8
```

5.18.4 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 серии MES3000 позволяет настроить работу протокола SNMP для удаленного мониторинга и управления устройством. Устройство поддерживает протоколы версий SNMPv1, SNMPv2, SNMPv3.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.153 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
system iftypes {*default* | *iana-new***}**	-	Изменяет отображение типов интерфейсов LAG и vlan, хранящихся в поле ifType таблицы ifTable. При вводе "system iftypes iana-new": - значение поля ifType для Port-Channel'ов в таблице ifTable отображается как ieee8023adLag; - значение поля ifType для Vlan'ов в таблице ifTable отображается как l2vlan. При вводе "system iftypes default": - значение поля ifType для Port-Channel'ов в таблице ifTable отображается как ethernetCsmacd; - значение поля ifType для Vlan'ов в таблице ifTable отображается как propVirtual. Для вступления в силу изменений после ввода команды требуется сохранение конфигурации и перезагрузка.
snmp-server server	По умолчанию поддержка протокола SNMP включена	Включить поддержку протокола SNMP.
no snmp-server server		Отключает поддержку протокола SNMP.
snmp-server community *community* [**view** *viewname*] **[ro|rw|su]** [*ipv4_address*| *ipv6_address*| *ipv6z_address*] [*mask* | *prefix_length*] [**use-acl** *ip-acl-name*] **snmp-server community-group** *community groupname* [*ipv4_address*|*ipv6_address*] [mask | prefix_length]	community: 1..20 символов viewname: 1..30 символов groupname: 1..30 символов *mask по умолчанию 255.255.255.255* prefix_length по умолчанию 32 ip-acl-name: 1..32 символов формат IPv4: A.B.C.D IPv6: X:X:X:X::X IPv6z: X:X:X:X::X%<ID>	Устанавливает значение строки сообщества для обмена данными по протоколу SNMP. - *community* – строка сообщества (пароль) для доступа по протоколу SNMP; - **ro** – доступ только для чтения; - **rw** – доступ для чтения и записи; - **su** – доступ администратора; - *viewname* – определяет имя для правила обозрения SNMP, которое должно быть предварительно определено с помощью команды **snmp-server view**. Определяет объекты, доступные сообществу; - *ipv4*_address, ipv6_address, ipv6z_address – IP-адрес устройства; - *mask* – маска адреса IPv4, которая определяет, какие биты адреса источника пакета сравниваются с заданным IP-адресом; - *prefix-length* – число бит, которые составляют префикс IPv4-адреса; - *ip-acl-name* – имя существующего ACL-списка; - *groupname* – определяет имя группы, которое должно быть предварительно определено с помощью команды **snmp-server group**. Определяет объекты, доступные сообществу.
no snmp-server community *community* [*ipv4_address*| *ipv6_address*| *ipv6z_address*]		Удаляет параметры для строки сообщества.
snmp-server view *view-name OID* {**included|excluded**}	View-name: (1..30) символов	Создает или редактирует правило обозрения для SNMP – разрешающее правило, либо ограничивающее серверу-обозревателю доступ к OID. OID–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 обозревания;

		- **exclude** – OID исключена из правила для обозревания.
no snmp-server view *viewname* [*OID*]		Удаляет правило обозрения для SNMP.
snmp-server group *groupname* **{v1|v2|v3 {noauth|auth|priv} [notify** *notifyview***]}** **[read** *readview***] [write** *writeview***]**	groupname: (1..30) символов notifyview: (1..30) символов readview: (1..30) символов writeview: (1..30) 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); - *notifyview* – имя правила обозрения, которому разрешено определять сообщения SNMP-агента – inform и trap; - *readview* – имя правила обозрения, которому разрешено только чтение содержимого SNMP-агента коммутатора; - *writeview* – 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 *username groupname* **{v1 | v2c | remote** *host* **v3 | v3** *[encrypted] [auth {md5 | sha} auth_password]***}**	username: (1..20) символов groupname: (1..30) символов engineid_string: (5..32) символов auth_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::X IPv6z: X:X:X:X::X%<ID>	Создает SNMPv3-пользователя. - *username* – имя пользователя; - *groupname* – имя группы; - *engineid_string* – идентификатор удаленного SNMP-устройства, которому пользователь принадлежит; - *auth_password* – пароль для аутентификации и генерации ключа; - *md5* – ключ md5; - *sha* – ключ sha; - *host* – IP-адрес/ имя хоста.
no snmp-server user *username* [**remote** *engineid_string*]		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 inform и trap-сообщения, передаваемые SNMP-серверу. - *filter_name* – имя SNMP-фильтра; - *oid* – 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 фильтрации; - **exclude** – OID исключена из правила фильтрации.
snmp-server filter *filter_name* [*oid*]		Удаляет правило SNMP-фильтра.
snmp-server host {*ipv4_address* | *ipv6_address*| *hostname*} [**traps**|**informs**] [**version** {**1** | **2c** | 3 [**auth** | **noauth** | **priv**]}] *community* [**udp-port** *port*] [**filter** *filtername*] [**timeout** *seconds*] [**retries** *retries*]	hostname: (1..158) символов community: (1..20) символов port: (1..65535)/162	Определяет настройки для передачи сообщений уведомления inform и trap SNMPv1/v2-серверу. - *community* – строка сообщества для передачи сообщений уведомления; - **version** – определят тип сообщений trap – trap SNMPv1, trap SNMPv2, trap SNMPv3;

	filtername: (1..30) символов seconds: (1..300)/15 retries: (0..255)/3	- **auth** – указывает подлинность пакета без шифрования; - **noauth** – не указывает подлинность пакета; - **priv** – указывает подлинность пакета с шифрованием; - *port* – UDP-порт SNMP-сервера; - *seconds* – период ожидания подтверждений перед повторной передачей сообщений inform; - *retries* – количество попыток передачи сообщений inform, при отсутствии их подтверждения.
no snmp-server host {*ipv4_address*|*ipv6_address*| hostname} [**traps**|**informs**]		Удаляет настройки для передачи сообщений уведомления inform и trap SNMPv1/v2/v3-серверу.
snmp-server v3-host {*ipv4_address*|*ipv6_address*|*hostname*} *username* [**traps** | **informs**] {**noauth**|**auth**| **priv**} [**udp-port** *port*] [**filter** *filtername*] [**timeout** *seconds*] [**retries** *retries*]	hostname: (1..158) символов username: (1..24) символов port: (1..65535)/162 filtername: (1..30) символов seconds: (1..300)/15 retries: (0..255)/3	Определяет настройки для передачи сообщений уведомления inform и trap SNMPv3-серверу. - **noauth**,**auth**,**priv** – тип аутентификации, используемый протоколом SNMP v3 (noauth – без аутентификации, auth – аутентификация без шифрования, priv – аутентификация с шифрованием); - *port* – UDP-порт SNMP-сервера; - *seconds* – период ожидания подтверждений перед повторной передачей сообщений inform; - *retries* – количество попыток передачи сообщений inform, при отсутствии их подтверждения.
no snmp-server v3-host {*ipv4_address*|*ipv6_address*| *hostname*} *username* [**traps**|**informs**]		Удаляет настройки для передачи сообщений уведомления inform и trap SNMPv3-серверу.
snmp-server engineid local {*engineid_string* | **default**}	*engineid_string*: (5..32) символов	Создает идентификатор локального SNMP устройства – engineID. - *engineid_string* – 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 engineid remote **{***ipv4_address* **|** *ipv6_address***}** *engineid_string*	(5..32) символов	Создает идентификатор удаленного SNMP устройства – engine ID. - *engineid_string* – имя SNMP-устройства.
no snmp-server engineID remote **{***ipv4_address* **|** *ipv6_address***}**		Удаляет идентификатор удаленного SNMP устройства – engine ID.
snmp-server enable traps	-/enabled	Включает поддержку SNMP trap-сообщений.
no snmp-server enable traps		Отключает поддержку SNMP trap-сообщений.
snmp-server enable traps errdisable	-/disabled	Включает отправку SNMP trap-сообщений при переводе порта в состояние Errdisable.
no snmp-server enable traps errdisable		Выключает отправку SNMP trap-сообщений при переводе порта в состояние Errdisable.
snmp-server enable traps erps	-/enabled	Включает отправку SNMP trap-сообщений при изменении состояния ERPS-кольца.
no snmp-server enable traps erps		Отключает отправку SNMP trap-сообщений при изменении состояния ERPS-кольца.
snmp-server enable traps flex-link	-/enabled	Включает отправку SNMP trap-сообщений при изменении состояния пары flex-link интерфейсов.
no snmp-server enable traps flex-link		Отключает отправку SNMP trap сообщений при изменении состояния пары flex-link-интерфейсов.
snmp-server enable traps link-status	-/enabled	Включает отправку SNMP trap сообщений при изменении состояния порта.

no snmp-server enable traps link-status		Отключает отправку SNMP trap сообщений при изменении состояния порта.
snmp-server enable traps mac-notification change	-/disabled	Включает отправку SNMP trap сообщений при изменении в таблице изученных MAC-адресов.
no snmp-server enable traps mac-notification change		Отключает отправку SNMP trap сообщений при изменении в таблице изученных MAC-адресов.
snmp-server enable traps mac-notification flapping	-/enabled	Включает отправку SNMP trap сообщений при обнаружении флаппинга MAC-адресов.
no snmp-server enable traps mac-notification flapping		Отключает отправку SNMP trap сообщений при обнаружении флаппинга MAC-адресов.
snmp-server enable traps l2protocol-tunnel	-/ disabled	Включает отправку SNMP trap сообщений при срабатывании drop-treshold и shutdown-treshold в L2PT.
no snmp-server enable traps l2protocol-tunnel		Отключает отправку SNMP trap сообщений в L2PT.
snmp-server enable traps storm-control	-/enabled	Включает отправку SNMP trap сообщений при обнаружении широковещательного шторма.
no snmp-server enable traps storm-control		Выключает отправку SNMP trap сообщений при обнаружении широковещательного шторма.
snmp-server trap authentication	-	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*	(1..160) символов	Определяет контактную информацию устройства.
no snmp-server contact		Удаляет контактную информацию устройства.
snmp-server location *text*	(1..160) символов	Определяет информацию о местоположении устройства.
no snmp-server location		Удаляет информацию о местоположении устройства.
snmp-server set *variable_name name1 value1* [*name2 value2* …]	variable_name, name, value должны задаваться в соответствии со спецификацией	Позволяет установить значения переменных в базе данных MIB коммутатора. - *variable_name* – имя переменной; - *name*, *value* – пары соответствий имя – значение.

Команды режима конфигурирования интерфейса (диапазона интерфейсов) Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet:

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

Таблица 5.154 – Команды режима конфигурирования интерфейса Ethernet

Команда	***Действие***
snmp trap link-status	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#
```

Таблица 5.155 – Команды режима Privileged EXEC

Команда	*Действие*
show snmp	Показывает статус SNMP-соединений.
show snmp engineID	Показывает идентификатор локального SNMP-устройства – engineID.
show snmp views [*viewname***]**	Показывает правила обозрения SNMP.
show snmp groups [*groupname*]	Показывает SNMP-группы.
show snmp filters [*filtername*]	Показывает SNMP-фильтры.
show snmp users [*username*]	Показывает SNMP-пользователей.

Примеры выполнения команд

Установить значения для параметров contact, location. Установить доступ на чтение для строки сообщества public. Установить доступ на чтение и запись SNMP-серверу с адресом 192.168.16.3 в сообществе private.

```
console# configure
console (config)# snmp-server enable
console (config)# snmp-server contact support@eltex.nsk.ru
console (config)# snmp-server location "Okruzhnaya 29v"
console (config)# snmp-server community public ro
console (config)# snmp-server community private rw 192.168.16.3
```

5.18.5 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 глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.156 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
rmon event *index type* [**community** *text*] [**description** *text*] [**owner** *name*]	index: (1..65535) community text: (0..127) символов description text: (0..127) символов owner name: строка	Настраивает события, используемые в системе удаленного мониторинга. - *index* – индекс события; - *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; - **description** – описание события; - **owner** – имя создателя события.
no rmon event *index*		Удаляет событие, используемое в системе удаленного мониторинга.
rmon alarm *index mib_object_id interval rthreshold fthreshold revent fevent* [**type** *type*] [**startup**	index: (1..65535) mib_object_id: корректный OID;	Настраивает условия выдачи аварийных сигналов. - *index* – индекс аварийного события; - *mib_object_id* – идентификатор переменной части объекта OID; - *interval* – интервал, в течение которого данные

direction] [**owner** *name*]	interval: (1..4294967295) сек rthreshold: (0..4294967295) fthreshold: (0..4294967295) revent: (0..65535) fevent: (0..65535) owner name: строка По умолчанию метод отбора переменных – absolute По умолчанию инструкция для генерации событий rising-falling	отбираются и сравниваются с восходящей и нисходящей границами; - *rthreshold* – восходящая граница; - *fthreshold* – нисходящая граница; - *revent* – индекс события, которое используется при пересечении восходящей границы; - *fevent* – индекс события, которое используется при пересечении нисходящей границы; **-** *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** – 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; - **owner** – имя создателя аварийного события.
no rmon alarm *index*		Удаляет условие выдачи аварийных событий.
rmon table-size **{history** *entries* | **log** *entries***}**	history (20..32767)/270 log (20..32767)/100	Задает максимальный размер RMON-таблиц. - **history** – максимальное количество строк в таблице истории; - **log** – максимальное количество строк в таблице записей. **Значение вступит в силу только после перезагрузки устройства.**
no rmon table-size **{history** | **log}**		Устанавливает значение по умолчанию.

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

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

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

Таблица 5.157– Команды режима конфигурирования интерфейса Ethernet, группы интерфейсов

Команда	***Значение***	***Действие***
rmon collection stats *index* **[owner** *name* **|** **buckets** *bucket_num***]** **[interval** *interval***]**	index: (1..65535); name: корректная строка; bucket-num: (1..50)/50;	Включает формирование истории по группам статистики для базы данных (MIB) удаленного мониторинга. - *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*	interval: (1..3600)/1800 сек	Выключает формирование истории по группам статистики для базы данных (MIB) удаленного мониторинга.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

console>

Таблица 5.158 – Команды режима EXEC

Команда	***Значение***	***Действие***
show rmon statistics { gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group* **}**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Показывает статистику интерфейса Ethernet, либо группы портов, используемую для удаленного мониторинга.
show rmon collection stats [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group* **]**		Отображает информацию по запрашиваемым группам статистики.
show rmon history *index* **{throughput | errors | other} [period** *period***]**	index: (1..65535) period: (1..2147483647) сек	Показывает историю Ethernet статистики RMON. - *index* – запрошенная группа статистики; - **throughput** – показывает счетчики производительности (пропускной способности); - **errors** – показывает счетчики ошибок; - **other** – показывает счетчики обрывов и коллизий; - *period* – показывает историю за запрошенный период времени.
show rmon alarm-table	-	Показывает сводную таблицу аварийных событий.
show rmon alarm *number*	(1..65535)	Показывает конфигурацию настройки аварийных событий. - *number* – индекс аварийного события.
show rmon events	-	Показывает таблицу событий удаленного мониторинга RMON.
show rmon log [*event*]	(0..65535)	Показывает таблицу записей удаленного мониторинга RMON. - *event* - индекс события.

Примеры выполнения команд

- Показать статистику 10 интерфейса Ethernet:

console# **show rmon statistics gigabitethernet** 1/0/10

```
Port gi0/10
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 5.159 - 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 gigabitethernet** *1/0/8*

```
Index Interface Interval Requested Samples Granted Samples        Owner
----- --------- -------- ----------------- --------------- --------------------
  1      gi0/8     300           50               50                Eltex
```

Таблица 5.160 - 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: gi0/1           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 5.161 - Описание результатов

Параметр	***Описание***
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 5.162 - 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 5.163 - 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 большем либо равном 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 большем либо равном 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 использующегося, когда восходящая граница пересечена.
Falling Event	Индекс события использующегося, 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                           CLINov 10 2009 18:47:17
2      High Broadcast Log-Trap    router       Manager    Nov 10 2009 18:48:48
```

Таблица 5.164 – 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 5.165 – Описание результатов

Параметр	*Описание*
Index	Индекс, уникально идентифицирующий запись.
Description	Комментарий, описывающий событие.
Time	Время создания записи.

5.18.6 Списки доступа ACL для управления устройством

Программное обеспечение коммутаторов серии MES3000 позволяет разрешить либо ограничить доступ к управлению устройством через определенные порты или группы VLAN. Для этой цели создаются списки доступа (ACL) для управления.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

console(config)#

Таблица 5.166 – Команды режима глобального конфигурирования

Команда	*Значение*	*Действие*
management access-list *name*	(1..32) символа	Создает список доступа для управления. Вход в режим конфигурирования списка доступа для управления.
no management access-list *name*		Удаляет список доступа для управления.
management access-class {**console-only** | *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 конфигурирования списка доступа для управления

Вид запроса командной строки в режиме конфигурирования списка доступа для управления:

console(config)# **management access-list** *eltex_manag*
console (config-macl)#

Таблица 5.167 – Команды режима конфигурирования списка доступа для управления

Команда	*Значение*	*Действие*
permit **[gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***| vlan** *vlan_id***]** [**service** *service*]	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12); vlan_id(1..4094)	Задает разрешающее условие для управляющего списка доступа. - *service* – тип доступа – Telnet, SSH, SNMP, HTTP, HTTPS.
permit ip-source {*ipv4_address* | *ipv6_address/prefix_length*} [**mask** {*mask*| *prefix_length*}] **[gigabitethernet** *gi_port* **|**		

tengigabitethernet *te_port* **|port-channel** *group***|vlan** *vlan_id***]** [**service** *service*]		
deny **[gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***|vlan** *vlan_id***]** [**service** *service*]	gi_port: (1..8/0/1..24}; te_port: (1..8/0/1..4}; group: (1..12); vlan_id: (1..4094)	Задает запрещающее условие для управляющего списка доступа. - *service* – тип доступа – Telnet, SSH, SNMP, HTTP, HTTPS.
deny ip-source {*ipv4_address* | *ipv6_address/prefix_length*} [**mask** {*mask*| *prefix_length*}] **[gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***| vlan** *vlan_id***]** [**service** *service*]		

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 5.168 – Команды режима Privileged EXEC

Команда	***Действие***
show management access-list [*name*]	Показывает списки доступа (access list) для управления.
show management access-class	Показывает информацию об активных списках доступа (access list) для управления.

5.18.7 Настройка доступа

5.18.7.1 Telnet, SSH, HTTP и FTP

Данные команды предназначены для настройки серверов доступа для управления коммутатором. Поддержка серверов TELNET и SSH коммутатором позволяет удаленно подключаться к нему для мониторинга и конфигурирования.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.169 – Команды режима глобального конфигурирования

Команда	***Значение/Значение по умолчанию***	***Действие***
ip telnet server	По умолчанию Telnet сервер включен.	Разрешает удаленное конфигурирование устройства через Telnet.
no ip telnet server		Запрещает удаленное конфигурирование устройства через Telnet.
ip ssh server	По умолчанию SSH сервер включен.	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 crypto key generate rsa и crypto key generate dsa) сервер перейдет в рабочее состояние.
no ip ssh server		Запрещает удаленное конфигурирование устройства через SSH.
ip ssh port *port_number*	(1..65535)/22	TCP-порт, используемый SSH-сервером.
no ip ssh port		Устанавливает значение по умолчанию.
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 password-auth	По умолчанию отключено	Включение режима аутентификации по паролю
no ip ssh password-auth		Отключение режима аутентификации по паролю
crypto key pubkey-chain ssh	По умолчанию ключ не создан	Вход в режим конфигурации публичного ключа.
crypto key generate dsa	-	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 rsa	-	Генерирует пару ключей RSA – частный и публичный для SSH-сервиса. **Если хотя бы один из пары ключей уже создан, то система предложит перезаписать ключ.**
ip ftp server	По умолчанию FTP-сервер включен	Включает FTP-сервер.
no ip ftp server		Отключает FTP-сервер.
ip http port *port*	1..65535/80	Задает порт HTTP-сервера.
no ip http port		Восстанавливает значение по умолчанию.
ip http secure-port *port*	1..65535/443	Задает порт HTTPS-сервера.
no ip http secure-port		Восстанавливает значение по умолчанию.
ip http secure-server	По умолчанию HTTPS-сервер выключен	Включает HTTPS-сервер.
no ip http secure-server		Выключает HTTPS-сервер.
ip http server	По умолчанию HTTP-сервер включен	Включает HTTP-сервер.
no ip http server		Выключает HTTP-сервер.
ip http timeout-policy *seconds*	0..86400/600	Задает таймаут HTTP-сессии.
no ip http timeout-policy		Восстанавливает значение по умолчанию.
Ip https certificate {1|2}	1	Определяет активный HTTPS-сертификат.
crypto certificate {1|2} generate		Генерирует SSL-сертификат.
crypto certificate {1|2} import		Импортирует SSL-сертификат, назначенный центром сертификации.

Ключи, сгенерированные командами crypto key generate rsa и crypto key generate dsa, сохраняются в закрытом для пользователя файле конфигурации.

Команды режима конфигурирования публичного ключа

Вид запроса командной строки в режиме конфигурирования публичного ключа:

```
console# configure
console(config)# crypto key pubkey-chain ssh
console(config-pubkey-chain)#
```

Таблица 5.170 – Команды режима конфигурирования публичного ключа

Команда	*Значение*	*Действие*
user-key *username* {**rsa**|**dsa**}	(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 5.171 – Команды режима создания индивидуального публичного ключа

Команда	*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 key-string row без символов.**

Команды режима EXEC

Команды данного раздела доступны только для привилегированных пользователей.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.172 – Команды режима EXEC

Команда	*Значение*	*Действие*
show ip ssh	-	Показывает конфигурацию SSH-сервера, а также активные входящие SSH-сессии.
show crypto key pubkey-chain ssh [**username** *username*] [**fingerprint** {**bubble-babble** | **hex**}]	(1..48) символов. По умолчанию отпечаток ключа в шестнадцатеричном формате.	Показывает публичные SSH-ключи, сохраненные на коммутаторе. - *username* – имя удаленного клиента; - **bubble-babble** – отпечаток ключа в коде Bubble Babble; - **hex** – отпечаток ключа в шестнадцатеричном коде.
show crypto key mypubkey [**rsa** | **dsa**]	-	Показывает публичные ключи SSH-коммутатора.
show crypto certificate mycertificate [1|2]	-	Отображает SSL-сертификаты для HTTPS-севера
show ip http	-	Отображает состояние HTTP-сервера
show ip https	-	Отображает состояние HTTPS-сервера

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
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWlAl4kpqIw9GBRonZQZxjHKcqKL6rMlQ+ZN
XfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1gkTwm
l75QR9gHujS6KwGN2QWXgh3ub8gDjTSqmuSn/Wd05iDX2IExQWu08licglk02LYciz+Z4TrE
U/9FJxwPiVQOjc+KBXuR0juNg5nFYsY0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA6w9o44t6
```

```
+AINEICBCCA4YcF6zMzaT1wefWwX6f+Rmt5nhhqdAtN/4oJfce166DqVX1gWmNzNR4DYDvSz
g0lDnwCAC8Qh
Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

5.18.7.2 Команды конфигурирования терминала

Команды конфигурирования терминала служат для настройки параметров локальной и удаленной консоли.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.173 – Команды режима глобального конфигурирования

Команда	***Действие***
line {console|telnet|ssh}	Вход в режим соответствующего терминала (локальная консоль, удаленная консоль – Telnet или удаленная защищенная консоль – SSH).

Команды режима конфигурирования терминала

Вид запроса командной строки в режиме конфигурирования терминала

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

Таблица 5.174 – Команды режима конфигурирования терминала

Команда	***Значение/Значение по умолчанию***	***Действие***
speed *bps*	2400, 9600, 19200, 38400, 57600, 115200/115200 бод	Устанавливает скорость доступа по локальной консоли (команда доступна только в режиме конфигурирования локальной консоли).
no speed		Устанавливает значение по умолчанию.
autobaud	-	Включает автоматическое определение скорости доступа по локальной консоли (команда доступна только в режиме конфигурирования локальной консоли).
no autobaud		Выключает автоматическое определение скорости доступа по локальной консоли.
exec-timeout *minutes* [*seconds*]	*minutes:* (0..65535) мин *seconds:* (0..59) сек По умолчанию 10 минут	Задает 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 5.175 – Команды режима EXEC

Команда	***Действие***
show line [console|telnet|ssh]	Показывает параметры терминала.

5.19 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 5.176 - Команды режима глобальной конфигурации

Команда	***Значение/Значение по умолчанию***	***Действие***
logging on	-/ регистрация включена	Включает регистрацию отладочных сообщений и сообщений об ошибках.
no logging on		Выключает регистрацию отладочных сообщений и сообщений об ошибках. **При выключенной регистрации отладочные сообщения и сообщения об ошибках будут передаваться на консоль.**
logging host {*ip_address*|*host*} [**port** *port*] [**severity** *level*] [**facility** *facility*] [**description** *text*]	host: (1..158) символов; port: (1..65535)/514; level: (см. табл. 6.101); facility: (local0..7)/ local7; text: (1..64) символов	Включает передачу аварийных и отладочных сообщений на удаленный SYSLOG сервер. - *ip_address*– IPv4 или IPv6-адрес SYSLOG-сервера; - *host* – сетевое имя SYSLOG-сервера; - *port* – номер порта для передачи сообщений по протоколу SYSLOG; - *level* – уровень важности сообщений, передаваемых на SYSLOG-сервер; - *facility* – услуга, передаваемая в сообщениях; - *text* – описание SYSLOG-сервера.
no logging host {*ip_address*|*host*}		Удаляет выбранный сервер из списка используемых SYSLOG-серверов.
logging console *level*	level: (см. табл. Таблица 5.177 – Типы важности сообщений) Значение по умолчанию - 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 [*severity_level*]	severity_level: (см. табл. Таблица 5.177 – Типы важности сообщений) Значение по умолчанию – 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 buffered size *size*	(20..400)/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 *level*	level: (см. табл. Таблица 5.177 – Типы важности сообщений) Значение по умолчанию – 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	-/enable	Заносить в журналы события аутентификации, авторизации и учета (AAA).
no aaa logging login		Не заносить в журналы события аутентификации, авторизации и учета (AAA).
logging events spanning-tree	-/enabled	Включает регистрацию изменения статуса интерфейсов в STP.

port-state-change		
no logging events spanning-tree port-state-change		Отключает регистрацию изменения статуса интерфейсов в STP.
logging events spanning-tree topology-change	-/disable	Включает регистрацию изменений топологии в STP.
no logging events spanning-tree topology-change		Отключает регистрацию изменений топологии в STP.
file-system logging {copy | delete-rename}	По умолчанию регистрация включена	Включает регистрацию событий файловой системы. - **copy** – регистрация сообщений, связанных с операциями копирования файлов; - **delete-rename** – регистрация сообщений, связанных с удалением файлов и переименованием операций.
no file-system logging {copy | delete-rename}		Выключает регистрацию событий файловой системы.
management logging deny	По умолчанию регистрация включена	Включает регистрацию событий доступа управления.
no management logging deny		Выключает регистрацию событий доступа управления.
logging aggregation on	-	Включает контроль агрегации syslog-сообщений.
no logging aggregation on		Отключает агрегацию syslog-сообщений.
logging aggregation aging-time *sec*	(15..3600)	Устанавливает время хранения сгруппированных syslog-сообщений.
no logging aggregation aging-time		Устанавливает значение по умолчанию.
logging cli-commands	По умолчанию ведение учета запрещено	Разрешает ведение учета (аккаунта) для введенных в CLI команд.
no logging cli-commands		Устанавливает значение по умолчанию.
logging service cpu-rate-limits *traffic*	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 фреймов для определенного типа трафика.
no logging service cpu-rate-limits *traffic*		Отключает логирование.

Каждое сообщение имеет свой уровень важности, в таблице 6.101 приведены типы сообщений в порядке убывания их важности.

Таблица 5.177 – Типы важности сообщений

Тип важности сообщений	***Описание***
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 5.178 – Команда режима Privileged EXEC для просмотра файла журнала

Команда	*Действие*
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
```

5.20 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.

При зеркалировании более одного физического интерфейса возможны потери трафика. Отсутствие потерь гарантируется только при зеркалировании одного физического интерфейса.

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.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 5.179 - Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
port monitor mode {monitor-only|network}	-/monitor-only	Задает режим работы порта - **monitor-only –** фреймы, поступающие на порт, отбрасываются; - **network –** позволяет вести обмен данными.

port monitor remote vlan *vlan_id* [cos *priority*] **[tx|rx]**	vlan_id: 1..4094 priority: 0..7	Определение VLAN для удаленного мониторинга, в который будут отображаться пакеты с контролируемых интерфейсов.
no port monitor remote vlan *vlan_id***[tx|rx]**		Удаление VLAN для удаленного мониторинга.

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet:

`console(config-if)#`

Данные команды нельзя выполнять в режиме конфигурирования диапазона интерфейсов Ethernet.

Таблица 5.180 - Команды доступные в режиме конфигурирования интерфейса Ethernet

Команда	***Значение/Значение по умолчанию***	***Действие***
port monitor {gigabitethernet *gi_port* **| tengigabitethernet** *te_port***} [rx|tx]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4)	Включает функцию мониторинга на настраиваемом интерфейсе. Данный интерфейс будет контролирующим портом для указанного в команде контролируемого порта. - *gi_port/te_port*– контролируемый порт; - **rx** – копировать пакеты принятые контролируемым портом; - **tx** – копировать пакеты, переданные контролируемым портом; При отсутствии параметра rx/tx с контролируемого порта копируются все пакеты. **Функция мониторинга может быть настроена на двух портах одновременно**
no port monitor { gigabitethernet *gi_port* **| tengigabitethernet** *te_port***}**		Выключает функцию мониторинга на настраиваемом интерфейсе. Данный интерфейс больше не будет контролирующим портом для указанного в команде контролируемого порта.
port monitor vlan *vlan_id*	vlan_id: (1..4096)	Включает функцию мониторинга на настраиваем интерфейсе. Данный интерфейс будет контролирующим портом для указанной VLAN. **Порт мониторинга не должен принадлежать к настраиваемой VLAN.** Мониторинг VLAN может быть включен лишь в том случае, если в системе настроено не более одного контролирующего порта. **Если контролирующий порт настроен ранее, то только этот порт может быть использован для мониторинга VLAN.**
no port monitor vlan *vlan_id*		Удаляет указанную VLAN из мониторинга.
port monitor remote	-	Включает функцию удаленного мониторинга на настраиваемом интерфейсе.
no port monitor remote		Выключает функцию удаленного мониторинга на настраиваемом интерфейсе.

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

`console>`

Таблица 5.181 – Команды, доступные в режиме EXEC

Команда	*Действие*
show ports monitor	Выводит информацию по контролирующим и контролируемым портам.

Примеры выполнения команд

- Установить 13 Ethernet интерфейс контролирующим для 18 интерфейса Ethernet. Весь трафик с 18 интерфейса передавать на 13.

```
console# configure
console(config)# interface gigabitethernet 1/0/13
console(config-if)# port monitor gigabitethernet 1/0/18
```

- Вывести информацию по контролирующим и контролируемым портам.

```
console# show ports monitor
```

```
Source Port Destination Port  Type     Status
----------- ---------------- ------- ----------
    gi0/18           gi0/13         RX,TX   notReady
```

5.21 Функция sFlow

sFlow – технология, позволяющая мониторить трафик 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 5.182 - Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
sflow receiver *id* {ipv4_address|ipv6_address| ipv6z_address|url} [port *port*] [max-datagram-size *byte*]	id: (1 .. 8) port: (1 .. 65535) / 6343 byte: положительное целое число /1400 формат IPv4: A.B.C.D IPv6: X:X:X:X::X IPv6z: X:X:X:X::X%<ID>	Задает адрес сервера сбора статистики sflow. - *id* – номер sflow-сервера; - *IPv4, IPv6, IPv6z* – IP-адрес; - *url* – доменное имя хоста; - *port* – номер порта; - *byte* – максимальное количество байт, которое может быть отправлено в один пакет данных.
no sflow receiver *id*		Удаляет адрес сервера сбора статистики sflow

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet:

```
console# configure
console(config)# interface {gigabitethernet gi_port| tengigabitethernet
te_port}
console(config-if)#
```

Таблица 5.183 – Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
sflow flow-sampling *rate id* [**max-header-size** *bytes*]	rate: (0, 1024..107374823) id: (0 .. 8) bytes: (20 .. 256)/128	Задает среднюю скорость выборки пакетов. Итоговая скорость выборки считается как 1/rate*current_spped (current_speed – текущая средняя скорость). - *rate* – средняя скорость выборки пакетов; - *id* – номер sflow-сервера; - *bytes* – максимальное количество байт, которое будет скопировано из образца пакета.
no sflow flow-sampling		Отключает счетчики выборки на порту.
sflow counters-sampling *sec id*	sec: (0, 15 .. 86400) id: (0 .. 8)	Определяет максимальный интервал между успешными выборками пакетов. - *sec* - максимальный интервал между выборками, секунды. Значение «0» отключает выборку; - *id* - номер sflow-сервера (задается командой sflow receiver в глобальном режиме конфигурации).
no sflow counters-sampling		Отключает счетчики выборки на порту.

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 5.184 – Команды, доступные в режиме EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show sflow configuration [gigabitethernet *gi_port* **| tengigabitethernet** *te_port***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4)	Выводит настройки sflow.
clear sflow statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port***]**		Очищает статистику sFlow. Если интерфейс не указан, команда очищает все счетчики статистики sFlow.
show sflow statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port***]**		Отображает статистику sFlow.

Примеры выполнения команд

- Установить IP-адрес 10.0.80.1 сервера 1 для сбора статистики sflow. Для ethernet-интерфейсов g1-g24 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 gigabitethernet 1/0/1-24
console(config-if-range)# sflow flowing-sample 1 10240
console (config-if)# sflow counters-sampling 240 1
```

5.22 Функции диагностики физического уровня

Сетевые коммутаторы серии MES3000 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.

5.22.1 Диагностика медного кабеля

Оценка длины кабеля при использовании команды *'show cable-diagnostics cable-length'* выполняется по величине затухания сигнала. Функция green-ethernet, поддерживаемая коммутатором, уменьшает уровень передаваемого сигнала при отсутствии активности на линии и поэтому корректное измерение длины кабеля становится невозможным на устройстве, принимающем ослабленный сигнал. В связи с этим необходимо на время измерений длины кабеля отключать режим green-ethernet на удаленном устройстве.

По умолчанию на коммутаторах серии MES3000 режим green-ethernet включен. Допустимая погрешность измерения определяется разбросом параметров линии и составляет 6 м.

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 5.185 - Команды диагностики медного кабеля

Команда	*Значение*	*Действие*
test cable-diagnostics tdr interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port***}**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Выполняет виртуальное тестирование кабеля для указанного интерфейса.

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 5.186 - Команды диагностики медного кабеля

Команда	*Значение*	*Действие*
show cable-diagnostics tdr [interface gigabitethernet *gi_port* **| interface tengigabitethernet** *te_port***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Отображает результаты последнего виртуального тестирования кабеля для указанного интерфейса (если номер порта не задан, то команда выполняется для всех портов).
show cable-diagnostics cable-length [interface gigabitethernet *gi_port* **|interface tengigabitethernet** *te_port***]**		Отображает 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 100Мбит/с или 1000Мбит/с.**

Максимальная длина кабеля при тестировании не должна составлять более 120 метров.

Примеры выполнения команд:

- Протестировать порт 24:

console# **test cable-diagnostics tdr interface gigabitethernet** 1/0/24

```
console#test cable-diagnostics tdr interface GigabitEthernet0/24
..
 Port     Pair Result              Length [m] Date
--------- ---- ------------------- ---------- --------------------------
gi1/0/24  1-2         Open             10      14-Mar-2014 13:41:43
          3-6         Open             10
          4-5         Open             10
          7-8         Open             10
```

Ниже приведены возможные значения результатов теста по парам:

- Test failed – физическая неисправность;
- OK – пара в порядке;
- Open – разрыв;
- Short – контакты пары замкнуты;
- Impedance-mismatch – разница в сопротивлении (слишком большое затухание в линии);
- Short-with-pair – замыкание между парами;
- Not tested – тестирование не проводилось.

Показать результаты последнего тестирования:

console# **show cable-diagnostics tdr**

```
console#show cable-diagnostics tdr

   Port         Result      Length [meters]             Date
----------- --------------- ---------------- --------------------------
  gi1/0/1         OK               --          14-Mar-2014 13:48:12
  gi1/0/2     Not tested
  gi1/0/3     Not tested
  gi1/0/4     Short cable          4           14-Mar-2014 13:51:08
  gi1/0/5     Not tested
  gi1/0/6     Not tested
  gi1/0/7     Not tested
  gi1/0/8     Not tested
  gi1/0/9     Not tested
 gi1/0/10     Not tested
 gi1/0/11     Not tested
 gi1/0/12     Not tested
 gi1/0/13     Not tested
 gi1/0/14     Not tested
 gi1/0/15     Not tested
 gi1/0/16     Not tested
 gi1/0/17     Not tested
 gi1/0/18     Not tested
 gi1/0/19     Not tested
 gi1/0/20     Not tested
 gi1/0/21     Not tested
 gi1/0/22     Not tested
 gi1/0/23     Not tested
 gi1/0/24     Open cable               10          14-Mar-2014 13:41:43
```

```
te1/0/1        Fiber
te1/0/2        Fiber
te1/0/3        Fiber
te1/0/4        Fiber
```

5.22.2 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. В случае необходимости пороговые значения могут быть переопределены администратором.

Вид запроса командной строки в режиме глобальной конфигурации:

console(config)#

Таблица 5.187 - Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
optical-transceiver threshold notify-interval interval	interval: (30..3600)/600 сек	Устанавливает минимальный интервал времени между формированием информационных сообщений syslog/snmp. Сообщения формируются в случае выхода параметров оптической линии за допустимые пределы.
no optical-transceiver threshold notify-interval		Устанавливает значение интервала по умолчанию.

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet:

console# **configure**
console(config)# **interface** {**gigabitethernet** *gi_port*| **tengigabitethernet** *te_port*}
console(config-if)#

Таблица 5.188 – Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
optical-transceiver threshold action { *parameter* **| all** } { **none | syslog | snmp-trap** }	parameter: (current, input-power, output-power, temperature, voltage)	Назначает действие (не выполнять действий, генерация syslog-сообщения, генерация snmp-трапа), которое должно быть выполнено при выходе параметра «*parameter*» за допустимые пределы. Действие по умолчанию «*none*». Возможные типы параметров - current –ток питания трансивера; - voltage – напряжение питания. - input-power – мощность оптического сигнала на приёме; - output-power – мощность передаваемого оптического сигнала; - temperature – температура.

optical-transceiver threshold values *parameter high-alarm high-warning low-warning low-alarm*	parameter: (current, input-power, output-power, temperature, voltage)	Указывает пороговые значения, при превышении которых будет происходить генерация syslog/snmp сообщения для указанного параметра. - *high-warning*, *low-warning* - верхний и нижний пределы для формирования предупреждающих сообщений; - *high-alarm*, *low-alarm* - верхний и нижний пределы для формирования аварийных сообщений. Допустимый диапазон значений для параметров: current: 0…131000 мкА input-power: -40000…8200 mdBm output-power: -40000-8200 mdBm temperature: -127…127 °C voltage: 0…6550 000 мкВ Пороговые значения задаются в указанных единицах.
no optical-transceiver threshold values *parameter*		Удаляет заданные пользователем пороговые значения для указанного параметра. Значения по умолчанию считываются из трансивера при установке.

Запрос командной строки в режиме EXEC имеет следующий вид:

console>

Таблица 5.189 – Команда диагностики оптического трансивера

Команда	***Значение***	***Действие***
show fiber-ports optical-transceiver [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port}* **] [detailed]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Отображает результаты диагностики оптического трансивера. - **detailed** – подробная диагностика, eeprom-параметры трансивера.
show fiber-ports optical-transceiver theshold [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port}* **]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Отображает текущие настройки автоматического мониторинга выбранного порта или всех портов системы.

Пример выполнения команды:

sw1#**show fiber-ports optical-transceiver interface** gi1/0/24 **detailed**

```
   Port      Temp  Voltage Current  Output        Input        LOS  Transceiver
             [C]   [V]     [mA]     Power         Power             Type
                                    [mW / dBm]    [mW / dBm]
----------- ------ ------- ------- ------------- ------------- --- -------------
  gi1/0/24     58    3.25    20.09  0.58 / -2.30  0.00 / -40.00 Yes     Fiber

 Temp         - Internally measured transceiver temperature
 Voltage      - Internally measured supply voltage
 Current      - Measured TX bias current
 Output Power - Measured TX output power in milliWatts
 Input Power  - Measured RX received power in milliWatts
 LOS          - Loss of signal
 N/A - Not Available, N/S - Not Supported, W - Warning, E - Error

        Transceiver information:
Vendor name: OEM
Serial number: SX31221300026
Connector type: LC
```

```
Type: SFP/SFP+
Compliance code: 10GBASE-LR
Laser wavelength: 1310 nm
Transfer distance: 10000
Diagnostic: supported
```

Таблица 5.190 – 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.

При подробной диагностике для параметров Temp, Voltage, Current, Power измеренные значения выводятся на дисплей. При обычной диагностике измеренные значения для этих параметров сравниваются с допустимыми, и на дисплей выводится результат сравнения (W, E, OK).

Значения результатов диагностики и сравнения параметров:

- N/A - недоступно,
- N/S - не поддерживается,
- W - предупреждение,
- E – ошибка,
- OK – значение в порядке.

5.23 IP Service Level Agreements (IP SLA)

IP SLA (соглашения об уровне обслуживания в IP-сетях) – технология активного мониторинга, использующаяся 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.

Измерение параметров сети может осуществляться при помощи различных типов операций IP SLA. Типы операций различаются протоколами генерируемого трафика, а также методами проведения измерений и измеряемыми параметрами. Типы поддерживаемых на данный момент операций IP SLA:

- ICMP Echo;
- UDP Jitter.

Для использования операций IP SLA необходимо выполнить следующие действия:

- Создать операцию нужного типа и сконфигурировать её.
- Запустить циклическое выполнение операции, и позволить ей выполняться в течение некоторого времени.
- Просмотреть статистику, собранную за время жизни операции.
- При необходимости, прекратить циклическое выполнение операции.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 5.191 - Команды режима глобальной конфигурации

Команда	*Значение*	*Действие*
ip sla operation *index*	index: (1..20)	Перейти в контекст конфигурирования операции.
no ip sla operation *index*		Удалить существующую операцию IP SLA.

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 5.192 - Команды режима privileged EXEC

Команда	*Значение*	*Действие*
set ip sla start *index*	index: (1..20)	Запустить циклическое выполнение операции.
set ip sla stop *index*		Остановить циклическое выполнение операции.
show ip sla statistics *index*	index: (1..20)	Отобразить статистику для операции IP SLA.

Статистика операций IP SLA имеет общий для всех типов операций заголовок:

```
IP SLA Statistics for Index 8
Operational state of entry: Active
Type of operation: udp-jitter
```

где

- *IP SLA Statistics for Index* – номер операции, для которой отображается статистика;
- *Operational state of entry* – статус выполнения операции:
  - *Active* – операция активна и в данный момент находится в процессе циклического выполнения;
  - *Inactive* – операция не активна, находится в режиме ожидания и доступна для конфигурирования.
- *Type of operation* – тип операции IP SLA. Принимает одно значение из списка поддерживаемых операций.

При переводе операции в состояние «Active» статистика операции очищается. Статистика накапливается за то время, пока операция находится в этом состоянии. Статистика сохраняется после прекращения циклического выполнения операции и перехода в состояние «Inactive» до тех пор, пока операция снова не будет переведена в активное состояние.

Более подробная информация о содержании статистики представлена в разделах, описывающих типы операций IP SLA.

5.23.1 Операция ICMP Echo

При каждом выполнении операции ICMP Echo устройство отправляет *ICMP Echo request* сообщение на адрес назначения, ожидает получения сообщения *ICMP Echo reply* и измеряет время двустороннего прохождения ICMP-пакета. Операция ICMP Echo также предоставляет

информацию о минимальном, среднем и максимальном временных значениях и количестве измерений, завершившихся неудачно по той или иной причине.

Команды режима создания операций IP SLA

Вид запроса командной строки в режиме создания операций IP SLA:

```
console(config-ip-sla)#
```

Таблица 5.193 - Команды режима создания операций IP SLA

Команда	*Значение*	*Действие*
icmp-echo *target-address* **[source-address** *source-address***] [source-interface** *source-interface***]**	source-interface*:* gi_port(1..8/0/1..24); te_port(1..8/0/1..4)	Создать операцию ICMP Echo. - *target-address* – IPv4-адрес, на который будут отправляться ICMP Echo request сообщения; - *source-address* – IPv4-адрес, подставляющийся в заголовок ICMP-пакета, опциональный параметр; - *source-interface* – порт, с которого осуществляется отправка пакетов, опциональный параметр.

Параметры target-address, source-address и source-interface могут быть определены только при создании операции и недоступны для дальнейшего редактирования. Для задания других параметров необходимо удалить существующую операцию и создать новую.

Команды режима конфигурирования операции ICMP Echo

Вид запроса командной строки в режиме конфигурирования операции ICMP Echo:

```
console(config-ip-sla-icmp-echo)#
```

Таблица 5.194 - Команды режима конфигурирования операции ICMP Echo

Команда	*Значение/Значение по умолчанию*	*Действие*
frequency *sec*	sec: (1..128)/60 с.	Установить частоту выполнения ICMP Echo операции в секундах. - *sec* – частота выполнения ICMP Echo операций в секундах.
no frequency		Установить значение частоты по умолчанию.
timeout *msec*	msec: (1..3600000)/1000 мс	Установить таймаут операции ICMP Echo в миллисекундах. - *msec* – частота выполнения ICMP Echo операций в миллисекундах.
no timeout		Установить значение таймаута по умолчанию.
request-data-size *bytes*	bytes: (1..1432)/56 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.
tos *byte*	byte: (1..255)/0	Установить значение байта *Type of Service*, передающегося в заголовке IP-пакета в поле *Differentiated Services Field*. - *byte* – значение байта *Type of Service* в поле *Differentiated Services Field*.
no tos		Установить значение байта *Type of Service* по умолчанию.
tag *string*	string: (1..63) символов	Задать текстовый тег для операции.
no tag		Убрать текстовый тег.

Для нормального выполнения операции ICMP Echo рекомендуется устанавливать значение частоты выполнения операции большим, чем значение таймаута операции.

Пример вывода статистики для операции ICMP Echo:

```
IP SLA Statistics for Index 12
Operational state of entry: Active
Type of operation: icmp-echo
      Latest operation return code: OK
      Latest latency value: 7 ms
Latency values:
      Number of operations: 2182
      Latency Min/Avg/Max: 1/6/18 ms
Number of successes: 2178
Number of failures: 4
Failed operations due to TimeOut/Unable Send/Bad Reply: 4/0/0
Failed operations due to Unreachable Net/Host/Protocol: 0/0/0
Failed operations due to Exceeded TTL/Time of reassembly: 0/0
```

где

- *Latest operation return code* – код завершения последней выполненной операции:
  - OK – успешное завершение предыдущей операции;
  - *Failed* – неудачное завершение последней попытки измерения.
- *Latest latency value* – значение последнего успешно измеренного периода времени прохождения ICMP-пакета.
- *Number of operations* – количество проведённых запусков операции.
- *Latency Min/Avg/Max* – минимальное, среднее и максимальное значения времени прохождения пакета, подсчитанные за время жизни операции.
- *Number of successes* – количество успешно законченных операций.
- *Number of failures* – количество неудачно законченных операций.
- *Failed operations* – счётчики, отображающие количество измерительных операций, закончившихся с соответствующим кодом ошибки.

5.23.2 Операция UDP Jitter

Каждая операция UDP Jitter инициирует отправку последовательности из нескольких UDP-пакетов. Последовательность характеризуется такими параметрами, как количество пакетов в последовательности и временной промежуток между отправлениями. Основной измеряемой характеристикой является джиттер – изменение межпакетного временного интервала. Операция UDP Jitter также позволяет измерять двустороннее и одностороннее время прохождения пакетов от отправителя к получателю и обратно. Для измерения времени прохождения UDP-пакетов в одну сторону необходима точная синхронизация часов на отправляющем и принимающем устройствах.

Операция UDP Jitter требует поддержки на удалённом устройстве функционала IP SLA и не совместима с устройствами других производителей.

Для измерения времени прохождения UDP-пакетов в одну сторону необходима точная синхронизация часов на отправляющем и принимающем устройствах.

Перед созданием операции UDP Jitter необходимо выполнить настройку UDP-портов для IP SLA Responder на удалённом устройстве, с которым происходит обмен пакетами. Этот UDP-порт следует указать при создании операции UDP Jitter в качестве порта назначения.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 5.195 – Команды режима глобальной конфигурации

Команда	*Значение*	*Действие*
ip sla responder udp_jitter *port*	port: (1..65535)	Включить IP SLA Resonder и установить прослушиваемый порт для операции UDP Jitter. - *port* – номер порта.
no ip sla responder udp_jitter		Отключить IP SLA Responder.

Команды режима создания операций IP SLA

Вид запроса командной строки в режиме создания операций IP SLA:

```
console(config-ip-sla)#
```

Таблица 5.196 – Команды режима создания операций IP SLA

Команда	*Значение/Значение по умолчанию*	*Действие*
udp-jitter *target-address target-port* **[source-address** *source-address***] [source-port** *source-port***] [num-packets** *num-packets***] [interval** *interval***]**	target-port: (1..65535) source-port: (1..65535)/61040 num-packets: (1-1000)/10 пакетов interval: (1-60000)/20 мс	Создать операцию UDP Jitter. - *target-address* – IPv4 адрес, на который будут отправляться UDP-пакеты; - *target-port* – UDP-порт назначения, должен совпадать с UDP-портом, настроенным на респондере; - *source-address* – IPv4 адрес, подставляющийся в заголовок UDP-пакета; - *num-packets* – количество UDP-пакетов в каждой последовательности; - *interval* – временной промежуток между пакетами в последовательности.

Параметры команды «*udp-jitter*» могут быть определены только при создании операции и недоступны для дальнейшего редактирования. Для задания других параметров необходимо удалить существующую операцию и создать новую.

Команды режима конфигурирования операции ICMP Echo

Вид запроса командной строки в режиме конфигурирования операции UDP Jitter:

```
console(config-ip-sla-udp-jitter)#
```

Таблица 5.197 – Команды режима конфигурирования операции ICMP Echo

Команда	*Значение/Значение по умолчанию*	*Действие*
frequency *secs*	*secs*: (1..128)/60 сек	Установить частоту выполнения операции UDP Jitter в секундах. - *secs* – частота выполнения операции UDP Jitter в секундах.
no frequency		Установить значение частоты по умолчанию.
timeout *msec*	*msec*: (1..3600000)/1000 мс	Установить таймаут операции UDP Jitter в миллисекундах. - *msecs* – частота выполнения операции UDP Jitter в миллисекундах.
no timeout		Установить значение таймаута по умолчанию.
request-data-size *bytes*	*bytes*: (20..1432)/30 байт	Установить количество байт, передаваемых в UDP-пакете в качестве данных (*payload*). - *bytes* – количество байт.
no request-data-size		Установить значение количества байт по умолчанию.
tos *byte*	*byte*: (1..255)/0	Установить значение байта *Type of Service*, передающегося в заголовке IP пакета в поле *Differentiated Services Field*. - *byte* – значение байте *Type of Service* в поле *Differentiated Services Field.*

no tos		Установить значение байта *Type of Service* по умолчанию.
tag *string*	*string*: (1..63) символов	Задать текстовый тег для операции. - *string* – текстовый тег.
no tag		Убрать текстовый тег.

Пример вывода статистики для операции UDP Jitter:

```
IP SLA Statistics for Index 2
Operational state of entry: Active
Type of operation: udp-jitter
      Latest operation return code: OK
      Latest latency value: 7 ms
Latency two-way values:
      Number of Latency two-way samples: 455
      Latency Min/Avg/Max: 5/7/24 ms
Latency one-way values:
      Number of SD Latency samples: 0
      Number of DS Latency samples: 0
      Source to Destination Latency one way Min/Avg/Max: 0/0/0 ms
      Source to Destination Latency one way Sum: 0 ms
      Destination to Source Latency one way Min/Avg/Max: 0/0/0 ms
      Destination to Source Latency one way Sum: 0 ms
Jitter values:
      Source to Destination positive jitter Min/Avg/Max: 1/2/20 ms
      Source to Destination positive jitter Num/Sum: 272/706 ms
      Source to Destination negative jitter Min/Avg/Max: 2/3/6 ms
      Source to Destination negative jitter Num/Sum: 91/311 ms
      Destination to Source positive jitter Min/Avg/Max: 1/2/17 ms
      Destination to Source positive jitter Num/Sum: 96/241 ms
      Destination to Source negative jitter Min/Avg/Max: 1/1/6 ms
      Destination to Source negative jitter Num/Sum: 29/46 ms
Packet Loss values:
      Out Of Sequence: 0
Number of successes: 91
Number of failures: 0
Operations failed due to TimeOut/Unable Send/Bad Reply: 0/0/0
Operations failed due to Unreachable Net/Host/Port/Prot: 0/0/0/0
Operations failed due to Exceeded TTL/Time of reassembly: 0/0
```

Статистика одностороннего прохождения пакетов может быть пуста из-за отсутствия синхронизации времени на устройствах и возникновения некорректных значений.

где

- *Latest operation return code* – код завершения последней выполненной операции:
  - *OK* – успешнее завершение предыдущей операции;
  - *Failed* – неудачное завершение последней попытки измерения.
- *Latest latency value* – значение последней успешно измеренной двусторонней задержки.
- *Latency two-way values* – статистика измерения двустороннего времени прохождения пакетов.
- *Latency one-way values* – статистика измерения одностороннего времени прохождения пакетов:
  - *SD* – от отправителя к получателю (*source-to-destination*);
  - *DS* – от получателя к отправителю (*destination-to-source*).
- *Jitter values* – статистика измерения одностороннего джиттера. Отдельно учитываются положительные и отрицательные значения джиттера в каждом из направлений.
- *Out Of Sequence* – количество пакетов, вернувшихся вне очереди.
- *Number of successes* – количество успешно законченных операций.
- *Number of failures* – количество неудачно законченных операций.

– *Failed operations* – счётчики, отображающие количество измерительных операций, завершившихся неудачно 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. Для коммутаторов MES3000 это ограничение равно 128 адресам на порт.

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

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

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

Таблица 5.198 – Команды режима конфигурирования интерфейса Ethernet, группы интерфейсов

Команда	*Значение/Значение по умолчанию*	*Действие*
port security max *num*	(1..128)/1	Задает 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 защищенный MAC-адрес.
no port security routed secure-address [*mac_address*]		Удаляет защищенный MAC-адрес.
port security	(1..1000000) сек	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.**
port security forward [**trap** *trap*]}		Включает функцию защиты на интерфейсе. Блокирует функцию изучения новых адресов для интерфейса. Пакеты с неизученными MAC-адресами источника пересылаются.
port security discard [**trap** *trap*]		Включает функцию защиты на интерфейсе. Блокирует функцию изучения новых адресов для интерфейса. Пакеты с неизученными MAC-адресами источника отбрасываются.
port security discard-shutdown [**trap** *trap*]		Включает функцию защиты на интерфейсе. Выключает порт при поступлении пакетов с неизученными MAC-адресами. Пакеты с неизученными MAC-адресами источника отбрасываются.

port security trap *trap*		Задает частоту генерируемых сообщений протокола SNMP trap при поступлении несанкционированных пакетов.
no port security		Выключает функцию защиты на интерфейсе.
port security mode {max-addresses | lock}	-/lock	Задает режим ограничения изучения MAC-адресов для настраиваемого интерфейса. - **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 файл 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 5.199 – Команды режима EXEC

Команда	*Значение*	*Действие*
show ports security {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***}**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Показывает настройки функции безопасности на выбранном интерфейсе.
show ports security addresses {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***}**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Показывает текущие динамические адреса для заблокированных портов.
set interface active {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **|port-channel** *group***}**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Активизирует 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 портов – 1 порт. 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 gigabitethernet 1/0/15
console(config-if)# port security max 1
```

- 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 глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

`console(config)#`

Таблица 5.200 – Команды режима глобального конфигурирования

Команда	*Значение/ Значение по умолчанию*	*Действие*
dot1x system-auth-control	-/ force-authorized	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	Задает один или два метода проверки подлинности, авторизации и учета (AAA), для использования на интерфейсах IEEE 802.1X. - **none** – не выполнять аутентификацию; - **radius** – использовать список RADIUS-серверов для аутентификации пользователя. **Второй метод аутентификации используется только в случае, если по первому аутентификация была неуспешной.**
no aaa authentication dot1x default		Устанавливает значение по умолчанию.

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet:

`console(config-if)#`

Протокол EAP (Extensible Authentication Protocol) выполняет задачи для аутентификации удаленного клиента, при этом определяя механизм аутентификации.

Таблица 5.201 – Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
dot1x port-control {auto | force-authorized | force-unauthorized} [time-range *time***]**	-/ force-authorized time: (1 .. 32)	Настраивает аутентификацию 802.1X на интерфейсе. Разрешает ручной контроль за состоянием авторизации порта. - **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 reauth-	300..4294967295/	Устанавливает период между повторными проверками

period *period*	3600 сек	подлинности.
no dot1x timeout reauth-period		Устанавливает значение по умолчанию.
dot1x timeout quiet-period *period*	0..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 *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 *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 *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 *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.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

console#

Таблица 5.202 – Команды режима Privileged EXEC

Команда	***Значение***	***Действие***
dot1x re-authenticate [gigabitethernet *gi_port* **| tengigabitethernet** *te_port***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4)	Вручную осуществляет повторную проверку подлинности указанного порта в команде, либо всех портов, поддерживающих 802.1X.
show dot1x interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port***}**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4)	Показывает состояние 802.1X для коммутатора либо для указанного интерфейса.
show dot1x users [username *username***]**	(1..160) символов	Показывает активных аутентифицированных пользователей 802.1X коммутатора.
show dot1x statistics interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port***}**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4)	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 18 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 gigabitethernet 1/0/18
console(config-if)# dot1x port-control auto
```

- Показать состояние 802.1X для коммутатора, для 12 интерфейса Ethernet.

console# **show dot1x**

```
802.1x is disabled
         Admin               Oper          Reauth   Reauth     Username
Port     Mode                Mode          Control  Period
-------- ------------------ ------------- -------- ---------- -----------------
gi0/1    Force Authorized   Authorized*   Disabled 3600       n/a
gi0/2    Force Authorized   Authorized*   Disabled 3600       n/a
gi0/3    Force Authorized   Authorized*   Disabled 3600       n/a
gi0/4    Force Authorized   Authorized*   Enabled  3600       n/a
gi0/5    Force Authorized   Authorized*   Disabled 3600       n/a

…
gi0/10   Force Authorized   Authorized*   Disabled 3600       n/a
gi0/11   Force Authorized   Authorized    Disabled 3600       n/a
gi0/12   Force Authorized   Authorized*   Disabled 3600       n/a
gi0/13   Force Authorized   Authorized*   Disabled 3600       n/a
gi0/14   Force Authorized   Authorized*   Disabled 3600       n/a
gi0/15   Force Authorized   Authorized*   Disabled 3600       n/a
gi0/16   Force Authorized   Authorized*   Disabled 3600       n/a
More: <space>,  Quit: q, One line: <return>
```

console# **show dot1x interface gigabitethernet** *1/0/12*

```
802.1x is disabled

         Admin               Oper          Reauth   Reauth     Username
Port     Mode                Mode          Control  Period
-------- ------------------ ------------- -------- ---------- -----------------
gi0/12   Force Authorized   Authorized*   Disabled 3600       n/a

* Port is down or not present

Quiet period:            60 Seconds
Tx period:               30 Seconds
Max req:                 2
Supplicant timeout:      30 Seconds
Server timeout:          30 Seconds
Session Time (HH:MM:SS): 00:00:00
MAC Address:
Authentication Method:   Remote
Termination Cause:       Port re-initialize
Authenticator State Machine
State:                   INITIALIZE
Backend State Machine
State:                   INITIALIZE
Authentication success:  0
Authentication fails:    0
```

Таблица 5.203 – Описание результатов выполнения команд

Параметр	***Описание***
Port	Номер порта.
Admin mode	Режим аутентификации 802.1X: Force-auth, Force-unauth, Auto.
Oper mode	Операционный режим порта: авторизованный, неавторизованный, либо выключенный (Authorized, Unauthorized, Down).
Reauth Control	Контроль переаутентификации.

Reauth Period	Период между повторными проверками подлинности.
Username	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.
Quiet period	Период, в течение которого коммутатор остается в состоянии молчания после неудачной проверки подлинности.
Tx period	Период, в течение которого коммутатор ожидает ответ на запрос либо идентификацию по протоколу EAP от клиента, перед повторной отправкой запроса.
Max req	Максимальное число попыток передачи запросов протокола EAP клиенту перед новым запуском процесса проверки подлинности.
Supplicant timeout	Период между повторными передачами запросов протокола EAP клиенту.
Server timeout	Период, в течение которого коммутатор ожидает ответа от сервера аутентификации.
Session Time	Время подключения пользователя к устройству.
Mac address	MAC-адрес пользователя.
Authentication Method	Метод аутентификации установленной сессии.
Termination Cause	Причина закрытия сессии.
State	Текущее значение автомата состояний определителя подлинности и выходного автомата состояний.
Authentication success	Количество полученных сообщений об успешной аутентификации от сервера.
Authentication fails	Количество полученных сообщений о неуспешной аутентификации от сервера.
VLAN	Группа VLAN назначенная пользователю.
Filter ID	Идентификатор группы фильтрации.

- Показать статистику по 802.1X для интерфейса Ethernet 13.

```
console# show dot1x statistics interface gigabitethernet 1/0/13
```

```
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 5.204– Описание результатов выполнения команд

Параметр	***Описание***
EapolFramesRx	Количество корректных пакетов любого типа протокола EAPOL (Extensible Authentication Protocol over LAN), принятых данным определителем подлинности.
EapolFramesTx	Количество корректных пакетов любого типа протокола EAPOL, переданных данным определителем подлинности.
EapolStartFramesRx	Количество пакетов Start протокола EAPOL, принятых данным определителем подлинности.
EapolLogoffFramesRx	Количество пакетов Logoff протокола EAPOL, принятых данным определителем подлинности.

EapolRespIdFramesRx	Количество пакетов Resp/Id протокола EAPOL, принятых данным определителем подлинности.
EapolRespFramesRx	Количество пакетов ответов (кроме Resp/Id) протокола EAPOL, принятых данным определителем подлинности.
EapolReqIdFramesTx	Количество пакетов Resp/Id протокола EAPOL, переданных данным определителем подлинности.
EapolReqFramesTx	Количество пакетов запросов (кроме Resp/Id) протокола EAPOL, переданных данным определителем подлинности.
InvalidEapolFramesRx	Количество пакетов протокола EAPOL с нераспознанным типом, принятых данным определителем подлинности.
EapLengthErrorFramesRx	Количество пакетов протокола EAPOL с некорректной длиной, принятых данным определителем подлинности.
LastEapolFrameVersion	Версия протокола EAPOL, принятая в самом последнем на данный момент пакете.
LastEapolFrameSource	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. Также к расширенным настройкам относится администрирование гостевых VLAN, к которым имеют доступ не прошедшие аутентификацию пользователи.

Порт доступа (Access) не может быть членом неаутентифицированной VLAN. Native VLAN порта в режиме Trunk не может быть неаутентифицированной VLAN. Но для порта в режиме General PVID может быть неаутентифицированной VLAN (в этом случае только тегированные пакеты могут быть приняты в неавторизованном состоянии).

Команды режима глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

`console(config)#`

Таблица 5.205 – Команды режима глобального конфигурирования

Команда	***Значение/Значение по умолчанию***	***Действие***
dot1x bpdu {filtering | bridging}	-/filtering	Задает обработку защиты портов 802.1x BPDU, когда 802.1x глобально выключен. - **filtering** – фильтровать пакеты 802.1x BPDU; - **bridging** – передавать пакеты 802.1x BPDU как обычные пакеты данных. **Функция работает только когда режим аутентификации 802.1x на коммутаторе выключен. Для выключения аутентификации 802.1x используется команда: no dot1x system-auth-control.**
no dot1x bpdu		Устанавливает значение по умолчанию.
dot1x guest-vlan timeout *timeout*	timeout: (30 .. 180) /	Устанавливает время задержки между включением режима аутентификации 802.1x (или включением порта) и

		добавлением порта в guest VLAN.
no dot1x guest-vlan timeout		Устанавливает значение по умолчанию.
dot1x traps mac-authentication success	-/ disable	Разрешает отправку trap-сообщений, когда клиент успешно проходит аутентификацию по MAC-адресу, основанную на стандарте 802.1x.
no dot1x traps mac-authentication success		Устанавливает значение по умолчанию.
dot1x traps mac-authentication failure	-/ disable	Разрешает отправку trap-сообщений, когда клиент не прошел аутентификацию по MAC-адресу, основанную на стандарте 802.1x.
no dot1x traps mac-authentication failure		Устанавливает значение по умолчанию.
dot1x radius-attributes errors filter-id resource {accept | reject}	-/ reject	Устанавливает обработку ошибок для атрибутов RADIUS: - **accept** – пользователь принят, если фильтрация по ID не может быть произведена по причинам распределения ресурсов. Если фильтрация по ID не может быть произведена по другим причинам, пользователь будет отклонен; - **reject** – Если фильтрация по ID не может быть задана, то пользователь будет отклонен.
no dot1x radius-attributes errors filter-id resources		Устанавливает значение по умолчанию.
dot1x radius-attributes nas-port format-type {default | human}	-/default	Устанавливает формат нумерации портов в атрибуте NAS-Port при аутентификации по 802.1x: - **deafult** - значение по умолчанию, нумерация соответствует внутренним ifIndex'ам; - **human** - нумерация портов начинается с 1 (как на передней панели).
no dot1x radius-attributes nas-port format-type		Устанавливает значение по умолчанию.

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet:

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

Таблица 5.206 – Команды режима конфигурирования 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** }	-/protect	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; Частота генерируемых сообщений протокола SNMP trap при поступлении несанкционированных пакетов составляет 1 секунду. **Команда игнорируется в режиме multiple hosts.**

no dot1x single-host-violation		Устанавливает значение по умолчанию.
dot1x guest-vlan enable	-/доступ запрещен	Разрешает неавторизованным пользователям данного интерфейса доступ к гостевой VLAN. **На устройстве должен быть настроен хотя бы один гостевой VLAN (команда dot1x guest-vlan в настройках интерфейса VLAN).**
no dot1x guest-vlan enable		Запрещает неавторизованным пользователям данного интерфейса доступ к гостевой VLAN.
dot1x mac-authentication {**mac-only** | **mac-and-802.1x**}	-/выключена	Включает аутентификацию, основанную на MAC-адресах пользователей. - **mac-only** – включает аутентификацию, основанную только на MAC-адресах, пакеты 802.1x игнорируются; - **mac-and-802.1x** – включает аутентификацию, основанную на 802.1x и MAC-адресах. **- Гостевая VLAN должна быть включена, когда используется аутентификация по MAC-адресу.** **- Не должно быть статических привязок MAC-адресов.** **- Функция повторной аутентификации должна быть включена.**
no dot1x mac-authentication		Выключает аутентификацию, основанную на MAC-адресах пользователей.
dot1x mac-authentication format username { *lowercase* **|** *uppercase* **} [separator {** - **|** *:* **|** . **}] [groupsize {** *1* **|** *2* **|** *4* **}]**	-/ lowercase без разделителей и деления на группы (a1b2c3d4e5e6)	Команда задаёт формат строки с MAC адресом клиента, передаваемой в атрибуте User-Name. - lowercase**,** uppercase - определяют регистр буквенных символов; - separator - задаёт разделитель между группами символов; - groupsize - количество символов в каждой группе. Задание параметров separator и groupsize не обязательно (т.е., если требуется, можно указать только регистр), но для того, чтобы MAC адрес отображался разделённым на группы, необходимо задать оба этих параметра. Пример конфигурации: **dot1x mac-authentication format username uppercase separator : groupsize 4** Формат строки в атрибуте: A1B2:C3D4:E5F6
no dot1x mac-authentication format username		Устанавливает значение по умолчанию
dot1x mac-authentication format password {*password_string*}	-/User-Name	Строка password_string передаётся в RADIUS атрибуте User-Password. По умолчанию в атрибуте передаётся MAC адрес клиента в формате, заданном командой dot1x mac-authentication format username. Максимальная длина передаваемой строки - 128 символов.
no dot1x mac-authentication format password		Устанавливает значение по умолчанию.
dot1x radius-attributes filter-id	-/выключен	Включить проверку подлинности, основанную на ACL/ назначить QOS-Policy.
no dot1x radius-attributes filter-id		Устанавливает значение по умолчанию.
dot1x radius-attributes vlan	-/выключен	Включает обработку опции Tunnel-Private-Group-ID (81) в сообщениях RADIUS-сервера.
no dot1x radius-		Выключает обработку опции Tunnel-Private-Group-ID (81) в

attributes vlan		сообщениях RADIUS-сервера.

Команды режима конфигурирования VLAN

Вид запроса командной строки в режиме конфигурирования интерфейса VLAN:

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

Таблица 5.207 – Команды режима конфигурирования интерфейса VLAN

Команда	*Значение*	*Действие*
dot1x auth-not-req	По умолчанию доступ неавторизованным пользователям запрещен	Разрешает доступ к данной VLAN неавторизованным пользователям.
no dot1x auth-not-req		Запрещает доступ к данной VLAN неавторизованным пользователям.
dot1x guest-vlan	По умолчанию VLAN не определена как гостевая	Определяет 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		Устанавливает значение по умолчанию.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 5.208– Команды режима Privileged EXEX

Команда	*Значение*	*Действие*
show dot1x advanced [gigabitethernet *gi_port* **| tengigabitethernet** *te_port***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4)	Показывает дополнительные сведения о настройках протокола 802.1x (команда доступна только для привилегированного пользователя).

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.209 – Команды режима Privileged EXEC

Команда	*Значение*	*Действие*
show dot1x bpdu	-	Показывает обработку защиты портов 802.1x BPDU когда 802.1x глобально выключен.

5.24.3 Контроль протокола DHCP и опции 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, в виде DHCP-запроса, принятого от клиента. 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 5.210 - Формат полей опции 82

Поле	***Передаваемая информация***
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. Для включения DHCP relay агента используется команда ip dhcp relay enable в режиме глобального конфигурирования (см. соответствующий раздел документации).

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 глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.211 – Команды режима глобального конфигурирования

Команда	***Значение/Значение по умолчанию***	***Действие***
ip dhcp snooping	-/ выключено	Разрешает коммутатору контролирование протокола DHCP.
no ip dhcp snooping		Запрещает коммутатору контролирование протокола DHCP.
ip dhcp snooping vlan *vlan_id*	vlan_id: (1..4094)/ выключено	Разрешает контролирование протокола DHCP в пределах указанного VLAN.
no ip dhcp snooping vlan *vlan_id*		Запрещает контролирование протокола DHCP в пределах указанного 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 snooping database update-freq *seconds*	seconds: (600..86400)/1200	Задает частоту обновления файла (базы) контроля протокола DHCP.
no ip dhcp snooping database update-freq *seconds*		Устанавливает значение по умолчанию.
ip dhcp information option	-/разрешено	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..32 символов	Установка идентификатора Access Node_ID опции 82.
no ip dhcp information option format-type access-node-id		Установка значения по умолчанию
ip dhcp information option format-type remote-id *remote_id*	remote_id*:* (1..32) символов/-	Установка идентификатора Remote agentID опции 82.
no ip dhcp information option format-type remote-id		Установка значения по умолчанию.
ip dhcp information option format-type option *format* **[delimiter** *delimiter***]**	format: (sp, sv, pv, spv, bin, user-defined); delimiter: (.,;#)/пробел	Настройка формата 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. При определении используются следующие шаблоны: %h: hostname; %p: короткое имя порта, например gi1/0/1; %P: длинное имя порта, например, gigabitethernet 1/0/1; %t: тип порта (значение поля ifTable::ifType в шестнадцатеричном виде); %m: мак-адрес порта в формате H-H-H-H-H-H-H; %M: мак-адрес системы в формате H-H-H-H-H-H-H; %u: номер юнита; %s: номер слота; %n: номер порта (как на лицевой панели); %i: ifIndex порта; %v: идентификатор VLAN.
no ip dhcp information option format-type option		Установка значения по умолчанию
ip dhcp information	-/tr101	Установка формата опции 82.

option suboption type {**tr101**|**custom**}		- **tr101** – устанавливает формат опции 82 согласно синтаксису, принятому в рекомендациях TR-101 (см. таблицу **Ошибка! Источник ссылки не найден.**); - **custom** – устанавливает формат опции 82 в соответствии с форматом, приведенном в таблице **Ошибка! Источник ссылки не найден.**.
no ip dhcp information option suboption type		Возвращает значение по умолчанию.

Таблица 5.212 – 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 5.213 – Формат полей опции 82 режима custom

Поле	***Передаваемая информация***
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 конфигурирования интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов

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

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

Таблица 5.214 – Команды режима конфигурирования интерфейса Ethernet, группы интерфейсов

Команда	***Значение/Значение по умолчанию***	***Действие***
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 snooping limit rate *rate*	rate: (1..2048) pps/Выключено	Устанавливает ограничение для данного порта на количество принимаемых DHCP-пакетов в секунду .
no ip dhcp snooping limit rate		Снимает ограничение на приём DHCP-пакетов с данного порта.
ip dhcp information option	circuit-id: 1..63 символов/-	Устанавливает специфичный *Circuit-id* на интерфейсе.

format-type circuit-id *circuit_id*		
no ip dhcp information option format-type circuit-id		Устанавливает значение по умолчанию.
ip dhcp information option format-type remote-id *remote_id*	remote -id: 1..63 символов/-	Устанавливает специфичный *Remote-id* на интерфейсе.
no ip dhcp information option format-type remote-id		Устанавливает значение по умолчанию.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

console#

Таблица 5.215 – Команды режима Privileged EXEC

Команда	***Значение***	***Действие***
ip dhcp snooping binding *mac_address vlan_id ip_address* **{gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} expiry {***seconds***|infinity}**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4) vlan_id: (1 .. 4094); group:(1 .. 12); seconds: (10..4294967295)	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). - *seconds* – время жизни записи; - **infinity** – время жизни записи не ограничено.
no ip dhcp snooping binding *mac_address vlan_id*		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 5.216 – Команды режима EXEC

Команда	***Значение***	***Действие***
show ip dhcp information option	-	Показывает информацию об использовании опции 82 протокола DHCP.
show ip dhcp snooping [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Показывает конфигурацию функции контроля протокола DHCP.
show ip dhcp snooping binding [mac-address *mac_address***] [ip-address** *ip_address* **] [vlan** *vlan_id***] [gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12) vlan_id: (1..4094)	Показывает соответствия из файла (базы) контроля протокола DHCP.

Примеры выполнения команд

- Разрешить использование DHCP опции 82:

```
console# configure
console(config)# ip dhcp relay enable
console(config)# ip dhcp information option
```

- Показать все соответствия из файла (базы) контроля протокола DHCP:

```
console# show ip dhcp snooping
```

```
DHCP snooping is globally Enabled
DHCP snooping is configured on following VLANs: 2, 5
DHCP snooping database: Enabled
Relay agent Information option 82 is Enabled
Option 82 on untrusted port is allowed
Verification of hwaddr field is Enabled
DHCP snooping file update frequency is configured to: 1200 secondsInterface
Trusted   Rate Limit (pps)
----------- --------- ------------------
gi1/0/1     No         5
gi1/0/5     Yes        --
gi1/0/11    Yes        --
gi2/0/11    Yes        9
gi3/0/5     No        1781
gi3/0/11    No         7
```

5.24.4 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 таблицу 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 глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.217 – Команды режима глобального конфигурирования

Команда	*Значение*	*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 *mac_address vlan_id ip_address* **{gigabitethernet** *gi_port* **|**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); vlan_id: (1..4094); group: (1..12)	Создание статической записи в таблице соответствия между IP-адресом клиента, его MAC-адресом и группой VLAN для указанного в команде интерфейса.

tengigabitethernet *te_port* **| port-channel** *group***}**		
no ip source-guard binding *mac_address vlan_id*		Удаление статической записи в таблице соответствия.
ip source-guard tcam retries-freq {*seconds* | **never**}	(10..600, never)/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 конфигурирования интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов

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

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

Таблица 5.218 – Команды режима конфигурирования интерфейса Ethernet, группы интерфейсов

Команда	***Значение***	***Действие***
ip source-guard	По умолчанию функция выключена.	Включает функцию защиты IP-адреса клиента для настраиваемого интерфейса.
no ip source-guard		Выключает функцию защиты IP-адреса клиента для настраиваемого интерфейса.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 5.219 – Команды режима Privileged EXEC

Команда	***Значение***	***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 5.220 – Команды режима EXEC

Команда	***Значение***	***Действие***
show ip source-guard configuration [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Команда отображает настройку функции защиты IP-адреса на заданном, либо на всех интерфейсах устройства.
show ip source-guard status [mac-address *mac_address***] [ip-address** *ip_address* **] [vlan** *vlan_id***] [gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); vlan_id: (1..4094); group: (1..12)	Команда отображает статус функции защиты IP-адреса для указанного интерфейса, IP-адреса, MAC-адреса или группы VLAN.

show ip source-guard inactive	-	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
---------       ------
gi0/4           Enabled
gi0/21          Enabled
gi0/22          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 3-й 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 **gigabitethernet** 1/0/12

5.24.5 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 глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

console(config)#

Таблица 5.221 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
ip arp inspection	По умолчанию функция выключена	Включает контроль протокола ARP (функцию ARP Inspection).
no ip arp inspection		Выключает контроль протокола ARP (функцию ARP Inspection).

ip arp inspection vlan *vlan_id*	vlan_id: (1..4094) По умолчанию функция выключена	Разрешает проверку протокола ARP, основанную на базе соответствий DHCP snooping, в выбранной группе VLAN.
no ip arp inspection vlan *vlan_id*		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-пакета на наличие некорректных IP-адресов.
no ip arp inspection validate		Запрещает специфичные проверки для контроля протокола ARP.
ip arp inspection list create *name*	Имя списка 1..32 символа	1. Создание списка статических ARP соответствий. 2. Вход в режим конфигурирования ARP-списков.
no ip arp inspection list create *name*		Удаление списка статических ARP соответствий.
ip arp inspection list assign *vlan_id name*	vlan_id:(1 .. 4094)	Назначает список статических ARP соответствий для указанной VLAN.
no ip arp inspection list assign *vlan_id*		Отменяет назначение списка статических ARP соответствий для указанной VLAN.
ip arp inspection logging interval {*seconds* | **infinite**}	(0..86400, infinite)/5 сек	Задает 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 конфигурирования интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов

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

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

Таблица 5.222 – Команды режима конфигурирования интерфейса Ethernet, группы интерфейсов

Команда	***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 конфигурирования ARP-списков

Вид запроса командной строки в режиме конфигурирования ARP-списков:

```
console# configure
console(config)# ip arp inspection list spisok
console(config-ARP-list)#
```

Таблица 5.223 – Команды режима конфигурирования ARP списков

Команда	*Действие*
ip *ip_address* **mac** *mac_address*	Добавляет статическое соответствие IP- и MAC-адресов.
no ip *ip_address* **mac** *mac_address*	Удаляет статическое соответствие IP- и MAC-адресов.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

console#

Таблица 5.224 – Команды режима EXEC

Команда	*Значение*	*Действие*
show ip arp inspection [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4) group: (1..12)	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 [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***] [vlan** *vlan_id***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4) group: (1..12) 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 [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***] [vlan** *vlan_id***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4) group: (1..12) 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 spisok
console(config-ARP-list)# ip 192.168.16.98 mac 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
```

5.24.6 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 глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

`console(config)#`

Таблица 5.225 - Команды режима глобального конфигурирования

Команда	*Значение/ Значение по умолчанию*	*Действие*
[no] 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. Отрицательная форма команды (с префиксом no) выключает функцию глобально и отменяет соответствующие настройки на всех интерфейсах. Для работы функции необходимо дополнительно разрешать генерацию уведомлений на интерфейсах (см. ниже).
mac address-table notification change interval {*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.
mac address-table notification change history {*value***}**	[0..500]/1	Команда задает 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] snmp-server enable traps mac-notification change	-/выключено	Команда предназначена для включения или отключения отправки 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 flapping	-/включена	Включить/выключить отправку трапов о флаппинге MAC-адресов (eltMnFlappingNotification).

Команды режима конфигурирование интерфейса Ethernet

Вид запроса командной строки:

`console(config-if)#`

Таблица 5.226 - Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение по умолчанию*	*Действие*
snmp trap mac-notification change [added | removed]	выключена	Включение генерации уведомлений на каждом интерфейсе о событиях изменения состояния MAC-адресов. Отдельно можно разрешить генерацию уведомлений только об изучении MAC адресов, либо только об их удалении.

Команды режима privileged EXEC

Вид запроса командной строки в режиме privileged EXEC:

console#

Таблица 5.227 - Команды режима privileged EXEC

Команда	*Значение*	*Действие*
show mac address-table notification change history [*interfaces***]**	-	Отображение всех уведомлений об изменении состояния MAC-адресов, сохраненных в истории. Возможна фильтрация событий по портам, группам портов (LAG) и VLAN.
show mac address-table notification change statistics	-	Отображение статистики сервиса: общее количество событий об изучении MAC-адресов, общее количество событий об удалении MAC-адресов, общее количество отправленных SNMP-сообщений.

Примеры использования команд

- Пример показывает 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)#
```

5.25 Функции DHCP Relay посредника

Коммутаторы MES3000 поддерживает 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 глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.228 – Команды режима глобального конфигурирования

Команда	*Значение*	*Действие*
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 *ip_addr*	Может быть задано до 8-ми серверов	Задаёт IP-адрес доступного DHCP-сервера для DHCP Relay агента.
no ip dhcp relay address [*ip_addr*]		Удаляет IP-адрес из списка DHCP-серверов для DHCP Relay агента.
ip dhcp relay broadcast enable	По умолчанию режим выключен	Включает режим широковещательной рассылки ответов DHCP-сервера.
no ip dhcp relay broadcast enable		Устанавливает режим по умолчанию
ip dhcp relay information policy {keep | replace | drop}	По умолчанию включен режим **keep**	Определяет режим обработки DHCP-пакетов с опцией 82: - **keep** – пропускает пакеты без изменений; - **replace** – замещает содержимое опции 82; - **drop** – отбрасывает пакеты с опцией 82.
no ip dhcp relay information policy		Устанавливает режим по умолчанию.
ip dhcp relay information option format-type option *format* [**delimiter** *delimiter*]	format: (sp, sv, pv, spv, bin, user-defined); delimiter: (.,;#)/пробел	Настройка формата 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. При определении используются следующие шаблоны: %h: hostname; %p: короткое имя порта, например gi1/0/1; %P: длинное имя порта, например, gigabitethernet 1/0/1; %t: тип порта (значение поля ifTable::ifType в шестнадцатеричном виде); %m: мак-адрес порта в формате H-H-H-H-H-H-H; %M: мак-адрес системы в формате H-H-H-H-H-H-H; %u: номер юнита; %s: номер слота; %n: номер порта (как на лицевой панели); %i: ifIndex порта; %v: идентификатор VLAN.
no ip dhcp relay information option format-type option		Установка значения по умолчанию
ip dhcp relay information option suboption-type {tr101 | custom}	-/tr101	Настройка формата опции 82. - **tr101** – устанавливает формат опции 82 согласно синтаксису, принятому в рекомендациях TR-101 (см. таблицу 5.212); - **custom** – устанавливает формат опции 82 в соответствии с форматом, приведенном в таблице 5.213.
no ip dhcp relay information option suboption-type		Возвращает значение по умолчанию

Команды режима конфигурирования интерфейса VLAN

Вид запроса командной строки в режиме конфигурирования интерфейса VLAN:

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

Таблица 5.229 – Команды режима конфигурирования интерфейса VLAN

Команда	*Значение*	*Действие*
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.

Команды режима конфигурирование интерфейса Ethernet

Вид запроса командной строки:

`console(config-if)#`

Таблица 5.230 - Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
ip dhcp relay information policy {keep | replace | drop | global}	-/global	Определяет режим обработки DHCP-пакетов с опцией 82. - **keep** – пропускает пакеты без изменений; - **replace** – замещает содержимое опции 82; - **drop** – отбрасывает пакеты с опцией 82. Значение на портах имеет более высокий приоритет, чем глобальная настройка.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

`console#`

Таблица 5.231 – Команды режима EXEC

Команда	*Действие*
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 Функции Lightweight DHCPv6 Relay Agent (LDRA)

Наравне с DHCP для протокола IPv4 коммутатор может выполнять функции посредника (relay agent) для DHCPv6. Данный функционал реализован в виде Lightweight DHCPv6 Relay Agent согласно RFC6221.

В рамках выполнения функции посредника коммутатор вставляет в клиентские DHCPv6-пакеты опции 18 и 37. Для включения функции требуется выполнить следующие предварительные шаги по настройке:

- Включить функционал DHCP snooping (для IPv4) – глобально и на целевом VLAN;
- Включить функционал DHCPv6 guard – глобально и на целевом VLAN;
- На «доверенных» интерфейсах коммутатора («trusted» по терминологии RFC3046) выполнить DHCPv4-настройку «ip dhcp snooping trust»;

- На «доверенных» интерфейсах коммутатора выполнить настройку «ipv6 dhcp guard trusted-port»

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.232– Команды режима глобального конфигурирования

Команда	*Значение*	*Действие*
ipv6 dhcp-ldra enable	По умолчанию выключена	Включает функцию Lightweight DHCPv6 Relay Agent (LDRA).
no ipv6 dhcp-ldra enable		Отключает функцию LDRA.
ipv6 dhcp-ldra information option format-type remote-id *word*	word: (1..63) символов	Задает идентификатор remote-id (опция 37)
no ipv6 dhcp-ldra information option format-type remote-id		Удаляет идентификатор remote-id.

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки:

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

Таблица 5.233– Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение по умолчанию*	*Действие*
ipv6 dhcp-ldra information option format-type interface-id *word*	word: (1..63) символов	Задает идентификатор порта (опция 18)
no ipv6 dhcp-ldra information option format-type interface-id		Восстанавливает значение по умолчанию.
ipv6 dhcp-ldra information option format-type remote-id *word*	word: (1..63) символов	Задает идентификатор remote-id (опция 37)
no ipv6 dhcp-ldra information option format-type remote-id		Восстанавливает значение по умолчанию.

5.27 Конфигурирование PPPoE Intermediate Agent

Функция PPPoE IA реализована в соответствии с требованиями документа DSL Forum TR-101 и предназначена для использования на коммутаторах, работающих на уровне доступа.

Функция позволяет дополнять пакеты PPPoE Discovery информацией, характеризующей интерфейс доступа. Это необходимо для идентификации пользовательского интерфейса на сервере доступа (BRAS, Broadband Remote Access Server). Управление перехватом и обработкой пакетов PPPoE Active Discovery осуществляется глобально для всего устройства и выборочно для каждого интерфейса.

Реализация функции PPPoE IA предоставляет дополнительные возможности контроля сообщений протокола путем назначения доверенных интерфейсов.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

console(config)#

Таблица 5.234 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
[no] pppoe intermediate-agent	по умолчанию PPPoE IA отключен	Разрешение/запрет работы PPPoE Intermediate Agent.
[no] pppoe intermediate-agent format-type access-node-id ***word***	word*:* строка от 1 до 32 символов По умолчанию идентификатор устройства не назначен.	Установка строки идентификации устройства доступа. Отрицательная форма команды (no) восстанавливает настройки по умолчанию.
[no] pppoe intermediate-agent format-type generic-error-message ***word***	word*:* строка до 128 символов По умолчанию назначено сообщение «PPPoE Discover packet is too large to process.».	Установка текста сообщения об ошибке превышения размера пакета (MTU), отправляемого PPPoE IA в PADO или PADS пакетах. Отрицательная форма команды восстанавливает значение параметра по умолчанию. **Примечание:** если сообщение содержит символы пробела, его необходимо заключить в кавычки.
[no] pppoe intermediate-agent format-type option {sp | sv | pv | spv | user-defined} **delimeter [.,:#/]**	-/установлен формат в соответствии с TR-101: slot / port : vlan;	Настройка набора параметров и разделителя между ними, которые используются для формирования подопции circuit -id. В команде используются следующие условные обозначения: - **sp** – slot + port - **sv** – slot + vlan - **pv** – port + vlan - **spv** – slot + port + vlan - **user-defined** – формат определяется пользователем. При определении используются следующие шаблоны: %h: hostname; %p: короткое имя порта, например gi1/0/1; %P: длинное имя порта, например, gigabitethernet 1/0/1; %t: тип порта (значение поля ifTable::ifType в шестнадцатеричном виде); %m: мак-адрес порта в формате H-H-H-H-H-H-H; %M: мак-адрес системы в формате H-H-H-H-H-H-H; %u: номер юнита; %s: номер слота; %n: номер порта (как на лицевой панели); %i: ifIndex порта; %v: идентификатор VLAN.

Команды режима конфигурирования интерфейса

Вид запроса командной строки в режиме конфигурирования интерфейса:

console(config-if)#

Таблица 5.235 – Команды режима конфигурирования интерфейса Ethernet, группы портов

Команда	*Значение/Значение по умолчанию*	*Действие*
[no] pppoe intermediate-agent	-	Разрешение/запрет работы PPPoE Intermediate Agent на интерфейсе.
[no] pppoe intermediate-agent format-type circuit-id *circuit_id*	*circuit_id*: строка от 1 до 63 символов	Назначение идентификатора circuit-id, добавляемого коммутатором. Идентификатор, заданный в команде, полностью переопределяет идентификатор, вычисляемый на основе глобальных параметров access-node-id и option/delimeter. Отрицательная форма команды восстанавливает настройку на основе глобальных

		параметров access-node-id и option/delimeter.
[no] pppoe intermediate-agent format-type remote-id *remote_id*	remote_id: строка от 1 до 63 символов. По умолчанию в качестве remote-id используется MAC-адрес коммутатора.	Назначение идентификатора remote-id, добавляемого коммутатором. Идентификатор должен быть сконфигурирован на всех интерфейсах коммутатора, где работает PPPoE IA. Отрицательная форма команды восстанавливает настройку по умолчанию.
[no] pppoe intermediate-agent timeout [*timeout***]**	timeout : (0..600)/600 сек	Задание времени жизни клиентской сессии. При вводе параметра timeout равным нулю, таймаут новых сессий будет равен бесконечности. Отрицательная форма команды восстанавливает настройку по умолчанию.
[no] pppoe intermediate-agent trust	По умолчанию интерфейс не является доверенным.	Управление режимом доверия к интерфейсу. Команда добавляет или удаляет интерфейс из списка доверенных. Интерфейсы, к которым подключены PPPoE-серверы, настраиваются как доверенные. Интерфейсы, к которым подключены пользователи, настраиваются как недоверенные. Отрицательная форма команды восстанавливает значение по умолчанию.
[no] pppoe intermediate-agent vendor-tag strip	По умолчанию режим удаления выключен.	Разрешение или запрет удаления vendor-specific опции из пакетов PADO, PADS, PADT перед отправкой их в сторону пользователя. Функция удаления может быть использована только на интерфейсе, на котором разрешена работа PPPoE IA и который является доверенным интерфейсом. Обычно функция удаления настраивается на интерфейсе, обращенном в сторону PPPoE-сервера. Отрицательная форма команды выключает режим удаления.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

`console#`

Таблица 5.236 – Команды режима EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show pppoe intermediate-agent info [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***}]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4) group: (1..12)	Отображение настроек PPPoE Intermediate Agent. Если в команде явно не задан интерфейс, то команда выполняется для всех интерфейсов, где разрешена работа PPPoE IA и всех доверенных портов.
show pppoe intermediate-agent statistics [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***}]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4) group: (1..12)	Отображение статистики работы PPPoE Intermediate Agent. Если в команде не задан явно интерфейс, то команда выполняется для всех интерфейсов с разрешенным PPPoE IA и всех доверенных портов.
clear pppoe intermediate-agent statistics [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***}]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4) group: (1..12)	Очистка статистики работы PPPoE Intermediate Agent. Если в команде не задан явно интерфейс, то команда выполняется для всех интерфейсов с разрешенным PPPoE IA и всех доверенных портов.
show pppoe intermediate-agent sessions {interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***}]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4) group: (1..12)	Отображение всех зарегистрированных клиентских сессий. Если в команде не задан явно интерфейс, то отображаются все сессии с сортировкой по интерфейсам.
clear pppoe intermediate-agent sessions [*mac_address***]**	mac_address:(H.H.H или H:H:H:H:H:H или H-H-H-H-H-H)	Удаление клиентской сессии. Если *mac_address* не задан, удаляются все сессии.

5.28 Конфигурирование 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 MES3000 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 глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

console(config)#

Таблица 5.237 – Команды режима глобального конфигурирования

Команда	***Значение/Значение по умолчанию***	***Действие***
ip dhcp server	-/выключена	Включение функции DHCP-сервера на коммутаторе.
no ip dhcp server		Выключение функции DHCP-сервера на коммутаторе.
ip dhcp pool host *name*	(1-32) символов	Вход в режим конфигурирования статических адресов DHCP-сервера.
no ip dhcp pool host *name*		Удаляет конфигурацию DHCP-клиента с заданным именем.
ip dhcp pool network *name*	(1-32) символов	Вход в режим конфигурирования DHCP-пула адресов DHCP-сервера. - **name –** имя DHCP-пула адресов (до 64 **dhcp pool network)**.
no ip dhcp pool network *name*		Удаляет DHCP-пул с заданным именем.
ip dhcp excluded-address *low_address* **[***high_address***]**	-	Указывает IP-адреса, которые DHCP-сервер не будет назначать для DHCP-клиентов. - *low-address* – начальный IP-адрес диапазона; - *high-address* – конечный IP-адрес диапазона.
no ip dhcp excluded-address *low_address* **[***high_address***]**		Удаление IP-адреса из списка исключений для назначения его DHCP-клиентам.
ip dhcp ping enable	-/выключена	Включить передачу ICMP-запросов на назначаемый адрес для проверки, что IP-адрес является свободным, прежде чем он будет назначен DHCP-клиенту.
no ip dhcp ping enable		Установить значение по умолчанию.
ip dhcp ping count *number*	number: (1..10)/2	Определяет количество отправляемых ICMP-запросов.
no ip dhcp ping count		Установить значение по умолчанию.
ip dhcp ping timeout *time*	time: (300 .. 1000)/500 мс	Определяет таймаут, в течение которого DHCP-сервер ожидает ответ с адреса, на который отправлен ICMP-запрос.
no ip dhcp ping timeout		Установить значение по умолчанию.

Команды режима конфигурирования статических адресов DHCP-сервера

Вид запроса командной строки в режиме конфигурирования статических адресов DHCP-сервера:

console# **configure**
console(config)# **ip dhcp pool host** *name*
console(config-dhcp)#

Таблица 5.238 – Команды режима конфигурирования

Команда	*Значение*	*Действие*
address *ip_address* {*mask* **|** *prefix_length*} {**client-identifier** *id***|** **hardware-address** *mac_address*}	-	Ручное резервирование IP-адресов для DHCP-клиента. - *ip_address* – IP-адрес, который будет сопоставлен с физическим адресом клиента; - *mask/ prefix_length* – маска подсети/ длина префикса; - *id* – физический адрес (идентификатор) сетевой карты; - *mac_address* – MAC-адрес.
no address		Удаляет зарезервированные IP-адреса.
client-name *name*	(1-32) символов	Определяет имя DHCP-клиента.
no client-name		Удаляет имя DHCP-клиента.

Команды режима конфигурирования пула DHCP-сервера

Вид запроса командной строки в режиме конфигурирования пула DHCP-сервера:

console# **configure**
console(config)# **ip dhcp pool network** *name*
console(config-dhcp)#

Таблица 5.239– Команды режима конфигурирования

Команда	*Значение*	*Действие*
address {*network_number* **|** **low** *low_address* **high** *high_address*} {*mask* **|** *prefix_length*}	-	Устанавливает номер подсети и маску подсети для пула адресов DHCP-сервера. - *network_number* – IP-адрес номера подсети; - *low_address* – начальный IP-адрес диапазона адресов; - *high_address* – конечный IP-адрес диапазона адресов. - *mask/ prefix_length* – маска подсети/ длина префикса.
no address		Удаляет конфигурацию DHCP - пула адресов
lease {*days* [{*hours*} [*minutes*]] **|** **infinite**}	-/1 день	Время аренды IP-адреса, который назначен от DHCP. - *infinite* – время аренды не ограничено; - *days* – количество дней; - *hours* - количество часов; - *minutes* – количество минут.
no lease		Установить значение по умолчанию.
ping enable	-/выключена	Включить передачу ICMP-запросов для проверки, что IP-адрес является свободным, прежде чем он будет назначен DHCP-клиенту.
no ping enable		Установить значение по умолчанию.

Команды режима конфигурирования пула DHCP-сервера и статических адресов DHCP-сервера

Вид запроса командной строки:

console(config-dhcp)#

Таблица 5.240 – Команды режима конфигурирования

Команда	*Значение*	*Действие*
default-router *ip_address_list*	По умолчанию список маршрутизаторов не определен.	Определяет список маршрутизаторов по умолчанию для DHCP-клиента: - *ip_address_list* – 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 *ip_address_list*	По умолчанию список DNS-серверов не определен.	Определяет список DNS-серверов, доступных для клиентов DHCP. - *ip_address_list* – список IP-адресов DNS-серверов,

		может содержать до 8 записей, разделенных пробелом.
no dns-server		Устанавливает значение по умолчанию.
domain-name *domain*	(1-32) символов	Определяет доменное имя для DHCP-клиентов.
no domain-name		Устанавливает значение по умолчанию.
netbios-name-server *ip_address _list*	По умолчанию список WINS-серверов не определен.	Определяет список WINS-серверов, доступных для клиентов DHCP. - *ip_address_list* – список IP-адресов WINS-серверов, может содержать до 8 записей, разделенных пробелом.
no netbios-name-server		Устанавливает значение по умолчанию.
netbios-node-type {b-node | p-node | m-node | h-node}	По умолчанию тип узла NetBIOS не определен.	Определяет тип узла NetBIOS Microsoft для клиентов DHCP: - *b-node* – широковещательный; - *p-node* – точка-точка; - *m-node* – комбинированный; - *h-node* – гибридный.
no netbios-node-type		Устанавливает значение по умолчанию.
next-server *ip_address*	-	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 *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 *filename*	(1..128) символов	Указывает имя файла, используемого для начальной загрузки DHCP-клиента.
no bootfile		Устанавливает значение по умолчанию.
time-server *ip_address_list*	По умолчанию список серверов не определен.	Определяет список серверов времени, доступных для клиентов DHCP. - *ip_address_list* – список IP-адресов серверов времени, может содержать до 8 записей, разделенных пробелом.
no time-server		Устанавливает значение по умолчанию.
option *code* **{ascii** *ascii_string* **| hex** *hex_string* **| ip** *ip_address* **}** **option ip-list** *code ip_address_list*		Настраивает опции DHCP-сервера. - *code* – код опции DHCP-сервера; - *ascii_string* – строка в формате ASCII; - *hex_string* – строка в 16-ом формате; - *ip_address* – IP-адрес; - ip-list – указывает, что за кодом следует список IP-адресов.
no option code		Удаляет опции для DHCP-сервера.
tftp-server *ip_address_list*	По умолчанию список серверов не определен.	Настройка опции 150 – адреса TFTP-сервера: - *ip_address_list* – список IP-адресов TFTP-серверов, может содержать до 8 записей, разделенных пробелом.
no tftp-server		Устанавливает значение по умолчанию.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

`console#`

Таблица 5.241 – Команды режима Privileged EXEC

Команда	***Значение***	***Действие***
clear ip dhcp binding { *ip_address* | *}	-	Удаление записей из таблицы соответствия физических адресов и адресов, выданных с пула DHCP-сервером: - *ip_address* – 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 [*ip_address* | *name*]	(1-32) символов	Просмотр конфигурации для статических адресов DHCP-сервера: - *ip_address* – IP-адрес клиента; - *name* – имя DHCP-пула адресов.
show ip dhcp pool network [*name*]	(1-32) символов	Просмотр конфигурации DHCP-пула адресов DHCP-сервера: - *name* – имя DHCP-пула адресов.
show ip dhcp binding [*ip_address*]	-	Просмотр IP-адресов, которые сопоставлены с физическими адресами клиентов, а так же время аренды, способ назначения и состояние IP-адресов.
show ip dhcp server statistics	-	Просмотр статистики DHCP-сервера.

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
```

5.29 Конфигурирование ACL (списки контроля доступа)

ACL (Access Control List – список контроля доступа) – таблица, которая определяет правила фильтрации входящего 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. Список ACL на базе MAC-адресации не может совмещаться со списками для IPv4 или IPv6. Два списка одинакового типа не могут работать вместе на интерфейсе.

Команды для создания и редактирования списков ACL доступны в режиме глобального конфигурирования.

Команды режима глобального конфигурирования

Командная строка в режиме глобального конфигурирования имеет вид:

```
console (config)#
```

Таблица 5.242 – Команды для создания и конфигурирования списков ACL

Команда	*Значение*	*Действие*
ip access-list extended *access_list*	access_list: (1..32) символа	Создание нового расширенного списка ACL для адресации IPv4 и вход в режим его конфигурирования (если список с данным именем еще не создан) либо вход в режим конфигурирования ранее созданного списка.
no ip access-list extended *access_list*		Удаление списка ACL для адресации IPv4.
ipv6 access-list *access_list*		Создание нового расширенного списка ACL для адресации

		IPv6 и вход в режим его конфигурирования (если список с данным именем еще не создан) либо вход в режим конфигурирования ранее созданного списка.
no ipv6 access-list *access_list*		Удаление списка ACL для адресации IPv6.
mac access-list extended *access_list*		Создание нового списка ACL на базе MAC-адресации и вход в режим его конфигурирования (если список с данным именем еще не создан) либо вход в режим конфигурирования ранее созданного списка.
no mac access-list extended *access_list*		Удаление списка ACL на базе MAC-адресации.
time-range *time_name*	time_name: (1..32) символа	Вход в режим конфигурирования time-range и определение временных интервалов для списка доступа. - *time_name* - имя профиля настроек time-range.
no time-range *time_name*		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 конфигурирования интерфейса Ethernet, VLAN, группы портов.

Командная строка в режиме конфигурирования интерфейса Ethernet, группы портов имеет вид:

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

Таблица 5.243 – Команда назначения списка ACL интерфейсу.

Команда	***Значение***	***Действие***
service-acl input *access_list* **[profile** *profile_id***]**	access_list: (1..32) символа; profile_id: (0..2)	В настройках определённого физического интерфейса команда привязывает указанный список к данному интерфейсу. **Параметр profile доступен только в режиме acl-only.** **В режиме acl-only конфигурирование ACL на VLAN недоступно.**
no service-acl input [profile *profile_id***]**		Удаление списка с интерфейса.

Команды режима Privileged EXEC

Командная строка в режиме Privileged EXEC имеет вид:

```
console#
```

Таблица 5.244 – Команды для просмотра списков ACL

Команда	***Значение***	***Действие***
show access-lists [*access_list***]**	access_list: (1..32) символа	Показывает списки ACL, созданные на коммутаторе.
show access-lists time-range-active [*access_list***]**		Показывает списки ACL, созданные на коммутаторе, которые в настоящее время являются активными.
show interfaces access-lists [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***| vlan** *vlan_id***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); vlan_id: (1..4094); group: (1..12)	Показывает списки ACL назначенные интерфейсам.
clear access-lists counters [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Обнулить все счетчики списков ACL, либо счетчики для списков ACL заданного интерфейса.
show interfaces access-lists counters [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12)	Показывает счетчики списков доступа.

Команды режима EXEC

Командная строка в режиме EXEC имеет вид:

console#

Таблица 5.245 – Команды для просмотра списков ACL

Команда	*Значение*	*Действие*
show time-range *time_name*	time_name: (1..32) символа	Показывает конфигурацию time-range

5.29.1 Конфигурирование 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 5.246 – 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.
protocol	Протокол	Поле предназначено для указания протокола (или всех протоколов), на основе которого будет осуществляется фильтрация. При выборе протокола возможны следующие варианты: arp, icmp, igmp, ip, tcp, egp, igp, 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.**
source	Адрес источника	Определяет IP-адрес источника пакета.
source_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.
destination	Адрес назначения	Определяет IP-адрес назначения пакета.
destination_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 source_wildcard.
vlan	Идентификатор Vlan	Определяет Vlan, для которого будет применяться правило.
dscp	Поле DSCP в заголовке L3	Определяет значение DSCP-поля diffserv. Возможные коды сообщений поля **dscp: (**0 – 63).
precedence	Приоритет IP	Определяет приоритет IP-трафика: (0-7).

time_name	Имя профиля конфигурации time-range	Определяет конфигурацию временных интервалов.
icmp_type	-	Тип сообщений протокола ICMP, используемый для фильтрации ICMP-пакетов. Возможные типы сообщений поля **icmp_type:** 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).
icmp_code	Код сообщения протокола ICMP	Код сообщений протокола ICMP, используемый для фильтрации ICMP-пакетов. Возможные коды сообщений поля **icmp_code:** (0 – 255).
igmp_type	Тип сообщения протокола IGMP	Тип сообщений протокола IGMP, используемый для фильтрации пакетов IGMP. Возможные типы сообщений поля igmp_type**:** *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).
destination_port	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).
source_port	UDP/TCP-порт источника	
list_of_flags	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.
offset_list_name	Наименование списка шаблонов пользователя	Задает использование списка шаблонов пользователя для распознавания пакетов. Для каждого списка ACL может быть определен свой список шаблонов.
index	Индекс правила	Индекс задает 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».

После того как хоть одна запись добавлена в список ACL, последней по умолчанию добавляется запись deny any any any, которая означает игнорирование всех пакетов не удовлетворяющих условиям ACL.

Таблица 5.247 - 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***] [index** *index***]** **[offset-list** *offset_list_name***]**	Добавляет разрешающую запись фильтрации для протокола. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit arp **{any/*source-mac source-mac-wildcard* }** **{any/** *destination mac destination mac wildcard***}** **{any/*sender-ip sender-ip-wildcard* }** **{any/*target-ip target-ip-wildcard*}** **[vlan** *vlan_id***] [index** *index***]**	Добавляет разрешающую запись фильтрации для протокола ARP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit ip **{any|***source_mac source-mac-wildcard***}** **{any|***destination_mac destination_mac_wildcard***}** **{any|***source_ip source_ip_wildcard***}** **{any|***destination_ip destination_ip_wildcard***}** **[dscp** *dscp* **| precedence** *precedence***]** **[time-range** *range_name***] [index** *index***]** **[offset-list** *offset_list_name***]** **[vlan** *vlan_id***]**	Добавляет разрешающую запись фильтрации для протокола IP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
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***] [index** *index***]** **[offset-list** *offset_list_name***]** **[vlan** *vlan_id***]**	Добавляет разрешающую запись фильтрации для протокола ICMP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit igmp **{any|***source source_wildcard* **}** **{any|***destination destination_wildcard***}** **[***igmp_type***]** **[dscp** *dscp* **| precedence** *precedence***]** **[time-range** *time_name***] [index** *index***]** **[offset-list** *offset_list_name***]** **[vlan** *vlan_id***]**	Добавляет разрешающую запись фильтрации для протокола IGMP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
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***] [index** *index***]** **[offset-list** *offset_list_name***]** **[vlan** *vlan_id***]**	Добавляет разрешающую запись фильтрации для протокола TCP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit udp **{any|** *source source_wildcard***}** **{any|** *source_port***}** **{any|***destination destination_wildcard***}** **{any|***destination_port***}** **[dscp** *dscp* **| precedence** *precedence***]**	Добавляет разрешающую запись фильтрации для протокола UDP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.

[time-range *time_name*] **[index** *index*] [**offset-list** *offset_list_name*] **[vlan** *vlan_id*]	
deny *protocol* **{any|***source source_wildcard***}** **{any|***destination destination_wildcard***}** **[dscp** *dscp* **| precedence** *precedence*] **[time-range** *time_name*] **[disable-port|log-input]** **[index** *index*] **[offset-list** *offset_list_name*] **[vlan** *vlan_id*]	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.
deny arp {*any/source-mac source-mac-wildcard* **}** **{any/** *destination mac destination mac wildcard* **}** **{any/***sender-ip sender-ip-wildcard* **}** **{any/***target-ip target-ip-wildcard* **}** **[{log-input} {disable-port}]** **[vlan** *vlan_id*]	Добавляет запрещающую запись фильтрации для протокола ARP. 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.
deny ip **{any|***source_mac source-mac-wildcard***}** **{any|***destination_mac destination_mac_wildcard***}** **{any|***source_ip source_ip_wildcard***}** **{any|***destination_ip destination_ip_wildcard***}** **[dscp** *dscp* **| precedence** *precedence*] **[time-range** *range_name*] **[disable-port|log-input] [index** *index*] **[offset-list** *offset_list_name*] **[vlan** *vlan_id*]	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.
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]** **[index** *index*] **[offset-list** *offset_list_name*] **[vlan** *vlan_id*]	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.
deny igmp {any|*source source_wildcard***}** **{any|***destination destination_wildcard***}** [*igmp_type*] **[dscp** *dscp* **| precedence** *precedence*] **[time-range** *time_name*] **[disable-port|log-input] [index** *index*] **[offset-list** *offset_list_name*] **[vlan** *vlan_id*]	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.
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] [index** *index*] **[offset-list** *offset_list_name*] **[vlan** *vlan_id*]	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.
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] [index** *index*] **[offset-list** *offset_list_name*]	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.

[vlan *vlan_id***]**	
offset-list *offset_list_name* **{** *offset_base offset mask value***}** …	Создаёт список шаблонов пользователя с именем *name*. Имя может включать от 1 до 32 символов. В одной команде может содержаться до пяти шаблонов, состоящих из следующих параметров: *offset_base* – базовое смещение. Возможные значения: L3 – начало заголовка IPv4 L4 – конец заголовка IPv4 *offset* – смещение байта данных в пределах пакета. Базовое смещение принимается за начало отсчета *mask* – маска. В анализе пакета принимают участие только те разряды байта, для которых в соответсвующих разрядах маски задана '1'. value – искомое значение
no offset-list *offset_list_name*	Удаляет созданный ранее список.

5.29.2 Конфигурирование 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 5.248 – 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.
protocol	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.**
source_prefix/ length	Адрес отправителя и его длина	Определяет IPv6-адрес и длину префикса сети (0-128) (количество старших бит адреса) источника пакета.
destination_prefix/ length	Адрес назначения и его длина	Определяет IPv6-адрес и длину префикса сети (0-128) (количество старших бит адреса) назначения пакета.
dscp	Поле DSCP в заголовке L3	Определяет значение DSCP-поля diffserv. Возможные коды сообщений поля **dscp: (**0 – 63).
precedence	Приоритет IP	Определяет приоритет IP-трафика:(0-7).
time_name	Имя профиля конфигурации time-range	Определяет конфигурацию временных интервалов.
icmp_type	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).
icmp_code	Код сообщений протокола ICMP	Используется для фильтрации ICMP-пакетов. Возможные значения поля 0 – 255.

destination_port	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).
source_port	UDP/TCP-порт источника	
list_of_flags	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**.
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.
offset_list_name	Имя списка битовых полей	Задает использование списка шаблонов пользователя для распознавания пакетов. Для каждого списка ACL может быть определен свой список шаблонов.
index	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 5.249 – Команды, используемые для настройки ACL списков на основе IPv6-адресации

Команда	***Действие***
permit *protocol* **{any|***source_prefix/length***}** **{ any|***destination_prefix/length***}** **[dscp** *dscp* **| precedence** *precedence***]** **[time-range** *time_name***]** [**offset-list** *offset_list_name*]	Добавляет разрешающую запись фильтрации для протокола. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit icmp **{any|***source_prefix/length***}** **{ any|***destination_prefix/length***}** **{any|***icmp_type***}** **{any|***icmp_code***}** **[dscp** *dscp* **| precedence** *precedence***]** **[time-range** *time_name***]** [**offset-list** *offset_list_name*]	Добавляет разрешающую запись фильтрации для протокола ICMP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.

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***]** [**offset-list** *offset_list_**name***]	Добавляет разрешающую запись фильтрации для протокола TCP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit udp **{any|***source_prefix/length***}** **{any | *source_port*}** **{ any|***destination_prefix/length***}** **{any| *destination_port*}** **[dscp** *dscp* **| precedence** *precedence***]** **[time-range** *time_name***]** [**offset-list** *offset_list_name*]	Добавляет разрешающую запись фильтрации для протокола UDP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
deny *protocol* **{any|***source_prefix/length***}** **{ any|***destination_prefix/length***}** **[dscp** *dscp* **| precedence** *precedence***]** **[time-range** *time_name***]** **[disable-port|log-input]** [**offset-list** *offset_list_name*]	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.
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]** [**offset-list** *offset_list_name*]	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.
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]** [**offset-list** *offset_list_name*]	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.
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]** [**offset-list** *offset_list_name*]	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.
offset-list *offset_list_name { offset_base offset mask value} …*	Создаёт список шаблонов пользователя с именем *name*. Имя может включать от 1 до 32 символов. В одной команде может содержаться до пяти шаблонов, состоящих из следующих параметров: *offset_base* – базовое смещение. Возможные значения: L3 – начало заголовка IPv4; L4 – конец заголовка IPv4. *offset* – смещение байта данных в пределах пакета. Базовое смещение принимается за начало отсчета

	mask – маска. В анализе пакета принимают участие только те разряды байта, для которых в соответсвующих разрядах маски задана '1'. value – искомое значение
no offset-list *offset_list_name*	Удаляет созданный ранее список.

5.29.3 Конфигурирование 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 5.250 - 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.
source	Адрес отправителя	Определяет MAC-адрес источника пакета.
source_wildcard	Битовая маска, применяемая к MAC-адресу источника пакета	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-адрес 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.
destination	Адрес назначения	Определяет MAC-адрес назначения пакета.
destination_wildcard	Битовая маска, применяемая к MAC-адресу назначения пакета	Маска определяет биты MAC-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Маска используется аналогично маске source_wildcard.
vlan_id	Диапазон значений 0 – 4095	Подсеть VLAN фильтруемых пакетов.
cos	Диапазон значений 0 – 7	Класс обслуживания (CoS) фильтруемых пакетов.
cos_wildcard	Битовая маска, применяемая к классу 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)).
eth_type	Диапазон значений 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.
time_name	Имя профиля	Определяет конфигурацию временных интервалов.

	конфигурации time-range	
offset_list_name	Побайтовое смещение от ключевой точки	Задает использование списка шаблонов пользователя для распознавания пакетов. Для каждого списка ACL может быть определен свой список шаблонов.
index	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, последней по умолчанию добавляется запись deny-any-any, которая означает игнорирование всех пакетов не удовлетворяющих условиям ACL.

Таблица 5.251– Команды, используемые для настройки ACL-списков на основе MAC-адресации

Команда	***Действие***
permit **{any|{***source source-wildcard***}** **{any|***destination destination_wildcard***}** **[vlan** *vlan_id***]** **[cos** *cos cos_wildcard***] [***eth_type***]** **[time-range** *time_name***] [index** *index***]** [**offset-list** *offset_list_name***]**	Добавляет разрешающую запись фильтрации. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
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] [index** *index***]** **[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 *log-input* будет отправлено сообщение в системный журнал.
offset-list *offset_list_name* **{** *offset_base offset mask value***}** …	Создаёт список шаблонов пользователя с именем *name*. Имя может включать от 1 до 32 символов. В одной команде может содержаться до пяти шаблонов, состоящих из следующих параметров: *offset_base* – базовое смещение. Возможные значения: L2 начало смещения от Ethertype- outer-tag начало смещения от STAG inner-tag начало смещения от CTAG src-mac начало смещения с MAC-адреса источника dst-mac начало смещения с MAC-адреса назначения offset.*offset* – смещение байта данных в пределах пакета. Базовое смещение принимается за начало отсчета *mask* – маска. В анализе пакета принимают участие только те разряды байта, для которых в соответсвующих разрядах маски задана ‘1’. value – искомое значение
no offset-list *offset_list_name*	Удаляет созданный ранее список.

5.30 Конфигурирование защиты от DoS-атак

Данный класс команд позволяет блокировать некоторые распространенные классы DoS-атак.

Команды режима глобального конфигурирования

Командная строка в режиме глобального конфигурирования имеет вид:

```
console (config)#
```

Таблица 5.252 – Команды для настройки защиты от DoS-атак

Параметр	*Значение*	*Действие*
security-suite deny martian-addresses {reserved|add *ip_address* **|remove** *ip_address* **}**	*ip_address:* IP-адрес	Запрещает прохождение фреймов с недопустимыми («марсианскими») IP-адресами источника (loopback, broadcast, multicast).
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	-	Включает класс команд security-suite.
no security-suite enable		Отключает класс команд security-suite.

Команды режима конфигурирования интерфейса Ethernet, группы портов.

Командная строка в режиме конфигурирования интерфейса Ethernet, группы портов имеет вид:

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

Таблица 5.253– Команда конфигурирования защиты от DoS-атак для интерфейсов

Команда	*Значение*	*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/удаялет правило, запрещающее прохождение трафика, соответствующего критериям. - **fragmented** – фрагментированные пакеты - **icmp** – ICMP-трафик - **syn** – syn-пакеты
no security-suite deny {fragmented|icmp|syn} {add|remove} {any| *ip_address* **[***mask***]}**		Восстанавливает значение по умолчанию
security-suite dos syn-attack *rate* **{any|** *ip_address* **[***mask***]}**	rate: 5..1000 пакетов в секунду *ip_address*: –IP-адрес mask: маска в формате IP-адреса или префикса	Задает порог syn-запросов на определенный IP-адрес/сеть, при превышении которого лишние фреймы будут отбрасываься
no security-suite dos syn-attack {any| *ip_address* [*mask*]}		Восстанавливает значение по умолчанию

5.31 Качество обслуживания - QOS

По умолчанию на всех портах коммутатора используется организация очереди пакетов по методу FIFO: первый пришел – первый ушёл (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 MES3000, позволяет организовать восемь очередей приоритета пакетов в зависимости от типа передаваемых данных.

Обслуживание очередей

Алгоритмы обслуживания очередей позволяют предоставлять разный уровень QoS трафику разных классов. Каждая очередь занимается пакетами с определенным приоритетом. Требуется, чтобы высокоприоритетный трафик обрабатывался с минимальной задержкой, но

при этом не занимал всю полосу пропускания, и чтобы трафик каждого из остальных типов обрабатывался в соответствии с его приоритетом. Это реализуется при помощи механизма «отсечения хвоста» (tail-drop), использования виртуальных пакетных буферов и настройки размеров очередей.

В коммутаторе имеется настройка по умолчанию для размеров очередей и параметров виртуальных пакетных буферов. При необходимости данную настройку можно изменить при помощи механизма «qos tail-drop profile».

5.31.1 Настройка QoS

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.254 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
qos [basic | advanced]	-/basic	Разрешает коммутатору использовать QoS. - **basic** – базовый режим QoS; - **advanced** – расширенный режим конфигурирования QoS, включающий полный перечень команд настройки QoS.
no qos		Установить механизм передачи данных FIFO. **Настройки QOS при этом будут удалены.**
qos statistics interface	-/disable	Включить режим статистики классификации трафика на физических интерфейсах.
no qos statistics interface		Отключить режими статистики.
qos tail-drop profile *profile_id*	profile_id: (1..4)	Создать профиль **qos tail-drop.**
no qos tail-drop profile *profile_id*		Удалить профиль **qos tail-drop.**
class-map *class_map_name* **[match-all|match-any]**	(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*	(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		Удаляет правило классификации трафика.

policy_map_name		
qos aggregate-policer *aggregate_policer_name committed_rate_kbps excess_burst_byte* **[exceed-action {drop | policed-dscp-transmit}]**	aggregate_policer_name: (1..32) символа committed_rate_kbps: (3..57982058) committed_burst_byte: (3000..19173960)	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». - *committed-rate-kbps* – среднее значение скорости трафика, кбит/с. Данная скорость гарантируется при передаче информации; - *committed-burst-byte* – размер сдерживающего порога в байтах; - **drop** – пакет будет отброшен, когда «корзина» переполнится; - **policed-dscp-transmit** – при переполнении «корзины» значение DSCP будет переопределено. **Нельзя удалить шаблон настроек, если он используется в стратегии policy map, перед удалением следует удалить назначение шаблона стратегии: no police aggregate aggregate-policer-name** **Действует только для режима qos advanced.**
no qos aggregate-policer *aggregate_policer_name*		Удаляет шаблон настроек регулирования скорости канала.
wrr-queue cos-map *queue_id cos1…cos8*	queue_id: (1..8); cos1…cos8: (0..7); Значения CoS по умолчанию для очередей: CoS = 0 – очередь 3 CoS = 1 – очередь 1 CoS = 2 – очередь 2 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 [*queue_id*]		Устанавливает значения по умолчанию.
wrr-queue bandwidth *weight1 weight2 weight3 weight4*	(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 *number_of_queues*	number_of_queues: (0..8) По умолчанию, все очереди обрабатываются по алгоритму «strict priority».	Задает 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 wrr-queue threshold gigabitethernet *queue_id threshold_percentage*	queue_id: (1..8) threshold_percentage: (0..100) По умолчанию значение	Устанавливает пороговые значения для отбрасывания избыточного трафика очереди. **Объем трафика в зависимости от его приоритета сравнивается с соответствующим порогом. Если порог превышен, пакеты с соответствующим**

	пороговых настроек для отбрасывания избыточного трафика равно 80%	**приоритетом сброса будут отбрасываться в течение всего времени, пока порог превышен.** **Действует только для режима qos advanced.**
no qos wrr-queue threshold gigabitethernet *queue_id*		Устанавливает значения порогов по умолчанию
qos wrr-queue wrtd	По умолчанию WRTD выключено	Включает WRTD (Weighted Random Tail Drop) весовой мезанизм удаления пакетов из очередей. **Изменения вступят в силу после перезагрузки устройства.** **После перезагрузки устройства удаляются настройки очередей, в которых были настройки Y-sharing, а также все настройки port-limit. Также запрещаются настройки Y-sharing и настройки port-limit.**
no qos wrr-queue wrtd		Выключает WRTD.
qos map policed-dscp *dscp_list* **to** *dscp_mark_down*	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. - *dscp_list* – определяет до 8 значений DSCP, значения разделяются знаком пробела. - *dscp_mark_down* – определяет новое значение dscp. **Действует только для режима qos advanced.**
no qos map policed-dscp [*dscp_list***]**		Устанавливает значение по умолчанию.
qos map dscp-queue *dscp_list* **to** *queue_id*	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. - *dscp_list* – определяет до 8 значений DSCP, значения разделяются знаком пробела.
no qos map dscp-queue [*dscp_list***]**		Устанавливает значения по умолчанию
qos map dscp-dp *dscp_list* **to** *dp*	dscp_list: (0..63) dp: (0..2) По умолчанию все пакеты имеют приоритет сброса dp=0	Ставит в соответствие значению DSCP приоритет отброса (чем выше числовое значение приоритета, тем ниже вероятность того, что пакет будет отброшен; в первую очередь отбрасываются пакеты с приоритетом сброса 0, затем 1, затем 2) - *dscp_list* – определяет до 8 значений DSCP, значения разделяются знаком пробела. **Действует только для режима qos advanced.**
no qos map dscp-dp [*dscp_list***]**		Устанавливает значения по умолчанию.
qos map dscp-cos *dscp_list* **to** *cos*	dscp_list: (0..63); cos: (0..7)	Заполняет таблицу перемаркировки DSCP. Заменяет значение DSCP на CoS.
no qos map dscp-cos [*dscp_list***]**		Вернуться к значениям по умолчанию.

qos trust {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. **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. **Применить таблицу изменений DSCP возможно только для входящего трафика доверенных портов.** **Действует только для режима qos basic.**
no qos dscp-mutation		Отменяет использование карты изменений dscp.
qos map dscp-mutation *in_dscp* **to** *out_dscp*	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. - *in-dscp* – определяет до 8 значений DSCP, значения разделяются знаком пробела. - *out-dscp* – определяет до 8 новых значений DSCP, значения разделяются знаком пробела. **Действует только для режима qos basic.**
no qos map dscp-mutation [*in_dscp*]	-	Устанавливает значения по умолчанию.
rate-limit *vlan_id rate burst*	vlan_id: (1 .. 4094); rate: (3 .. 57982058) кбит/с burst: (3000 .. 19173960) байт /128кбайт	Устанавливает ограничение скорости для входящего трафика для заданной VLAN. - *vlan_id* – номер VLAN: - *rate* – средняя скорость трафика (CIR), кбит/с; - *burst* – размер сдерживающего порога (ограничение скорости) в байтах.
no rate-limit		Снимает ограничение скорости входящего трафика.

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 5.255 – Команды режима редактирования списка критериев классификации трафика

Команда	*Значение*	*Действие*
match access-group *acl_name*	(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 *acl_name*		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 5.256 - Команды режима редактирования стратегии классификации трафика

Команда	*Значение*	*Действие*
class *class_map_name* [**access-group** *acl_name*]	(1..32) символов	Определяет правило классификации трафика и входит в режим конфигурирования правила классификации – policy-map class. - *acl_name* – определяет правила фильтрации трафика по списку ACL для классификации. При создании нового правила классификации, опциональный параметр access-group обязателен. **Для того чтобы использовать настройки стратегии policy-map для интерфейса, используйте команду service-policy в режиме конфигурации интерфейса.** **Действует только для режима qos advanced.**
no class *class_map_name*		Удаляет правило классификации трафика class-map из стратегии policy-map.

Команды режима конфигурирования правила классификации

Вид запроса командной строки режима конфигурирования 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 5.257 – Команды режима конфигурирования правила классификации

Команда	*Значение*	*Действие*
trust [cos | dscp | cos-dscp]	По умолчанию режим доверия не установлен	Определяет режим доверия к определенному типу трафика. Данной командой выбирается значение, которое QoS будет использовать в качестве внутреннего DSCP. - **cos** – в качестве внутреннего DSCP используется CoS; - **dscp** – в качестве внутреннего DSCP используется DSCP входящих пакетов (значение по умолчанию); - **cos-dscp** – в качестве внутреннего DSCP используется DSCP входящих пакетов, если это IP-пакеты, иначе CoS. **Действует только для режима qos advanced.**
no trust		Устанавливает значение по умолчанию.
set {**dscp** *new_dscp* | **queue** *queue_id* | **cos** *new_cos*}	new_dscp: (0..63) queue_id: (1..8) new_cos: (0..7)	Устанавливает новые значения для IP-пакета. **Команда set является взаимоисключающей с командой trust для одной и той же стратегии policy-map.** **Стратегии policy-map, использующие команды set, trust или имеющий классификацию ACL, назначаются только для исходящих интерфейсов.** **Действует только для режима qos advanced.**
no set		Удаляет новые значения для IP-пакета.
police *committed_rate_kbps committed_burst_byte* [**exceed-action {drop | policed-dscp-transmit }**]	committed_rate: (3..12582912) кбит/с committed_burst: (3000..19173960) байт	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». - *committed_rate_kbps* – среднее значение скорости трафика, кбит/с. Данная скорость гарантируется при передаче информации; - *committed_burst_byte* – размер сдерживающего порога в байтах; - **drop** – пакет будет отброшен, когда «корзина» переполнится; - **policed-dscp-transmit** – при переполнении «корзины», значение DSCP будет переопределено. **Действует только для режима qos advanced.**
no police		Отключает регулирование скорости канала.
police agregate *aggregate_policer_name*	(1..32) символов	Назначает правилу классификации трафика шаблон настроек, который позволяет ограничить полосу пропускания канала и в то же время гарантировать определенную скорость передачи данных. **Действует только для режима qos advanced.**
no police agregate *aggregate_policer_name*		Удаляет шаблон настроек регулирования скорости канала из правила классификации трафика.

Команды режима конфигурирования профиля qos tail-drop

Вид запроса командной строки режима конфигурирования профиля qos tail-drop:

```
console# configure
console(config)# qos tail-drop profile profile_id
console(config-tdprofile)#
```

Таблица 5.258 - Команды режима конфигурирования профиля qos tail-drop

Команда	*Значение/Значение по умолчанию*	*Действие*
port-limit *limit*	limit: (0..400)/64	Задать размер пакетного разделяемого пула для порта.
no port-limit		Установить значение по умолчанию.
queue *queue_id* **[limit** *limit***] [without-sharing | with-sharing]**	limit: (0..400)/64; queue_id: (1..8)	Изменить парамеры очереди: - *queue_id* – номер очереди; - *limit* – количество пакетов в очереди; - **without-sharing** –запретить доступ к общему пулу; - **with-sharing** – разрешить доступ к общему пулу.
no queue *queue_id*		Установить значение по умолчанию.

Команды режима конфигурирования интерфейса Ethernet, группы портов

Вид запроса командной строки режима конфигурирования интерфейса Ethernet, группы портов:

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

Таблица 5.259 – Команды режима конфигурирования интерфейса Ethernet, группы портов

Команда	*Значение*	*Действие*
service-policy input *policy_map_name*	(1..32) символов	Назначает интерфейсу стратегию классификации трафика. **В одном направлении интерфейсом поддерживается только одна стратегия классификации трафика.** **Действует только для режима qos advanced.**
no service-policy input		Удаляет стратегию классификации трафика с интерфейса.
traffic-shape	committed_rate:	Устанавливает ограничение скорости для исходящего

committed_rate [*committed_burst*]	(36..1000000) кбит/с committed_burst: (4096..16769020) байт	трафика через интерфейс. - *committed_rate* – средняя скорость трафика, кбит/с; - *committed_burst* – размер сдерживающего порога (ограничение скорости) в байтах.
no traffic-shape		Снимает ограничение скорости исходящего трафика через интерфейс.
traffic-shape queue *queue_id committed_rate* [*committed_burst*]	committed_rate: (36..1000000) кбит/с committed_burst: (4096..16769020) байт queue_id: (0-8)	Устанавливает ограничение скорости трафика через интерфейс для исходящей очереди. - *committed_rate* – средняя скорость трафика, кбит/с; - *committed_burst* – размер сдерживающего порога (ограничение скорости) в байтах.
no traffic-shape queue *queue_id*		Снимает ограничение скорости трафика через интерфейс для исходящей очереди.
qos trust	-/включено	Включает базовый механизм qos для интерфейса. **Действует только для режима qos basic.**
no qos trust		Выключает базовый механизм qos для интерфейса.
rate-limit *rate* [*burst*]	rate: (3 .. 10000000) кбит/с burst: (3000 .. 19173960) байт /128кбайт	Устанавливает ограничение скорости для входящего трафика. **Данная команда доступна только в режиме конфигурирования интерфейса Ethernet.**
no rate-limit		Снимает ограничение скорости входящего трафика.
qos tail-drop profile *profile_id*	profile_id: (1..4)/-	Использовать заданный профиль на интерфейсе.
no qos tail-drop profile		Значение по умолчанию.
qos cos *default_cos*	(0..7)/0	Устанавливает значение CoS по умолчанию для порта (CoS, применяемый для всего нетегированного трафика, проходящего через интерфейс) **Данная команда доступна только в режиме конфигурирования интерфейса Ethernet.**
no qos cos		Устанавливает значение по умолчанию.

Команды режима конфигурирования интерфейса Vlan

Вид запроса командной строки режима конфигурирования интерфейса Vlan:

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

Таблица 5.260 - Команды режима конфигурирования интерфейса Vlan

Команда	*Значение*	*Действие*
qos cos egress *cos*	cos: (0..7)/0	Устанавливает значение параметра поля приоритета 802.1p для исходящего тегированного трафика.
no qos cos egress		Устанавливает значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.261 – 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) символов	Показывает списки критериев классификации трафика. **Действует только для режима qos advanced.**
show policy-map [*policy_map_name*]	policy_map_name: (1..32) символов	Показывает правила классификации трафика. **Действует только для режима qos advanced.**
show qos aggregate-policer [*aggregate_policer_name*]	aggregate_policer_name: (1..32) символов	Показывает настройки средней скорости, и ограничения полосы пропускания для правил классификации трафика. **Действует только для режима qos advanced.**
show qos interface [buffers | queueing | policers | shapers | rate-limit] [gigabitethernet *gi_port* **| fastethernet** *fa_port* **| port-channel** *group***| vlan** *vlan_id***]**	gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24); group (1..8); vlan_id: (1..4094)	Показывает QoS-параметры для интерфейса. - *vlan_id* – номер VLAN; - *gi_port* – номер интерфейсов Gigabit Ethernet; - *fa_port* – номер интерфейсов Fast Ethernet; - *group* – номер группы портов; - **buffers** – настройки буфера для очередей интерфейса; - **queueing** – 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; - **rate-limit** – ограничение скорости для входящего трафика.
show qos map [dscp-queue | **dscp-dp** | **policed-dscp** | **dscp-mutation | dscp-cos]**	-	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 соответствия меток DSCP и значения CoS.
show qos tail-drop	-	Просмотр параметров tail-drop.
show qos tail-drop [gigabitethernet *gi_port* **| fastethernet** *fa_port***]**	gi_port: (1..3/0/1..28); fa_port: (1..3/0/1..24);	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 (Доступно только в режиме стека).

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-al)# permit tcp any any dscp 12
console(config-ip-al)# permit tcp any any dscp 16
console(config-ip-al)# 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 gigabitethernet 1/0/14
console(config-if)# service-policy input traffic
```

```
console(config-if)# exit
console(config)# interface gigabitethernet 1/0/16
console(config-if)# service-policy input traffic
console(config-if)# exit
console(config)#
```

5.31.2 Статистика QoS

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.262 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
qos statistics aggregate-policer *aggregate_policer_name*	(1..32) символов По умолчанию QoS-статистика отключена	Включает QoS-статистику по ограничению полос пропускания.
no qos statistics aggregate-policer *aggregate_policer_name*		Отключает QoS-статистику по ограничению полос пропускания.
qos statistics queues *set* **{***queue* **| all} {** *dp* **| all} { gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| all}**	set: (1..2) queue: (1..8) dp: (high, low) gi_port: (1..8/0/1..24) te_port:(1..8/0/1..4) Значение по умолчанию: set 1: все приоритеты, все очереди, высокий приоритет сброса. set 2: все приоритеты, все очереди, низкий приоритет сброса.	Включает QoS -статистику для выходных очередей. - *set* – определяет набор счетчиков; - *dp* – определяет приоритет сброса.
no qos statistics queues *set*		Отключает QoS-статистику для выходных очередей.

Команды режима конфигурирования интерфейса Ethernet, группы портов

Вид запроса командной строки режима конфигурирования интерфейса Ethernet, группы портов:

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

Таблица 5.263 – Команды режима конфигурирования интерфейса Ethernet.

Команда	*Значение*	*Действие*
qos statistics policer *policy_map_name class_map_name*	policy_map_name: (1..32) символов class_map_name: (1..32) символов По умолчанию сбор QoS-статистики отключен	Включает сбор QoS-статистики на интерфейсе. - *policy-map_name* – стратегия классификации трафика; - *class_map_name* – список критериев классификации трафика.
no qos statistics policer *policy_map_name class_map_name*		Отключает сбор QoS-статистики на интерфейсе.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.264 – Команды режима EXEC.

Команда	*Действие*
clear qos statistics	Очищает статистику QoS.
show qos statistics	Показывает статистику QoS.

Примеры выполнения команд

Показать сводную информацию о состоянии, настройке и статистике Ethernet-порта (режим отображения статистики классификации трафика)

console#**show interfaces** *GigabitEthernet 1/0/1*

```
gigabitethernet 1/0/1 is down (not connected)
  Interface index is 49
  Hardware is gigabitethernet, MAC address is a8:f9:4b:85:42:c1
  Interface MTU is 1500
  Port is down
  Flow control is off, MDIX mode is off
  15 second input rate is 0 Kbit/s
  15 second output rate is 0 Kbit/s
      0 packets input, 0 bytes received
      0 broadcasts, 0 multicasts
      0 input errors, 0 FCS, 0 alignment
      0 oversize, 0 internal MAC
      0 pause frames received
      0 packets output, 0 bytes sent
      0 broadcasts, 0 multicasts
      0 output errors, 0 collisions
      0 excessive collisions, 0 late collisions
      0 pause frames transmitted
      0 symbol errors, 0 carrier, 0 SQE test error
  Output queues: (queue #: passed/dropped)
      1: 14/20
      2: 0/20
      3: 0/20
      4: 0/20
      5: 0/20
      6: 0/20
      7: 0/20
      8: 0/20
```

- passed - счетчик переданных пакетов
- dropped – количество отброшенных пакетов

5.32 Конфигурация протоколов маршрутизации

5.32.1 Конфигурация статической маршрутизации

Статическая маршрутизация – вид маршрутизации, при котором маршруты указываются в явном виде при конфигурации маршрутизатора. Вся маршрутизация при этом происходит без участия каких-либо протоколов маршрутизации.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

console(config)#

Таблица 5.265 – Команды режима глобального конфигурирования

Команда	*Значение*	*Действие*
ip route *prefix* **{***mask* **|** *prefix_length***}** *gateway* **[metric** distance**] [reject]**	distance: (1..255)/1	Создает статический маршрут. - *prefix* – сеть назначения (например 172.16.0.0); - *mask* – маска сети (в формате десятичной системы исчисления); - *prefix_length* – префикс маски сети (количество единиц в маске – 0..32); - *gateway* – шлюз для доступа к сети назначения; - *distance* – вес маршрута; - **reject** – запрещает маршрутизацию к сети назначения через все шлюзы.
no ip route *prefix* **{***mask* **|** *prefix_length***} [***gateway***]**		Удаляет статический маршрут.
ipv6 route *ipv6_prefix/len gateway* **[metric** *distance***]**	distance: (1..65535)/1	Создает статический IPv6-маршрут. - *ipv6_prefix/len* – префикс сети назначения; - *gateway* – шлюз для доступа к сети назначения; - *distance* – вес маршрута. **Поддерживается только маршрутизация пакетов, формируемых самим коммутатором (трафика с CPU).**
no ipv6 route *ipv6_prefix/len* **[***gateway***]**		Удаляет статический IPv6 маршрут
ip proxy-arp	-/Выключено	Включает режим проксирования ARP-запросов
no ip proxy-arp		Отключает режим проксирования ARP-запросов

Команды режима EXEC

Вид запроса командной строки режима EXEC:

console#

Таблица 5.266 – Команды режима EXEC

Команда	*Действие*
show ip route [connected | static | {address *ip_address* **[***mask* **|** *prefix_length***] [longer-prefixes]}]**	Показывает 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.
sh ipv6 route	Показать таблицу маршрутизации IPv6.

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 5.267– 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.

5.32.2 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 глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

```
console(config)#
```

Таблица 5.268 - Команды режима глобального конфигурирования

Команда	*Значение по умолчанию*	*Действие*
router rip	-	Вход в режим конфигурации протокола RIP.
no router rip		Удаление глобальной конфигурации протокола RIP.

Команды режима конфигурирования протокола RIP

Вид запроса командной строки:

```
console(config-rip)#
```

Таблица 5.269 - Команды режима конфигурирования протокола RIP

Команда	*Значение/Значение по умолчанию*	*Действие*
default-metric [*metric* **]**	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 *A.B.C.D*	A.B.C.D: IP-адрес интерфейса	Устанавливает IP-адрес интерфейса, который будет участвовать в процессе маршрутизации.
no network *A.B.C.D*		Удаляет IP-адрес интерфейса, который будет участвовать в процессе маршрутизации.
redistribute static **[metric transparent]**	-	Разрешает анонсирование статических 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 **[metric transparent]**		Запрещает анонсирование статических маршрутов через RIP.

		- **metric transparent** – запрещает использовать метрику из таблицы маршрутизации**.**
shutdown	-/enabled	Выключают процесс маршрутизации по протоколу RIP.
no shutdown		Включают процесс маршрутизации по протоколу RIP.
clear statistics	-	Очистка счетчиков RIP статистики для всех интерфейсов и соседей.

Команды режима конфигурирования интерфейса ip

Вид запроса командной строки:

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

Таблица 5.270 - Команды режима конфигурирования интерфейса ip

Команда	***Значение/ Значение по умолчанию***	***Действие***
ip rip shutdown	-/enabled	Включают процесс маршрутизации по протоколу RIP на данном интерфейсе.
no ip rip shutdown		Выключают 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 *offset*	offset: (1 .. 15)/1	Добавляет смещение к метрике.
no ip rip offset		Устанавливает значение по умолчанию.
ip rip default-route originate *metric*	metric: (1 .. 15) По умолчанию функция отключена	Устанавливает метрику для маршрута по умолчанию транслируемого через RIP.
no ip rip default-route 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 *key_chain*	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 *clear_text*	clear_text: (1..16) символов	Определяет ключ для аутентификации открытым текстом.
no ip rip authentication-key		Устанавливает значение по умолчанию.
ip rip distribute-list *acl_name*	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 5.271- Команды режима privileged EXEC

Команда	***Значение***	***Действие***
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
```

5.32.3 Настройка протокола OSPF

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.

OSPF не поддерживается в режиме стекирования.

Команды режима глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

```
console(config)#
```

Таблица 5.272 - Команды режима глобального конфигурирования

Команда	*Значение по умолчанию*	*Действие*
router ospf enable	-	Включает маршрутизацию по протоколу OSPF.
no router ospf enable		Выключает маршрутизацию по протоколу OSPF.
router ospf redistribute { connected, rip, static }	-	Разрешает анонсирование маршрутов через OSPF: - **connected** – сетей, объявленных на коммутаторе; - **rip** – маршрутов, полученных через протокол RIP; - **static** – статических маршрутов.
no router ospf redistribute { connected, rip, static }		Устанавливает значение по умолчанию.
router ospf compatible rfc1583	enabled	Включает совместимость с RFC 1583.
no router ospf compatible rfc1583		Выключает совместимость с RFC 1583.
router ospf router-id *A.B.C.D*	-	Устанавливает идентификатор маршрутизатора, который уникально идентифицирует маршрутизатор в пределах одной автономной системы. - *A.B.C.D* – идентификатор маршрутизатора в формате IPv4-адреса.
no router ospf router-id		Устанавливает значение по умолчанию.
router ospf area A.B.C.D	-	Устанавливает идентификатор зоны по умолчанию. Зона - совокупность сетей и маршрутизаторов, имеющих один и тот же идентификатор. - *A.B.C.D* – идентификатор маршрутизатора в формате IPv4-адреса.
no router ospf area		Устанавливает значение по умолчанию.
router ospf area *A.B.C.D* **default-cost** *cost*	cost: (0-16777215)	Устанавливает стоимость суммарного маршрута по умолчанию для зоны типа stub.

		- *A.B.C.D* – идентификатор маршрутизатора в формате IPv4-адреса.
no router ospf area *A.B.C.D* **default-cost**		Устанавливает значение по умолчанию.
router ospf area *A.B.C.D* **nssa**	-	Устанавливает для указанной зоны тип NSSA. - *A.B.C.D* – идентификатор маршрутизатора в формате IPv4-адреса.
no router ospf area *A.B.C.D* **nssa**		Устанавливает для указанной зоны стандартный тип.
router ospf area *A.B.C.D* **stub**	-	Устанавливает для указанной зоны тип stub. - *A.B.C.D* – идентификатор маршрутизатора в формате IPv4-адреса.
no router ospf area *A.B.C.D* **stub**		Устанавливает для указанной зоны стандартный тип.
router ospf area *A.B.C.D* **virtual-link** *E.F.G.H*	-	Устанавливает виртуальный линк для зоны A.B.C.D к маршрутизатору E.F.G.H. - *A.B.C.D* – идентификатор маршрутизатора в формате IPv4-адреса. - *E.F.G.H* – идентификатор маршрутизатора в формате IPv4-адреса.
router ospf area *A.B.C.D* **virtual-link**		Устанавливает для зоны A.B.C.D стандартный тип.

Команды режима конфигурирования интерфейса ip

Вид запроса командной строки:

`console(config-ip)#`

Таблица 5.273 - Команды режима конфигурирования интерфейса ip

Команда	***Значение/ Значение по умолчанию***	***Действие***
ospf	-/disabled	Разрешает конфигурировать OSPF на интерфейсе.
no ospf		Запрещает конфигурировать OSPF на интерфейсе.
ospf enable	-/enabled	Включает маршрутизацию по протоколу OSPF на интерфейсе.
no ospf enable		Выключает маршрутизацию по протоколу OSPF на интерфейсе.
ospf cost *cost*	cost: (1..65535)/10	Устанавливает метрику состояния канала, которая является условным показателем "стоимости" пересылки данных по каналу.
no ospf cost		Устанавливает значение по умолчанию.
ospf priority *priority*	priority: (0..255)/1	Устанавливает приоритет маршрутизатора, который используется для выбора DR и BDR.
no ospf priority		Устанавливает значение по умолчанию.
ospf area *A.B.C.D*	A.B.C.D: идентификатор зоны в формате IPv4-адреса	Устанавливает идентификатор зоны по умолчанию.
no ospf area		Устанавливает значение по умолчанию.
ospf authentication **{ text** *text* **| md5** *key_chain* **}**	text: (1..8) символов key_chain: (1..32) символов По умолчанию аутентификация отключена	Включает аутентификацию в OSPF и определяет ее тип: - *text* – аутентификация открытым текстом; - *key_chain* – имя набора ключей, созданного командой key chain.
no ospf authentication		Устанавливает значение по умолчанию.
ospf dead-interval *interval*	interval: (1..2147483647)/40	Устанавливает интервал времени в секундах, по истечении которого сосед будет считаться "мертвым". Этот интервал должен быть кратным значению hello-interval. Как правило, dead-interval равен 4 интервалам отправки hello-пакетов, то есть 40 секундам.
no ospf dead-interval		Устанавливает значение по умолчанию.
ospf hello-interval *interval*	interval: (1..65535)/10	Устанавливает интервал времени в секундах, по истечении

		которого маршрутизатор отправляет следующий hello-пакет с интерфейса.
no ospf hello-interval		Устанавливает значение по умолчанию.
ospf retransmit-interval *interval*	interval: (1..3600)/5	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).
no ospf retransmit-interval		Устанавливает значение по умолчанию.
ospf transmit-delay *delay*	delay: (1..3600)/1	Устанавливает примерное время в секундах, необходимое для передачи пакета состояния канала.
no ospf transmit-delay		Устанавливает значение по умолчанию.
ospf mtu *mtu*	mtu: (128..10218)	Устанавливает значение MTU (maximum transmission unit) для IP-интерфейса. Если требуется задать MTU более 1500 байт, то необходимо разрешить поддержку «jumbo frame» командой: console(config)# **port jumbo-frame.**
no ospf mtu		Устанавливает значение по умолчанию. MTU по умолчанию: - при включенном « jumbo frame» - 10218; - при отключенном « jumbo frame» - 1500.
ospf passive-interface {default | gigabitethernet *gi_port* **| tengigabitethernet** *te_port***}**	gi_port: (1..8/0/1..24) te_port:(1..8/0/1..4) /disabled	Запрещает IP-интерфейсу обмениваться протокольными сообщениями с соседями через указанный физический интерфейс. При использовании параметра **default** настройка применяется ко всем физическим интерфейсам.
no ospf passive-interface {default | gigabitethernet *gi_port* **| tengigabitethernet** *te_port***}**		Разрешает IP-интерфейсу обмениваться протокольными сообщениями с соседями.

Команды режима privileged EXEC

Вид запроса командной строки в режиме privileged EXEC:

console#

Таблица 5.274 - Команды режима privileged EXEC

Команда	***Значение***	***Действие***
show ip ospf	-	Отображает конфигурации OSPF.
show ip ospf neighbor	-	Отображает информации о OSPF соседях.
show ip ospf neighbor *A.B.C.D*	A.B.C.D: IP-адрес интерфейса	Отображает информации о OSPF соседях на данном IP-интерфейсе.
show ip ospf interface		Отображает конфигурации всех OSPF интерфейсов.
show ip ospf interface *A.B.C.D*	A.B.C.D: IP-адрес интерфейса	Отображает конфигурации конкретного OSPF интерфейса.
show ip ospf database [router] [network] [summary] [asbr-summary] [external] [*A.B.C.D***] [adv-router] [self-originate] [database-summary]**	A.B.C.D: IP-адрес интерфейса E.F.G.H: идентификатор зоны.	Отображает состояние базы данных протокола OSPF.
show ip ospf *E.F.G.H* **database [router] [network] [summary] [asbr-summary] [external] [***A.B.C.D***] [adv-router] [self-originate] [database-summary]**		Отображает состояние базы данных протокола OSPF для указанной зоны.
show ip ospf virtual-links	A.B.C.D: IP-адес	Отображает параметры и текущее состояние виртуальных

[router *A.B.C.D* **]** **[area** *E.F.G.H* **]**	интерфейса E.F.G.H: идентификатор зоны.	линков: - для указанного маршрутизатора (опционально); - для указанной зоны (опционально).

5.32.4 Настройка протокола BFD

Bidirectional Forwarding Detection (BFD) - сетевой протокол, используемый для определения неисправности линка между двумя маршрутизаторами, взаимодействующими друг с другом. BFD устанавливает сессию между двумя конечными точками через определенный линк. Если существует более чем один линк между двумя системами, возможна настройка нескольких BFD-сессий для мониторинга каждого из них. Сессия BFD устанавливается на основании алгоритма "тройного рукопожатия" и разрывается аналогичным способом.

Команды режима глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

```
console(config)#
```

Таблица 5.275 - Команды режима глобального конфигурирования

Команда	*Значение по умолчанию*	*Действие*
router ospf bfd all-interfaces	-	Включает поддержку BFD для OSPF
no router ospf bfd all-interfaces		Выключает поддержку BFD для OSPF

Команды режима конфигурирования интерфейса ip

Вид запроса командной строки:

```
console(config-ip)#
```

Таблица 5.276 - Команды режима конфигурирования интерфейса ip

Команда	*Значение/ Значение по умолчанию*	*Действие*
bfd interval *send_interval* **min_rx** *recv_interval*	send_interval: (50-1000)/- recv_interval: 50-1000)/-	Включает BFD на интерфейсе и устанавливает интервалы отправки и приема BFD-анонсов. Интервал отправки регулирует параметр *send_interval.* Минимальный допустимый интервал приема анонсов регулирует параметр *recv_interval*
no bfd interval		Восстанавливает значение по умолчанию
ospf bfd [disable]	-/включено	Включает/отключает BFD для данного интерфейса

Таблица 5.277 - Команды режима privileged EXEC

Команда	*Значение*	*Действие*
show bfd neighbors	-	Отображает информацию о BFD-соседях

5.32.5 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 master'a повторяется. Наивысший приоритет имеет маршрутизатор с собственным IP-адресом, совпадающим с виртуальным. В случае доступности он всегда становится VRRP master. Максимальное количество VRRP процессов – 50.

Команды режима конфигурирования интерфейсов Ethernet, VLAN, интерфейса группы портов:

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

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

Таблица 5.278 – Команды режима конфигурирования интерфейса Ethernet, VLAN, интерфейса группы портов

Команда	***Значение/Значение по умолчанию***	***Действие***
vrrp *vrid* **description** *text*	vrid: (1-255); text: (1-160 символов).	Добавление описания цели или использования для VRRP маршрутизатора с идентификатором *vrid.*
no vrrp *vrid* **description**		Удаление описания VRRP маршрутизатора.
vrrp *vrid* **ip** *ip_address*	vrid: (1-255)	Определение IP-адреса VRRP маршрутизатора
no vrrp *vrid* **ip [***ip_address* **]**		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.
vrrp *vrid* **preempt**	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. **Маршрутизатор, который является владельцем IP-адреса маршрутизатора, будет перехватывать на себя роль master независимо от настроек данной команды.**
no vrrp *vrid* **preempt**		Установка значения по умолчанию
vrrp *vrid* **priority** *priority*	vrid: (1-255); priority: (1-254). По умолчанию: 255 для владельца IP-адреса, 100 для остальных	Назначение приоритета VRRP маршрутизатора.
no vrrp *vrid* **priority**		Установка значения по умолчанию.
vrrp *vrid* **shutdown**	vrid: (1-255) По умолчанию: выключен	Выключение VRRP протокола на данном интерфейсе
no vrrp *vrid* **shutdown**		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 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**	По умолчанию: 3	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 VRRPv2 анонсы. 2&3 - поддерживается VRRPv3, определенный в RFC5798 с обратной совместимостью с VRRPv2. Получаемые VRRPv2 сообщения обрабатываются маршрутизатором. Отправляются VRRPv2 и VRRPv3 анонсы. Поддерживается только VRRP версии 3. Режимы 2 и 2&3 будут поддерживаться в будущих версиях ПО.
no vrrp *vrid* **version**		Установка значения по умолчанию

Команды режима privileged EXEC

Все команды доступны для привилегированного пользователя.

Вид запроса командной строки режима privileged EXEC:

console#

Таблица 5.279 – Команды режима privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show vrrp [all | **brief** | **interface { gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **/ port-channel** *group* **}]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4); group: (1..12).	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.

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
```

6 СЕРВИСНОЕ МЕНЮ, СМЕНА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

6.1 Меню Startup

Меню ***Startup*** используется для выполнения специальных процедур, таких как: обновление программного обеспечения, удаление содержимого флэш-памяти, восстановление пароля, диагностика, задание скорости работы терминала, работа с параметрами стека устройства.

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]  Download Software
[2]  Erase Flash File
[3]  Password Recovery Procedure
[4]  Set Terminal Baud-Rate
[5]  Stack menu
[6]  Back

Enter your choice or press 'ESC' to exit:
```

Для выхода из меню и загрузки устройства нажмите клавишу **<6>**, 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 6.1 – Описание меню Startup

№	***Название***	***Описание***
<1>	**Download Software** Обновление программного обеспечения	Для загрузки программного обеспечения используется протокол X-Modem. При нажатии клавиши **<1>** на консоль будет выведено следующее сообщение: Downloading code using XMODEM. Теперь, когда устройство готово к приему файла, необходимо передать его при помощи протокола X-Modem. После приема файла устройство перезагрузится автоматически.
<2>	**Erase Flash File** Удаление содержимого флэш-памяти	Данная процедура используется для удаления конфигурации устройства. Для удаления файла нажать клавишу **<2>**, появится предупреждение (подтвердите нажатием клавиши **<y>**): Ввести имя файла конфигурации: Write Flash file name (Up to 8 characters, Enter for none.):CDB File CDB (if present) will be erased after system initialization. ==== Press Enter To Continue ==== Для возврата в меню ***Startup*** нажать клавишу **<enter>**. ==== Press Enter To Continue ====
<3>	**Password Recovery Procedure** Восстановление пароля	Данная процедура используется для восстановления утраченного пароля, она позволяет подключиться к устройству без пароля. Для восстановления пароля нажать клавишу **<3>**, 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 ====
<4>	**Set Terminal Baud-Rate** Задание скорости работы терминала	Процедура используется для установки скорости работы терминала (по умолчанию 115200 Бод). Для задания новой скорости работы терминала нажать клавишу **<5>** и введите значение: Set new device Baud rate: 115200 Для возврата в меню Startup нажать клавишу **<enter>**. ==== Press Enter To Continue ====
<5>	**Stack menu** Работа с параметрами стека устройства	Для увеличения количества портов коммутатора существует возможность объединения устройств в стек. Устройство с идентификатором 1 будет ведущим, остальные - ведомыми. Коммутаторы MES3000 могут работать как автономно, так и в составе стека[1]. Для идентификации и установки режима работы устройства в стеке используется меню стека **(Stack menu)**. Для входа в меню стека нажать клавишу **<5>:** Stack menu [1] Show unit stack id [2] Set unit stack id [3] Set unit working mode [4] Back Enter your choice or press 'ESC' to exit: Описание *Stack menu* указано в таблице 4.3
<6>	**Back** Выход из меню	Для выхода из меню и загрузки устройства нажмите клавишу **<6>**, либо **<esc>**.

Таблица 6.2 – Описание меню Stack menu, работа с параметрами стека устройства

№	***Название меню***	***Описание***
<1>	**Show unit stack id** Просмотр идентификатора устройства в стеке	Для просмотра идентификатора устройства в стеке нажмите клавишу **<1>:** Current working mode is stacking. Unit stack id set to 1.
<2>	**Set unit stack id** Назначение идентификатора устройства в стеке	Для назначения идентификатора устройства в стеке нажмите клавишу **<2>:** Enter unit stack id [0-8]: 1 Unit stack id updated to 1. где значение от «1» до «8» – номер устройства в стеке, значение «0» - автономный режим работы коммутатора. Для возврата в меню стека нажмите клавишу **<enter>.** ==== Press Enter To Continue ====
<3>	**Set unit working mode** Установка режима работы устройства	Для установки режима работы устройства нажмите клавишу **<3>:** Enter unit working mode [1- standalone, 2- stacking]:1 Unit working mode changed to standalone. где значение 1 – автономный режим, значение 2 – режим стекирования. Для возврата в меню стека нажмите клавишу **<enter>.** ==== Press Enter To Continue ====
<4>	**Back** Выход из меню	Для выхода из меню нажмите клавишу **<4>**

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 флэш-памяти. При обновлении, новый файл системного ПО сохраняется в специально выделенной области памяти. При загрузке устройство запускает активный файл системного ПО. Выбор активного файла задается командой:

boot system { **image-1** | **image-2** } [**unit** *unit_id*]

где *unit_id* – номер устройства в стеке (для устройства, работающего в автономном режиме, номер устройства не задается), *image-1, image-2* – файл системного ПО.

При работе в стеке, **если номер устройства не задан, данная команда применяется к ведущему устройству.**

Для просмотра текущей версии системного программного обеспечения, работающего на устройстве, введите команду **show version**:

console#**show version**

```
SW version    2.5.44[0b70e656] ( date  24-Nov-2015 time  17:28:25 )
Boot version    0.0.1.2 ( date  12-Dec-2012 time  19:10:41 )
HW version    02.07
CPLD version    03
```

Процедура обновления ПО:

Командой **copy** скопировать новый файл программного обеспечения на устройство в выделенную область памяти (image2). Формат команды:

copy tftp://*tftp_ip_address*/*[directory/]filename* **image**

Пример выполнения команды:

console# **copy tftp://192.168.16.34/file1 image**

```
Accessing file `file1' on 192.168.16.34
Loading file1 from 192.168.16.34:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Copy took 00:01:11 [hh:mm:ss]
```

Знак восклицания указывает на то, что идет процесс копирования. Каждый восклицательный знак соответствует успешной передаче 10 пакетов по 512 байт информации каждый. Точка указывает на то, что в процессе копирования произошел таймаут ожидания пакетов от TFTP-сервера. Несколько точек в строке может означать, что возникла ошибка в процессе копирования.

Командой **boot** выберите активный файл системного ПО для последующей загрузки:

```
console# boot system image-2
```

Если не выбран новый загруженный файл системного ПО активным, то устройство выполнит загрузку с использованием текущего активного образа.

Убедитесь, что правильно выбран активный файл системного ПО. Для просмотра данных о версиях программного обеспечения и их активности введите команду **show bootvar**:

```
console#show bootvar
```

```
Image  Filename   Version               Date                    Status
-----  ---------  -------------------   ---------------------   -----------
1      image-1    2.5.44[0b70e656]      24-Nov-2015  17:28:25   Active*
2      image-2    2.5.44[1537c93f]      12-Nov-2015  15:45:10   Not active
```

Символом «*» отмечается файл программного обеспечения, который будет исполняться при последующей загрузке.

Перезагрузите коммутатор командой **reload**.

```
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'**.

6.2.2 Обновление загрузочного файла устройства (начального загрузчика)

Начальный загрузчик запускается сразу после включения питания устройства. Посредством загрузочного файла осуществляется процедура «тестирования системы при включении» (POST), распаковка и запуск файла системного ПО. При обновлении новый файл начального загрузчика сохраняется на flash на месте старого.

Для просмотра текущей версии загрузочного файла, работающего на устройстве, введите команду **show version**:

```
console#show version
```

```
SW version    2.5.44[0b70e656] ( date  24-Nov-2015 time  17:28:25 )
Boot version    0.0.1.2 ( date  12-Dec-2012 time  19:10:41 )
HW version    02.07
CPLD version    03
```

Процедура обновления ПО:

1. Командой **copy** скопировать новый загрузочный файл на устройство. Формат команды:

copy tftp://*tftp_ip_address*/*[directory/]filename* **boot**

Пример выполнения команды:

console# **copy tftp://192.168.16.34/332448-10018.rfb boot**

```
Erasing file..done.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Copy: 2739187 bytes copied in 00:01:18 [hh:mm:ss]
```

Знак восклицания указывает на то, что идет процесс копирования. Каждый восклицательный знак соответствует успешной передаче 10 пакетов по 512 байт информации каждый. Точка указывает на то, что в процессе копирования произошел таймаут ожидания пакетов от TFTP-сервера. Несколько точек в строке может означать, что возникла ошибка в процессе копирования.

2. Перезагрузите коммутатор командой **reload**.

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 КОНФИГУРИРОВАНИЯ 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 g1 и g2. Ниже приведена схема, изображающая логическую топологию сети.

Рисунок 25 - 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 mstp
console(config)# interface range gigabitethernet 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 add vlan 10,20,30
console(config-mst)# instance 2 add vlan 40,50,60
console(config-mst)# exit
console(config)# do copy running-config startup-config
```

```
01-Oct-2006 01:09:34 %COPY-I-FILECPY: Files Copy - source URL running-config
destination URL flash://startup-config
01-Oct-2006 01:09:44 %COPY-N-TRAP: The copy operation was completed successfully
Copy succeeded
console(config)# do copy startup-config tftp://192.168.16.2/mstp.conf
01-Oct-2006 01:10:44 %COPY-I-FILECPY: Files Copy - source URL flash://startup-
config destination URL tftp://192.168.16.2/mstp.conf
01-Oct-2006 01:10:44 %COPY-N-TRAP: The copy operation was completed successfully
!
Copy: 726 bytes copied in 00:00:01 [hh:mm:ss]
```

```
console(config)# spanning-tree mst 1 priority 0
console(config)# end
```

2. Конфигурация второго коммутатора

```
console# configure
console(config)# interface vlan 1
console(config-if)# ip address 192.168.16.1 /24
console(config-if)# do copy tftp://192.168.16.2/mstp.conf startup-config
```

```
01-Oct-2006 02:17:14 %COPY-I-FILECPY: Files Copy - source URL
tftp://192.168.16.2/mstp.conf destination URL flash://startup-config
...........01-Oct-2006 02:17:27 %COPY-N-TRAP: The copy operation was completed
successfully
!
726 bytes copied in 00:00:13 [hh:mm:ss]
```

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

```
You haven't saved your changes. Are you sure you want to continue ? (Y/N)[N] Y
This command will reset the whole system and disconnect your current session. Do
you want to continue ? (Y/N)[N] Y
Shutting down ...
```

```
console# configure
console(config)# interface vlan 1
console(config-if)# no ip address
console(config-if)# ip address 192.168.16.100 /24
console(config-if)# exit
console(config)# spanning-tree priority 0
console(config)# end
```

3. Конфигурация третьего коммутатора

```
console# configure
console(config)# interface vlan 1
console(config-if)# ip address 192.168.16.1 /24
console(config-if)# do copy tftp://192.168.16.2/mstp.conf startup-config
```

```
01-Oct-2006 02:17:14 %COPY-I-FILECPY: Files Copy - source URL
tftp://192.168.16.2/mstp.conf destination URL flash://startup-config
...........01-Oct-2006 02:17:27 %COPY-N-TRAP: The copy operation was completed
successfully
```

```
!
726 bytes copied in 00:00:13 [hh:mm:ss]
```

console(config-if)# **do reload**

```
You haven't saved your changes. Are you sure you want to continue ? (Y/N)[N] Y
This command will reset the whole system and disconnect your current session. Do
you want to continue ? (Y/N)[N] Y
Shutting down ...
```

console# **configure**
console(config)# **interface vlan** 1
console(config-if)# **no ip address**
console(config-if)# **ip address** 192.168.16.101 /24
console(config-if)# **exit**
console(config)# **spanning-tree mst** 2 **priority** 0
console(config)# **end**

Настройка selective-qinq

Добавление SVLAN

Приведенный здесь пример конфигурации коммутатора демонстрирует, как добавлять метку SVLAN 20 ко всем VLAN за исключением VLAN 27.

console# **show running-config**

```
vlan database
vlan 20,27
exit
!
interface gigabitethernet 1/0/1
 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
!
```

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:

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 100-102
 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
 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

exit
```

Настройка функции IGMP Proxy

Функция маршрутизации многоадресного трафика IGMP Proxy дает возможность коммутатору серии MES3000, используя информацию, получаемую при обработке сообщений протокола IGMP, распознавать сведения о принадлежности интерфейсов к многоадресным группам и осуществлять на основе этих данных пересылку многоадресных данных между сетями.

Данный пример описывает настройку функции IGMP Proxy на коммутаторе.

- в качестве интерфейса к вышестоящей сети 10.1.0.0 использовать VLAN 100;
- в качестве интерфейсов к нижестоящим сетям 10.2.0.0 и 10.3.0.0 использовать VLAN 101 и 102 соответственно;
- на uplink-интерфейсе использовать версию v2 протокола IGMP.

```
console# configure
console (config)# vlan database 100-102
console (config)# ip multicast-routing igmp-proxy
console (config)# ip igmp-proxy version 2
console (config)# interface vlan 100
console (config-if)# ip address 10.1.0.1 /24
console (config-if)# exit
console (config)# interface vlan 101
console (config-if)# ip igmp-proxy vlan 100
console (config-if)# ip address 10.2.0.1 /24
console (config-if)# exit
console (config)# interface vlan 102
console (config-if)# ip igmp-proxy vlan 100
console (config-if)# ip address 10.3.0.1 /24
console (config-if)# exit
```

Настройка multicast-TV VLAN

Функция *«Multicast-TV VLAN»* дает возможность использовать для передачи многоадресного трафика одну VLAN в сети оператора и доставлять этот трафик пользователям даже в том случае, если они не являются членами этой VLAN. За счет функции «Multicast-TV VLAN» может быть сокращена нагрузка на сеть оператора за счет отсутствия дублирования многоадресных данных, например, при предоставлении услуги IPTV.

Схема применения функции предполагает, что порты пользователей работают в режиме «access» или «customer» и принадлежат к любой VLAN за исключением multicast-tv VLAN. Пользователи имеют возможность только получать многоадресный трафик из multicast-tv VLAN и

не могут передавать данные в этой VLAN. Кроме того, в коммутаторе должен быть настроен порт-источник multicast-трафика, который должен быть участником multicast-tv VLAN.

Пример настройки для порта в режиме работы access

1. Включить фильтрацию многоадресных данных:

```
console(config)# bridge multicast filtering
```

2. Настроить VLAN пользователей (VID 100-124), multicast-tv VLAN (VID 1000), VLAN управления (VID 1200):

```
console(config)# vlan database
console(config-vlan)# vlan 100-124,1000,1200
console(config-vlan)# exit
```

3. Настроить порты пользователей:

```
console(config)# interface range fa1/0/1-24
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 100
console(config-if)# switchport access multicast-tv vlan 1000
console(config-if)# bridge multicast unregistered filtering
console(config-if)# exit
```

4. Настроить uplink-порт, разрешив передачу многоадресного трафика, трафика пользователей и управление:

```
console(config)# interface gi1/0/1
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk allowed vlan add 100-124,1000,1200
console(config-if)# exit
```

5. Настроить IGMP snooping глобально и на интерфейсах, добавить привязку групп:

```
console(config)# ip igmp snooping
console(config)# ip igmp snooping vlan 1000
console(config)# ip igmp snooping vlan 100
console(config)# ip igmp snooping vlan 101
console(config)# ip igmp snooping vlan 102
console(config)# ip igmp snooping vlan 103
…
console(config)# ip igmp snooping vlan 124
```

6. Настроить интерфейс управления:

```
console(config)# interface vlan 1200
console(config-if)# ip address 192.168.33.100 255.255.255.0
console(config-if)# exit
```

Пример настройки для порта в режиме customer

Данный тип подключения может быть использован для того, чтобы помечать пользовательские IGMP-report'ы определенных VLAN (CVLAN) отдельными внешними метками (SVLAN).

1. Включить фильтрацию многоадресных данных:

```
console(config)# bridge multicast filtering
```

2. Настроить VLAN пользователей (VID 100), multicast-tv VLAN (VID 1000, 1001), VLAN управления (VID 1200):

```
console(config)# vlan database
console(config-vlan)# vlan 100,1000-1001,1200
console(config-vlan)# exit
```

3. Настроить порт пользователя:

```
console(config)# interface  fa1/0/1
console(config-if)# switchport mode customer
console(config-if)# switchport customer vlan 100
console(config-if)# switchport customer multicast-tv vlan add 1000,1001
console(config-if)# exit
```

4. Настроить uplink-порт, разрешив передачу многоадресного трафика, трафика пользователей и управление:

```
console(config)# interface gi1/0/1
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk allowed vlan add 100,1000-1001,1200
console(config-if)# exit
```

5. Настроить IGMP snooping глобально и на интерфейсах, добавить правила маркировки пользовательских IGMP-report'ов:

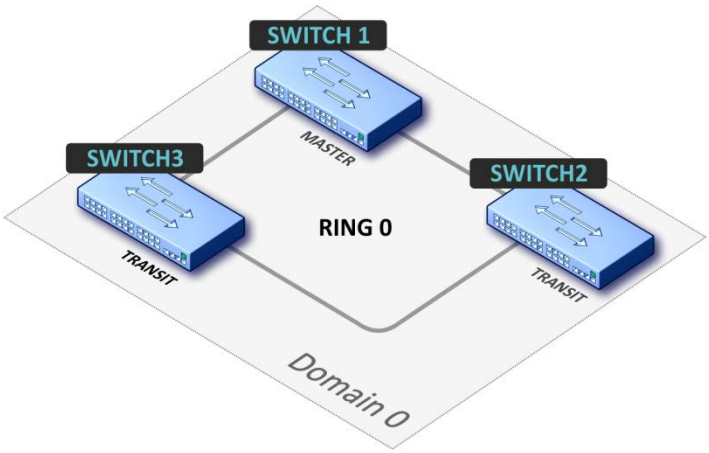
```
console(config)# ip igmp snooping
console(config)# ip igmp snooping vlan 100
console(config)# ip igmp snooping map cpe vlan 5 multicast-tv vlan 1000
console(config)# ip igmp snooping map cpe vlan 6 multicast-tv vlan 1001
```

6. Настроить интерфейс управления:

```
console(config)# interface vlan 1200
console(config-if)# ip address 192.168.33.100 255.255.255.0
console(config-if)# exit
```

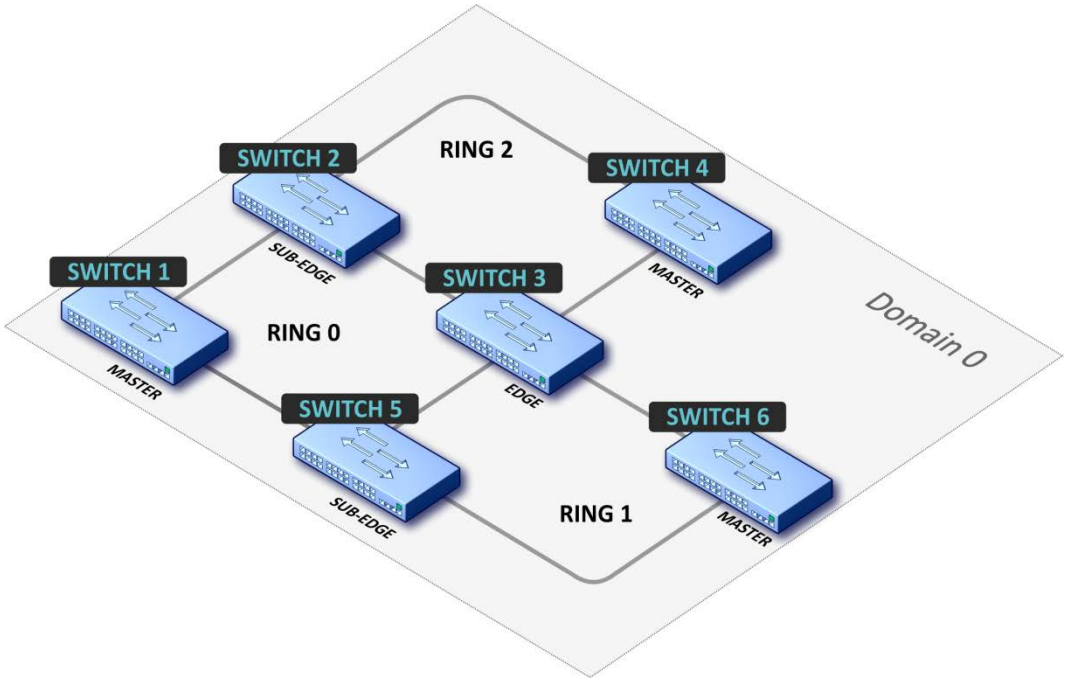
ПРИЛОЖЕНИЕ Б ТИПОВЫЕ СХЕМЫ ПОСТРОЕНИЯ СЕТЕЙ НА БАЗЕ ПРОТОКОЛА EAPS

1. Топология простое «кольцо»



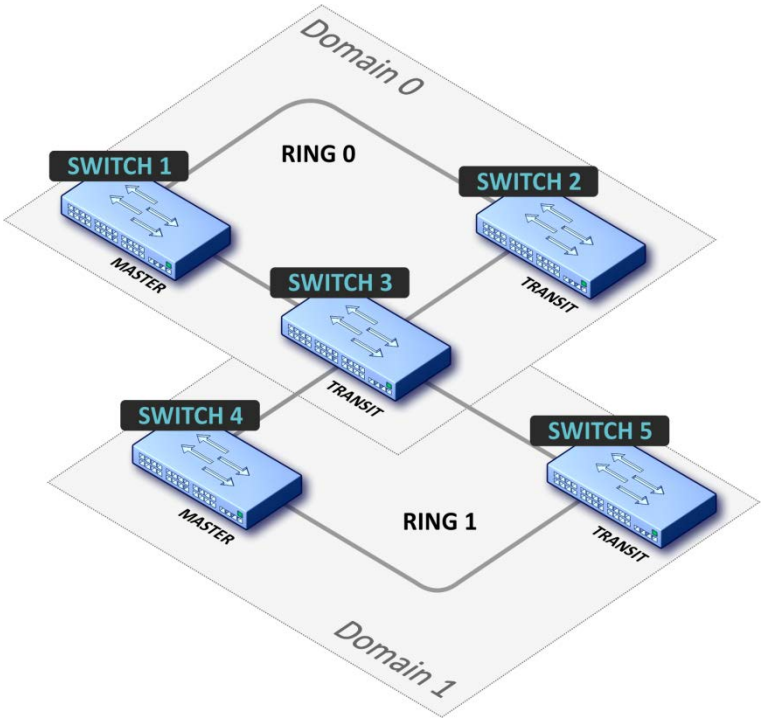
В топологии сети только одно кольцо. В этом случае необходимо определить для него только EAPS domain.

2. Топология один домен с несколькими «кольцами»



В топологии сети 3 кольца (может быть 2 и более) и 2 общих узла между ними. В этом случае необходимо определить EAPS-domain и установить одно кольцо в качестве основного, а другие как вторичные.

3. Топология несколько доменов со смежными «кольцами»



В топологии сети 2 кольца (может быть более двух) с одним общим узлом. В этом случае необходимо определить EAPS-domain для каждого кольца.

ПРИЛОЖЕНИЕ В ОПИСАНИЕ ПРОЦЕССОВ КОММУТАТОРА

Таблица - Описание процессов коммутатора

Имя процесса	Описание процесса
3SMA	Ageing 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 мастера/слейва, изучение топологии, обновление версии ПО слейва
BRGS	Brige security - arp inspection, dhcp snooping, dhcp relay agent, ip source guard, pppoe intermediate agent
BRMN	Bridge Management: EAPS, STP, операции с FDB (добавление, удаление записей), зеркалирование, конфигурирование портов/VLAN, GVRP, GARP, LLDP, IGMP snooping, IP multicast, OAM
BSNC	Автомат синхронизации мастера и слейва в стеке
BTPC	Клиент BOOTP
CDB	Копирование конфигурационных файлов
CFM	Реализация Ethernet CFM
CNLD	Загрузка/выгрузка конфигурации
COPY	Управление копированием файлов
D_LM	Link Manager – поток, который следит за состояние стек-линков
D_SP	Stacking Protocol
DACT	Diacnostic ACTive tests. Поток, в котором выполняются VCT-тесты.
DDFG	Работа с файловой системой
DHCP	Сервер и Relay Agent DHCP
DMNG	Dinstant Manager – получение информации с удаленных юнитов (версия ПО, uptime, установка активного образа ПО)
DNSC	Клиент 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
ESTC	Логирование событий о превышении порогов трафика на CPU (cpu input-rate detailed)
EVAU	Обработка событий Address Update, нижний уровень, передача выше
EVLC	Обработка событий о смене состояния порта, нижний уровень, передача выше
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
FLNK	Функция FlexLink
FTPD	Реализация протокола FTP
FTPM	Управление FTP-сервером (обработка конфигурационных запросов из CLI/SNMP)
GOAH	Реализация web-сервера GoAhead
GRN_	Реализация Green Ethernet
HCLT	Получение и обработка команд настройки устройства нижнего уровня
HDEB	Сбор статистики работы задач системы
HLTX	Отправка пакетов из CPU в коммутатор
HOST	Основной host-поток, холостой ход
HSCS	Stack Config – настройка функций свича на удаленном юните
HSES	Stack Events – обработка событий link changed, address update с удаленных юнитов на мастере
ICMP	Реализация протокола ICMP
IDLE	Бездействие системы
IGMP	Реализация протокола IGMP (хостовой части)
IOD	IO Debug task
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
IPSL	Реализация IP SLA
KEYM	Управление ключами аутентификации
L2HU	Передача пакетов на уровень 3
L2PS	Обработка событий смены состояния/настроек интерфейсов и передача сообщений зарегистрированным службам
L2SC	Логирование storm-control
L2UT	Утилизация портов (show interfaces utilization)
LACP	Реализация протокола LACP (IEEE 802.1AX)
LBDR	Реализация функции Loopback Detection
MACT	Обработка события об окончании действия в FDB (ageing MAC-адресов)
MLDP	Marvell Link Layer Reliable Datagram Protocol, stack transport
MRDP	Marvell Reliable Datagram Protocol, stack transport
MROR	Резервирование конфигурационного файла в энергонезависимой памяти
MSCm	Менеджер для работы с терминальными сессиями
NSCT	Настройка ограничения скорости перехвата пакетов на CPU, ведение статистики по перехваченным пакетам
NTPL	Периодическая генерация сигнала для опроса таблиц MAC, VLAN, портов, мультикаста, маршрутизации, приоритезации
NTST	Добавление и удаление юнитов в стеке, сброс на дефолт состояния юнита, на сетевом уровне
OAM	Реализация Ethernet OAM
OUIs	Обработка команды на восстановление OUI для Voice VLAN
PLCR	Обработка событий смены состояния портов устройств стека
PLCT	Обработка событий смены состояния портов

PNGA	Реализация ping
POLI	Policy Management
PTPT	Precise Time Protocol
ROOT	Родительский таск для всех задач
RPTS	Routing protocol
SCPT	Автообновление и автоконфигурирование
SEAU	Получение событий Address Update, нижний уровень
SELC	Получение событий о смене состояния порта, нижний уровень
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, CLI/SNMP запросов, таймеров
SFSM	sFlow Sampler
SFTR	Протокол Sflow
SNMP	Реализация протокола SNMP
SNPR	Задача, которая разбивает большие SNMP запросы на более мелкие (проксирует)
SNTP	Реализация протокола SNTP
SOCK	Управление работой сокетов
SQIN	Настройка selective qinq
SS2M	Slave To Master – передача сообщений со слейва на мастер
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)
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
STSF	CLI-сессия через VLAN
STSG	CLI-сессия через VLAN
STSH	CLI-сессия через VLAN
STSI	CLI-сессия через VLAN
SW2M	Обработка событий Adress update от FDB, блокировка порта при возникновении ошибок на порту
SWTR	Разрешение прохождения траффика через каскадные интерфейсы
SYLG	Вывод сообщений в syslog
TBI_	Таблица временных промежутков для ACL
TCPP	Реализация протокола TCP
TFTP	Реализация протокола TFTP
TMNG	Управление приоритетами задач
TMON	Monitor Task – отслеживает состояние закольцовки буферов и, в случае обнаружения, перезагружает юнит (другого способа решения проблемы найдено не было)
TNSL	Клиент telnet
TNSR	Сервер telnet
TRCE	Реализация trace route
TRIG	Запуск действия в FDB (ageing MAC-адресов)
TRMT	Управление юнитами в стеке с поддержкой транзакций
TRNS	File Transfer – копирование файлов между юнитами стека (ПО)

TUNT	Реализация туннелей: конфигурирование, обработка пакетов
UDPR	UDP relay
VRRP	Реализация протокола VRRP
WBSR	Управление и таймеры web-сервера
WDHI	Не используется (раньше была связана с watchdog таймером).
WDLO	Сброс watchdog таймера. При срабатывании таймера (это происходит при зависании) коммутатор перезагружается.
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:

Российская Федерация ,630020, г. Новосибирск, ул. Окружная, дом 29 в.
Телефон:
+7(383) 274-47-87
+7(383) 272-83-31
E-mail: techsupp@eltex.nsk.ru

На официальном сайте компании Вы можете найти техническую документацию и программное обеспечение для продукции ООО «Предприятие «Элтекс», обратиться к базе знаний, проконсультироваться у инженеров Сервисного центра на техническом форуме.

Официальный сайт компании: http://eltex.nsk.ru
Технический форум: http://eltex.nsk.ru/forum
База знаний: http://eltex.nsk.ru/support/knowledge
Центр загрузок: http://eltex.nsk.ru/support/downloads