Комплексные решения для построения сетей

MES5000

MES5148, MES5248

Руководство по эксплуатации, версия ПО 2.2.14

Коммутаторы магистрального уровня, коммутаторы уровня агрегации

Версия программного обеспечения		**2.2.14**
Версия документа	**Дата выпуска**	**Содержание изменений**
Версия 1.11	28.04.2018	Изменения: - 5.24.1 Настройка QoS
Версия 1.10	17.10.2017	Изменения: - 5.24.1 Настройка QoS
Версия 1.9	19.05.2017	Изменения: - 5.14.5 Семейство протоколов STP (STP, RSTP, MSTP)
Версия 1.8	13.02.2017	Изменения: - 5.4 Команды управления системой - 5.11 Группы агрегации каналов – Link Aggregation Group (LAG) - 5.14.8 Настройка протокола G.8032v2 (ERPS) - 5.15.1 Правила групповой адресации (multicast addressing) - 5.16.4 Протокол управления сетью (SNMP) - 5.24 Качество обслуживания - QOS
Версия 1.7	29.04.2016	Добавлено: -5.14.6 Реализация Flex-link Изменения: - 5.10 Контроль широковещательного «шторма» - 5.14.5 Семейство протоколов STP (STP, RSTP, MSTP) - 5.18 Зеркалирование (мониторинг) портов
Версия 1.6	31.08.2015	Добавлено: - 5.26 Настройка Virtual Router Redundancy Protocol (VRRP) Изменения: - 5.4 Команды управления системой - 5.8.1 Параметры Ethernet-интерфейсов и интерфейсов Port-Channel - 5.14.2 Настройка протокола ARP - 5.14.5 Семейство протоколов STP (STP, RSTP, MSTP) - 5.16.2 Протокол RADIUS
Версия 1.5	04.02.2015	Добавлено: - 5.6.3 Команды для настройки резервирования конфигурации Изменения: - 5.17 Журнал аварий, протокол SYSLOG - 5.20.1 Диагностика оптического трансивера
Версия 1.4	13.11.2014	Добавлено: - 5.25 Конфигурация протоколов маршрутизации Изменения: - 5.5 Работа коммутатора в режиме стекирования - 5.8 Конфигурирование интерфейсов
Версия 1.3	17.09.2014	Добавлено: - 5.14.4 Механизм обнаружения петель (loopback-detection) Изменения: - 5.8.1 Параметры Ethernet-интерфейсов и интерфейсов Port-Channel
Версия 1.2	03.06.2014	Добавлено: - 5.9 Selective-qinq Изменения: - 5.8.2 Настройка интерфейса VLAN
Версия 1.1	28.04.2014	Добавлено: - 5.2 Фильтрация сообщений командной строки - 5.13.5 Настройка протокола EAPS - 5.13.6 Настройка протокола G.8032v2 (ERPS) Изменения: - 4 Включение и начальная настройка коммутатора - 5.5 Работа коммутатора в режиме стекирования
Версия 1.0	27.06.2013	Первая публикация.

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ 7
2 ОПИСАНИЕ ИЗДЕЛИЯ 8
2.1 Назначение 8
2.2 Функции коммутатора 8
2.2.1 Базовые функции 8
2.2.2 Функции при работе с MAC – адресами 8
2.2.3 Функции второго уровня сетевой модели OSI 9
2.2.4 Функции третьего уровня сетевой модели OSI 10
2.2.5 Функции QoS 11
2.2.6 Функции обеспечения безопасности 11
2.2.7 Функции управления коммутатором 12
2.2.8 Дополнительные функции 13
2.3 Основные технические характеристики 13
2.4 Конструктивное исполнение 14
2.4.1 Передняя панель устройства 15
2.4.2 Задняя панель устройства 16
2.4.3 Боковые панели устройства 17
2.4.4 Световая индикация 17
2.5 Комплект поставки 19
3 УСТАНОВКА И ПОДКЛЮЧЕНИЕ 20
3.1 Крепление кронштейнов 20
3.2 Установка устройства в стойку 20
3.3 Установка модулей питания и вентиляторов. 21
3.4 Подключение питающей сети 22
3.5 Установка и удаление SFP-трансиверов. 23
4 ВКЛЮЧЕНИЕ И НАЧАЛЬНАЯ НАСТРОЙКА КОММУТАТОРА 25
4.1 Включение устройства 25
4.2 Интерфейс начального загрузчика 26
4.3 Выбор режима стекирования 28
4.4 Базовая настройка коммутатора 29
4.4.1 Задание пароля для пользователя «admin» и создание новых пользователей 29
4.4.2 Настройка сетевых параметров доступа 30
4.4.3 Получение IP-адреса от сервера DHCP 31
4.4.4 Настройка параметров протокола SNMP 31
4.5 Настройка параметров системы безопасности 32
4.5.1 Установка пароля для консоли 32
4.5.2 Установка пароля для Telnet 33
4.5.3 Установка пароля для SSH 33
4.6 Настройка баннера 33
5 УПРАВЛЕНИЕ УСТРОЙСТВОМ. ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ 34
5.1 Общие сведения об интерфейсе командной строки 34
5.2 Фильтрация сообщений командной строки 35
5.3 Базовые команды 35
5.4 Команды управления системой 37
5.5 Работа коммутатора в режиме стекирования 41
5.6 Работа с файлами 43
5.6.1 Описание аргументов команд 43
5.6.2 Команды для работы с файлами 43
5.6.3 Команды для настройки резервирования конфигурации 45
5.7 Настройка системного времени 46
5.8 Конфигурирование интерфейсов 50

5.8.1 Параметры Ethernet-интерфейсов и интерфейсов Port-Channel 50
5.8.2 Настройка интерфейса VLAN 56
5.9 Selective Q-in-Q 61
5.10 Контроль широковещательного «шторма» 62
5.11 Группы агрегации каналов – Link Aggregation Group (LAG) 64
5.11.1 Статические группы агрегации каналов 65
5.11.2 Протокол агрегации каналов LACP 65
5.12 Настройка IPv4-адресации 67
5.13 Настройка IPv6-адресации 68
5.13.1 Протокол IPv6 68
5.13.2 Туннелирование протокола IPv6 (ISATAP) 71
5.14 Настройка протоколов 73
5.14.1 Настройка протокола DNS – системы доменных имен 73
5.14.2 Настройка протокола ARP 74
5.14.3 Настройка протокола GVRP 76
5.14.4 Механизм обнаружения петель (loopback-detection) 78
5.14.5 Семейство протоколов STP (STP, RSTP, MSTP) 79
5.14.6 Настройка функции flex-link 85
5.14.7 Настройка протокола EAPS 86
5.14.8 Настройка протокола G.8032v2 (ERPS) 88
5.14.9 Настройка протокола LLDP 89
5.15 Групповая адресация 95
5.15.1 Правила групповой адресации (multicast addressing) 95
5.15.2 Функция посредника протокола IGMP (IGMP Snooping) 100
5.15.3 MLD snooping – протокол контроля многоадресного трафика в IPv6 103
5.16 Функции управления 105
5.16.1 Механизм AAA 105
5.16.2 Протокол RADIUS 109
5.16.3 Протокол TACACS+ 112
5.16.4 Протокол управления сетью (SNMP) 113
5.16.5 Протокол удалённого мониторинга сети (RMON) 117
5.16.6 Списки доступа ACL для управления устройством 124
5.16.7 Настройка локальной и удаленной консоли 126
5.17 Журнал аварий, протокол SYSLOG 129
5.18 Зеркалирование (мониторинг) портов 131
5.19 Функция SFlow 133
5.20 Функции диагностики физического уровня 134
5.20.1 Диагностика оптического трансивера 134
5.21 Функции обеспечения безопасности 136
5.21.1 Функции обеспечения защиты портов 136
5.21.2 Проверка подлинности клиента на основе порта (стандарт 802.1x) 137
5.21.3 Контроль протокола DHCP и опция 82 145
5.21.4 Контроль протокола ARP (ARP Inspection) 149
5.22 Функции DHCP Relay Intermediate Agent 151
5.23 Конфигурирование ACL (списки контроля доступа) 153
5.23.1 Конфигурирование ACL на базе IPv4 154
5.23.2 Конфигурирование ACL на базе IPv6 157
5.23.3 Конфигурирование ACL на базе MAC 160
5.24 Качество обслуживания - QOS 161
5.24.1 Настройка QoS 161
5.24.2 Статистика QoS 169
5.25 Конфигурация протоколов маршрутизации 170
5.25.1 Конфигурация статической маршрутизации 170
5.25.2 Настройка протокола RIP 171

5.25.3 Настройка протокола OSPF 172
5.25.4 Настройка протокола BFD 176
5.26 Настройка Virtual Router Redundancy Protocol (VRRP) 177
6 СМЕНА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ 179
6.1 Обновление программного обеспечения с сервера TFTP 179
6.1.1 Обновление системного программного обеспечения 179
6.1.2 Обновление загрузочного файла устройства (начального загрузчика) 180
7 ПРИМЕРЫ ПРИМЕНЕНИЯ И КОНФИГУРИРОВАНИЯ УСТРОЙСТВА....182
7.1 Настройка протокола множества связующих деревьев (MSTP) 182

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 и 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 MES5000 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 MES5000:

- MES5148 48 портов 10GBaseX(SFP+) или 1000Base-X(SFP), дублированная система электропитания;
- MES5248 48 портов 10GBaseX(SFP+) или 1000Base-X(SFP), управляющий сетевой порт (Management interface), дублированная система электропитания и система вентиляции.

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 MES5000 являются мощными многоцелевыми сетевыми коммутаторами, выполняющими свои коммутационные функции на канальном и сетевом уровнях модели OSI. Коммутаторы серии MES5000 обеспечивают высокую плотность оптических портов, 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 MES5000, 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 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. Поддерживаются пакеты размером до 10 К.
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 до 8 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 MES5000 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. MES5000 поддерживают до 32К MAC-адресов и резервируют определенные MAC-адреса для использования системой.
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.

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
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 MES5000 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.
Private VLAN Edge	Данная функция позволяет изолировать группу портов (в пределах одного коммутатора), находящихся в одном широковещательном домене между собой, позволяя при этом обмен трафиком с другими портами, находящимися в этом же широковещательном домене, но не принадлежащими к этой группе.
Private VLAN (light version)	Обеспечивает изоляцию между устройствами, находящимися в одном широковещательном домене, в пределах всей L2-сети. Реализованы только два режима работы порта Promiscuous и Isolated (Isolated-порты не могут обмениваться друг с другом).
Поддержка протокола STP (Spanning Tree Protocol)	Spanning Tree Protocol — сетевой протокол, основной задачей которого является приведение сети Ethernet с множественными связями к древовидной топологии, исключающей зацикливание пакетов. 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 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 MES5000 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. Сетевой коммутатор позволяет определить до тридцати двух объединенных каналов, каждый из которых может содержать до восьми портов. Группа LAG состоит из портов с одинаковой скоростью, работающих в дуплексном режиме.

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 MES5000 способны автоматически получать IP-адрес по протоколу BootP/DHCP.
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.

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 8 выходных очередей с разными приоритетами для каждого порта. 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 MES5000 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.
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 512 правил, согласно которым пакет будет обработан, либо отброшен.
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 серии MES5000

Загрузка и выгрузка файла настройки	Параметры устройств MES5000 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 MES5000 поддерживает 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 MES5000 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 MES5000 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.

2.2.8 Дополнительные функции

В таблице 2.8 приведены дополнительные функции устройства.

Таблица 2.8 – Дополнительные функции устройства

Диагностика оптического трансивера	Устройство позволяет тестировать оптический трансивер. При тестировании отслеживаются такие параметры, как ток и напряжение питания, температура трансивера. Для реализации требуется поддержка этих функций в трансивере.

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 98DX8248
Интерфейсы	MES5148	48x (10GBase-X(SFP+)/1000Base-X (SFP))
	MES5248	48x (10G Base-X (SFP+)/1000Base-X (SFP)) 1x 10/100/1000BASE-T (RJ-45)
Оптические трансиверы		SFP+/SFP
Дуплексный/Полудуплексный режим		Дуплексный режим для оптических портов
Производительность коммутатора		960 Gbps
Объем буферной памяти		32 Mb
Скорость передачи данных		Оптические интерфейсы 1/10 Гбит/с
Таблица MAC-адресов		32К записей
Поддержка VLAN		согласно 802.1Q до 4К активных VLAN
Качество обслуживания QoS		Приоритезация трафика, 8 уровней. 8 выходных очереди с разными приоритетами для каждого порта.

Multicast		До 4000 статических multicast-групп
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: -48В+30-20% Варианты питания: - один источник питания постоянного или переменного тока; -два источника питания постоянного или переменного тока, с возможностью горячей замены.
Потребляемая мощность, не более	MES5148	280 Вт
	MES5248	350 Вт
Масса		не более 10 кг
Габаритные размеры		450x44x460 мм
Интервал рабочих температур		от 0 до +45 °С
Интервал температуры хранения		от 0 до +45 °С
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 источников 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 MES5000 выполнены в металлическом корпусе с возможностью установки в 19” каркас, высота корпуса 1U.

Коммутаторы имеют фронтальную систему вентиляции, что обеспечивает эффективное охлаждение при использовании устройств в условиях современных ЦОД.

2.4.1 Передняя панель устройства

Внешний вид передней панели MES5148 показан на рисунке 1. Внешний вид передней панели MES5248 показан на рисунке Рисунок 2.

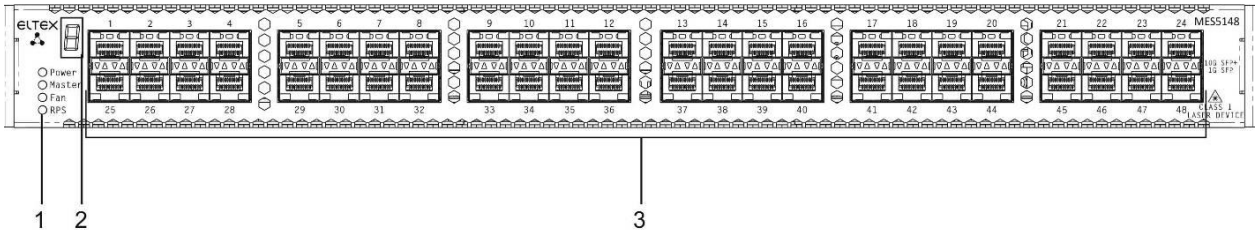


Рисунок 1 – MES5148 передняя панель

В таблице 2.10 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели коммутатора MES5148.

Таблица 2.10 – Описание разъемов, индикаторов и органов управления передней панели MES5148

№	Элемент панели передней	Описание
1	Power	Индикатор питания устройства
	Master	Индикатор режима работы устройства (ведущий/ведомый)
	Fan	Индикатор работы вентиляторов
	RPS	Индикатор резервного электропитания
2		Индикатор номера устройства в стеке
3	[1 .. 48]	48 слотов для установки SFP-трансиверов

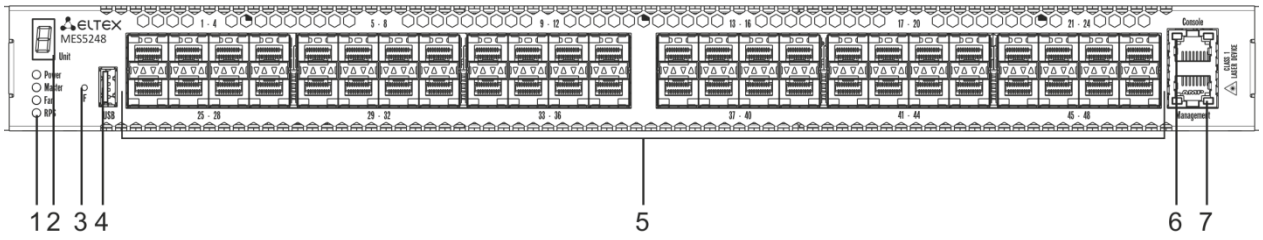


Рисунок 2 – MES5248 передняя панель

В таблице 2.11 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели коммутатора MES5248.

Таблица 2.11 – Описание разъемов, индикаторов и органов управления передней панели MES5248

№	Элемент панели передней	Описание
1	Power	Индикатор питания устройства
	Master	Индикатор режима работы устройства (ведущий/ведомый)
	Fan	Индикатор работы вентиляторов
	RPS	Индикатор резервного электропитания
2	Unit	Индикатор номера устройства в стеке
3	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.
4	USB	USB-порт для подключения внешнего накопителя
5	[1 .. 48]	48 слотов для установки SFP-трансиверов
6	Console	Консольный порт RS-232 для локального управления устройством
7	Management[1]	Ethernet-порт для управления устройством

2.4.2 Задняя панель устройства

Внешний вид задней панели коммутатора MES5148 приведен на рисунке 3.

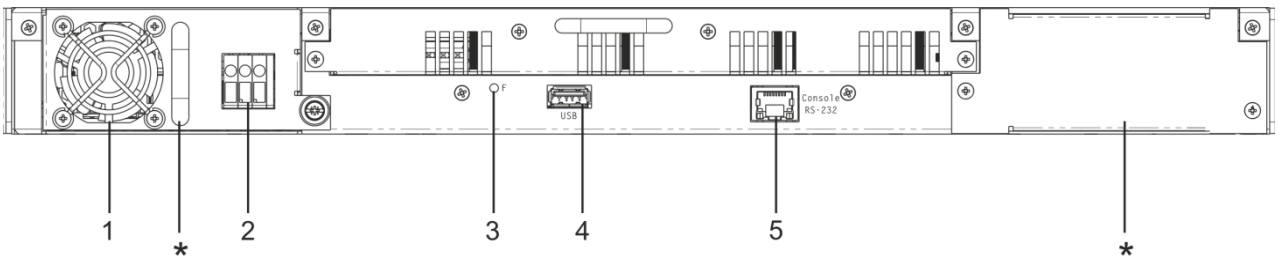


Рисунок 3 - MES5148 задняя панель[2]

В таблице 2.12 приведен перечень разъемов, расположенных на задней панели коммутатора MES5148.

Таблица 2.12 – Описание разъемов задней панели коммутатора MES5148

№	Элемент задней панели	Описание
*		Места для установки модулей питания и вентиляции
1	Вентилятор	Съемный вентиляционный модуль с возможностью горячей замены.
2		Модуль питания

[1] В текущей версии ПО не поддерживается

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

3	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.
4	USB	USB-порт для подключения внешнего накопителя.
5	Console	Консольный порт RS-232 для локального управления устройством

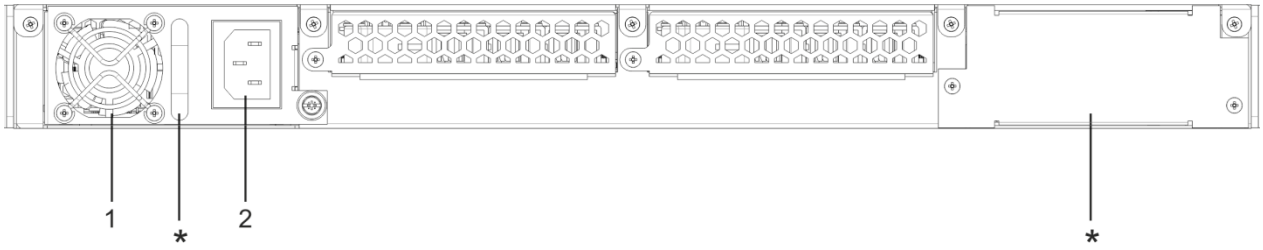


Рисунок 4 - MES5248 задняя панель[1]

В таблице 2.13 приведен перечень разъемов, расположенных на задней панели коммутатора MES5148.

Таблица 2.13 – Описание разъемов задней панели коммутатора MES5148

№	Элемент задней панели	Описание
*		Места для установки модулей питания и вентиляции
1	Вентилятор	Съемный вентиляционный модуль с возможностью горячей замены.
2		Модуль питания

2.4.3 Боковые панели устройства

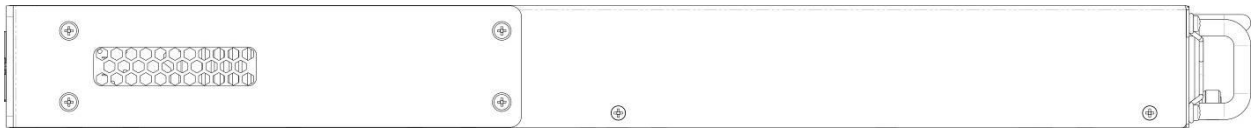


Рисунок 5 – Боковая панель MES5148

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 оптических интерфейсов определяется светодиодными индикаторами.

Значение индикаторов меняется в зависимости от режима:

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

- 1, 3 – индикатор нижнего порта;
- 2, 4 – индикатор верхнего порта;
- 1, 2 – индикатор активности;
- 3, 4 – индикатор скорости.

Расположение светодиодов показано на рисунке 6.

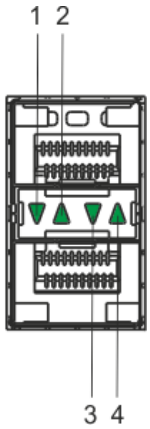


Рисунок 6 – Внешний вид разъема для установки SFP-трансиверов

Таблица 2.14 – Световая индикация состояния оптических интерфейсов

Свечение индикатора скорости	Свечение индикатора активности	Состояние оптического интерфейса
Выключен	Выключен	Порт выключен или соединение не установлено
Выключен	Горит постоянно	Установлено соединение на скорости 1Гбит/с
Горит постоянно	Горит постоянно	Установлено соединение на скорости 10Гбит/с
X	Мигание	Идет передача данных

Индикатор *Unit* служит для обозначения номера устройства в стеке.

Системные индикаторы (Power, Master, Fan, RPS) служат для определения состояния работы узлов коммутаторов серии MES5000. Их значение показано в таблице 2.15.

Таблица 2.15 – Световая индикация системных индикаторов

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Power	Состояние источников питания	Выключен	Питание выключено
		Зеленый, горит постоянно	Питание включено, нормальная работа устройства
		Зеленый, мерцает	Самотестирование устройства при старте (POST)
		Красный	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 серии MES5000;
- Модуль питания PM350-48/12 или PM350-220/12;
- шнур питания (в случае комплектации модулями питания на 220В);
- адаптер консольного порта RJ-45-DB9,
- 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:

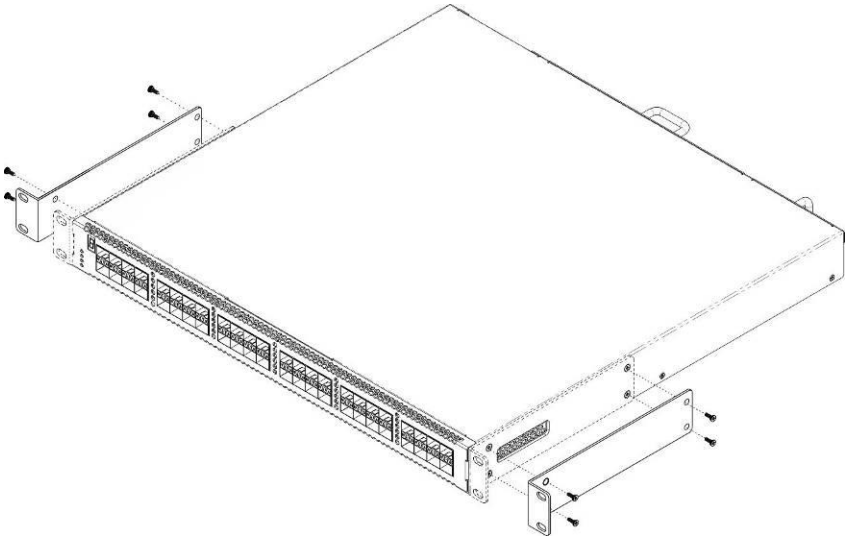


Рисунок 7 – Крепление кронштейнов

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.

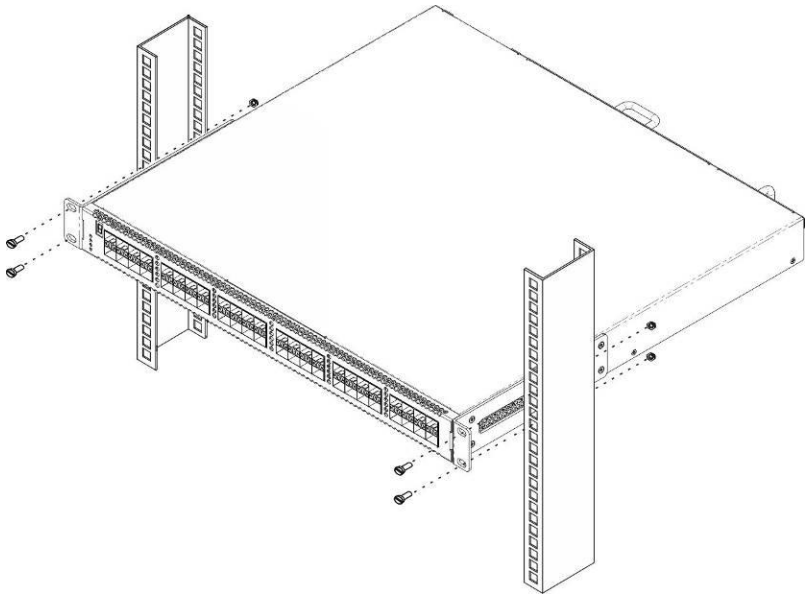


Рисунок 8 – Установка устройства в стойку

На рисунке 9 приведен пример размещения коммутаторов в стойке.

Рисунок 9 – Размещение коммутаторов 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 и вентиляторов.

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 слева, считается основным,

справа – резервным. Модули питания могут устанавливаться и извлекаться без выключения устройства. При установке или извлечении дополнительного модуля питания коммутатор продолжает работу без перезапуска.

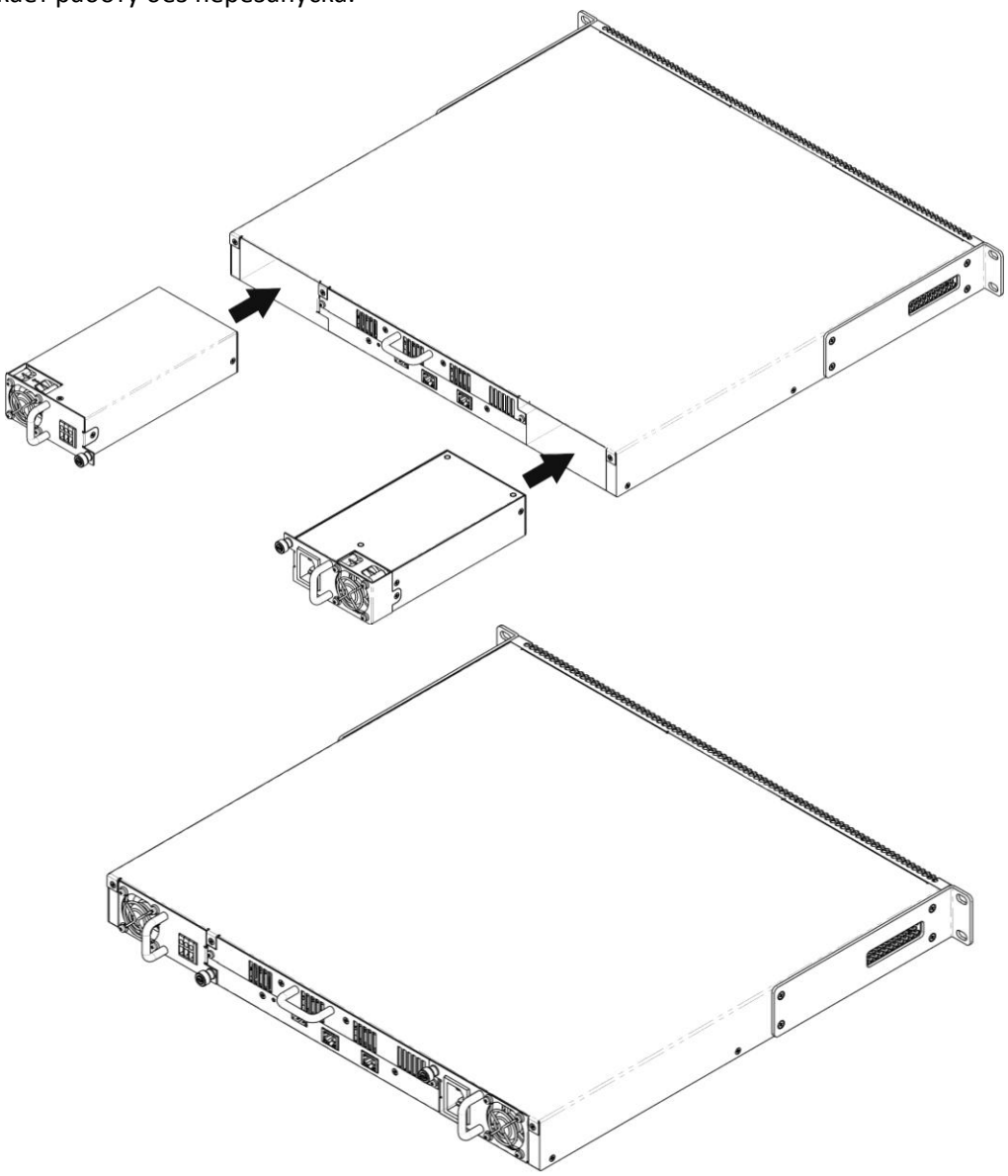


Рисунок 10 – Установка модулей питания.

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 SFP-модуль в слот открытой частью разъема вниз.

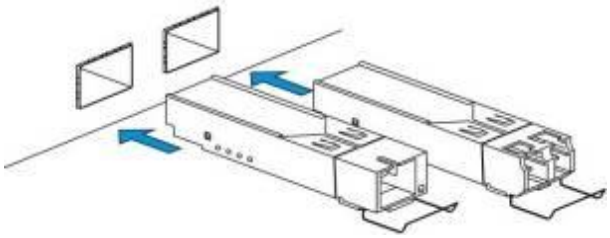


Рисунок 11 – Установка SFP-трансиверов

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

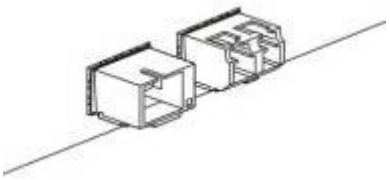


Рисунок 12 – Установленные SFP-трансиверы

Для удаления трансивера:

1. Откройте защелку модуля.

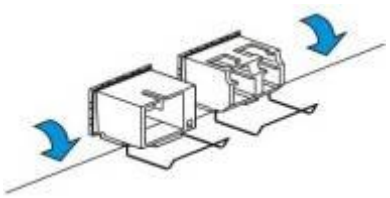


Рисунок 13 – Открытие защелки SFP-трансиверов

2. Извлеките модуль из слота.

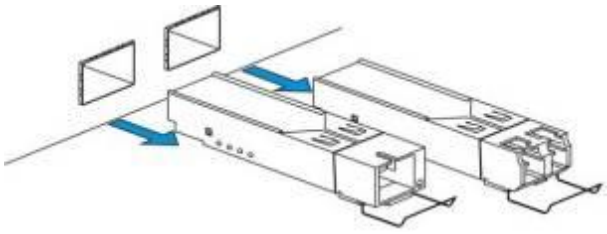


Рисунок 14 – Извлечение SFP-трансиверов

4 ВКЛЮЧЕНИЕ И НАЧАЛЬНАЯ НАСТРОЙКА КОММУТАТОРА

В данном разделе описаны операции, выполнение которых может потребоваться перед началом эксплуатации устройства. Эти операции включают в себя:

- выбор режима стекирования устройства;
- базовое конфигурирование устройства, в том числе:
  - настройка учетной записи администратора;
  - настройка учетных записей пользователей;
  - установка сетевых параметров коммутатора для удаленного доступа;
  - настройка параметров доступа по протоколу SNMP;
- расширенное конфигурирование:
  - конфигурирование параметров безопасности.

Кроме того, в разделе описан порядок старта устройства после подачи питания, приведены объяснения некоторых сообщений во время загрузки программного обеспечения, описан порядок работы с меню начального загрузчика.

4.1 Включение устройства

1. Подготовьте оборудование к работе в соответствии с требованиями раздела 3.
2. Подключите компьютер к консольному порту коммутатора с помощью кабеля.
3. Для связи с коммутатором на компьютере должна быть установлена программа эмуляции терминала, например HyperTerminal. Настройте параметры связи терминала:
   - последовательный интерфейс компьютера (RS-232) - в соответствии с подключением;
   - скорость передачи данных 115200 бод;
   - формат данных 8 бит данных, 1 бит стоповый, без контроля четности (8,n,1);
   - управление потоком данных отключено;
   - режим эмуляции терминала VT100.
4. Включите устройство. При каждом включении коммутатора запускается процедура «тестирования системы при включении» (Power On Self-Testing, POST), которая позволяет проверить работоспособность устройства перед загрузкой исполняемой программы в оперативную память (ОЗУ).

Отображение хода выполнения процедуры POST на коммутаторах серии MES5000:

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

BOOT Software Version 1.0.3.00 Built  25-May-2013  20:36:13
MES-5000 board based on Disco Duo MV78200 ARM926EJ processor
512 MByte SDRAM. I-Cache 32 KB. D-Cache 32 KB. Cache Enabled.

MAC Address    :  a8:f9:4b:02:03:00.

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.

Пример дальнейшей загрузки устройства.

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

OK
Running from RAM...
****************************************************************
*** Running  SW  Ver. 2.1.0  Date  07-Jun-2013  Time  14:00:50 ***
****************************************************************

HW version 01.01.01. CPLD version 1
Base Mac address is: a8:f9:4b:02:03:00
Dram size is  : 512M bytes
Dram first block size is  : 389120K bytes
Dram first PTR is  : 0x8000000
Dram second block size is  : 4096K bytes
Dram second PTR is  : 0x1FC00000
Flash size is: 32M
01-Jan-2010 14:01:00 %CDB-I-LOADCONFIG: Loading running configuration.
01-Jan-2010 14:01:00 %CDB-I-LOADCONFIG: Loading startup configuration.
The monitor is activated with Trace Enabled.
It will be automatic enabled after system reset also.
Device configuration:
Unit 1 - MES-5248

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

Tapi Version: v1.9.4
Core Version: v1.9.4
```

После успешной загрузки коммутатора появится системное приглашение интерфейса командной строки CLI или запрос параметров аутентификации пользователя.

Устройство поставляется производителем с параметрами конфигурации, установленными в начальное состояние.

При этом имя пользователя и пароль не заданы и не запрашиваются системой.

Для быстрого вызова справки о доступных командах используйте комбинацию клавиш «SHIFT» и «?».

4.2 Интерфейс начального загрузчика

Интерфейс начального загрузчика используются 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 управления параметрами начального загрузчика используется система меню (*Startup menu*).

Войти в меню можно во время старта устройства, прервав загрузку нажатием клавиши ***<Esc>*** или ***<Enter>*** в течение двух секунд после появления следующего сообщения.

```
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:
```

Для выхода из меню и продолжения 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 4.1 – 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>**): Warning! About to erase a Flash file. Are you sure (Y/N) ? y Ввести имя файла конфигурации (в примере ниже, имя – CDB): Write Flash file name (Up to 8 characters, Enter for none.):CDB File config (if present) will be erased after system initialization. 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. В стек может быть объединено до 8 устройств, устройство с идентификатором 1 будет ведущим, остальные - ведомыми. Коммутаторы MES5000 могут работать как автономно, так и в составе стека.

		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 Таблица 4.2
<6>	**Back** Выход из меню	Для выхода из меню и загрузки устройства нажмите клавишу **<6>**, либо **<ESC>**.

Таблица 4.2 – 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>**

4.3 Выбор режима стекирования

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 MES5000 работают в режиме автономного устройства.

Выбор режима работы коммутатора доступен в меню начального загрузчика.

```
          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 [5] - управление стеком.

```
     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:
```

В меню управления стеком доступны следующие пункты:

- [1] – отображение идентификатора устройства в стеке;
- [2] – назначение идентификатора устройства;
- [3] – выбор режима работы ([1] – автономный режим, [2] – режим стекирования).

Подробнее о работе устройства в режиме стека можно узнать из пункта 5.5.

4.4 Базовая настройка коммутатора

Базовую настройку коммутатора необходимо выполнить прежде, чем устройство будет установлено на сеть. Основные задачи, которые решаются при проведении базового конфигурирования, это настройка удаленного доступа для определённого круга пользователей, разграничение уровней доступа пользователей, настройка интерфейсов и протоколов доступа.

Описанная далее базовая настройка включает:

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

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

```
console# copy running-config startup-config
```

4.4.1 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#
```

4.4.2 Настройка сетевых параметров доступа

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        Status
------------------- ----------- -----------
192.168.25.54/24      static       Valid
```

4.4.3 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.

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   Status
------------------  ------------ ------
192.168.16.149 /24        DHCP    Valid
```

4.4.4 Настройка параметров протокола SNMP

Устройство содержит встроенного агента 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 MES5000 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      Mask
--------------------- ------------------ -------------- ------------ ------------
      private             read write        Default     192.168.16.44

 Community-String   Group name      IP address              Mask          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 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.

4.5.1 Установка пароля для консоли

Последовательность команд при конфигурировании:

```
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 Установка пароля для Telnet

Последовательность команд при конфигурировании:

```
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'.*

4.5.3 Установка пароля для SSH

Последовательность команд при конфигурировании:

```
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. В приведенном примере пароль *'ssh'*.

4.6 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: Deribasovskaya 10, str.
```

5 УПРАВЛЕНИЕ УСТРОЙСТВОМ. ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ

5.1 Общие сведения об интерфейсе 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)#
```

Для быстрого вызова справки о доступных командах используйте комбинацию клавиш «SHIFT» и «?».

5.2 Фильтрация сообщений командной строки

Фильтрация сообщений позволяет уменьшить объем данных, отображаемых 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 5.1 – Опции фильтрации при отображении данных

Опции	*Действие*
begin *pattern*	Выбирает строки, первые символы которых соответствуют шаблону *pattern*
include *pattern*	Выбирает все строки, содержащие шаблон
exclude *pattern*	Выводит все строки, не содержащие шаблон

- Пример использования фильтрации:

```
console# show running-config | begin interfaces
```

5.3 Базовые команды

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 5.2 – 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 справки разделяется по страницам	Вывести справки по командам 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

Таблица 5.3 – 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 5.4 – 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, доступные в глобальном режиме конфигурирования

Запрос командной строки имеет следующий вид:

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

Таблица 5.5 – 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, доступные в режиме конфигурирования терминала

Запрос командной строки в режиме конфигурирования терминала имеет следующий вид:

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

Таблица 5.6 – 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 size		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	-/ выключен	Включить вывод приветственных сообщений exec.
no exec-banner		Выключить вывод приветственных сообщений exec.

5.4 Команды управления системой

Команды режима EXEC

Таблица 5.7 – 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;

		- source – 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 5.9, 5.10**
traceroute ipv6 **{***A.B.C.D.E.F*|*host***}** **[size** *size***]** **[ttl** *ttl***]** **[count** *count***]** **[timeout** *timeout***]** **[***source* ***ip-address*****]** **[tos** *tos***]**	host: (1..158) символов; size: (66..1518)/66 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.E.F - IPv6-адрес узла сети. - host – доменное имя узла сети; - size – размер пакета для отправки, количество байт в пакете; - ttl – максимальное количество участков в маршруте; - count – количество попыток передачи пакета на каждом участке; - timeout – время ожидания ответа на запрос; - source – 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 5.9, 5.10**
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 5.11 , 5.12**
resume [*connection***]**	(1..4)/последняя установленная сессия	Переключение на другую установленную TELNET-сессию. - connection – номер установленной telnet-сессии.
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 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 (трехмерная 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.**
show mac address-table mode	-	Отображение текущих настроек длины цепочки хэширования MAC-адресов и настроек, применяемых после перезагрузки.

Команды режима privileged EXEC

Запрос командной строки в режиме privileged EXEC имеет следующий вид:

```
console#
```

Таблица 5.8 – Команды управления системой в режиме privileged EXEC

Команда	*Значение/ Значение по умолчанию*	*Действие*
show cpu utilization	-	Отображение статистики по уровню загрузки ресурсов центрального процессора.
clear cpu counters	-	Обнуление счетчиков пакетов центрального процессора.
show system id [unit unit**]**	(1..8)/-	Отображение информации системной идентификации устройства. - unit[1] – 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| network-security| ip-addressing| qos-acl }]	-	Отображение заводских настроек устройства
show system tcam utilization	-	Отображает использование TCAM (Ternary Content Addressable Memory)

- Пример использования команды **traceroute**:

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

```
Tracing the route to eltex.com. (212.2.32.5) from , 30 hops max, 40 byte packets
Type Esc to abort.
 1  192.168.25.1 (192.168.25.1)  <20 ms  <20 ms  <20 ms
 2  router.eltex.loc. (172.16.0.1)  <20 ms  <20 ms  <20 ms
 3   *  *  *
```

Таблица 5.9 – 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 5.10 – 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 MES5000 поддерживает специальные команды – функции контроля терминала. Для входа в режим специальных команд во время активной Telnet-сессии используется комбинация клавиш Ctrl-shift-6.

Таблица 5.11 – 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 5.12 – 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, доступные в режиме глобального конфигурирования:

Запрос командной строки в режиме глобального конфигурирования имеет следующий вид:

```
console(config)#
```

Таблица 5.13 – 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.
service cpu-utilization	-	Разрешение 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 входящего трафика, обрабатываемого центральным процессором коммутатора.

no service cpu-input-rate		Запретить устройству программно измерять скорость входящего трафика, обрабатываемого 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, web-auth, igmp-snooping, mld-snooping, sflow, log-deny-aces, ptp, other pps: (8..1024)	Установка ограничений скорости входящих фреймов для определенного типа трафика. - *traffic* – тип трафика; - *pps* – количество пакетов в секунду.
reset-button {enable | disable| reset-only}	-/enable	Настройка реакции коммутатора на нажатие кнопки F. **- 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.
mac address-table lookup-length *length*	length: (1..8)/3	Установить длину цепочки хэширования таблицы MAC-адресов. Реальное количество адресов в цепочке – *length**4. Изменение длины произойдёт только после перезагрузки коммутатора.
no mac address-table lookup-length		Установить значение по умолчанию.

5.5 Работа коммутатора в режиме стекирования

Стек MES5000 функционирует как единое устройство и может состоять из 8 устройств, имеющих следующие роли, определяемые их порядковыми номерами (UnitID):

- *Master* (UnitID устройства 1) – ведущий коммутатор, он управляет всеми устройствами в стеке.
- *Backup* (UnitID устройства 2) – резервный ведущий коммутатор. Если в стеке присутствует и корректно функционирует устройство с UnitID 1, то этот коммутатор является подчиненным. При выходе из строя master-коммутатора backup берет на себя роль ведущего устройства. В процессе работы происходит синхронизация startup-конфигурации между master и backup.
- *Slave* (UnitID устройств от 3 до 8) – устройства, подчиняющиеся master. Не могут работать в автономном режиме (если отсутствует master и backup).

В режиме стекирования коммутаторы MES5148 и MES5248 используют порты XG47 и XG48 для передачи служебной информации и транзитного трафика между коммутаторами стека. Возможны две топологии при объединении устройств в стек – кольцевая и линейная. Рекомендуется использовать кольцевую топологию для повышения отказоустойчивости стека.

Команды режима privileged EXEC

Запрос командной строки имеет следующий вид:

```
console#
```

Таблица 5.14 – Базовые команды, доступные в режиме privileged EXEC

Команда	***Значение/ значение по умолчанию***	***Действие***
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.
reload [unit *unit_id***]**	unit_id: (1..8)	Команда служит для перезапуска устройства. - *unit_id* – номер устройства в стеке.

Таблица 5.15 – Команды режима глобального конфигурирования

Команда	***Значение/ Значение по умолчанию***	***Действие***
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.
switch *current_id* **renumber** *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.
stack display-order top ***unit-id*** **bottom** *unit_id*	unit_id: (1..8)/-	Изменяет порядок отображения устройств в стеке.
no stack display-order		Установить значение по умолчанию.

- Пример использования команды **show unit**:

```
console# show unit 1

Unit:                    1
MAC address:             a8:f9:4b:87:4b:40
Master:                  Forced.
Product:                 MES-5248. Software: 2.2.4
Uplink unit:             3 Downlink unit: 3.
Status:                  master
Active image:            image2.
Selected for next boot: image2.
Topology is Chain
Stack image auto synchronization is disabled
Unit Num After Reset:    1
```

Таблица 5.16 – 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 (XG47)
Downlink unit	Идентификатор коммутатора, подключенного к порту Downlink (XG48)
Status	Текущая роль коммутатора в стеке
Active image	Активный образ ПО
Selected for next boot	Образ ПО, который будет активным после перезагрузки
Topology	Текущая топология стека - chain (цепочка) или ring (кольцо)
Unit Num After Reset	Идентификатор коммутатора, который применится после перезагрузки

Устройства с одинаковыми U*nit*ID не могут работать совместно в одном стеке.

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 5.17.

Таблица 5.17 – 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 – может быть IPv4-адресом, IPv6-адресом или сетевым именем устройства, directory – каталог, папка, 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 5.18 – 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.
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 |** *<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; - *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 running-config	-	Отображает содержимое файла текущей конфигурации.
show startup-config	-	Отображает содержимое файла первоначальной конфигурации.
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**
rename *url new_url*	url: (1 .. 160)	Изменение имени файла. - *url* – текущее имя файла; - *new_url* – новое имя файла.

Существуют некоторые недопустимые комбинации источника данных 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 к нулевому указателю (null);**
- **сервер TFTP не может быть источником и приёмником данных в одной команде 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 5.19 - 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 передача блока данных прошла неудачно, будет предпринята попытка повторной передачи.

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 настройки резервирования конфигурации

В данном разделе описаны команды настройки резервирования конфигурации по таймеру или при сохранении текущей конфигурации на flash-накопитель.

Команды, доступные в режиме глобального конфигурирования

Запрос командной строки в режиме глобального конфигурирования имеет следующий вид:

```
console(config)#
```

Таблица 5.20 – Команды управления системой в режиме глобального конфигурирования

Команда	*Значение/ Значение по умолчанию*	*Действие*
backup server *server*	server: (1..22) символов	Задает TFTP-сервер, на который будет производиться резервирование конфигурации. Строка в формате «tftp://XXX.XXX.XXX.XXX».
no backup server		Удаляет сервер для резервирования.

backup path *path*	path: (1..128) символов	Указывает путь расположения файла на сервере и префикс файла. При сохранении к префиксу будет добавляться текущая дата и время в формате ггггммддччммсс.
no backup path		Удаляет путь для резервирования.
backup time-period *timer*	timer: (1..35791394) мин/720 мин	Указывает промежуток времени, по истечении которого будет осуществляться автоматическое резервирование конфигурации.
no backup time-period		Восстанавливает значение по умолчанию.
backup auto	/disabled	Включает автоматическое резервирование конфигурации.
no backup auto		Устанавливает значение по умолчанию.
backup write-memory	/disabled	Включает резервирования конфигурации при сохранении пользователем конфигурации на flash.
no backup write-memory		Устанавливает значение по умолчанию.

Таблица 5.21 – Команды управления системой в режиме Privileged EXEC

Команда	*Действие*
show backup	Отображает информацию о настройках резервирования конфигурации.

5.7 Настройка системного времени

Автоматический переход на летнее время осуществляется в соответствии со стандартами США и Европы. Кроме того, возможно переключение на летнее время и обратно в заданные в конфигурации моменты.

Команды режима Privileged EXEC

Запрос командной строки в режиме Privileged EXEC имеет следующий вид:

```
console#
```

Таблица 5.22 - 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 5.23 - 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, доступные в режиме глобального конфигурирования

Запрос командной строки в режиме глобального конфигурирования имеет следующий вид:

```
console(config)#
```

Таблица 5.24 – 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 { tengigabitethernet *te_port* **| port-channel** *group***| vlan** *vlan_id***}**	te_port: (1..8/0/1..48); group: (1..8); 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 { 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 5.25 – 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
```

```
*21:27:33 UTC Jan 1 2010
No time source

Time zone:
Offset is UTC+0
```

- 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 unsynchronized

Unicast servers:
   Server       Status      Last Response     Offset   Delay
                                               [mSec]   [mSec]
--------------- --------- ------------------- --------- -------
Anycast server:

    Server      Interface  Status        Last Response       Offset   Delay
                                                             [mSec]   [mSec]
--------------- --------- --------- ----------------------- --------- -------
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 7.23 с.

5.8 Конфигурирование интерфейсов

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 Меню Startup.

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

5.8.1 Параметры Ethernet-интерфейсов и интерфейсов Port-Channel

Команды режима конфигурирования интерфейса (диапазона интерфейсов)

```
console# configure
console(config)# interface { 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.

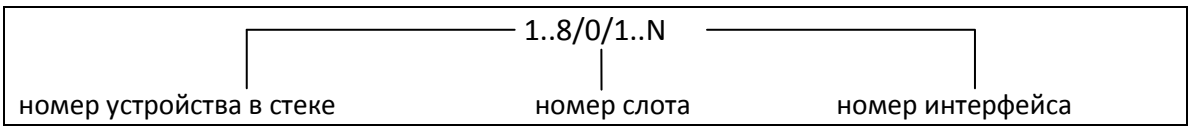
Выбор интерфейса осуществляется при помощи команд:

- **interface tengigabitethernet** *te_port* **–** для настройки интерфейсов Ethernet;
- **interface port-channel** *group* – для настройки группы каналов,

где

- group – порядковый номер группы каналов принимает значения (1..8);
- te_port – порядковый номер интерфейса Ethernet, задается в виде: 1..8/0/1..48.

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 tengigabitethernet 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 tengigabitethernet** *portlist* - для настройки диапазона интерфейсов;
- **interface range port-channel** *grouplist* – для настройки всех 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 tengigabitethernet 1/0/1-10
console(config-if)#

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

Таблица 5.26 – Команды режима конфигурирования интерфейсов 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*	(1..64) символов/ нет описания	Добавить описание интерфейса (Ethernet, port-channel).
no description		Удалить описание интерфейса.
speed *mode*	1000, 10000	Задать скорость передачи данных (Ethernet, port-channel).
no speed		Установить значение по умолчанию.
flowcontrol *mode*	on, off, auto	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.
switchport dot1q ethertype ingress stag { add *tpid_list***| remove** *tpid_list* **}**	tpid_list: (0..ffff (hex))/ 8100	Добавить *tpid_list* в таблицу идентификаторов VLAN. - *tpid_list* – список значений поля TPID. Максимум можно задать 6 значений. **Значение TPID не должно совпадать с зарезервированными номерами протоколов или быть меньше минимального размера.**
no switchport dot1q ethertype ingress stag		Удалить *tpid_list* из таблицы идентификаторов VLAN.
switchport dot1q ethertype egress stag *tpid*	tpid: (0..ffff (hex))/TPID не меняется	Заменить метку TPID в исходящих с данного интерфейса пакетах. **Значение TPID не должно совпадать с зарезервированными номерами протоколов или быть меньше минимального размера.**
no switchport dot1q ethertype egress stag		Устанавливает значение по умолчанию.

Команды режима глобального конфигурирования

Вид запроса командной строки в режиме конфигурирования интерфейса:

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

Таблица 5.27 – Команды режима общих настроек интерфейсов Ethernet и Port-Channel

Команда	*Значение*	*Действие*
port jumbo-frame	-/запрещено	Разрешает коммутатору работать с фреймами большого размера. **Значение maximum transmission unit (MTU) по умолчанию 1628 байт.** **Настройка вступит в силу только после перезагрузки устройства.**
no port jumbo-frame		Запрещает коммутатору работать с фреймами большого размера.
errdisable recovery cause { port-security | dot1x-src-address | acl-deny | stp-bpdu-guard | stp-loopback-guard }	-/запрещено	Включить автоматическую активацию интерфейса после его отключения в следующих случаях: - **port-security** — нарушение безопасности для port security; - **dot1x-src-address** —не прохождение аутентификации, основанной на MAC-адресах пользователей; - **acl-deny** —не соответствие спискам доступа (ACL); - **stp-bpdu-guard** — активация защиты BPDU Guard (передача несанкционированного пакета BPDU через интерфейс); - **stp-loopback-guard** — обнаружение петель.
no errdisable recovery cause { 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.

Команды режима EXEC

Вид запроса командной строки в режиме EXEC:

```
console#
```

Таблица 5.28 – Команды режима EXEC

Команда	*Значение*	*Действие*
clear counters	-	Сброс статистики для всех интерфейсов.
clear counters { tengigabitethernet *te_port***}**	te_port: (1..8/0/1..48);	Сброс статистики для Ethernet-порта.
clear counters port-channel *group*	group: (1..32}	Сброс статистики для группы портов.
set interface active { tengigabitethernet *te_port***}**	te_port: (1..8/0/1..48);	Активирует порт, выключенный командой **shutdown**.
show interfaces configuration [tengigabitethernet *te_port* **| port-channel** *group***]**	te_port: (1..8/0/1..48); group: (1..32)	Показать конфигурацию интерфейсов.
show interfaces mtu { tengigabitethernet *te_port***}**	te_port: (1..8/0/1..48)	Показать значение MTU на интерфейсах.
set interface active port-channel *group*	group: (1..32}	Активирует группу портов, выключенную командой **shutdown**.
show interfaces status	-	Показать состояние всех интерфейсов.

show interfaces status { tengigabitethernet *te_port***}**	te_port: (1..8/0/1..48);	Показать состояние Ethernet-порта.
show interfaces status port-channel *group*	group: (1..32}	Показать состояние группы портов.
show interfaces advertise	-	Показать параметры автосогласования, объявленные для всех интерфейсов.
show interfaces advertise { tengigabitethernet *te_port***}**	te_port: (1..8/0/1..48);	Показать параметры автосогласования, объявленные для Ethernet-порта.
show interfaces advertise port-channel *group*	group: (1..32)	Показать параметры автосогласования, объявленные для группы портов.
show interfaces description	-	Показать описания всех интерфейсов.
show interfaces description { tengigabitethernet *te_port***}**	te_port: (1..8/0/1..48);	Показать описание Ethernet-порта.
show interfaces description port-channel *group*	group: (1..32)	Показать описание группы портов.
show interfaces counters	-	Показать статистику для всех интерфейсов.
show interfaces counters { tengigabitethernet *te_port***}**	te_port: (1..8/0/1..48);	Показать статистику для Ethernet-порта.
show interfaces counters port-channel *group*	group: (1..32}	Показать статистику для группы портов.
show interfaces utilization	-	Показать статистику по нагрузке для всех интерфейсов.
show interfaces utilization [tengigabitethernet *te_port* **| port-channel** *group***]**	te_port: (1..8/0/1..4); group: (1..12)	Показать статистику по нагрузке для Ethernet-интерфейса
show ports jumbo-frame	-	Показать настройку jumbo-frames в коммутаторе.
show errdisable recovery	-	Показать настройки для автоматической повторной активации интерфейса.
show errdisable interfaces [tengigabitethernet *te_port* **| port-channel** *group***]**	te_port: (1..8/0/1..48); group: (1..32)	Показать причину отключения интерфейса/интерфейсов и состояние автоматической активации.

Примеры выполнения команд.

- Показать состояние интерфейсов:

```
console# show interfaces status
```

```
                                  Flow        Link
Port     Type           Speed     control     State             Port Mode
-------- ----------     ------    -------     ---------------   ---------
te1/0/1  10G-Fiber        --        --         Down              Trunk
te1/0/2  10G-Fiber        --        --         Down              Trunk
te1/0/3  10G-Fiber      1000        Off        Up                Access
te1/0/4  10G-Fiber        --        --         Down              Access
te1/0/5  10G-Fiber        --        --         Down              Access

…

te1/0/15 10G-Fiber        --        --         Down              General
te1/0/16 10G-Fiber        --        --         Down              General
te1/0/17 10G-Fiber        --        --         Down              Customer

…
```

- Показать параметры авто-согласования:

```
console# show interfaces advertise
```

```
Port      Type         Neg      Operational Link Advertisement
--------- ------------ -------- ----------------------------------
te1/0/1   10G-Fiber    Disabled                 --
te1/0/2   10G-Fiber    Disabled                 --                …
te1/0/46  10G-Fiber    Disabled                 --
te1/0/47  10G-Fiber    Disabled                 --
te1/0/48  10G-Fiber    Disabled                 --

Ch        Type         Neg      Operational Link Advertisement
--------- ------------ -------- ----------------------------------
Po1            --      Disabled                 --
Po2            --      Disabled                 --
Po3            --      Disabled                 --
…
Po31           --      Disabled                 --
Po32           --      Disabled                 --
```

- Показать статистику по интерфейсам:

```
console# show interfaces counters
```

```
      Port       InUcastPkts  InMcastPkts  InBcastPkts    InOctets
---------------- ------------ ------------ ------------ ------------
    te1/0/1           0            0            0            0
    te1/0/2           0            0            0            0
    te1/0/3           0            0            0            0
    te1/0/4           0            0            0            0
    te1/0/5           0            0            0            0
    te1/0/6           0            0            0            0
    te1/0/7           0            0            0            0
    te1/0/8           0            0            0            0
    te1/0/9           0            0            0            0
    te1/0/10          0            0            0            0
    te1/0/11          0            0            0            0
    te1/0/12          0            0            0            0
    te1/0/13          0            0            0            0
    te1/0/14          0            0            0            0
    te1/0/15          0            0            0            0
    te1/0/16          0            0            0            0
    te1/0/17          0            0            0            0
    te1/0/18          0            0            0            0
    te1/0/19          0            0            0            0
    te1/0/20          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            0            0            0            0

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

```
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 5.29 - 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 интерфейса VLAN

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 5.30 – Команды режима конфигурирования VLAN

Команда	*Значение/значение по умолчанию*	*Действие*
vlan *vlan_range*	vlan_range: (2 .. 4094)	Добавить VLAN, или несколько VLAN.
no vlan *vlan_range*		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).

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 5.31 – 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 | 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 четырех режимах:

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

Таблица 5.32 – Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение/значение по умолчанию*	*Действие*
switchport mode *mode*	access, trunk, general, customer/ trunk	Задать 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.
no switchport access vlan		Установить значение по умолчанию.
switchport trunk allowed vlan add *VLANlist*	VLANlist: (2..4094, all)	Добавить список VLAN для интерфейса.

switchport trunk allowed vlan remove *VLANlist*		Удалить список VLAN для интерфейса.
switchport trunk native vlan *vlan_id*	vlan_id: (1..4095)/ 1 – если установлен VLAN по умолчанию, иначе 4095 – нетегированный трафик отбрасывается	Добавляет указанный VLAN в качестве Default VLAN для данного интерфейса (port default vlan_id – PVID), весь нетегированный трафик, поступающий на данный порт, определяется в данный VLAN.
no switchport trunk native vlan		Установить значение по умолчанию.
switchport general allowed vlan add *VLANlist* **[tagged| untagged]**	VLANlist: (2..4094, all)	Добавить список VLAN для интерфейса. Порт будет передавать: **- tagged** – тегированные, **- untagged** – нетегированные пакеты для VLAN.
switchport general allowed vlan remove *VLANlist*		Удалить список VLAN для интерфейса.
switchport general pvid *vlan_id*	vlan_id: (1..4094)/ 1 – если установлен VLAN по умолчанию, иначе 4095	Добавить идентификатор VLAN порта (PVID) для основного интерфейса.
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 для основного интерфейса, основанное на привязке к протоколу.
no switchport general map protocols-group *group*		Удалить правило классификации.
switchport general map subnets-group *group* **vlan** *vlan_id*	vlan_id: (1..4094) group: (1.. 2147483647)	Установить правило классификации для основного интерфейса, основанное на привязке к подсети.
no switchport general map subnets-group *group*		Удалить правило классификации
switchport customer vlan *vlan_id*	vlan_id: (1..4094)/1	Добавить VLAN для пользовательского интерфейса.
no switchport customer vlan		Установить значение по умолчанию.
switchport forbidden vlan add *VLANlist*	vlan_id: (2..4094, all)/ все VLAN разрешены порту	Добавить VLAN, указанные в команде, в список запрещенных для данного порта. Это может быть использовано для предотвращения добавления порта в VLAN протоколом GVRP.
switchport forbidden vlan remove *VLANlist*	vlan_id: (2..4094, all)/ все VLAN разрешены порту	Исключить VLAN, указанные в команде, из списка запрещенных для данного порта.
switchport protected-port	-	Переводит порт в режим Private VLAN Edge – изоляцию внутри группы портов.
no switchport-protected-port		Восстанавливает значение по умолчанию.

switchport protected { tengigabitethernet *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..48); group: (1..32)	Отменяет маршрутизацию по базе данных изученных MAC-адресов (FDB) и направляет весь одноадресный, многоадресный и широковещательный трафик на порт, указанный в команде.
no switchport protected		Восстанавливает маршрутизацию по базе данных изученных MAC-адресов (FDB).
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**).

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

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

Таблица 5.33 – Команды режима глобального конфигурирования

Команда	*Значение*	*Действие*
vlan database	-	Вход в режим конфигурирования VLAN

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 5.34 – 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.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.35 – Команды режима EXEC

Команда	*Значение*	*Действие*
show vlan protocols-groups	-	Показать информацию о группах протоколов.
show vlan subnets-groups	-	Показать информацию о группах подсетей.
show interfaces switchport { tengigabitethernet *te_port* | **port-channel** *group* **}**	te_port: (1..8/0/1..48); group: (1..32)	Показать конфигурацию порта, группы портов.
show interfaces protected-ports [**tengigabitethernet** *te_port* | **port-channel** *group* **]**	te_port: (1..8/0/1..48); group: (1..32)	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       Name                    Ports                Type      Authorization
---- ---------------- --------------------------- ------------ -------------
 1           1               te1/0/1-48,Po1-32         Default      Required
```

- 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 конфигурацию порта Ethernet 22:

```
console# show interfaces switchport tengigabitethernet 1/0/22
```

```
Port : te1/0/22
Port Mode: Access
Gvrp Status: disabled
Ingress Filtering: true
Acceptable Frame Type: admitAll
Ingress UnTagged VLAN ( NATIVE ): 1
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
-------- -------
Mac based VLANs:
Group ID Vlan ID
-------- -------
Subnet based VLANs:
Group ID Vlan ID
-------- -------
```

5.9 Selective Q-in-Q

Данная функция позволяет выполнять манипуляции с внешней меткой VLAN пакетов данных и фильтровать трафик на основе сконфигурированных правил.

Пример выполняемых действий:

- выборочное добавление второй метки VLAN на основании принадлежности данных к VLAN;
- выборочная замена внешней метки VLAN;
- фильтрация (запрет или разрешение прохождения) данных на основании принадлежности их к VLAN.

Обработка производится на основании списка правил, назначаемых на интерфейсы коммутатора. При обработке данных список просматривается последовательно в порядке создания правил. Применяется только первое из правил, которому соответствуют параметры пакета. Создаются раздельные правила для входящего и исходящего трафика.

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

Вид запроса командной строки режима конфигурирования интерфейса:

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

Таблица 5.36 – 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	vlan_id: (1..4094)	Создает правило, на основании которого внешняя метка

override_vlan *vlan_id* **[ingress_vlan** *ingress_vlan_id***]**	*ingress_vlan_id*:(1..4094)	*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* **[ingress_vlan** *ingress_vlan_id***]**	vlan_id (1..4094) ingress_vlan_id (1..4094)	Создает правило, на основании которого внешняя метка *ingress_vlan_id* исходящего пакета будет заменяться на vlan_id. Если *ingress_vlan_id* не указывать – правило будет применяться как правило по умолчанию.
no selective-qinq list ingress [ingress-vlan *ingress_vlan_id***]**	*ingress_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 *ingress_vlan_id*	*ingress_vlan_id:* (1-4094)	Удаляет список правил selective qinq для исходящих пакетов.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.37 – Команды режима EXEC

Команда	***Значение***	***Действие***
show selective-qinq [interface {**tengigabitethernet** *te_port***| port-channel** *group* }]	te_port: (1..8/0/1..48); group: (1..32)	Отображает список правил selective qinq для указанного порта

Примеры выполнения команд.

- Создать правило для интерфейса te 1/0/1, на основании которого внешняя метка входящего пакета 11 будет заменяться на 100.

```
console# configure
console(config)# interface tengigabitethernet 1/0/1
console(config-if)# selective-qinq list ingress override_vlan 10
ingress_vlan 11
console(config-if)# exit
```

- Отобразить список созданных правил selective qinq:

```
console# show selective-qinq
Direction Interface Rule type       Vlan ID   Classification     by Parameter
--------- --------- --------------- -------- ---------------- ------------------
ingress   te1/0/1     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 передаваемого и 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 5.38 – 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-multicast unknown-unicast	-/функция выключена	Добавляет контроль неизвестного одноадресного трафика к контролю широковещательного.
no storm-control include-multicast unknown-unicast		Выключает контроль неизвестного одноадресного 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 level kbps *rate*	(3500-1000000)/ 100000 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 5.39 – Команды режима EXEC

Команда	*Значение*	*Действие*
show storm-control [**tengigabitethernet** *te_port*]	te_port: (1..8/0/1..48)	Показывает конфигурацию функции контроля широковещательного «шторма» для указанного порта, либо всех портов.

Примеры выполнения команд

Включить контроль широковещательного, многоадресного и неизвестного одноадресного трафика на интерфейсе Ethernet te1/0/15. Установить максимальную скорость для контролируемого трафика – 5000 Кб/с:

```
console# configure
console(config)# interface tengigabitethernet 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 Aggregation Group (LAG)

Коммутаторы MES5000 обеспечивает поддержку до восьми интерфейсов Ethernet в одной группе портов LAG и до тридцати двух 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 5.40 – Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение*	*Действие*
channel-group *group* **mode** *mode*	group (1..32) mode (on, auto)	Добавить ethernet-интерфейс в группу портов (on – добавить порт в канал без lacp, auto – добавить порт в канал с lacp).
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 5.41 – Команды режима глобального конфигурирования

Команда	*Значение*	*Действие*
port-channel load-balance {src-dst-mac-ip|src-dst-mac|src-dst-ip|src-dst-mac-ip-port} [mpls-aware]	src-dst-mac	Задает механизм балансировки нагрузки для группы агрегированных портов. - **src-dst-mac-ip –** Механизм балансировки основывается на MAC-адресе и IP-адресе; - **src-dst-mac –** Механизм балансировки основывается на MAC-адресе; - **src-dst-ip –** Механизм балансировки основывается на IP-адресе; - **src-dst-mac-ip-port –** Механизм балансировки основывается на MAC-адресе, IP-адресе и порте

		назначения ; - **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 5.42 – Команды режима EXEC

Команда	*Значение*	*Действие*
show interfaces port-channel [*group***]**	group (1..32)	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 5.43 – 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 5.44 – 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 5.45 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show lacp {tengigabitethernet *te_port* **} [parameters | statistics | protocol-state]**	te_port: (1..8/0/1..48);	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..32)	Показывает информацию о протоколе LACP для группы портов.

Примеры выполнения команд

- Создать первую группу портов, работающую по протоколу LACP и включающую два интерфейса Ethernet – te1/0/3 и te1/0/4. Скорость работы группы – 1000 Мбит/с. Установить приоритет системы – 6, приоритеты 12 и 13 для портов te1/0/3 и te1/0/4 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 tengigabitethernet 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 tengigabitethernet 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.

В режиме коммутатора нельзя задать более одного IP-адреса для устройства.

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 5.46 – Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение*	*Действие*
ip address *ip_address mask* **[***gateway*| prefix-length**]**	ip_address:(A.B.C.D) gateway:(A.B.C.D) prefix-length:(8 .. 30)	Назначение физическому интерфейсу Ethernet IP-адреса, маски подсети, адреса шлюза по умолчанию
no ip address [*ip_address***]**		Удаление IP-адреса на физическом интерфейсе Ethernet.
ip address dhcp	(1..20) символов	Получение IP-адреса для настраиваемого интерфейса от DHCP-сервера.
no ip address dhcp		Не получать для настраиваемого интерфейса IP-адрес от сервера DHCP.

Команды режима глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

```
console(config)#
```

Таблица 5.47 - Команды режима глобального конфигурирования

Команда	*Значение/значение по умолчанию*	*Действие*
ip default-gateway *ip_address*	-/шлюз по умолчанию не задан	Задает для коммутатора шлюз по умолчанию.
no ip default-gateway		Удаляет для коммутатора шлюз по умолчанию.

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 5.48 - 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 (команда доступна только для привилегированного пользователя). * - удалить все соответствия.
renew dhcp {tengigabitethernet *te_port* **| port-channel** *group***| vlan** *vlan_id***} [force-autoconfig]**	te_port: (1..8/0/1..48); group: (1..32); vlan_id (1..4094)	Отправляет запрос к DHCP-серверу на обновление IP-адреса. force-autoconfig – при обновлении IP-адреса загружается конфигурация с TFTP-сервера.

Команды режима EXEC

Вид запроса командной строки в режиме Exec:

```
console>
```

Таблица 5.49 - Команды режима EXEC

Команда	*Значение*	*Действие*
show ip interface [tengigabitethernet *te_port* **| port-channel** *group***| vlan** *vlan_id***]**	te_port: (1..8/0/1..48); group: (1..32); 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
```

5.13 Настройка IPv6-адресации

5.13.1 Протокол IPv6

Коммутаторы MES5000 поддерживают работу по протоколу IPv6. Поддержка IPv6 является важным достоинством, поскольку протокол IPv6 призван, в перспективе, полностью заменить адресацию протокола IPv4. По сравнению с IPv4 протокол IPv6 имеет расширенное адресное пространство – 128 бит вместо 32. Адрес IPv6 представляет собой 8 блоков, разделенных двоеточием, в каждом блоке 16 бит, записанных в виде четырех шестнадцатеричных чисел.

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

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

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

где
interface-name – имя интерфейса:
interface-name = vlan<integer> | ch<integer> |<physical-port-name>

integer = <decimal-number> | <integer><decimal-number>
decimal-number = 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9
physical-port-name = **tengigabitethernet** (1..8/0/1..48)

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 5.50 – Команды режима глобального конфигурирования

Команда	*Значение*	*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_addr* **{ tengigabitethernet** *te_port* **| port-channel** *group***| vlan** *vlan_id***}** *hw_addr*	te_port: (1..8/0/1..48); group: (1..32); vlan_id (1..4094)	Создает статическое соответствие между MAC-адресом соседнего устройства и его IPv6-адресом. - *ipv6_addr* – IPv6-адрес; - *hw_addr* – 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 5.51 – 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.
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	-	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 Privileged EXEC:

```
console#
```

Таблица 5.52 – Команды режима Privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
ipv6 set mtu { tengigabitethernet *te_port* **| port-channel** *group* **}** **{** *bytes* **| default}**	te_port: (1..8/0/1..48); group: (1..32) bytes: (1280 .. 65535) /1500	Задает значение MTU для IPv6-пакетов.
show ipv6 neighbors {**static** | **dynamic**} [**ipv6-address** *ipv6_address*] [**mac-address** *mac-address*] [**tengigabitethernet** *te_port* **| port-channel** *group***| vlan** *vlan_id***]**	te_port: (1..8/0/1..48); group: (1..32); vlan_id (1..4094)	Показывает информацию о соседних IPv6-устройствах, содержащихся в кэше. - **static** – показывает статические записи; - **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 5.53 – Команды режима EXEC

Команда	*Значение*	*Действие*
show ipv6 interface [**tengigabitethernet** *te_port* **| port-channel** *group* **| vlan** *vlan_id*]	te_port: (1..8/0/1..48); group: (1..32); 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.

5.13.2 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 5.54 – 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 5.55 – Команды режима туннелирования

Команда	*Значение*	*Действие*
tunnel mode ipv6ip isatap	По умолчанию 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*	По умолчанию, доменным именем является строка ‘isatap’	Задаёт доменное имя для туннеля IPv6. Пользователи с адресацией IPv4 будут иметь возможность доступа к устройству (устройство тунеллирования) при выполнении стандартной процедуры DNS.
no tunnel isatap router		Устанавливает значение по умолчанию
tunnel source { auto | ip-address *ipv4_address* **}**	По умолчанию, 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 5.56 – 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 Настройка протоколов

5.14.1 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 5.57 - Команды режима глобального конфигурирования

Команда	*Действие*
ip domain lookup	Разрешает использование протокола DNS.
no ip domain lookup	Запрещает использование протокола DNS.

ip name-server *server_ip_address_list*	Определяет IPv4/IPv6-адреса для доступных DNS-серверов. Можно определить IP-адреса для восьми серверов. IP-адреса серверов указываются через пробел.
no ip name-server *server_ip_address_list*	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 5.58 - 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 eltex-sw-1
```

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
```

5.14.2 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 5.59 - Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
arp *ip_address hw_addr* **[tengigabitethernet** *te_port* **| port-channel** *group***| vlan** *vlan_id***]**	формат ip_address: A.B.C.D; формат hw_addr: H.H.H H:H:H:H:H:H H-H-H-H-H-H; te_port: (1..8/0/1..48); group: (1..32); 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_addr* – MAC-адрес.
no arp *ip_address* **[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). - *sec* – период времени.
no arp timeout		Устанавливает значение по умолчанию.
arp table-size *size*	size: (20..4096)	Задаёт максимальное количество записей в ARP-таблице. - *size* – максимальное количество записей в ARP-таблице. **Для корректной работы нужно также увеличить параметр *hosts* при помощи команды «system resources routing».**

Команды режима privileged EXEC

Вид запроса командной строки в режиме privileged EXEC:

```
console#
```

Таблица 5.60 - Команды режима privileged EXEC

Команда	*Значение*	*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_address* **| 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; te_port: (1..8/0/1..48); group: (1..32).	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; - *te_port* – номер интерфейса Ethernet; - *group* – группа каналов.
show arp configuration	-	Показывает глобальную конфигурацию ARP и конфигурацию ARP для интерфейсов.
ip arp proxy disable	-	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 5.61 - Команды режима interface configuration

Команда	*Значение/Значение по умолчанию*	*Действие*
ip proxy-arp	-	Отключает режим проксирования ARP-запросов на настраиваемом интерфейсе.
no ip proxy-arp		Включает режим проксирования ARP-запросов на настраиваемом интерфейсе.
arp timeout *sec*	(1-40000000)/ 60000 сек.	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 00:00:0C:40:0F:BC, установить время жизни динамических записей в ARP-таблице – 12000 секунд:

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

- Показать содержимое ARP таблицы:

```
console# show arp
```

```
  VLAN    Interface     IP address        HW address          status
-------------------- -------------- ------------------ ---------------
vlan 1     te1/0/3      192.168.25.1    a8:f9:4b:80:7d:00   dynamic
vlan 1     te1/0/3      192.168.25.8    00:26:18:9d:1d:05   dynamic
```

5.14.3 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 5.62 – 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 {tengigabitethernet te_port|port-channel
group}
console(config-if)#
```

Таблица 5.63 – 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 5.64). - *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	-/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 5.64 – 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 5.65 – Команды режима privileged EXEC

Команда	*Значение*	*Действие*
clear gvrp statistics [**tengigabitethernet** *te_port* **| port-channel** *group*]	te_port: (1..8/0/1..48); group: (1..32)	Очищает накопленную статистику протокола GVRP.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 5.66 – Команды режима EXEC

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

5.14.4 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 5.67 – 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*	(30-60)/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}	-/src-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.

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|port-channel
group}
console(config-if)#
```

Таблица 5.68 – 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 5.69 – Команды режима EXEC

Команда	*Значение*	*Действие*
show loopback-detection [**tengigabitethernet** *te_port* **| port-channel** *group*]	te_port: (1..8/0/1..48); group: (1..32).	Отображает состояние механизма loopback-detection. - *te_port* – номер интерфейса Ethernet; - *group* – группа каналов.

5.14.5 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.

5.14.5.1 Настройка протокола STP, RSTP

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*
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}	-/flooding	Определяет режим обработки пакетов BPDU интерфейсом, на котором выключен протокол STP. - **filtering** – на интерфейсе с выключенным протоколом STP BPDU пакеты фильтруются; - **flooding** – на интерфейсе с выключенным протоколом STP нетегированные BPDU пакеты передаются, тегированные – фильтруются.
no spanning-tree bpdu		Устанавливает значение по умолчанию.

При задании таких параметров STP, как forward-time, hello-time, max-age необходимо учитывать следующее справедливое неравенство-формулу: 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 5.71 – 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 5.72	Устанавливает ценность пути через данный интерфейс.
no spanning-tree cost		Устанавливает значение, определяемое на основании скорости порта и метода определения ценности пути, таблица 5.72.
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 mac-address {dot1d | dot1ad}	-/dot1d	Изменяет MAC-адрес, с которым отправляются и принимаются BPDU. - **dot1d** – отправляются и принимаются BPDU с MAC-адресом 01-80-C2-00-00-00; - **dot1ad** – отправляются и принимаются BPDU с MAC-адресом 01-80-C2-00-00-08.
no spanning tree mac-address		Устанавливает значение по умолчанию.
spanning-tree bpduguard	-/отключено	Включает защиту от приема BPDU. При получении пакета BPDU, интерфейс выключается.
no spanning-tree bpduguard		Выключает защиту от приема BPDU.
spanning-tree restricted-tcn	-/отключено	Запрещает прием BPDU с флагом TCN. Пакеты BPDU с флагом TCN отбрасываются.
no spanning-tree restricted-tcn		Разрешает прием BPDU с флагом TCN
spanning-tree link-type {point-to-point | shared}	Значение по умолчанию для дуплексного порта «точка-точка», для полудуплексного – «разветвленный»	Устанавливает протокол RSTP в передающее состояние и определяет тип связи для выбранного порта - «точка-точка», «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.

Таблица 5.72 – 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 privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 5.73 – Команды режима privileged EXEC

Команда	***Значение***	***Действие***
show spanning-tree [**tengigabitethernet** *te_port* **| port-channel** *group*]	te_port: (1..8/0/1..48); group: (1..32).	Показывает конфигурацию протокола STP.
show spanning-tree [detail] [active | blockedports]	-	Показывает подробную информацию о настройке протокола STP, информацию об активных или заблокированных портах.
clear spanning-tree detected-protocols [**tengigabitethernet** *te_port* **| port-channel** *group*]	te_port: (1..8/0/1..48); group: (1..32).	Перезапускает процесс миграции протокола. Заново происходит просчёт дерева STP.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.74 – Команды режима EXEC

Команда	***Значение***	***Действие***
show spanning-tree bpdu [**tengigabitethernet** *te_port* **| port-channel** *group*]	te_port: (1..8/0/1..48); group: (1..32).	Показывает режим обработки пакетов BPDU на интерфейсах.

5.14.5.2 Настройка протокола MSTP

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.75 – 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: (1..15); priority: (0..61440)/32768	Устанавливает приоритет для данного коммутатора перед остальными, использующими общий экземпляр MSTP. **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.
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 5.76 – Команды режима конфигурирования протокола MSTP

Команда	*Значение/Значение по умолчанию*	*Действие*
instance *instance_id* **vlan** *vlan_range*	instance_id:(1..15); vlan_range: (1..4094)	Создает соответствие между экземпляром протокола MSTP и группами 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.
no name		Удаляет имя конфигурации MST.
revision *value*	(0..65535)/0	Задает номер ревизии конфигурации MST.
no revision		Устанавливает значение по умолчанию.
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 5.77 – 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..15); priority:(0..240)/128	Устанавливает приоритет интерфейса в экземпляре MSTP. **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..15); cost: (1..200000000)	Устанавливает ценность пути через выбранный интерфейс, для определенного экземпляра протокола MSTP.
no spanning-tree mst *instance_id* **cost**		Устанавливает значение, определяемое на основании скорости порта и метода определения ценности пути, таблица 5.72.
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 5.78 – Команды режима EXEC

Команда	*Значение*	*Действие*
show spanning-tree [**tengigabitethernet** *te_port* **| port-channel** *group*] [**instance** *instance_id*]	te_port: (1..8/0/1..48); group: (1..32). instance_id: (1..15)	Показывает конфигурацию протокола STP. - *instance_id* – идентификатор экземпляра протокола MSTP.
show spanning-tree [detail] [active | blockedports] [**instance** *instance_id*]	instance_id: (1..15)	Показывает подробную информацию о настройке протокола STP, информацию об активных или заблокированных портах. - *instance_id* – идентификатор экземпляра протокола MSTP.
show spanning-tree mst-configuration	-	Показывает информацию о сконфигурированных экземплярах MSTP
clear spanning-tree detected-protocols [**tengigabitethernet** *te_port* **| port-channel** *group*]	te_port: (1..8/0/1..48); group: (1..32).	Перезапускает процесс миграции протокола. Заново происходит просчёт дерева STP.

Примеры выполнения команд

Включить поддержку протокола STP, установить значение приоритета связующего дерева RSTP – 12899, 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:80:b0:80
             This switch is the root
             Hello Time  5 sec  Max Age 38 sec  Forward Delay 20 sec

  Number of topology changes 2 last change occurred 01:41:53 ago
  Times:  hold 1, topology change 58, notification 5
          hello 5, max age 38, forward delay 20

Interfaces
  Name      State    Prio.Nbr   Cost     Sts    Role PortFast        Type
--------- -------- --------- -------- ------ ---- -------- -----------------
 te1/0/1  enabled    128.1   2000000   Dsbl  Dsbl     No             -
 te1/0/2  enabled    128.2    20000    Lsn   Desg     No        P2P (RSTP)
 te1/0/3  enabled    128.3   2000000   Dsbl  Dsbl     No             -
```

5.14.6 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 5.79 – Команды режима конфигурирования интерфейса Ethernet, группы портов

Команда	*Значение/Значение по умолчанию*	*Действие*
flex-link backup {tengigabitethernet *te_port* **| port-channel** *port_channel***}**	te_port: (1..8/0/1..48); group: (1..32).	Включает flex-link на интерфейсе и назначает выбранному интерфейсу роль backup-интерфейса в flex-link паре.

no flex-link backup [tengigabitethernet *te_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 сек	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 5.80 - 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..48); port_channel: (1..12)	Показывает конфигурацию функции flex-link.

5.14.7 Настройка протокола 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 5.81 – 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*	(1..10)/3 сек	Задает время отсутствия тестовых пакетов, по истечении которого будет зафиксирована авария кольца.
no eaps fail-timer		Устанавливает значение таймера по умолчанию.
eaps hello-timer *seconds*	(1..10)/1 сек	Таймер периодичности отправки hello-пакетов.
no eaps hello-timer		Устанавливает значение таймера по умолчанию.

eaps domain *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 5.82 – Команды режима конфигурирования EAPS домена

Команда	*Значение/Значение по умолчанию*	*Действие*
control-vlan *vlan_id*	1..4093	Идентификатор VLAN, используемой для управления EAPS. Кроме того, следующий по порядку идентификатор VLAN используется для управления вторичными кольцами. Управляющая VLAN EAPS не должна использоваться для передачи любого иного трафика.
no control-vlan		Отмена назначения VLAN.
ring *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**}	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 5.83 – Команды режима конфигурирования EAPS кольца

Команда	*Значение/Значение по умолчанию*	*Действие*
primary-port tengigabitethernet *te_port*	te_port: (1..8/0/1..4)	Выбор первичного порта коммутатора, включенного в кольцо.
secondary-port tengigabitethernet *te_port*	te_port: (1..8/0/1..4)	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.
role {edge | sub-edge}	-	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.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.84 – 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.

5.14.8 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 5.85 – 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*	1..4094/-	Создание ERPS-кольца с идентификатором R-APS VLAN, по которой будет передаваться служебная информация и переход в режим конфигурирования кольца.
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 5.86 – Команды режима конфигурирования ERPS кольца

Команда	*Значение/Значение по умолчанию*	*Действие*
protected vlan add *vlan_range*	vlan_range:(2..4094, all)/-	Добавляет диапазон VLAN в список защищенных VLAN.
protected vlan remove *vlan_range*	vlan_range:(2..4094, all)/-	Удаляет диапазон VLAN из списка защищенных VLAN.
port {west | east} {tengigabitethernet *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..4); group: (1..32)/-	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.
no rpl		Удаление RPL порта коммутатора.
level *level*	level: (0..7)/1	Настройка уровня R-APS сообщений. Необходимо для прохождения сообщений через CFM MEP.
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.
no version		Установка значения по умолчанию.
revertive	-/revertive	Выбор режима работы кольца.
no revertive		Установка значения по умолчанию.
sub-ring vlan *vlan_id*	vlan_id:(1..4094)	Указание подкольца для данного кольца.
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 5.87 – 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.

5.14.9 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 MES5000 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 5.88 – 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: (1..4094); 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 notifications interval *seconds*	(5..3600)/5	Устанавливает максимальную скорость передачи 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 5.89 – 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 *tlv1* [*tlv2.. tlv5*]	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 | ppvid {add|remove} *ppvid* **| 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 [tengigabitethernet** *te_port* **|port-channel** *group***| vlan** *vlan_id***] }**	формат ip_address: A.B.C.D te_port: (1..8/0/1..48); group: (1..32); 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 {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 если несколько IP-адресов, то 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 [*tlv1 … tlv4*]	network-policy, location, poe-pse, inventory По умолчанию запрещено использование расширения протокола LLDP MED.	Разрешает использование расширения протокола LLDP MED. В команду можно включить специальные 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_addres_data* | **ecs-elin** *ecs_elin_data***}**	coordinate: 16 байт; civic_addres_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_addres_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.

LLDP-данные, принятые через группу агрегации каналов, запоминаются индивидуально портами группы, принявшими сообщения. LLDP шлет разрозненные 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 5.90 – 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 [tengigabitethernet *te_port***]**	te_port: (1..8/0/1..48).	Показывает LLDP конфигурации всех физических интерфейсов устройства, либо заданных интерфейсов.
show lldp med configuration [tengigabitethernet *te_port***]**	te_port: (1..8/0/1..48).	Показывает конфигурации расширения протокола LLDP - MED для всех физических интерфейсов, либо заданных интерфейсов.
show lldp local {tengigabitethernet *te_port***}**	te_port: (1..8/0/1..48).	Показывает LLDP-информацию, которую анонсирует данный порт.
show lldp local tlvs-overloading [tengigabitethernet *te_port***]**	te_port: (1..8/0/1..48).	Показывает статус перезагрузки TLVs LLDP.
show lldp neighbors [tengigabitethernet *te_port***]**	te_port: (1..8/0/1..48).	Показывает информацию о соседних устройствах, на которых работает протокол LLDP.
show lldp statistics [tengigabitethernet *te_port***]**	te_port: (1..8/0/1..48).	Показывает статистику LLDP.

Примеры выполнения команд

Установить для порта te 1/0/3 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
Notifications Interval: 5 Seconds


  Port       State       Optional TLVs          Address       Notifications
--------- ----------- -------------------- ----------------- ---------------
te1/0/1    Rx and Tx                            None            Disabled
te1/0/2    Rx and Tx                            None            Disabled
te1/0/3    Rx and Tx                            None            Disabled
te1/0/4    Rx and Tx                            None            Disabled
te1/0/5    Rx and Tx                            None            Disabled
te1/0/6    Rx and Tx                            None            Disabled
…
te1/0/46   Rx and Tx                            None            Disabled
te1/0/47   Rx and Tx                            None            Disabled
te1/0/48   Rx and Tx                            None            Disabled
```

Таблица 5.91 - Описание результатов

Поле	***Описание***
Timer	Определяет, как часто устройство шлет LLDP-обновления.
Hold multiplier	Определяет величину времени для принимающего устройства, в течение которого нужно удерживать принимаемые пакеты LLDP перед их сбросом.
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  TTL
--------- ----------------- ------------- ----------------- ------------ -----
te1/0/2   a8:f9:4b:a4:54:80    gi1/0/3                           B        111
```

Показать информацию о соседнем устройстве на порту te1/0/1

```
console# show lldp neighbors tengigabitethernet 1/0/1
Device ID: a8:f9:4b:85:a2:00
Port ID: te1/0/1
Capabilities: B
System Name:
System description: MES-1024
Port description: #UplinkPort#
Management Address: 10.100.100.20
Time To Live: 96
802.3 MAC/PHY Configuration/Status
Auto-negotiation support: Supported
Auto-negotiation status:  Disabled
Auto-negotiation Advertised Capabilities: other or unknown
Operational MAU type: Unknown
802.3 Link Aggregation
Aggregation capability: Capable of being aggregated
Aggregation status: Currently not in aggregation
802.3 Maximum Frame Size: 1522
802.1 PVID: None
802.1 PPVID:
802.1 VLAN:
802.1 Protocol:
```

Таблица 5.92 - 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 Групповая адресация

5.15.1 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 5.93 – 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] { tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..48); group: (1..32).	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** - ставит в соответствие групповому MAC-адресу диапазон Ethernet-портов или групп портов. - **remove** – удаляет соответствие 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} {tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..48); group: (1..32).	Создает запрещающее правило для группового MAC-адреса. - *mac_multicast_address* – групповой MAC-адрес; - *ip_multicast_address* – IP-адрес многоадресной рассылки; **- add** – создает правило, запрещающее ставить в соответствие групповой MAC-адрес списку портов/групп портов; - **remove** – отменяет данное правило для списка портов/групп портов. 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} {tengigabitethernet *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..48); group: (1..32). По умолчанию передача всех многоадресных пакетов запрещена.	Разрешает передачу всех многоадресных пакетов на порту. - **add** – создает правило, разрешающее передачу всех групповых пакетов в списке портов/объединенных портов; - **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**} **{tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..48); group: (1..32)/ По умолчанию портам не запрещено динамически присоединяться к многоадресной группе.	Запрещает порту динамически добавляться к многоадресной группе. - **add** – создает правило, запрещающее передачу всех групповых пакетов на список портов/объединенных портов; - **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] {tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..48); group: (1..32)	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} {tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..48); group: (1..32)	Запрещает добавление/удаление группового IP-адреса на порт. - *ip_multicast_address* – групповой IP-адрес; - **add** – запрет на добавление порта/портов в группу; - **remove** – запрет на удаление порта/портов из группы. 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] {tengigabitethernet** *te_port* **| port-channel** *group***}]**	te_port: (1..8/0/1..48); group: (1..32)	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} {tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..48); group: (1..32)	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] {tengigabitethernet** *te_port* **| port-channel** *group***}]**	te_port: (1..8/0/1..48); group: (1..32)	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 ipv6forbidden ip-address *ipv6_multicast_address* **{add | remove} {tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..48); group: (1..32)	Запрещает назначать/отменять групповой IPv6-адрес на определенный порт. - *ip_multicast_address* – групповой IP-адрес; - **add** – запрет на добавление порта/портов в группу; - **remove** – запрет на удаление порта/портов из группы. 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] {tengigabitethernet** *te_port* **|port-channel** *group***}]**	te_port: (1..8/0/1..48); group: (1..32)	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; - *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 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} {tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..48); group: (1..32)	Устанавливает запрет на добавление/удаление соответствия между IPv6-адресом пользователя и групповым адресом в таблице групповой адресации для определенного порта. - *ip_address* – исходный IPv6-адрес; - *ip_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.

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 | port-channel
group | range {…}}
console(config-if)#
```

Таблица 5.94 – 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 5.95 – 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*	(10..630)/300 секунд	Задает время хранения MAC-адреса в таблице.
no mac address-table aging-time		Устанавливает значение по умолчанию.
mac address-table static *mac_address* **vlan** *vlan_id* **interface {tengigabitethernet** *te_port* **| port-channel** *group***} [permanent | delete-on-reset | delete-on-timeout | secure]**	te_port: (1..8/0/1..48); group: (1..32); vlan_id: (1..4094)	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 bridge address;** **- delete-on-reset** – данный адрес удалится после перезагрузки устройства; - **delete-on-timeout** – данный адрес удалится по тайм-ауту; - **secure** – данный адрес удалится только с помощью команды **no bridge address** или после возвращения порта в режим обучения (**no port security**).
no mac address-table static [*mac_address***] vlan** *vlan_id*		Удаляет MAC-адрес из таблицы групповой адресации.
mac address-table learning vlan *vlan_id*	vlan_id: (1..4094)/ 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 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 5.96 – Команды режима Privileged EXEC

Команда	*Значение*	*Описание*
clear mac address-table {dynamic| secure} [interface {tengigabitethernet *te_port* **|port-channel** *group***}]**	te_port: (1..8/0/1..48); group: (1..32)	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 5.97 – Команды режима EXEC

Команда	*Значение*	*Описание*
show mac address-table [dynamic | static| secure] [vlan *vlan_id***] [interface {tengigabitethernet** *te_port* **| port-channel** *group}* **] [address** *mac_address***]**	te_port: (1..8/0/1..48); group: (1..32); 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.
show mac address-table count [vlan *vlan* **| interface {tengigabitethernet** *te_port* **| port-channel** *group***}]**	-	Показывает количество записей в таблице MAC-адресов для указанного интерфейса, либо для всех интерфейсов.
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_multicast_address**}]**	vlan_id: (1..4094)	Показывает таблицу групповых адресов для указанного интерфейса либо всех интерфейсов VLAN (команда доступна только для привилегированного пользователя). - **ip** – показывать по IP-адресам; - **mac** – показывать по MAC-адресам.
show bridge multicast address-table static [vlan *vlan_id***] [address** *mac_multicast_address* **|** *ipv4_multicast_address* **|** *ipv6_multicast_address***] [source** *ipv4_source_address* **|** ipv6_multicast_address**] [all | mac | ip]**	vlan_id: (1..4094)	Показывает таблицу статических групповых адресов для указанного интерфейса либо всех интерфейсов VLAN.

show bridge multicast filtering *vlan_id*	vlan_id: (1..4094)	Показывает конфигурацию фильтра групповых адресов для указанного VLAN.
show bridge multicast unregistered [tengigabitethernet *te_port* **| port-channel** *group* **]**	te_port: (1..8/0/1..48); group: (1..32)	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.
show bridge multicast reserved-addresses	-	Отображает правила, установленные для групповых зарезервированных адресов.

Примеры выполнения команд

Включить фильтрацию групповых адресов коммутатором. Разрешить передачу незарегистрированные многоадресных пакетов на 11 порту коммутатора.

```
console # configure
console(config) # bridge multicast filtering
console(config) # interface tengigabitethernet 1/0/11
console(config-if) # bridge multicast unregistered forwarding
```

5.15.2 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 5.98 – 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.
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_address* **[interface {tengigabitethernet** *te_port* **|port-channel** *group***}]**	vlan_id: (1-4094); te_port: (1..8/0/1..48); group: (1..32)	Регистрирует групповой IP-адрес в таблице групповой адресации, и статически добавляет интерфейсы из группы для текущей VLAN. - *ip_address* – групповой IP-адрес; Перечисление интерфейсов осуществляется через «–» и «,»
no ip igmp snooping vlan *vlan_id* **static** *ip_address* **[interface {tengigabitethernet** *te_port* **|port-channel** *group***}]**		Удаляет групповой IP-адрес из таблицы.
ip igmp snooping vlan *vlan_id* **mrouter learn pim-dvmrp**	vlan_id: (1-4094) По умолчанию – разрешено	Разрешает для данной группы VLAN автоматическое распознавание портов, к которым подключены многоадресные маршрутизаторы.
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 {tengigabitethernet** *te_port* **|port-channel** *group***}**	vlan_id: (1-4094) te_port: (1..8/0/1..48); group: (1..32)	Определяет порт, к которому подключен маршрутизатор многоадресной рассылки для заданной VLAN.
no ip igmp snooping vlan *vlan_id* **mrouter interface {tengigabitethernet** *te_port* **|** **port-channel** *group* **}**		Указывает, что к порту не подключен маршрутизатор многоадресной рассылки.
ip igmp snooping vlan *vlan_id* **forbidden mrouter interface {tengigabitethernet** *te_port* **|** **port-channel** *group* **}**	vlan_id: (1-4094) te_port: (1..8/0/1..48); group: (1..32)	Устанавливает запрет на определение порта (статически, динамически) как порта, к которому подключен маршрутизатор многоадресной рассылки.
no ip igmp snooping vlan *vlan_id* **forbidden mrouter interface {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* **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.
no ip igmp snooping vlan *vlan_id* **immediate-leave**		Отключить процесс IGMP Snooping Immediate-Leave на текущей VLAN.

Команды режима конфигурирования интерфейса VLAN

Вид запроса командной строки режима конфигурирования VLAN:

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

Таблица 5.99 – Команды режима конфигурирования интерфейса VLAN

Команда	***Значение/Значение по умолчанию***	***Действие***
ip igmp robustness *count*	(1-7)/2	Устанавливает значение робастности для IGMP. Если на канале наблюдается потеря данных, значение робастности 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*	(100-25500)/1000 мс	Устанавливает интервал запроса для последнего участника.
no ip igmp last-member-query-interval		Устанавливает значение по умолчанию.

Команды режима EXEC

Все команды доступны только для привилегированного пользователя.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.100 – 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.

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 робастности 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
```

5.15.3 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 5.101 – 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_address* **[interface {tengigabitethernet** *te_port* | **port-channel** *group***}]**	vlan_id: (1-4094); te_port: (1..8/0/1..48); group: (1..8)	Регистрирует групповой IPv6-адрес в таблице групповой адресации, и статически добавляет/удаляет интерфейсы из группы для текущей VLAN. - *ipv6_address* – групповой IPv6-адрес; Перечисление интерфейсов осуществляется через «–» и «,»
no ipv6 mld snooping vlan *vlan_id* **static** *ipv6-address* **[interface {tengigabitethernet** *te_port* **|** **port-channel** *group***}]**		Удаляет групповой IP-адрес из таблицы.
ipv6 mld snooping vlan *vlan_id* **forbidden mrouter interface {tengigabitethernet** *te_port* **| port-channel** *group***}**	vlan_id: (1..4094); te_port: (1..8/0/1..48); group: (1..8)	Добавляет правило, запрещающее регистрировать MLD-mrouter порты из списка.

no ipv6 mld snooping vlan *vlan_id* **forbidden mrouter interface {tengigabitethernet** *te_port* **|port-channel** *group***}**		Удаляет правило, запрещающее регистрировать MLD-mrouter порты из списка.
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 {tengigabitethernet** *te_port* **|port-channel** *group***}**	vlan_id: (1 .. 4094); te_port: (1..8/0/1..48); group: (1..8)	Добавляет список mrouter-портов.
no ipv6 mld snooping vlan *vlan_id* **mrouter interface {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 5.102 – Команды режима конфигурирования интерфейса VLAN

Команда	***Значение/Значение по умолчанию***	***Действие***
ipv6 mld join-group *multicast_ipv6_address*	multicast_ipv6_address – Групповой адрес IPv6	Создает статическую группу многоадресной IPv6-рассылки
no ipv6 mld join-group *multicast_ipv6_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 5.103 – Команды режима конфигурирования интерфейса Ethernet, группы интерфейсов

Команда	*Значение/Значение по умолчанию*	*Описание*
ipv6 mld join-group *ipv6_address*	-	Дает указание рассылать MLD-report сообщения на присоединение к *ipv6_address* группы с данного порта. ipv6_address– групповой адрес IPv6
no ipv6 mld join-group *ipv6_address*		Удаляет указание рассылать MLD-report сообщения на присоединение к *ipv6_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 5.104 – Команды режима EXEC

Команда	*Значение*	*Действие*
show ipv6 mld snooping groups [vlan *vlan_id***] [address** *ipv6_multicast_address***] [source** *ipv6_source_address***]**	vlan_id – 1..4094 ipv6_multicast_address – групповой адрес IPv6 ipv6_source_address – IPv6-адрес	Отображает информацию о зарегистрированных группах в соответствии с заданными в команде параметрами фильтрации.
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.

5.16 Функции управления

5.16.1 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 5.105 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
aaa authentication login {**default** | *list-name*} *method1* [*method2*...]	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 (method1 [method2...]): - 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 без аутентификационных проверок.** **Создание списка осуществляется командой:** aaa authentication login list-name method1 [method2...]**.** **Использование списка:** aaa authentication login list-name
no aaa authentication login {**default** | *list_name*}		Устанавливает значение по умолчанию.
aaa authentication enable {**default** | *list_name*} *method1* [*method2*...]	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 (method1 [method2...]): - 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 без пароля (aaa authentication enable default enable none).** **Создание списка осуществляется командой aaa authentication enable** list-name method1 [method2...]**. 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* – задать 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 5.106).**
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 5.107).** **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 *method1 [method2...]*	Method: 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. - 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.

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

Таблица 5.106 – 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 5.107 – 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 5.108 – Команды режима конфигурирования интерфейса Ethernet

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 auto - использовать 802.1X для изменен; - *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 auto - использовать 802.1X для изменен; - *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 5.109 – Команды режима Privileged EXEC

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Все команды данного раздела доступны только для привилегированных пользователей.

Таблица 5.110 – Команды режима EXEC

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

5.16.2 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 5.111 - 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*] [**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; 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; - *source ip_address* – 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.
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	-/выключено	Включает добавление атрибута NAS-ID (32). Требует задания форматной строки или имя хоста (hostname) не короче 3 символов.
no radius-server attributes nas-id include-in-access-req		Выключает добавление атрибута NAS-ID (32).
radius-server attributes nas-id include-in-access-req format *nas_id*	nas_id: (3..32) символов/%h	Задаёт формат для атрибута NAS-ID (32). - *nas_id* – формат атрибута.
no radius-server attributes nas-id include-in-access-req format		Устанавливает значение по умолчанию. - %*h* – имя хоста (hostname).

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 5.112 - Команды режима Privileged EXEC

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

Примеры использования команд

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

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

- Показать параметры настройки RADIUS серверов

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

```
  IP address     Port  port  Time-   Ret-  Dead-      source IP     Prio. Usage
                 Auth  Acct  Out     rans  Time
---------------- ----- ----- ------ ------ ------ --------------- ----- -----
 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 : ::
```

5.16.3 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 5.113 - 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*] **[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; priority: (0..65535)/0; В случае отсутствия в команде параметров timeout, key, source_ip-addr для данного TACACS-сервера используются значения настроенные с помощью команд, указанных ниже (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; - *secret_key* – ключ 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).
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 5.114 - 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.

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
```

5.16.4 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 MES5000 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 5.115 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
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_adrress*| *ipv6_address*| *ipv6z_adrress*] [*mask* | *prefix_length*] **snmp-server community-group** *community groupname* [*ipv4_adrress*| *ipv6_address*| ipv6z_adrress] [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 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_adrress, ipv6_address, ipv6z_adrress* – 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; - *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_adrr*| *ipv6_addr*| *ipv6z_adrr*]		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. - 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 udp_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 SNMPv1/v2-серверу. - *community* – строка сообщества для передачи сообщений уведомления; - **version** – определят тип сообщений trap – trap SNMPv1, trap SNMPv2, trap SNMPv3; - **auth** – указывает подлинность пакета без шифрования; - **noauth** – не указывает подлинность пакета; - **priv** – указывает подлинность пакета с шифрованием; - *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 udp_port: (1..65535)/162 filtername:	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;

	(1..30) символов	- *retries* – количество попыток передачи сообщений inform, при отсутствии их подтверждения.
no snmp-server v3-host {*ipv4_address*| *ipv6_address*|*hostname*} *username* [**traps**|**informs**]	seconds: (1..300)/15 retries: (0..255)/3	Удаляет настройки для передачи сообщений уведомления inform и trap SNMPv3-серверу.
snmp-server engineID local {engineid_string | **default**}	(5..32) символов	Создает идентификатор локального SNMP устройства – engineID. - **default** – при использовании данной настройки engineID будет автоматически создан, на основе MAC-адреса устройства.
no snmp-server engineID local		Удаляет идентификатор локального SNMP устройства – engineID
snmp-server engineID remote {*ipv4_ip_address* **|** *ipv6_address*} *engineid_string*	(5..32) символов	Создает идентификатор удаленного SNMP устройства – engineID.
no snmp-server engineID remote {*ipv4_ip_address* **|** *ipv6_address*}		Удаляет идентификатор удаленного SNMP устройства – engineID.
snmp-server enable traps	-	Включает поддержку SNMP trap сообщений.
no snmp-server enable traps		Отключает поддержку SNMP trap сообщений.
snmp-server trap authentication	-	Разрешает передавать сообщения trap серверу не прошедшему аутентификацию.
no snmp-server trap authentication		Запрещает передавать сообщения trap серверу не прошедшему 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.
snmp-server enable traps	-/включено	Включает отправку SNMP trap сообщений.
no snmp-server enable traps		Отключает отправку SNMP trap сообщений.
snmp-server enable traps mac-notification flapping	-/включено	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 flex-link	-/включено	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 storm-control	-/включено	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 enable traps erps	-/включено	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.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 5.116 – 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 Objedineniya-street, 9
console (config)# snmp-server community-string public ro
console (config)# snmp-server community-string private rw 192.168.16.3
```

5.16.5 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 5.117 – 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** *direction*] [**owner** *name*]	index: (1..65535) mib_object_id: корректный OID; 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	Настраивает условия выдачи аварийных сигналов. - *index* – индекс аварийного события; - **mib_object_id** – идентификатор переменной части объекта OID; - *interval* – интервал, в течение которого данные 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.

<u>Команды режима конфигурирования интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов</u>

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

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

Таблица 5.118 – 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; interval: (1..3600)/1800 сек	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*		Выключает формирование истории по группам статистики для базы данных (MIB) удаленного мониторинга.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 5.119 – Команды режима EXEC

Команда	*Значение*	*Действие*
show rmon statistics {tengigabitethernet *te_port* **|port-channel** *group* **}**	te_port: (1..8/0/1..48); group: (1..32)	Показывает статистику интерфейса Ethernet, либо группы портов, используемую для удаленного мониторинга.
show rmon collection stats [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 tengigabitethernet 1/0/10
```

```
Port te1/0/10

Dropped: 0
Octets: 0                       Packets: 0
Broadcast: 0                    Multicast: 0
CRC Align Errors: 0             Collisions: 0
```

```
Undersize Pkts: 0                Oversize Pkts: 0
Fragments: 0                     Jabbers: 0
64 Octets: 0                     65 to 127 Octets: 0
128 to 255 Octets: 0             256 to 511 Octets: 0
512 to 1023 Octets: 0            1024 to max Octets: 0
```

Таблица 5.120 - Описание результатов

Параметр	***Описание***
Dropped	Количество задетектированных событий, когда пакеты были отброшены.
Octets	Количество байт данных (включая байты плохих пакетов), принятых из сети (исключая фреймовые биты, но включая биты контрольной суммы).
Packets	Количество принятых пакетов (включая плохие, широковещательные и многоадресные пакеты).
Broadcast	Количество принятых широковещательных пакетов (только корректные пакеты).
Multicast	Количество принятых многоадресных пакетов (только корректные пакеты).
CRC Align Errors	Количество принятых пакетов длиной от 64 до 1518 байт включительно, имеющих неверную контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы – FCS), либо с нецелым числом байт (ошибки выравнивания – Alignment).
Collisions	Оценка количества коллизий на данном Ethernet сегменте.
Undersize Pkts	Количество принятых пакетов длиной меньше 64 байт (исключая фреймовые биты, но включая биты контрольной суммы), но в остальном правильно сформированных.
Oversize Pkts	Количество принятых пакетов длиной больше 1518 байт (исключая фреймовые биты, но включая биты контрольной суммы), но в остальном правильно сформированных.
Fragments	Количество принятых пакетов длиной меньше 64 байт (исключая фреймовые биты, но включая биты контрольной суммы), имеющих неверную контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы – FCS), либо с нецелым числом байт (ошибки выравнивания – Alignment).
Jabbers	Количество принятых пакетов длиной больше 1518 байт (исключая фреймовые биты, но включая биты контрольной суммы), имеющих неверную контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы – FCS), либо с нецелым числом байт (ошибки выравнивания – Alignment).
64 Octet	Количество принятых пакетов (включая плохие пакеты) длиной 64 байта (исключая фреймовые биты, но включая биты контрольной суммы).
65 to 127 Octets	Количество принятых пакетов (включая плохие пакеты) длиной от 65 до 127 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы).
128 to 255 Octets	Количество принятых пакетов (включая плохие пакеты) длиной от 128 до 255 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы).
256 to 511 Octets	Количество принятых пакетов (включая плохие пакеты) длиной от 256 до 511 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы).
512 to 1023 Octets	Количество принятых пакетов (включая плохие пакеты) длиной от 512 до 1023 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы).
1024 to 1518 Octets	Количество принятых пакетов (включая плохие пакеты) длиной от 1024 до 1518 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы).

- Показать информацию по группам статистики для порта 8:

```
console# show rmon collection stats tengigabitethernet 1/0/8
```

```
Index Interface Interval Requested Samples Granted Samples        Owner
----- --------- -------- ----------------- --------------- -------------------
  1   te1/0/8  300           50                50                Eltex
```

Таблица 5.121 - Описание результатов

Параметр	*Описание*
Index	Индекс, уникально идентифицирующий запись.
Interface	Ethernet-интерфейс, на котором запущен опрос.
Interval	Интервал в секундах между опросами.
Requested Samples	Запрошенное количество отсчетов, которое может быть сохранено.
Granted Samples	Разрешенное (оставшееся) количество отсчетов, которое может быть сохранено.
Owner	Владелец данной записи.

- Показать счетчики пропускной способности для группы статистики 1:

```
console# show rmon history 1 throughput
```

```
Sample set: 1        Owner: MES
Interface: te1/0/1               Interval: 1800
Requested samples: 50      Granted samples: 50

Maximum table size: 100
Time                        Octets       Packets      Broadcast    Multicast
  %
Nov 10 2009 18:38:00        204595549    278562       2893         675218.67%
```

Таблица 5.122 - 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 5.123 - 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 5.124 - 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 5.125 – 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 5.126 – Описание результатов

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

5.16.6 Списки доступа ACL для управления устройством

Программное обеспечение коммутаторов серии MES5000 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 5.127 – 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 5.128 – Команды режима конфигурирования списка доступа для управления

Команда	*Значение*	*Действие*
permit [tengigabitethernet *te_port* **|port-channel** *group***| vlan** *vlan_id***]** [**service** *service*]	te_port: (1..8/0/1..48); group: (1..32); 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*}] **[tengigabitethernet** *te_port* **|port-channel** *group***|vlan** *vlan_id***]** [**service** *service*]		
deny [tengigabitethernet *te_port* **|port-channel** *group***|vlan** *vlan_id***]** [**service** *service*]	te_port: (1..8/0/1..48}; group: (1..32); 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*}] **[tengigabitethernet** *te_port* **|port-channel** *group***| vlan** *vlan_id***]** [**service** *service*]		

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 5.129 – 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.

5.16.7 Настройка локальной и удаленной консоли.

5.16.7.1 Telnet и SSH

Данные команды предназначены для настройки серверов TELNET и SSH. 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 5.130 – 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.
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.**

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 5.131 – 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 5.132 – 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 5.133 – 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.

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
```

5.16.7.2 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 5.134 – 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 5.135 – Команды режима конфигурирования терминала

Команда	***Значение***	***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	Задает интервал, в течение которого система ожидает ввода пользователя. Если в течение данного интервала пользователь ничего не вводит, то консоль отключается.
no exec-timeout	По умолчанию 10 минут	Устанавливает значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.136 – Команды режима EXEC

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

5.17 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 5.137 - 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. 5.138); 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 {*ipaddr*|*host***}**		Удаляет выбранный сервер из списка используемых SYSLOG-серверов.
logging console *level*	level: (см. табл. 5.138) 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 [level *level***] [size** *size***]**	level: (см. табл. 5.138)/ informational size: (20..400)/200	Включает передачу аварийных или отладочных сообщений во внутренний буфер. - *level* - уровень важности сообщений, передаваемых во внутренний буфер; - *size* - изменяет количество сообщений, запоминаемых во внутреннем буфере. Новое значение размера буфера применится после перезагрузки устройства.

no logging buffered		Выключает передачу аварийных или отладочных сообщений во внутренний буфер.
logging file *level*	level: (см. табл. 5.138)/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).
file-system logging {copy | delete-rename}	-/включено	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	-/включено	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	-/ведение учета запрещено	Разрешает ведение учета (аккаунта) для введенных в CLI команд.
no logging cli-commands		Устанавливает значение по умолчанию.

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

Таблица 5.138 – 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 5.139 – 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
```

5.18 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 не сконфигурирован 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;
- Порт не может быть членом группы портов.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 5.140 - 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*		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 5.141 – Команды, доступные в режиме конфигурирования интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
port monitor tengigabitethernet *te_port* **[rx|tx]**	te_port: (1..8/0/1..48)	Включает функцию мониторинга на настраиваемом интерфейсе. Данный интерфейс будет контролирующим портом для указанного в команде контролируемого порта. - **rx** – копировать пакеты принятые контролируемым портом; - **tx** – копировать пакеты, переданные контролируемым портом; При отсутствии параметра rx/tx с контролируемого порта копируются все пакеты.
no port monitor {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..4094)	Включает функцию мониторинга на настраиваемом интерфейсе. Данный интерфейс будет контролирующим портом для указанной VLAN. **Порт мониторинга не должен принадлежать к настраиваемой VLAN**
no port monitor vlan *vlan_id*		Удаляет указанную VLAN из мониторинга.

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 5.142 – Команды, доступные в режиме EXEC

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

Примеры выполнения команд

- Установить интерфейс te1/0/13 контролирующим для интерфейса te1/0/18. Весь трафик с интерфейса te1/0/18 передавать на te1/0/13.

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

- Вывести информацию по контролирующим и контролируемым портам.

```
console# show ports monitor
```

```
Port monitor mode: monitor-only

    RSPAN configuration
RX: not configured
TX: not configured

Source Port Destination Port  Type     Status   RSPAN
----------- ---------------- ------- ---------- -----
 te1/0/18       te1/0/13      RX,TX   notReady  false
```

5.19 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 5.143 - Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
sflow receiver *id* **{***IPv4***|** *IPv6***|***IPv6z***|***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 tengigabitethernet te_port
console(config-if)#
```

Таблица 5.144 – 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 5.145 – Команды, доступные в режиме EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show sflow configuration tengigabitethernet *te_port*	te_port: (1..8/0/1..48)	Выводит настройки sflow.
clear sflow statistics tengigabitethernet *te_port*		Очищает статистику sFlow. Если интерфейс не указан, команда очищает все счетчики статистики sFlow.
show sflow statistics 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 tengigabitethernet 1/0/1-24
console(config-if-range)# sflow flowing-sample 1 10240
console (config-if)# sflow counters-sampling 240 1
```

5.20 Функции диагностики физического уровня

Сетевые коммутаторы MES5000 содержат аппаратные и программные средства для тестирования оптических трансиверов.

5.20.1 Диагностика оптического трансивера

Команда диагностики оптического трансивера доступна в режиме Privileged EXEC. Запрос командной строки в режиме EXEC имеет следующий вид:

```
console#
```

Таблица 5.146 – Команда диагностики оптического трансивера

Команда	*Значение*	*Действие*
show fiber-ports optical-transceiver [interface tengigabitethernet *te_port***] [detailed]**	te_port: (1..8/0/1..48).	Отображает результаты диагностики оптического трансивера. - **detailed** – подробная диагностика

Пример выполнения команды:

```
console# show fiber-ports optical-transceiver interface
tengigabitethernet 1/0/1 detailed
```

```
   Port      Temp  Voltage Current  Output        Input         LOS  Transceiver
             [C]   [V]     [mA]     Power         Power              Type
                                    [mW / dBm]    [mW / dBm]
----------- ------ ------- ------- ------------- ------------- --- -------------
  te1/0/1     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 m
Diagnostic: supported
```

Таблица 5.147 – 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).
TX Fault	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.

5.21 Функции обеспечения безопасности

5.21.1 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 MES5000 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 5.148 – 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 5.149 – Команды режима EXEC

Команда	*Значение*	*Действие*
show ports security {tengigabitethernet *te_port* **|port-channel** *group***}**	te_port: (1..8/0/1..48); group: (1..32)	Показывает настройки функции безопасности на выбранном интерфейсе.
show ports security addresses {tengigabitethernet *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..48); group: (1..32)	Показывает текущие динамические адреса для заблокированных портов.
set interface active {tengigabitethernet *te_port* **|port-channel** *group***}**	te_port: (1..8/0/1..48); group: (1..32)	Активизирует интерфейс, отключенный функцией защиты порта (команда доступна только для привилегированного пользователя).

Примеры выполнения команд

- Включить функцию защиты на интерфейсе Ethernet te1/0/15. Установить ограничение на изучение адресов – 1 адрес. После изучения MAC-адреса заблокировать функцию изучения новых адресов для интерфейса с целью отбросить пакеты с неизученными MAC-адресами источника. Сохранить в файл изученный адрес.

```
console# configure
console(config)# interface tengigabitethernet 1/0/15
console(config-if)# port security max 1
```

- Подключить клиента к порту и изучить MAC-адрес.

```
console(config-if)# port security discard
console(config-if)# port security mode lock
```

5.21.2 Проверка подлинности клиента на основе порта (стандарт 802.1x)

5.21.2.1 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 5.150 – 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 5.151 – 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-period *period*	300..4294967295/ 3600 сек	Устанавливает период между повторными проверками 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 5.152 – Команды режима Privileged EXEC

Команда	***Значение***	***Действие***
dot1x re-authenticate [tengigabitethernet *te_port***]**	te_port: (1..8/0/1..48)	Вручную осуществляет повторную проверку подлинности указанного порта в команде, либо всех портов, поддерживающих 802.1X.
show dot1x interface tengigabitethernet *te_port*	te_port: (1..8/0/1..48)	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 tengigabitethernet *te_port*	te_port: (1..8/0/1..48)	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 интерфейса Ethernet te1/0/18 использовать режим аутентификации 802.1x.

```
console# configure
```

```
console(config)# dot1x system-auth-control
console(config)# aaa authentication dot1x default radius
console(config)# interface tengigabitethernet 1/0/18
console(config-if)# dot1x port-control auto
```

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

```
console# show dot1x
```

```
802.1x is enabled

         Admin              Oper          Reauth   Reauth     Username
Port     Mode               Mode          Control  Period
-------- ------------------ ------------- -------- ---------- -----------------
te1/0/1  Force Authorized   Authorized    Disabled 3600       n/a
te1/0/2  Force Authorized   Authorized    Disabled 3600       n/a
te1/0/3  Force Authorized   Authorized*   Disabled 3600       n/a
te1/0/4  Force Authorized   Authorized*   Disabled 3600       n/a
te1/0/5  Force Authorized   Authorized*   Disabled 3600       n/a
te1/0/6  Force Authorized   Authorized*   Disabled 3600       n/a
te1/0/7  Force Authorized   Authorized*   Disabled 3600       n/a
te1/0/8  Force Authorized   Authorized*   Disabled 3600       n/a
te1/0/9  Force Authorized   Authorized*   Disabled 3600       n/a
te1/0/10 Force Authorized   Authorized*   Disabled 3600       n/a
te1/0/11 Force Authorized   Authorized*   Disabled 3600       n/a
te1/0/12 Force Authorized   Authorized*   Disabled 3600       n/a
te1/0/13 Force Authorized   Authorized*   Disabled 3600       n/a
te1/0/14 Force Authorized   Authorized*   Disabled 3600       n/a
te1/0/15 Force Authorized   Authorized*   Disabled 3600       n/a
te1/0/16 Force Authorized   Authorized*   Disabled 3600       n/a
te1/0/17 Force Authorized   Authorized*   Disabled 3600       n/a
te1/0/18 Force Authorized   Authorized*   Disabled 3600       n/a
te1/0/19 Force Authorized   Authorized*   Disabled 3600       n/a
te1/0/20 Force Authorized   Authorized*   Disabled 3600       n/a              …
te1/0/48 Force Authorized   Authorized*   Disabled 3600       n/a

* Port is down or not present
```

```
console# show dot1x interface tengigabitethernet 1/0/12
```

```
802.1x is disabled

         Admin              Oper          Reauth   Reauth     Username
Port     Mode               Mode          Control  Period
-------- ------------------ ------------- -------- ---------- -----------------
te1/0/1  Force Authorized  Authorized*  Disabled3600      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 5.153 – 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 te1/0/13.

```
console# show dot1x statistics interface tengigabitethernet 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 5.154 – 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.

5.21.2.2 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.

Команды режима глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

```
console(config)#
```

Таблица 5.155 – 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.

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet:

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

Таблица 5.156 – 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, когда multiple hosts используется. Команда значима для режима multiple sessions.**
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 авторизован 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.** **- Статический MAC-адрес не должен быть прописан.** **- Функция переаутентификации должна быть включена.**
no dot1x mac-authentication		Выключает аутентификацию, основанную на MAC-адресах пользователей.
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.

Команды режима конфигурирования VLAN

Вид запроса командной строки в режиме конфигурирования интерфейса VLAN:

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

Порт доступа (Access) не может быть членом не аутентифицированной VLAN, родной (native) VLAN транкового порта (Trunk) не может быть не аутентифицированным VLAN, но для главного (General) порта PVID может быть не аутентифицированным VLAN (но только тегированные пакеты могут быть приняты в неавторизованном состоянии).

Таблица 5.157 – 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 5.158 – Команды режима Privileged EXEC

Команда	*Значение*	*Действие*
show dot1x advanced [tengigabitethernet *te_port***]**	te_port: (1..8/0/1..48)	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 5.159 – Команды режима Privileged EXEC

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

5.21.3 Контроль протокола DHCP и опция 82

DHCP (Dynamic Host Configuration Protocol) – сетевой протокол, позволяющий клиенту по запросу получать IP-адрес и другие требуемые параметры, необходимые для работы в сети TCP/IP.

Протокол DHCP может использоваться злоумышленниками для совершения атак на устройство, как со стороны клиента, заставляя DHCP-сервер выдать все доступные адреса, так и со стороны сервера, путем его подмены. Программное обеспечение коммутатора позволяет обеспечить защиту устройства от атак с использованием протокола DHCP, для чего применяется функция контроля протокола DHCP – DHCP snooping.

Устройство способно отслеживать появление DHCP-серверов в сети, разрешая их использование только на «доверенных» интерфейсах, а также контролировать доступ клиентов к DHCP-серверам по таблице соответствий.

Опция 82 протокола DHCP (option 82) используется для того, чтобы проинформировать DHCP-сервер о том, от какого DHCP-ретранслятора (Relay Agent) и через какой его порт был получен запрос. Применяется для установления соответствий IP-адресов и портов коммутатора,

а также для защиты от атак с использованием протокола DHCP. Опция 82 представляет собой дополнительную информацию (имя устройства, номер порта), добавляемую коммутатором, который работает в режиме DHCP Relay агента, 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 5.160 - Формат полей опции 82.

Поле	***Общая длина (в байтах)***	***Передаваемая информация***
Circuit ID	4	Первые два байта – идентификатор vlan, через которую был получен dhcp-запрос. Третий байт – номер устройства в стеке. Последний байт – номер порта, к которому подключено устройство, отправляющее dhcp-запрос.
Remote agent ID	6	MAC-адрес устройства.

Для примера, рассмотрим часть фрейма, содержащую опцию 82:

52 12 01 06 00 04 00 02 01 0e 02 08 00 06 02 10 00 10 11 12 13 00

Ниже приведена таблица, описывающая значения данной последовательности:

Таблица 5.161 – Значение байтов в фрейме

Последовательность байт	***Значение***
52 12	Первый байт – идентификатор опции 82: $52_{(16)}$ = 82 Второй байт – длина опции $12_{(16)}$ = 18
01 06	Первый байт - идентификатор саб-опции Circuit ID Второй байт – длина саб-опции
00 04	Первый байт – идентификатор типа Circuit ID Второй байт – длина Circuit ID
00 02	Два байта – идентификатор VLAN, в которой был получен DHCP-запрос
01 0e	Первый байт – Unit ID Второй байт – номер порта $0e_{(16)}$ = 15
02 08	Первый байт – идентификатор подопции Remote ID Второй байт – длина подопции
00 06	Первый байт – идентификатор типа Remote ID Второй байт – длина Remote ID
02 10 11 12 13 00	MAC-адрес коммутатора

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-сервера 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 5.162 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
ip dhcp snooping	По умолчанию контролирование протокола DHCP 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 По умолчанию контролирование протокола DHCP 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*	(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	По умолчанию добавление опции 82 разрешено	Разрешает устройству добавление опции 82 при работе протокола DHCP.
no ip dhcp information option		Запрещает устройству добавление опции 82 при работе протокола DHCP.

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 5.163– Команды режима конфигурирования интерфейса Ethernet, группы интерфейсов

Команда	*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.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 5.164 – Команды режима Privileged EXEC

Команда	*Значение*	*Действие*
ip dhcp snooping binding *mac_address vlan_id ip_address* **{tengigabitethernet** *te_port* **| port-channel** *group* **} expiry {***seconds***|infinity}**	te_port: (1..8/0/1..48) vlan_id: (1 .. 4094); group:(1 .. 32); period: (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 5.165 – Команды режима EXEC

Команда	*Значение*	*Действие*
show ip dhcp information option	-	Показывает информацию об использовании опции 82 протокола DHCP.
show ip dhcp snooping [tengigabitethernet *te_port* **| port-channel** *group***]**	te_port: (1..8/0/1..48); group: (1 .. 32)	Показывает конфигурацию функции контроля протокола DHCP.
show ip dhcp snooping binding [mac-address *mac_address***] [ip-address** *ip_address***] [vlan** *vlan_id***] [tengigabitethernet** *te_port* **| port-channel** *group***]**	te_port: (1..8/0/1..48); group: (1 .. 32) 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 Disabled
DHCP snooping is configured on following VLANs:
DHCP snooping database is Disabled
Relay agent Information option 82 is Enabled
Option 82 on untrusted port is forbidden
Verification of hwaddr field is Enabled
DHCP snooping file update frequency is configured to: 1200 seconds

Interface           Trusted
-----------    ------------
te1/0/17                yes
```

5.21.4 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 5.166 – 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 5.167 – 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 5.168 – 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 5.169 – Команды режима EXEC

Команда	*Значение*	*Действие*
show ip arp inspection [tengigabitethernet *te_port* **| port-channel** *group***]**	te_port: (1..8/0/1..48) group: (1..32}	Показывает конфигурацию функции контроля протокола ARP Inspection на выбранном интерфейсе/всех интерфейсах.
show ip arp inspection list	-	Показывает списки статических соответствий IP- и MAC-адресов (команда доступна только для привилегированного пользователя).
show ip arp inspection statistics [vlan *vlan_id***]**	vlan_id:(1 .. 4094)	Показывает статистику для следующих типов пакетов, которые были обработаны при помощи функции ARP: - переданные пакеты (forwarded); - потерянные пакеты (Dropped); - ошибки в IP/MAC (IP/MAC Failures).
clear ip arp inspection statistics [vlan *vlan_id***]**	vlan_id:(1 .. 4094)	Очищает статистику контроля протокола ARP Inspection.

Примеры выполнения команд

- Включить контроль протокола ARP и добавить в список spisok статическое соответствие: MAC-адрес: 00:60:70:AB:CC:CD, IP-адрес: 192.168.16.98. Назначить список spisok статических ARP соответствий для VLAN 11:

```
console# configure
console(config)# ip arp inspection list 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
```

5.22 Функции DHCP Relay Intermediate Agent

Коммутаторы MES5000 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 5.170 – 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_address*	Может быть задано до 8-ми серверов	Задаёт IP-адрес доступного DHCP-сервера для DHCP Relay агента.
no ip dhcp relay address [*ip_address***]**		Удаляет IP-адрес из списка DHCP-серверов для DHCP Relay агента.

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 5.171 – 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 EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.172 – 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
```

5.23 Конфигурирование ACL (списки контроля доступа)

ACL (Access Control List – список контроля доступа) – таблица, которая определяет правила фильтрации входящего и исходящего трафика на основании передаваемых в пакетах протоколов, TCP/UDP портов, IP-адресов или MAC-адресов.

ACL-списки на базе IPv6, IPv4 и MAC-адресов не должны иметь одинаковые названия.

IPv6 и IPv4-списки могут работать вместе на одном физическом интерфейсе. 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 5.173 – Команды для создания и конфигурирования списков ACL

Команда	*Значение*	*Действие*
ip access-list extended *access_list*	(0..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[1].
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[1].

Для того чтобы активизировать список ACL, необходимо связать его с интерфейсом. Интерфейсом, использующим список, может быть либо интерфейс Ethernet, либо группа портов.

[1] В текущей версии программного обеспечения не поддерживается

Команды режима конфигурирования интерфейса Ethernet, группы портов.

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

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

Таблица 5.174 – Команда назначения списка ACL интерфейсу.

Команда	*Значение*	*Действие*
service-acl input *access_list*	(0 .. 32) символа	В настройках определённого физического интерфейса команда привязывает указанный список к данному интерфейсу.
no service-acl input		Удаление списка с интерфейса.

Команды режима Privileged EXEC

Командная строка в режиме Privileged EXEC имеет вид:

```
console#
```

Таблица 5.175 – Команды для просмотра списков ACL

Команда	*Значение*	*Действие*
show access-lists [*access_list***]**	(0..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 [tengigabitethernet *te_port* **| port-channel** *group***| vlan** *vlan_id***]**	te_port: (1..8/0/1..48); vlan_id: (1..4094); group (1..32)	Показывает списки ACL назначенные интерфейсам.
clear access-lists counters [tengigabitethernet *te_port* **| port-channel** *group***]**	te_port: (1..8/0/1..48); group (1..32)	Обнулить все счетчики списков ACL, либо счетчики для списков ACL заданного интерфейса.
show interfaces access-lists counters [tengigabitethernet *te_port* **| port-channel** *group***]**	te_port: (1..8/0/1..48); group (1..32)	Показывает счетчики списков доступа.

5.23.1 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 5.176 – 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, 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**.
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).
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 (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
source-port	UDP/TCP-порт источника	

		(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).
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.

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 5.177 - 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***]**	Добавляет разрешающую запись фильтрации для протокола. 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***]**	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***]**	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***]**	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.
deny *protocol* **{any|***source source_wildcard***}** **{any|***destination destination_wildcard***}** **[dscp** *dscp* **| precedence** *precedence***]** **[disable-port|log-input]**	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 source_wildcard***}** **{any|***destination destination_wildcard***}** **{any|***icmp_type***} {any|***icmp_code***}** **[dscp** *dscp* **| precedence** *precedence***]** **[disable-port|log-input]**	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***]** **[disable-port|log-input]**	Добавляет запрещающую запись фильтрации для протокола IGMP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова *disable-port* физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова *log-input* будет отправлено сообщение в системный журнал.
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***]** **[disable-port|log-input]**	Добавляет запрещающую запись фильтрации для протокола TCP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова *disable-port* физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова *log-input* будет отправлено сообщение в системный журнал.
deny udp {any| *source source_wildcard***}** **{any|** *source_port***}** **{any|***destination destination_wildcard***}** **{any|***destination_port***}** **[dscp** *dscp* **| precedence** *precedence***]** **[disable-port|log-input]**	Добавляет запрещающую запись фильтрации для протокола UDP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова *disable-port* физический интерфейс, принявший такой пакет, будет выключен.

5.23.2 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 5.178 – 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).
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.

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 по умолчанию добавляются записи permit-icmp any any nd-ns any, permit-icmp any any nd-na any и deny ipv6 any any, две первых из которых разрешают поиск соседних IPv6 устройств с помощью протокола ICMPv6, а последняя означает игнорирование всех пакетов, не удовлетворяющих условиям ACL.

Таблица 5.179 – 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***]**	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***]**	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***]** **[match-all** *list_of_flags***]**	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***]**	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***]** **[disable-port|log-input]**	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***]** **[disable-port|log-input]**	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***]** **[disable-port|log-input]**	Добавляет запрещающую запись фильтрации для протокола TCP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова disable-port физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова *log-input* будет отправлено сообщение в системный журнал.
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***]** **[disable-port|log-input]**	Добавляет запрещающую запись фильтрации для протокола UDP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова disable-port физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова *log-input* будет отправлено сообщение в системный журнал.

5.23.3 Конфигурирование ACL на базе MAC1

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 5.180 - 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.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.

Для выбора всего диапазона параметров, кроме dscp и ip-precedence используется параметр «any».

[1] В текущей версии программного обеспечения не поддерживается

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 5.181 – 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***]**	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***]** **[disable-port|log-input]**	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.

5.24 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 MES5000, 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».

5.24.1 Настройка QoS

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.182 – 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 tail-drop profile {*profile_id* | **cpu}**	profile_id: (1..3)	Создать профиль **qos tail-drop.**
no qos tail-drop profile {*profile_id* | **cpu}**		Удалить профиль **qos tail-drop.**
qos tail-drop mirror-limit {rx | tx} *packets*	packets : (0..5902)/10	Задать размер буфера для зеркалирования входящего/исходящего трафика
no qos tail-drop mirror-limit {rx | tx}		Установить значение по умолчанию.
qos tail-drop multicast-limit *value*	value: (0..4096)/2688	Задать значение используемых multicast-пакетов.
no qos tail-drop multicast-limit		Установить значение по умолчанию.
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 *policy_map-name*		Удаляет правило классификации трафика.
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..4); cos1…cos8: (0..7); Значения CoS по умолчанию для очередей: CoS = 1 – очередь 1 CoS = 2 – очередь 1 CoS = 0 – очередь 2 CoS = 3 – очередь 2 CoS = 4 – очередь 3 CoS = 5 – очередь 3 CoS = 6 – очередь 4 CoS = 7 – очередь 4	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). **При использовании веса исходящих очередей необходимо задавать приоритетность очереди на интерфейсе: priority-queue out.**
no wrr-queue bandwidth		Устанавливает значение по умолчанию.
priority-queue out num-of-queues *number_of_queues*	number_of_queues: (0..8) По умолчанию, приоритетных очередей нет.	Задает номер приоритетной очереди. **Для приоритетной очереди вес WRR будет игнорироваться.**
no priority-queue out num-of-queues		Устанавливает значение по умолчанию.
qos wrr-queue threshold tengigabitethernet *queue_id threshold_percentage*	queue_id: (1..8) threshold_percentage: (0..100) По умолчанию значение пороговых настроек для отбрасывания избыточного трафика равно 80%	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 приоритетом сброса будут отбрасываться в течение всего времени, пока порог превышен.** **Действует только для режима qos advanced.**
no qos wrr-queue threshold tengigabitethernet *queue_id*		Устанавливает значения порогов по умолчанию
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: (0..63)	Устанавливает соответствие между значениями DSCP

dscp_list **to** *queue_id*	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	входящих пакетов и очередями. - *dscp_list* – определяет до 8 значений DSCP, значения разделяются знаком пробела. **Действует только для режима qos advanced.**
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 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.

*Команды 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 5.183– Команды режима конфигурирования профиля qos tail-drop

Команда	*Значение*	*Действие*
port-limit *value*	value: (0..1200)/88	Установить ограничение (в пакетах) использования разделяемого пула портом.
no port-limit		Установить настройки по умолчанию
queue *queue_num* **[limit** *value***] [with-sharing | without-sharing]**	value: (0..1200)/18 /with-sharing queue_num: (1..8)/0	Установить размер очереди (в пакетах) и разрешить/запретить для очереди доступ к разделяемому пулу.
no queue *queue_num*		Удалить настройки очереди

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 5.184 – 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 5.185 – 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. - **access_group** – 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 5.186 – 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 aggregate *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 aggregate *aggregate_policer_name*		Удаляет шаблон настроек регулирования скорости канала из правила классификации трафика.

Команды режима конфигурирования интерфейса Ethernet, группы портов

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

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

Таблица 5.187 – 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* [*committed_burst*]	committed_rate: (64..1000000) кбит/с committed_burst: (4096.. 12578880) байт	Устанавливает ограничение скорости для исходящего 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: (64..1000000) кбит/с committed_burst: (4096.. 12578880) 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. **Ограничение скорости для конкретного порта может быть применено, только если к нему не применена команда port storm-control broadcast enable.** **Данная команда доступна только в режиме конфигурирования интерфейса Ethernet.**
no rate-limit		Снимает ограничение скорости входящего трафика.
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.
qos tail-drop profile *value*	value : (1..3)	Назначить профиль qos tail-drop на интерфейс
no qos tail-drop profile		Удалить профиль qos tail-drop

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.188 – Команды режима EXEC

Команда	*Действие*
show qos	Показывает режим QOS настроенный на устройстве. В базовом режиме показывает «доверенный» режим (trust mode).
show class-map [*class_map_name*]	Показывает списки критериев классификации трафика. **Действует только для режима qos advanced.**
show policy-map [*policy_map_name*]	Показывает правила классификации трафика. **Действует только для режима qos advanced.**
show qos aggregate-policer [*aggregate_policer_name*]	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**] **[tengigabitethernet** *te_port* **|port-channel** *group***| vlan** *vlan_id***]**	Показывает QoS-параметры для интерфейса. - *vlan_id* – номер VLAN (1..4094); - *te_port* – номер интерфейса Ethernet (1..8/0/1..48); - *group* – номер группы портов (1..32); - **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**]	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.
show qos tail-drop [interface {tengigabitethernet *te_port* **| port-channel** *group***}]**	Просмотр параметров tail-drop. - *te_port* – номер интерфейса Ethernet (1..8/0/1..48); - *group* – номер группы портов (1..32);

Примеры выполнения команд.

- Включить режим QoS advanced. Распределить трафик по очередям, пакеты с DSCP 12 в первую очередь, пакеты с DSCP 16 во вторую. Первая 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 te1/0/14 и te1/0/16.

```
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 tengigabitethernet 1/0/14
console(config-if)# service-policy input
console(config-if)# exit
console(config)# interface tengigabitethernet 1/0/16
console(config-if)# service-policy input
console(config-if)# exit
console(config)#
```

5.24.2 Статистика QoS

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.189 – 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}** {**tengigabitethernet** *te_port* **| all**}	set: (1..2) queue: (1..8) dp: (high, low) te_port:(1..8/0/1..48) 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 5.190 – 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 5.191 – Команды режима EXEC.

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

5.25 Конфигурация протоколов маршрутизации

5.25.1 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 5.192 – Команды режима глобального конфигурирования

Команда	*Действие*
ip route *prefix* **{***mask* **|** *prefix_length***}** *gateway* **[metric** *distance***] [reject]**	Создает статическое правило маршрутизации. - *prefix* – сеть назначения (например, 172.7.0.0); - *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 (1..255) (если не указано, то по умолчанию значение 1); - **reject** – запрещает маршрутизацию к сети назначения через все шлюзы.
no ip route *prefix* **{***mask* **|** *prefix_length***}** **[***gateway***]**	Удаляет правило из таблицы статической маршрутизации.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.193 – Команды режима EXEC

Команда	*Действие*
show ip route [address |connected | static | ospf | rip | {address *ip_address* **[***mask* **|** *prefix_length***] [longer-prefixes]}]**	Показывает таблицу маршрутизации, удовлетворяющую заданным критериям. - **address** – показывает информацию по определенному маршруту; - **connected** – подключенный маршрут, то есть маршрут, взятый с непосредственно подключенного и функционирующего интерфейса; - **static** – статический маршрут, прописанный в таблице маршрутизации; - **ospf** – динамический маршрут, полученный по протоколу OSPF; - **rip** – динамический маршрут, полученный по протоколу RIP; - *ip_address* – IP-адрес; - *mask* – маска подсети; - *prefix_length* – длина префикса; - **longer-prefixes** – параметр, необходимый для отображения точного соответствия

	указанной подсети и маске.

Пример выполнения команды

- Показать таблицу маршрутизации:

```
console# show ip route
```

```
Maximum Parallel Paths: 4 (4 after reset)
Codes: C - connected, S - static, D - DHCP, R - RIP, O - OSPF, E - OSPF external
C 10.0.1.0/24 is directly connected, Vlan  1
E 10.0.2.0/24 [110/1] via 10.0.1.15 1:31:14    Vlan 10
S 10.9.1.0/24 [5/2]     via 10.0.1.2, 17:19:18, Vlan 12
```

Таблица 5.194 – 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); - E – OSPF external (динамический маршрут, полученный по протоколу OSPF).
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.
1:31:14	Определяет время последнего обновления маршрута (часы, минуты, секунды).
Vlan 1	Определяет интерфейс, через который проходит маршрут до сети.

5.25.2 Настройка протокола RIP

Протокол RIP (англ. Routing Information Protocol) — внутренний протокол, который позволяет маршрутизаторам динамически обновлять маршрутную информацию, получая ее от соседних маршрутизаторов. Протокол основан 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.

Команды режима глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

```
console(config)#
```

Таблица 5.195 – Команды режима глобального конфигурирования

Команда	*Значение по умолчанию*	*Действие*
router rip enable	-	Включает маршрутизацию по протоколу RIP.
no router rip enable		Выключает маршрутизацию по протоколу RIP.
router rip redistribute | ospf | static |	-	Включает анонсирование статических или ospf маршрутов: - **ospf** – включить анонсирование OSPF-маршрутов; - **static** – включить анонсирование статических

		маршрутов.
router rip redistribute | ospf | static |		Выключает анонсирование статических или ospf маршрутов.

Команды режима конфигурирования интерфейса ip

Вид запроса командной строки:

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

Таблица 5.196 – Команды режима конфигурирования интерфейса ip

Команда	*Значение/ Значение по умолчанию*	*Действие*
rip authentication | text | md5 |	-/отключена	Включает аутентификацию в RIP и определяет ее тип: - **text** – аутентификация открытым текстом; - **md5** – аутентификации MD5.
no rip authentication		Отключает аутентификацию в RIP.
rip auto-send	-/включена	Включение автоматического определения необходимости рассылки полной маршрутной информации RIP.
no rip auto-send		Отключение автоматического определения необходимости рассылки полной маршрутной информации RIP.
ip rip default-route originate *metric*	(1 .. 15)/ отключена	Устанавливает метрику для маршрута по умолчанию транслируемого через RIP.
no ip rip default-route originate		Устанавливает значение по умолчанию.
rip offset *offset*	1-15/1	Добавляет смещение к метрике. - *offset* – смещение к метрике.
rip-passive interface	-/включена	Выключает отправку обновлений на интерфейсе.
no rip-passive interface		Устанавливает значение по умолчанию.
rip version | 1 | 2 |	2	Выбор версии протокола RIP 1 / RIP 2.

Команды режима privileged EXEC

Вид запроса командной строки в режиме privileged EXEC:

```
console#
```

Таблица 5.197 – Команды режима privileged EXEC

Команда	*Значение*	*Действие*
show ip rip [statistics | peers]	-	Просмотр информации о RIP-маршрутизации: - **statistics** – статистические данные; - **peers** – информация участника сети.

5.25.3 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.

Команды режима глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

```
console(config)#
```

Таблица 5.198 – 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)/110	Устанавливает стоимость суммарного маршрута по умолчанию для зоны типа stub. - *A.B.C.D* – идентификатор маршрутизатора в формате IPv4-адреса; - *cost* – стоимость суммарного маршрута по умолчанию для зоны типа stub.
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 5.199 – 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. - *cost* – метрика состояния канала, чем ниже значение, тем выше приоритет канала.
no ospf cost		Устанавливает значение по умолчанию.
ospf priority *priority*	priority: (0..255)/1	Устанавливает приоритет маршрутизатора, который используется для выбора DR и BDR. - *priority* – приоритет маршрутизатора, чем ниже значение, тем выше приоритет канала.
no ospf priority		Устанавливает значение по умолчанию.
ospf area *A.B.C.D*	-	Устанавливает идентификатор зоны по умолчанию. - *A.B.C.D* – идентификатор зоны в формате IPv4-адреса.
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. - *interval* – период времени, в секундах.
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. - *interval* – период времени, в секундах.
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). - *interval* – период времени, в секундах.
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. - *delay* – период времени, в секундах.
no ospf transmit-delay		Устанавливает значение по умолчанию.
ospf mtu *mtu*	mtu: (128..10218)/	Устанавливает значение MTU (maximum transmission unit)

	- при включенном « jumbo frame» - 10218; - при отключенном « jumbo frame» - 1500.	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.
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. **- default –** при использовании команды 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 5.200 – 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*	-	Отображает информации о OSPF-соседях на данном IP-интерфейсе. - *A.B.C.D* – IP-адрес интерфейса.
show ip ospf interface	-	Отображает конфигурации всех OSPF-интерфейсов.
show ip ospf interface *A.B.C.D*	-	Отображает конфигурации определенного OSPF-интерфейса. - *A.B.C.D* – IP-адрес интерфейса.
show ip ospf database [router] [network] [summary] [asbr-summary] [external] [*A.B.C.D***] [adv-router] [self-originate] [database-summary]**		Отображает состояние базы данных протокола OSPF. - **router** – отображает объявления коммутатора; - **network** – отображает объявления сети; - **summary** – отображает информацию о маршрутах от ABR; **- asbr-summary** – отображает информацию о маршрутах от ASBR; - **external** – отображает информацию о внешних маршрутах; - *A.B.C.D* – IP-адрес интерфейса; **- adv-router –** отображает информацию определенного маршрутизатора; **- self-originate –** отображает информацию о собственных маршрутах; **- database-summary** – отображает всю информацию в базе данных 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 [router *A.B.C.D* **] [area** *E.F.G.H* **]**	-	Отображает параметры и текущее состояние виртуальных линков: - **router –** для указанного маршрутизатора (опционально); - **area –** для указанной зоны (опционально);

		- *A.B.C.D* – IP-адес интерфейса; - *E.F.G.H* – идентификатор зоны.

5.25.4 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 5.201 – 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 5.202 – 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. - *send_interval* – интервал отправки; - *recv_interval* – минимальный допустимый интервал приема анонсов.
no bfd interval		Восстанавливает значение по умолчанию.
ospf bfd [disable]	-/включено	Включает/отключает BFD для данного интерфейса.

Команды режима privileged EXEC

Вид запроса командной строки в режиме privileged EXEC:

```
console#
```

Таблица 5.203 – Команды режима privileged EXEC

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

5.26 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 5.204 – Команды режима конфигурирования интерфейса Ethernet, VLAN, интерфейса группы портов

Команда	*Значение/Значение по умолчанию*	*Действие*
vrrp *vrid* **authentication** *password*	vrid: (1..255); password: (1..8) символов	Добавление пароля для аутентификации VRRP. - *vrid* – идентификатор виртуального маршрутизатора; - *password* – строка для аутентификации.
no vrrp *vrid* **authentication**		Удаление пароля для аутентификации.
vrrp *vrid* **ip** *ip_address*	vrid: (1..255)	Определение IP-адреса VRRP-маршрутизатора. - *vrid* – идентификатор виртуального маршрутизатора; - *ip_address* – IP-адрес виртуального маршрутизатора.
no vrrp *vrid* **ip**		Удаление IP-адреса VRRP с маршрутизатора, что приведет к удалению виртуального маршрутизатора *vrid* на данном интерфейсе.
vrrp *vrid* **preempt**	vrid: (1..255)/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. - *vrid* – идентификатор виртуального маршрутизатора. **Маршрутизатор, который является владельцем IP-адреса маршрутизатора, будет перехватывать на себя роль master независимо от настроек данной команды.**
no vrrp *vrid* **preempt**		Отключение режима.
vrrp *vrid* **priority** *priority*	vrid: (1..255); priority: (1..254). По умолчанию priority: 255 для владельца IP-адреса, 100 для остальных	Назначение приоритета VRRP-маршрутизатора. - *vrid* – идентификатор виртуального маршрутизатора; - *priority* – приоритет виртуального маршрутизатора.
no vrrp *vrid* **priority**		Установка значения по умолчанию.
vrrp *vrid* **up**	vrid: (1..255)/выключен	Включение VRRP-протокола на данном интерфейсе. - *vrid* – идентификатор виртуального маршрутизатора.
no vrrp *vrid* **up**		Выключение VRRP-протокола на данном интерфейсе.

vrrp *vrid* **source-ip** *ip_address*	vrid: (1..255). По умолчанию ip_address: 0.0.0.0	Определение реального VRRP-адреса, который будет использоваться в качестве IP-адреса отправителя для VRRP-сообщений. - *vrid* – идентификатор виртуального маршрутизатора; - *ip_address* – IP-адрес виртуального маршрутизатора.
no vrrp *vrid* **source-ip**		Установка значения по умолчанию.
vrrp *vrid* **timer** *seconds*	vrid: (1..255); seconds: (1..255)/1 с	Определение интервала между анонсами master-маршрутизатора. - *vrid* – идентификатор виртуального маршрутизатора; - *seconds* – период времени между анонсами master-маршрутизатора в секундах.
no vrrp *vrid* **timer**		Установка значения по умолчанию.

Команды режима privileged EXEC

Все команды доступны для привилегированного пользователя.

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 5.205 – Команды режима privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show vrrp configuration [{tengigabitethernet *te_port* **| port-channel** *group* **| vlan** *vlan_id***}]**	te_port: (1..8/0/1..48); group: (1..12); vlan_id: (1..4094)	Просмотр информации о настройке VRRP для всех или одного виртуального маршрутизатора.
show vrrp status [{tengigabitethernet *te_port* **| port-channel** *group* **| vlan** *vlan_id***}]**	te_port: (1..8/0/1..48); group: (1..12); vlan_id: (1..4094)	Просмотр информации о состоянии всех или одного виртуального маршрутизатора VRRP.

Примеры выполнения команд

▪ Настроить IP-адрес 10.10.10.1 на VLAN 10, использовать этот адрес в качестве адреса виртуального маршрутизатора. Включить VRRP-протокол на интерфейсе VLAN.

```
console(config-vlan)# interface vlan 10
console(config-if)# ip address 10.10.10.1 /24
console(config-if)# vrrp 1 ip 10.10.10.1
console(config-if)# vrrp 1 up
```

- Посмотреть конфигурацию VRRP:

```
console# show vrrp configuration
```

```
Interface VRID     Address      Priority Timer Auth Preempt    Source-ip     State
--------- ---- --------------- -------- ----- ---- ------- --------------- -----
 vlan 10   1     10.10.10.1      255      1    No    Yes       0.0.0.0       up
```

6 СМЕНА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

6.1 Обновление программного обеспечения с сервера TFTP

Сервер TFTP должен быть запущен и настроен на компьютере, с которого будет загружаться программное обеспечение. Файлы с загрузочным и/или системным программным обеспечением должны быть доступны серверу. Компьютер с запущенным TFTP-сервером доступен коммутатору (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.

6.1.1 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 [unit unit] { image-1 | image-2 }
```

где *unit* – 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    2.0.0.1 ( date  21-Jun-2011 time  20:38:14 )
Boot version    1.0.2.01 ( date  16-Mar-2011 time  16:50:30 )
HW version    01.00.00
```

Процедура обновления ПО:

Командой **copy** скопировать новый файл программного обеспечения на устройство в выделенную область памяти (image2). Формат команды **copy tftp://{tftp ip address}/{file name} 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: **boot system [unit unit] { image-1 | image-2 }**.

```
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    2.0.0.1     21-Jun-2011  20:38:14   Not active
2      image-2    2.1.0       07-Jun-2013  14:00:50   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'**.

6.1.2 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    2.0.0.1 ( date  21-Jun-2011 time  20:38:14 )
Boot version    1.0.2.01 ( date  16-Mar-2011 time  16:50:30 )
HW version    01.00.00
```

Процедура обновления ПО:

1. Командой **copy** скопировать новый загрузочный файл на устройство. Формат команды: **copy tftp://{tftp ip address}/{file name} boot.**

```
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’**.

7 ПРИМЕРЫ ПРИМЕНЕНИЯ И КОНФИГУРИРОВАНИЯ УСТРОЙСТВА

7.1 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 15 - 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 tengigabitethernet 1/0/1-2
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk allowed vlan add 10,20,30,40,50,60
console(config-if)# exit
```

```
console(config)# spanning-tree mst configuration
console(config-mst)# name sandbox
console(config-mst)# instance 1 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
```

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 29В.
Телефон:
+7(383)274-10-01,
+7(383) 274-47-87,
+7(383) 272-83-31,
+7(383)274-47-88.
E-mail: techsupp@eltex.nsk.ru

На официальном сайте компании Вы можете найти техническую документацию и программное обеспечение для продукции ООО «Предприятие «ЭЛТЕКС» или проконсультироваться у инженеров Сервисного центра на техническом форуме:

http://eltex-co.ru/
http://eltex-co.ru/support/
http://forum.eltex-co.ru/