Комплексные решения для построения сетей

MES3124
MES3124F

Руководство по эксплуатации, версия 1.1 (01.2011)

Коммутаторы магистрального уровня, коммутаторы уровня агрегации

Версия документа	Дата выпуска	Содержание изменений
Версия 1.1	26.01.2011	Изменения в следующих разделах: 4.3 Загрузочное меню 4.4 Режимы работы коммутатора 4.5.1 Базовая настройка коммутатора 5.7 Selective Q-in-Q 6.1 Меню Startup
Версия 1.0	28.05.2010	Первая публикация.
Версия программного обеспечения	**1.0.16**	

СОДЕРЖАНИЕ

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 обязательные параметры.
«,» **«-»**	Данные знаки в описании команды используются для указания диапазонов.
«|»	Данный знак в описании команды обозначает «или».
«/»	Данный знак при указании значений переменных разделяет возможные значения и значения по умолчанию.
Курсив Calibri	Курсивом Calibri указываются переменные или параметры, которые необходимо заменить соответствующим словом или строкой.
Полужирный курсив	Полужирным курсивом 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 MES3124, MES3124F 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) и возможность подключения резервного источника питания.

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

Устройство MES3124 является мощным многоцелевым сетевым коммутатором, выполняющем свои коммутационные функции на канальном и сетевом уровнях модели OSI. Коммутаторы MES3124/3124F обеспечивают высокую плотность электрических/оптических гигабитных портов, позволяют подключаться к оптическим линиям посредством комбинированных интерфейсов и имеют порты 10G uplink, что позволяет постепенно перейти от скоростей 1G к скоростям 10G.

2.2 Функции MES3124

2.2.1 Основные функции

В таблице 2.1 приведен список основных функций устройства MES3124/MES3124F, доступных для администрирования.

Таблица 2.1 – Основные функции устройства

Защита от блокировки очереди (HOL)	Блокировка возникает в случаях перегрузки выходных портов устройства трафиком от нескольких входных портов. Это приводит к задержкам передачи данных и потере пакетов.
Поддержка обратного давления (Back pressure)	Метод обратного давления используется на полудуплексных соединениях для регулирования потока данных от встречного устройства путем создания коллизий. Метод позволяет избежать переполнения буферной памяти устройства и потери данных.
Поддержка MDI/MDIX	Автоматическое определение типа кабеля - перекрестный кабель или кабель прямого подключения. – MDI (Media-Dependent Interface – прямой) – стандарт кабелей для подключения оконечных устройств; – MDIX (Media-Dependent Interface with Crossover – перекрестный) - стандарт кабелей для подключения концентраторов и коммутаторов.
Поддержка сверхдлинных кадров (Jumbo frames)	Сетевой коммутатор MES3124 способен 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 устройства MES3124 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. MES3124 поддерживает до 16000 MAC-адресов и резервирует 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, поступивший кадр, предназначенный для хоста, MAC-адрес которого уже есть в таблице, передается только через указанный порт в таблице.
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 Multicast (IGMP Snooping)	Реализация протокола IGMP позволяет MES3124 на основе информации, полученной при анализе содержимого IGMP пакетов, определить, какие устройства в сети участвуют в группах многоадресной рассылки, и адресовать трафик на соответствующие порты.
Функция MLD Snooping	Реализация протокола MLD позволяет устройству минимизировать многоадресный IPv6 трафик
Функция MVR	Функция, позволяющая перенаправлять многоадресный трафик из одной VLAN в другую на основании IGMP-сообщений, что позволяет уменьшить нагрузку на uplink-порту. Применяется в решениях III-play
Защита от широковещательного «шторма» (Broadcast Storm Control)	Широковещательный шторм – это размножение широковещательных сообщений в каждом узле, которое приводит к лавинообразному росту их числа и парализует работу сети. Устройство MES3124 имеет 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 MES3124 есть возможность задать контролирующий и контролируемые порты и выбрать тип трафика (входящий и/или исходящий), который будет передан на контролирующий порт.
Изоляция портов (Protected ports)	Данная функция позволяет назначить порту его uplink-порт, на который безусловно будет перенаправляться весь трафик, обеспечивая тем самым изоляцию с другими портами (в пределах одного коммутатора), находящихся в этом же широковещательном домене (VLAN) в пределах одного коммутатора.
Private VLAN Edge	Данная функция позволяет изолировать группу портов (в пределах одного коммутатора), находящихся в одном широковещательном домене между собой, позволяя при этом обмен трафиком с другими портами, находящимися в этом же широковещательном домене, но не принадлежащими к этой группе.
Private VLAN (light version)	Обеспечивает изоляцию между устройствами, находящимися в одном широковещательном домене, в пределах всей L2-сети. Реализованы только два режима работы порта Promiscious 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 spaning 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	Сетевой коммутатор MES3124 поддерживает работу виртуальных сетей VLAN.
Поддержка GVRP (GARP VLAN)	Протокол регистрации GARP VLAN обеспечивает динамическое добавление/удаление групп VLAN на портах MES3124. 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 устройстве MES3124 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 восьми объединенных каналов, каждый из которых может содержать до восьми портов. Группа LAG состоит из портов с одинаковой скоростью, работающих в дуплексном режиме.
Поддержка Auto Voice VLAN	Предоставляет возможность идентифицировать голосовой трафик на основании OUI (Organizationally Unique Identifier – первые 24 бита MAC-адреса). Если в MAC-таблице коммутатора присутствует MAC-адрес с OUI голосового шлюза или же IP-телефона, то данный порт автоматически добавляется в voice vlan (идентификация по протоколу SIP или же по MAC-адресу получателя не поддерживается)
Selective Q-in-Q	Позволяет назначать внешний VLAN SPVLAN (Service Provider's VLAN) на основе сконфигурированных правил фильтрации по номерам внутренних VLAN (Customer VLAN). Применение Selective Q-in-Q позволяет разобрать трафик абонента на несколько VLAN, изменить метку SPVLAN у пакета в отдельном участке сети

2.2.4 Функции третьего уровня сетевой модели OSI

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

Таблица 2.4 – Описание функций третьего уровня (Layer 3)

Клиенты BootP и DHCP (Dynamic Host Configuration Protocol)	Устройство MES3124 способно автоматически получать IP-адрес по протоколу BootP/DHCP.
Статические IP-маршруты	Администратор MES3124 имеет возможность добавлять и удалять статические записи в таблицу маршрутизации.
Протокол ARP (Address Resolution Protocol)	ARP – протокол сопоставления IP-адреса и физического адреса устройства. Соответствие устанавливается на основе анализа ответа от узла сети, адрес узла запрашивается в широковещательном пакете.

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. MES3124 может использовать значение приоритета 802.1p для распределении кадров по приоритетным очередям.

2.2.6 Функции обеспечения безопасности

Таблица 2.6 – Функции обеспечения безопасности

DHCP snooping	Функция коммутатора, предназначенная для защиты от атак с использованием протокола DHCP. Обеспечивает фильтрацию DHCP сообщений, поступивших с ненадежных портов путем построения и поддержания базы данных привязки DHCP (DHCP snooping binding database). DHCP snooping выполняет действия брандмауэра между ненадежными портами и серверами DHCP.
Опция 82 протокола DHCP	Опция, которая позволяет проинформировать DHCP – сервер о том, с какого DHCP-ретранслятора и через какой порт пришел запрос. По умолчанию коммутатор, использующий функцию DHCP snooping, обнаруживает и отбрасывает любой DHCP-запрос содержащий опцию 82, который он получил через ненадёжный (untrusted) порт.
UDP relay	Перенаправление широковещательного UDP-трафика на указанный IP-адрес
IP Source address guard	Функция коммутатора, которая ограничивает IP-трафик, фильтруя его на основании таблицы соответствий базы данных привязки DHCP – DHCP snooping и статически сконфигурированных IP-адресов. Функция используется для борьбы с подменой IP-адресов.
Dynamic ARP Inspection (Protection)	Функция коммутатора, предназначенная для защиты от атак с использованием протокола ARP. Сообщение, которое поступает с ненадежного порта, подвергается проверке – соответствует ли IP-адрес в теле принятого ARP-пакета IP-адресу отправителя. Если адреса не совпадают, то коммутатор отбрасывает пакет.
L2 – L3 – L4 ACL (Access Control List)	На основе информации, содержащейся в заголовках уровней 2, 3 и 4, у администратора есть возможность настроить до 512 правил, согласно которым пакет будет обработан, либо отброшен.
Time-Based ACL	Позволяет сконфигурировать временные рамки, в течение которых данный ACL будет действовать
Поддержка заблокированных портов	Основная функция блокировки – повысить безопасность сети, предоставляя доступ к порту коммутатора только для устройств имеющих MAC – адреса, закрепленные за этим портом.
Проверка подлинности на основе порта (802.1x)	Проверка подлинности IEEE 802.1x представляет собой механизм контроля доступа к ресурсам через внешний сервер. Прошедшие проверку подлинности пользователи получают доступ к ресурсам выбранной сети.

2.2.7 Функции управления коммутатором

Таблица 2.7 – Основные функции управления коммутатором MES3124

Загрузка и выгрузка файла настройки	Параметры устройства MES3124 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. Устройство MES3124 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 устройством MES3124 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. Коммутатор MES3124 содержит клиентскую часть протокола RADIUS.
TACACS+ (Terminal Access Controller Access Control System)	Устройство предоставляет поддержку проверки подлинности клиентов посредством протокола TACACS+. Протокол TACACS+ обеспечивает централизованную систему безопасности для проверки пользователей, получающих доступ к устройству, а так же централизованную систему управления при соблюдении совместимости с RADIUS и другими процессами проверки подлинности.

Сервер SSH	Функция сервера SSH позволяет клиенту SSH установить с устройством защищенное соединение для управления им.
Поддержка макрокоманд	Данная функция предоставляет возможность создавать макрокоманды, представляющие собой набор команд, и применять их для конфигурации устройства

2.2.8 Дополнительные функции

В таблице приведены дополнительные функции устройства.

Таблица 2.8 – Дополнительные функции устройства

Виртуальное тестирование кабеля (VCT)	Сетевой коммутатор MES3124 имеет в своём составе программные и аппаратные средства, позволяющие выполнять функции виртуального тестирования кабеля – VCT: – определение проблем связи при использовании медных кабелей (обрыв, замыкание проводов); – отчет по результатам тестирования.
Диагностика оптического трансивера	Устройство позволяет тестировать оптический трансивер. При тестировании отслеживаются такие параметры, как ток и напряжение питания, температура трансивера. Для реализации требуется поддержка этих функций в трансивере.
Green Ethernet	Данный механизм позволяет коммутатору снизить энергопотребление за счет отключения неактивных электрических портов

2.3 Основные технические характеристики

Основные технические параметры коммутатора приведены в таблице 2.9

Таблица 2.9 – Основные технические характеристики

Общие параметры		
Пакетный процессор		98DX4122
Интерфейсы	MES3124	24x 10/100/1000Base-T 4x (10GBase-X(SFP+)/1000Base-X (SFP)
	MES3124F	20x 1000 Base-X (SFP) 4xCombo (10/100/1000Base-T/1000Base-X) 4x (10G Base-X (SFP+)/1000Base-X (SFP))
Оптические трансиверы		SFP, SFP+
Дуплексный/Полудуплексный режим		Дуплексный/ полудуплексный режим для электрических портов, дуплексный режим для оптических портов
Производительность коммутатора		128 Gbps
Объем буферной памяти		12 Mb
Скорость передачи данных		Электрические интерфейсы 10/100/1000 Мбит/с Оптические интерфейсы 1/10 Гбит/с

Таблица MAC-адресов	16К записей
Поддержка VLAN	согласно 802.1Q до 4К
Качество обслуживания QoS	Приоритезация трафика, 8 уровней. 8 выходных очереди с разными приоритетами для каждого порта.
Multicast	До 256 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
Физические характеристики и условия окружающей среды	
Напряжение питания	с питанием от переменного тока: 220В, 50 Гц с питанием от постоянного тока: -48..-60В Варианты питания: - один источник питания AC или DC; - один источник питания (AC или DC) с возможностью горячей замены и вход для резервного источника питания 12V (RPS); -два источника питания(AC или DC) с возможностью горячей замены.
Потребляемая мощность	не более 50Вт
Масса	не более 2,6 кг
Габаритные размеры	430x44x265 мм
Интервал рабочих температур	от -10 до +45 ^{o}C
Влажность	относительная влажность 80%
Средний срок службы	20 лет

Тип питания устройства определяется при заказе.

2.4 Конструктивное исполнение

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

Ethernet-коммутаторы MES3124/MES3124F выполнены в металлическом корпусе с возможностью установки в 19” каркас типоразмером 1U.

2.4.1 Передняя панель устройства

Внешний вид передней панели MES3124/MES3124F показан на рисунках 1, 2.

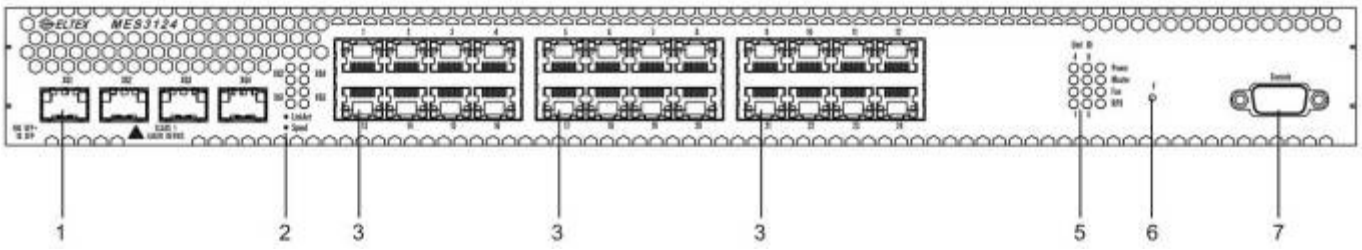

Рисунок 1 – MES3124, передняя панель

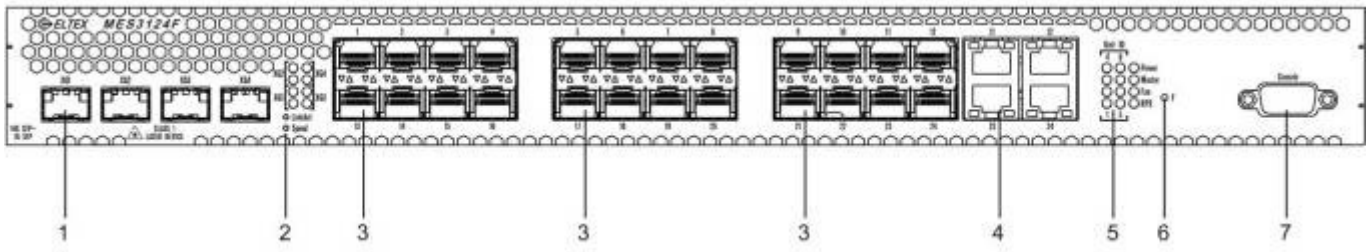

Рисунок 2 – MES3124F, передняя панель

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

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

№	Элемент панели	Описание
1	XG1-XG4	Слоты для установки трансиверов SFP+/SFP
2	XG1-XG4	Индикаторы работы оптических интерфейсов XG1-XG4
3	[1 .. 24]	24 порта Gigabit Ethernet (10/100/1000 Мбит/с., RJ-45)
4	11, 12, 23, 24[1]	Слоты для установки SFP-трансиверов
5	Unit ID (1-8)	Индикаторы номера устройства в стеке
	Power	Индикатор питания устройства
	Master	Индикатор режима работы устройства (ведущий/ведомый)

[1] Только для модели MES3124F

	Fan	Индикатор работы вентиляторов
	RPS	Индикатор резервного электропитания
6	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: - при нажатии на кнопку длительностью менее 10 с происходит перезагрузка устройства. - при нажатии на кнопку длительностью более 10 с. происходит сброс устройства до заводской конфигурации.
7	Console	Консольный порт RS-232 для локального управления устройством

Четыре электрических интерфейса Ethernet и четыре оптических интерфейса являются комбинированными (combo-порты 11,12,23,24). В комбинированных портах может быть активным только один из интерфейсов, но не оба одновременно.

2.4.2 Задняя панель устройства

Внешний вид задней панели MES3124/MES3124F приведен на рисунке 3[1].

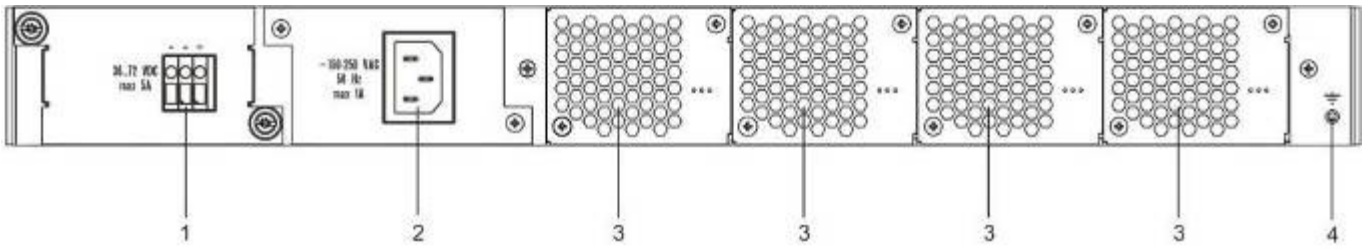

Рисунок 3- MES3124/MES3124F задняя панель

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

Таблица 2.11 – Описание разъемов задней панели коммутатора

№	Элемент задней панели	Описание
1	36 .. 72 VDC, max 5A	Разъем для подключения к источнику электропитания постоянного тока
2	~150-250VAC, 50Hz, max 1A	Разъем для подключения к источнику электропитания переменного тока
3	Съемные вентиляторы	До 4-х съемных вентиляторов
4	Клемма заземления ⏚	Клемма для заземления устройства.

[1] На рисунках приведена комплектация коммутатора с 1 источником питания постоянного тока и с 1 источником питания переменного тока.

2.4.3 Боковые панели устройства

Рисунок 4 – Правая боковая панель Ethernet-коммутатора MES3124/MES3124-DC

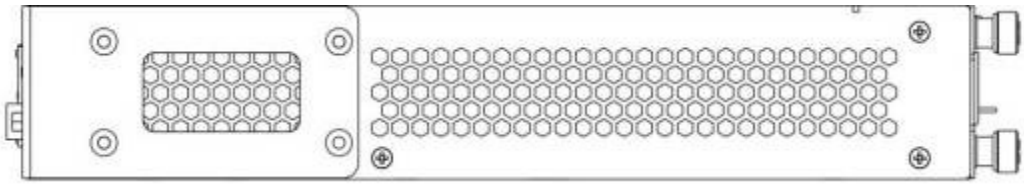

Рисунок 5– Левая боковая панель Ethernet-коммутатора MES3124/MES3124-DC

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 интерфейса Ethernet индицируется двумя светодиодными индикаторами, LINK1000 и ACT зеленого цвета, расположенными в разъеме RJ-45 этого интерфейса. Расположение светодиодов показано на рисунке 6.

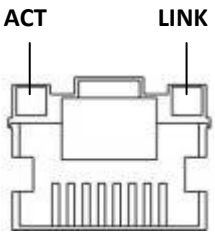

Рисунок 6– Внешний вид разъема RJ-45

Таблица 2.12 – Световая индикация состояния интерфейсов Ethernet

Свечение индикатора LINK1000	Свечение индикатора ACT	Состояние интерфейса Ethernet
Выключен	Выключен	Порт выключен или соединение не установлено
Выключен	Горит постоянно	Установлено соединение на скорости 10 или 100Мбит/с
Горит постоянно	Горит постоянно	Установлено соединение на скорости 1000Мбит/с
X	Мигание	Идет передача данных

Состояние оптических интерфейсов индицируется светодиодными индикаторами связанных с ними электрических портов и индикаторами «SFP Act». Режим работы индикаторов LINK1000 и ACT остается неизменным. Поскольку оптический интерфейс всегда работает на скорости 1000Мбит/с, индикатор LINK1000 горит постоянно. Индикаторы “SFP Act” показывают, какой интерфейс порта активен в данный момент – оптический или электрический. Светящийся индикатор «SFP Act» соответствует активности оптического интерфейса.

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

Системные индикаторы (Power, Master, Fan, RPS) служат для определения состояния работы узлов коммутатора MES 3124/MES3124F.

Таблица 2.13 – Световая индикация системных индикаторов и индикаторов XG портов

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
XG1-XG4	Режим работы порта	Активен нижний из пары (зеленый цвет)	скорость работы порта – 1000Мбит/с
		Активны (мерцают) оба индикатора (нижний – зеленый, верхний – оранжевый)	передача данных на скорости 10 Гбит/с
Power	Состояние источников питания	Выключен	Питание выключено
		Зеленый, горит постоянно	Питание включено, нормальная работа устройства
		Зеленый, мерцает	Самотестирование устройства при старте (POST)
		Красный, мерцает	Авария устройства
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	Зеленый, горит постоянно	Вентилятор исправен
		Красный, мерцает	Отказ вентилятора
RPS	Режим работы резервного источника питания	Зеленый, горит постоянно	Резервный источник подключен и работает нормально
		Выключен	Резервный источник не подключен
		Красный, мерцает	Авария резервного источника

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 MES3124/MES3124F;
- Модуль питания PM75-48/12 или PM-150-220/12;
- шнур питания (в случае комплектации модулем питания на 220В);
- комплект крепежа в стойку;
- документация.

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

3 УСТАНОВКА И ПОДКЛЮЧЕНИЕ

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

3.1 Крепление кронштейнов

В комплект поставки устройства входят кронштейны для установки в стойку и винты для крепления кронштейнов к корпусу устройства. Для установки кронштейнов:

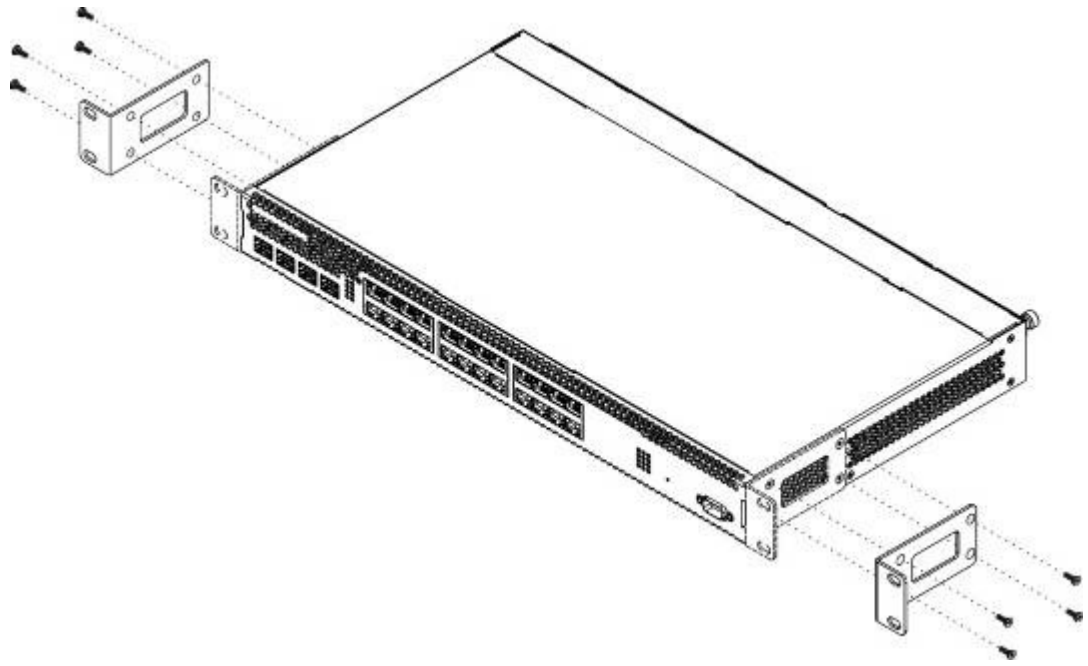

Рисунок 7– Крепление кронштейнов

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.

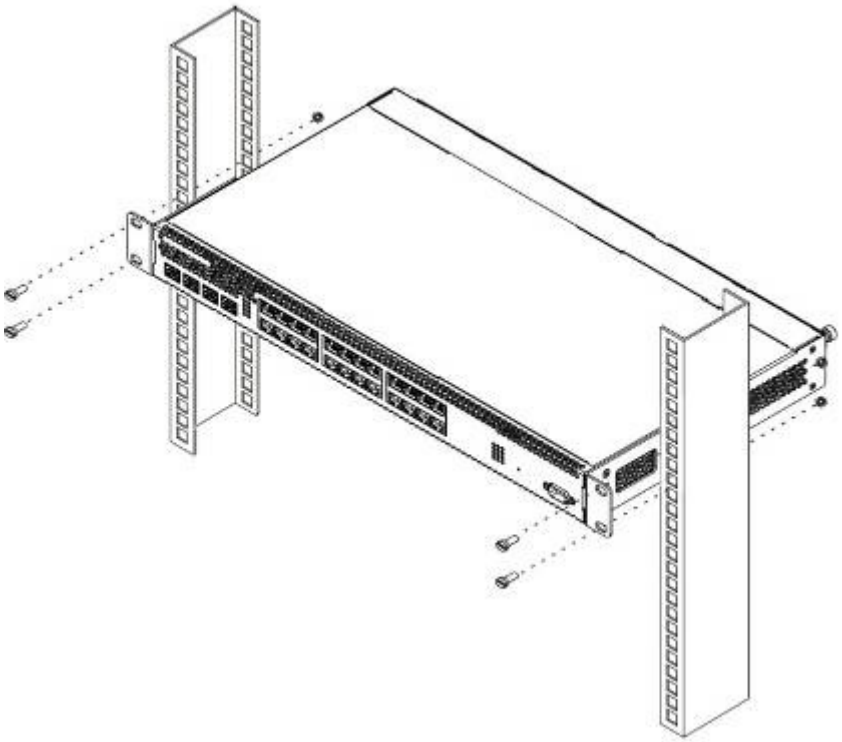

Рисунок 8 – Установка устройства в стойку

На рисунке 9 приведен пример размещения коммутаторов MES3124 в стойке.

Рисунок 9 – Размещение коммутаторов MES-3124 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.

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

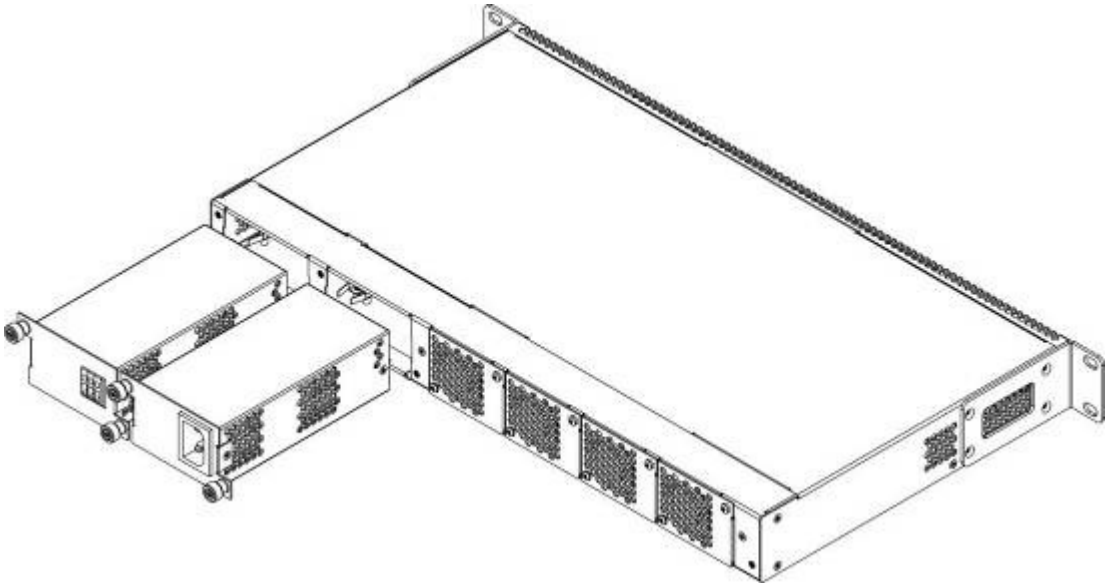

Рисунок 10 – Установка модулей питания.

Порядок установки модулей питания:

1. Установите модуль питания в основную позицию и подайте питание. Загорится зеленый индикатор *Power* на передней панели устройства. В случае аварии модуля питания и при наличии выходного напряжения 12V индикатор *Power* должен быть красным. Индикатор *RSP* должен быть погашен.
2. При наличии резервного источника питания установите модуль питания в резервную позицию. Загорится красный индикатор *RSP* на передней панели. Подайте питание на резервный источник. Цвет свечения индикатора *RSP* должен смениться на зеленый.

При пропадании первичного питания основного источника, цвет свечения индикатора *Power* должен стать желтым (есть питание, авария основного источника).

Порядок замены модулей питания:

1. Проверьте наличие напряжения на неисправном модуле.
2. В случае наличия напряжения – отключите питание и замените неисправный модуль (при наличии второго работающего источника питания устройство должно продолжить работу без перезагрузки).

3.4 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.

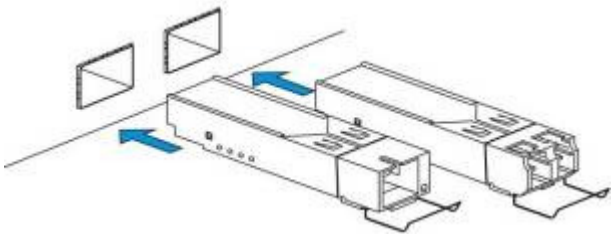

Рисунок 11– Установка SFP-трансиверов

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

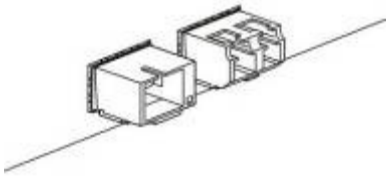

Рисунок 12– Установленные SFP-трансиверы

Для удаления трансивера:

1. Откройте защелку модуля.

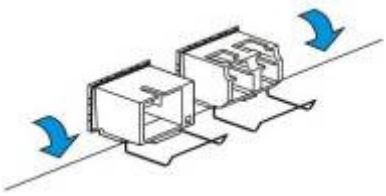

Рисунок 13– Открытие защелки SFP-трансиверов

2. Извлеките модуль из слота.

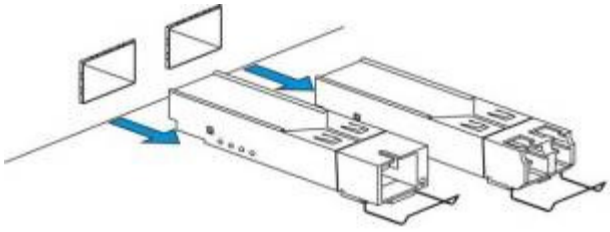

Рисунок 94– Извлечение SFP-трансиверов

3.5 Подключение питающей сети

Порядок установки устройства:

1. Смонтировать устройство. В случае установки устройства в 19” конструктив, необходимо прикрепить к нему кронштейны, входящие в комплект устройства.
2. Заземлить корпус устройства. Это необходимо выполнить прежде, чем к устройству будет подключена питающая сеть. Заземление необходимо выполнять изолированным многожильным проводом. Правила устройства заземления и сечение заземляющего провода должны соответствовать требованиями ПУЭ.
3. Если предполагается подключение компьютера или иного оборудования к консольному порту коммутатора, это оборудование также должно быть надежно заземлено.
4. Подключить к устройству кабель питания. В зависимости от прилагающихся источников, питание может осуществляться от заземленной розетки 220/110В переменного тока 50/60 Гц, либо от источника постоянного тока -48 ..-60В. При подключении сети переменного тока 220В следует использовать кабель, входящий в комплект устройства. Для подключения к сети постоянного тока использовать провод сечением не менее 1 мм^2.
5. Включить питание устройства и убедиться в отсутствии аварий по состоянию индикаторов на передней панели.

4 НАЧАЛЬНАЯ НАСТРОЙКА КОММУТАТОРА ETHERNET MES3124

4.1 Настройка терминала

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

1. Выбрать соответствующий последовательный порт.
2. Установить скорость передачи данных – 115200 бод.
3. Задать формат данных: 8бит данных, 1 стоповый бит, без контроля четности.
4. Отключить аппаратное и программное управление потоком данных.
5. Задать режим эмуляции терминала VT100 (многие терминальные программы используют данный режим эмуляции терминала в качестве режима по умолчанию).

4.2 Включение устройства

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

Включить устройство. При каждом включении коммутатора MES3124 запускается процедура «тестирования системы при включении» (POST), которая позволяет определить работоспособность устройства перед загрузкой исполняемой программы в оперативную память (ОЗУ).

Отображение хода выполнения процедуры POST на коммутаторе MES3124:

```
Boot1 Checksum Test.............................PASS
Boot2 Checksum Test.............................PASS
Flash Image Validation Test.....................PASS
BOOT Software Version 3.0.0.0 Built  16-Nov-2008  14:35:11
Networking device with 88F5181 CPU based on ARM926EJ-S core.
Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.
```

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

Пример дальнейшей загрузки устройства.

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

****************************************************************
*** Running  SW  Ver. 3.0.0.0  Date  17-Nov-2008  Time  11:51:22 ***
****************************************************************

HW version is 01.00.00
```

```
Base Mac address is: 02:00:00:01:00:00
Dram size is  : 128M bytes
Dram first block size is  : 102400K bytes
Dram first PTR is  : 0x1800000
Dram second block size is  : 4096K bytes
Dram second PTR is  : 0x7C00000
Flash size is: 16M
01-Oct-2006 01:01:15 %CDB-I-LOADCONFIG: Loading running configuration.
01-Oct-2006 01:01:15 %CDB-I-LOADCONFIG: Loading startup configuration.
Device configuration:
Slot 1 - 24-GE HW Rev. 7
CPLD revision: 1

------------------------------------
-- Unit Number1                    --
------------------------------------

01-Oct-2006 01:01:22 %Entity-I-SEND-ENT-CONF-CHANGE-TRAP: entity
configuration change trap.
01-Oct-2006 01:01:30 %INIT-I-InitCompleted: Initialization task is
completed

>
------------------------------------
-- Unit Number 1  Master Enabled --
------------------------------------

Tapi Version: v1.3.3.1
Core Version: v1.3.3.1
01-Oct-2006 01:01:58 %SNMP-I-CDBITEMSNUM: Number of running configuration
items loaded: 0
01-Oct-2006 01:01:58 %SNMP-I-CDBITEMSNUM: Number of startup configuration
items loaded: 0
>01-Oct-2006 01:01:58 %Stack-I-STCK-CFG-CHNG: Configuration changed:
chain
lcli

User Name:
```

После успешной загрузки коммутатора необходимо ввести имя пользователя. Далее появится системное приглашение интерфейса командной строки CLI .

```
console#
```

Имя пользователя по умолчанию – admin, пароль по умолчанию - admin. Уровень привилегий данного пользователя – 15 (администратор).

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

4.3 Загрузочное меню

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

```
Boot1 Checksum Test.............................PASS
Boot2 Checksum Test.............................PASS
Flash Image Validation Test.....................PASS
BOOT Software Version 3.0.0.0 Built  16-Nov-2008  14:35:11
Networking device with 88F5181 CPU based on ARM926EJ-S core.
Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.
```

Вид загрузочного меню:

```
           Startup Menu

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

Таблица 4.1. – Функции интерфейса загрузочного меню

Функция	***Описание***
Download Software	Загрузить новую версию программного обеспечения коммутатора, используя XMODEM
Erase Flash File	Стереть информацию с Flash
Password Recovery Procedure	Сбросить настройки аутентификации
Set Terminal Baud-Rate	Установить скорость работы терминального режима
Stack Menu	Вход в меню управления стеком
Back	Продолжить загрузку

4.4 Режимы работы коммутатора

Устройство может работать в двух режимах – автономном и режиме стекирования. В режиме стекирования несколько MES3124 могут быть объединены в стек и функционировать как единое устройство. По умолчанию MES3124 работает в режиме стекирования.

4.4.1 Выбор режима работы коммутатора

Выбор режима работы коммутатора доступен в меню управления стеком (пункт [6] загрузочного меню):

```
          Startup Menu

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

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

```
     Stack menu

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

4.4.2 Работа коммутатора в режиме стекирования

Стек MES3124 функционирует как единое устройство и может состоять из 8 устройств, имеющих следующие роли, определяемые их порядковыми номерами (UID):

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

Устройства с одинаковыми UID не могут работать в одном и том же стеке.

4.5 Настройка функций коммутатора

Функции по начальному конфигурированию устройства можно разделить на два типа.

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

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
```

4.5.1 Базовая настройка коммутатора

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

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

Базовая настройка включает следующее:

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

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> level <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 level 1
console (config) # exit
console#
```

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

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

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

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

Параметры интерфейса:

IP-адрес, назначаемый для интерфейса VLAN 1 – 192.168.16.144
Маска подсети – 255.255.255.0
IP-адрес шлюза по умолчанию - 192.168.16.1

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

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

```
console# show ip interface vlan 1


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


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

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 Ethernet 10:

```
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 vlan 1
```

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

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

Настройка параметров протокола SNMP для доступа к устройству

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. Коммутатор MES3124/MES3124F поддерживает 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 enable
console(config)# snmp-server community private rw 192.168.16.44
console (config)# exit
console#
```

Для просмотра созданных строк сообщества и настроек SNMP используется команда:

```
console# show snmp
```

```
SNMP is enabled.


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

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

```
Traps are enabled.
Authentication-failure trap is enabled.

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

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

System Contact:
System Location:
```

4.5.2 Настройка параметров системы безопасности

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

Authentication (аутентификация) — сопоставление запроса существующей учётной записи в системе безопасности.

Authorization (авторизация, проверка уровня доступа) — сопоставление учётной записи в системе (прошедшей аутентификацию) и определённых полномочий.

Accounting (учёт) — слежение за потреблением ресурсов пользователем.

При использовании настроек устройства по умолчанию имя пользователя – ***admin***, пароль не задан. Пароль назначается пользователем. В случае если пароль утрачен, можно перезагрузить устройство и через серийный порт прервать загрузку, нажав клавишу ***<Esc>*** или ***<Enter>*** в течение первых двух секунд после появления сообщения автозагрузки. Откроется меню ***Startup***, в котором нужно запустить процедуру восстановления пароля ([3] Password Recovery Procedure).

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

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

Установка пароля для консоли

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

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

Установка пароля для Telnet

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

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

Установка пароля для SSH

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

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

4.5.3 Настройка баннера

Для удобства эксплуатации устройства можно задать баннер – сообщение, которое будет выводиться при попытке получения доступа к устройству.

```
console(config)# banner motd ;

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

5 НАСТРОЙКА КОММУТАТОРА MES3124

Для конфигурирования настроек коммутатора используется четыре основных режима. В каждом режиме доступен определенный список команд.

Режимы и команды входа в режим.

- *Командный (EXEC),* данный режим доступен сразу после успешной загрузки коммутатора и ввода имени пользователя.

```
console#
```

- *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)#
```

- *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)
```

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

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

5.1 Базовые команды для работы с коммутатором MES3124

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console#
```

Таблица 5.1 – Базовые команды доступные в режиме EXEC

Команда	***Значение/ значение по умолчанию***	***Действие***
enable [*priv***]**	[1..15]/15	Переключиться в привилегированный режим (если значение не указано – то уровень привилегий 15).
disable [*priv***]**	[1..15]/1	Вернуться в нормальный режим из привилегированного (если значение не указано – то уровень привилегий 1).
login	-	Сменить пользователя.
configure	-	Перейти в режим конфигурирования.

exit (EXEC)	-	Закрыть активную терминальную сессию.
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***}**	{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.
debug-mode	-	Перейти в режим отладки (команда доступна только для привилегированного пользователя).
show history	-	Показать историю команд, введенных в текущей терминальной сессии.
show privilege	-	Показать уровень привилегий текущего пользователя.

Команды, доступные во всех режимах конфигурирования

Запрос командной строки имеет один из следующих видов:

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

Таблица 5.2 – Базовые команды доступные в любом режиме конфигурирования

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

Команды доступные в режиме конфигурирования терминала

Запрос командной строки в режиме конфигурирования терминала имеет следующий вид:

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

Таблица 5.3 – 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.

5.2 Команды управления системой

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console#
```

Таблица 5.4 – Команды управления системой в режиме EXEC

Команда	*Значение/ Значение по умолчанию*	*Действие*
ping {A.B.C.D|*host*} [**size** *size*] [**count** *count*] [**timeout** *timeout*]	host {1..158} символов; size [56..1472]/56 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 [56..1452]/56 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 {A.B.C.D |*host*} [**size** *size*] [**ttl** *ttl*] [**count** *count*] [**timeout** *timeout*] [**source** *ip-address*] [**tos** *tos*]	host {1..158} символов; size [40..1500]/40 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 MES3124 используемый для передачи пакетов; - tos – тип сервиса, передаваемый в заголовке протокола IP. ***Описание ошибок при выполнении команд и результатов приведено в таблицах 5.5, 5.6***
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 [40..1500]/40 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 MES3124, используемый для передачи пакетов; - tos – тип сервиса, передаваемый в заголовке протокола IP. ***Описание ошибок при выполнении команд и результатов приведено в таблицах 5.5, 5.6***
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 5.7, 5.8
resume [*connection*]	[1..4]/последняя установленная сессия	Переключение на другую установленную TELNET-сессию. - connection – номер установленной telnet-сессии.
reload	-	Команда служит для перезапуска устройства (команда доступна только для привилегированного пользователя).
stack reload [*unit*]	[1..8]/все устройства в стеке	Перезапуск всех или отдельного устройства из стека устройств (команда доступна только для привилегированного пользователя).
show stack [**unit** *unit*]	[1..8]/все устройства в стеке	Отображение информации по одному или всем устройствам в стеке. ***Данная команда доступна только в режиме стекирования.***
show cpu utilization	-	Отображение статистики по уровню загрузки ресурсов центрального процессора (команда доступна только для привилегированного пользователя).
clear counters [ethernet {*port***} | port-channel {***group***}]**	port: {1/g(1-48).. 8/g(1-48), g1..g24}; group {1..8}	Обнуление счётчиков устройства для указанного порта или группы портов.
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.***
set system mode [**router**|**switch**] **policy-based-vlans** {**active**|**inactive**} **qos {active | inactive}**	-	Установка режима работы для устройства (коммутатор, маршрутизатор). Команда доступна только для привилегированного пользователя. - mode – режим работы: router – маршрутизатор; switch – коммутатор. - policy – активация/деактивация правил использования VLAN: active – активация; inactive – деактивация.
show system mode	-	Отображение информации о текущем режиме работы устройства.
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 system id [unit unit**]**	[1..8]/-	Отображение информации системной идентификации устройства. - unit – номер устройства в стеке (для коммутатора, работающего в автономном режиме, параметр не используется). ***Параметр [unit unit] при выполнении команды доступен только в режиме стекирования***
show system defaults [{management|ipv6|802.1x|port|fdb|multicast|port-mirroring|spanning-tree|vlan|voice-vlan|network-security}]	-	Отображение заводских настроек устройства

show tech-support [{config|memory}]	-	Отображение системной информации. Если выбрана опция **config –** будет отображена информация о настройках устройства с помощью команд CLI Если выбрана опция **memory –** будет отображена информация о состоянии памяти и регистров процессора
show system flowcontrol	-	Отображение конфигурации системы для управления потоком передачи данных

- Пример использования команды **traceroute**:

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

```
Type Esc to abort.
Tracing the route to eltex.com (148.21.11.69)
   1 gateway.eltex (192.168.1.101)  0 msec 0 msec 0 msec
   2 eltexsrv (192.168.0.1) 0 msec 0 msec 0 msec
   3 * * *
```

Таблица 5.5 – 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 5.6

Таблица 5.6 – 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 коммутатора MES3124/MES3124F поддерживает специальные команды – функции контроля терминала. Для входа в режим специальных команд во время активной Telnet-сессии используется комбинация клавиш Ctrl-shift-6.

Таблица 5.7 – 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 удаление линии (EL).
^^ x	Возврат в режим командной строки.

Также возможно использование дополнительных опций при открытии Telnet-сессии:

Таблица 5.8 – 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 5.9 – Команды управления системой в режиме глобального конфигурирования

Команда	***Значение/ Значение по умолчанию***	***Действие***
hostname *name*	1..158 символов/-	Команда служит для задания сетевого имени устройства.
no hostname		Вернуть сетевое имя устройства в значение по умолчанию.
stack master unit *unit*	1..2/ нет ведущего устройства	Назначение ведущего устройства в стеке. Данная команда доступна только в режиме стекирования.
no stack master unit		Установить значение по умолчанию.
stack change unit-id *unit-number* **to** *new-unit-number*	unit-number 1..8; new-unit-number 1..8	Изменение порядкового номера устройства в стеке. Данная команда доступна только в режиме стекирования.
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.

5.3 Команды для настройки параметров для задания паролей

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

Команды доступные в режиме глобального конфигурирования:

Запрос командной строки в режиме глобального конфигурирования имеет следующий вид:

```
console(config)#
```

Таблица 5.10 – Команды управления системой в режиме глобального конфигурирования

Команда	*Значение/ Значение по умолчанию*	*Действие*
passwords aging <age>	0-365/0 дней	Задает время жизни паролей. По истечению заданного срока будет предложено сменить пароль. Значение 0 говорит о том, что время жизни паролей не задано
no password aging		Восстанавливает значение по умолчанию
passwords complexity enable	-/disabled	Включает ограничение на формат пароля
passwords complexity min-classes <value>	0..4/3	Включает ограничение, задающее минимальное количество классов символов (строчные буквы, заглавные буквы, цифры, символы)
no passwords complexity min-classes		Восстанавливает значение по умолчанию
passwords complexity min-length <value>	0..64/8	Включает ограничение на минимальную длину пароля.
no passwords complexity min-length		Восстанавливает значение по умолчанию
passwords complexity not-manufacturer-name	-/enabled	Запрещает использовать в качестве паролей системные имена (admin)
no passwords complexity not-manufacturer-name		Разрешает использовать в качестве паролей системные имена
passwords complexity not-current	-/enabled	Запрещает при смене пароля использовать в качестве нового старый
no passwords complexity not-current		Разрешает использовать старый пароль при смене
passwords complexity not-username	-/enabled	Запрещает использовать в качестве пароля имя пользователя
no passwords complexity not-username		Разрешает использовать в качестве пароля имя пользователя

Таблица 5.11 – Команды управления системой в режиме EXEC

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

5.4 Работа с файлами

5.4.1 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 5.12.

Таблица 5.12 – 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.

5.4.2 Команды для работы с файлами

Команды для работы с файлами доступны только привилегированному пользователю.

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console#
```

Таблица 5.13 – Команды для работы с файлами в режиме EXEC

Команда	*Значение*	*Действие*
copy source-url destination-url **[snmp]**	source-url: 1..160 символов;	Копирование файла из местоположения источника в местоположение назначения. - snmp – используется только когда копирование

	destination-url: 1..160 символов;	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..152 символов	Отображает содержимое файла
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**

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

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

Таблица 5.14 - Описание признаков копирования

Признак	*Описание*
!	Восклицательный знак означает, что процесс копирования идет успешно. Каждый восклицательный знак указывает на успешную передачу десяти пакетов (512 байтов каждый).
.	Точка означает, что процесс копирования прерван. Несколько точек подряд означает, что в процессе копирования возникла ошибка.

Примеры использования команд.

Удалить файл *test* из энергонезависимой памяти:

```
console# delete flash:test

Delete flash:test? [confirm]
```

Результат выполнения команды: после подтверждения файл будет удален.

5.5 Настройка системного времени

Автоматический переход на летнее время осуществляется в соответствии со стандартами США и Европы, также возможно переключение на летнее время для указанного периода.

Команды режима EXEC

Запрос командной строки в режиме «EXEC» имеет следующий вид:

```
console#
```

Таблица 5.15 - 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.
clock set hh:mm:ss date month year **clock set** hh:mm:ss month date year	hh 0..23, mm 0..59, ss 0..59, date 1..31; month Jan..Dec; year 1998 – 2097	Ручная установка системного времени (команда доступна только для привилегированного пользователя). - hh – часы, mm – минуты, ss – секунды; - date – число; - month – месяц; - year – год.

show sntp configuration	-	Показывает конфигурацию протокола SNTP (команда доступна только для привилегированного пользователя).
show sntp status	-	Показывает статус протокола SNTP (команда доступна только для привилегированного пользователя).

Команды доступные в режиме глобального конфигурирования

Запрос командной строки в режиме глобального конфигурирования имеет следующий вид:

```
console(config)#
```

Таблица 5.16 – 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 *hours-offset* **[minutes** *minutes-offset***] [zone** *acronym***]**	hours-offset -12..+13/0; minutes-offset [0..59]/0; acronym [1..4] символа/ нет описания зоны	Устанавливает значение часового пояса. - hours-offset – часовое смещение относительно нулевого меридиана UTC; - minutes-offset – минутное смещение относительно нулевого меридиана UTC; - acronym –слово, сформированное из первых букв словосочетания, которое оно заменяет (описание зоны).
no clock timezone		Устанавливает значение по умолчанию.
clock summer-time date *date month year hh:mm date month year hh:mm* **[offset** *offset***] [zone** *acronym***]**	week 1..4, first, last; day mon..sun; date 1..31; month Jan..Dec; year 1998 – 2097; hh 0..23, mm 0..59; offset [1..1440]/60 мин; acronym [1..4] символа/ нет описания зоны 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 время для перехода на летнее время, вторым время для возврата. - hh – часы, mm – минуты; - date – число; - month – месяц; - year – год; - offset – количество минут, добавляемых при переходе на летнее время; - acronym – слово, сформированное из первых букв словосочетания, которое оно заменяет (описание зоны).
clock summer-time date *month date year hh:mm month date year hh:mm* **[offset** *offset***] [zone** *acronym***]**		
clock summer-time recurring {usa|eu| {*week day month hh:mm week day month hh:mm***}} [offset** *offset***] [zone** *acronym***]**		Задает дату и время для автоматического перехода на летнее время и возврата обратно в режиме ежегодно. - 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; - acronym –слово, сформированное из первых букв словосочетания, которое оно заменяет (описание зоны).
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 {ethernet *interface-number* **| vlan** *vlan-id* **| port-channel** *number***}**	-/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 {ethernet *interface-number* **| vlan** *vlan-id* **| port-channel** *number***}**		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 {A.B.C.D / A.B.C.D.E.F / *hostname***}** **[poll]** **[key** *keyid***]**	hostname 1..158 символов; keyid 1..4294967295	Задает адрес SNTP-сервера. - A.B.C.D - Ipv4-адрес узла сети; - A.B.C.D.E.F - Ipv6-адрес узла сети; - hostname – доменное имя узла сети; - poll – включает опрос; - keyid – идентификатор ключа.
no sntp server {*ipv4-address* **|** *ipv6-address* **|** *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.

Команды режима конфигурирования интерфейса

Запрос командной строки в режиме конфигурирования интерфейса имеет следующий вид:

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

Таблица 5.17 – Список команд для настройки системного времени в режиме конфигурирования интерфейса

Команда	*Значение/Значение по умолчанию*	*Действие*
sntp client enable (interface)	-/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.
no sntp client enable (interface)		Устанавливает значение по умолчанию.

Примеры выполнения команд.

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

```
console# show clock detail
15:29:08 PDT(UTC-7) Jun 17 2009
 Time source is SNTP

Time zone:
Acronym is PST
Offset is UTC-8

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

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

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

- Отобразить статус протокола SNTP:

```
console# show sntp status
Clock is synchronized, stratum 0, reference is 192.168.16.1, unicast
Reference time is cec866d5.8a20cccb 05:47:01.0 UTC Dec 8 2009

Unicast servers:

    Server       Status      Last Response     Offset   Delay
                                                [mSec]   [mSec]
--------------- --------- ------------------- --------- -------
 192.168.16.1      up     05:47:01.0 UTC Dec     7230  -1000
                          8 2009

Anycast server:

    Server      Interface  Status        Last Response        Offset   Delay
                                                              [mSec]   [mSe
--------------- --------- --------- ---------------------- --------- -------
Broadcast:

 Interface     IP address         Last Response
```

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

5.6 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: gN, где N – номер интерфейса; при работе в составе стека запись для интерфейса имеет вид: K/gN, 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.

5.6.1 Параметры Ethernet-интерфейсов и интерфейсов Port-Channel

Команды режима конфигурирования интерфейса (диапазона интерфейсов)

```
console# configure
console(config)# interface {ethernet {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 ethernet {**port**}** – для настройки Ethernet-интерфейса;
- **interface port-channel {**group**}** – для настройки группы каналов.

Команды, введенные в данном режиме, 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 ethernet 1/g10
console(config-if)#
console# configure
console(config)# interface port-channel 1
console(config-if)#
```

Выбор диапазона интерфейсов осуществляется при помощи команд:

- **interface range ethernet {**portlist|all**}** - для настройки диапазона интерфейсов;
- **interface range port-channel {**grouplist|all**}**. – 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 ethernet 1/g(1-10)
console(config-if)#

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

Таблица 5.18 – Команды режима конфигурирования интерфейса Ethernet и Port-Channel

Команда	*Значение/значение по умолчанию*	*Действие*
shutdown	-/включен	Выключить конфигурируемый интерфейс (Ethernet, port-channel).
no shutdown		Включить конфигурируемый интерфейс.
description {*descr***}**	{WORD 1-64}/ нет описания	Добавить описание интерфейса (Ethernet, port-channel).
no description		Удалить описание интерфейса.
speed {*mode***}**	{10, 100, 1000, 10000}	Задать скорость передачи данных (Ethernet, port-channel). ***Для портов xg(1-4) возможно переключение скорости (1000-10000)***
no speed		Установить значение по умолчанию.
duplex {*mode***}**	{full, half}/ full	Задать режим дуплекса интерфейса (полнодуплексное соединение, полудуплексное соединение, Ethernet). ***Данная команда недоступна для портов xg(1-4)***
no duplex		Установить значение по умолчанию.
negotiation*[cap1 [cap2… cap5]]*	[10f, 10h, 100f, 100h, 1000f]	Включает автосогласование для скорости и дуплекса на настраиваемом интерфейсе. Можно указать определенные совместимости параметра автосогласования, если параметры не заданы, то поддерживаются все совместимости (Ethernet, port-channel). ***Данная команда недоступна для портов xg(1-4)***
no negotiation		Выключает автосогласование для скорости и дуплекса на настраиваемом интерфейсе.
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.
mdix {*mode***}**	{on, auto}	Позволяет использование «перекрещенного» кабеля на настраиваемом интерфейсе (Ethernet). ***Данная команда недоступна для портов xg(1-4)***
no mdix		Запрещает использование «перекрещенного» кабеля на настраиваемом интерфейсе.
back-pressure	-/выключен	Включает функцию «обратного давления» на настраиваемом интерфейсе (Ethernet).
no back-pressure		Выключает функцию «обратного давления» на настраиваемом интерфейсе.

Команды режима глобального конфигурирования

Вид запроса командной строки в режиме конфигурирования интерфейса:

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

Таблица 5.19– Команды режима общих настроек интерфейса 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.

Команды режима EXEC

Вид запроса командной строки в режиме EXEC:

```
console#
```

Таблица 5.20 – Команды режима EXEC

Команда	*Значение*	*Действие*
clear counters	-	Сброс статистики для всех интерфейсов.
clear counters ethernet {*port***}**	{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}	Сброс статистики для Ethernet-порта.
clear counters port-channel {*group***}**	{1..8}	Сброс статистики для группы портов.
set interface active ethernet {*port***}**	{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}	Активирует порт, выключенный командой **shutdown**.
set interface active port-channel {*group***}**	{1..8}	Активирует группу портов, выключенную командой **shutdown**.
show interfaces status	-	Показать состояние всех интерфейсов.
show interfaces status ethernet {*port***}**	{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}	Показать состояние Ethernet-порта.
show interfaces status port-channel {*group***}**	{1..8}	Показать состояние группы портов.
show interfaces advertise	-	Показать параметры автосогласования, объявленные для всех интерфейсов.
show interfaces advertise ethernet {*port***}**	{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}	Показать параметры автосогласования, объявленные для Ethernet-порта.
show interfaces advertise port-channel {*group***}**	{1..8}	Показать параметры автосогласования, объявленные для группы портов.
show interfaces description	-	Показать описания всех интерфейсов.
show interfaces description ethernet {*port***}**	{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}	Показать описание Ethernet-порта.

show interfaces description port-channel {*group*}	{1..8}	Показать описание группы портов.
show interfaces counters	-	Показать статистику для всех интерфейсов.
show interfaces counters ethernet {*port*}	{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}	Показать статистику для Ethernet-порта.
show interfaces counters port-channel {*group*}	{1..8}	Показать статистику для группы портов.
show ports jumbo-frame	-	Показать настройку jumbo-frames в коммутаторе.

Примеры выполнения команд.

- Показать состояние интерфейсов:

```
console# show interfaces status
```

```
                                                Flow Link          Back   Mdix
Port     Type         Duplex  Speed Neg      ctrl State       Pressure Mode
-------- ------------ ------  ----- -------- ---- ----------- -------- -------
g1       1G-Copper      --      --     --     --  Down           --     --
g2       1G-Copper      --      --     --     --  Down           --     --
g3       1G-Copper      --      --     --     --  Down           --     --
g4       1G-Copper      --      --     --     --  Down           --     --
g5       1G-Copper      --      --     --     --  Down           --     --
g6       1G-Copper      --      --     --     --  Down           --     --
g7       1G-Copper      --      --     --     --  Down           --     --
g8       1G-Copper      --      --     --     --  Down           --     --
g9       1G-Copper      --      --     --     --  Down           --     --
g10      1G-Copper      --      --     --     --  Down           --     --
g11      1G-Copper      --      --     --     --  Down           --     --
g12      1G-Copper      --      --     --     --  Down           --     --
g13      1G-Copper      --      --     --     --  Down           --     --
g14      1G-Copper      --      --     --     --  Down           --     --
g15      1G-Copper      --      --     --     --  Down           --     --
g16      1G-Copper      --      --     --     --  Down           --     --
g17      1G-Copper      --      --     --     --  Down           --     --
g18      1G-Copper      --      --     --     --  Down           --     --
g19      1G-Copper      --      --     --     --  Down           --     --
g20      1G-Copper      --      --     --     --  Down           --     --
g21      1G-Copper      --      --     --     --  Down           --     --
g22      1G-Copper      --      --     --     --  Down           --     --
g23      1G-Copper      --      --     --     --  Down           --     --
g24      1G-Copper    Full    1000  Enabled  Off  Up         Disabled On
xg1      10G-Fiber      --      --     --     --  Down           --     --
xg2      10G-Fiber      --      --     --     --  Down           --     --
xg3      10G-Fiber      --      --     --     --  Down           --     --
xg4      10G-Fiber      --      --     --     --  Down           --     --

                                             Flow    Link
Ch       Type    Duplex  Speed  Neg      control  State
-------- ------- ------  -----  -------- -------  -----------
ch1        --      --      --      --       --    Not Present
ch2        --      --      --      --       --    Not Present
ch3        --      --      --      --       --    Not Present
ch4        --      --      --      --       --    Not Present
ch5        --      --      --      --       --    Not Present
ch6        --      --      --      --       --    Not Present
ch7        --      --      --      --       --    Not Present
ch8        --      --      --      --       --    Not Present
```

- Показать параметры авто-согласования:

```
console# show interfaces advertise
```

```
Port      Type         Neg      Operational Link Advertisement
--------- ------------ -------- ----------------------------------
g1        1G-Copper    Enabled                  --
g2        1G-Copper    Enabled                  --
g3        1G-Copper    Enabled                  --
g4        1G-Copper    Enabled                  --
g5        1G-Copper    Enabled                  --
g6        1G-Copper    Enabled                  --
g7        1G-Copper    Enabled                  --
g8        1G-Copper    Enabled                  --
g9        1G-Copper    Enabled                  --
g10       1G-Copper    Enabled                  --
g11       1G-Copper    Enabled                  --
g12       1G-Copper    Enabled                  --
g13       1G-Copper    Enabled                  --
g14       1G-Copper    Enabled                  --
g15       1G-Copper    Enabled                  --
g16       1G-Copper    Enabled                  --
g17       1G-Copper    Enabled                  --
g18       1G-Copper    Enabled                  --
g19       1G-Copper    Enabled                  --
g20       1G-Copper    Enabled                  --
g21       1G-Copper    Enabled                  --
g22       1G-Copper    Enabled                  --
g23       1G-Copper    Enabled                  --
g24       1G-Copper    Enabled  1000f, 100f, 100h, 10f, 10h
xg1       10G-Fiber    Disabled                 --
xg2       10G-Fiber    Disabled                 --
xg3       10G-Fiber    Disabled                 --
xg4       10G-Fiber    Disabled                 --

Ch        Type         Neg      Operational Link Advertisement
--------- ------------ -------- ----------------------------------
ch1            --      Enabled                  --
ch2            --      Enabled                  --
ch3            --      Enabled                  --
ch4            --      Enabled                  --
ch5            --      Enabled                  --
ch6            --      Enabled                  --
ch7            --      Enabled                  --
ch8            --      Enabled                  --
```

- Показать статистику по интерфейсам:

```
console# show interfaces counters
```

```
      Port       InUcastPkts  InMcastPkts  InBcastPkts    InOctets
---------------- ------------ ------------ ------------ ------------
      1/g1             0            0            0            0
      1/g2             0            0            1          247
      1/g3             0            0            0            0
      1/g4             0            0            0            0
      1/g5             0            0            0            0
      1/g6             0            0            0            0
      1/g7             0            0            0            0
      1/g8             0            0            0            0
      1/g9             0            0            0            0
     1/g10             0            0            0            0
     1/g11             0            0            0            0
     1/g12             0            0            0            0
     1/g13             0            0            0            0
     1/g14             0            0            0            0
     1/g15             0            0            0            0
     1/g16             0            0            0            0
```

```
     1/g17            0            0            0            0
     1/g18            0            0            0            0
     1/g19            0            0            0            0
     1/g20            0            0            0            0
More: <space>,  Quit: q, One line: <return>
```

- Показать статистику по группе каналов 1:

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

console# sho int counters port-channel 1
```

```
       Ch        InUcastPkts  InMcastPkts  InBcastPkts    InOctets
---------------- ------------ ------------ ------------ ------------
      ch1              0            14           123          17913


       Ch        OutUcastPkts OuPkts       OutBcastPkt  OutOctets
---------------- ------------ ------------ ------------ ------------
      ch1              0            78           21           9810


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
```

Таблица 5.21 - 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.

- Показать настройку jumbo-frames в коммутаторе:

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

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

5.6.2 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 5.22 – Команды режима конфигурирования VLAN

Команда	*Значение/значение по умолчанию*	*Действие*
vlan {*vlan range***}**	{1..4094}	Добавить VLAN, или несколько VLAN.
no vlan {*vlan range***}**	-	Удалить VLAN, или несколько VLAN.
default vlan vlan {*vlan id***}**	{1..4094}/1	Определить VLAN по умолчанию.
no default vlan vlan		Установить значение по умолчанию.
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. ***Данная команда доступна только в режиме коммутатора (set system mode switch policy-based vlan active)***
no map protocol {*protocol***} [***encaps***]**		Удалить привязку. * - номер протокола (16 бит).
map subnet {*ip-address***} {***mask***} subnets-group {***group***}**	ip-address {A.B.C.D} mask {1..32} group {1.. 2147483647}	Привязать IP–адрес подсети к группе подсетей ***Данная команда доступна только в режиме коммутатора (set system mode switch policy-based vlan active)***
no map subnet {*ip-address***} {***mask***}**		Удалить привязку[1].

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|all}}
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|all}`.

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)#
```

[1] В данной версии программного обеспечения не поддерживается

Таблица 5.23 – Команды режима конфигурирования интерфейса VLAN

Команда	*Значение/значение по умолчанию*	*Действие*
name *{name}*	{WORD 1-64}/ 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 {ethernet {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 5.24 – 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***}**	{1..4094}/1	Добавить VLAN для интерфейса доступа.
no switchport access vlan		Установить значение по умолчанию.
switchport trunk allowed vlan add {*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***}**	{1..4094}/ 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***} [***tag***]**	VLANlist {2..4094, all} tag [tagged, untagged] / tagged	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***}**	{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	-/принимать все типы фреймов	Принимать на основном интерфейсе только тегированные фреймы.
no switchport general acceptable-frame-type tagged-only		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. ***Данная команда доступна только в режиме коммутатора (set system mode switch policy-based vlan active)***
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. ***Данная команда доступна только в режиме коммутатора (set system mode switch policy-based vlan active)***
no switchport general map subnets-group {*group***}**		Удалить правило классификации
switchport customer vlan {*VLAN ID***}**	{1..4094}/1	Добавить VLAN для пользовательского интерфейса.
no switchport customer vlan		Установить значение по умолчанию.
switchport customer multicast-tv vlan {*VLAN ID***}**	{1..4094}	Разрешает принимать многоадресный трафик из указанной VLAN (не являющейся VLAN пользовательского интерфейса) на настраиваемом интерфейсе, совместно с пользователями других пользовательских портов, принимающих многоадресный трафик из данной VLAN.
no switchport customer multicast-tv vlan		Запрещает принимать многоадресный трафик на настраиваемом интерфейсе.
switchport forbidden vlan add {*VLANlist***}**	{2..4094, all}/ все VLAN разрешены порту	Запретить добавление указанных VLAN порту.
switchport forbidden vlan remove {*VLANlist***}**		Разрешить добавление указанных VLAN порту.
switchport protected-port	-	Переводит порт в режим Private VLAN Edge – изоляцию внутри группы портов.
no switchport-protected-port		Восстанавливает значение по умолчанию.
switchport community	-	Добавляет порт в private-vlan-edge-сообщество. Порты одного сообщества не могут обмениваться трафиком между собой.
no switchport community		Восстанавливает значение по умолчанию
switchport protected ethernet {*port***}** **switchport protected port-channel {***group***}**	Port {1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24};	Отменяет маршрутизацию по базе данных изученных MAC-адресов (FDB) и направляет весь одноадресный, многоадресный и широковещательный трафик на uplink-порт.

no switchport protected	group {1..8} По умолчанию используется маршрутизация по базе данных изученных MAC-адресов (FDB)	Отключает отмену маршрутизации по базе данных изученных MAC-адресов (FDB).
ip internal-usage-vlan {*VLAN ID***}**	{1..4094}/ нет резерва	Зарезервировать VLAN для внутреннего использования на интерфейсе.
no ip internal-usage-vlan		Установить значение по умолчанию.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

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

Таблица 5.25 – 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 EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.26 – Команды режима EXEC

Команда	*Значение*	*Действие*
show vlan	-	Показать информацию по всем VLAN.
show vlan name {*name***}**	{WORD 1..32}	Показать информацию по VLAN, поиск по имени.
show vlan tag {*VLAN ID***}**	{1..4094}	Показать информацию по VLAN, поиск по идентификатору.
show vlan multicast-tv vlan {*VLAN ID***}**	{1..4094}	Показать порты-источники и приемники многоадресного трафика в данной VLAN. Порты источники могут, как передавать, так и принимать многоадресный трафик.
show vlan protocols-groups	-	Показать информацию о группах протоколов.
show vlan subnets-groups	-	Показать информацию о группах подсетей.
show vlan internal usage	-	Показать список VLAN для внутреннего использования коммутатором.
show interfaces switchport ethernet {*port***}**	{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}	Показать конфигурацию порта.
show interfaces switchport port-channel {*group***}**	{1..8}	Показать конфигурацию группы портов.

Примеры выполнения команд

- Показать информацию о всех VLAN:

```
console# show vlan
```

```
Vlan       Name                    Ports                Type
Authorization
---- ----------------- -------------------------- ------------ ---------
----
 1           1         1/g(1-48),2/g(1-48),           other
Required
                       3/g(1-48),4/g(1-48),
                       5/g(1-48),6/g(1-48),
                       7/g(1-4g(1-48),ch(1-8)
 4           4                                    permanent
Required
```

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

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

```
Source ports  : 1/g1
Receiver ports: 1/g(2,4,8)
```

- Показать информацию о группах протоколов:

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

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

- Показать информацию о группах подсетей:

```
console# show vlan subnets-groups
```

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

- Показать список VLAN для внутреннего использования коммутатором:

```
console# show vlan internal usage
```

```
Usage   VLAN   Reserved   IP address
------ ------ ---------- ------------
1/g22    9       Yes       Inactive
```

- Показать конфигурацию порта Ethernet 22:

```
console# show interfaces switchport ethernet 1/g22
```

```
Port : 1/g22
Port Mode: Access
Gvrp Status: disabled
```

```
Ingress Filtering: true
Acceptable Frame Type: admitAll
Ingress UnTagged VLAN ( NATIVE ): 1
Protected: Disabled

Port is member in:

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

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

Classification rules:

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

5.7 Selective Q-in-Q.

Позволяет назначать внешний VLAN SPVLAN (Service Provider's VLAN) на основе сконфигурированных правил фильтрации по номерам внутренних VLAN (Customer VLAN). Применение Selective Q-in-Q позволяет разобрать трафик абонента на несколько VLAN, изменить метку SPVLAN у пакета в отдельном участке сети.

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

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

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

Таблица 5.27 – Команды режима глобального конфигурирования

Команда	***Значение***	***Действие***
selective-qinq list ingress add_vlan {*VLAN ID***} [ingress_vlan** *Outer Vlan ID***] priority {***priority***}**	VLAN ID {1..4094} Outer Vlan ID [1..4094] priority {1-100}	Создает правило, на основании которого к внешней метке Outer Vlan ID входящего пакета будет добавляться VLAN ID. Если ingress_vlan не указывать – правило будет применяться ко всем входящим пакетам.
selective-qinq list ingress deny [ingress_vlan *Outer Vlan ID***] priority {***priority***}**	Outer Vlan ID [1..4094] priority {1-100}	Создает запрещающее правило, на основании которого входящие пакеты с внешней меткой тега Outer Vlan ID будут отбрасываться. Если ingress_vlan не указывается – будут отбрасываться все входящие пакеты.
selective-qinq list ingress permit [ingress_vlan *Outer Vlan ID***] priority {***priority***}**	Outer Vlan ID [1..4094] priority {1-100}	Создает разрешающее правило, на основании которого входящие пакеты с внешней меткой тега Outer Vlan ID будут передаваться без изменений. Если ingress_vlan не указывается – будут передаваться все входящие пакеты без изменений.
selective-qinq list ingress override_vlan {*VLAN ID***} [ingress_vlan** *Outer Vlan ID***] priority {***priority***}**	VLAN ID {1..4094} Outer Vlan ID [1..4094] priority {1-100}	Создает правило, на основании которого внешняя метка входящего пакета Outer Vlan ID будет заменяться на VLAN ID. Если Outer Vlan ID не указывать – правило будет применяться ко всем входящим пакетам.

selective-qinq list egress override_vlan {*VLAN ID***} [ingress_vlan** *Outer Vlan ID***] priority {***priority***}**	VLAN ID {1..4094} Outer Vlan ID [1..4094] priority {1-28}	Создает правило, на основании которого внешняя метка исходящего пакета Outer Vlan ID бует заменяться на VLAN ID. Если ingress_vlan не указывать – правило будет применяться ко всем исходящим пакетам.
no selective-qinq list ingress [priority *priority***]**	priority [1-100]	Удаляет список правил selective qinq для входящих пакетов
no selective-qinq list egress [priority *priority***]**	priority [1-28]	Удаляет список правил selective qinq для исходящих пакетов

Команды режима EXEC

Вид запроса командной строки режима EXEC:

console#

Таблица 5.28 – Команды режима EXEC

Команда	***Значение***	***Действие***
show selective-qinq	-	Отображает список правил selective qinq

Примеры выполнения команд.

- Создать правило, на основании которого внешняя метка входящего пакета 1198 будет заменяться на 100.

```
console# configure
console(config)# selective-qinq list ingress override_vlan 100 ingress_vlan 1198 priority 1
console(config)# exit
```

- Отобразить список созданных правил selective qinq:

```
console# show selective-qinq
Direction Priority Rule type       Vlan ID   Classification  Outer Vlan ID
--------- -------- --------------- -------- ---------------- --------------
ingress   1        override_vlan   100      ingress_vlan     1198
egress    1        override_vlan   1198     ingress_vlan     100
```

5.8 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 5.29 – Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение*	*Действие*
port storm-control include-multicast	По умолчанию функция выключена	Добавляет контроль многоадресного трафика к контролю широковещательного.
no port storm-control include-multicast		Выключает контроль многоадресного трафика.
port storm-control include-multicast unknown-unicast	По умолчанию функция выключена	Добавляет контроль неизвестного одноадресного трафика к контролю широковещательного.
no port storm-control include-multicast unknown-unicast		Выключает контроль неизвестного одноадресного трафика.
port storm-control broadcast enable	По умолчанию функция выключена	Включает контроль широковещательного трафика.
no port storm-control broadcast enable		Выключает контроль широковещательного трафика.
port storm-control broadcast rate *rate*	3500-1000000/ 3500 Кбит/с	Задает максимальную скорость для широковещательного, многоадресного и неизвестного одноадресного трафика.
no port storm-control broadcast rate		Устанавливает значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.30 – Команды режима EXEC

Команда	*Значение*	*Действие*
show ports storm-control [*port*]	{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}	Показывает конфигурацию функции контроля широковещательного «шторма» для указанного порта, либо всех портов.

Примеры выполнения команд

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

```
console# configure
console(config)# interface ethernet 1/g15
console(config-if)# port storm-control broadcast enable
console(config-if)# port storm-control include-multicast
console(config-if)# port storm-control include-multicast unknown-unicast
console(config-if)# port storm-control broadcast rate 5000
```

5.9 Группы агрегации каналов – Link Agregation Group (LAG)

Коммутатор MES3124 обеспечивает поддержку до восьми интерфейсов Ethernet в одной группе портов LAG и до восьми групп LAG на устройстве или стеке устройств. Каждая группа портов должна состоять из интерфейсов Ethernet с одинаковой скоростью, работающих в дуплексном режиме. Объединение портов в группу увеличивает пропускную способность канала между взаимодействующими устройствами и повышает отказоустойчивость. Группа портов является для коммутатора одним логическим портом.

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

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

Для создания интерфейса группы портов используется команда **interface port-channel group** в глобальном режиме конфигурирования:

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

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 5.31 – Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение/ значение по умолчанию*	*Действие*
channel-group {group**} mode {**mode**}**	group {1..8} 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 5.32 – Команды режима глобального конфигурирования

Команда	*Значение*	*Действие*
port-channel load-balance {layer-2-3|layer-2|layer-3|layer-2-3-4	layer-2	Задает механизм балансировки нагрузки для группы агрегированных портов. **layer2-3 –** Механизм балансировки основывается на MAC-адресе и IP-адресе **layer-2 –** Механизм балансировки основывается на MAC-адресе **layer-3 –** Механизм балансировки основывается на IP-адресе **layer-2-3-4 –** Механизм балансировки основывается на MAC-адресе, IP-адресе и порте назначения

Для просмотра информации по группе каналов используется команда **show interfaces port-channel [group]** в режиме EXEC.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.33 – Команды режима EXEC

Команда	*Значение/ значение по умолчанию*	*Действие*
show interfaces port-channel [group**]**	group [1..8]	Показывает информацию по группе каналов.

5.9.1 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.

5.9.2 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 5.34 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
lacp system-priority *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 5.35 – 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*	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 5.36 – Команды режима EXEC

Команда	*Значение/ Значение по умолчанию*	*Действие*
show lacp ethernet *port* **[parameters | statistics | protocol-state]**	1/g(1-24)..8/g(1-24), g1..g24	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*]	[1..8]	Показывает информацию о протоколе LACP для группы портов.

Примеры выполнения команд

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

```
console# configure
console(config)# lacp system-priority 6
console(config)# interface port-channel 1
console(config-if)# speed 1000
console(config-if)# exit
console(config)# interface ethernet 1/g3
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 ethernet 1/g4
console(config-if)# speed 1000
console(config-if)# channel-group 1 mode auto
console(config-if)# lacp port-priority 13
console(config-if)# exit
console(config)#
```

5.10 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 (set system mode switch policy-based-vlans active) нельзя задать более одного IP-адреса для устройства. В связи с этим необходимо отключить получение IP-адреса по протоколу DHCP на интерфейсе vlan 1, если настройки параметров IP-адресации следует произвести для другого интерфейса.

Команды режима конфигурирования интерфейса

Вид запроса командной строки в режиме конфигурирования интерфейса:

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

Таблица 5.37 – Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение*	*Действие*
ip address *IP-addr mask* **[***gateway***]**	-	Назначение физическому интерфейсу Eternet IP-адреса, маски подсети, адреса шлюза по умолчанию.
no ip address		Удаление IP-адреса на физическом интерфейсе Eternet.
ip address dhcp [hostname *hostname***]**	[1..20] символов	Получение IP-адреса для настраиваемого интерфейса от DHCP-сервера. - hostname – задает сетевое имя интерфейса, передаваемое в опции 12 протокола DHCP. Используется для передачи имени устройства, отличного от глобального имени коммутатора. Данная команда доступна только в режиме коммутатора (set system mode switch policy-based vlan active)
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 5.38 - Команды режима глобального конфигурирования

Команда	*Значение*	*Действие*
ip default-gateway *IP-адрес*	-/шлюз по умолчанию не задан	Задает для коммутатора шлюз по умолчанию. Данная команда доступна только в режиме коммутатора (set system mode switch policy-based vlan active)
no ip default-gateway		Удаляет для коммутатора шлюз по умолчанию.

Команды режима EXEC

Вид запроса командной строки в режиме EXEC:

```
console#
```

Таблица 5.39 - Команды режима EXEC

Команда	*Значение*	*Действие*
show ip interface [ethernet *port* **| vlan** *vlan-id* **| port-channel** *group***]**	port [{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}]; vlan-id [1..4094]; group [1..8]	Показывает конфигурацию IP-адресации для указанного интерфейса.
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. Данная команда доступна только в режиме коммутатора (set system mode switch policy-based vlan active)
dhcp renew { ethernet *port* **| vlan** *vlan-id* **| port-channel** *group* **}**	port {1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}; vlan-id {1..4094}; group {1..8}	Отправляет запрос к DHCP-серверу на обновление IP-адреса. Данная команда доступна только в режиме коммутатора (set system mode switch policy-based vlan active)

Примеры выполнения команд

- Установить IP-адрес шлюза по умолчанию - 192.168.16.2:

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

5.11 Настройка Green Ethernet

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

Команды режима глобального конфигурирования

Вид запроса командной строки в режиме глобального конфигурирования:

```
console(config)#
```

Таблица 5.40 - Команды режима глобального конфигурирования

Команда	*Значение*	*Действие*
green-ethernet energy-detect	-/Включен	Включает энергосберегающий режим для неактивных портов
no green-ethernet energy-detect		Отключает энергосберегающий режим для неактивных портов
green-ethernet short-reach	-/Включен	Включает энергосберегающий режим для портов, к которым подключаются устройства с длиной кабеля подключения меньше порогового значения, устанавливаемого с помощью команды **green-ethernet short-reach threshold**
no green-ethernet short-reach		Отключает энергосберегающий режим на основании длины кабеля

green-ethernet short-reach threshold <value>	0-70/10 метров	Устанавливает пороговое значение для энергосберегающего режима short-reach.
no green-ethernet short-reach threshold		Возвращает настройки по умолчанию

Команды режима конфигурирования интерфейса

Вид запроса командной строки в режиме конфигурирования интерфейса:

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

Таблица 5.41 – Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение*	*Действие*
green-ethernet energy-detect	-/Включен	Включает энергосберегающий режим для интерфейса
no green-ethernet energy-detect		Отключает энергосберегающий режим для интерфейса
green-ethernet short-reach	-/Включен	Включает энергосберегающий режим на основании длины кабеля
no green-ethernet short-reach		Отключает энергосберегающий режим на основании длины кабеля
green-ethernet short-reach force	-/Отключен	Перманентно включает энергосберегающий режим для порта
no green-ethernet short-reach force		Перманентно включает энергосберегающий режим для порта

Команды режима EXEC

Вид запроса командной строки в режиме EXEC:

```
console#
```

Таблица 5.42 - Команды режима EXEC

Команда	*Значение*	*Действие*
show green-ethernet	-	Отображает статистику green-ethernet
show green-ethernet port <port>	1/g(1-24)..8/g(1-24), g1..g24	Отображает статистику green-ethernet для порта

Примеры выполнения команд

- Отобразить статистику green-ethernet:

```
console# show green-ethernet

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

Port     Energy-Detect       Short-Reach           VCT Cable
      Admin Oper Reason   Admin Force Oper Reason   Length
----  ----- ---- -------  ----- ----- ---- -------  ------
g1     on    off  LU        on    off   off  LL       < 50
```

```
g2      on    off   LU          on    off    off   LL        < 50
g3      on    off   LU          on    off    on              < 50
g4      on    on                on    off    off   LD
g5      on    on                on    off    off   LD
g6      on    on                on    off    off   LD
g7      on    on                on    off    off   LD
g8      on    on                on    off    off   LD
g9      on    on                on    off    off   LD
g10     on    off   LU          on    off    off   LL        50 - 80
g11     on    off   LU          on    off    on              < 50
g12     on    off   LU          on    off    on              < 50
g13     on    off   LU          on    off    on              < 50
g14     on    off   LU          on    off    on              < 50
g15     on    off   LU          on    off    off   LL        50 - 80
g16     on    on                on    off    off   LD
g17     on    on                on    off    off   LD
g18     on    on                on    off    off   LD
g19     on    on                on    off    off   LD
g20     on    on                on    off    off   LD
g21     on    on                on    off    off   LD
g22     on    off   LU          on    off    on              < 50
g23     on    off   LU          on    off    off   LL        50 - 80
g24     on    off   LU          on    off    off   LL        50 - 80
xg1     on    off   LT          on    off    off   LT
xg2     on    off   LT          on    off    off   LT
xg3     on    off   LT          on    off    off   LT
xg4     on    off   LT          on    off    off   LT
```

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

5.12 Настройка IPv6-адресации

5.12.1 Протокол IPv6

Коммутатор MES3124 поддерживает 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 = {1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}

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 5.43 – Команды режима глобального конфигурирования

Команда	*Значение*	*Действие*
ipv6 default-gateway *ipv6-address*	-	Задает значение локального адреса IPv6-шлюза по умолчанию. Данная команда доступна только в режиме коммутатора (set system mode switch policy-based vlan active).
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 hw_addr* {**ethernet** *port* | **vlan** *vlan-id* **/ port-channel** *group* }	port: {1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}; vlan-id: {1..4094}; group: {1..8}	Создает статическое соответствие между MAC-адресом соседнего устройства и его IPv6-адресом.
no ipv6 neighbor		Удаляет статическое соответствие между MAC-адресом соседнего устройства и его IPv6-адресом.

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

Вид запроса командной строки режима конфигурирования интерфейса:

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

Таблица 5.44 – Команды режима конфигурирования интерфейса (Ethernet, VLAN, Port-channel)

Команда	*Значение/Значение по умолчанию*	*Действие*
ipv6 enable	-	Включает поддержку IPv6 на интерфейсе.
no ipv6 enable		Отключает поддержку IPv6 на интерфейсе.
ipv6 address *ipv6-address/ prefix-length* [**eui-64**]	prefix-length: 3..128 (64 если используется	Задает IPv6-адрес на интерфейсе. - ipv6-address – IPv6 сеть, назначенная интерфейсу (8

	параметр eui-64)	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.
no ipv6 address [*ipv6-address/ prefix-length*] [**eui-64**]		Удаляет IPv6-адрес с интерфейса.
ipv6 address *ipv6-address* **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* **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.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.45 – Команды режима EXEC

Команда	***Значение***	***Действие***
show ipv6 interface [**ethernet** *port* | **vlan** *vlan-id* **/ port-channel** *group*]	port: [{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}]; vlan-id: [1..4094]; group: [1..8]	Показывает настройки протокола IPv6 для указанного интерфейса.
show ipv6 route	-	Показывает таблицу IPv6-маршрутов.
show ipv6 neighbors {**static** | **dynamic**} [**ipv6-address** *ipv6-address*] [**mac-address** *mac-address*] [**ethernet** *port* | **vlan** *vlan-id* **/ port-channel** *group*]	port: [{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}]; vlan-id: [1..4094]; group: [1..8]	Показывает информацию о соседних IPv6 устройствах, содержащуюся в кэше. (Команда доступна только для привилегированного пользователя). - 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. (Команда доступна только для привилегированного пользователя).

Примеры выполнения команд

Показать динамические записи в таблице маршрутизации о соседних IPv6 устройствах.

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

```
Interface    IPv6 address                          HW address        State
---------    ------------------------------------ ----------------- -----
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.

5.12.2 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 5.46 – 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 5.47 – 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* **| ethernet** *port* **| vlan** *vlan-id* **| port-channel** *group* **}**	По умолчанию, IP-адрес не назначен port: [{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}]; vlan-id: [1..4094]; group: [1..8]	Команда назначает локальный IP-адрес туннелю, который будет использоваться, в качестве адреса источника, при отправке пакетов. - auto – IP-адрес будет автоматически назначен системой - при выборе интерфейса Ethernet, Vlan, Port-channel в качестве адреса источника, при отправке пакетов будет использоваться IP-адрес соответствующего интерфейса.
no tunnel source		Удаляет локальный IP-адрес туннеля.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.48 – Команды режима EXEC

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

Примеры выполнения команд

Включить интерфейс туннелирования, назначить доменное имя туннеля – mes3124, 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 MES3124
console(config-tunnel)# tunnel source ip-address 192.168.16.88
```

5.13 Настройка макрокоманд

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

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.49 – Команды режима глобального конфигурирования

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.50 – Команды режима EXEC

Команда	*Действие*	
macro apply *{word}*	1..32 символов	Применяет указанный макрос
macro trace *{word}*	1..32 символов	Проверяет указанный макрос на валидность

Команды режима конфигурации интерфейса

Вид запроса командной строки режима EXEC:

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

Таблица 5.51 – Команды режима EXEC

Команда	*Действие*	
macro apply *{word}*	1..32 символов	Применяет указанный макрос
macro trace *{word}*	1..32 символов	Проверяет указанный макрос на валидность
macro description *{word}*	1..160 символов	Устанавливает строку-дескриптор макроса
no macro description		Удаляет строку-дескриптор

5.14 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 5.52 - Команды режима глобального конфигурирования

Команда	*Действие*
ip domain-lookup	Разрешает использование протокола DNS.
no ip domain-lookup	Запрещает использование протокола DNS.
ip name-server {server1-ipv4-address|server1-ipv6-address} [server-address2 … server-address8]	Определяет IP-адреса для доступных DNS-серверов. Можно определить IP-адреса для восьми серверов.
no ip name-server [server-address1 … server-address8]	Удаляет IP-адрес DNS-сервера из списка доступных.
ip domain-name name	Определяет доменное имя по умолчанию, которое будет использоваться программой, для дополнения неправильных доменных имен (доменных имен без точки). Для доменных имен без точки в конец имени будет добавляться точка и указанное в команде доменное имя. Имя должно содержать от 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.
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 5.53 - Команды режима EXEC

Команда	*Действие*
clear host {*name*|***}**	Удаляет запись соответствия имени узла сети IP-адресу кэша либо все записи (*) . (Команда доступна только для привилегированного пользователя). 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 5.54 - Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
arp *ip_addr hw_addr* **{ethernet** *port* **| vlan** *vlanID* **| port-channel** *group***}**	port: {1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}; vlanID {1..4094}; group {1..8}	Добавляет статическую запись соответствия IP и MAC-адресов в таблицу ARP для указанного в команде интерфейса. ip_addr – IP-адрес hw_addr – MAC-адрес
no arp *ip_addr* **{ethernet** *port* **| vlan** *vlanID* **| port-channel** *group***}**		Удаляет статическую запись соответствия IP и MAC-адресов из таблицы ARP для указанного в команде интерфейса.

arp timeout *sec*	1-40000000/ 60000 сек	Настраивает время жизни динамических записей в таблице ARP (сек).
no arp timeout		Устанавливает значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки в режиме EXEC:

```
console#
```

Таблица 5.55 - Команды режима 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*] [**ethernet** *port* **| port-channel** *group*]	port: {1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}; group {1..8}	Показывает записи ARP-таблицы. ip_address – IP-адрес; mac_address – MAC-адрес.

Примеры использования команд

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

```
console# configure
console(config)# arp 192.168.16.32 00-00-0c-40-0f-bc ethernet g1/21
console(config)# exit
console# arp timeout 12000
```

- Показать содержимое ARP таблицы:

```
console# show arp
```

```
ARP timeout: 120000 Seconds


 VLAN     Interface     IP address         HW address           status
---------------------- --------------- -------------------- ---------------
vlan 1      1/g2       192.168.16.1     00:26:18:9d:1c:ee   dynamic
vlan 1      1/g21      192.168.16.32    00:00:0c:40:0f:bc   static
```

5.14.3 Настройка протокола GVRP

Generic 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 5.56 – 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 {ethernet {port}|port-channel {group}}
console(config-if)#
```

Таблица 5.57 – 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 6.47). ***Значение таймера должно быть кратно 10.***
no garp timer {join | leave | leaveall}		Установить значения по умолчанию.
gvrp vlan-creation-forbid	-/разрешено	Запрещает динамическое изменение или создание VLAN для настраиваемого интерфейса.
no gvrp vlan-creation-forbid		Разрешает динамическое изменение или создание VLAN для настраиваемого интерфейса.
gvrp registration-forbid	По умолчанию создание и регистрация VLAN на интерфейсе разрешена	Выполняет снятие регистрации для всех VLAN и не допускает создания или регистрации новых VLAN на данном интерфейсе.
no gvrp registration-forbid		Устанавливает значение по умолчанию.

Таблица 5.58 – 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 EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.59 – Команды режима EXEC

Команда	*Действие*
clear gvrp statistics [**ethernet** *port* | **port-channel** *group*]	Очищает накопленную статистику протокола GVRP. (Команда доступна только для привилегированного пользователя).
show gvrp configuration [**ethernet** *port* | **port-channel** *group*]	Показывает конфигурацию протокола GVRP для указанного интерфейса, либо для всех интерфейсов.
show gvrp statistics [**ethernet** *port* | **port-channel** *group*]	Показывает накопленную статистику по протоколу GVRP для указанного интерфейса, либо для всех интерфейсов.
show gvrp error-statistics [**ethernet** *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 5.60 - Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
loopback-detection enable	-/disabled	Включает механизм обнаружения петель
no loopback-detection enable		Восстанавливает значение по умолчанию
loopback-detection interval <value>	30-60/30 секунд	Устанавливает интервал между loopback-фреймамми
no loopback-detection interval		Восстанавливает значение по умолчанию
loopback-detection mode {src-mac-addr|base-mac-addr}	-	**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 {ethernet {port}|port-channel {group}}
console(config-if)#
```

Таблица 5.61 – 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 5.62 – Команды режима EXEC

Команда	*Значение*	*Действие*
show loopback-detection [ethernet *port* **| port-channel** *group***]**	port [{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4),	Отображает состояние механизма loopback-detection

	g1..g24, xg1..xg24}]; group [1..8]	

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.

Настройка протокола STP, RSTP

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.63 – 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}	-/STP	Устанавливает режим работы протокола STP.
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 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**}	-/long	Устанавливает метод определения ценности пути. - long – значение ценности в диапазоне 1..200000000;

		- short – значение ценности в диапазоне 1..65535.
no spanning-tree pathcost method		Устанавливает значение по умолчанию.
spanning-tree bpdu {filtering | flooding}	-/flooding	Определяет режим обработки пакетов BPDU интерфейсом, на котором выключен протокол STP. - filtering – на интерфейсе с выключенным протоколом STP BPDU пакеты фильтруются. - flooding – на интерфейсе с выключенным протоколом STP нетегированные BPDU пакеты передаются, тегированные – фильтруются.
no spanning-tree bpdu		Устанавливает значение по умолчанию.

При задании 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 5.64 – 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	Устанавливает ценность пути через выбранный интерфейс.
no spanning-tree cost		Устанавливает значение, определяемое на основании скорости порта и метода определения ценности пути.
spanning-tree port-priority	0..240/128	Устанавливает приоритет интерфейса в связующем дереве STP. ***Значение приоритета должно быть кратно 16.***
no spanning-tree port-priority		Устанавливает значение по умолчанию.
spanning-tree portfast [auto]	-	Включает режим, в котором порт при поднятии на нем «линка» сразу становится в состояние передачи, не дожидаясь истечения таймера. - auto – добавляет задержку 3 секунды перед переходом в состояние передачи.
no spanning-tree portfast		Выключает режим моментального перехода в состояние передачи по поднятию «линка».
spanning-tree guard root	-/защита выключена	Включает защиту «корня» для всех связующих деревьев STP выбранного порта. Данная защита запрещает интерфейсу быть корневым портом коммутатора.
no spanning-tree guard root		Устанавливает значение по умолчанию.
spanning-tree bpduguard	-/защита выключена	Разрешает защиту, выключающую интерфейс при приёме пакетов BPDU.
no spanning-tree bpduguard		Запрещает защиту, выключающую интерфейс при приёме пакетов BPDU.
spanning-tree link-type {point-to-point | shared}	Значение по умолчанию для дуплексного порта	Устанавливает протокол RSTP в передающее состояние и определяет тип связи для выбранного порта - «точка-

	«точка-точка», для полудуплексного – «разветвленный»	точка», «разветвлённый».
no spanning-tree link-type		Устанавливает значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.65 – Команды режима EXEC

Команда	*Значение*	*Действие*
show spanning-tree [ethernet *port* **| port-channel** *group***]**	port [{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}]; group [1..8]	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 [ethernet *port* **| port-channel** *group***]**	port [{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}]; group [1..8]	Перезапускает процесс миграции протокола. Заново происходит просчёт дерева STP.

Настройка протокола MSTP

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.66 – 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}	-/STP	Устанавливает режим работы протокола STP.
no spanning-tree mode		Устанавливает значение по умолчанию.
spanning-tree pathcost method {**long** | **short**}	-/long	Устанавливает метод определения ценности пути. - long – значение ценности в диапазоне 1..200000000; - short – значение ценности в диапазоне 1..65535.
no spanning-tree pathcost method		Устанавливает значение по умолчанию.
spanning-tree mst *instance-id* **priority** *priority*	instance: 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 5.67 – Команды режима конфигурирования протокола MSTP

Команда	*Значение/Значение по умолчанию*	*Действие*
instance *instance-id* **[add | remove] vlan** *vlan-range*	instance: 1..15; vlan-range: 1..4094	Создает, либо удаляет соответствия 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 5.68 – 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* **priority** *priority*	instance: 1..15; priority: 0..240/128	Устанавливает приоритет интерфейса в экземпляре MSTP. ***Значение приоритета должно быть кратно 16.***
no spanning-tree mst *instance-id* **priority**		Устанавливает значение по умолчанию.

spanning-tree mst *instance-id* **cost** *cost*	instance: 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.
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 EXEC

Все команды доступны только для привилегированного пользователя.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.69 – Команды режима EXEC

Команда	*Значение*	*Действие*
show spanning-tree [ethernet *port* **| port-channel** *group***]** [**instance** *instance-id*]	port [{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}]; group [1..8]; instance: 1..15	Показывает конфигурацию протокола STP. - instance-id – идентификатор экземпляра протокола MSTP.
show spanning-tree [detail] [active | blockedports] [**instance** *instance-id*]	instance: 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 [ethernet *port* **| port-channel** *group***]**	port [{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}]; group [1..8]	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



  Root ID    Priority    12288
             Address     02:10:11:12:13:00
             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
------ -------- -------- --------- ------ ---- -------- -----------------
 1/g1  enabled   128.1    2000000   DSBL  Dsbl    No            -
 1/g2  enabled   128.2    200000    FRW   Desg    No       P2p (RSTP)
 1/g3  enabled   128.3    2000000   DSBL  Dsbl    No            -
```

5.14.6 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.

Коммутатор MES3124 поддерживает 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 5.70 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
lldp enable	enabled	Разрешает коммутатору использование протокола LLDP.
no lldp enable		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-delay *seconds*	1..10/2 сек	Минимальное время, которое LLDP-порт будет ожидать перед повторной инициализацией LLDP.
no lldp reinit-delay		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 med network-policy *number application* [**vlan** *id*] [**vlan-type** {**tagged** | **untagged}**] [**up** *priority*] [**dscp** *value*]	application: voice, voice-signaling, guest-voice, guest-voice-signaling, softphone-voice, video-conferencing, streaming-video, video-signaling	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). - dscp value – значение DSCP, используемое данным правилом.
no lldp med network-policy *number*		Удаляет созданное правило для параметра network-policy.

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet:

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

Таблица 5.71 – Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
lldp enable [tx | rx | both]	По умолчанию разрешено использование в обоих направлениях	Разрешает использование протокола LLDP на интерфейсе. - rx – разрешен прием LLDP-пакетов - tx– разрешена передача LLDP-пакетов - both – разрешен прием и передача LLDP-пакетов
no lldp enable		Запрещает использование протокола LLDP на интерфейсе.
lldp optional-tlv *tlv1* [*tlv2.. tlv5*]	port-desc, sys-name, sys-desc, sys-cap, 802.3-mac-phy По умолчанию опциональные TLV не	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

no lldp optional-tlv	включены в пакет	Устанавливает значение по умолчанию.
lldp management-address *IP-addr*	-	Определяет управляющий IP-адрес, объявленный на интерфейсе.
no lldp management-address		Удаляет управляющий IP-адрес.
lldp med enable [*tlv1* … *tlv3*]	network-policy, location, poe-pse	Разрешает использование расширения протокола LLDP MED. В команду можно включить от одного до трех специальных TLV: network-policy, location, poe-pse.
no lldp med enable		Запрещает использование расширения протокола LLDP MED.
lldp med network-policy {add|remove} *number*	-	Назначает правило network-policy данному интерфейсу. - add – назначает правило - remove – удаляет правило
no lldp med network-policy *number*		Удаляет правило network-policy с данного интерфейса.
lldp med location {coordinate *coordinate*| **civic-address** *civic-address-data* | **ecs-elin** *ecs-elin-data* | *data***}**	coordinate: 16; civic address: 6..160; ecs-elin: 10 – 25	Задает местоположение устройства для протокола LLDP (значение параметра location протокола LLDP MED). - coordinate – адрес в системе координат; - civic-address – административный адрес устройства; - ecs-elin – адрес в формате, определенном ANSI/TIA 1057.
no lldp med location		Удаляет настройки параметра местоположения location.

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 EXEC

Все команды доступны только для привилегированного пользователя.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.72 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
clear lldp rx	-	Очищает таблицу адресов обнаруженных соседних устройств и начинает новый цикл обмена пакетами по протоколу LLDP MED.
show lldp configuration	-	Показывает LLDP конфигурации всех физических интерфейсов устройства.
show lldp med configuration	-	Показывает конфигурации расширения протокола LLDP - MED для всех физических интерфейсов.

show lldp local ethernet *port*	{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}	Показывает LLDP-информацию, которую анонсирует данный порт.
show lldp neighbors	-	Показывает информацию о соседних устройствах, на которых работает протокол LLDP.

Примеры выполнения команд

Установить для порта 1/g1 следующие tlv-поля: port-description, sytem-name, system-description. Для данного интерфейса добавить управляющий адрес 192.168.17.55

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

Посмотреть конфигурацию lldp:

```
console# show lldp configuration
```

```
LLDP state: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds

   Port          State             Optional TLVs            Address
---------- --------------- ------------------------ ---------------
1/g1          Rx and Tx             PD, SN, SD          192.168.16.55
1/g2          Rx and Tx
1/g3          Rx and Tx
1/g4          Rx and Tx
1/g5          Rx and Tx
1/g6          Rx and Tx
1/g7          Rx and Tx
1/g8          Rx and Tx
1/g9          Rx and Tx
1/g10         Rx and Tx
1/g11         Rx and Tx
1/g12         Rx and Tx
1/g13         Rx and Tx
1/g14         Rx and Tx
1/g15         Rx and Tx
1/g16         Rx and Tx
1/g17         Rx and Tx
1/g18         Rx and Tx
1/g19         Rx and Tx
1/g20         Rx and Tx
1/g21         Rx and Tx
1/g22         Rx and Tx
More: <space>,  Quit: q, One line: <return>
```

Таблица 5.73 - 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.

Показать информацию о соседних устройствах

```
console# show lldp neighbors
```

```
Port           Device ID           Port ID  System Name   Capabilities
---------      -----------------  -------- ----------    -------------
g1             0060.704C.73FE      1       ts-7800-2     B
g2             0060.704C.73FD      1       ts-7800-2       B
g3             0060.704C.73FC      9       ts-7900-1     B, R
g4             0060.704C.73FB      1       ts-7900-2       W
```

```
console# show lldp neighbors ethernet g1
```

```
Device ID: 02:10:11:12:13:00
Port ID: g23
Capabilities: B
System Name: sandbox2
System description: 24-port 10/100/1000 Ethernet Switch
Port description: Ethernet Interface

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

Таблица 5.74 - 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 Voice VLAN

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

- VoIP-оборудование настраивается, чтобы рассылать тегированные пакеты, с ID Voice VLAN, настроенным на MES3124.
- VoIP-оборудование рассылает нетегированные DHCP-запросы. В ответе от DHCP-сервера присутствует опция 132 (VLAN ID) с ID Voice VLAN, с помощью которой устройство автоматически назначает себе VLAN для маркировки трафика.

По умолчанию в таблицу Voice VLAN добавлены OUI производителей VoIP-оборудования, доминирующих на рынке.

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

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

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.75 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
voice vlan aging timeout <timeout>	1-43200/1440	Устанавливает таймаут, для порта, принадлежащего к voice-vlan. Если с порта в течение заданного времени не было фреймов с OUI VoIP-оборудования, то voice vlan удаляется с данного порта
no voice vlan aging timeout		Восстанавливает значение по умолчанию
voice vlan cos <cos>	0-7/6	Устанавливает COS, которым маркируются фреймы, принадлежащие Voice VLAN
no voice vlan cos		Восстанавливает значение по умолчанию
voice vlan id <id>	2..4094/-	Устанавливает идентификатор VLAN для Voice VLAN
no voice vlan id		Удаляет идентификатор VLAN для Voice VLAN ***Для удаления идентификатора VLAN требуется предварительно отключить функцию voice vlan на всех портах***
voice vlan oui-table {add|remove} {oui} [word]	oui – первые 3 байта MAC-адреса word – 1..32 символов	Позволяет редактировать таблицу OUI
no voice vlan oui-table		Удаляет все пользовательские изменения OUI-таблицы

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet:

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

Таблица 5.76 – Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
voice vlan enable	Отключена	Включает Voice VLAN для порта
no voice vlan enable		Отключает Voice VLAN для порта
voice vlan cos mode {src|all}	?	Включает маркировку трафика для всех фреймов, либо только для источник
no voice vlan cos mode		Восстанавливает значение по умолчанию

5.16 Групповая адресация

5.16.1 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 5.77 – Команды режима конфигурирования интерфейса VLAN

Команда	*Значение/Значение по умолчанию*	*Описание*
bridge address *mac-address* {**ethernet** *port* **/ port-channel** *group*} [**permanent** | **delete-on-reset** | **delete-on-timeout** | **secure**]	port: [{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}]; group: [1..8]	Добавляет MAC-адрес в таблицу групповой адресации. - 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 bridge address [*mac-address***]**		Удаляет MAC-адрес из таблицы групповой адресации.
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**] { **ethernet** *interface-list* **/ port-channel** *port-channel-number-list* }	-	Добавляет групповой MAC-адрес в таблицу групповой адресации. - mac-multicast-address – групповой MAC-адрес; - interface-list – список интерфейсов Ethernet; - port-channel-number-list – список групп портов; - add - ставит в соответствие групповому MAC-адресу диапазон Ethernet-портов или групп портов. - remove – удаляет соответствие групповому MAC-адресу.
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**} {**ethernet** *interface-list* **/ port-channel** *port-channel-number-list* }	-	Создает запрещающее правило для группового MAC-адреса. - mac-multicast-address – групповой MAC-адрес; - interface-list – список интерфейсов Etherne;t - port-channel-number-list – список групп портов; - add – создает правило, запрещающее ставить в соответствие групповой MAC-адрес списку портов/групп портов; - remove – отменяет данное правило для списка портов/групп портов.
no bridge multicast forbidden address *[mac-multicast-address | ip-multicast-address]*		Удаляет запрещающее правило для группового MAC-адреса.

bridge multicast forward-all {**add** | **remove**} {**ethernet** *interface-list* **/ port-channel** *port-channel-number-list*}	-	Разрешает передачу всех многоадресных пакетов на порту. - mac-multicast-address – групповой MAC-адрес; - interface-list – список интерфейсов Ethernet; - port-channel-number-list – список групп портов; - add – создает правило, разрешающее передачу всех групповых пакетов в списке портов/объединенных портов; - remove – убирает группу портов/объединенных портов из разрешающего правила.
bridge multicast forbidden forward-all {**add** | **remove**} {**ethernet** *interface-list* **/ port-channel** *port-channel-number-list*}	-	Запрещает передачу всех многоадресных пакетов на порту. - mac-multicast-address – групповой MAC-адрес; - interface-list – список интерфейсов Ethernet; - port-channel-number-list – список групп портов; - add – создает правило, запрещающее передачу всех групповых пакетов на список портов/объединенных портов; - remove – убирает группу портов/объединенных портов из запрещающего правила.

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

Таблица 5.78 – 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 5.79 – 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.
bridge aging-time *seconds*	10..630/300 секунд	Задает время хранения MAC-адреса в таблице.
no bridge aging-time		Устанавливает значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.80 – Команды режима EXEC

Команда	*Значение*	*Описание*
clear bridge	-	Очищает таблицу MAC-адресов в таблице групповой адресации (команда доступна только для привилегированного пользователя).
show bridge address-table [**vlan** *vlan*] [**ethernet** *port* **/ port-channel** *group*] [**address** *mac-address*]	port: [{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}]; group: [1..8]; VLAN ID [1..4094]	Показывает таблицу MAC-адресов для указанного интерфейса, либо всех интерфейсов (команда доступна только для привилегированного пользователя)
show bridge address-table static [**vlan** *vlan*] [**ethernet** *port* **/ port-channel** *group*]		Показывает статические записи в таблице MAC-адресов для указанного интерфейса, либо для всех интерфейсов (команда доступна только для привилегированного пользователя).
show bridge address-table count [**vlan** *vlan* | **ethernet** *port* **/ port-channel** *group*]		Показывает количество записей в таблице MAC-адресов для указанного интерфейса, либо для всех интерфейсов (команда доступна только для привилегированного пользователя).
show bridge multicast address-table [vlan *vlan-id*] [**address {***mac-multicast-address* | *ipv4-multicast-address*}] [**format ip** | **mac**] [**source** *ipv4-source-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*] [**source** *ipv4-source-address*]	VLAN ID [1..4094]	Показывает таблицу статических групповых адресов для указанного интерфейса, либо всех интерфейсов VLAN (команда доступна только для привилегированного пользователя).
show bridge multicast filtering *vlan-id*	VLAN ID [1..4094]	Показывает конфигурацию фильтра групповых адресов для указанного VLAN (команда доступна только для привилегированного пользователя).
show bridge multicast unregistered [**ethernet** *port* **/ port-channel** *group*]	port: [{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}]; group: [1..8]	Показывает конфигурацию фильтра для незарегистрированных групповых адресов (команда доступна только для привилегированного пользователя).
show bridge multicast mode [vlan *vlan-id***]**	VLAN ID [1..4094]	Показывает режим групповой адресации для указанного интерфейса, либо всех интерфейсов VLAN.

Примеры выполнения команд

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

```
console # configure
console(config) # bridge aging-time 450
console(config) # bridge multicast filtering
console(config) # interface ethernet 1/g11
console(config-if) # bridge multicast unregistered forwarding

console# show bridge multicast address-table format ip
```

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

Forbidden ports for multicast addresses:

Vlan IP/MAC Address            Ports
---- ------------------ -------------------
1    224-239.130|2.2.3         2/8
19   224-239.130|2.2.8         2/8
```

5.16.2 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 5.81 – 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 map cpe vlan *vlan-id* **multicast-tv vlan** *vlan-id*	vlan 1..4094	Добавляет соответствие между VLAN пользователя (CPE-VLAN) и VLAN телевещания (multicast-tv-vlan). Если IGMP-сообщение приходит на порт с тэгом CPE-vlan и существует соответствие CPE-vlan – multicast-tv-vlan, то IGMP-сообщение будет ассоциировано с VLAN для телевещания.
no ip igmp snooping map cpe vlan *vlan-id*		Удаляет соответствие между VLAN пользователя и VLAN телевещания
ip igmp snooping multicast-tv vlan *vlan-id* {**add** | **remove**} *ip-multicast-address* [**count** *number*]	1..256	Ассоциирует многоадресные IP-адреса к VLAN для телевещания - number – количество IP-адресов, используется для задания непрерывного диапазона многоадресных IP-адресов (если параметр не указан в команде, то он принимает значение – 1). ***Данная команда доступна только в режиме коммутатора (set system mode switch policy-based-vlans active).***
no ip igmp snooping multicast-tv vlan *vlan-id*		Удаляет ассоциацию

Команды режима конфигурирования интерфейса VLAN

Вид запроса командной строки режима конфигурирования VLAN:

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

Таблица 5.82 – Команды режима конфигурирования интерфейса VLAN

Команда	*Значение/Значение по умолчанию*	*Действие*
ip igmp snooping	-	Разрешает использование функции IGMP Snooping в настраиваемой группе VLAN.
no ip igmp snooping		Запрещает использование функции IGMP Snooping в настраиваемой группе VLAN.
ip igmp snooping mrouter learn-pim-dvmrp	По умолчанию – разрешено	Разрешает для данной группы VLAN автоматическое распознавание портов, к которым подключены многоадресные маршрутизаторы.
no ip igmp snooping mrouter learn-pim-dvmrp		Запрещает для данной группы VLAN автоматическое распознавание портов, к которым подключены многоадресные маршрутизаторы.
ip igmp snooping host-time-out *timeout*	60..2147483647/ 260 сек	Устанавливает время ожидания сообщения IGMP Report. Если по истечении таймаута сообщение не принято от порта, принадлежащего многоадресной группе, то этот порт удаляется из списка членов группы.

		Таймаут должен быть больше значения, рассчитанного по формуле 2*query_interval+max_response_time. В формуле используются параметры IGMP маршрутизатора.
ip igmp snooping mrouter-time-out *seconds*	1–2147483647/300 сек	Задает период, в течение которого коммутатор ожидает многоадресные пакеты от группового маршрутизатора после изучения его адреса на порту.
no ip igmp snooping mrouter-time-out		Устанавливает значение по умолчанию.
ip igmp snooping leave-time-out {*time-out* | **immediate-leave}**	0..2147483647/10 сек	Устанавливает значение leave-таймера - времени ожидания сообщения IGMP report после приема IGMP leave. Если в течение этого времени сообщение IGMP report не получено, то порт удаляется из IGMP группы. - immediate-leave означает, что порт должен быть немедленно удален из группы IGMP после получения сообщения IGMP leave.
no ip igmp snooping leave-time-out		Устанавливает значение по умолчанию.
ip igmp snooping querier enable	-/выдача запросов отключена	Включает поддержку выдачи запросов igmp-query коммутатором в данной VLAN.
no ip igmp snooping querier enable		Отключает поддержку выдачи запросов igmp-query коммутатором в данной VLAN.
ip igmp snooping querier version {**2** | **3**}	-/IGMPv3	Устанавливает версию IGMP-протокола, на основании которой будут формироваться IGMP-query запросы.
no ip igmp snooping querier version		Устанавливает значение по умолчанию.

Команды режима EXEC

Все команды доступны только для привилегированного пользователя.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.83 – Команды режима EXEC

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

Примеры выполнения команд

Включить функцию IGMP snooping на коммутаторе. Для VLAN 6 разрешить автоматическое распознавание портов, к которым подключены многоадресные маршрутизаторы. Установить время ожидания сообщения IGMP Report – 360 сек. Задать период, в течение которого коммутатор ожидает многоадресные пакеты от группового маршрутизатора после изучения его адреса – 200 сек. Установить значение leave-таймера – 20 сек.

```
console# configure
console (config)# ip igmp snooping
console (config)# interface vlan 6
console (config-if)# ip igmp snooping mrouter learn-pim-dvmrp
console (config-if)# ip igmp snooping host-time-out 360
console (config-if)# ip igmp snooping mrouter-time-out 200
console (config-if)# ip igmp snooping leave-time-out 20
```

5.16.3 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 5.84 – Команды глобального режима конфигурирования

Команда	*Значение*	*Действие*
ipv6 mld snooping vlan <vlan>	vlan – 1..4094	

Команды режима конфигурирования интерфейса VLAN

Вид запроса командной строки режима глобального конфигурирования:

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

Таблица 5.85 – 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 MES3124 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 секунд	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 <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
ipv6 mld snooping	-	Включает MLD snooipng в данной VLAN
no ipv6 mld snooping		Отключает MLD snooping в данной VLAN
ipv6 mld snooping forbidden mrouter port <add|remove> <ethernet <port>**|port-channel** <group>**>**	port: [{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}]; group: [1..8]	Добавляет/удаляет правило, запрещающее регистрировать MLD-mrouter порты из списка
ipv6 mld snooping mrouter learn	-/включено	Изучать порты, подключенные к mrouter'у по MLD-query-пакетам
no ipv6 mld snooping mrouter learn		Не изучать порты, подключенные к mrouter'у по MLD-query-пакетам
ipv6 mld snooping mrouter ports <add|remove> <ethernet <port> **| port-channel** <group>**>**	port: [{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}]; group: [1..8]	Добавляет/удаляет список mrouter-портов
ipv6 mld snooping version <version>	version 1..2/2	Устанавливает версию протокола, по которой работает коммутатор
no ipv6 mld snooping version		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 {ethernet {port}|port-channel {group}}
console(config-if)#
```

Таблица 5.86 – Команды режима конфигурирования интерфейса Ethernet, группы интерфейсов

Команда	*Значение/Значение по умолчанию*	*Описание*
ipv6 mld join-group <ipv6_address>	ipv6_address – групповой адрес IPv6	Дает указание рассылать MLD-report сообщения на присоединение к *ipv6_address* группы с данного порта
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 порте коммутатора.
no ipv6 mld version		Восстанавливает значение по умолчанию

Таблица 5.87 – 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>	vlan 1..4094	Отображает информацию о конфигурации MLD-snooping для данной VLAN
show ipv6 mld snooping mrouter	-	Отображает информацию о mrouter-портах

5.17 Функции управления

5.17.1 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 5.88 – 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* [**password** *password*] [**level** *level*] [**encrypted**]	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 – задать зашифрованный пароль (например, пароль в зашифрованном виде, скопированный с другого устройства).
no username *name*		Удаляет пользователя из локальной базы данных
aaa accounting login 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 6.70).***

no aaa accounting login		Устанавливает значение по умолчанию.
aaa accounting dot1x 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 6.71).*** ***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		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 5.89 – 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 5.90 – 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 5.91 – 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 EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Все команды данного раздела доступны только для привилегированных пользователей.

Таблица 5.92 – Команды режима EXEC

Команда	***Действие***
show authentication methods	Показывает информацию об аутентификационных методах на коммутаторе. (Команда доступна только для привилегированного пользователя).
show users accounts	Показывает локальную базу данных пользователей и их привилегий. (Команда доступна только для привилегированного пользователя).
show accounting	Показывает информацию о настроенных методах ведения учета (аккаунта).

5.17.2 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 5.93 - Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
radius-server host {*ip-addr*| *hostname*} [**auth-port** *auth_port*] [**acct-port** *acct-port*] [**timeout** *timeout*] [**retransmit** *retries*] [**deadtime** *time*] [**key** *secret_key*] [**source** *source_ip-addr*] [**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	Добавляет указанный сервер в список используемых RADIUS серверов. - ip-addr – 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-addr - IPv4 или IPv6-адрес, используемый в качестве адреса источника, передаваемого в сообщениях протокола RADIUS; - priority – приоритет использования RADIUS-сервера (чем ниже значение, тем приоритетнее сервер); - type – тип использования RADIUS-сервера.
no radius-server host {*ip-addr*|*hostname*}	В случае отсутствия в команде параметров timeout, retries, time, secret_key, source_ip-addr для данного RADIUS-сервера используются значения настроенные с помощью команд указанных ниже (значения по умолчанию)	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_addr*	-	Задает определенный IPv4-адрес, используемый по умолчанию в качестве адреса источника передаваемого в сообщениях протокола RADIUS
no radius-server source-ip [*ip_addr***]**	-	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_addr*	-	Задает определенный IPv6-адрес, используемый по умолчанию в качестве адреса источника передаваемого в сообщениях протокола RADIUS
no radius-server source-ipv6 [*ip_addr***]**	-	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.

Команды режима EXEC

Вид запроса командной строки в режиме EXEC:

```
console#
```

Таблица 5.94 - Команды режима 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
```

```
start

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

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


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

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

5.17.3 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 5.95 - Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
tacacs-server host {*ip-addr*|*hostname***} [single-connection] [port** *port***] [timeout** *timeout***] [key** *secret_key***] [source** *source_ip-addr***] [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-addr – IP адрес TACACS-сервера; - hostname – сетевое имя TACACS-сервера; - single connection – в каждый момент времени иметь не больше одного соединения для обмена данными с TACACS-сервером; - port – номер порта для обмена данными с TACACS-сервером; - timeout - интервал ожидания ответа от сервера; - key – ключ для аутентификации и шифрования всего обмена данными TACACS; - source ip-addr – 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-addr* | *hostname***}**		Удаляет указанный сервер из списка используемых TACACS-серверов.
tacacs-server key [*key***]**	[0..128] символов/ по умолчанию ключ -	Устанавливает ключ, используемый по умолчанию, для аутентификации и шифрования всего обмена данными

	пустая строка	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-addr*	-	Задает IP-адрес коммутатора, используемый по умолчанию для обмена сообщениями с TACACS-сервером
no tacacs-server source-ip *source_ip-addr*	-	Устанавливает использование IP-адреса интерфейса коммутатора для обмена сообщениями с TACACS-сервером.

Команды режима EXEC

Вид запроса командной строки в режиме EXEC:

```
console#
```

Таблица 5.96 - Команды режима EXEC

Команда	*Значение*	*Действие*
show tacacs [*ip-addr*]	-	Отображает настройку и статистику для сервера TACACS+.

Примеры использования команд

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

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

5.17.4 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.

Коммутатор MES3124 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 5.97 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
snmp-server enable	По умолчанию поддержка протокола SNMP включена	Включить поддержку протокола SNMP.
no snmp-server enable		Отключает поддержку протокола SNMP.
snmp-server community *community* **[ro|rw|su]** [*ipv4-adrr| ipv6-addr*] [**view** *viewname*] **snmp-server community-group** *community groupname* [*ipv4-adrr| ipv6-addr*]	community: 1..20 символов viewname: 1..30 символов groupname: 1..30 символов	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; - 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*]		Удаляет параметры для строки сообщества.
snmp-server view *viewname OID* {**included|excluded**}	viewname: 1..30 символов	Создает или редактирует правило обозрения для SNMP – правило, разрешающее, 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* [**remote** *engineid-string*] [**auth-md5** *password* | **auth-sha** *password* | **auth-md5-key** *md5-des-keys* |	username: 1..24 символов groupname: 1..30 символов	Создает SNMPv3-пользователя. - username – имя пользователя; - groupname – имя группы; - engineid-string – идентификатор удаленного SNMP-устройства, которому пользователь принадлежит;

auth-sha-key *sha-des-keys*]	engineid-string: 5..32 символов password: 1..32 символа md5-des-keys: 16 или 32 байт sha-des-keys: 20 или 36 байт	- password – пароль для аутентификации и генерации ключа; - md5-des-keys – ключ md5; - sha-des-keys – ключ sha.
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*} *community* [**traps**|**informs**] [**1**|**2**] [**udp-port** *port*] [**filter** *filtername*] [**timeout** *seconds*] [**retries** *retries*]	hostname: 1..158 симолов 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; - 1/2 – определят тип сообщений trap – trap SNMPv1, или trap SNMPv2; - 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-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 симолов username: 1..24 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 SNMPv3-серверу. - noauth,auth,priv – тип аутентификации, используемый протоколом SNMP v3 (noauth – без аутентификации, auth – аутентификация без шифрования, priv – аутентификация с шифрованием); - port – UDP-порт SNMP-сервера; -seconds – период ожидания подтверждений перед повторной передачей сообщений inform; - retries – количество попыток передачи сообщений inform, при отсутствии их подтверждения.
no snmp-server v3-host {*ipv4-address*|*ipv6-address*|*hostname*} *username* [**traps**|**informs**]		Удаляет настройки для передачи сообщений уведомления inform и trap SNMPv3-серверу.
snmp-server engineID local {engineid-string | **default**}	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 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.

Команды режима EXEC

Команды данного раздела доступны только для привилегированных пользователей.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.98 – Команды режима 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 ip-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
```

5.17.5 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 5.99 – 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	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

	fevent: 0..65535 owner name: строка По умолчанию метод отбора переменных – absolute По умолчанию инструкция для генерации событий rising-falling	пересечении нисходящей границы; - type – метод отбора указанных переменных и подсчета значения для сравнения с границами: Метод **absolute** – абсолютное значение выбранной переменной будет сравнено с границей на конце исследуемого интервала; Метод **delta** – значение выбранной переменной при последнем отборе будет вычтено из текущего значения и разница будет сравнена с границами (разница между значениями переменной в конце и в начале контрольного интервала); - startup – инструкция для генерации событий на первом контрольном интервале. Определяет правила генерации аварийных событий для первого контрольного интервала путем сравнения отобранной переменной с одной, либо обеими границами: **rising** – генерировать единичное аварийное событие по восходящей границе, если значение отобранной переменной на первом контрольном интервале больше либо равно этой границе; **falling** – генерировать единичное аварийное событие по нисходящей границе, если значение отобранной переменной на первом контрольном интервале меньше либо равно этой границе; **rising-falling** – генерировать единичное аварийное событие по восходящей и/или нисходящей границе, если значение отобранной переменной на первом контрольном интервале больше либо равно восходящей границе, и/или меньше либо равно нисходящей границе; - **owner** – имя создателя аварийного события.
no rmon alarm *index*		Удаляет условие выдачи аварийных событий.
rmon table-size {history *entries* | **log** *entries***}**	history 20..32767/270 log 20..32767/100	Задает максимальный размер RMON-таблиц. - history – максимальное количество строк в таблице истории; - log – максимальное количество строк в таблице записей. ***Значение вступит в силу только после перезагрузки устройства.***
no rmon table-size {history | log}		Устанавливает значение по умолчанию.

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

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

```
console# configure
console(config)# interface {ethernet {port}|port-channel {group}}
console(config-if)#
```

Таблица 5.100 – Команды режима конфигурирования интерфейса Ethernet, группы интерфейсов

Команда	*Значение*	*Действие*
rmon collection history *index* **[owner** *name* **| buckets** *bucket_num***] [interval** *interval***]**	index: 1..65535; name: корректная строка; bucket-num: 1..50/50;	Включает формирование истории по группам статистики для базы данных (MIB) удаленного мониторинга. - index – индекс требуемой группы статистики; - name – владелец группы статистики; - bucket_num – значение, ассоциируемое с количеством

	interval: 1..3600/1800 сек	ячеек для сбора истории по группе статистики; - interval – период опроса для формирования истории.
no rmon collection history *index*		Выключает формирование истории по группам статистики для базы данных (MIB) удаленного мониторинга.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.101 – Команды режима EXEC

Команда	*Значение*	*Действие*
show rmon statistics {ethernet *port*| **port-channel** *group***}**	port {1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}; group {1..8}	Показывает статистику интерфейса Ethernet либо группы портов, используемую для удаленного мониторинга.
show rmon collection history [ethernet *port*| **port-channel** *group***]**	port {1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}; group {1..8}	Отображает информацию по запрашиваемым группам статистики.
show rmon history *index* **{throughput | errors | other} [period** *period***]**	index: 1..65535 period: 0..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 первого устройства в стеке:

```
console# show rmon statistics ethernet 1/g10
```

```
Port 1/g10
Dropped: 8
Octets: 878128 Packets: 978
Broadcast: 7 Multicast: 1
CRC Align Errors: 0 Collisions: 0
Undersize Pkts: 0 Oversize Pkts: 0
Fragments: 0 Jabbers: 0
64 Octets: 98 65 to 127 Octets: 0
128 to 255 Octets: 0 256 to 511 Octets: 0
512 to 1023 Octets: 491 1024 to 1518 Octets: 389
```

Таблица 5.102 - 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 history ethernet 1/g8
```

```
Index Interface Interval Requested Samples Granted Samples        Owner
----- --------- -------- ----------------- --------------- --------------------
  1      1/g8     300           50                50                Eltex
```

Таблица 5.103 - 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: 1/g1             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 5.104 - 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 5.105 - Описание результатов

Параметр	*Описание*
Index	Индекс, уникально идентифицирующий запись
OID	OID контролируемой переменной
Owner	Пользователь, создавший запись.

```
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 5.106 - 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 5.107 – 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 5.108 – Описание результатов

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

5.17.6 Списки доступа ACL для управления устройством

Программное обеспечение коммутатора MES3124 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 5.109 – 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 5.110 – Команды режима конфигурирования списка доступа для управления

Команда	*Значение*	*Действие*
permit [**ethernet** *port* | **vlan** *vlan-id* **/ port-channel** *group*] [**service** *service*]	port: [{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}]; group: [1..8]; VLAN ID [1..4094]	Задает разрешающее условие для управляющего списка доступа. - service – тип доступа – Telnet, SSH, SNMP.
permit ip-source {*ipv4-address* | *ipv6-address/ prefix-length*} [**mask** *mask*] [**ethernet** *port* | **vlan** *vlan-id* **/ port-channel** *group*] [**service** *service*]		
deny [**ethernet** *port* | **vlan** *vlan-id* **/ port-channel** *group*] [**service** *service*]	port: [{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}]; group: [1..8]; VLAN ID [1..4094]	Задает запрещающее условие для управляющего списка доступа. - service – тип доступа – Telnet, SSH, SNMP.
deny ip-source {*ipv4-address* | *ipv6-address/ prefix-length*} [**mask** *mask*] [**ethernet** *port* | **vlan** *vlan-id* **/ port-channel** *group*] [**service** *service*]		

Команды режима EXEC

Все команды доступны только для привилегированного пользователя.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.111 – Команды режима 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.

5.17.7 Настройка локальной и удаленной консоли.

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 5.112 – 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 5.113 – 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 5.114 – 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 5.115 – 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 AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTn
RwPWlAl4kpqIw9GBRonZQZxjHKcqKL6rMlQ+ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+V
```

```
u4GRfpSwoQUvV35LqJJk67IOU/zfwOl1gkTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSqmuSn
/Wd05iDX2IExQWu08licglk02LYciz+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY0ZCk0N
/W9a/tnkm1shRE7Di71+w3fNiOA6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+Rmt5nhh
qdAtN/4oJfce166DqVX1gWmNzNR4DYDvSzg0lDnwCAC8Qh

Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

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 5.116 – 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 5.117 – 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 5.118 – Команды режима EXEC

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

5.18 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 5.119 - 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 {*ipaddr*|*host***} [port** *port***] [severity** *level***] [facility** *facility***] description** *text***]**	host {1..158} символов; port [1..65535]/514; level [см. табл. 6.101]; facility [local0..7]/ local7; text [1..64] символа	Включает передачу аварийных и отладочных сообщений на удаленный SYSLOG сервер. - ipaddr – 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 {*ipaddr*|*host***}**		Удаляет выбранный сервер из списка используемых SYSLOG-серверов.
logging console *level*	level [см. табл. 6.101] 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 [см. табл. 6.101] Значение по умолчанию - informational	Включает передачу аварийных или отладочных сообщений выбранного уровня важности во внутренний буфер.
no logging buffered	-	Выключает передачу аварийных или отладочных сообщений во внутренний буфер.

logging buffered size *size*	20-400/200	Изменяет количество сообщений, запоминаемых во внутреннем буфере. Новое значение размера буфера применится после перезагрузки устройства.
no logging buffered size		Устанавливает значение по умолчанию.
logging file *level*	level [см. табл. 6.101] Значение по умолчанию - errors	Включает передачу аварийных или отладочных сообщений выбранного уровня важности в файл журнала.
no logging file	-	Выключает передачу аварийных или отладочных сообщений в файл журнала.
aaa logging login	-	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	По умолчанию регистрация включена	Включает регистрацию событий файловой системы.
no file-system logging copy		Выключает регистрацию событий файловой системы.
management logging deny	По умолчанию регистрация включена	Включает регистрацию событий доступа управления.
no management logging deny		Выключает регистрацию событий доступа управления.

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

Таблица 5.120 – 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 EXEC

Все команды доступны только для привилегированных пользователей.

Вид запроса командной строки в режиме EXEC:

```
console#
```

Таблица 5.121 - Команда режима 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
```

5.19 Зеркалирование (мониторинг) портов

Функция зеркалирования портов предназначена для контроля сетевого трафика путем пересылки копий входящих и/или исходящих пакетов с одного или нескольких контролируемых портов на один контролирующий порт.

К контролирующему порту применяются следующие ограничения:

- Порт не может быть контролирующим и контролируемым портом одновременно;
- Порт не может быть членом группы портов;
- IP-интерфейс 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 5.122 - 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

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet:

```
console# configure
console(config)# interface ethernet port
console(config-if)#
```

Данные команды нельзя выполнять в режиме конфигурирования диапазона интерфейсов Ethernet.

Таблица. 5.123 - Команды доступные в режиме конфигурирования интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
port monitor *{src-port}* **[rx|tx]**	**{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}**	Включает функцию мониторинга на настраиваемом интерфейсе. Данный интерфейс будет контролирующим портом для указанного в команде контролируемого порта. - src-port – контролируемый порт; - rx – копировать пакеты принятые контролируемым портом; - tx – копировать пакеты, переданные контролируемым портом; При отсутствии параметра rx/tx с контролируемого порта копируются все пакеты.
no port monitor *{src-port}*		Выключает функцию мониторинга на настраиваемом интерфейсе. Данный интерфейс больше не будет контролирующим портом для указанного в команде контролируемого порта.
port monitor vlan *{id}*	1..4096	Включает функцию мониторинга на настраиваем интерфейсе. Данный интерфейс будет контролирующим портом для указанной VLAN. ***Порт мониторинга не должен принадлежать к настраиваемой VLAN***
no port monitor vlan *{id}*		Удаляет указанную VLAN из мониторинга.

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console#
```

Таблица. 5.124 – Команды, доступные в режиме EXEC

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

Примеры выполнения команд

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

```
console# configure
console(config)# interface ethernet g13
console(config-if)# port monitor g18
```

- Вывести информацию по контролирующим и контролируемым портам.

```
console# show ports monitor
```

```
Source Port Destination Port  Type     Status
----------- ---------------- ------- ----------
    g18           g13         RX,TX   notReady
```

5.20 Функции диагностики физического уровня

Сетевой коммутатор MES3124 содержит аппаратные и программные средства для тестирования медных кабелей, подключенных к электрическим портам устройства, и оптического трансивера.

5.20.1 Диагностика медного кабеля

Все команды диагностики доступны в режиме EXEC. Запрос командной строки в режиме EXEC имеет следующий вид:

```
console#
```

Таблица. 6.125 - Команды диагностики медного кабеля

Команда	*Значение*	*Действие*
test copper-port tdr *interface*	{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}	Выполняет виртуальное тестирование кабеля для указанного интерфейса (команда доступна только для привилегированного пользователя).
show copper-port tdr [*interface***]**		Отображает результаты последнего виртуального тестирования кабеля для указанного интерфейса (если номер порта не задан, то команда выполняется для всех портов).
show copper-port cable-length [*interface***]**		Отображает предположительную длину кабеля, подключенного к указанному интерфейсу (если номер порта не задан, то команда выполняется для всех портов). ***Интерфейс должен быть активным и работать в режиме 100Мбит/с или 1000Мбит/с.***

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

Примеры выполнения команд:

- Протестировать порт 23 первого устройства в стеке:

```
console# test copper-port tdr g23
```

```
.01-Oct-2006 01:38:14 %LINK-W-Down:  Vlan 1
01-Oct-2006 01:38:14 %LINK-W-Down:  g23
```

```
.
Cable on port g23 is good
sandbox1# 01-Oct-2006 01:38:17 %LINK-I-Up:  Vlan 1
01-Oct-2006 01:38:17 %LINK-I-Up:  g23
```

- Показать результаты последнего тестирования:

```
console# show copper-ports tdr
```

```
   Port       Result    Length [meters]             Date
----------- ----------- ---------------- -------------------------
    g1      Not tested
    g2      Not tested
    g3      Not tested
    g4      Not tested
    g5      Not tested
    g6      Not tested
    g7      Not tested
    g8      Not tested
    g9      Not tested
    g10     Not tested
    g11     Not tested
    g12     Not tested
    g13     Not tested
    g14     Not tested
    g15     Not tested
    g16     Not tested
    g17     Not tested
    g18     Not tested
    g19     Not tested
    g20     Not tested
    g21     Not tested
    g22     Not tested
    g23         OK
    g24     Not tested
```

5.20.2 Диагностика оптического трансивера

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

```
console#
```

Таблица. 6.126 – Команда диагностики оптического трансивера

Команда	***Значение***	***Действие***
show fiber-ports optical-transceiver [*interface***] [detailed]**	{1/g(1-48)..8/g(1-48)}, g1..g24	Отображает результаты диагностики оптического трансивера. - detailed – подробная диагностика

Пример выполнения команды:

```
console# show fiber-ports optical-transceiver g11
```

```
   Port       Temp  Voltage Current Output Input LOS
                                    Power  Power
----------- ------ ------- ------- ------ ----- ---
    g11      N/S     N/S     N/S    N/S    N/S  N/S

 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
```

Таблица 6.127 – 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 коммутатора MES3124 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# configure
console(config)# interface {ethernet {port}|port-channel {group}}
console(config-if)#
```

Таблица 5.128 – 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-addr*	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-addr***]**		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. Переизучение 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 5.129 – Команды режима EXEC

Команда	*Значение*	*Действие*
show ports security {**ethernet** *port* | **port-channel** *group*}	port {1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}; group {1..8}	Показывает настройки функции безопасности на выбранном интерфейсе.
set interface active {ethernet *port* | **port-channel** *group*}	port {1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}; group {1..8}	Активизирует интерфейс, отключенный функцией защиты порта (команда доступна только для привилегированного пользователя).

Примеры выполнения команд

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

```
console# configure
console(config)# interface ethernet 1/g15
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)

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 5.130 – Команды режима глобального конфигурирования

Команда	*Значение/ Значение по умолчанию*	*Действие*
dot1x system-auth-control	-	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 6.131 – Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
dot1x port-control {auto | force-authorized | force-unauthorized}	-/ force-authorized	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.
no dot1x port-control		Устанавливает значение по умолчанию.
dot1x re-authentication	-/ периодические повторные проверки подлинности выключены	Включает периодические повторные проверки подлинности (переаутентификацию) клиента.
no dot1x re-authentication	-	Выключает периодические повторные проверки подлинности (переаутентификацию) клиента.
dot1x timeout re-authperiod *period*	30..4294967295/ 3600 сек	Устанавливает период между повторными проверками подлинности.
no dot1x timeout re-authperiod	<300-4294967295>	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	<0-65535>	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	<30-65535>	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	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	Устанавливает период, в течение которого коммутатор ожидает ответа от сервера аутентификации.
no dot1x timeout server-timeout	<1-65535>	Устанавливает значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Все команды данного раздела доступны только для привилегированных пользователей.

Таблица 5.132 – Команды режима EXEC

Команда	***Значение***	***Действие***
dot1x re-authenticate [ethernet *port***]**	{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}	Вручную осуществляет повторную проверку подлинности указанного порта в команде, либо всех портов, поддерживающих 802.1X.
show dot1x ethernet [ethernet *port***]**	{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}	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 ethernet *port*	{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}	Показывает статистику по 802.1X для выбранного интерфейса.

Примеры выполнения команд

- Включить режим аутентификации 802.1X на коммутаторе. Использовать RADIUS-сервер для проверки подлинности клиентов на интерфейсах IEEE 802.1X. Для 18 интерфейса Ethernet использовать режим аутентификации 802.1x.

```
console# configure
console(config)# dot1x system-auth-control
console(config)# aaa authentication dot1x default radius
console(config)# interface ethernet 1/g18
console(config-if)# dot1x port-control auto
```

- Показать состояние 802.1X для коммутатора, для 13 интерфейса Ethernet и для пользователя Oleg.

```
console# show dot1x
```

```
802.1x is enabled

Port           Admin        Oper           Reauth      Reauth       Username
              Mode         Mode           Control      Period
---------     -----------  --------       ----------  ------       ------------
1/g1          Auto         Authorized      Ena          3600       Eltex
1/g2          Force-auth   Unauthorized*  Dis          3600       Andrew

* Port is down or not present
```

```
console# show dot1x ethernet 1/g13
```

```
802.1x is enabled

Port           Admin        Oper          Reauth       Reauth       Username
              Mode         Mode     Control      Period
---------     -----------  --------     ----------  ------        ------------
1/g13         Auto         Unauthorized  Ena         3600          Boris

Quiet period: 60 Seconds
Tx period:           30 Seconds
Max req:             2
Supplicant timeout: 30 Seconds
Server timeout:             30 Seconds
Session Time (HH:MM:SS): 07:39:27
MAC Address:         00:00:02:AA:9B:65
Authentication Method:     Remote
Termination Cause:   Supplicant logoff
Authenticator State Machine
State:               HELD
Backend State Machine
State:               IDLE
Authentication success:     7
Authentication fails:       0
console# show dot1x users username Oleg

Username: Oleg
Port           Username     Session      Auth         MAC           VLAN  Filter ID
                            Time         Method      Address
---------      ---------    -----------  -------    ------------   ----- --------
1/g16          Oleg         04:56:14     Remote    0000.0479.9886   2     ACL-1
```

Таблица 5.133 – Описание результатов выполнения команд

Параметр	***Описание***
Port	Номер порта.
Admin mode	Режим аутентификации 802.1X: Force-auth, Force-unauth, Auto.
Oper mode	Операционный режим порта: авторизованный, неавторизованный, либо выключенный (Authorized, Unauthorized, Down).
Reauth Control	Контроль переаутентификации.
Reauth Period	Период между повторными проверками подлинности.
Username	Имя пользователя при использовании 802.1X. Если порт авторизован, то отображается имя текущего пользователя. Если порт не авторизован, то отображается имя последнего успешно авторизованного пользователя на порту.
Quiet period	Период, в течение которого коммутатор остается в состоянии молчания после неудачной проверки подлинности.
Tx period	Период, в течение которого коммутатор ожидает ответ на запрос либо идентификацию по протоколу EAP от клиента, перед повторной отправкой запроса.
Max req	Максимальное число попыток передачи запросов протокола EAP клиенту перед новым запуском процесса проверки подлинности.
Supplicant timeout	Период между повторными передачами запросов протокола EAP клиенту.
Server timeout	Период, в течение которого коммутатор ожидает ответа от сервера аутентификации.
Session Time	Время подключения пользователя к устройству.
Mac address	MAC-адрес пользователя.
Authentication Method	Метод аутентификации установленной сессии.
Termination Cause	Причина закрытия сессии.
State	Текущее значение автомата состояний определителя подлинности и выходного автомата состояний.
Authentication success	Количество полученных сообщений об успешной аутентификации от сервера.
Authentication fails	Количество полученных сообщений о неуспешной аутентификации от сервера.
VLAN	Группа VLAN назначенная пользователю.
Filter ID	Идентификатор группы фильтрации.

- Показать статистику по 802.1X для интерфейса Ethernet 13.

```
console# show dot1x statistics ethernet 1/g13
```

```
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 5.134 – 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.

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 5.135 – 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.

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки в режиме конфигурирования интерфейса Ethernet:

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

Таблица 5.136– Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
dot1x multiple-hosts [authentication]	-/наличие нескольких клиентов запрещено	Разрешает наличие нескольких клиентов на авторизованном порту 802.1X. Для этих портов должен быть включен режим аутентификации 802.1x командой **dot1x port-control auto**. Если в команде указано ключевое слово authentication, то каждый подключенный клиент должен аутентифицироваться индивидуально (режим multiple sessions), иначе достаточно аутентификации одного клиента (режим multiple hosts). ***Для неаутентифицированных VLAN режим multiple hosts всегда включен.***
no dot1x multiple-hosts		Устанавливает значение по умолчанию.
dot1x single-host-violation {**forward** |**discard** |**discard-shutdown**} **trap** [*seconds*]	1..1000000 сек/ передача SNMP trap выключена. Значение по умолчанию - discard	Задает действие, которое необходимо выполнить, когда станция, чей MAC-адрес отличается от MAC-адреса клиента, осуществляет попытку доступа к интерфейсу. - forward - блокирует функцию изучения новых адресов для интерфейса. Пакеты с MAC-адресом, отличным от MAC-адреса клиента, пересылаются; -discard – пакеты с MAC-адресом, отличным от MAC-адреса клиента, отбрасываются; -discard-shutdown – порт выключается, пакеты с MAC-адресом, отличным от MAC-адреса клиента, отбрасываются; - trap - задает частоту генерируемых сообщений протокола SNMP trap при поступлении несанкционированных пакетов. ***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.

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 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 5.137 – 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 EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.138 – Команды режима EXEC

Команда	*Значение*	*Действие*
show dot1x advanced [ethernet *port***]**	{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}	Показывает дополнительные сведения о настройках протокола 802.1x (команда доступна только для привилегированного пользователя).
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 5.139 - 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 5.140 – 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 MES3124

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 5.141 – 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# configure
console(config)# interface {ethernet {port}|port-channel {group}}
console(config-if)#
```

Таблица 5.142 – 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 EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.143 – Команды режима EXEC

Команда	*Значение*	*Действие*
ip dhcp snooping binding *mac-address vlan-id ip-address* **{ethernet** *port* **| port-channel** *group***}** **expiry** *period*	port {1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}; vlan-id 1..4094; group {1..8};	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 пошлёт запрос на DHCP-сервер на обновление. Таймер обнуляется в случае получения от клиента запроса на обновление (команда доступна только для привилегированного

	period 10..4294967295	пользователя). - period – время жизни записи.
no ip dhcp snooping binding *mac-address vlan-id*		Удаляет из файла (базы) контроля протокола DHCP соответствие MAC-адреса клиента и группы VLAN (команда доступна только для привилегированного пользователя).
clear ip dhcp snooping database	-	Очищает файл (базу) контроля протокола DHCP (команда доступна только для привилегированного пользователя).
show ip dhcp information option	-	Показывает информацию об использовании опции 82 протокола DHCP.
show ip dhcp snooping [ethernet port | port-channel group]	port [{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}]; group [1..8]	Показывает конфигурацию функции контроля протокола DHCP.
show ip dhcp snooping binding [mac-address *mac-address***] [ip-address** *ip-address***] [vlan** *vlan***] [ethernet** *port* **| port-channel** *group***]**	port [{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}]; vlan-id [1..4094]; group [1..8]	Показывает соответствия из файла (базы) контроля протокола DHCP.

Примеры выполнения команд

- Разрешить использование DHCP опции 82:

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

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

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

```
DHCP snooping is globally enabled
DHCP snooping is configured on following VLANs: 2, 5
DHCP snooping database: enabled
Option 82 on untrusted port is allowed
Verification of hwaddr field is enabled

Interface            Trusted
-----------    ------------
1/g17                yes
```

5.21.4 Защита IP-адреса клиента (IP-source Guard)

Функция защиты IP-адреса (IP Source Guard) предназначена для фильтрации трафика, принятого с интерфейса, на основании таблицы соответствий DHCP snooping и статических соответствий IP Source Guard. Таким образом, IP Source Guard позволяет бороться с подменой IP-адресов в пакетах.

Поскольку функция контроля защиты IP-адреса использует таблицы соответствий DHCP snooping, имеет смысл использовать данную функцию, предварительно настроив и включив DHCP snooping.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.144 – Команды режима глобального конфигурирования

Команда	*Значение*	*Действие*
ip source-guard	По умолчанию функция выключена	Включает функцию защиты IP-адреса клиента для всего коммутатора.
no ip source-guard		Выключает функцию защиты IP-адреса клиента для всего коммутатора.
ip source-guard binding *mac-address vlan-id ip-address* **{ethernet** *port* **| port-channel** *group***}**	port {1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}; vlan-id 1..4094; group {1..8}	Создание статической записи в таблице соответствия между IP-адресом клиента, его MAC-адресом и группой VLAN для указанного в команде интерфейса.
no ip source-guard binding *mac-address vlan-id*		Удаление статической записи в таблице соответствия.
ip source-guard tcam retries-freq {*seconds* | **never**}	{10-600, never}/60 сек	Задает частоту обращения устройства к внутренним ресурсам с целью записи в память неактивных защищенных IP-адресов. - never – запрещает запись в память неактивных защищенных IP-адресов.
no ip source-guard tcam retries-freq		Устанавливает значение по умолчанию.

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

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

```
console# configure
console(config)# interface {ethernet {port}|port-channel {group}}
console(config-if)#
```

Таблица 5.145 – Команды режима конфигурирования интерфейса Ethernet, группы интерфейсов

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.146 – Команды режима EXEC

Команда	*Значение*	*Действие*
ip source-guard tcam locate	–	Вручную запускает процесс обращения устройства к внутренним ресурсам с целью записи в память неактивных защищенных IP-адресов. Команда доступна только для

		привилегированного пользователя.
show ip source-guard configuration [ethernet *port* **/ port-channel** *group***]**	port [1/g(1-24)..8/g(1-24), g1..g24]; group [1..8]	Команда отображает настройку функции защиты IP-адреса на выбранном, либо на всех интерфейсах устройства.
show ip source-guard status [mac-address *mac-address***] [ip-address** *ip-address***] [vlan** *vlan***] [ethernet** *port* **/ port-channel** *group***]**	port [{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}]; vlan-id [1..4094]; group [1..8]	Команда отображает статус функции защиты IP-адреса для указанного интерфейса, IP-адреса, MAC-адреса или группы VLAN.

Примеры выполнения команд

- Показать настройку функции защиты IP-адреса для всех интерфейсов:

```
console# show ip source-guard configuration
```

```
IP source guard is globally enabled.

Interface        State
---------       ------
1/g4           Enabled
1/g21          Enabled
1/g22          Enabled
```

- Включить функцию защиты IP-адреса для фильтрации трафика на основании таблицы соответствий DHCP snooping и статических соответствий IP Source Guard. Создать статическую запись в таблице соответствия для интерфейса Ethernet 12 первого устройства в стеке: IP-адрес клиента – 192.168.16.14, его MAC-адрес – 00:60:70:4A:AB:AF. Интерфейс в 3-й группе VLAN:

```
console# configure
console(config)# ip dhcp snooping
console(config)# ip source-guard
console(config)# ip source-guard binding 0060.704A.ABAF 3 192.168.16.14
ethernet 1/g12
```

5.21.5 Контроль протокола ARP (ARP Inspection)

Функция контроля протокола **ARP (ARP Inspection)** предназначена для защиты от атак с использованием протокола ARP (например, ARP-spoofing – перехват ARP-траффика). 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 5.147 – 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 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.
show ip arp inspection [ethernet *port* **/ port-channel** *group***]**	port [{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}]; group [1..8]	Показывает конфигурацию функции контроля протокола ARP Inspection на выбранном интерфейсе, либо на всех интерфейсах.
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# configure
console(config)# interface {ethernet {port}|port-channel {group}}
console(config-if)#
```

Таблица 5.148 – 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 5.149 – 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 6.150 – Команды режима EXEC

Команда	*Значение*	*Действие*
show ip arp inspection [ethernet *port* **/ port-channel** *group***]**	Port [{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}]; group [1..8]	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).

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 посредника

Коммутатор MES3124 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 5.151 – Команды режима глобального конфигурирования

Команда	*Значение*	*Действие*
ip dhcp relay enable	По умолчанию агент выключен	Включение функций DHCP Relay агента на коммутаторе.
no ip dhcp relay enable		Выключение функций DHCP Relay агента на коммутаторе.
ip dhcp relay address *ip-addr*	Может быть задано до 8-ми серверов	Задаёт IP-адрес доступного DHCP-сервера для DHCP Relay агента.
no ip dhcp relay address [*ip-addr*]		Удаляет IP-адрес из списка DHCP-серверов для DHCP Relay агента.

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 5.152 – 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 5.153– 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 5.154 – Команды для создания и конфигурирования списков ACL

Команда	*Значение*	*Действие*
ip access-list *access-list*	0..32 символа	Создание нового 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 *access-list*		Удаление списка ACL для адресации IPv4.
ipv6 access-list *access-list*		Создание нового 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 *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 *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.

Команды режима конфигурирования интерфейса Ethernet, группы портов.

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

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

Таблица 5.155 – 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. Для удаления списка с интерфейса используется отрицательная форма no этой команды.

Команды режима EXEC

Команды для просмотра списков ACL доступны только для привилегированных пользователей в режиме EXEC.

Командная строка в режиме EXEC имеет вид:

```
console#
```

[1] В текущей версии программного обеспечения не поддерживается

Таблица 5.156 – Команды для просмотра списков ACL

Команда	*Значение*	*Действие*
show access-lists [*access-list***]**	0..32 символа	Показывает списки ACL, созданные на коммутаторе.
show interfaces access-lists [ethernet *port* **| port-channel** *group***]**	port [{1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}]; group [1..8]	Показывает списки ACL назначенные интерфейсам.

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 access-list`. Например, для создания списка ACL под названием EltexAL необходимо выполнить следующие команды:

```
console#
console# configure
console(config)# ip access-list EltexAL
console(config-ip-al)#
```

Таблица 5.157 – 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**, **idrp**, **rsvp**, **gre**, **esp**, **ah**, **eigrp**, **ospf**, **ipip**, **pim**, **l2tp**, **isis**, либо числовое значение протокола, в диапазоне 0 – 255.
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 еденицы. 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 еденицы. Маска используется аналогично маске **source-wildcard**.
dscp	Поле DSCP в заголовке L3	Определяет значение DSCP-поля diffserv. Возможные коды сообщений поля **dscp:** 0 – 63.
ip-precedence	Приоритет IP	Определяет приоритет IP-трафика.
icmp-type	-	Тип сообщений протокола ICMP, используемый для фильтрации ICMP-пакетов. Возможные типы сообщений поля **icmp-type:** *echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-*

		advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain-name-request, domain-name-reply, skip, photuris, либо числовое значение типа сообщения, в диапазоне 0 – 255.
icmp-code	Код сообщения протокола ICMP	Код сообщений протокола ICMP, используемый для фильтрации ICMP-пакетов. Возможные коды сообщений поля **icmp-code:** 0 – 255.
igmp-type	Тип сообщения протокола IGMP	Тип сообщений протокола IGMP, используемый для фильтрации пакетов IGMP. Возможные типы сообщений поля **igmp-type:** *host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3*, либо числовое значение типа сообщения, в диапазоне 0 – 255.
destination-port	UDP/TCP-порт назначения	Возможные значения поля 0 – 65535.
source-port	UDP/TCP-порт источника	Возможные значения поля 0 – 65535.
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**.**

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 5.158 - Команды, используемые для настройки ACL списков на основе IP-адресации

Команда	***Действие***
permit **{***protocol***}** **{any|{***source source-wildcard***}}** **{any|{***destination destination-wildcard***}}** **[dscp** *number* **|** **ip-precedence** *number***]**	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** *number* **|** **ip-precedence** *number***]**	Добавляет разрешающую запись фильтрации для протокола ICMP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit-igmp **{any|{***source source-wildcard***}}** **{any|{***destination destination-wildcard***}}** **{any|***igmp-type***}** **[dscp** *number* **|** **ip-precedence** *number***]**	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** *number* **|** **ip-precedence** *number***] [flags** *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** *number* **|** **ip-precedence** *number***]**	Добавляет разрешающую запись фильтрации для протокола UDP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
deny [disable-port] **{any/** *protocol***}** **{any|{***source source-wildcard***}}** **{any|{***destination destination-wildcard***}}** **[dscp** *number* **|** **ip-precedence** *number***]**	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.
deny-icmp [disable-port] {any|{*source source-wildcard***}}** **{any|{***destination destination-wildcard***}}** **{any|***icmp-type***}** **{any|***icmp-code***}** **[dscp** *number* **| ip-precedence** *number***]**	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.
deny-igmp [disable-port] {any|{*source source-wildcard***}}** **{any|{***destination destination-wildcard***}}** **{any|***igmp-type***}** **[dscp** *number* **|** **ip-precedence** *number***]**	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.
deny-tcp [disable-port] {any|{ *source source-wildcard***}}** **{any/***source-port***}** **{any|{** *destination destination-wildcard***}}** **{any/*destination-port*}** **[dscp** *number* **|** **ip-precedence** *number***] [flags** *list-of-flags***]**	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.
deny-udp [disable-port] {any|{ *source source-wildcard***}}** **{any/** *source-port***} {any|{***destination destination-wildcard***}} {any/***destination-port***}** **[dscp** *number* **|** **ip-precedence** *number***]**	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[1]

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)#
```

[1] В текущей версии программного обеспечения не поддерживается

Таблица 5.159 – 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).
source-prefix/ length	Адрес отправителя и его длина	Определяет IPv6-адрес и длину префикса сети (количество старших бит адреса) источника пакета.
destination-prefix/ length	Адрес назначения и его длина	Определяет IPv6-адрес и длину префикса сети (количество старших бит адреса) назначения пакета.
dscp	Поле DSCP в заголоке L3	Определяет значение DSCP-поля diffserv. Возможные коды сообщений поля **dscp:** 0 – 63.
ip-precedence	Приоритет IP	Определяет приоритет IP-трафика (ip-precedence).
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 0 – 65535.
source-port	UDP/TCP-порт источника	Возможные значения 0 – 65535.
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**.**

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 5.160 – Команды, используемые для настройки ACL списков на основе IPv6-адресации

Команда	*Действие*
permit **{any|** *protocol***}** **{***source-prefix/length* **| any} {***destination-prefix/* *length* **| any}** **[dscp** *number* **|** **ip-precedence** *number***]**	Добавляет разрешающую запись фильтрации для протокола. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit-icmp **{***source-prefix/length* **| any} {***destination-prefix/* *length* **| any}**	Добавляет разрешающую запись фильтрации для протокола ICMP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.

{any|*icmp-type***}** **{any|***icmp-code***}** **[dscp** *number* **|** **ip-precedence** *number***]**	
permit-tcp **{***source-prefix/length* **| any} {any /** *source-port***} {***destination-prefix/* *length* **| any}{any/** *destination-port***}** **[dscp** *number* **|** **ip-precedence** *number***] [flags** *list-of-flags***]**	Добавляет разрешающую запись фильтрации для протокола TCP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit-udp **{***source-prefix/length* **| any}{any /** *source-port***} {***destination-prefix/* *length* **| any}** **{any/** *destination-port***} [dscp** *number* **|** **ip-precedence** *number***]**	Добавляет разрешающую запись фильтрации для протокола UDP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
deny [disable-port] **{any/** *protocol***}** **{***source-prefix/length* **| any}{***destination-prefix/* *length* **| any}** **[dscp** *number* **|** **ip-precedence** *number***]**	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.
deny-icmp [disable-port] {*source-prefix/length* **| any}{***destination-prefix/* *length* **| any}** **{any|***icmp-type***}** **{any|***icmp-code***}** **[dscp** *number* **|** **ip-precedence** *number***]**	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.
deny-tcp [disable-port] {*source-prefix/length* **|** **any} {any |** *source-port***} {***destination-prefix/* *length* **| any}{any|** *destination-port***} [dscp** *number* **| ip-precedence** *number***] [flags** *list-of-flags***]**	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.
deny-udp [disable-port] {*source-prefix/length* **| any}{any /** *source-port***} {***destination-prefix/* *length* **| any}** **{any/** *destination-port***} [dscp** *number* **|** **ip-precedence** *number***]**	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.

5.23.3 Конфигурирование ACL на базе MAC[1]

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 access-list`. Например, для создания списка ACL под названием MESmac необходимо выполнить следующие команды:

```
console#
console# configure
console(config)# ipv6 access-list MESmac
console(config-mac-al)#
```

[1] В текущей версии программного обеспечения не поддерживается

Таблица 5.161 - 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).
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 еденицы. Например, используя маску, можно определить для правила фильтрации диапазона MAC-адресов. Чтобы добавить в правило фильтрации все MAC-адрес начинающиеся на 00:00:02:AA.xx.xx, необходимо задать значение маски 0.0.0.0.FF.FF, то есть, согласно данной маске, последние 32 бита MAC-адреса будут не важны для анализа.
destination	Адрес назначения	Определяет MAC-адрес назначения пакета.
destination-wildcard	Битовая маска, применяемая к MAC-адресу назначения пакета	Маска определяет биты MAC-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны еденицы. Маска используется аналогично маске **source-wildcard**.
vlan	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 еденицы. 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)).
ethtype eth-type	Диапазон значений 0 – 0xFFFF	Ethernet тип фильтруемых пакетов в шестнадцатеричной записи.
inner-vlan	Диапазон значений 0 – 4095	Внутренний VLAN при фильтрации дважды тегированного трафика.
disable-port	-	Выключает порт, с которого был принят пакет, удовлетворяющий условиям команды запрета **deny.**

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

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

Таблица 5.162 – 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***] [ethtype** *eth-type***]** **[inner-vlan** *vlan-id***]**	Добавляет разрешающую запись фильтрации. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
deny [disable-port] {any|{*source source-wildcard***}** **{any|{** *destination destination- wildcard***}}** **[vlan** *vlan-id***]** **[cos** *cos cos-wildcard***] [ethtype** *eth-type***]** **[inner-vlan** *vlan-id***]**	Добавляет запрещающую запись фильтрации. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова disable-port, физический интерфейс, принявший такой пакет, будет выключен.

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 коммутаторе MES3124, позволяет организовать четыре очереди приоритета пакетов в зависимости от типа передаваемых данных.

5.24.1 Настройка QoS

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.163 – 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.***
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*	1..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 *queue-id threshold-percentage0 threshold-percentage1 threshold-percentage2*	queue-id: 1..8 threshold-percentage 0,1,2: 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 0 превышен, пакеты с соответствующим приоритетом сброса (DP) будут отбрасываться в течение всего времени, пока порог превышен. Несмотря на это, пакеты с приоритетом, соответствующим порогам 1 и 2, будут ставиться в очередь и отправляться до того времени, пока эти пороги не будут превышены.*** ***Действует только для режима qos advanced.***
no qos wrr-queue threshold *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* **to** *queue-id*	dscp-list: 0..63 queue-id: 1..8 Значения по умолчанию: DSCP: 0-7, очередь 1 DSCP: 8-15, очередь 2 DSCP: 16-23, очередь 3 DSCP: 24-31, очередь 4 DSCP: 32-39, очередь 5 DSCP: 40-47, очередь 6 DSCP: 48-55, очередь 7 DSCP: 56-63, очередь 8	Устанавливает соответствие между значениями DSCP входящих пакетов и очередями. - dscp-list – определяет до 8 значений DSCP, значения разделяются знаком пробела. ***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 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 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 5.164 – 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 5.165 – 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 5.166– Команды режима конфигурирования правила классификации

Команда	*Значение*	*Действие*
trust [cos | dscp | cos-dscp]	По умолчанию режим доверия не установлен	Определяет режим доверия к определенному типу трафика. Данной командой выбирается значение, которое QoS будет использовать в качестве внутреннего DSCP. - cos – в качестве внутреннего DSCP используется CoS; - dscp – в качестве внутреннего DSCP используется DSCP входящих пакетов (значение по умолчанию); - cos-dscp – в качестве внутреннего DSCP используется DSCP входящих пакетов, если это IP-пакеты, иначе CoS. ***Действует только для режима qos advanced.***
no trust		Устанавливает значение по умолчанию.
set **{dscp** *new-dscp* | **queue** *queue-id* | **cos** *new-cos*}	new-dscp: 0..63 queue-id: 1..8 new-cos: 0..7	Устанавливает новые значения для IP-пакета. ***Команда set является взаимоисключающей с командой trust для одной и той же стратегии policy-map.*** ***Стратегии policy-map, использующие команды set, trust или имеющий классификацию ACL, назначаются только для исходящих интерфейсов.*** ***Действует только для режима qos advanced.***
no set		Удаляет новые значения для IP-пакета.
police *committed-rate-kbps committed -burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit** }]	committed-rate: 3..12582912 кбит/с committed-burst: 3000..19173960 байт	Позволяет ограничить полосу пропускания канала и в то же время гарантировать определенную скорость передачи данных. При работе с полосой пропускания используется алгоритм маркированной «корзины». Задачей алгоритма является принятие решения: передать пакет или отбросить.

		Параметрами алгоритма являются – скорость поступления (CIR) маркеров в «корзину» и объём (CBS) «корзины». - committed-rate-kbps – среднее значение скорости трафика, кбит/с. Данная скорость гарантируется при передаче информации; - committed-burst-byte – размер сдерживающего порога в байтах; - drop – пакет будет отброшен, когда «корзина» переполнится; - policed-dscp-transmit – при переполнении «корзины», значение DSCP будет переопределено. ***Действует только для режима qos advanced.***
no police		Отключает регулирование скорости канала.
police agregate *aggregate-policer-name-list*	1..32 символов	Назначает правилу классификации трафика шаблон настроек, который позволяет ограничить полосу пропускания канала и в то же время гарантировать определенную скорость передачи данных. ***Действует только для режима qos advanced.***
no police agregate *aggregate-policer-name-list*		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 5.167 – 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..16769020 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..16769020 байт	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*	queue-id: 0-8	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.
qos dscp-mutation	-	Позволяет применить карту изменений dscp к совокупности dscp-доверенных портов. Использование карты изменений позволяет перезаписать значения dscp в IP-пакетах на новые значения. ***Применить карту изменений DSCP возможно только для входящего трафика доверенных портов.*** ***Действует только для режима qos basic.***
no qos dscp-mutation		Отменяет использование карты изменений dscp.
rate-limit *rate*	3500..1000000 кбит/с	Устанавливает ограничение скорости для входящего трафика. ***Ограничение скорости для конкретного порта может быть применено, только если к нему не применена команда port storm-control brodcast 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 cos override	-	Переписывает значение CoS тегированных пакетов на значение CoS по умолчанию. ***Данная команда доступна только в режиме конфигурирования интерфейса Ethernet.***
no qos cos override		Запрещает переназначение CoS для тегированных пакетов

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.168 – 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**] [**ethernet** *port* **/ port-channel** *group*]	Показывает QoS-параметры для интерфейса. - ethernet – номер Ethernet-интерфейса ({1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24}); - port-channel – номер группы портов (1..8); - 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.

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 14 и 16.

```
console#
console# configure
console(config)# ip access-list tcp_ena
console(config-ip-al)# permit tcp any any dscp 12
console(config-ip-al)# permit tcp any any dscp 16
console(config-ip-al)# exit
console(config)# qos advanced
console(config)# qos map dscp-queue  12  to  1
console(config)# qos map dscp-queue  16  to  2
console(config)# priority-queue out num-of-queues 1
console(config)# policy-map traffic
console(config-pmap)# class class1 access-group tcp_ena
console(config-pmap-c)# police 1000 200000 exceed-action drop
console(config-pmap-c)# exit
console(config-pmap)# exit
console(config)# interface ethernet 1/g14
console(config-if)# service-policy input
console(config-if)# exit
console(config)# interface ethernet 1/g16
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 5.169 – 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* {*interface* **| all**} {*queue* | **all}** { *dp* | **all}**	set: 1..2 interface: {1/g(1-24). 1/xg(1-4)..8/g(1-24). 8/xg(1-4), g1..g24, xg1..xg24} queue: 1..8 dp: {high | low} Значение по умолчанию: Set 1: все приоритеты, все очереди, высокий приоритет сброса. Set 2: все приоритеты, все очереди, низкий риоритет сброса.	Включает QoS -статистику для очередей. - set – определяет набор счетчиков; - dp – определяет приоритет сброса.
no qos statistics queues *set*		Отключает QoS-статистику для очередей.

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки режима конфигурирования интерфейса Ethernet:

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

Таблица 5.170 – 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 5.171 – Команды режима EXEC.

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

5.25 Работа в режиме маршрутизатора

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.

Функции статической маршрутизации доступны только при работе устройства в режиме маршрутизатора. Перевод устройства в режим маршрутизатора осуществляется командой set system mode router policy-based-vlans inactive в режиме EXEC. При включении данного режима часть функций, доступных в режиме коммутатора, становится недоступной.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 5.172 – 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 еденицы 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. ***Команда доступна только в режиме маршрутизатора.***
no ip route *prefix* {*mask* | *prefix-length*} [*gateway*]	Удаляет правило из таблицы статической маршрутизации. ***Команда доступна только в режиме маршрутизатора.***
ip proxy-arp	Включает режим проксирования ARP-запросов
no ip proxy-arp	Отключает режим проксирования ARP-запросов

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 5.173 – Команды режима EXEC

Команда	*Действие*
show ip route [connected | static | address *ip-addr* [*mask* | *prefix-length*] [**longer-prefixes**]**]**	Показывает таблицу маршрутизации, удовлетворяющую заданным критериям. – connected – подключенный маршрут, то есть маршрут, взятый с непосредственно подключенного и функционирующего интерфейса; – static – статический маршрут, прописанный в таблице маршрутизации.

Пример выполнения команды

- Показать таблицу маршрутизации:

```
console# show ip route
```

```
Maximum Parallel Paths: 2 (4 after reset)

Codes: C - connected, S - static
C 10.0.1.0/24 is directly connected, Vlan  1
S  10.9.1.0/24 [5/2]     via 10.0.1.2, 17:19:18, Vlan 12
S  10.9.1.0/24 [5/3]     via 10.0.2.2, Backup Not Active
S 172.1.1.1/32 [5/3]    via 10.0.3.1, 19:51:18, Vlan 12
```

Таблица 5.174 – Описание результата выполнения команды

Поле	*Описание*
C	Показывает происхождение маршрута: C – Connected (маршрут взят из непосредственно подключенного и функционирующего интерфейса), S – Static (статический маршрут, прописанный в таблице маршрутизации).
10.9.1.0/24	Адрес сети.
[5/2]	Первое значение в скобках – административная дистанция (степень доверия маршрутизатору, чем число выше, тем меньше доверие к источнику), второе число – метрика маршрута.
via 10.0.1.2	Определяет IP-адрес следующего маршрутизатора, через который проходит маршрут до сети.
00:39:08	Определяет время последнего обновления маршрута (часы, минуты, секунды)
Vlan 1	Определяет интерфейс, через который проходит маршрут до сети.

6 СЕРВИСНОЕ МЕНЮ, СМЕНА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

6.1 Меню Startup

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

Для входа в меню ***Startup*** необходимо прервать загрузку нажатием клавиши ***<Esc>*** или ***<Enter>*** в течение первых двух секунд после появления сообщения автозагрузки (по окончании выполнения процедуры POST).

```
Startup Menu

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

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

Для выхода из меню и загрузки устройства нажмите клавишу **<6>**, либо **<esc>**.

Если в течение 15 секунд (значение по умолчанию) не выбран ни один из пунктов меню, то загрузка устройства продолжится. Время ожидания можно увеличить с помощью команд консоли

Таблица 6.1 – Описание меню Startup

№	*Название*	*Описание*
<1>	**Download Software** Обновление программного обеспечения	Для загрузки программного обеспечения используется протокол X-Modem. При нажатии клавиши **<1>** на консоль будет выведено следующее сообщение: Downloading code using XMODEM. Теперь, когда устройство готово к приему файла, необходимо передать его при помощи протокола X-Modem. После приема файла устройство перезагрузится автоматически.
<2>	**Erase Flash File** Удаление содержимого флэш-памяти	Данная процедура используется для удаления конфигурации устройства. Для удаления файла нажать клавишу **<2>**, появится предупреждение (подтвердите нажатием клавиши **<y>**): Warning! About to erase a Flash file. Are you sure (Y/N) ? y Ввести имя для нового файла конфигурации (в примере ниже, имя – config): Write Flash file name (Up to 8 characters, Enter for none.):config File config (if present) will be erased after system initialization. Для возврата в меню ***Startup*** нажать клавишу **<enter>**. ==== Press Enter To Continue ==== **Для нового файла конфигурации имя должно быть отлично от имени конфигурации записанной на данный момент.**
<3>	**Password Recovery Procedure**	Данная процедура используется для восстановления утраченного пароля, она

	Восстановление пароля	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 **<4>** и ввести 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. Коммутатор MES3124 может 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 4.3
<6>	**Back** Выход из меню	Для выхода из меню и загрузки устройства нажмите клавишу **<6>**, либо **<esc>**.

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

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

6.2 Обновление программного обеспечения с сервера TFTP

Сервер TFTP должен быть запущен и настроен на компьютере, с которого будет загружаться программное обеспечение. Файлы с загрузочным и/или системным программным обеспечением должны быть доступны серверу. Компьютер с запущенным TFTP-сервером доступен коммутатору MES3124 (можно проконтролировать, выполнив на коммутаторе команду ping {A.B.C.D}, где A.B.C.D – IP-адрес компьютера).

Обновление программного обеспечения может осуществляться только привилегированным пользователем.

6.2.1 Обновление системного программного обеспечения

Загрузка устройства осуществляется из файла системного программного обеспечения (ПО), который хранится во флэш-памяти. При обновлении, новый файл системного ПО сохраняется в специально выделенной области памяти. При загрузке устройство запускает активный файл системного ПО. Выбор активного файла задается командой:

```
boot system [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
```

```
Unit           SW version   Boot version     HW version
----------    -------------   -------------------  -----------------
1             3.0.0.0          3.0.0.0          01.00.00
```

Процедура обновления ПО:

1. 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.

2. 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.

3. 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
```

```
Unit   Image  Filename   Version    Date                    Status
----   -----  ---------  ---------  ----------------------  -----------
1      1      image-1    3.0.0.0    17-Nov-2008  11:51:22   Active
1      2      image-2    3.0.0.0    28-Nov-2008  16:35:43   Not active*
```

Символом «*» отмечается файл программного обеспечения, который будет исполняться при последующей загрузке.

4. Перезагрузите коммутатор командой **reload.**

```
console# reload
```

```
This command will reset the whole system and disconnect your current
session. Do you want to continue (y/n) [n]?
```

Подтвердите перезагрузку вводом '**y**'.

6.2.2 Обновление загрузочного файла устройства (начального загрузчика)

Начальный загрузчик запускается сразу после включения питания устройства. Посредством загрузочного файла осуществляется процедура «тестирования системы при включении» (POST), распаковка и запуск файла системного ПО. При обновлении новый файл начального загрузчика сохраняется на flash на месте старого.

Для просмотра текущей версии загрузочного файла, работающего на устройстве, введите команду **show version**:

```
console# show version
```

```
Unit           SW version   Boot version     HW version
----------     -------------   -------------------  -----------------
1              3.0.0.0            3.0.0.0           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 10- 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 ethernet g(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: eltex@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.nsk.ru
http://eltex.nsk.ru/support/documentations
http://eltex.nsk.ru/forum

СВИДЕТЕЛЬСТВО О ПРИЕМКЕ И ГАРАНТИИ ИЗГОТОВИТЕЛЯ

Коммутатор магистрального уровня, коммутатор уровня агрегации MES 3124/MES3124F зав. № _____ соответствует требованиям технических условий ТУ6650-038-33433783-2009 и признан годным для эксплуатации.

Предприятие-изготовитель ООО «Предприятие «Элтекс» гарантирует соответствие коммутатора MES3124/MES3124F требованиям технических условий ТУ6650-038-33433783-2009 при соблюдении потребителем условий эксплуатации, установленных в настоящем руководстве.

Гарантийный срок 1 год.

Изделие не содержит драгоценных материалов.

Директор предприятия _____ Черников А. Н.
подпись Ф.И.О.

Начальник ОТК предприятия _____ Игонин С.И.
подпись Ф.И.О.