Комплексные решения для построения сетей

Ethernet-коммутаторы уровня доступа

MES14xx
MES24xx

Руководство по эксплуатации, версия ПО 10.1.8.2

Версия документа	Дата выпуска	Содержание изменений
Версия 4.3		Изменения в разделах: - 1.3 Основные технические характеристики - 4.3 Команды управления системой - 4.19.2 Электропитание по линиям Ethernet (PoE) - 4.20.4 DSLAM Controller Solution (DCS) Добавлены разделы: - 4.2 Фильтрация сообщений командной строки - 4.4 Команды для настройки параметров для задания паролей - 4.5.3 Команды для резирвирования конфигурации - 4.27 Режим отладки
Версия 4.2	08.2019	Изменения в разделах: - 3.4.2.4 Настройка параметров протокола SNMP для доступа к устройству - 4.7.2 Настройка VLAN и режимов коммутации интерфейсов - 4.15.1 Функция посредника протокола IGMP (IGMP Snooping) - 4.16.3 Протокол TACACS+ - 4.20.3 Контроль протокола DHCP и опция 82 - 4.20.4 DSLAM Controller Solution (DCS) - 4.22 Конфигурация PPPoE Intermediate Agent - 4.26 Обновление программного обеспечения с сервера TFTP Добавлены разделы: - 4.24 Конфигурация защиты от DOS-атак
Версия 4.1	06.2019	Изменения в разделах: – 4.9 Контроль широковещательного «шторма»
Версия 4.0	06.2019	Изменения в разделах: – Начальная настройка коммутатора – Настройка параметров протокола SNMP для доступа к устройству – Электропитание по линиям Ethernet (PoE)
Версия 3.0	03.2019	Добавлена информация об устройствах серии MES2408x и MES2428P Добавлены разделы: – Автоматическая настройка параметров коммутатора (Zero Touch Provisioning) – Selective Q-in-Q – Настройка IPv6-адресации – Настройка функции Layer 2 Protocol Tunneling (L2PT) – Настройка протокола OAM – MLD snooping – протокол контроля многоадресного трафика в IPv6 – Протокол TACACS+ – Электропитание по линиям Ethernet (PoE) – Протокол UDLD – Защита IP-адреса клиента (IP-source Guard)
Версия 2.0	01.2019	Вторая публикация.
Версия 1.0	12.2018	Первая публикация.
Версия программного обеспечения 10.1.8.2		

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 возможные обязательные параметры. Необходимо выбрать один из параметров.
«,» **«-»**	Данные знаки в описании команды используются для указания диапазонов.
«|»	Данный знак в описании команды обозначает «или».
«/»	Данный знак в описание команды указывает на значение по умолчанию.
Курсив Calibri	Курсивом Calibri указываются переменные или параметры, которые необходимо заменить соответствующим словом или строкой.
Полужирный курсив	Полужирным шрифтом выделены примечания и предупреждения.
<Полужирный курсив>	Полужирным курсивом в угловых скобках указываются названия клавиш на клавиатуре.
`Courier New`	Полужирным Шрифтом Courier New записаны примеры ввода команд.
`Courier New`	Шрифтом Courier New в рамке с тенью указаны результаты выполнения команд.

ПРИМЕЧАНИЯ И ПРЕДУПРЕЖДЕНИЯ

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

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

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

Коммутаторы серий MES24xx и MES14xx, могут использоваться на сетях крупных предприятий и предприятий малого и среднего бизнеса (SMB), в операторских сетях. Они обеспечивают высокую производительность, гибкость, безопасность, многоуровневое качество обслуживания (QoS).

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

1 ОПИСАНИЕ ИЗДЕЛИЯ

1.1 Назначение

Устройства серий MES14xx и MES24xx являются управляемыми коммутаторами, выполняющими свои коммутационные функции на канальном и сетевом уровнях модели OSI.

Сетевые коммутаторы MES1428 имеют в своём составе 24 электрических порта Fast Ethernet и 4 оптических порта Gigabit Ethernet для установки SFP-трансиверов (Combo-порты).

Сетевые коммутаторы MES2408x имеют в своём составе 8 электрических порта Gigabit Ethernet и 2 оптических порта Gigabit Ethernet для установки SFP-трансиверов.

Сетевые коммутаторы MES2428x имеют в своём составе 24 электрических порта Gigabit Ethernet и 4 оптических порта Gigabit Ethernet для установки SFP-трансиверов (Combo-порты).

1.2 Функции коммутатора

1.2.1 Базовые функции

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

Таблица 1 – Базовые функции устройства

Защита от блокировки очереди (HOL)	Блокировка возникает в случаях перегрузки выходных портов устройства трафиком от нескольких входных портов. Это приводит к задержкам передачи данных и потере пакетов.
Поддержка сверхдлинных кадров (Jumbo frames)	Способность поддерживать передачу сверхдлинных кадров, что позволяет передавать данные меньшим числом пакетов. Это снижает объем служебной информации, время обработки и перерывы.
Управление потоком (IEEE 802.3X)	Управление потоком позволяет соединять низкоскоростное устройство с высокоскоростным. Для предотвращения переполнения буфера низкоскоростное устройство имеет возможность отправлять пакет PAUSE, тем самым информируя высокоскоростное устройство о необходимости сделать паузу при передаче пакетов.

1.2.2 Функции при работе с MAC-адресами

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

Таблица 2 – Функции работы с MAC-адресами

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

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

1.2.3 Функции второго уровня сетевой модели OSI

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

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

Функция IGMP Snooping	Реализация протокола IGMP позволяет на основе информации, полученной при анализе содержимого IGMP-пакетов, определить, какие устройства в сети участвуют в группах многоадресной рассылки, и адресовать трафик на соответствующие порты.
Функция MLD Snooping	Реализация протокола MLD позволяет устройству минимизировать многоадресный IPv6-трафик.
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. Коммутаторы имеют функцию, позволяющую ограничить скорость передачи многоадресных и широковещательных кадров, принятых и переданных коммутатором.
Зеркалирование портов (Port Mirroring)	Зеркалирование портов позволяет дублировать трафик наблюдаемых портов, пересылая входящие и/или исходящие пакеты на контролирующий порт. У пользователя коммутатора есть возможность задать контролирующий и контролируемые порты и выбрать тип трафика (входящий и/или исходящий), который будет передан на контролирующий порт.
Изоляция портов (Protected ports)	Данная функция позволяет назначить порту его uplink-порт, на который безусловно будет перенаправляться весь трафик, обеспечивая тем самым изоляцию с другими портами (в пределах одного коммутатора), находящихся в этом же широковещательном домене (VLAN) в пределах одного коммутатора.
Private VLAN Edge	Данная функция позволяет изолировать группу портов (в пределах одного коммутатора), находящихся в одном широковещательном домене между собой, позволяя при этом обмен трафиком с другими портами, находящимися в этом же широковещательном домене, но не принадлежащими к этой группе.
Поддержка протокола STP (Spanning Tree Protocol)	Spanning Tree Protocol – сетевой протокол, основной задачей которого является приведение сети Ethernet с избыточными соединениями к древовидной топологии, исключающей петли. Коммутаторы обмениваются конфигурационными сообщениями, используя кадры специального формата, и выборочно включают и отключают передачу на порты.

Поддержка протокола RSTP (IEEE 802.1w Rapid spanning tree protocol)	Rapid (быстрый) STP (RSTP) – является усовершенствованием протокола STP, характеризуется меньшим временем приведения сети к древовидной топологии и имеет более высокую устойчивость.
Поддержка VLAN	VLAN – это группа портов коммутатора, образующих одну широковещательную область (домен). Коммутатор поддерживает различные средства классификации пакетов для определения их принадлежности к определенной VLAN.
Поддержка протокола OAM (Operation, Administration and Maintenance, IEEE 802.3ah)	Ethernet OAM (Operation, Administration and Maintenance), IEEE 802.3ah – функции уровня канала передачи данных, представляющие собой протокол мониторинга состояния канала. В этом протоколе для передачи информации о состоянии канала между непосредственно подключенными устройствами Ethernet используются блоки данных протокола OAM (OAMPDU). Оба устройства должны поддерживать стандарт IEEE 802.3ah.
Поддержка VLAN на базе портов (Port-Based VLAN)	Распределение по группам VLAN выполняется по входящим портам. Данное решение позволяет использовать на каждом порту только одну группу VLAN.
Поддержка 802.1Q	IEEE 802.1Q — открытый стандарт, который описывает процедуру тегирования трафика для передачи информации о принадлежности к VLAN. Позволяет использовать несколько групп VLAN на одном порту.
Объединение каналов с использованием LACP	Протокол LACP обеспечивает автоматическое объединение отдельных связей между двумя устройствами (коммутатор–коммутатор или коммутатор–сервер) в единый канал передачи данных. В протоколе постоянно определяется возможность объединения каналов, и в случае отказа соединения, входящего в объединенный канал, его трафик автоматически перераспределяется по не отказавшим компонентам объединенного канала.
Создание групп LAG	В устройствах поддерживается функция создания групп каналов. Агрегация каналов (Link aggregation, trunking) или IEEE 802.3ad — технология объединения нескольких физических каналов в один логический. Это способствует не только увеличению пропускной способности магистральных каналов коммутатор—коммутатор или коммутатор—сервер, но и повышению их надежности. Возможны три типа балансировки – на основании MAC-адресов, на основании IP-адресов и на основании порта (socket) назначения. Группа LAG состоит из портов с одинаковой скоростью, работающих в дуплексном режиме.
Selective Q-in-Q	Позволяет назначать внешний VLAN SPVLAN (ServiceProvider'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.

1.2.4 Функции третьего уровня сетевой модели OSI

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

Таблица 4 – Описание функций третьего уровня (Layer 3)

Статические IP-маршруты	Администратор коммутатора имеет возможность добавлять и удалять статические записи в таблицу маршрутизации.
Клиенты BootP и DHCP (Dynamic Host Configuration Protocol)	Устройства способны автоматически получать IP-адрес по протоколу BootP/DHCP.

Протокол ARP (Address Resolution Protocol)	ARP – протокол сопоставления IP-адреса и физического адреса устройства. Соответствие устанавливается на основе анализа ответа от узла сети, адрес узла запрашивается в широковещательном пакете.

1.2.5 Функции QoS

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

Таблица 5 – Основные функции качества обслуживания

Поддержка приоритетных очередей	Устройство поддерживает приоритезацию исходящего трафика по очередям на каждом порту. Распределение пакетов по очередям может производиться в результате классификации пакетов по различным полям в заголовках пакетов.
Поддержка класса обслуживания 802.1p	Стандарт 802.1p специфицирует метод указания приоритета кадра и алгоритм использования приоритета в целях своевременной доставки чувствительного к временным задержкам трафика. Стандарт 802.1p определяет восемь уровней приоритетов. Коммутаторы могут использовать значение приоритета 802.1p для распределения кадров по приоритетным очередям.

1.2.6 Функции обеспечения безопасности

Таблица 6 – Функции обеспечения безопасности

DHCP snooping	Функция коммутатора, предназначенная для защиты от атак с использованием протокола DHCP. Обеспечивает фильтрацию DHCP-сообщений, поступивших с ненадежных портов путем построения и поддержания базы данных привязки DHCP (DHCP snooping binding database). DHCP snooping выполняет действия брандмауэра между ненадежными портами и серверами DHCP.
Опция 82 протокола DHCP	Опция, которая позволяет проинформировать DHCP-сервер о том, с какого DHCP-ретранслятора и через какой порт пришел запрос. По умолчанию коммутатор, использующий функцию DHCP snooping, обнаруживает и отбрасывает любой DHCP-запрос содержащий опцию 82, который он получил через ненадёжный (untrusted) порт.
Dynamic ARP Inspection (Protection)	Функция коммутатора, предназначенная для защиты от атак с использованием протокола ARP. Сообщение, которое поступает с ненадежного порта, подвергается проверке – соответствует ли IP-адрес в теле принятого ARP-пакета IP-адресу отправителя. Если адреса не совпадают, то коммутатор отбрасывает пакет.
L2 – L3 – L4 ACL (Access Control List)	На основе информации, содержащейся в заголовках уровней 2, 3 и 4, у администратора есть возможность настроить до 100 правил, согласно которым пакет будет обработан, либо отброшен.
Проверка подлинности на основе порта (802.1x)[1]	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.
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.

[1] Не поддерживается в текущей версии ПО 10.1.8.2

1.2.7 Функции управления коммутатором

Таблица 7 – Основные функции управления коммутаторами

Загрузка и выгрузка файла настройки	Параметры устройств сохраняются в файле настройки, который содержит данные конфигурации как всей системы в целом, так и определенного порта устройства.
Протокол TFTP (Trivial File Transfer Protocol)	Протокол TFTP используется для операций записи и чтения файлов. Протокол основан на транспортном протоколе UDP. Устройства поддерживают загрузку и передачу по данному протоколу файлов настройки и образов программного обеспечения.
Протокол SNMP	Протокол SNMP используется для мониторинга и управления сетевым устройством. Для управления доступом к системе определяется список записей сообщества, каждая из которых содержит привилегии доступа.
Интерфейс командной строки (CLI)	Управление коммутаторами посредством CLI осуществляется локально через последовательный порт RS-232, либо удаленно через Telnet. 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) SNMP SSH
Локальная аутентификация	Для локальной аутентификации поддерживается хранение паролей в базе данных коммутатора.
Фильтрация IP-адресов для SNMP	Доступ по SNMP разрешается для определенных IP-адресов, являющихся членами SNMP-сообщества.
Клиент RADIUS	Протокол RADIUS используется для аутентификации, авторизации и учета. Сервер RADIUS использует базу данных пользователей, которая содержит данные проверки подлинности для каждого пользователя. Коммутаторы содержат клиентскую часть протокола RADIUS.
TACACS+ (Terminal Access Controller Access Control System)	Устройство предоставляет поддержку проверки подлинности клиентов посредством протокола TACACS+. Протокол TACACS+ обеспечивает централизованную систему безопасности для проверки пользователей, получающих доступ к устройству, а также централизованную систему управления при соблюдении совместимости с RADIUS и другими процессами проверки подлинности.

1.2.8 Дополнительные функции

В таблице 8 приведены дополнительные функции устройства.

Таблица 8 – Дополнительные функции устройства

Виртуальное тестирование кабеля (VCT)	Сетевые коммутаторы имеют в своём составе программные и аппаратные средства, позволяющие выполнять функции виртуального тестера кабеля – VCT. Тестер позволяет определить состояние медного кабеля связи.
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.
UDLD (Unidirectional Link Detection)	Протокол второго уровня, созданный для автоматического обнаружения потери двухсторонней коммуникации на оптических линиях связи.

1.3 Основные технические характеристики

Основные технические параметры коммутаторов приведены в таблице 9.

Таблица 9 – Основные технические характеристики

Общие параметры		
Пакетный процессор	MES1428	Realtek RTL8332M
	MES2408 MES2408B MES2408IP DC1 MES2408P MES2408PL	Realtek RTL8380M
	MES2408C MES2408CP MES2428 MES2428P MES2428B MES2428T	Realtek RTL8382M
Интерфейсы	MES1428	24 x 10/100BASE-TX (RJ-45) 4 x 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo)
	MES2408 MES2408B	8 x 10/100/1000BASE-T (RJ-45) 2 x 100BASE-FX/1000BASE-X (SFP)
	MES2408C	8 x 10/100/1000BASE-T (RJ-45) 2 x 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo)
	MES2408CP	8 x 10/100/1000BASE-T (PoE/PoE+) 2 x 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo)
	MES2408IP DC1 MES2408P MES2408PL	8 x 10/100/1000BASE-T (PoE/PoE+) 2 x 100BASE-FX/1000BASE-X (SFP)
	MES2428 MES2428B MES2428T	24 x 10/100/1000BASE-T (RJ-45) 4 x 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo)

	MES2428P	24 x 10/100/1000BASE-T (PoE/PoE+) 4 x 10/100/1000BASE-T/100BASE-FX/1000BASE-X (Combo)
Пропускная способность	MES1428	12,8 Гбит/с
	MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL	20 Гбит/с
	MES2428 MES2428P MES2428B MES2428T	56 Гбит/с
Производительность на пакетах длиной 64 байта	MES1428	9 MPPS
	MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL	14,88 MPPS
	MES2428 MES2428P MES2428B MES2428T	41,658 MPPS
Объем буферной памяти		512 Кбайт
Объем ОЗУ (DDR3)		256 Мбайт
Объем ПЗУ (RAW NAND)		32 Мбайт
Таблица MAC-адресов		8K
Объем TCAM		1,5K
Количество ARP-записей		1K
Количество групп L2 Multicast (IGMP snooping)		509

Скорость передачи данных	MES1428 MES2408 MES2408B MES2408C MES2408CP MES2408IP DC1 MES2408P MES2408PL MES2428 MES2428P MES2428B MES2428T	Оптические интерфейсы 100/1000 Мбит/с Электрические интерфейсы 10/100/1000 Мбит/с
Количество правил SQinQ		128(ingress)/128(egress)
Поддержка VLAN		согласно 802.1Q до 4K активных VLAN
Качество обслуживания QoS		приоритизация трафика, 8 уровней 8 выходных очередей с разными приоритетами для каждого порта
Количество виртуальных Loopback-интерфейсов		10
Агрегация каналов (LAG)		8 групп
Количество экземпляров MSTP		64
Сверхдлинные кадры (jumbo frames)		максимальный размер пакетов 10000 байт
Соответствие стандартам		IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-T Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z Fiber Gigabit Ethernet IEEE 802.3x Full Duplex, Flow Control IEEE 802.3ad Link Aggregation (LACP) IEEE 802.1p Traffic Class IEEE 802.1q VLAN IEEE 802.1v IEEE 802.3 ac IEEE 802.1d Spanning Tree Protocol (STP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) IEEE 802.1x Authentication IEEE 802.3af PoE, IEEE 802.3at PoE+ (только MES2408CP, MES2408IP DC1, MES2408P, MES2408PL и MES2428P)
Управление		
Локальное управление		Console
Удаленное управление		SNMP, Telnet, SSH
Физические характеристики и условия окружающей среды		
Источники питания	MES1428 MES2408C MES2408CP MES2408PL	сеть переменного тока: 110-250В AC, 50 Гц

	MES2408 MES2428 MES2428T	сеть переменного тока: 110-250В AC, 50 Гц сеть постоянного тока: 18–72В
	MES2408IP DC1	сеть постоянного тока: 36–72В
	MES2408P	сеть переменного тока: 176-250В AC, 50 Гц сеть постоянного тока: 36–72В
	MES2428P	сеть переменного тока: 170-264В AC, 50 Гц сеть постоянного тока: 36–72В
	MES2408B MES2428B	сеть переменного тока: 110-250В AC, 50 Гц аккумуляторная батарея: 12В DC
Потребляемая мощность	MES1428 MES2408 MES2408C	не более 10 Вт
	MES2408B	не более 37 Вт (с учетом заряда АКБ)
	MES2408CP	не более 160 Вт (с учетом нагрузки PoE)
	MES2408IP DC1	не более 135 Вт (с учетом нагрузки PoE)
	MES2408P	не более 280 Вт (с учетом нагрузки PoE)
	MES2408PL	не более 93 Вт (с учетом нагрузки PoE)
	MES2428 MES2428T	не более 18 Вт
	MES2428B	не более 45 Вт (с учетом заряда АКБ)
	MES2428P	не более 440 Вт (с учетом нагрузки PoE)
Бюджет PoE	MES2408CP MES2408IP DC1	120 Вт
	MES2408P	256 Вт
	MES2408PL	65 Вт
	MES2428P	370 Вт
Аппаратная поддержка Dying Gasp	MES1428 MES2408C MES2408CP MES2428 MES2428P AC	есть
	MES1428B MES2408 MES2408B MES2408IP DC1 MES2408P MES2408PL MES2428B MES2428P DC MES2428T	нет

Габаритные размеры	MES1428 MES2408IP DC1 MES2408P MES2428 MES2428B MES2428T	430 x 178 x 44 мм
	MES2408 MES2408B MES2408C MES2408CP MES2408PL	310 x 177 x 44 мм
	MES2428P AC	430 x 204 x 44 мм
	MES2428P DC	430 x 305 x 44 мм
Интервал рабочих температур	MES1428 MES2408 DC MES2408B MES2408C MES2408P AC MES2408PL MES2428 MES2428B MES2428P MES2428T	от -20 до +50 °C
	MES2408CP MES2408P DC	от -20 до +50 °C **При использовании коммерческих SFP-трансиверов температура окружающей среды не должна превышать +45 °C**
	MES2408 AC	от -20 до +60 °C
	MES2408IP DC1	от -40 до +60 °C
Интервал температуры хранения		от -40 до +70 °C
Относительная влажность при эксплуатации (без образования конденсата)		не более 80%
Относительная влажность при хранении (без образования конденсата)		от 10% до 95%
Средний срок службы		10 лет

Тип питания устройства определяется при заказе.

1.4 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 серий MES14xx, MES24xx выполнены в металлическом корпусе с возможностью установки в 19” каркас, высота корпуса 1U.

1.4.1 Внешний вид и описание передней панели устройств

Внешний вид передней панели MES1428 показан на рисунке 1.

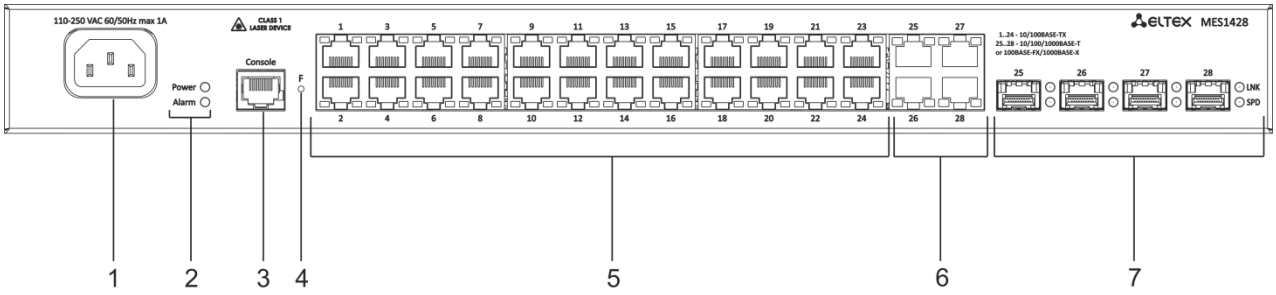

Рисунок 1 – Передняя панель MES1428

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

Таблица 10 – Описание разъемов, индикаторов и органов управления передней панели MES1428

№	Элемент передней панели	Описание
1	~110-250VAC, 60/50Hz max 1A	Разъем для подключения к источнику электропитания переменного тока
2	Power	Индикатор питания устройства
	Alarm	Индикатор перегрева
3	Console	Консольный порт для локального управления устройством. Распиновка разъема следующая: 1 не используется 2 не используется 3 RX 4 GND 5 GND 6 TX 7 не используется 8 не используется 9 не используется Распайка консольного кабеля приведена в приложении В.
4	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: - при нажатии на кнопку длительностью менее 10 с происходит перезагрузка устройства; - при нажатии на кнопку длительностью более 10 с происходит сброс настроек устройства до заводской конфигурации.

5	[1-24]	Порты 10/100BASE-TX (RJ-45).
6	25, 26, 27, 28	Комбо-порты: порты 10/100/1000Base-T (RJ-45)
7	25, 26, 27, 28	Комбо-порты: слоты для установки трансиверов 1000Base-X Combo. LNK/SPD – световая индикация состояния оптических интерфейсов.

Внешний вид передней панели устройств серии MES2408 показан на рисунках 2 – 10.

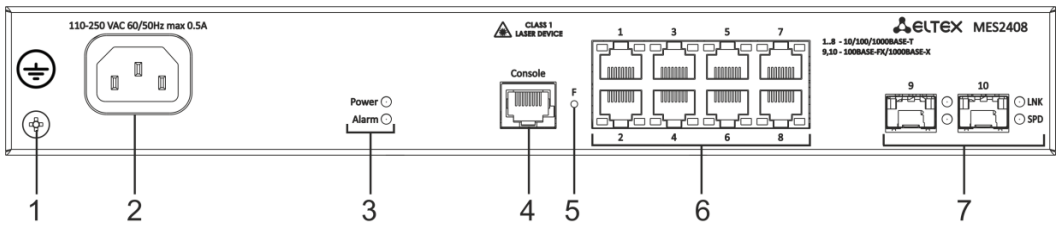

Рисунок 2 – Передняя панель MES2408 AC

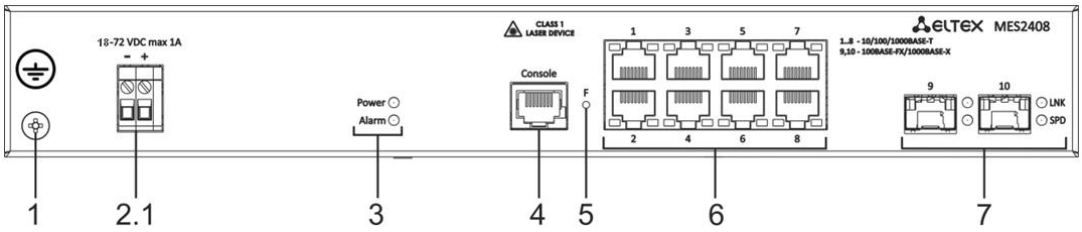

Рисунок 3 – Передняя панель MES2408 DC

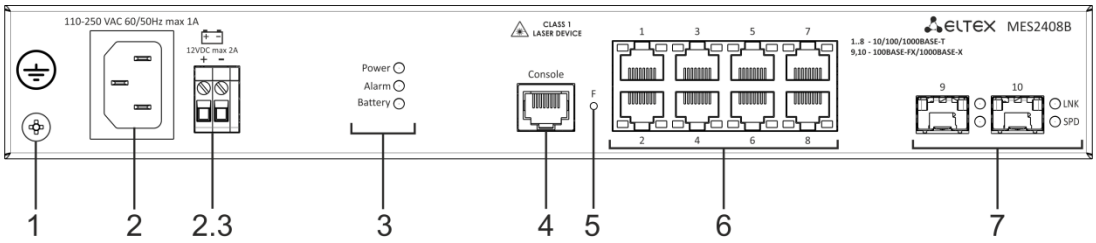

Рисунок 4 – Передняя панель MES2408B

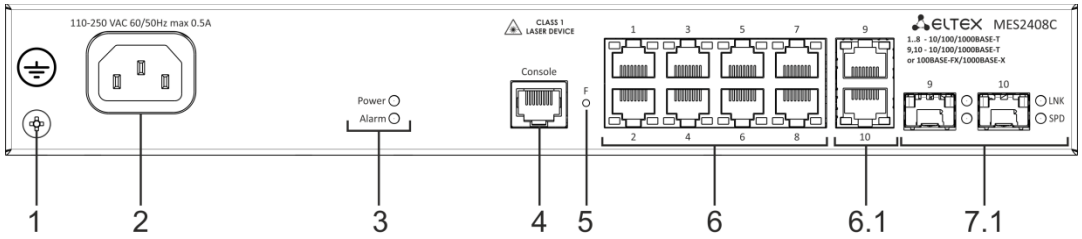

Рисунок 5 – Передняя панель MES2408C

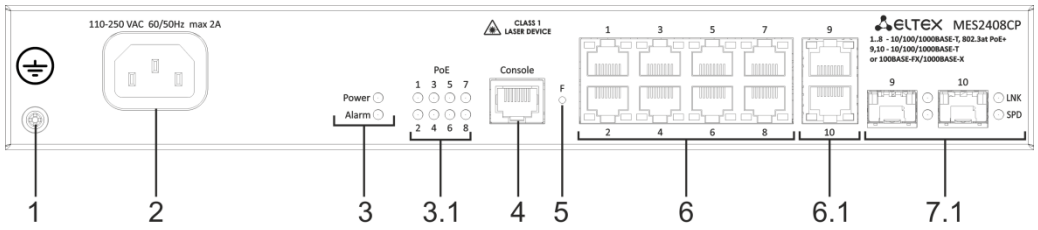

Рисунок 6 – Передняя панель MES2408CP

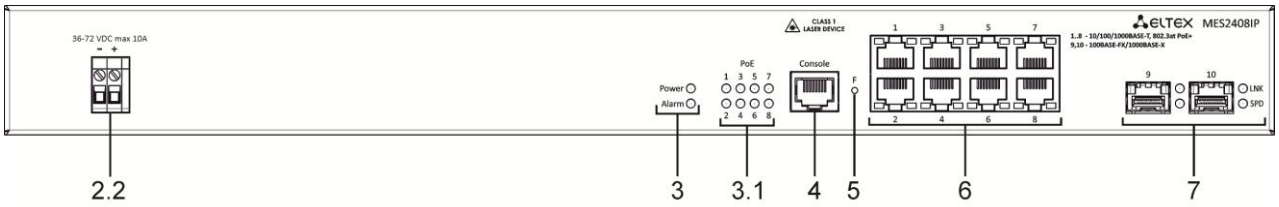

Рисунок 7 – Передняя панель MES2408IP DC1

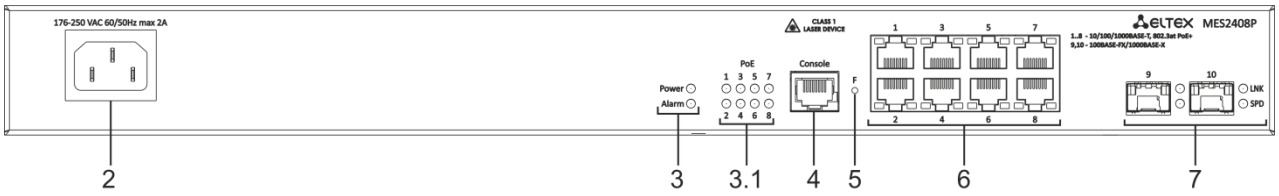

Рисунок 8 – Передняя панель MES2408P AC

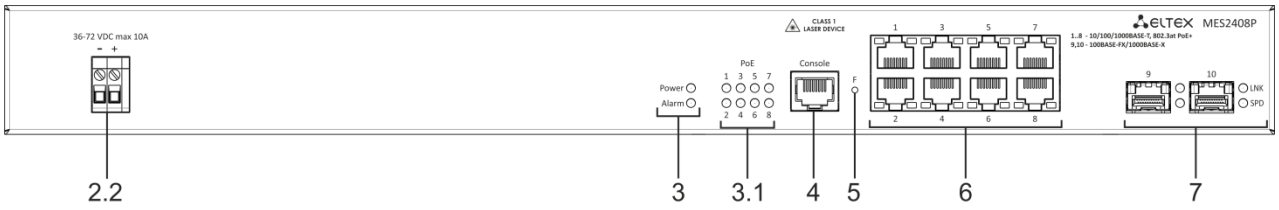

Рисунок 9 – Передняя панель MES2408P DC

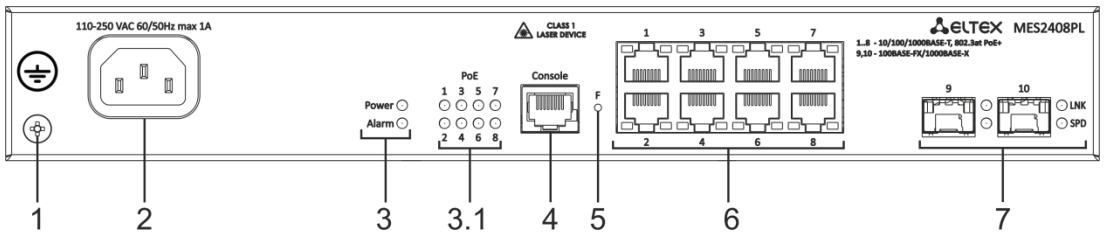

Рисунок 10 – Передняя панель MES2408PL

В таблице 11 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели коммутаторов серии MES2408.

Таблица 11 – Описание разъемов, индикаторов и органов управления передней панели коммутаторов серии MES2408

№	Элемент передней панели	Описание
1	⏚	Клемма для заземления устройства
2	~110-250VAC, 60/50Hz max 1A	Разъем для подключения к источнику электропитания переменного тока
2.1	18-72 VDC max 10A	Разъем для подключения к источнику электропитания постоянного тока
2.2	36-72 VDC max 1A/10A	Разъем для подключения к источнику электропитания постоянного тока
2.3	12VDC max 2A	Разъем для подключения к аккумуляторной батареи
3	Power	Индикатор питания устройства
	Alarm	Индикатор перегрева
	Battery (для MES2408B)	Индикатор работы аккумуляторной батареи
3.1	PoE 1-8	Индикаторы состояния PoE-портов
4	Console	Консольный порт для локального управления устройством. Распиновка разъема следующая: 1 не используется 2 не используется 3 RX 4 GND 5 GND 6 TX 7 не используется 8 не используется 9 не используется Распайка консольного кабеля приведена в приложении В.
5	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: - при нажатии на кнопку длительностью менее 10 с происходит перезагрузка устройства; - при нажатии на кнопку длительностью более 10 с происходит сброс настроек устройства до заводской конфигурации.
6	[1-8]	Порты 10/100/1000BASE-T (RJ-45)
6.1	9, 10	Комбо-порты: порты 10/100/1000Base-T (RJ-45)
7	9, 10, LNK/SPD	Слоты для установки оптических трансиверов 100BASE-FX/1000BASE-X (SFP). LNK/SPD – световая индикация состояния оптических интерфейсов
7.1	9, 10, LNK/SPD	Комбо-порты: слоты для установки трансиверов 1000Base-X Combo. LNK/SPD – световая индикация состояния оптических интерфейсов

Внешний вид передней панели устройств серии MES2428 показан на рисунках 11–16.

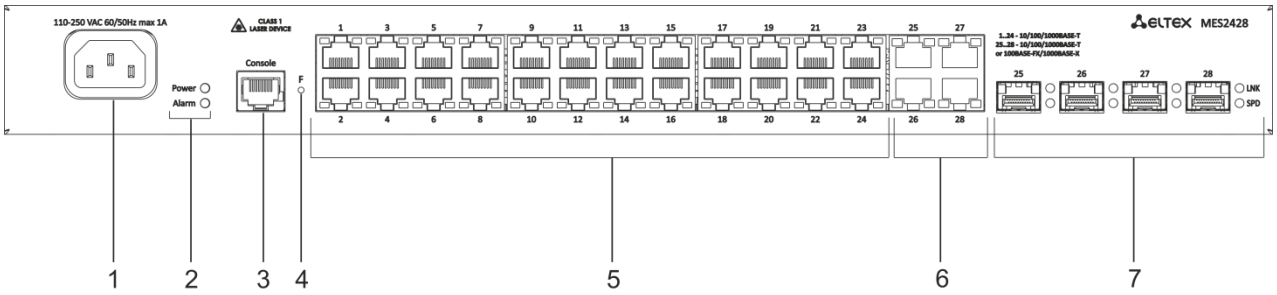

Рисунок 11 – Передняя панель MES2428 AC

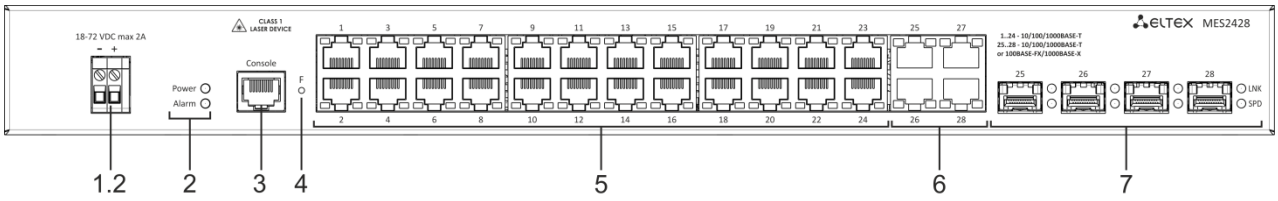

Рисунок 12 – Передняя панель MES2428 DC

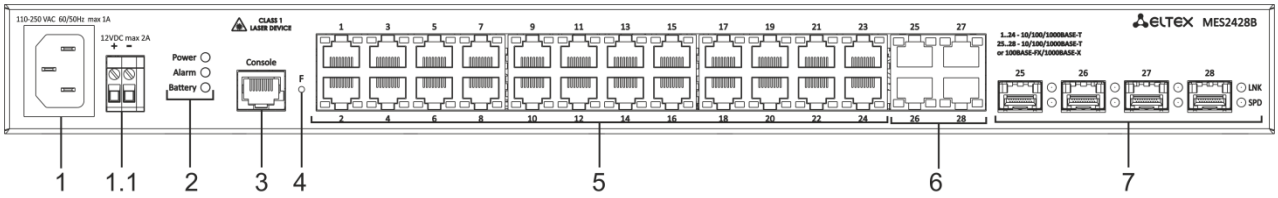

Рисунок 13 – Передняя панель MES2428B

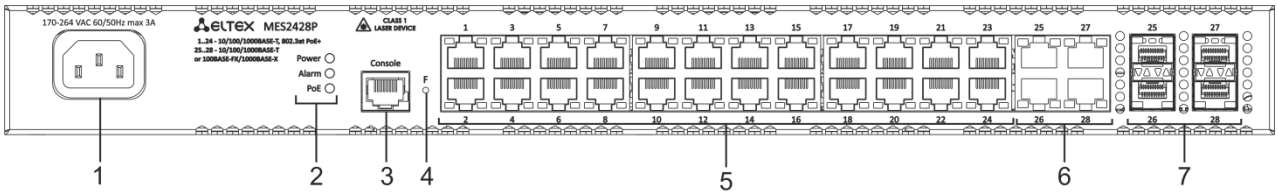

Рисунок 14 — Передняя панель MES2428P AC

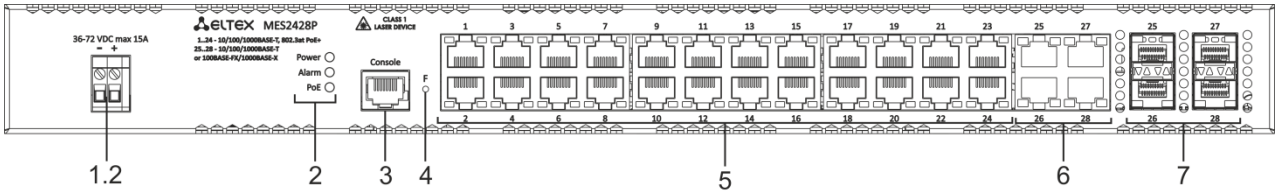

Рисунок 15 — Передняя панель MES2428P DC

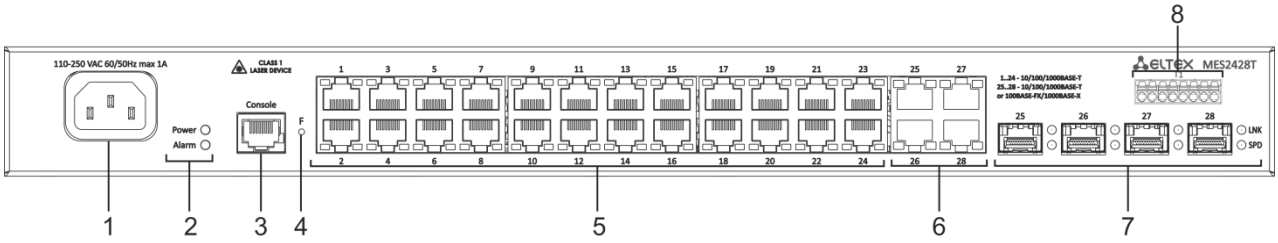

Рисунок 16 – Передняя панель MES2428T

В таблице 12 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели коммутаторов серии MES2428.

Таблица 12 – Описание разъемов, индикаторов и органов управления передней панели коммутаторов серии MES2428

№	Элемент передней панели	Описание
1	~110-250VAC, 60/50Hz max 1A (170-264 VAC 60/50 Hz max 3A для MES2428P)	Разъем для подключения к источнику электропитания переменного тока
1.1	12VDC max 2A	Разъем для подключения к аккумуляторной батареи
1.2	18-72 VDC max 2A (36-72 VDC max 15A для MES2428P DC)	Разъем для подключения к источнику электропитания постоянного тока
2	Power	Индикатор питания устройства
	Alarm	Индикатор перегрева
	PoE	Индикатор работы PoE
	Battery (для MES2428B)	Индикатор работы аккумуляторной батареи
3	Console	Консольный порт для локального управления устройством. Распиновка разъема следующая: 10 не используется 11 не используется 12 RX 13 GND 14 GND 15 TX 16 не используется 17 не используется 18 не используется Распайка консольного кабеля приведена в приложении В.
4	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: - при нажатии на кнопку длительностью менее 10 с происходит перезагрузка устройства; - при нажатии на кнопку длительностью более 10 с происходит сброс настроек устройства до заводской конфигурации.
5	[1-24]	Порты 10/100/1000BASE-T (RJ-45).
6	25, 26, 27, 28	Комбо-порты: порты 10/100/1000Base-T (RJ-45)
7	25, 26, 27, 28, LNK, SPD	Комбо-порты: слоты для установки трансиверов 1000Base-X Combo. LNK/SPD – световая индикация состояния оптических интерфейсов
8	T1	4 пары входных сухих контактов

1.4.2 Задняя панель устройства

Внешний вид задней панели коммутаторов MES14xx и MES24xx приведен на рисунке 17.

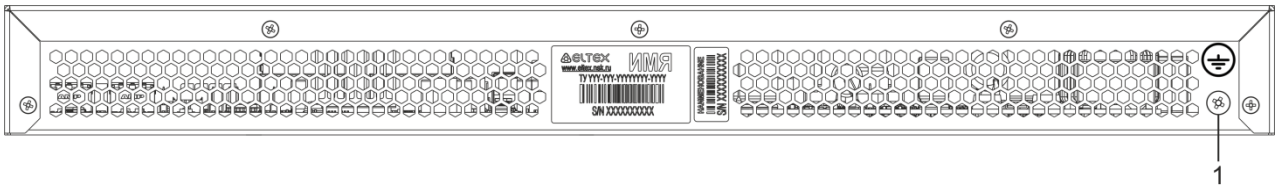

Рисунок 17 – Задняя панель коммутаторов MES1428, MES2428, MES2428T, MES2428B, MES2408IP DC1 и MES2408P

Рисунок 18 – Задняя панель коммутаторов MES2408, MES2408B, MES2408C, MES2408CP, MES2408PL

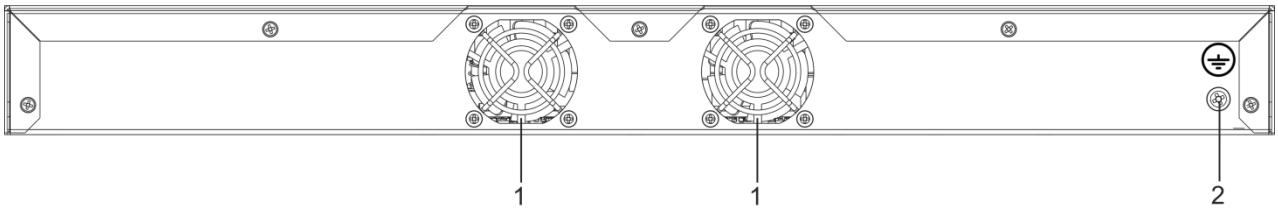

Рисунок 19 – Задняя панель коммутатора MES2428P

В таблицах 13 и 14 приведен перечень разъемов, расположенных на задней панели коммутаторов.

Таблица 13 – Описание разъемов задней панели коммутаторов MES1428, MES2428, MES2428T, MES2428B, MES2408IP DC1, MES2408P

№	Элемент задней панели	Описание
1	Клемма заземления ⏚	Клемма для заземления устройства.

Таблица 14 – Описание разъемов задней панели коммутатора MES2428P

№	Элемент задней панели	Описание
1		Вентиляторы для охлаждения устройства.
2	Клемма заземления ⏚	Клемма для заземления устройства.

1.4.3 Боковые панели устройства

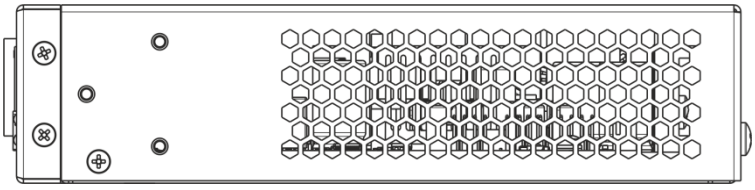

Рисунок 20 – Правая боковая панель Ethernet-коммутаторов

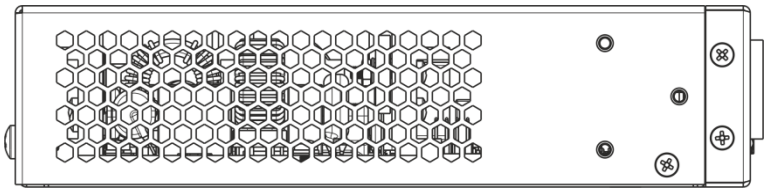

Рисунок 21 – Левая боковая панель Ethernet-коммутаторов

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».

1.4.4 Световая индикация

Состояние интерфейсов Ethernet индицируется двумя светодиодными индикаторами, *LINK/ACT* зеленого цвета и *SPEED* янтарного цвета. Расположение светодиодов показано на рисунках 22, 23.

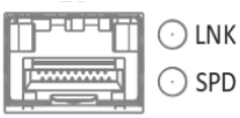

Рисунок 22 – Внешний вид разъема SFP

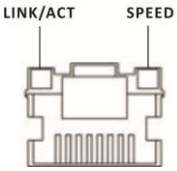

Рисунок 23 – Внешний вид разъема RJ-45

Таблица 15 – Световая индикация состояния Ethernet-портов 10/100/1000BASE-T

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

Системные индикаторы (Power, Alarm) служат для определения состояния работы узлов коммутаторов серии MES14xx, MES24xx.

Таблица 16 – Световая индикация системных индикаторов

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Power	Состояние источников питания	Выключен	Питание выключено
		Зеленый, горит постоянно	Питание включено, нормальная работа устройства
		Зеленый, мерцает	Самотестирование устройства при старте (POST)
Alarm	Состояние устройства	Не горит	Нормальная работа устройства
		Красный, горит постоянно	Перегрев
PoE	Индикатор состояния PoE-портов	Зеленый, горит постоянно	Подключен потребитель PoE (горит индикатор, соответствующий порту)
		Красный, горит постоянно	Ошибка PoE на порту
		Выключен	Потребитель PoE не подключен

Если индикатор Alarm и индикатор PoE одновременно горят красным цветом, – это сигнализирует о критической ошибке PoE.

1.5 Комплект поставки

В базовый комплект поставки входят:

- Ethernet-коммутатор;
- Шнур питания (в случае комплектации модулем питания на 220В);
- Комплект крепежа в стойку;
- Руководство по эксплуатации (поставляется на CD-диске);
- Паспорт.

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

2 УСТАНОВКА И ПОДКЛЮЧЕНИЕ

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

2.1 Крепление кронштейнов

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

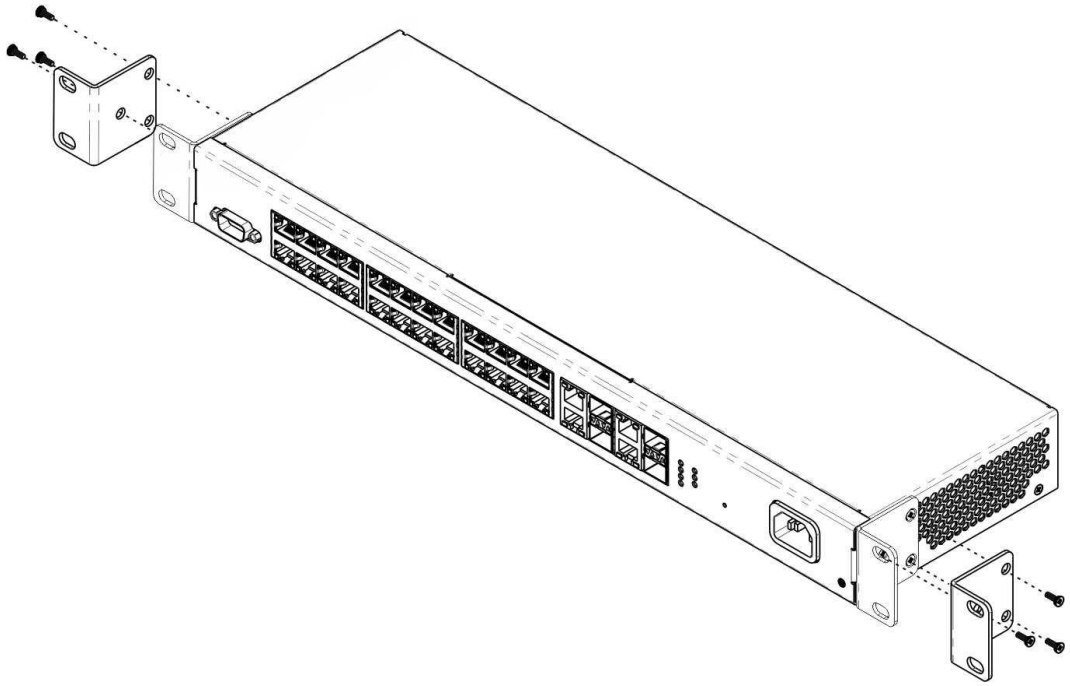

Рисунок 24 – Крепление кронштейнов

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.

2.2 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.

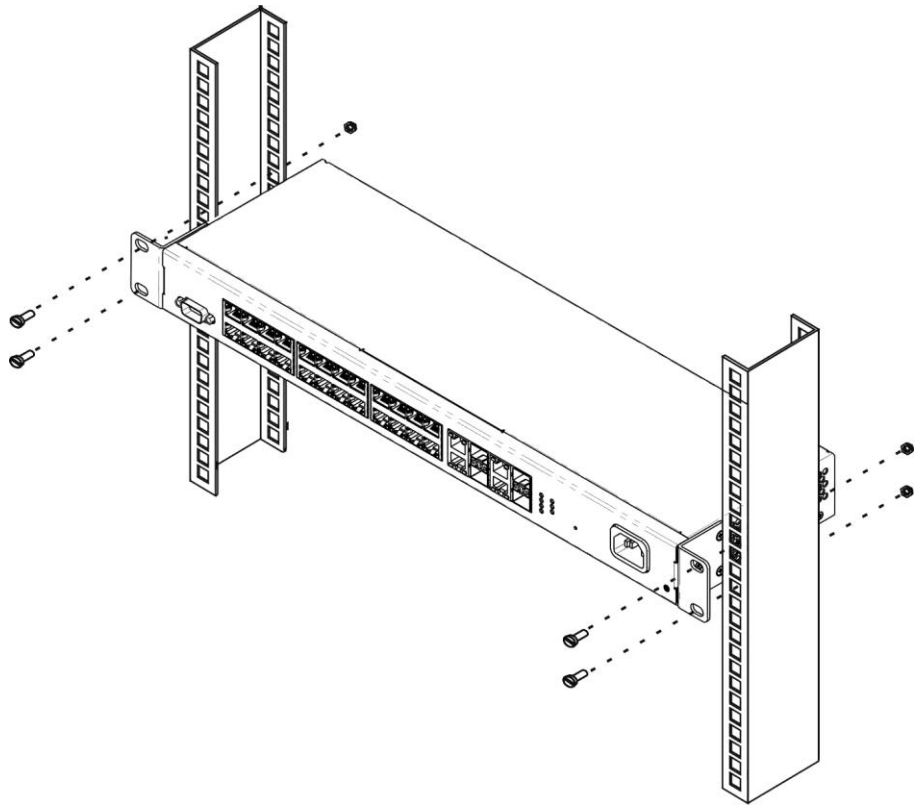

Рисунок 25 – Установка устройства в стойку

На рисунке 26 приведен пример размещения коммутаторов MES14xx и MES24xx в стойке.

Рисунок 26 – Размещение коммутаторов MES14xx и MES24xx в стойке

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

2.3 Подключение питающей сети

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

2.4 Установка и удаление SFP-трансиверов

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

Рекомендуется раздельное подключение SFP-трансивера и оптического патч-корда в слот.

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

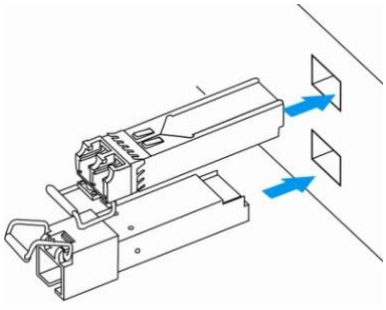

Рисунок 27 – Установка SFP-трансиверов

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

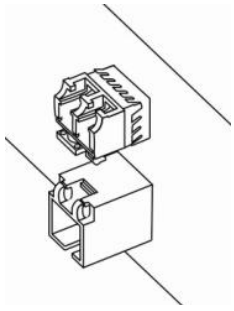

Рисунок 28 – Установленные SFP-трансиверы

Для удаления трансивера:

1. Откройте защелку модуля.

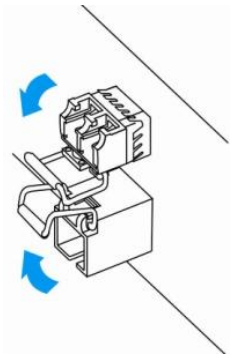

Рисунок 29 – Открытие защелки SFP-трансиверов

2. Извлеките модуль из слота.

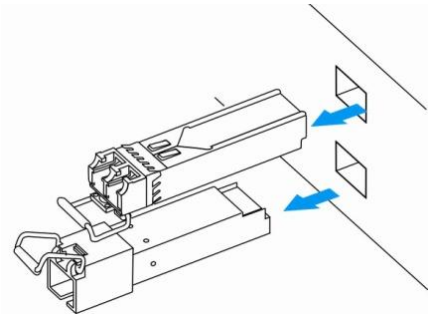

Рисунок 30 – Извлечение SFP-трансиверов

3 НАЧАЛЬНАЯ НАСТРОЙКА КОММУТАТОРА

3.1 Горячие клавиши

Сочетание клавиш	Описание
Ctrl+A	Вернуться к началу строки
Ctrl+E	Вернуться к концу строки
Ctrl+F	Продвинуться вперед на один символ
Ctrl+B	Продвинуться назад на один символ
Ctrl+D	Удалить данный символ
Ctrl+U,X	Удалить начало строки до символа
Ctrl+K	Удалить конец строки после символа
Ctrl+W	Удалить предыдущее слово
Ctrl+T	Переместить предыдущий символ
Ctrl+P	Перейти к предыдущей строке в истории команд
Ctrl+N	Перейти к следующей строке в истории команд
Ctrl+Z	Возврат к корневому режиму CLI

3.2 Настройка терминала

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

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

3.3 Включение устройства

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

Включить устройство. При каждом включении коммутатора запускается процесс инициализации устройства, после которой необходимо пройти процедуру авторизации для дальнейшей работы с коммутатором:

```
ISS login:admin
Password:*****  (admin)

console#
```

3.4 Настройка функций коммутатора

Функции по начальному конфигурированию устройства можно разделить на два типа.

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

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

```
console# write startup-config
```

3.4.1 Автоматическая настройка параметров коммутатора (Zero Touch Provisioning)

В целях автоматизации управления коммутатором на устройстве поддержана функция ZTP (Zero Touch Provisioning). Данная функция позволяет получить настройку некоторых опций от DHCP-сервера на этапе подключения устройства. По умолчанию ZTP включен автоматически.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 17 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ztp enable	-/включен, запускается вначале старта прошивки	Включить работу функции ZTP. **По умолчанию ZTP поддерживает передачу опций 43, 66, 67. Подопции для 43 опции:** 1 – image 2 – bootfile 3 – config-file 4 - tftpserver
ztp disable		Отключить работу функции ZTP

3.4.2 Базовая настройка коммутатора

Для начала конфигурации устройства необходимо подключить устройство к компьютеру через последовательный порт. Запустить на компьютере программу эмуляции терминала согласно пункту 3.2 «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. Настройка параметров протокола SNMP.

3.4.2.1 Задание пароля на начальный загрузчик

На устройстве существует возможность установить пароль на начальный загрузчик. Длина пароля не должна превышать 16 символов. Чтобы задать пароль необходимо в командной строке коммутатора выполнить команду:

```
console# boot password password
```

Команда для сброса пароля:

```
console# no boot password
```

Для того, чтобы перейти в u-boot коммутатора необходимо во время загрузки устройства ввести пароль после строчек:

```
U-Boot 2011.12.(2.1.5.67086) (Feb 18 2019 - 06:43:17)

Board: RTL838x CPU:500MHz LXB:200MHz MEM:300MHz
DRAM:  256 MB
SPI-F: 1x32 MB
Loading 65536B env. variables from offset 0x110000
chip_index=      23
Switch Model: MES2428_board (Port Count: 28)
Switch Chip: RTL8382
************************************************
#### RTL8218B config - MAC ID = 0 ####
Now External 8218B
************************************************
#### RTL8218B config - MAC ID = 8 ####
Now Internal PHY
************************************************
#### RTL8218B config - MAC ID = 16 ####
Now External 8218B
************************************************
**** RTL8214FC config - MAC ID = 24 ****
Now External 8214FC
Net:   Net Initialization Skipped
rtl8380#0
Autobootin 3 seconds..
```

Пароль по умолчанию для всех устройств «eltex».

Пароль на начальный загрузчик также можно изменить из самого u-boot. Для этого после перехода в u-boot необходимо задать пароль следующей командой (пример для MES2428):

```
MES2428# password set password
```

Команда для сброса пароля из u-boot:

```
MES2428# password erase
```

После введения этой команды требуется подтверждение сброса пароля клавишей «y».

Сброс пароля восстанавливает пароль по умолчанию – «eltex».

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

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

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

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

Уровень привилегий с 1 по 14 разрешает доступ к устройству, но запрещает настройку. Уровень привилегий 15 разрешает как доступ, так и настройку устройства.

Пароль должен состоять из 5 символов минимум, содержать в себе латинские буквы верхнего и нижнего регистра, а также хотя бы один специальный символ и цифру. Можно отключить проверку на наличие вышеуказанных символов командами с помощью команд passwordvalidate.

Пример команд для задания пользователю **«admin»** пароля **«Eltex_1»** и создания пользователя **«operator»** с паролем **«Pass_2»** и уровнем привилегий 1:

```
console# configure
console(config)# username admin password Eltex_1
console(config)# username operator password Pass_2 privilege 1
console(config)# exit
console#
```

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

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

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 – 192.168.1.1

```
console# configure
console(config)# interface vlan 1
console(config-if)# ip address 192.168.16.144 255.255.255.0
console(config-if)# no shutdown
console(config-if)# exit
console(config)#iproute 0.0.0.0 0.0.0.0 192.168.1.1
```

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

```
console# show ip interface
```

```
vlan1 is up, line protocol is up
```

```
Internet Address is 192.168.16.144/24
Broadcast Address  192.168.16.255
Vlan counters disabled
```

3.4.2.4 Настройка параметров протокола SNMP для доступа к устройству

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

Для возможности администрирования устройства посредством протокола SNMP, необходимо создать хотя бы одну строку сообщества.

Формат конфигурации SNMP должен принимать следующий вид:

```
snmp user <user>
snmp community index <indexNumber> name <community> security <user>
snmp group <groupname> user <user> security-model v2c
snmp access <groupname> v2c read <view> write <view> notify <view>
snmp view <view><oid> included
snmp targetaddr <targetAddr> param <targetParam><ip-address> taglist
<taglist>
snmp targetparams <targetParam>user<user> security-model v2c message-
processing v2c
snmp notify <user> tag <taglist> type Trap
!
```

В качестве примера будем использовать версию snmpv2c. Создадим пользователя USER, принадлежащего группе GROUP. Данный пользователь должен иметь возможность использовать community NETMAN, которой присвоим индекс 1. Группе GROUP будет разрешен доступ на чтение/запись/получение snmp-trap по объектам, принадлежащим viewiso. Объекты, для которых разрешена отправка трапов, должны принадлежать тег-листу TAG, отправляться на группу адресов ADDR, в которую входит IP-адрес 192.168.1.1. Параметры отправки указываются в targetparamTRAPS, определяемом для пользователя USER.

```
console(config)#!
console(config)#snmp user USER
console(config)#snmp community index 1 name NETMAN security USER
console(config)#snmp group GROUP user USER security-model v2c
console(config)#snmp access GROUP v2c read iso write iso notify iso
console(config)#snmp view iso 1 included
console(config)#snmp targetaddr ADDR param TRAPS 192.168.1.1 taglist TAG
console(config)#snmp targetparams TRAPS user USER security-model v2c
message-processing v2c
console(config)#snmp notify USER tag TAG type Trap
```

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 18 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
snmp notify *notify_name***tag***tag_name***type {trap | inform}**	notify_name: (1..32) символа; tag_name: (1..32) символа -/выключено	Активировать отправку трапов по событию login/logout
snmp notify *notify_name*		Отключить отправку трапов по событию login/logout
snmp-server enable traps dry-contacts	-/выключено	Активировать отправку трапов по событию замыкания/ размыкания сухих контактов
no snmp-server enable traps dry-contacts		Отключить отправку трапов по событию замыкания/ размыкания сухих контактов
snmp user user_*name***{EngineID***EngineID***}**	user_name: (1..32) символов	Создать SNMP-пользователя. EngineID – идентификатор SNMP-устройства
no snmp user *name*		Удалить SNMP-пользователя.
snmp community index *index***name** *name***security** *user_name*	index: (1..32) символов; user_name: (1..32) символов	Привязать сообщество с заданным индексом к ранее созданному пользователю. Чтобы разрешить использование любого специального символа в названии и индексе сообщества, укажите его в двойных кавычках. Если название и индекс сообщества содержат только буквы и цифры, тогда двойные кавычки не нужны.
no snmp community index *index*		Удалить SNMP-сообщество с указанным индексом.
snmp group *group_name* **user** *user_name* **security-model {v1 | v2c |v3}**	user_name: (1..32) символов; group_name: (1..32) символов	Создает SNMP-группу или таблицу соответствий SNMP-пользователей и правил обозрений SNMP
no snmp group *group_name* **user** *user_name* **security-model {v1 | v2c |v3}**		Удаляет SNMP-группу.
snmp access *group_name* **{v1 | v2c |v3} read** *read_view***write** *write_view* **notify** *notify_view*	group_name: (1..32) символов	Разрешить SNMP-группе доступ на чтение, запись и отправку snmp-трапов по объектам, принадлежащим read/write/notify-view.
no snmp access *group_name* **{v1 | v2c |v3auth}**		Запретить SNMP-группе доступ на чтение, запись и отправку snmp-трапов по объектам, принадлежащим read/write/notify-view.
snmp view *view_nameOID***{included | excluded}**	view_name: (1..32) символов	Создает или редактирует правило обозрения для SNMP— разрешающее правило, либо ограничивающее серверу-обозревателю доступ к OID. OID – идентификатора обекта MIB, предствленный в виде дерева ASN.1 included – OID включена в правило для обозревания; excluded – OID исключена в правило для обозревания.
snmp view *view_name OID*		Удаляет правило обозрения для SNMP.
snmp targetaddr *targetAddr* **param** *targetParamIP_addr* **taglist** *tagList*	targetAddr: (1..32) символов; targetParam: (1..32) символов; tagList: (1..255) символов	Создать группу адресов, на которые будут отправляться трапы согласно параметрам тег-листа
no snmp targetaddr *targetAddr*		Удалить группу адресов, на которые будут отправляться трапы согласно параметрам тег-листа
snmp targetparams *target_param***user** *user_name***security-model {v1 | v2c | v3} message-processing {v1 | v2c | v3}**	user_name: (1..32) символов; target_param: (1..32) символов;	Указать параметры отправки трапов, определяемые пользоваелем
no snmp targetparams *target_param*		Удалить параметры отправки трапов, определяемые пользоваелем

3.4.3 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 – ***admin***. Пароль назначается пользователем.

Методы аутентификации и авторизации могут быть настроены глобально или на отдельные линии.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Для входа в режим конфигурации линий используются команды:

```
line{console | telnet | ssh}
```

Вид запроса командной строки режима конфигурации линий:

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

Таблица 19 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
enable authentication {local | radius | tacacs}	-/выключено	Задает метод аутентификации пользователя при повышении уровня привилегий для консоли, telnet, ssh. - *radius* – использовать список RADIUS-серверов для аутентификации; - *tacacs* – использовать список TACACS-серверов для аутентификации.
no enable authentication		Устанавливает значение по умолчанию.
login authentication {radius | tacacs} [local]	-/local	Задает метод аутентификации пользователя при входе для консоли, telnet, ssh
no login authentication		Устанавливает значение по умолчанию.

4 УПРАВЛЕНИЕ УСТРОЙСТВОМ. ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ

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

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

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

```
console>
```

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

```
console#
```

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

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

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

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

4.1 Базовые команды

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 20 – Базовые команды, доступные в режиме EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
enable [*priv***]**	priv: (1..15)/15	Переключиться в привилегированный режим (если значение не указано – то уровень привилегий 15).
logout	-	Завершение текущей сессии и смена пользователя.
exit	-	Закрыть активную терминальную сессию.
help	-	Запрос справочной информации о работе интерфейса командной строки.
show privilege	-	Показать уровень привилегий текущего пользователя.

Команды режима privileged EXEC

Запрос командной строки имеет следующий вид:

```
console#
```

Таблица 21 – Базовые команды, доступные в режиме privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
disable [*priv***]**	priv: (1, 7, 15)/1	Вернуться в нормальный режим из привилегированного.
configure terminal	-	Перейти в режим конфигурации.

Команды, доступные во всех режимах конфигурации

Запрос командной строки имеет один из следующих видов:

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

Таблица 22 – Базовые команды, доступные во всех режимах конфигурации

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

4.2 Фильтрация сообщений командной строки

Фильтрация сообщений позволяет уменьшить объем отображаемых данных в ответ на запросы пользователя и облегчить поиск необходимой информации. Для фильтрации требуется добавить в конец командной строки символ «|» и использовать одну из опций фильтрации, перечисленных в таблице 23. Фильтрация работает только для show-команд.

Команды режима privilegedEXEC

Запрос командной строки имеет следующий вид:

```
console#
```

Таблица 23 – Базовые команды, доступные в режиме privilegedEXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
grep		Выводит все строки, содержащие шаблон.
grep - v	-	Выводит все строки, не содержащие шаблон
grep -c "*regexp***"**	-	Выводит все строки, содержащие регулярные выражения: . – соответствует любому отдельному символу; * – предыдущий символ соответствует 0 или более раз; ^ – соответсвует пробелу в начале строки; \b – соответствует пробелу в конце слова; [] – выводит все строки, в которых содержатся символы из квадратных скобок; \ – игноритует символ, следующий за регулярным выражением

4.3 Команды управления системой

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 24 – Команды управления системой в режиме EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
ping [ip] {*A.B.C.D* **|** *host***} [size** *size***] [count** *count***] [timeout** *timeout***]**	host: (1..158) символов; size: (36..2080)/64 байт; count: (0..10)/3; timeout: (1..100)	Команда служит для передачи запросов (ICMP Echo-Request) протокола ICMP указанному узлу сети, а также 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.
traceroute{*A.B.C.D* **| ipv6***AAAA::BBBB***} [size***size***] [ttl***ttl***] [count***count***] [timeout***timeout***]**	size: (64..1518)/64 байт; ttl: (1..255)/30; count: (1..10)/3; timeout: (1..60)/3 с	Определение маршрута трафика до узла назначения. - *A.B.C.D* – IPv4-адрес узла сети; - *AAAA::BBBB*–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; **Описание ошибок при выполнении команд и результатов приведено в таблице 26.**
show users	-	Отображение информации о пользователях, использующих ресурсы устройства.
show system information	-	Вывод системной информации.
show nvram	-	Отображение информации об устройстве в энергонезависимой памяти.
show tech-support	-	Отображение информации об устройстве, необходимой для начальной диагностики проблем.

Команды режима privileged EXEC

Запрос командной строки в режиме privileged EXEC имеет следующий вид:

```
console#
```

Таблица 25 – Команды управления системой в режиме privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
reload	-	Команда служит для перезапуска устройства
show env CPU	-	Мониторинг утилизации CPU
show env tasks	-	Мониторинг утилизации CPU по процессам
show env RAM	-	Мониторинг утилизации RAM
show env temperature	-	Мониторинг термодатчика
show env flash	-	Мониторинг flash-памяти
show env power	-	Мониторинг питания
show env all	-	Мониторинг всех параметров окружения
show env dry-contacts	-	Мониторинг текущего состояния сухих контактов
show env fan	-	Мониторинг состояния вентиляторов

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

Таблица 26 – 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.

Команды режима глобальной конфигурации

Запрос командной строки в режиме глобальной конфигурации имеет следующий вид:

```
console(config)#
```

Таблица 27 – Команды управления системой в режиме глобальной конфигурации

Команда	***Значение/Значение по умолчанию***	***Действие***
hostname *name*	name: (1..32) символов/-	Команда служит для задания сетевого имени устройства.
no hostname		Вернуть сетевое имя устройства в значение по умолчанию.
cpu rate limit queue <*queue*> **maxrate** *pps*	queue: (1-8)pps: 1..2000	Установка ограничений скорости входящих фреймов для определенной очереди - *pps* - пакетов в секунду. Пример трафика и номер очереди: 3-DHCP 4-ARP 5-IGMP/MLD 6-CPU MAC 8-LBD
cpu-rate limit queue *queue* **maxrate 128**		Восстанавливает значение *pps* по умолчанию для определенной очереди
reset-button {enable | disable | reset-only}	-/enable	**enable** – при нажатии кнопки F длительностью менее 10 секунд, происходит перезагрузка устройства; при нажатии на кнопку более 10 секунд, происходит сброс устройства до заводской конфигурации; **disable** – кнопка F отключена (не реагирует на нажатие); **reset-only –** только перезагрузка.

Таблица 28 – Команды режима Privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
clear cpu rate limit counters	-	Очистить счетчики rate limit на CPU
show cpu rate limit	-	Отображение счетчиков rate limit на CPU
set cli pagination on	-/on	Включить постраничный вывод конфигурации
set cli pagination off		Отключить постраничный вывод конфигурации

4.4 Команды для настройки параметров для задания паролей

Данный раздел предназначен для настройки задания паролей для пользователей.

Команды режима глобальной конфигурации

Запрос командной строки в режиме глобальной конфигурации имеет следующий вид:

```
console(config)#
```

Таблица 29 – Команды управления системой в режиме глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
password validate char {lowercase | numbers | symbols | uppercase}	-/выключено	Включить механизм проверки паролей. - *lowercase* – пароль должен содержать символы нижнего регистра; - *numbers* – пароль должен содержать хотя бы одну цифру; - *symbols* – пароль должен сожержать хотя бы один символ; - *uppercase*–пароль должен содержать символы верхнего регистра.
no password validate		Отключить механизм проверки паролей.
password validate length *length*	length: (0..20)/0	Задать минимальную длину пароля.
no password validate		Установить значение по умолчанию.

Запрос командной строки в режиме Privileged EXEC имеет следующий вид:

```
console#
```

Таблица 30 – Команды для работы с файлами в режиме Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show password validate rules	-	Просмотр текущей настройки механизма проверки паролей.

4.5 Работа с файлами

4.5.1 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 31.

Таблица 31 – 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.
active-image	Файл с активным образом.
inactive-image	Файл с неактивным образом.
tftp://	Исходный адрес или адрес места назначения для TFTP-сервера. Синтаксис: **tftp://host/[directory]/ filename.** - *host* – IPv4-адрес или сетевое имя устройства; - *directory* – каталог; - *filename* – имя файла.
logging	Файл с историей команд.

4.5.2 Команды для работы с файлами

Запрос командной строки в режиме Privileged EXEC имеет следующий вид:

```
console#
```

Таблица 32 – Команды для работы с файлами в режиме Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
copy *source_url destination_url* **image**	source_url: (1..160) символов; destination_url: (1..160) символов	Копирование файла из местоположения источника в местоположение назначения. - *source_url* – местоположение копируемого файла; - *destination_url* – адрес места назначения, куда файл будет скопирован.
copy startup-config *destination_url*		Сохранение первоначальной конфигурации на сервере.
copy*source_url***boot**		Копирование файла начального загрузчика из местоположения источника в систему.
erase *url*	-	Удаление файла.
erase startup-config	-	Удаления файла первоначальной конфигурации.
erase nvram:	-	Сбросить до дефолтной энергонезависимую память.
boot system inactive	-	Загрузиться с неактивного образа ПО.
boot system active	-	Загрузиться с активного образа ПО.
delete startup-config	-	Удаление файла первоначальной конфигурации вместе с очисткой глобальных настроек nvram и удалением пользователей.
show running-config [**interface {gigabitethernet** *gi_port* **| fastethernet** *fa_port* **| port-channel** *group* **| vlan** *vlan_id* **][module]**	fa_port: (0/1..24); gi_port: (0/1..24); group: (1..8); vlan: (2..4094); module: (igs, la, stp..)	Отображает содержимое файла первоначальной конфигурации (startup-config) или текущей конфигурации (running-config). - **interface –** конфигурация интерфейсов коммутатора - физических интерфейсов, групп интерфейсов (port-channel), VLAN-интерфейсов, интерфейса замыкания на себя; - *igs*– IGMP snooping; - *la* – link-aggregation; - *stp* – spanning-tree.
show startup-config	-	Отображает содержимое файла первоначальной конфигурации.
show bootvar	-	Показывает активный файл системного ПО, который устройство загружает при запуске.
write {startup-config | *url***}**	-	Сохранение текущей конфигурации в файл первоначальной конфигурации.

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

Просмотр активного и неактивного образа досутпен из u-boot. Для этого в командной строке u-boot необходимо ввести:

```
MES2428# bootimg print
```

Команда для смены активного образа из u-boot:

```
MES2428# bootimg inactive
```

Команда «bootimg inactive» применяется без ожидания подтверждения.

4.5.3 Команды для резирвирования конфигурации

В данном разделе описаны команды, позволяющие резервировать конфигурацию на сервер. Для резервирования конфигурации необходимо указать адрес сервера.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 33 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
backup server *dest_url*	-	Указать адрес сервера, на который будет производиться резервирование конфигурации. Строка в формате «tftp://XXX.XXX.XXX.XXX».
no backup server		Удалить адрес сервера.
backup path *path*	-	Указать путь расположения файла на сервере с префиксом имени файла. При сохранении к префиксу будет добавлена текущая дата и время в формате ггггммддччммсс.
no backup path		Удалить путь для резервирования.
backup auto	-	Включить автоматическое резервирование конфигурации.
no backup auto		Выключить автоматическое резервирование конфигурации.
backup history enable	-	Включить сохранение истории резервных копий.
no backup history enable		Выключить сохранение истории резервных копий.
backup time-period *timer*	timer: (1..35791394)/720 минут	Указать промежуток времени, по истечении которого будет осуществляться овтоматическое резервирование конфигурации.
no backup time-period		Установить значение по умолчанию.
backup write-memory	-/выключено	Включение резервирования конфигурации при сохранении пользователем конфигурации на flash-накопитель.
no backup write-memory		Установить значение по умолчанию.

Команды режима PrivilegedEXEC

Запрос командной строки в режиме Privileged EXEC имеет следующий вид:

```
console#
```

Таблица 34– Команды настройки системного времени в режиме Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
backup running-config	-	Создать резервную копию конфигурацию на сервере.

4.6 Настройка системного времени

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

Команды режима Privileged EXEC

Запрос командной строки в режиме Privileged EXEC имеет следующий вид:

```
console#
```

Таблица 35 – Команды настройки системного времени в режиме Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
clock set *hh:mm:ss day month year*	hh: (0..23); mm: (0..59); ss: (0..59); day: (1..31); month: (Jan..Dec); year: (2000..2037)	Ручная установка системного времени (команда доступна только для привилегированного пользователя). - *hh* – часы, *mm* – минуты, *ss* – секунды; - *day* – день; *month* – месяц; *year* – год.

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 36 – Команды настройки системного времени в режиме «EXEC»

Команда	*Значение/Значение по умолчанию*	*Действие*
show clock	-	Показывает системное время и дату.
show clock properties		Отображает свойства.

Команды режима глобальной конфигурации

Запрос командной строки в режиме глобальной конфигурации имеет следующий вид:

```
console(config)#
```

Таблица 37 – Список команд для настройки системного времени в режиме глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
clock time source {atomic-clock | gps | internal-oscillator | ntp | ptp}	-	Установить источник синхронизации времени для устройства.
clock time source		Установить значение по умолчанию.
clock utc-offset *utc*	utc: (+00:00..+14:00)	Установить часовое смещение относительно нулевого меридиана.
no clock utc-offset		Установить значение по умолчанию.

Команды режима конфигурации SNTP[1]

Для перехода в режим конфигурации SNTP необходимо использовать команду:

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

Запрос командной строки в режиме конфигурации интерфейса имеет следующий вид:

```
console(config-sntp)#
```

Таблица 38 – Список команд для настройки системного времени в режиме конфигурации sntp

Команда	*Значение/Значение по умолчанию*	*Действие*
sntp	-	Перейти в режим конфигурирования протокола SNTP
set sntp broadcast-mode send-request enabled	-/выключено	Включить отправку request на сервер в broadcast режиме
set sntp broadcast-mode send-request disabled		Выключить отправку request на сервер в broadcast режиме
set sntp multicast-mode send-request enabled	-/выключено	Включить отправку request на сервер в multicast режиме
set sntp multicast-mode send-request disabled		Выключить отправку request на сервер в multicast режиме
set sntp unicast-server auto-discovery enabled	-	Включить автоматический поиск sntp-сервера в режиме unicast
set sntp unicast-server auto-discovery disabled		Выключить автоматический поиск sntp-сервера в режиме unicast
set sntp unicast-server domain-name *name* **[primary | secondary] [version** *version***] [port** *udp_port***]**	port: (1025..36564); version: (3..4)	Указать домен сервера SNTP.
no sntp unicast-server domain-name *name*		Удалить домен сервера SNTP.
set sntp unicast-server ipv4 *ip_addr* **[secondary]**	-	Указать ipv4-адрес SNTP-сервера - secondary — указать резервный ntp-сервер
no sntp unicast-server ipv4 *ip_addr*		Удалить ipv4-адрес SNTP-сервера
set sntp client enable	-	Включить работу SNTP-клиента
set sntp client disable		Выключить работу SNTP-клиента
set sntp client addressing-mode {broadcast | multicast | unicast}	-	Указать режим работы SNTP-клиента
set sntp client authentication-key *key* **md5** *parametrs*	key: (0..65535)	Установить ключ аутентификации для SNTP-клиента
set sntp client clock-format {ampm | hours}	-/hours	Установить формат часов для SNTP
set sntp client port *port_num*	port_num: (123, 1025-65535)	Установить udp-порт для sntp-клиента
set sntp client time-zone *zone*	zone: (+00:00 to +14:00)	Задать значение часового пояса
set sntp client version *version*	version: (v1,,v4)	Задать версию протокола для работы sntp-клиента
show sntp statistics	-	Показывает статистику протокола SNTP.
show sntp status	-	Показывает статус протокола SNTP.

Пример настройки SNTP-клиента для сервера 192.168.1.1:

```
console(config)# sntp
console(config-sntp)# set sntp client enabled
```

[1] В версии 10.1.8.2 поддержан только режим unicast-server

```
console(config-sntp)# set sntp client addressing-mode unicast
console(config-sntp)# set sntp unicast-server ipv4 192.168.1.1
console(config-sntp)#
exit
console(config)#clock time source ntp
```

4.7 Конфигурация интерфейсов и VLAN

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

Команды режима конфигурации интерфейса (диапазона интерфейсов)

```
console# configure
console(config)# interface { gigabitethernet gi_port | fastethernet
fa_port | port-channel group | range {…} | loopback loopback_id }
console(config-if)#
```

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

Выбор интерфейса осуществляется при помощи команд приведённых в таблице 39:

Таблица 39 – Команды выбора интерфейса для MES1424, MES2428

Команда	*Назначение*
interface gigabitethernet *gi_port*	Для настройки 1G-интерфейсов
interface fastethernet *fa_port*	Для настройки интерфейсов Fast Ethernet
interface port-channel *group*	Для настройки групп каналов
interface loopback *loopback_id*	Для настройки виртуальных интерфейсов

где:

- *gi_port* – порядковый номер 1G-интерфейса, задается в виде: 0/1;
- *fa_port* – порядковый номер 100MB-интерфейса, задается в виде: 0/1;
- *group* – порядковый номер группы, общее количество согласно таблице 9 (строка «Агрегация каналов (LAG)»);
- *loopback_id* – порядковый номер виртуального интерфейса, общее количество согласно таблице 9 (строка «Количество виртуальных Loopback-интерфейсов»).

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

Таблица 40 – Команды режима конфигурации интерфейсов Ethernet и Port-Channel

Команда	*Значение/Значение по умолчанию*	*Действие*
shutdown	-/включен	Выключить конфигурируемый интерфейс (Ethernet, port-channel).
no shutdown		Включить конфигурируемый интерфейс.
description *descr*	descr: (1..64) символов/нет описания	Добавить описание интерфейса (Ethernet, port-channel).
no description		Удалить описание интерфейса.
speed *mode*	mode: (10, 100, 1000)	Задать скорость передачи данных (Ethernet).
no speed		Установить значение по умолчанию.
duplex *mode*	mode: (full, half)/full	Задать режим дуплекса интерфейса (полнодуплексное соединение, полудуплексное соединение, Ethernet).
no duplex		Установить значение по умолчанию.
negotiation	on,off/on	Включает автосогласование для скорости и дуплекса на настраиваемом интерфейсе.

no negotiation		Выключает автосогласование для скорости и дуплекса на настраиваемом интерфейсе.
flowcontrol *mode*	mode: (on, off, auto)/off	Задать режим управления потоком flowcontrol (включить, отключить или автосогласование). Автосогласование flowcontrol работает только в случае, если режим автосогласования negotiation включен на настраиваемом интерфейсе (Ethernet, port-channel).
no flowcontrol		Отключить режим управления потоком.
media-type { force-fiber | force-copper | prefer-fiber }	-/prefer-fiber	Выбор типа комбо-порта в качестве основного носителя. **- force-fiber**– разрешена активность только оптической части комбо-порта; **- force-cooper –** разрешена активноч ть только медной части комбо-порта; **- prefer-fiber**– преимущество оптического линка.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 41 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
errdisable recovery interval *interval*	interval: (30..86400)/300	Установить временной интервал для автоматического повторного включения интерфейса. При смене интервала таймер обновляется для всех заблокированных портов, на которых включено автосогласование.
errdisable recovery interval		Установить значение по умолчанию.
errdisable recovery cause {storm-control|loopback-detection | udld}	-/запрещено	Включить автоматическую активацию интерфейса после его отключения в следующих случаях: - **loopback-detection** – обнаружение петель; - **udld** – активация защиты UDLD; - **storm-control –** широковещательный шторм.
no errdisable recovery cause {storm-control|loopback-detection | udld}		Установить значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки в режиме EXEC:

```
console#
```

Таблица 42 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
clear counters	-	Сброс статистики для всех интерфейсов.
clear counters { gigabitethernet *gi_port* **| fastethernet** *fa_port* **| port-channel** *group* **}**	fa_port: (0/1..24); gi_port: (0/1..24); group: (1..8)	Сброс статистики для интерфейса.
show interfaces {gigabitethernet *gi_port* **| fastethernet** *fa_port* **| port-channel** *group*}	fa_port: (0/1..24); gi_port: (0/1..24); group: (1..8)	Показать сводную информацию о состоянии, настройке и статистике порта.
show interfaces status	-	Показать состояние всех интерфейсов.
show interfaces description	-	Показать описания всех интерфейсов.
show interfaces counters	-	Показать статистику для всех интерфейсов.
show interfaces counters { gigabitethernet *gi_port* **| fastethernet fa_port | port-channel** *group* **| vlan** *vlan_id* **}**	fa_port: (0/1..24); gi_port: (0/1..24); group: (1..8); vlan: (1..4094)	Показать статистику для интерфейса.

show errdisable interfaces { gigabitethernet *gi_port* **| fastethernet** *fa_port* **}**	fa_port: (0/1..24); gi_port: (0/1..24);	Показать причину отключения порта, группы портов, заблокированные порты.
show errdisable recovery	-	Показать настройки для автоматической повторной активации порта.
set interface active {gigabitethernet *gi_port* **| fastethernet** *fa_port***}**	fa_port: (0/1..24); gi_port: (0/1..24);	Активировать интерфейс после errdisable.
show interfaces utilization {gigabitethernet *gi_port* **| fastethernet** *fa_port***} {interval** *interval***}**	fa_port: (0/1..24); gi_port: (0/1..24); interval: (5, 60, 300) сек	Показать статистику по нагрузке для интерфейса. - *Interval* – интервал в секундах.

4.7.2 Настройка VLAN и режимов коммутации интерфейсов

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 43 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
vlan *vlan_id*	vlan_id: (2..4094)	Перейти в режим конфигурирования указанного VLAN
mapprotocol {appletalk | ip | netbios | novell | otherprotocol} {enet-v2 | llcOther | snap} protocols-groupgroup-id	-/PBV глобально включен	Настраивает группу протоколов, по которым будет производится классификация кадров. В одну группу можно объединить несколько протоколов, указывая для них один и тот же Group ID. Номер протокола можно выбрать из списка предустановленных значений или задать вручную через параметр other в формате XX:XX. Расположение поля с номером протокола зависит от типа L2-заголовка и инкапсуляции: **- enet-v2** – кадр с заголовком Ethernet II, протокол определяется по полю EtherType. При наличии VLAN-тегов выбирается самый последний EtherType, с наибольшим оффсетом. **- llcOther** – кадр формата RFC1042 (IEEE 802). Двухбайтный номер протокола соответствует полям DSAP:SSAP в LLC-заголовке. **- snap** – кадр с LLC/SNAP-инкапсуляцией. Номер протокола соответствует полю Protocol ID в SNAP-заголовке.
no protocol-vlan		Выключает Protocol-based VLAN на всех портах устройства.

Команды режима конфигурации VLAN (диапазон VLAN'ов)

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

Таблица 44 – Команды режима конфигурацииVLAN

Команда	*Значение/Значение по умолчанию*	*Действие*
vlan active	–	Активировать vlan или группу vlan'ов
set unicast-mac learning { enable | disable}	–	Включить/выключить изучение MAC-адресов для VLAN
set unicast-mac learning default		Установить значение по умолчанию

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

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

```
console# configure
console(config)# interface { fastethernet fa_port | gigabitethernet
gi_port | port-channel group}
console(config-if)#
```

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

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;

Таблица 45 – Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
switchport mode *mode*	mode: (access, trunk, general)/general	Задать режим работы порта в VLAN. - *mode* – режим работы порта в VLAN.
no switchport mode		Установить значение по умолчанию.
switchport access vlan *vlan_id*	vlan_id: (1..4094)/1	Добавить VLAN для интерфейса доступа. - *vlan_id* – идентификационный номер VLAN.
no switchport access vlan		Установить значение по умолчанию.
switchport dot1q tunnel	-	Перевести порт режим работы с внешним VLAN-тегом. Команда используется для настройки функции Q-in-Q.
switchport trunk native vlan *vlan_id*	vlan_id: (1..4094)/1	Добавляет номер VLAN в качестве Default VLAN для данного интерфейса. Весь нетегированный трафик, поступающий на данный порт, определяется в данную VLAN. - *vlan_id* – идентификационный номер VLAN.
no switchport trunk native vlan		Установить значение по умолчанию.
switchport dot1q tunnel	-	Перевести порт режим работы с внешним VLAN-тегом. Команда используется для настройки функции Q-in-Q.
switchport general allowed vlan add *vlan_list* **[untagged]**	vlan_list: (2..4094)	Добавить список VLAN для интерфейса. - *vlan_list* – список VLAN ID. Диапазон VLAN можно задать перечислением через запятую или указать начальное и конечное значения диапазона через дефис "-".
switchport general allowed vlan remove *vlan_list*		Удалить список VLAN для интерфейса.
switchport general pvid *vlan_id*	vlan_id: (1..4094)/1 – если установлен VLAN по умолчанию	Добавить идентификатор VLAN порта (PVID) для основного интерфейса. - *vlan_id* – идентификационный номер VLAN порта.
no switchport general pvid		Установить значение по умолчанию.
switchport ingress-filter	-/фильтрация включена	Включить 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.
no switchport ingress-filter		Выключить фильтрацию входящих пакетов на основе присвоенного им значения VLAN ID.

switchport acceptable-frame-type {untaggedAndPrioritytagged | tagged | all}	-/all	-untaggedAndPrioritytagged - на порту разрешается прием только нетегированных фреймов -tagged --//- только тегированны -all - любых фреймов
switchport forbidden vlan add *vlan_list*	vlan_list: (2..4094, all)/все VLAN разрешены порту	Запретить добавление указанных VLAN порту. - *vlan_list* – список VLAN ID. Диапазон VLAN можно задать перечислением через запятую или указать начальное и конечное значения диапазона через дефис "-".
switchport forbidden vlan remove *vlan_list*		Разрешить добавление указанных VLAN-порту.
switchport protected	-	Переводит порт в режим изоляции внутри группы портов.
no switchport protected		Восстанавливает значение по умолчанию.
port-isolation { gigabitethernet *gi_port* **| fastethernet** *fa_port* **| port-channel** *group* **}**	fa_port: (0/1..24); gi_port: (0/1..24); group: (1..8)	Создать или перезаписывает существующий список портов на указанный новый.
port-isolation {add | remove} {gigabitethernet *gi_port* **| fastethernet** *fa_port* **| port-channel** *group***}**	fa_port: (0/1..24); gi_port: (0/1..24); group: (1..8)	Добавить список указанных портов к уже существующему списку.
switchport default-vlan tagged	-	Установить порт как тегирующий в дефолтной VLAN.
no switchport default-vlan tagged		Установить значение по умолчанию.
switchport map protocols-group *group-id* **vlan** *vlan-id*	group_id: (1..2147483647); vlan_id: (1..4094)/по умолчанию PBV включен на всех портах	Назначает VLAN ID пакетам, попадающим в указанную Group ID на этом порту. Разные порты одной и той же группы могут соответствовать разным VLAN.
no port protocol-vlan		Выключает PBV на порту.
Port mac-vlan	-/отключено	Перевести порт в режим работы PBV.
no port mac-vlan		Отключить режим PBVна интерфейсе.
mac-map *aa:bb:cc:dd:ee:ee 00:ff:ff:00:00:00* **vlan** *vlan_id*	-	Привязать MAC-адрес или диапазон MAC-адресов по маске к группе MAC-адресов.
no mac-map *aa:bb:cc:dd:ee:ee*		Отменить привязку

При совместной работе port-isolation и port-protected должно соблюдаться правило: для защищённого ingress порта, в списке разрешённых, команды `port-isolation`, не может быть другого защищённого порта. Это подразумевает возможность делать защищёнными egress порты в изоляции или ingress порт, но не ingress и egress порты одновременно.

Пример настройки Q-in-Q с добавлением метки 99 VLAN:

```
console#configure terminal
console(config)# user-defined tpid 0x9999
console(config)# switch  default
console(config-rag)# !
console(config)# interface gi 0/1
console(config-if)# switchport acceptable-frame-type
untaggedAndPriorityTagged
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 99
console(config-if)# switchport dot1q tunnel
console(config-if)# switchport dot1q ethertype ingress stag 0x8100 0x88a8
console(config-if)# !
console(config)# interface gi 0/2
console(config-if)# switchport mode trunk
console(config-if)# switchport dot1q tunnel
```

Клиентский порт для работы Q-in-Q обязательно должен быть в режиме access.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 46 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
mac-address-table static unicast *mac_add* **vlan** *vlan* **interface [gigabitethernet gi_port | fastethernet** *fa_port***] status [deleteOnReset | deleteOnTimeout | permanent]**	vlan_id: (1..4094); fa_port: (0/1..24); gi_port: (0/1..24)	Добавляет исходный MAC-адрес в таблицу групповой адресации. *Permanent* – данный MAC-адрес остается в таблице адресации после переключения статуса интерфейса; *Deleteonreset* – данный адрес удалится после перезагрузки устройства; *Deleteontimeout* – данный адрес удалится по тайм-ауту
no mac-address-table static unicast *mac_add* **vlan** *vlan*		Удаляет MAC-адрес из таблицы групповой адресации
clear mac-address-table dynamic [interface {gigabitethernet *gi_port* **| fastethernet** *fa_port***} | vlan** *vlan***]**	vlan_id: (1..4094); fa_port: (0/1..24); gi_port: (0/1..24)	Удаляет динамические записи из таблицы групповой адресации.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 47 – Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show mac-address-table address *mac_addr*	-	Просмотр всей таблицы MAC-адресов
show mac-address-table count	-	Показывает количество записей в таблице MAC-адресов
show mac-address-table count summary	-	Показывает суммарную статистику по таблице MAC-адресов.
show mac-address-table dynamic unicast	-	Показывает таблицу с динамическими MAC-адресами
show mac-address-table interface [gigabitethernet *gi_port* **fastethernet** *fa_port***]**	fa_port: (0/1..24); gi_port: (0/1..24)	Показывает таблицу MAC-адресов для указанного интерфейса
show mac-address-table static unicast	-	Показывает таблицу со статическими MAC-адресами
show mac-address-table vlan *vlan*	vlan_id: (1..4094);	Показывает таблицу MAC-адресов для указанного VLAN

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 48 – Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show vlan	-	Показать информацию по всем VLAN.
show vlan id *vlan_id*	vlan_id: (1..4094)	Показать информацию по конкретному VLAN.
show vlan protocols-group	-	Показывает информацию о настроенных группах и протоколах.
show protocol-vlan	-	Показывает информацию о VLAN, соответствующих группам протоколов на разных портах.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 49 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show interfaces switchport {gigabitethernet *gi_port* **| fastethernet** *fa_port***}**	fa_port: (0/1..24); gi_port: (0/1..24)	Показать конфигурацию порта, группы портов.

4.8 Selective Q-in-Q

Данная функция позволяет на основе сконфигурированных правил фильтрации по номерам внутренних VLAN (CustomerVLAN) производить добавление внешнего SPVLAN (Service Provider's VLAN), подменятьCustomer VLAN, а также запрещать прохождение трафика.

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

Вид запроса командной строки режима конфигурации интерфейса конфигурации:

```
console# configure
console(config)# interface{fastethernet fa_port | gigabitethernet gi_port
| port-channelgroup|range{…}}
console(config-if)#
```

Таблица 50 – Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
selective-qinq list ingress override-vlan *vlan_id* **[ingress_vlan***ingress_vlan_id***]**	vlan_id: (1..4094) ingress_vlan_id: (1..4094)	Создает правило, на основании которого внешняя метка *ingress_vlan_id* входящего пакета будет заменяться на vlan_id. Если *ingress_vlan_id*не указывать – правило будет применяться ко всем входящим пакетам.
no selective-qinq list ingress ingress-vlan*vlan_id*		Удаляет указанное правило selective qinq для входящих пакетов. Команда без параметра «ingress vlan» удаляет правило по умолчанию.
selective-qinq list egress override_vlan *vlan_id* **[ingress_vlan** *ingress_vlan_id***]**	vlan_id(1..4094); ingress_vlan_id: (1..4094)	Создает правило, на основании которого внешняя метка *ingress_vlan_id* исходящего пакета будет заменяться на vlan_id. Если *ingress_vlan_id* не указывать – правило будет применяться как правило по умолчанию.
no selective-qinq list egress ingress_vlan *vlan_id*		Удаляет список правил selective qinq для исходящих пакетов.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 51 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show selective-qinq[fastethernet *fa_port* **| gigabitethernet** *gi_port* **| port-channel** *group***]**	-	Отображает список правил sqinq

4.9 Контроль широковещательного «шторма»

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

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

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 52 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
storm-control mode {kbps | pps}	-/pps	Установить глобально какие единицы измерения необходимо использовать. - *pps* - объем трафика пакетов в секунду - *kbps* - объем трафика кбит в секунду

Команды режима конфигурации интерфейса Ethernet

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

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

Таблица 53 – Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
storm-control multicast level *{pps | kbps}*	pps: (1..262142); kbps: (16..4194272)	Включает контроль многоадресного трафика: - *pps* - объем трафика пакетов в секунду - *kbps* - объем трафика кбит в секунду При обнаружении многоадресного трафика интерфейс может быть отключен (**shutdown**) или добавлена запись в журнал сообщений (**trap**).
no storm-control multicast level {pps | kbps}	-	Выключает контроль многоадресного трафика.

storm-control dlf level *{pps | kbps}*	pps: (1..262142); kbps: (16..4194272)	Включает контроль неизвестного одноадресного трафика. - *pps* - объем трафика пакетов в секунду - *kbps* - объем трафика кбит в секунду При обнаружении неизвестного одноадресного трафика интерфейс может быть отключен (**shutdown**) или добавлена запись в журнал сообщений (**trap**).
no storm-control dlf level {pps | kbps}	-	Выключает контроль одноадресного трафика.
storm-control broadcast level *{pps | kbps}*	pps: (1..262142); kbps: (16..4194272)	Включает контроль широковещательного трафика. - *pps* - объем трафика пакетов в секунду - *kbps* - объем трафика кбит в секунду При обнаружении широковещательного трафика интерфейс может быть отключен (**shutdown**) или добавлена запись в журнал сообщений (**trap**).
no storm-control broadcast level {pps | kbps}	-	Выключает контроль широковещательного трафика.
storm-control {multicast | dlf | broadcast} action shutdown	-	Отключает интерфейс при обнаружении многоадресного, неизвестного одноадресного или широковещательного трафика.
no storm-control {multicast | dlf | broadcast} action shutdown	-	Отменяет отключение интерфейса при обнаружении многоадресного, неизвестного одноадресного или широковещательного трафика.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 54 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show interface [fastethernet *fa_port* **| gigabitethernet** *gi_port* **| port-channel** *group***] storm-control**	fa_port: (0/1..24); gi_port: (0/1..24); group: (1..8)	Показывает конфигурацию функции контроля широковещательного «шторма» для указанного порта, либо всех портов.
Show storm-control	-	Отображает текущую настройку единиц измерения.

4.10 Группы агрегации каналов – Link Aggregation Group (LAG)

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

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

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

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

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

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

Таблица 55 – Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
channel-group *group* **mode** *mode*	group: (1..8); mode: (on, active, passive)	Добавить ethernet-интерфейс в группу портов. .
no channel-group		Удалить Ethernet-интерфейс из группы портов.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

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

Таблица 56 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
port-channel load-balance {src-dest-mac-ip | src-dest-mac | src-dest-ip | src-dest-mac-ip-port | dest-mac | dest-ip | src-mac | src-ip}	-/src-dest-mac	Задает механизм балансировки нагрузки для стратегии ECMP и для группы агрегированных портов. **- src-dest-mac-ip –** механизм балансировки основывается на MAC-адресе и IP-адресе; **- src-dest-mac –** механизм балансировки основывается на MAC-адресе; **- src-dest-ip –** механизм балансировки основывается на IP-адресе; - **src-dest-mac-ip-port –** механизм балансировки основывается на MAC-адресе, IP-адресе и TCP-порте назначения; - **dest-mac** – механизм балансировки основывается на MAC-адресе получателя; - **dest-ip** – механизм балансировки основывается на IP-адресе получателя;
set port-channel enable	-/отключено	Включить работу LAG
set port-channel disable		Отключить работу LAG
set port-channel independentmode enable		Включить автономный режим работы LAG
set port-channel independentmode disable		Выключить автономный режим работы LAG

4.10.1 Статические группы агрегации каналов

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

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

4.10.2 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 active/passive в режиме конфигурации соответствующего интерфейса.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 57 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
lacp system-priority *value*	value: (0..65535)/1	Устанавливает приоритет системы.
no lacp system-priority		Устанавливает значение по умолчанию.
lacp system-identifier *mac_addr*	-	Установить id участника lacp
No lacp system-identifier		Удалить id участника lacp

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

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

Таблица 58 – Команды режима конфигурации интерфейса Ethernet

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 59 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show lacp [neighbor | counters]	-	Показывает информацию о протоколе LACP.
show etherchannel summary	-	Просмотр информации о LAG.
show etherchannel detail	-	Просмотр подробной информации о LAG.
show etherchannel load-balance	-	Просмотр алгоритма балансировки LAG.
show etherchannel protocol	-	Просмотр протокола LAG.
show etherchannel port	-	Просмотр информации о портах в составе LAG.
show etherchannel port-channel	-	Просмотр информации о LAG.

Пример настройки:

```
console(config)#set port-channel enable
console(config)#interface port-channel 1
console(config-if)# no shut
console(config-if)#exit
console(config)#interface range fa 0/1-2
console(config-if-range)#no shutdown
console(config-if-range)#channel-group 1 mode active
```

4.11 Настройка IPv4-адресации

В данном разделе описаны команды для настройки статических параметров IP-адресации, таких как IP-адрес, маска подсети, шлюз по умолчанию.

Команды режима конфигурации интерфейса VLAN

Вид запроса командной строки в режиме конфигурации интерфейса VLAN:

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

Таблица 60 – Команды режима конфигурации интерфейса

Команда	*Значение/Значение по умолчанию*	*Действие*
ip address *ip_address prefix_length*	prefix_length: (8..32)	Назначение заданному интерфейсу IP-адреса и маски подсети.
no ip address [*IP_address***]**		Удаление IP-адреса интерфейса.
ip address dhcp	–	Получение IP-адреса от DHCP-сервера.
no ip address dhcp		Запрет использования протокола DHCP для получения IP-адреса от DHCP-сервера.

По-умолчанию, интерфейсы Vlan находятся в состоянии Admin down. Привести в состояние Admin Up их можно командой `no shutdown`.

Команды режима EXEC

Вид запроса командной строки в режиме EXEC:

```
console>
```

Таблица 61 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip interface vlan *vlan_id*	vlan_id: (1..4094)	Показывает конфигурацию IP-адресации для указанного интерфейса.

4.12 Настройка IPv6-адресации

4.12.1 Протокол IPv6

Коммутаторы поддерживают работу по протоколу IPv6, что является большим преимуществом, т.к. протокол IPv6 разработан для того, чтобы в будущем 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.

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.

4.12.2 Настройка функции IPv6 RA Guard

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

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 62 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
ipv6 nd ra-guardenable	-/выключен	Разрешает коммутатору контролирование посредством функции IPv6 RA guard.
no ipv6 nd ra-guardenable		Выключение функции IPv6 RA guard.
ipv6 nd ra-guard policy*policy_id*	policy_id: (1..65535)	Создать и сконфигурировать policy IPv6 RA guard.
no ipv6 nd ra-guard policy*policy_id*		Удалить policy IPv6 RA guard.
ipv6 rag-acl-list *access_list_num* **seq** *seqmac_addr*	access_list_num: (1..65535); seq: (1..5)	Создает запись в списке доступа RA Guard на основе link layer адреса
no ipv6 rag-acl-list *access_list_num* **seq** *seqmac_addr*		Удаляет запись в списке доступа RA Guard
ipv6 rag-prefix-list *list_id* **seq** *seq prefix*	prefix: (2000::1/64)	Создает запись в списке доступа RA Guard на основе IPv6 префикса
no ipv6 rag-prefix-list *list_id* **seq** *seq prefix*		Удаляет запись в списке доступа RA Guard

Команды режима глобального конфигурирования policy IPv6 RA Guard

Вид запроса командной строки режима конфигурирования policy IPv6 RA Guard:

```
console(config-rag)#
```

Таблица 63 – Команды режима конфигурирования policy IPv6 RA guard

Команда	*Значение/Значение по умолчанию*	*Действие*
device-role {host | router}	-/host	Выбор режима работы порта. - **host** – блокировка всех входящих RA-сообщений; - **router** – фильтрация RA-сообщений в соответствии с настроенными правилами.
other-config flag { on | off | none}	-/none	Управлять O-битом в RA-сообщениях
managed-config flag{ on | off | none}	-/none	Управлять M-битом в RA-сообщениях
router-preference {low | medium | high | none}	-/none	Управлять полем router-preference в RA-сообщениях
match rag-acl-list*acl_num*	acl_num: (1..100)	Осуществляет привязку acl к policy IPv6 RA guard
no match rag-acl-list*acl_num*		Удаляет привязку acl к policy IPv6 RA guard
match rag-prefix-list*prefix_id*	prefix_id: (1..100)	Осуществляет фильтрацию сообщений IPv6 RA guard по-префиксу
no match rag-prefix-list*prefix_id*		Удаляет фильтрацию по префиксу IPv6 RA Guard
match rag-src-ipv6-list*ipv6_prefix_id*	ipv6_prefix_id: (1..100)	Осуществляет фильтрацию сообщений IPv6 RA guard по IPv6-префиксу
no match rag-src-ipv6-list*ipv6_prefix_id*		Удаляет фильтрацию сообщений IPv6 RA Guard по IPv6-префиксу

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки режима конфигурирования интерфейса:

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

Таблица 64 – Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
ipv6 nd ra-guard	-/выключен	Разрешает коммутатору контролирование функции IPv6 RA guard на интерфейсе.
no ipv6 nd ra-guard		Выключение функции IPv6 RA guard на интерфейсе.
ipv6 nd ra-guard trust-state trusted	По умолчанию все порты являются untrusted	Добавляет порт в список доверенных.
ipv6 nd ra-guard trust-state untrusted		Удаление порта из trusted-list
ipv6 nd ra-guard attach-policy*policy_id*	policy_id: (1..65535)	Привязать сконфигурированный policy IPv6 RA guard к интерфейсу
no ipv6 nd ra-guard attach-policy*policy_id*		Удалить policy IPv6 RA Guard на интерфейсе

4.13 Настройка протоколов

4.13.1 Настройка протокола ARP

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

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 65 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
arp *ip_addr hw_addr [***fastethernet** *fa_port |* **gigabitethernet** *gi_port* | **port-channel** *group]*	формат ip_addr: A.B.C.D; формат hw_address: H.H.H H:H:H:H:H:H H-H-H-H-H-H; fa_port: (0/1-24) gi_port: (0/1..24); group: (1..8) vlan_id: (1..4094)	Добавляет статическую запись соответствия IP- и MAC-адресов в таблицу ARP для указанного в команде интерфейса. - *ip_*address – IP-адрес; - *hw_address* – MAC-адрес.
arp *ip_addr hw_addr [***fastethernet** *fa_port |* **gigabitethernet** *gi_port* | **port-channel** *group]*		Удаляет статическую запись соответствия IP- и MAC-адресов из таблицы ARP для указанного в команде интерфейса.
arp timeout *sec*	sec: (30..86400) сек	Настраивает время жизни динамических записей в таблице ARP (сек).
no arp timeout		Устанавливает значение по умолчанию.
clear ip arp	-	Удаляет все динамические записи из ARP-таблицы (команда доступна только для привилегированного пользователя).

Команды режима privileged EXEC

Вид запроса командной строки в режиме privileged EXEC:

```
console#
```

Таблица 66 – Команды режима privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip arp [ip-address *ip_address***] [mac-address** *mac_addres***] [vlan** *vlan_id***]**	формат *ip_address*: A.B.C.D формат *mac_address*: H.H.H или H:H:H:H:H:H или H-H-H-H-H-H; vlan: (1..4094)	Показывает записи ARP-таблицы: все записи, фильтр по IP-адресу; фильтр по MAC-адресу; фильтр по интерфейсу. - *ip_address* – IP-адрес; - *mac_address* – MAC-адрес.
show ip arp statistics	-	Показывает текущую статистику протокола arp

4.13.2 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 глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 67 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
shutdown loopback-detection	-/no shutdown	Отключить работу модуля loopback-detection на устройстве. **Данная команда отключает работу модуля loopback-detection с безвозвратным удалением всех настроек блока LBD.**
no shutdown loopback-detection		Включить работу loopback-detection на устройстве. **Команда по умолчанию включена.**
loopback-detection enable	-/выключено	Включает механизм обнаружения петель для коммутатора.
no loopback-detection enable		Восстанавливает значение по умолчанию.
loopback-detection interval *seconds*	seconds: (1..60)/30 секунд	Устанавливает интервал между loopback-фреймами. - *seconds* – интервал времени между LBD фреймами.
no loopback-detection interval		Восстанавливает значение по умолчанию
loopback-detection destination-address *mac_address*	-/ff:ff:ff:ff:ff:ff	Определяет MAC-адрес назначения, указанный в LDB-фрейме. **По умолчанию MAC-адрес назначения широковещательный.**

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

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

```
console# configure
console(config)# interface {gigabitethernet gi_port | fastethernet fa_port
| port-channel group}
console(config-if)#
```

Таблица 68 – Команды режима конфигурации интерфейса Ethernet

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 69 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show loopback-detection [gigabitethernet *gi_port* **| fastethernet** *fa_port* **| statistics]**	gi_port: (0/1..24); fa_port: (0/1..24)	Отображает состояние механизма loopback-detection.
debug loopback-detection [all | buffer-alloc | control | critical | pkt-dump | pkt-flow]	-/отключено	Включить отправку сообщений по событиям loopback-detection.

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

Максимально допустимое количество экземпляров MSTP – 64.

4.13.3.1 Настройка протокола STP, RSTP

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 70 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
spanning-tree	-/включено	Разрешает использование коммутатором протокола STP.
no spanning-tree		Запрещает использование коммутатором протокола STP.
spanning-tree mode { rst | mst}	-/MSTP	Устанавливает режим работы протокола STP: - **rst** – IEEE 802.1W Rapid Spanning Tree Protocol; - **mst** – IEEE 802.1S Multiple Spanning Tree Protocol.
no spanning-tree mode		Устанавливает значение по умолчанию.
spanning-tree forward-time *seconds*	seconds: (4..30)/15 сек	Устанавливает интервал времени, затрачиваемый на прослушивание и изучение состояний перед переключением в состояние передачи.
no spanning-tree forward-time		Устанавливает значение по умолчанию.
spanning-tree hello-time *seconds*	seconds: (1..2)/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*	seconds: (6..40)/20 сек	Устанавливает время жизни связующего дерева STP.
no spanning-tree max-age		Устанавливает значение по умолчанию.
spanning-tree priority *prior_val*	prior_val: (0..61440)/32768	Настраивает приоритет связующего дерева STP. Значение приоритета должно быть кратно 4096.
no spanning-tree priority		Устанавливает значение по умолчанию.
spanning-tree pathcost dynamic [lag-speed]	-/выключено	Включает динамическое определение ценности пути. lag-speed – определение ценности пути будет вычисляться при изменении скорости LAG
no spanning-tree pathcost		Устанавливает значение по умолчанию.
spanning-tree compatibility {mst | rst | stp}	-/включено	Версия совместимости STP
no spanning-tree compatibility		Установить значение по умолчанию
spanning-tree flush-indication-threshold *value*	value: (0..65535)	Пороговое количество tcn, при котором запускается таймер, который равен значению flush-interval
		Отменить пороговое значение

no spanning-tree flush-indication-threshold		
spanning-tree flush-interval *interval*	interval: (0..500)/0	Установить значение интервала, после которого произойдёт flash MAC-таблицы посде получения tcn
no spanning-tree flush-interval		Установить значение по умолчанию
spanning-tree transmit hold-count *count*	count: (1..10)	Это значение указывает максимальное количество пакетов, которые могут быть отправлены в заданный интервал времени hello-time.
no spanning-tree transmit hold-count		Отменить настройку ограничения пакетов в интервал hello-time
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.

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

Команды режима конфигурации интерфейса Ethernet, интерфейса группы портов

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

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

Таблица 71 – Команды режима конфигурации интерфейса Ethernet, группы портов

Команда	*Значение/Значение по умолчанию*	*Действие*
spanning-tree disable	-/разрешено	Запрещает работу протокола STP на конфигурируемом интерфейсе.
no spanning-tree disable		Разрешает работу протокола STP на конфигурируемом интерфейсе.
spanning-tree cost *cost*	cost: (1..200000000)/см. таблицу 72	Устанавливает ценность пути через данный интерфейс. - *cost* – ценность пути.
no spanning-tree cost		Устанавливает значение, определяемое на основании скорости порта и метода определения ценности пути, см.таблицу 72
spanning-tree port-priority *priority*	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	-	Включает режим, в котором порт при поднятии на нем линка сразу становится в состояние передачи, не дожидаясь истечения таймера.
no spanning-tree portfast		Выключает режим моментального перехода в состояние передачи по поднятию «линка».
spanning-tree loop-guard	-/запрещено	Разрешает защиту, выключающую указанный интерфейс при приеме пакетов BPDU.
no spanning-tree loop-guard		Запрещает защиту, выключающую интерфейс при приёме пакетов BPDU.
spanning-tree guard {root | loop | none}	-/использование глобальной настройки	Включает защиту «корня» для всех связующих деревьев STP выбранного порта. - **root** – запрещает интерфейсу быть корневым портом коммутатора; - **loop** – включает на интерфейсе дополнительную защиту от петель. В случае, если интерфейс находится в состоянии, отличном от Designated и при этом перестает получать BPDU, интерфейс блокируется; - **none** – отключает все Guard-функции на интерфейсе.
no spanning-tree guard		Использовать глобальную настройку.

spanning-tree bpduguard {enable | disable | none}	-/выключено	Разрешает защиту, выключающую интерфейс при приёме пакетов BPDU.
no spanning-tree bpduguard		Запрещает защиту, выключающую интерфейс при приёме пакетов BPDU.
spanning-tree link-type {point-to-point | shared}	-/для дуплексного порта «точка-точка», для полудуплексного – «разветвленный»	Устанавливает протокол RSTP в передающее состояние и определяет тип связи для выбранного порта: - **point-to-point –** точка-точка; - **shared –** разветвлённый.
no spanning-tree link-type		Устанавливает значение по умолчанию.
spanning-tree restricted-tcn	-/выключено	Запрещает прием BPDU с флагом TCN.
no spanning-tree restricted-tcn		Разрешает прием BPDU с флагом TCN.
spanning-tree bpdufilter {disable | enable | | none}	-/disabled	Определяет режим работы BPDU filtering на интерфейсе.
no spanning-tree bpdufilter		Устанавливает значение по умолчанию.
spanning-tree auto-edge	-/включено	Включить автоматическое определение клиентских портов.
no spanning-tree auto-edge		Выключить автоматическое определение клиентских портов.
spanning-tree {bpdu-receive | bpdu-transmit} enable	-/включено	Включает режим приёма и/или передачи на интерфейсе.
spanning-tree {bpdu-receive | bpdu-transmit} disable		Выключает режим приёма и/или передачи на интерфейсе.
spanning-tree layer2-gateway-port	-/выключено	Назначить порт как шлюз 2 уровня. **Spanning-tree на данном порту должен быть в состоянии disabled**
no spanning-tree layer2-gateway-port		Отменить настройку
spanning-tree pseudoRootId priority *priority*	priority: (0..61440)	Настроить приоритет для pseudoRoot на интерфейсе.
no spanning-tree pseudoRootId		Отменить настройку
spanning-tree {restricted-role | restricted-tcn}	-/	Включить на интерфейсе функцию защиты от атак.
no spanning-tree {restricted-role | restricted-tcn}		Отключить на интерфейсе функцию защиты от атак.

Таблица 72 – Ценность пути, установленная по умолчанию (spanning-tree cost)

Интерфейс	***Метод определения ценности пути***	
	Long	***Short***
Port-channel	20000	4
Fast Ethernet (100 Mbps)	2000000	19
Gigabit Ethernet (1000 Mbps)	2000000	100

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 73 – Команды режима privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show spanning-tree interface[**gigabitethernet** *gi_port* | **fastethernet** *fa_port* | **port-channel** *group*]	gi_port: (0/1..24); fa_port: (0/1..24); group: (1..8)	Показывает состояние протокола STP на интерфейсе.

show spanning-tree detail	-	Показывает подробную информацию о настройках протокола STP.
show spanning-tree active [detail]	-	Показывает информацию о состоянии о настройках STP на активных портах
show spanning-tree bridge [address | detail | forward-time| hello-time | id | max-age | priority | protocol]	-	Отображает настройки STP на bridge
show spanning-tree layer2-gateway-port	-	Отображает настройки шлюза 2 уровня
show spanning-tree pathcost method		Отображает метод определения стоимости пути
show spanning-tree root	-	Отображает root в топологии STP
show spanning-tree summary	-	Отображает состояние протокола STP относительно интерфейсов

4.13.3.2 Настройка протокола MSTP

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 74 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
spanning-tree mst *instance_id* **priority** *priority*	instance_id: (1..63); priority: (0..61440)/32768	Устанавливает приоритет для данного коммутатора перед остальными, использующими общий экземпляр MSTP. - *instance_id* – экземпляр MST; - *priority* – приоритет коммутатора. **Значение приоритета должно быть кратно 4096.**
no spanning-tree mst *instance_id* **priority**		Устанавливает значение по умолчанию.
spanning-tree mst max-hops *hop_count*	hop_count: (6..40)/20	Устанавливает максимальное количество транзитных участков для пакета BPDU, необходимых для формирования дерева и удержания информации о его строении. Если пакет уже прошел максимальное количество транзитных участков, то на следующем участке он отбрасывается. - *hop_count* – максимальное количество транзитных участков для пакета BPDU.
no spanning-tree mst max-hops		Устанавливает значение по умолчанию.
spanning-tree mst configuration	-	Вход в режим конфигурации протокола MSTP.

Команды режима конфигурации протокола MSTP

Вид запроса командной строки в режиме конфигурации протокола MSTP:

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

Таблица 75 – Команды режима конфигурации протокола MSTP

Команда	*Значение/Значение по умолчанию*	*Действие*
instance *instance_id* **vlan** *vlan_range*	instance_id:(1..63); vlan_range: (1..4094)	Создает соответствие между экземпляром протокола MSTP и группами VLAN. - *instance-id* – идентификатор экземпляра протокола MSTP; - *vlan-range* – номер группы VLAN.

no instance *instance_id* **vlan** *vlan_range*		Удаляет соответствие между экземпляром протокола MSTP и группами VLAN.
name *string*	string: (1..32) символа	Задает имя конфигурации MST. - *string* – имя конфигурации MST.
no name		Удаляет имя конфигурации MST.
revision *value*	value: (0..65535)/0	Задает номер ревизии конфигурации MST. - *value* – номер ревизии конфигурации MST.
no revision		Устанавливает значение по умолчанию (*value*).
exit	-	Выход из режима конфигурации протокола MSTP с сохранением конфигурации.

Команды режима конфигурации интерфейса Ethernet, интерфейса группы портов

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

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

Таблица 76 – Команды режима конфигурации интерфейса Ethernet, группы портов

Команда	*Значение/Значение по умолчанию*	*Действие*
spanning-tree guard root	-/защита выключена	Включает защиту «корня» для всех связующих деревьев STP выбранного порта. Данная защита запрещает интерфейсу быть корневым портом коммутатора.
no spanning-tree guard root		Устанавливает значение по умолчанию.
spanning-tree mst *instance_id* **port-priority** *priority*	instance_id: (1..63); priority: (0..240)/128	Устанавливает приоритет интерфейса в экземпляре MSTP. - *instance-id* – идентификатор экземпляра протокола MSTP; - *priority* – приоритет интерфейса. **Значение приоритета должно быть кратно 16.**
no spanning-tree mst *instance_id* **port-priority**		Устанавливает значение по умолчанию.
spanning-tree mst *instance_id* **cost** *cost*	instance_id: (1..4094); cost: (1..200000000)	Устанавливает ценность пути через выбранный интерфейс для определенного экземпляра протокола MSTP. - *instance-id* – идентификатор экземпляра протокола MSTP. - *cost* – ценность пути.
no spanning-tree mst *instance_id* **cost**		Устанавливает значение, определяемое на основании скорости порта и метода определения ценности пути, см. таблицу 72
spanning-tree port-priority *priority*	priority: (0..240)/128	Устанавливает приоритет интерфейса в корневом связующем дереве MSTP. **Значение приоритета должно быть кратно 16.**
no spanning-tree port-priority		Устанавливает значение по умолчанию.
spanning-tree mst *instance_id* **pseudoroot** *priority*	instance_id: (1..63); priority: (0..240)/128	Устанавливает приоритет pseudoroot в экземпляре MSTP.
no spanning-tree mst *instance_id* **pseudoroot**	instance_id: (1..63)	Устанавливает значение по умолчанию.

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 77 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show spanning-tree [gigabitethernet *gi_port* **| fastethernet** *fa_port***port-channel** *group***]**	gi_port: (0/1..24); fa_port: (0/1..24); group: (1..8)	Показывает конфигурацию протокола STP.

show spanning-tree detail	instance_id: (1..4094)	Показывает подробную информацию о настройке протокола STP.
show spanning-tree mst configuration	-	Показывает информацию о сконфигурированных экземплярах MSTP.
clear spanning-tree detected protocols {interface {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| port-channel** *group***}}**	gi_port: (0/1..24); fa_port: (0/1..24); group: (1..8)	Перезапускает процесс миграции протокола. Заново происходит просчёт дерева STP.

4.13.4 Настройка функции Layer 2 Protocol Tunneling (L2PT)

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

L2PT инкапсулирует PDU на граничном коммутаторе, передает их на другой граничный коммутатор, который ожидает специальные инкапсулированные кадры, а затем декапсулирует их, что позволяет пользователям передавать информацию 2-го уровня через сеть провайдера.

Команды режима конфигурации интерфейсов Ethernet

Вид запроса командной строки в режиме конфигурации интерфейсов Ethernet:

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

Таблица 78– Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
l2protocol-tunnel {stp | lacp | lldp | isis-l1 | isis-l2 | fctl }	-/выключено	Включение режима инкапсуляции пакетов в STP BPDU
no l2protocol-tunnel {stp | lacp | lldp | isis-l1 | isis-l2 | fctl }		Выключение режима инкапсуляции пакетов в STP BPDU

4.13.5 Настройка протокола LLDP

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

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

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 79 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
set lldp enable	-/выключено	Разрешает коммутатору использование протокола LLDP.
set lldp disable		Запрещает коммутатору использование протокола LLDP.
set lldp management-address {ipv4 *ipv4_address* **| ipv6** *ipv6_address***}**	-/управляющий адрес определяется автоматически	Определяет управляющий адрес на устройстве. - *ip_address* – задается статический IP-адрес; **В случае наличия нескольких IP-адресов система выбирает начальный IP-адрес из диапазона динамических IP-адресов. Если динамические адреса отсутствуют, то система выбирает начальный IP-адрес из диапазона возможных статических IP-адресов.**
set lldp version {v1 | v2}	-/v1	Задать версию протокола LLDP.
lldp *mac_address*	-	Указать MAC-адрес, на который будут отсыдаться lldp-фреймы. lldp-фреймы так же будут дублироваться на стандартный MAC-адрес.
lldp lldpdu flooding	-/filtering	Установить режим фильтрации пакетов LLDP BPDU
lldp lldpdu filtering		Установить значение по умолчанию
lldp chassis-id-subtype *type*	-/mac-address	Задать chassis-id-subtype для lldp-фрейма.
lldp chassis-id-subtype mac-addr		Вернуть к значению по умолчанию
lldp reinitialization-delay *delay*	delay: (1..10)/2	Устанавливает задержку повторной инициализации (время задержки, выполняемое LLDP для повторной инициализации на любом интерфейсе). **Чтобы отменить настройку необходимо выставить значение по умолчанию.**
lldp transmit-interval *interval*	interval: (5-32768)/30	Устанавливает интервал передачи lldp -фреймов. **Чтобы отменить настройку необходимо выставить значение по умолчанию.**
lldp notification-interval *seconds*	seconds: (5-3600)/5	Устанавливает максимальную скорость передачи lldp-фреймов. Seconds – период времени в течении которого устройство может отправить не более одного фрейма. **Чтобы отменить настройку необходимо выставить значение по умолчанию.**
lldp tx-delay *value*	value: (8192)/2	Установить минимальную длительность задержки, между последовательными кадрами LLDP. **Чтобы отменить настройку необходимо выставить значение по умолчанию.**
lldp txCreditmax *value*	value: (1..10)	Устанавливает значение Credit Max (максимальное количество последовательных LLDPDU, которые могут быть переданы в любое время)
lldp txFastInit *value*	value: (1..8)	Установить число пакетов, которое будут отправляться в период fast init.

Команды режима конфигурации интерфейсов Ethernet

Вид запроса командной строки в режиме конфигурации интерфейсов Ethernet:

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

Таблица 80 – Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
lldp dest-mac *mac_address*	-/выключено	Задать MAC-адрес, на который будут отсылаться lldp-фреймы.
lldp dest-mac mac_address		Удалить MAC-адрес, на который будут отсылаться lldp-фреймы.
lldp transmit [mac-address *mac_addr***]**	-/включено	Разрешает передачу пакетов по протоколу LLDP на интерфейсе.
no lldp transmit [mac-address *mac_addr***]**		Запрещает передачу пакетов по протоколу LLDP на интерфейсе.

lldp med-app-type *type* **{none | vlan}**	-	Назначает правило network-policy данному интерфейсу.
no lldp med-app-type *type*		Удалить правило.
lldp med-location {civic-location | coordinate-location | elin-location} location-id {*coordinate civic_address_data | elin_data***}**	-/выключено	Задает местоположение устройства для протокола LLDP (значение параметра location протокола LLDP MED). -coordinate–адрес в системе координат; -civic_address_data–административный адрес устройства; -elin_data–адрес в формате, определенном ANSI/TIA 1057.
no lldp med-location		Удалить местоположение.
lldp med-tlv-select {ex-power-via-mdi | inventory-management | location-id | med-capability | network-policy}	-/выключено	Сконфигурировать TLV LLDP-MED на данном интерфейсе.
no lldp med-tlv-select {ex-power-via-mdi | inventory-management | location-id | med-capability | network-policy}		Удалить настройку TLV LLDP-MED на интерфейсе.
lldp notification {mis-configuration | remote-table-chg} [mac-address *mac_addr***]**	-	Включить отправку трапов по событиям LLDP.
no lldp notification		Отключить отправку трапов по событиям LLDP.
lldp port-id-subtype *subtype*	subtype: (if-alias, if-name, local, mac-addr, port-comp) / interface alias	Задать ID Port Subtype для кадра LLDP
lldp receive [mac-address *mac_addr***]**	-/включено	Разрешить интерфейсу принимать кадры LLDP
no lldp receive [mac-address *mac_addr***]**		Запретить интерфейсу принимать кадры LLDP
lldp tlv-select basic-tlv *tlv_list*	tlv_list: (port-descr, sys-capab, sys-descr, sys-name)	Определяет какие базовые опциональные TLV-поля будут включены устройством в передаваемый LLDP-пакет.
no lldp tlv-select basic-tlv		Устанавливает значение по умолчанию
lldp tlv-select {dot1tlv | dot3tlv} *tlv_list*	tlv_list: (link-aggregation, macphy-config, max-framesize)	Определяет какие специальные опциональные TLV-поля будут включены устройством в передаваемый LLDP-пакет.
no lldp tlv-select {dot1tlv | dot3tlv}		Устанавливает значение по умолчанию

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

Работа протокола LLDP не зависит от состояния протокола STP на порту, пакеты LLDP отправляются и принимаются на заблокированных протоколом STP-портах.

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 81 – Команды режима privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show lldp local	-	Показывает LLDP-информацию, которую анонсируют порты.
show lldp neighbors [detail]	-	Показывает информацию о соседних устройствах, на которых работает протокол LLDP.
show lldp statistics	-	Показывает статистику LLDP.

Таблица 82 – Описание результатов

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

Таблица 83 – 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.

Пример настройки TLV-опций:

```
console(config)# set lldp enable
console(config)# !
```

```
console(config)# interface gigabitethernet 0/1
console(config-if)# no shutdown
console(config-if)# switchport mode trunk
console(config-if)# lldp tlv-select basic-tlv port-descr
console(config-if)# lldp tlv-select basic-tlv sys-name
console(config-if)# lldp tlv-select basic-tlv sys-descr
console(config-if)# lldp tlv-select basic-tlv sys-capab
console(config-if)# lldp tlv-select basic-tlv mgmt-addr ipv4 10.0.0.1
console(config-if)# lldp tlv-select dot1tlv port-vlan-id
console(config-if)# lldp tlv-select dot1tlv protocol-vlan-id all
console(config-if)# lldp tlv-select dot3tlv macphy-config
console(config-if)# lldp tlv-select dot3tlv link-aggregation
console(config-if)# lldp tlv-select dot3tlv max-framesize
console(config-if)# !
```

4.14 Настройка протокола OAM

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

Команды режима конфигурации интерфейсов Ethernet

Вид запроса командной строки в режиме конфигурации интерфейсов Ethernet:

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

Таблица 84– Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
ethernet-oam enable	-/выключено	Разрешить работу OAM
ethernet-oam disable		Запретить работу OAM
ethernet oam link-monitor frame threshold *count*	count: (1..900)/1	Устанавливает порог количества ошибок за указанный период (период устанавливается командой **ethernet oam link-monitor frame window**).
no ethernet-oam link-monitor frame threshold		Восстанавливает значение по умолчанию.
ethernet-oam link-monitor frame window *window*	window: (10..600)/100 мс	Устанавливает временной промежуток для подсчета количества ошибок.
no ethernet-oam link-monitor frame window		Восстанавливает значение по умолчанию.
ethernet-oam link-monitor frame-period threshold *count*	count: (1..900)/1	Устанавливает порог для события «frame-period» (период устанавливается командой **ethernet-oam link-monitor frame-period window**).
no ethernet-oam link-monitor frame-period threshold		Восстанавливает значение по умолчанию.
ethernet-oam link-monitor frame-period window *window*	window: (0xffff../123456..)	Устанавливает временной промежуток для события «frame-period».
no ethernet-oam link-monitor frame-period window		Восстанавливает значение по умолчанию.
ethernet oam link-monitor frame-sec-summary threshold *count*	count: (1..900)/1	Устанавливает порог для события «frame-period» (период устанавливается командой **Ethernet-oam link-monitor frame-seconds window**), в секундах.
no ethernet-oam link-monitor frame-sec-summary threshold		Восстанавливает значение по умолчанию.
ethernet-oam link-monitor frame-sec-summary window *window*	window: (100..9000)/100 мс	Устанавливает временной промежуток для события «frame-period».

no ethernet-oam link-monitor frame-seconds window		Восстанавливает значение по умолчанию.
ethernet-oam mode {active|passive}	-/active	Устанавливает режим работы протокола OAM: - **active** – коммутатор постоянно отправляет OAM PDU; - **passive** – коммутатор начинает отправлять OAM PDU только при наличии OAM PDU со встречной стороны.
ethernet oam remote-loopback {deny | disable | enable | permit}	-/выключено	Команда для управления поддержкой функции заворота трафика. **Deny –** игнорирует команды loopback **Disable –** блокирует loopback **Enable –** включает контроль для loopback **Permit –** включает обработку loopback
ethernet-oam uni-directional detection	-/выключено	Включает функцию обнаружения однонаправленных связей на базе протокола Ethernet OAM.
no ethernet-oam uni-directional detection		Восстанавливает значение по умолчанию.
ethernet-oam uni-directional detection action {log|errdisable}	-/log	Определяет реакцию коммутатора на однонаправленную связь: - **log** – отправка SNMP trap и запись в журнал; - **errdisable** – перевод порта в состояние «error-disable», запись в журнал и отправка SNMP trap.
no ethernet-oam uni-directional detection action		Восстанавливает значение по умолчанию.
ethernet-oam uni-directional detection agressive	-/выключено	Включает агрессивный режим определения однонаправленной связи. Если от соседнего устройства перестают приходить Ethernet OAM-сообщения – линк помечается как однонаправленный.
no ethernet-oam uni-directional detection aggressive		Восстанавливает значение по умолчанию.
ethernet oam uni-directional detection discovery-time *time*	time: (5..300)/5 сек	Устанавливает временной интервал для определения типа связи на порту.
no ethernet-oam uni-directional detection discovery-time		Восстанавливает значение по умолчанию.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 85 – Команды режима глобальной конфигурации

Команда	***Значение/Значение по умолчанию***	***Действие***
set ethernet-oam {enable|disable}	-/disable	Включить/выключить OAM в системе
set ethernet-oam oui *oui*	oui: (aa:aa:aa)	Задать OUI для OAM

Команды режима privileged EXEC

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

```
console#
```

Таблица 86 – Команды режима privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show port ethernet-oam	-	Отображает информацию о текущем состоянии oam
show port ethernet-oam{gigabitethernet *gi_port* **| fastethernet** *fa_port*}	gi_port: (1..8/0/1..48); o_port: (1..8/0/1..4).	Отображает информацию о текущем состоянии oam для конкретного интерфейса
show port ethernet-oam[gigabitethernet *gi_port* **| fastethernet** *fa_port*]**neighbor**	gi_port: (1..8/0/1..48); fo_port: (1..8/0/1..4)	Отображает состояние соседствующей конфигурации
show port ethernet-oam[gigabitethernet *gi_port* **| fastethernet** *fa_port*]**statistics**	gi_port: (1..8/0/1..48); fo_port: (1..8/0/1..4)	Отображает статистику OAM для интерфейсов/конкретного интерфейса
show port ethernet-oam{gigabitethernet *gi_port* **| fastethernet** *fa_port*} event-notifications	gi_port: (1..8/0/1..48); fo_port: (1..8/0/1..4)	Отображает OAM настройки порта
show port ethernet-oam[gigabitethernet *gi_port* **| fastethernet** *fa_port*]	gi_port: (1..8/0/1..48); fo_port: (1..8/0/1..4)	Отображает лог событий состояния OAM
Show ethernet-oam global information	-	Отображает глобальные настройки блока OAM

Пример настройки Ethernet OAM:

```
console(config)# set ethernet-oam enable
console(config)# int gi 0/1
console(config-if)# ethernet-oam enable
```

4.15 Групповая адресация

4.15.1 Функция посредника протокола IGMP (IGMP Snooping)

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

Поддерживаются версии протокола IGMP – IGMPv1, IGMPv2, IGMPv3.

Функция групповой фильтрации “bridge multicast filtering” включена по умолчанию.

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

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 87 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip igmp snooping	-/выключено	Разрешает использование функции IGMP Snooping коммутатором.
no ip igmp snooping		Запрещает использование функции IGMP Snooping коммутатором.
ip igmp snooping vlan *vlan_id*	vlan_id: (1..4094)/выключено	Разрешает использование функции IGMP Snooping коммутатором для данного интерфейса VLAN. - *vlan_id* – идентификационный номер VLAN.
no ip igmp snooping vlan *vlan_id*		Запрещает использование функции IGMP Snooping коммутатором для данного интерфейса VLAN.
ip igmp snooping vlan *vlan_id* **mrouter interface {gigabitethernet** *gi_port* **| fastethernet** *fa_port* **port-channel** *group***}**	fa_port: (0/1..24); gi_port: (0/1..24); group: (1..8);	Определяет порт, к которому подключен маршрутизатор многоадресной рассылки для заданной VLAN. - *vlan_id* – идентификационный номер VLAN.
no ip igmp snooping vlan *vlan_id* **mrouter interface {gigabitethernet** *gi_port* **| fastethernet** *fa_port* **port-channel** *group***}**		Указывает, что к порту не подключен маршрутизатор многоадресной рассылки.
ip igmp snooping vlan *vlan_id* **immediate-leave**	vlan_id: (1..4094); -/выключено	Включить процесс IGMP Snooping Immediate-Leave на текущей VLAN. Означает, что порт должен быть немедленно удален из группы IGMP после получения сообщения IGMP leave.
no ip igmp snooping vlan *vlan_id* **immediate-leave**		Отключить процесс IGMP Snooping Immediate-Leave на текущей VLAN.
ip igmp snooping vlan *vlan_id* **replace source-ip** *ip_add*	vlan_id: (1..4094)/выключено	Включить подмену коммутатором адреса источника на заданный IP-адрес в пакетах IGMP-report в указанном VLAN ip_addr – IP-адрес, который будет использоваться для подмены **Подмена на заданный адрес для транзитного трафика происходит при включенном ip igmp snooping. Подмена на заданный адрес для трафика, исходящего с CPU коммутатора, – при включенном ip igmp snooping и ip igmp snooping proxy-reporting.**
no ip igmp snooping vlan *vlan_id* **replace source-ip**		Выключить подмену коммутатором адреса источника на заданный IP-адрес в пакетах IGMP-report
Ip igmp snooping group-query-interval *value*	value: (2..5)	Установить интервал времени в секундах, после которого устройство отправляет group-query на mrouter
Ip igmp snooping group-query-interval		Установить значение по умолчанию
ip igmp snooping port-purge-interval *value*	value: (130..1225)	Установить интервал времени в секундах, по истечении которого mrouter удаляется, если не получает IGMP reports
No ip igmp snooping port-purge-interval		Отключить настройку
ip igmp snooping query-forward all-ports	-	Включает отправку query во все порты.
ip igmp snooping query-forward non-router		Включает отправку query в non-router-порты
ip igmp snooping report-suppression-interval *value*	value: (1..25)	Интервал (в секундах), для которого IGMPv2 report для одной и той же группы не будут перенаправлены
No ip igmp snooping report-suppression-interval		Отключить настройку
ip igmp snooping retry-count *value*	value: (1..5)	Максимальное количество query, относящихся к группе, отправленных на mrouter
No ip igmp snooping retry-count		Отключить настройку
ip igmp snooping send-query enable	-	Разрешает передачу query-пакетов на устройстве
ip igmp snooping send-query disable		Запрещает передачу query-пакетов на устройстве

ip igmp snooping source-only learning age-timer *interval*	interval: (130..1225)	Установить интервал (в секундах), после которого порт удаляется, если IGMP reports не получены
No ip igmp snooping source-only learning age-timer		Отключить таймер
ip igmp snooping sparse-mode enable	-	Включить режим фильтрации незарегистрированного трафика
ip igmp snooping sparse-mode disable		Отключить режим фильтрации незарегистрированного трафика

Команды режима конфигурации VLAN (диапазон VLAN'ов)

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

Таблица 88 – Команды режима конфигурации VLAN

Команда	*Значение/Значение по умолчанию*	*Действие*
ip igmp snooping replace source-ip*ip_add*	-	Включить подмену коммутатором адреса источника на заданный IP-адрес в пакетах IGMP-report. Ip_addr - IP-адрес, который будет использоваться для подмены **Подмена на заданный адрес для транзитного трафика происходит при включенном ip igmp snooping. Подмена на заданный адрес для трафика, исходящего с CPU коммутатора, – при включенном ip igmp snooping и ip igmp snooping proxy-reporting.**
no ip igmp snooping replace source-ip		Выключить подмену коммутатором адреса источника на заданный IP-адрес в пакетах IGMP-report
ip igmp snooping cos *cos*	cos: (0..7)	Установить значение 802.1p для IGMP-пакетов, которые будут использоваться коммутатором на интерфейсе VLAN.
no ip igmp snooping cos		Удаляет значение метки 802.1p для IGMP-пакетов на интерфейсе VLAN.
ip igmp snooping version {v1 | v2 | v3}	-/v3	Установить версию протокола IGMP в VLAN
ip igmp snooping		Установить значение по умолчанию
ip igmp snooping fast-leave	-/выключен	Включает функцию fast-leave для VLAN.
no ip igmp snooping fast-leave		Выключаетфункцию fast-leave для VLAN.
ip igmp snooping max-response-code*value*	value: (0..255)	Установить максимальное время ответа на запрос, задающееся в коде, где одна единица кода равна одной десятой секунды.
no ip igmp snooping max-response-code		Установить значение по умолчанию.
ip igmp snooping mrouter {gigabitethernet *gi_port* **| fastethernet** *fa_port***}**	fa_port: (0/1..24); gi_port: (0/1..24);	Статически настраивает порты маршрутизатора для VLAN
no ip igmp snooping mrouter-port{gigabitethernet *gi_port* **| fastethernet** *fa_port***}**		Удаляет указанные прты маршрутизатора для VLAN
ip igmp snooping mrouter-port {gigabitethernet *gi_port* **| fastethernet** *fa_port***} [time-out** *time***]**	time: (60..600)	Настраивает интервал ожидания до очистки порта маршрутизатора для интерфейса VLAN.
no ip igmp snooping mrouter {gigabitethernet *gi_port* **| fastethernet** *fa_port***}**		Установить значение по умолчанию.
ip igmp snooping mrouter-port {gigabitethernet *gi_port* **| fastethernet** *fa_port***} version {v1 | v2 | v3}**	fa_port: (0/1..24); gi_port: (0/1..24)	Настраивает версию IGMP для порта маршрутизатора для VLAN. v1- IGMP snooping Version 1 v2 - IGMP snooping Version 2 v3 - IGMP snooping Version 3
no ip igmp snooping mrouter {gigabitethernet *gi_port* **|**		Устанавливает версию по умолчанию.

fastethernet *fa_port***} version**		
ip igmp snooping multicast-vlan profile*index*	index: (1..4294967295)	Привязывает мультикаст-профиль с заданным индексом к VLAN
no ip igmp snooping multicast-vlan profile		Удалить привязку к VLAN
ip igmp snooping querier	-/выключено	Включает поддержку выдачи запросов igmp-query коммутатором во VLAN
no ip igmp snooping querier		Выключает поддержку выдачи запросов igmp-query коммутатором во VLAN
ip igmp snooping query-interval *interval*	interval: (60..600)/выключено	Устанавливает таймаут, по которому система отправляет основные запросы всем участникам группы многоадресной передачи для проверки их активности
no ip igmp snooping query-interval		Установить значение по умолчанию
ip igmp snooping sparse-mode enable	-/выключено	Включить режим фильтрации незарегистрированного трафика в VLAN
ip igmp snooping sparse-mode disable		Отключить режим фильтрации незарегистрированного трафика в VLAN
ip igmp snooping static-group *ip_add***[ports***ports***]**	-	Включение статического запроса multicast-группы в VLAN
no ip igmp snooping static-group *ip_add*		Выключение статического запроса multicast-группы в VLAN

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet

Вид запроса командной строки режима конфигурации интерфейса:

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

Таблица 89 – Команды режима конфигурации интерфейса Ethernet

Команда	***Значение/Значение по умолчанию***	***Действие***
switchport access multicast-tv vlan *vlan_id*	vlan_id: (1..4094)	Включает перенаправление IGMP-запросов с клиентских Vlan в Multicast Vlan и мультикастового трафика в клиентские Vlan для интерфейса в режиме «access».
no switchport access multicast-tv vlan		Выключает перенаправление IGMP-запросов с клиентских Vlan в Multicast Vlan и мультикастового трафика в клиентские Vlan для интерфейса в режиме «access».

Пример настройки подписки на статические группы:

```
console# c t
console(config)# vlan 10
console(config-vlan)#  vlan active
console(config-vlan)#ip igmp snooping static-group 232.0.0.1
console(config-vlan)#ip igmp snooping static-group 232.0.0.2
console(config)# !
console(config)# ip igmp snooping
console(config)# ip igmp snooping proxy-reporting
```

Пример настройки MVR:

В примере gi0/1 - mrouter-port, fa0/1 и fa0/2 - клиентские порты

```
console(config)# vlan 10,20,100
console(config-vlan)# vlan active
console(config-vlan)# exit
console(config)# ip mcast profile 1
console(config-profile)# permit
console(config-profile)# range 232.0.0.1 232.0.0.5
console(config-profile)# profile active
console(config-profile)# exit
```

```
console(config)# ip igmp snooping
console(config)# ip igmp snooping vlan 100
console(config)# ip igmp snooping multicast-vlan enable
console(config)# snooping multicast-forwarding-mode ip
console(config)# vlan 100
console(config-vlan)# ip igmp snooping multicast-vlan profile 1
console(config)# int gi 0/1
console(config-if)# no shut
console(config-if)# switchport mode trunk
console(config-if)# exit
console(config)# int fa 0/1
console(config-if)# switchport acceptable-frame-type untaggedAndPrioritytagged
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 10
console(config-if)# switchport access multicast-tv vlan 100
console(config-if)# exit
console(config)# int fa 0/2
console(config-if)# switchport general allowed vlan add 20untagged
console(config-if)# switchport general pvid 20
console(cofig-if)# switchport access multicast-tv vlan 100 tagged
console(config-if)# exit
```

Команды режима EXEC

Все команды доступны только для привилегированного пользователя.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 90 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip igmp snooping mrouter	-	Показывает информацию об изученных многоадресных маршрутизаторах в указанной группе VLAN.
show ip igmp snooping interface *vlan_id*	vlan_id: (1..4094)	Показывает информацию IGMP-snooping для данного интерфейса.
show ip igmp snooping groups	-	Показывает информацию об изученных многоадресных группах, участвующих в групповой рассылке.

4.15.2 Правила групповой адресации (multicast addressing)

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 91 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
Ip igmp snooping multicast-vlan enable	-	Включить функцию групповой фильтрации.
ip igmp snooping multicast-vlan disable		Выключить функцию групповой фильтрации.

snooping multicast-forwarding-mode ip	-/mac	Настраивает режим обработки multicast-трафика по IP-адресу. **В данном режиме часть multicast-трафика перехватывается устройством на CPU.**
snooping multicast-forwarding-mode mac		Настраивает режим обработки multicast-трафика по MAC-адресу.
snooping leave-process config-level port	-/vlan	Определяет уровень конфигурации механизмов обработки отпуска (конфигурации на основе VLAN или на основе порта)
snooping leave-process config-level vlan		Установить значение по умолчанию
snooping report-process config-levelall-ports	-/non-router-ports	Указывает на каких портах обрабатываются полученные репорты от хоста. Репорты могут обрабатываться на всех портах или на портах, которые не являются mrouter-портами.
snooping report-process config-level non-router-ports		Установить значение по умолчанию

4.15.3 MLD snooping – протокол контроля многоадресного трафика в IPv6

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 92 – Команды глобального режима конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ipv6 mld snooping	-/выключено	Включает MLD snooping
no ipv6 mld snooping		Отключает MLD snooping
ipv6 mld snooping group-query-interval *interval*	interval: (2..5)/2	Установить таймаут, по которому система отправляет основные query-запросы
no ipv6 mld snooping group-query-interval		Устанавливает значение по умолчанию
ipv6 mld snooping mrouter-time-out*time*	time: (60..600)	Устанавливает время ожидания очистки порта отслеживающего маршрутизатора MLD, после которого порт удаляется, если не получены controlpackets маршрутизатором MLD
no ipv6 mld snooping mrouter-time-out		Устанавливает значение по умолчанию
ipv6 mld snooping port-purge-interval*interval*	interval: (130..1225)/260	Задать интервал времени очистки порта отслеживания MLD, после которого порт удаляется, если MLD-reports не получены
no ipv6 mld snooping port-purge-interval		Устанавливает значение по умолчанию
ipv6 mld snooping proxy-reporting	-	Включить функцию proxy-report на устройстве
no ipv6 mld snooping proxy-reporting		Выключить функцию proxy-report на устройстве
ipv6 mld snooping report-forward {all-ports | router-ports}	-	Указать направление репортов: во все порты VLAN или только на порты роутера
no ipv6 mld snooping report-forward		Установить значение по умолчанию
ipv6 mld snooping report-suppression-interval*interval*	interval: (1..25)	Устанавливает временной интервал запрета передачи MLDvSnooping-reports, в течение которого сообщения отчетов MLDv1 не будут перенаправляться на порты маршрутизатора для той же группы

no ipv6 mld snooping report-suppression-interval		Устанавливает значение по умолчанию
ipv6 mld snooping retry-countinrerval*interval*	interval: (1..5)	Устанавливает максимальное количество групповых запросов, отправляемых на порт при получении сообщения MLDv1
no ipv6 mld snooping retry-countinrerval		Устанавливает значение по умолчанию
ipv6 mld snooping send-query enable	-/disable	Включает функцию передачи запросов MLD при изменении топологии
ipv6 mld snooping send-query disable		Выключает функцию передачи запросов MLD при изменении топологии

Команды режима EXEC

Все команды доступны только для привилегированного пользователя.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 93 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ipv6 mld snoopingglobal	-	Отображает глобальные настройки MLD
show ipv6 mld snoopingvlan *vlan_id*	-	Отображает информацию о конфигурации MSD-snooping для данной VLAN.

Команды режима конфигурацииVLAN (диапазон VLAN'ов)

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

Таблица 94 – Команды режима конфигурации VLAN

Команда	*Значение/Значение по умолчанию*	*Действие*
ipv6 mld snooping mrouter {gigabitethernet *gi_port* **| fastethernet** *fa_port***}**	fa_port: (0/1..24); gi_port: (0/1..24)	Привязать порт отслеживающего маршрутизатора MLD к VLAN
No ipv6 mld snooping mrouter {gigabitethernet *gi_port* **| fastethernet** *fa_port***}**		Удалить порт отслеживающего маршрутизатора MLD из VLAN
ipv6 mld snooping version {v1 | v2}	-/v2	Настраивает версию отслеживания MLD в VLAN. v1- IGMP snooping Version 1 v2 - IGMP snooping Version 2
ipv6 mld snooping version		Устанавливает значение по умолчанию

4.15.4 Функции ограничения multicast-трафика

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 95 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip mcast profile *index*	index: (1..4294967295)	Создать multicast-профиль и перейти в режим его конфигурирования
no ip mcast profile *index*		Удалить multicast-профиль

Команды режима конфигурации multicast-профиля

Вид запроса командной строки в режиме конфигурации multicast-профиля:

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

Таблица 96 – Команды режима конфигурации multicast-профиля

Команда	Значение/Значение по умолчанию	Описание
range *first_group_ip last_group_ip*	-	Задать диапазон адресов-источников multicast-трафика. Если задать только один адрес, он станет единственным источником мультикаста.
range *first_group_ip last_group_ip*		Удалить диапазон адресов-источников multicast-трафика.
permit	-/deny	В случае несоответствия одному из заданных диапазонов, IGMP-report будут пропускаться.
deny		В случае несоответствия одному из заданных диапазонов, IGMP-report будут отбрасываться.
profile active	-	Активировать работу профиля

Команды режима конфигурации VLAN

Вид запроса командной строки в режиме конфигурации VLAN:

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

Таблица 97 – Команды режима конфигурации VLAN

Команда	Значение/Значение по умолчанию	Описание
ip igmp snooping multicast-vlan profile *profile*	index: (1.. 4294967295)	Привязать указанный профиль к vlan.

4.16 Функции управления

4.16.1 Механизм AAA

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

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

Для шифрования данных используется *механизм SSH.*

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 98 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
aaa authentication dot1x default group {radius | tacacs+ | tacacsplus}[1]		Устанавливает способ аутентификации для входа в систему. - *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.** **Во избежание потери доступа следует вводить необходимый минимум настроек для указываемого метода аутентификации.**
no aaa authentication dot1x default		Устанавливает значение по умолчанию.
aaa authentication dot1x default local[1]	-	Устанавливает способ аутентификации использующий локальную базу имён пользователей
no aaa authentication dot1x default		Устанавливает значение по умолчанию.
enable password *password* **[level** *level***]**	level: (1..15)/1; password: (5..20) символов	Устанавливает пароль для контроля изменения привилегий доступа пользователей. - *level* – уровень привилегий; - *password* – пароль;
no enable password [level *level***]**		Удаляет пароль для соответствующего уровня привилегий.
username *name* **password** *password* **[privelige** *level***]**	name: (1..20) символов; password: (5..20) символов; level: (1..15)	Добавляет пользователя в локальную базу данных. - *level* – уровень привилегий; - *password* – пароль; - *name* – имя пользователя;
no username *name*		Удаляет пользователя из локальной базы данных

Таблица 99 – 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.

[1] Dot1x не поддержан в версии 10.1.8.2

Таблица 100 – 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 конфигурации терминала

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

Таблица 101 – Команды режима конфигурации терминала

Команда	*Значение/Значение по умолчанию*	*Действие*
login authentication {radius | local | tacacs}	-/настройки глобальной конфигурации	Задает метод аутентификации при входе для консоли, Telnet, SSH
no login authentication		Установить значение по умолчанию
enable authentication {radius | local | tacacs}	-/настройки глобальной гонфигурации	Задает метод аутентификации при повышении уровня привелегий для консоли, Telnet, SSH
no enable authentication		Установить значение по умолчанию

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 102 – Команды режима конфигурации терминальных сессий

Команда	*Значение/Значение по умолчанию*	*Действие*
login authentication {tacacs | default|*list_name***}**	list_name: (1..12) символов	Задает метод аутентификации при входе для консоли, telnet, ssh. - **default** – использовать список «по умолчанию» - ***list_name*** – имя списка аутентификационных методов, активизирующегося,когда пользователь входит в систему - **tacacs** - использовать список TACACS
no login authentication		Устанавливает значение по умолчанию.

4.16.2 Протокол RADIUS

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

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 103 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
radius-server host {*ipv4-address* **|** *ipv6-address* **|** *hostname*} **[timeout** *timeout*] **[retransmit** *retries*] **[key** *secret_key*] **[priority** *priority*]	hostname: (1..158) символов; (0..65535)/1813; timeout: (1..30) сек; retries: (1..15); secret_key: (0..128) символов; priority: (0..65535)/0	Добавляет указанный сервер в список используемых RADIUS-серверов. - *ip_address* – IPv4 или IPv6-адрес RADIUS-сервера; - *hostname* – сетевое имя RADIUS-сервера; - *timeout* – интервал ожидания ответа от сервера; - *retries* – количество попыток поиска RADIUS-сервера; - *secret_key* – ключ для аутентификации и шифрования всего обмена данными RADIUS; - *priority* – приоритет использования RADIUS-сервера (чем ниже значение, тем приоритетнее сервер); - *type* – тип использования RADIUS-сервера; В случае отсутствия в команде параметров *timeout*, *retries*, *secret_key* для данного RADIUS-сервера используются значения настроенные с помощью команд указанных ниже.
no radius-server host {*ipv4-address* **|** *ipv6-address* **|** *hostname*}		Удаляет указанный сервер из списка используемых RADIUS-серверов.

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 104 – Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show radius-servers	-	Отображает параметры настройки RADIUS-серверов (команда доступна только для привилегированных пользователей).
show radius statistics	-	Отображает статистику протокола Radius, информацию о пользователях, конфигурацию RADIUS-сервера.

4.16.3 Протокол TACACS+

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

- *Authentication (проверка подлинности).* Обеспечивается во время входа в систему по именам пользователей и определенным пользователями паролям.
- *Authorization (авторизация).* Обеспечивается во время входа в систему. После завершения сеанса проверки подлинности запускается сеанс авторизации с

использованием проверенного имени пользователя, также сервером проверяются привилегии пользователя.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 105 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
tacacs-server host {*ip_address* **|***hostname***} [single-connection] [port***port***] [timeout** *timeout***] [key***secret_key***]**	hostname: (1..63) символов; port: (0..65535)/49; timeout: (1..30) сек; secret_key: (0..128) символов	Добавляет указанный сервер в список используемых TACACS серверов. - *ip_address* – IP-адрес TACACS-сервера; - *hostname* – сетевое имя TACACS-сервера; - *single-connection* – в каждый момент времени иметь не больше одного соединения для обмена данными с TACACS-сервером; - *port* – номер порта для обмена данными с TACACS-сервером; - *timeout*– интервал ожидания ответа от сервера; - *secret_key* – ключ для аутентификации и шифрования всего обмена данными TACACS; При настройке сервера: «**tacacs-serverhost** *ip_address* **key** *secret_key»* автоматически включается accounting
no tacacs-server host {*ip_address***|** *hostname***}**		Удаляет указанный сервер из списка используемых TACACS-серверов.
tacacs-server retransmit *number*	-/2	Указать количество активных TACACS-серверов, к которым будет поочередно подключиться клиент, в случае неудачной аутентификации
no tacacs-server retransmit		Удалить настройку
tacacs use-server address {*ip_address* **|***hostname***}**	-	Выбирает сервер из таблицы серверов для Tacacs-клиента
no tacacs use-server		Отменяет использование заданного сервера
tacacs authentication type {ascii | pap }	-/pap	Определить метод аутентификации с помощью tacacs.

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 106 – Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show tacacs-servers	-	Отображает параметры настройки TACACS-серверов, метод аутентификации и статистику протокола (команда доступна только для привилегированных пользователей).

4.16.4 Списки доступа ACL для управления устройством

В ISS поддерживается фильтрация управляющего трафика с помощью списка авторизованных IP-менеджеров (IP Authorized Managers). В фильтре можно задать адрес или подсеть источника, VLAN, интерфейс и службу, с которых будет разрешено управление устройством.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 107 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
authorized-manager ip-source *ip_add* **[** *mask* **|** */ prefix_lenght* **| vlan** *vlan_id* **| cpu0] [service snmp | telnet | ssh]**	prefix_lenght: (0..32); vlan_id: (2..4094)	Ограничивает управление устройством по заданному фильтру доступа.
no authorized-manager ip-source *ip_add*		Отменяет ограничение на управление устройством.

На устройстве можно сконфигурировать не больше 10 правил. По умолчанию, если не задано ни одно правило, управление устройством доступно с любого источника.

После указания хотя бы одного правила authorized-manager для всех устройств, которые исключены правилом, будет действовать правило deny any any.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 108 – Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show authorized-managers [ip-source *ip_add***]**	-	Показывает списки доступа для управления.

4.16.5 Настройка доступа

4.16.5.1 Telnet, SSH

Данные команды предназначены для настройки серверов доступа для управления коммутатором. Поддержка серверов TELNET и SSH коммутатором позволяет удаленно подключаться к нему для мониторинга и конфигурации. Конфигурирование устройства через Telnet на устройстве разрешено по умолчанию.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 109 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ssh enable	-/включен	Разрешает удаленное конфигурирование устройства через SSH.
ssh disable		Запрещает удаленное конфигурирование устройства через SSH.
ssh server-address *ip_addr* **port** *port*	port: (1..65535)	Задать IP-адрес SSH-сервера и TCP-порт, используемый SSH-сервером.
ip ssh auth [hmac-md5 | hmac-sha1]	-/hmac-sha1	Выбрать тип аутентификации по протоколу SSH.
ip ssh cipher [3des-cdc | aes128-cdc | aes256-cdc | des-cdc]	-/3des-cdc	Выбрать шифр аутентификации по протоколу SSH.
crypto key generate rsa	-	Генерирует пару ключей RSA – частный и публичный для SSH-сервиса.
feature telnet	-/включено	Разрешает конфигурирование устройства через Telnet
no feature telnet		Запрещает конфигурирование устройства через Telnet

Команды режима EXEC

Команды данного раздела доступны только для привилегированных пользователей.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 110 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip ssh	-	Показывает конфигурацию SSH-сервера, а также активные входящие SSH-сессии.
show telnet server	-	Отображает статус сервера Telnet

4.16.5.2 Команды конфигурации терминала

Команды конфигурации терминала служат для настройки параметров локальной консоли.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 111 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
line console	-	Вход в режим соответствующего терминала

Команды режима конфигурации терминала

Вид запроса командной строки в режиме конфигурации терминала:

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

Таблица 112 – Команды режима конфигурации терминала

Команда	*Значение/Значение по умолчанию*	*Действие*
exec-timeout *seconds*	seconds*:* (0..18000)/0 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		Устанавливает значение по умолчанию
speed {4800 | 9600 | 19200 | 38400 | 57600 | 115200}	-	Установить скороть передачи в линии
enable authentication {radius | tacacs | local}	-/local	Задает метод аутентификации пользователя при повышении уровня привилегий для консоли
no enable authentication		Устанавливает значение по умолчанию
login authentication {radius | tacacs | local}	-/local	Задает метод аутентификации при входе для консоли
no login authentication		Устанавливает значение по умолчанию

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 113 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show line console	-	Показывает параметры терминала.

4.17 Журнал аварий, протокол SYSLOG

Системные журналы позволяют вести историю событий, произошедших на устройстве, а также контролировать произошедшие события в реальном времени. В журнал заносятся события восьми 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 114 **–** 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-server *priotity* **[ipv4 | ipv6]** *ip_address*	-	Включает передачу аварийных и отладочных сообщений на удаленный SYSLOG сервер. - ip_*address*– IPv4 или IPv6-адрес SYSLOG-сервера; - *priority* – приоритет передаваемых сообщений.
no logging-server *priotity* **[ipv4 | ipv6]** *ip_address*		Удаляет выбранный сервер из списка используемых SYSLOG-серверов.
logging console	level: (см. таблицу 115)/informational	Включает передачу аварийных или отладочных сообщений на консоль.

no logging console		Выключает передачу аварийных или отладочных сообщений на консоль.
logging buffered *size*	size: (1..200)50	Изменяет количество сообщений, запоминаемых во внутреннем буфере. Новое значение размера буфера применится после перезагрузки устройства.
no logging buffered		Устанавливает значение по умолчанию.
syslog {filename-one | filename-two | filename-three} *filename*	-	Создать файл записи аварийных и отладочных сообщений.
Erase flash:/LogDir/*filename*		Удалить файл записи аварийных и отладочных сообщений
Logging-file [*level***]** *filename*	level: (128..191) /- filename: (1..32)	Включает передачу аварийных или отладочных сообщений выбранного уровня важности в указанный файл журнала. Level - facility+severity. Например, событие для facility0(128) с уровнем informational (6) будет иметь level = 134.
no logging file		Выключает передачу аварийных или отладочных сообщений в файл журнала.
logging severity [*severity_level***]**	level: (см. таблицу 115)/0	Задать уровень логирования
no logging severity		Установить значение по умолчанию
logging facility local{0..7}	-/local0	Задать категорию логирования
no logging facility		Установить значение по умолчанию
syslog localstorage	-/включено	Активировать отправку аварийных или сообщений на сконфигурированные файлы записи

Каждое сообщение имеет свой уровень важности. В таблице 115 приведены типы сообщений в порядке убывания их важности.

Таблица 115 – 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.

Пример настройки logging-file:

Пусть facility = local0.

Создадим локальный файл с именем sl1, куда будут записываться события с типом от чрезвычайных до информационных.

```
console(config)# syslog localstorage
console(config)# syslog filename-one sl1
console(config)# logging severity 6
console(config)# logging-file 128 sl1
console(config)# logging-file 129 sl1
console(config)# logging-file 130 sl1
console(config)# logging-file 131 sl1
console(config)# logging-file 132 sl1
```

```
console(config)# logging-file 133 sl1
console(config)# logging-file 134 sl1
```

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 116 – Команда режима Privileged EXEC для просмотра файла журнала

Команда	*Значение/Значение по умолчанию*	*Действие*
clear logs	-	Удаляет все сообщения из внутреннего буфера.
show logging-file {filename-one | filename-two | filename-three}	-	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.

4.18 Зеркалирование (мониторинг) портов

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

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

К контролирующему порту применяются следующие ограничения:

- Порт не может быть контролирующим и контролируемым портом одновременно;
- IP-интерфейс должен отсутствовать для этого порта;

К контролируемым портам применяются следующие ограничения:

- Порт не может быть контролирующим и контролируемым портом одновременно.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 117 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
monitor session *session_id* **destination interface [fastethernet** *fa_port* **| gigabitethernet** *gi_port]*	fa_port: (0/1..24); gi_port: (0/1..24); session_id: (1..4)	Указывает зеркалирующий порт для выбранной сессии мониторинга.
no monitor session *session_id* **destination**		Выключает функцию мониторинга на настраиваемом интерфейсе.

monitor session *session_id* **destination remote vlan** *vlan_id*	vlan_id: (1..4094); session_id: (1..4)	Указывается служебный vlan для зеркалирования трафика с заданного рефлектор-порта для выбранной сессии. remote vlan – служебный vlan для зеркалирования трафика;
no monitor session *session_id* **destination**		Выключает функцию мониторинга на настраиваемом интерфейсе.
monitor session *session_id* **source interface [fastethernet |***fa_port* **gigabitethernet** *gi_port* **] [rx | tx | both]**	fa_port: (0/1..24); gi_port: (0/1..24); session_id: (1..4)	Добавляет указанный зеркалируемый порт для выбранной сессии мониторинга. *rx* – копировать пакеты принятые контролируемым портом; *tx* – копировать пакеты, переданные контролируемым портом; *both* – копировать все пакеты с контролируемого порта.
monitor session *session_id* **source interface [fastethernet** *fa_port* | **gigabitethernet** *gi_port]*		Выключает функцию мониторинга на настраиваемом интерфейсе.

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 118 – Команды, доступные в режиме EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show monitor session ***session_id***	session_id: (1..4)	Выводит информацию по сконфигурированной сессии мониторинга.

Примеры выполнения команд

```
console# configure terminal
console(config)# monitor session 2 destination interface gigabitethernet
0/1
```

Вывести информацию по контролирующим и контролируемым портам.

```
console# show  monitor session 2
```

```
Mirroring is globally Enabled.
  Session     : 2
 -------
 Source Ports
   Rx              : None
   Tx              : None
   Both            : None
 Destination Ports : Gi0/1
 Session Status    : Inactive
```

4.19 Функции диагностики физического уровня

Сетевые коммутаторы содержат аппаратные и программные средства для диагностики физических интерфейсов и линий связи. В перечень тестируемых параметров входят следующие:

Для электрических интерфейсов:

- длина кабеля;
- расстояние до места неисправности – обрыва или замыкания.

Для оптических интерфейсов 1G:

- параметры питания – напряжение и ток;
- выходная оптическая мощность;
- оптическая мощность на приеме.

4.19.1 Диагностика медного кабеля

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 119 – Команды диагностики медного кабеля

Команда	*Значение/Значение по умолчанию*	*Действие*
test cable-diagnostics gigabitethernet *gi_port* **| fastethernet** *fa_port* **]**	fa_port: (0/1..24); gi_port: (0/1..24)	Выполняет виртуальное тестирование кабеля для указанного интерфейса.

4.19.2 Электропитание по линиям Ethernet (PoE)

Модели коммутаторов MES2408CP, MES2408IP DC1, MES2408P, MES2408PL и MES2428P поддерживают электропитание устройств по линии Ethernet в соответствии с рекомендациями IEEE 802.3af (PoE) и IEEE 802.3at (PoE+).

Коммутаторы MES2408PL характеризуются меньшим бюджетом мощности, относительно других.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 120 – Команды режима глобальной конфигурации

Команда	*Значение/ Значение по умолчанию*	*Действие*
set poe enable	-	Включить электропитание по линиям Ethernet
Set poe disable		Выключить электропитание по линиям Ethernet

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet

Вид запроса командной строки режима конфигурации интерфейса:

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

Таблица 121 – Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
power inline auto	-/auto	Разрешает работу протокола PoE-устройств на интерфейсе и включает подачу электропитания на интерфейс.
power inline never		Запрещает работу протокола обнаружения PoE-устройств на интерфейсе и отключает подачу электропитания.
power inline priority { critical | high | low }	-/low	Задает приоритет интерфейса PoE при управлении электропитанием. - **critical**– устанавливает наивысший приоритет электропитания. Электропитание портов с таким приоритетом будет прекращаться в последнюю очередь при перегрузке системы PoE; - **high** – устанавливает высокий приоритет электропитания; - **low** – устанавливает низкий приоритет электропитания.
power inline limit-mode {class | user-definded *wattage***}**	wattage: (200..31200) милливатт/ class	Выбрать режим ограничения мощности. - **class** – лимит максимальной потребляемой мощности определяется классом подключаемого устройства **- user-definded** – лимит максимальной потребляемой мощности выставляется вручную, с шагом 200 мВт.
no power inline limit-mode		Выбрать режим по умолчанию.

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console#
```

Таблица 122 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show power inline [gigabitethernet *gi_port***]**	gi_port: (0/1..8)	Отображает состояние электропитания интерфейсов, поддерживающих питание по линии PoE.
show power inline detail	-	Отображает общую информацию по состоянию PoE и состоянию источника.
show power inline consumption	-	Отображает характеристики потребления мощности, тока и напряжения.

4.19.3 Протокол UDLD

UDLD (Unidirectional Link Detection) – это протокол второго уровня созданный для автоматического обнаружения потери двухсторонней коммуникации на оптических линиях связи.

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet

Вид запроса командной строки режима конфигурации интерфейса:

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

Таблица 123 – Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
ethernet-oam uni-directional detection	-/выключено	Включить диагностику состояния оптический линий.
no ethernet-oam uni-directional detection		Выключить диагностику состояния оптический линий.

ethernet-oam uni-directional detection aggressive	-/выключено	Включить агрессивный режим, при котором TLV отправляется в любом случае, даже если она не была получена от удаленного устройства.
no ethernet-oam uni-directional detection aggressive		Выключить агрессивный режим, при котором TLV отправляется в любом случае, даже если она не была полуена от удаленного устройства.
ethernet-oam uni-directional detection discovery-time *time*	time: (5..300)/5	Выставить таймер, по которому будет происходить определение текущего состояния линка.
no ethernet-oam uni-directional detection discovery-time		Установить значение по умолчанию.
ethernet-oam uni-directional detection action {errdisable | log}	-/log	Выбрать режим работы протокола UDLD. Errdisable – передача трафика блокируется при отсутствии приема водном из направлений в канале Log – сообщение о блокировке появляется в журнале.
noethernet-oamuni-directional detection action		Установить значение по умолчанию

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 124 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show port ethernet-oam uni-directional detection	-	Отображает состояние оптического линка.

4.19.4 Диагностика оптического трансивера

Функция диагностики позволяет оценить текущее состояние оптического трансивера и оптической линии связи.

Возможен автоматический контроль состояния линий связи. Для этого коммутатор периодически опрашивает параметры оптических интерфейсов и сравнивает их с пороговыми значениями, заданными производителями трансиверов. При выходе параметров за допустимые пределы коммутатор формирует предупреждающие и аварийные сообщения.

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 125 – Команды диагностики оптического трансивера

Команда	*Значение/Значение по умолчанию*	*Действие*
show fiber-ports optical-transceiver [{gigabitethernet *gi_port* **| fastethernet fa_port}]**	-	Отображает результаты диагностики оптического трансивера.

Таблица 126 – Параметры диагностики оптического трансивера

Параметр	*Значение*
Temp	Температура трансивера.

Voltage	Напряжение питания трансивера.
Current	Отклонение тока на передаче.
Output Power	Выходная мощность на передаче (мВт).
Input Power	Входная мощность на приеме (мВт).
LOS	Потеря сигнала.

Значения результатов диагностики:

- N/A – недоступно,
- N/S – не поддерживается.

4.20 Функции обеспечения безопасности

4.20.1 Функции обеспечения защиты портов

С целью повышения безопасности в коммутаторе существует возможность настроить какой-либо порт так, чтобы доступ к коммутатору через этот порт предоставлялся только заданным устройствам. Функция защиты портов основана на определении MAC-адресов, которым разрешается доступ. MAC-адреса могут быть настроены вручную или изучены коммутатором. После изучения необходимых адресов порт следует заблокировать, защитив его от поступления пакетов с неизученными MAC-адресами. Таким образом, когда заблокированный порт получает пакет, и MAC-адрес источника пакета не связан с этим портом, активизируется механизм защиты, в зависимости от которого могут быть приняты следующие меры: несанкционированные пакеты, поступающие на заблокированный порт, пересылаются, отбрасываются, либо же порт, принявший пакет, отключается. Функция безопасности *Locked Port* позволяет сохранить список изученных MAC-адресов в файле конфигурации, таким образом, этот список можно восстановить после перезагрузки устройства.

Существует ограничение на количество MAC-адресов, которое может изучить порт, использующий функцию защиты.

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

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

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

Таблица 127 – Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

Команда	*Значение/Значение по умолчанию*	*Действие*
switchport port-security enable	-/выключено	Включает функцию защиты на интерфейсе. Блокирует функцию изучения новых адресов для интерфейса. Пакеты с неизученными MAC-адресами источника отбрасываются.
no switchport port-security enable		Отключает функцию защиты на интерфейсе.
switchport port-security mac-limit	limit: (0..8192)/1	Задает максимальное количество адресов, которое может изучить порт.
no switchport port-security mac-limit		Устанавливает значение по умолчанию.

switchport port-security mode { max-addresses | lock}	-/lock	Задает режим ограничения изучения MAC-адресов для настраиваемого интерфейса. - *max-addresses* – удаляет текущие динамически изученные адреса, связанные с интерфейсом. Разрешено изучение максимального количества адресов на порту. Повторное изучение и старение разрешены. - *lock* – сохраняет в файл текущие динамически изученные адреса, связанные с интерфейсом и запрещает обучение новым адресам и старение уже изученных адресов.
no switchport port-security mode		Устанавливает значение по умолчанию.
switchport port-security violation [restrict | protect]	-/protect	Задать режим реагирования при нарушении безопасности. *Restrict* – в данном режиме при нарушении безопасности отправляется SNMP-трап на SYSLOG-сервер. *Protect* – в данном режиме оповещения о нарушении безопасности нет. Включает перехват MAC-адресов, которые должны быть отброшены, на CPU, после чего MAC-адреса помечаются как заблокированные и отбрасываются в течении aging-time.
no switchport port-security violation		Установить значение по умолчанию.
switchport port-security unicast *mac_address* **vlan** *vlan_id*	mac_address: (aa:aa:aa:aa:aa:aa); vlan_id: (1..4094)	Создаёт статическую MAC-запись для порта. Данная команда не отображается в конфигурации. Просмотреть статическую MAC-запись можно через команду `show mac-address-table static unicast`.

4.20.2 Проверка подлинности клиента на основе порта (стандарт 802.1x)[1]

4.20.2.1 Базовая проверка подлинности

Аутентификация на основе стандарта 802.1x обеспечивает проверку подлинности пользователей коммутатора через внешний сервер на основе порта, к которому подключен клиент. Только аутентифицированные и авторизованные пользователи смогут передавать и принимать данные. Проверка подлинности пользователей портов выполняется сервером RADIUS посредством протокола EAP (Extensible Authentication Protocol).

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 128 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
dot1x system-auth-control	-/выключено	Включает режим аутентификации 802.1X на коммутаторе.
no dot1x system-auth-control		Выключает режим аутентификации 802.1X на коммутаторе.
aaa authentication dot1x default {group | local} radius	-/radius	Задает метод проверки подлинности, авторизации и учета (AAA), для использования на интерфейсах IEEE 802.1X. - *radius* – использовать список RADIUS-серверов для аутентификации пользователя.
no aaa authentication dot1x default		Устанавливает значение по умолчанию.

[1] Не поддерживается в версии ПО 10.1.8.2

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

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

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

Таблица 129 – Команды режима конфигурации 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 enable	-/	Разрешить аутентификацию 802.1X на интерфейсе
Dot1x disale		Запретить аутентификацию 802.1X на интерфейсе
dot1x reauthentication	-/периодические повторные проверки подлинности выключены	Включает периодические повторные проверки подлинности (переаутентификацию) клиента.
no dot1x reauthentication		Выключает периодические повторные проверки подлинности (переаутентификацию) клиента.
dot1x timeout reauth-period *period*	period: (1..65535)/ 3600 сек	Устанавливает период между повторными проверками подлинности.
no dot1x timeout reauth-period		Устанавливает значение по умолчанию.
dot1x timeout quiet-period *period*	period: (0..65535)/60 сек	Устанавливает период, в течение которого коммутатор остается в состоянии молчания после неудачной проверки подлинности. В течение периода молчания коммутатор не принимает и не инициирует никаких аутентификационных сообщений.
no dot1x timeout quiet-period		Устанавливает значение по умолчанию
dot1x timeout tx-period *period*	period: (1..65535)/30 сек	Устанавливает период, в течение которого коммутатор ожидает ответ на запрос либо идентификацию по протоколу EAP от клиента, перед повторной отправкой запроса.
no dot1x timeout tx-period		Устанавливает значение по умолчанию.
dot1x max-req *count*	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*	period: (1..65535)/30 секунд	Устанавливает период между повторными передачами запросов протокола EAP-клиенту.
no dot1x timeout supp-timeout		Устанавливает значение по умолчанию.
dot1x timeout server-timeout *period*	period: (1..65535)/30 секунд	Устанавливает период, в течение которого коммутатор ожидает ответа от сервера аутентификации.
no dot1x timeout server-timeout		Устанавливает значение по умолчанию.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 130 – Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
dot1x re-authenticate [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **|]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24)	Вручную осуществляет повторную проверку подлинности указанного порта в команде, либо всех портов, поддерживающих 802.1X.
show dot1x interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| }**	fa_port: (0/1..24); gi_port: (0/1..24)	Показывает состояние 802.1X для коммутатора либо для указанного интерфейса.
show dot1x users [username *username***]**	username: (1..160) символов	Показывает активных аутентифицированных пользователей 802.1X коммутатора.
show dot1x statistics interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| }**	fa_port: (0/1..24); gi_port: (0/1..24)	Показывает статистику по 802.1X для выбранного интерфейса.

Таблица 131 – 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.

Таблица 132 – 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.

4.20.2.2 Расширенная проверка подлинности.

Расширенные настройки dot1x позволяют проводить проверку подлинности для нескольких клиентов, подключенных к порту. Существует два варианта аутентификации: первый, когда проверка подлинности на основе порта требует аутентификации только одного клиента, чтобы доступ к системе имели все клиенты (режим Multiple hosts), второй, когда проверка подлинности требует аутентификации всех подключенных к порту клиентов (режим Multiple sessions). Если порт в режиме Multiple hosts не проходит аутентификацию, то всем подключенным хостам будет отказано в доступе к ресурсам сети.

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

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

Таблица 133 – Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
dot1x host-mode {multi-host | single-host }	-/multi-host	Разрешает наличие одного/нескольких клиентов на авторизованном порту 802.1X. - *multi-host* – несколько клиентов; - *single-host* – один клиент.
no dot1x single-host-violation	-/protect; freq: (1..1000000)/1 сек	Устанавливает значение по умолчанию.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 134 – Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show dot1x interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fastethernet** *fa_port}***}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24)	Настройки протокола 802.1x на интерфейсе (команда доступна только для привилегированного пользователя).
show dot1x statistics interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fastethernet** *fa_port* **}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24)	Показывает статистику 802.1X на интерфейсах.

4.20.3 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 135 – Формат полей опции 82

Поле	*Передаваемая информация*
Circuit ID	Имя хоста устройства. строка вида eth <stacked/slotid/interfaceid>:<vlan> Последний байт – номер порта, к которому подключено устройство, отправляющее dhcp-запрос.
Remote agent ID	Enterprise number – 0089c1 MAC-адрес устройства.

Для корректной работы функции DHCP Snooping все используемые DHCP-серверы должны быть подключены к «доверенным» портам коммутатора. Для добавления порта в список «доверенных» используются команды port-security-state trusted, set port-role uplink в режиме конфигурации интерфейса. Для обеспечения безопасности все остальные порты коммутатора должны быть «недоверенными».

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 136 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip {dhcp| dhcpv6} snooping	-/выключено	Разрешает коммутатору контролирование протокола DHCP.
no ip {dhcp| dhcpv6} snooping		Запрещает коммутатору контролирование протокола DHCP.
ip {dhcp| dhcpv6} snooping vlan *vlan_id*	vlan_id: (1..4094)/выключено	Разрешает контролирование протокола DHCP в пределах указанного VLAN.
no ip {dhcp| dhcpv6} snooping vlan *vlan_id*		Запрещает контролирование протокола DHCP в пределах указанного VLAN.
ip dhcp snooping verify mac-address	-/включено	Включает верификацию MAC-адреса клиента и MAC-адреса источника, принятого в DHCP-пакете на «недоверенных» портах.
no ip dhcp snooping verify mac-address		Выключает верификацию MAC-адреса клиента и MAC-адреса источника, принятого в DHCP-пакете на «недоверенных» портах.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 137 – Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip {dhcp | dhcpv6} snooping	-	Отображает соответствия из файла (базы) контроля протокола DHCP.
show ip dhcp snooping global	-	Отобразить глобальную настройку DHCP Snooping.
show {ip | ipv6} binding	-	Показать все соответствия из файла (базы) контроля протокола DHCP.
clear {ipv4 | ipv6} binding	-	Очистить соответствия из файла (базы) контроля протокола DHCP.

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

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

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

Таблица 138 – Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

Команда	*Значение/Значение по умолчанию*	*Действие*
ip binding limit *limit*	limit (1..1024)	Включает ограничение количества DHCP-клиентов на порту
no ip binding limit		Выключает ограничение количества DHCP-клиентов на порту

4.20.4 DSLAM Controller Solution (DCS)

С помощью данной функции настраиваются значения идентификаторов circuit_id и remote_id при конфигурации DHCP snooping, DHCPv6 snooping и PPPoE Intermediate Agent.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 139 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
dcs information option [dhcp | dhcpv6 | pppoe-ia] enable	-/выключено	Включить добавление circuit id + remote id для всех опций (т.е. dhcp | dhcpv6 | pppoe-ia), либо задать конкретный протокол для вставки remote-id и circuit-id.
dcs information option [dhcp | dhcpv6 | pppoe-ia] disable		Выключить добавление remote-id и circuit-id.

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

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

Таблица 140 – Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
dcs agent-circuit-identifer *circuit_id*	circuit_id: (1..63) символов/передается hostname, port, vlan	Установка идентификатора интерфейса, с которого пришел запрос
no dcs agent-circuit-identifer		Установка значения по умолчанию.
dcs remote-agent-identifier enable	-/выключено	Активировать идентификатор remote_id.
dcs remote-agent-identifier disable		Отключить идентификатор remote_id для опции 82.
dcs remote-agent-identifier *remote_id*	remote_id: (1..63) символов/передается mac-адрес коммутатора	Установка идентификатора ретранслятора, на который пришел запрос
no dcs remote-agent-identifier		Установка значения по умолчанию.

dcs [agent-circuit-identifier | remote-agent-identifer] *identifer*	-	Настроить пользовательский шаблон circuit_id и remote_id. Для настройки используются следующие шаблоны: %a: IP-адрес %h: hostname; %p: короткое имя порта, например gi1/0/1; %P: длинное имя порта, например, gigabitethernet 1/0/1; %t: тип порта (значение поля ifTable::ifType в шестнадцатеричном виде); %m: MAC-адрес порта в формате H-H-H-H-H-H; %M: MAC-адрес системы в формате H-H-H-H-H-H; %u: номер юнита; %s: номер слота; %i: ifIndex порта; %c: MAC-адрес абонентского устройства; %v: идентификатор VLAN.

Таблица 141 – Формат полей опции 82 согласно рекомендациям TR-101

Поле	***Передаваемая информация***
Circuit ID	Имя хоста устройства. строка вида eth <stacked/slotid/interfaceid>: <vlan> Последний байт – номер порта, к которому подключено устройство, отправляющее запрос DHCP.
Remote agent ID	Enterprise number – 0089c1 MAC-адрес устройства.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 142 – Команды режима Privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show dcs-port-config [interface fastethernet *fa_port* **| gigabitethernet** *gi_port***]**	fa_port: (0/1..24); gi_port: (0/1..24)	Отображает текущую конфигурацию идентификаторов Remote ID и Circuit ID опции 82.
show dcs-global-config	-	Отображает дефолтную конфигурацию параметров идентификатора Circuit ID опции 82.

Пример настройки DHCP Snooping во VLAN10 с настройкой DCS-опций.

```
console(config)# !
console(config)# interface gigabitethernet 0/10
console(config-if)# port-security-state trusted
console(config-if)# set port-role uplink
console(config-if)# no shutdown
console(config-if)# !
console(config)# ip dhcp snooping
console(config)# !
console(config)# vlan 10
console(config-vlan)# ip dhcp snooping
console(config-vlan)# !
console(config)# interface gigabitethernet 0/12
console(config-if)# switchport general allowed vlan add 10 untagged
console(config-if)# switchport general pvid 10
console(config-if)# !
console(config)# !
console(config)# interface gigabitethernet 0/13
console(config-if)# dcs remote-agent-identifier enable
console(config-if)# dcs agent-circuit-identifier "%v %p %h"
```

```
console(config-if)# dcs remote-agent-identifier "%M"
console(config-if)# !
```

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

Функция защиты IP-адреса (IPSource 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 конфигурации интерфейса Ethernet

Вид запроса командной строки:

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

Таблица 143 – Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значениепоумолчанию*	*Действие*
{ip | ipv6} verify source port-security	-	Включает функцию защиты IP-интерфейса для порта. После включения на интерфесе все записи в таблице IP Binding устанавливаются в TCAM в качестве разрешающего правила.
no {ip | ipv6} verify source port-security		Команда удаляет записи из TCAM и отключает отбрасывание IP-пакетов на порту.

4.20.6 Контроль протокола ARP (ARP Inspection)

Функция контроля протокола ARP (ARP Inspection) предназначена для защиты от атак с использованием протокола ARP (например, ARP-spoofing – перехват ARP-трафика). Контроль протокола ARP осуществляется на основе статических соответствий IP- и MAC-адресов, заданных для группы VLAN.

Порт, сконфигурированный «недоверенным» для функции ARP Inspection, должен также быть «недоверенным» для функции DHCP snooping или соответствие MAC-адреса и IP-адреса для этого порта должно быть сконфигурировано статически. Иначе данный порт не будет отвечать на запросы ARP.

Для ненадежных портов выполняются проверки соответствий IP- и MAC-адресов.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 144 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip arp inspection enable	-/выключено	Включить контроль протокола ARP (функцию ARP Inspection)
ip arp inspection disable		Выключить контроль протокола ARP (функцию ARP Inspection)
ip arp inspection vlan *vlan_id*	vlan_id: (1..4094)/ выключено	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 {dstmac | dstmac-ipaddr | ipaddr |srcmac | srcmac-dstmac | srcmac-dstmac-ipaddr | srcmac-ipaddr}	-	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.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 145 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip arp inspection globals	-	Отображает системную конфигурацию функции контроля ARP протокола.
show ip arp inspection vlan [*vlan_id***]**	vlan_id: (1..4094)	Отображает список VLAN, на которых активен ARP Inspection.
show ip arp inspection statistics [vlan *vlan_id***]**	vlan_id: (1..4094)	Показывает статистику для следующих типов пакетов, которые были обработаны при помощи функции ARP: - переданные пакеты (forwarded); - потерянные пакеты (dropped); - ошибки в IP/MAC (IP/MAC Failures).
clear ip arp inspection statistics [vlan *vlan_id***]**	vlan_id: (1..4094)	Очищает статистику контроля протокола ARP Inspection.

4.20.7 Настройка функции MAC Address Notification

Функция MAC Address Notification позволяет отслеживать появление и исчезновение активного оборудования на сети путем сохранения истории изучения MAC-адресов. При обнаружении изменений в составе изученных MAC-адресов коммутатор сохраняет информацию в таблице и извещает об этом с помощью сообщений протокола SNMP. Функция имеет настраиваемые параметры – глубина истории о событиях и минимальный интервал отправки сообщений. Сервис MAC Address Notification отключен по умолчанию и может быть настроен выборочно для отдельных портов коммутатора.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 146 – Команды режима глобальной конфигурации

Команда	*Значение/ Значение по умолчанию*	*Действие*
mac-address-table notification change	-/выключена	Команда предназначена для глобального управления функцией MAC notification. Команда разрешает регистрацию событий добавления и удаления MAC-адресов из таблиц коммутатора и отправку уведомления о событиях. Для работы функции необходимо дополнительно разрешать генерацию уведомлений на интерфейсах (см. ниже).
no mac-address-table notification change		Выключает функцию MAC notification глобально и отменяет соответствующие настройки на всех интерфейсах.
mac-address-table notification change interval *value*	value: (0..4294967295)/1	Максимальный промежуток времени между отправками SNMP-уведомлений. Если значение интервала времени равно 0, то генерация уведомлений и сохранение событий в историю будет осуществляться немедленно по мере возникновения событий об изменении состояния таблицы MAC-адресов. Если значение интервала времени больше 0, то устройство будет накапливать события об изменении состояния таблицы MAC-адресов в течение этого времени, а затем отправлять уведомления протокола SNMP и сохранять события в истории.
no mac-address-table notification change interval		Восстанавливает значение по умолчанию.
mac-address-table notification change history *value*	value: (0..500)/1	Команда задает максимальное количество событий об изменении состояния таблицы MAC-адресов, которое сохраняется в истории. Если установлен размер истории равный 0, то события не сохраняются. При переполнении буфера истории новое событие помещается на место самого старого.
no mac-address-table notification change history		Восстанавливает значение по умолчанию.
logging events mac-address-table change	-/выключено	Включить отправку трапов в syslog о событиях изучения или удаления MAC-адресов.

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки:

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

Таблица 147 – Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
snmp trap mac-address-notification change [learnt | removed]	-/выключена	Включение генерации уведомлений на каждом интерфейсе о событиях изменения состояния MAC-адресов. Отдельно можно разрешить генерацию уведомлений только об изучении MAC-адресов, либо только об их удалении.
no snmp trap mac-notification change [learnt | removed]		Отключение генерации уведомлений на интерфейсе.
snmp-server enable traps errdisable { storm-control|loopback-detection| udld}	-/включена	Включение генерации уведомлений при блокировке порта по событиям: - **loopback-detection** – обнаружение петель; - **udld** – активация защиты UDLD; - **storm-control –** широковещательный шторм
no snmp-server enable traps errdisable { storm-control|loopback-detection|udld}		Отключение генерации уведомления на интерфейсе.

Команды режима privileged EXEC

Вид запроса командной строки в режиме privileged EXEC:

```
console#
```

Таблица 148 – Команды режима privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show mac-address-table notification change history	-	Отображение всех уведомлений об изменении состояния MAC-адресов, сохраненных в истории.
show snmp-server traps	-	Посмотреть события, при которых генерируются трапы.

4.21 Функции DHCP Relay посредника

Коммутаторы поддерживают функции DHCP Relay агента. Задачей DHCP Relay агента является передача DHCP-пакетов от клиента к серверу и обратно в случае, если DHCP-сервер находится в одной сети, а клиент в другой. Другой функцией является добавление дополнительных опций в DHCP-запросы клиента (например, опции 82).

Принцип работы DHCP Relay агента на коммутаторе: коммутатор принимает от клиента DHCP-запросы, передает эти запросы серверу от имени клиента (оставляя в запросе опции с требуемыми клиентом параметрами и, в зависимости от конфигурации, добавляя свои опции). Получив ответ от сервера, коммутатор передает его клиенту. Совместная работа dhcp relay и dhcp snooping в текущей версии невозможна.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 149 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
service dhcp-relay	-/выключено	Включение функций DHCP Relay агента на коммутаторе.
no service dhcp-relay		Выключение функций DHCP Relay агента на коммутаторе.
ip dhcp server *ip_add*	Может быть задано до пяти серверов	Задает IP-адрес доступного DHCP-сервера для DHCP Relay агента.
no ip dhcp server *ip_add*		Удаляет IP-адрес из списка DHCP-серверов для DHCP Relay агента.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 150 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip dhcp relay information {FastEthernet fa_port | Gigabitethernet gi_port | vlan | *vlan***}**	fa_port: (0/1..24); gi_port: (0/1..24); vlan: (1..4094)	Отображает конфигурацию настроенной функции DHCP Relay агента для коммутатора и отдельно для интерфейсов, а также список доступных серверов.
show dhcp server	-	Отображает список доступных серверов.

4.22 Конфигурация PPPoE Intermediate Agent

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

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

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 151 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
pppoe-ia snooping	-/выключено	Глобально включить контроль функции PPPoEIA.
no pppoe-ia snooping		Выключить контроль функции PPPoEIA.
pppoe-ia snooping session timeout *range*	range: (0..600)/300	Задать таймаут для работы функции PPPoE IA.
pppoe-ia snooping session timeout 0		Отключить таймаут для работы функции PPPoE IA
pppoe passthrough	-/отключено	Включение команды заставляет PPPoE-пакеты проходить через коммутатор как неизвестный L2-трафик, и делает их "невидимыми" для IP ACL.
no pppoe passthrough		Включает парсинг инкапсулированных в PPPoE-пакетах L3-заголовков, правила IP ACL начинают работать для инкапсулированных пакетов.

Для корректной работы функции PPPoE Intermediate Agent все используемые PPPoE-сервера должны быть подключены к «доверенным» портам коммутатора. Для добавления порта в список «доверенных» используются команды port-security-state trusted, set port-role uplink в режиме конфигурации интерфейса. Для обеспечения безопасности все остальные порты коммутатора должны быть «недоверенными»

4.23 Конфигурация ACL (списки контроля доступа)

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

На данный момент реализация ACL такова: каждый ACL содержит только 1 правило. Несколько ACL можно привязать к одному интерфейсу. Порядок отработки правил определяется по приоритету правила , указанному в ACL, при равенстве приоритетов - по номеру ACL.

ACL автоматически снимается с интерфейса при изменении в нем правила.

Максимальное число ACL – 100 IP/IPv6 и 100 MAC.

Команды для создания и редактирования списков ACL доступны в режиме глобальной конфигурации.

Команды режима глобальной конфигурации

Командная строка в режиме глобальной конфигурации имеет вид:

```
console (config)#
```

Таблица 152 – Команды для создания и конфигурации списков ACL

Команда	*Значение/Значение по умолчанию*	*Действие*
ip access-list standart *access_list_num*	access_list_num: (1..1000)	Создание стандартного списка ACL.
no ip access-list standart *access_list_num*		Удалить стандартный список ACL.
ip access-list extended *access_list*	access_list_num: (1001..65535)	Создание нового расширенного списка ACL для адресации IPv4 и вход в режим его конфигурации (если список с данным именем еще не создан), либо вход в режим конфигурации ранее созданного списка.
no ip access-list extended *access_list*		Удаление расширенного списка ACL для адресации IPv4.
ipv6 access-list extended *access_list_num*		Создание нового расширенного списка ACL для адресации IPv6 и вход в режим его конфигурации (если список с данным именем еще не создан), либо вход в режим конфигурации ранее созданного списка.
no ipv6 access-list extended *access_list*		Удаление расширенного списка ACL для адресации IPv6.
mac access-list extended *access_list*_num	mac_ access_list_num: (1..65535)	Создание нового списка ACL на базе MAC-адресации и вход в режим его конфигурации (если список с данным именем еще не создан), либо вход в режим конфигурации ранее созданного списка.
no mac access-list extended *mac_access_list*_num		Удаление списка ACL на базе MAC-адресации.
user-defined offset *offset_id* **{ l2 | ethtype | l3 | l4 }** *value*	offset_id: (1..4); value: (0..255)	Настройка смещения в байтах относительно выбранной стартовой позиции. Значение и маска, используемые для фильтрации, задаются через параметры ACL-правил. - *l2* – начало пакета (Destination MAC address). - *ethtype* – Ethertype (самый внутренний, при наличии VLAN-тегов) - *l3* – L3-заголовок - *l4* – L4-заголовок
no user-defined offset *offset_id*		Удаление смещения относительно выбранной стартовой позиции.

Для того чтобы активизировать список ACL, необходимо связать его с интерфейсом. Интерфейсом, использующим список, может быть либо интерфейс Ethernet, либо группа портов. На данный момент поддерживается только входящее направление на интерфейсах (in).

Команды режима конфигурации интерфейса Ethernet, VLAN

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

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

Таблица 153 – Команда назначения списка ACL-интерфейсу.

Команда	*Значение/Значение по умолчанию*	*Действие*
Ip access-group *access_list_num* **in**	access_list_num: (1..65535)	В настройках определённого физического интерфейса команда привязывает указанный список к данному интерфейсу.
no ip access-group *access_list_num in*		Удаление списка с интерфейса.
mac access-group *access_list_num* **in**	access_list_num: (1..65535)	В настройках определённого физического интерфейса команда привязывает указанный mac-список к данному интерфейсу.
no mac access-group access_list_num in		Удаление списка с интерфейса.

Команды режима Privileged EXEC

Командная строка в режиме Privileged EXEC имеет вид:

```
console#
```

Таблица 154 – Команды для просмотра списков ACL

Команда	*Значение/Значение по умолчанию*	*Действие*
show access-lists [*access_list_num***]**	access_list_num: (1-65535) символа	Показывает списки ACL, созданные на коммутаторе.

4.23.1 Конфигурация ACL на базе IPv4

В данном разделе приведены значения и описания основных параметров, используемых в составе команд настройки списков ACL, основанных на адресации IPv4. Создание и вход в режим редактирования списков ACL, основанных на адресации IPv4, осуществляется по команде: **`ip access-list {extended | standart}`** *`access-list_num`*.

Таблица 155 – 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, ip, tcp,udp, ipv6, ipv6:icmp, ospf, pim,либо числовое значение протокола, в диапазоне (0 – 255). Для соответствия любому протоколу используется значение IP.
source	Адрес источника	Определяет IP-адрес источника пакета.
source_mask	Маска адреса источника	Маска, применяемая к IP-адресу источника пакета. Маска определяет биты IP-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Например, используя маску, можно определить для правила фильтрации IP-сеть. Чтобы добавить в правило фильтрации IP-сеть 195.165.0.0, необходимо задать значение маски /16, то есть согласно данной маске последние 16 бит IP-адреса будут игнорироваться.
destination	Адрес назначения	Определяет IP-адрес назначения пакета.
destination_mask	Маска адреса назначения	Битовая маска, применяемая к IP-адресу назначения пакета. Маска определяет биты IP-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Маска используется аналогично маске *source_mask.*
vlan	Идентификатор Vlan	Определяет Vlan, для которого будет применяться правило.

dscp	Поле DSCP в заголовке L3	Определяет значение DSCP-поля diffserv. Возможные коды сообщений поля **dscp:** (0 – 63).
	Приоритет IP	Определяет приоритет IP-трафика: (0-7).
icmp_type	-	Тип сообщений протокола ICMP, используемый для фильтрации ICMP-пакетов. 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).
destination_port	UDP/TCP-порт назначения	Возможные значения поля TCP/UDP-порта: eq, gt, host,lt,range
source_port	UDP/TCP-порт источника	
priority	Приоритет записи	Индекс задает положение правила в списке и его приоритет. Чем меньше индекс – тем приоритетнее правило. Диапазон допустимых значений (1..255).
parametr	Опциональный параметр	Опциональный параметр при конфигурировании списка доступа: cvlan-id, cvlan-priority, dscp , priority, single-tag, tos, user-definded, traffic-class

В стандартных ip ACL возможна фильтрация только по префиксам, в расширенных ACL – по дополнительным параметрам.

После того, как любой ACL будет привязан к интерфейсу, для этого интерфейса применится правило implicit deny any any.

Таблица 156 – Команды, используемые для настройки ACL-списков на основе IP-адресации

Команда	***Действие***
permit *protocol* **{any |** *source* **host } {any |** *destination* **} [parametr]**	Добавляет разрешающую запись фильтрации для протокола. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit ip {any | *source* **host } {any |** *destination* **} [parametr]**	Добавляет разрешающую запись фильтрации для протокола IP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit icmp {any | *source* **host } {any |** *destination* **} [parametr]**	Добавляет разрешающую запись фильтрации для протокола ICMP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit tcp {any | *source* **host } {any |** *destination* **} [parametr]**	Добавляет разрешающую запись фильтрации для протокола TCP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit udp {any | *source* **host } {any |** *destination* **} [parametr]**	Добавляет разрешающую запись фильтрации для протокола UDP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
deny *protocol* **{any |** *source* **host } {any |** *destination* **} [parametr]**	Добавляет запрещающую запись фильтрации для протокола. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором.
deny ip {any | *source* **host } {any |** *destination* **} [parametr]**	Добавляет запрещающую запись фильтрации для протокола IP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором.
deny icmp {any | *source* **host } {any |** *destination* **} [parametr]**	Добавляет запрещающую запись фильтрации для протокола ICMP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором.
deny tcp {any | *source* **host } {any |** *destination* **} [parametr]**	Добавляет запрещающую запись фильтрации для протокола TCP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором.
deny udp {any | *source* **host } {any |** *destination* **} [parametr]**	Добавляет запрещающую запись фильтрации для протокола UDP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором.

4.23.2 Конфигурация ACL на базе IPv6

В данном разделе приведены значения и описания основных параметров, используемых в составе команд настройки списков ACL, основанных на адресации IPv6.

Создание и вход в режим редактирования списков ACL, основанных на адресации IPv6, осуществляется по команде: **ipv6 access-listextended***apv6_access-list*. Например, для создания списка ACL под названием MES IPv6 необходимо выполнить следующие команды:

```
console#
console# configure terminal
console(config)#ipv6 access-list extendedipv6 _access_list_num
console(config-ipv6-acl)#
```

Таблица 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, tcp,udp, ipv6.
source	Адрес источника	Определяет IP-адрес источника пакета.
destination	Адрес назначения	Определяет IP-адрес назначения пакета.
vlan	Идентификатор Vlan	Определяет Vlan, для которого будет применяться правило.
dscp	Поле DSCP в заголовке L3	Определяет значение DSCP-поля diffserv. Возможные коды сообщений поля **dscp:** (0 – 63).
icmp_type	-	Тип сообщений протокола ICMP, используемый для фильтрации ICMP-пакетов. Числовоезначениетипасообщения, вдиапазоне (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).
destination_port	UDP/TCP-порт назначения	Возможные значения поля TCP/UDP-порта: eq, gt, host,lt,range
source_port	UDP/TCP-порт источника	
priority	Приоритет записи	Индекс задает положение правила в списке и его приоритет. Чем меньше индекс – тем приоритетнее правило. Диапазон допустимых значений(1..255).
parametr	Опциональный параметр	Опциональный параметр при конфигурировании списка доступа: eq, gt, lt, range, dscp, traffic-class

После того, как любой ACL будет привязан к интерфейсу, для этого интерфейса применится правило implicit deny any any.

Таблица 158 – Команды, используемые для настройки ACL-списков на основе IP-адресации

Команда	*Действие*
permit *protocol***{any|***source* **host}{any|***destination***}[parametr]**	Добавляет разрешающую запись фильтрации для протокола. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit ipv6{any|*source* **host}{any|***destination***}[parametr]**	Добавляет разрешающую запись фильтрации для протокола IPv6. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit icmp{any|*source* **host}{any|***destination***}[parametr]**	Добавляет разрешающую запись фильтрации для протокола ICMP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.

permit tcp{any|*source* **host}{any|***destination***}[parametr]**	Добавляет разрешающую запись фильтрации для протокола TCP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit udp{any|*source* **host}{any|***destination***}[parametr]**	Добавляет разрешающую запись фильтрации для протокола UDP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
deny *protocol***{any|***source* **host}{any|***destination***}[parametr]**	Добавляет запрещающую запись фильтрации для протокола. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором.
deny ipv6{any|*source* **host}{any|***destination***}[parametr]**	Добавляет запрещающую запись фильтрации для протокола IPv6. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором.
deny icpm{any|*source* **host}{any|***destination***}[parametr]**	Добавляет запрещающую запись фильтрации для протокола ICMP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором.
deny tcp{any|*source* **host}{any|***destination***}[parametr]**	Добавляет запрещающую запись фильтрации для протокола TCP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором.
deny udp{any|*source* **host}{any|***destination***}[parametr]**	Добавляет запрещающую запись фильтрации для протокола UDP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором.

4.23.3 Конфигурация ACL на базе MAC

В данном разделе приведены значения и описания основных параметров, используемых в составе команд настройки списков ACL, основанных на MAC-адресации.

Создание и вход в режим редактирования списков ACL, основанных на MAC-адресации, осуществляется по команде: **mac access-list extended** *access-list_num*.

Таблица 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.
source	Адрес отправителя	Определяет MAC-адрес источника пакета.
source_mask	Битовая маска, применяемая к MAC-адресу источника пакета	Маска определяет биты MAC-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Например, используя маску, можно определить для правила фильтрации диапазона MAC-адресов. Чтобы добавить в правило фильтрации все MAC-адреса, начинающиеся на 00:00:02:AA.xx.xx, необходимо задать значение маски FF:FF:FF:FF:00:00, то есть, согласно данной маске, последние 16 бит MAC-адреса будут не важны для анализа
destination	Адрес назначения	Определяет MAC-адрес назначения пакета.
destination_ mask	Битовая маска, применяемая к MAC-адресу назначения пакета	Маска определяет биты MAC-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Маска используется аналогично маске source_ mask.
vlan_id	vlan_id: (0..4095)	Подсеть VLAN фильтруемых пакетов.
cvlan-priority	cvlan_priority: (0..7)	Класс обслуживания фильтруемых пакетов.
ethertype	eth_type: (0..0xFFFF)	Ethernet тип фильтруемых пакетов в шестнадцатеричной записи.
Encaptype value	Value: (1..65535)	Тип ethertype для фильтруемых пакетов.
etype_list	*etype_list: (1..65535)*	Список стандартных ethertype
priority	Индекс правила	Индекс правила в таблице, чем меньше индекс – тем приоритетнее правило 1-255

Таблица 160 – Команды, используемые для настройки ACL-списков на основе MAC-адресации

Команда	*Действие*
permit {any | host *source source_ mask* **} {any | host** *destination destination_ mask***} [encaptype** *value* **|** *etype_list* **] [priority** *priority***]**	Добавляет разрешающую запись фильтрации. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
deny {any | host *source source_ mask* **} {any | host** *destination destination_ mask***} [encaptype** *value* **|** *etype_list* **] [priority** *priority***]**	Добавляет запрещающую запись фильтрации. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором.

Пример настройки фильтрации padi/pado через User-defined offset:

```
console(config)# user-defined offset 1 ethtype 0
console(config)# !
console(config)# mac access-list extended 1
console(config-ext-macl)# permit 00:00:00:00:00:01 ff:ff:ff:ff:ff:00 any
user-defined offset1 0x8863 0xffff
console(config-ext-macl)# !
console(config)# interface gi 0/1
console(config-if)# mac access-group1 in
```

Пример фильтрации по src/dst IP, src/dst port, tos через User-defined offset:

```
console(config)#
console(config)# user-defined offset 1 ethtype 0
console(config)# !
console(config)# ip  access-list extended 1010
console(config-ext-nacl)# permit udp 1.1.0.0 255.255.0.0 gt 5000 2.2.2.0
255.255.255.0 lt 7000 traffic-class 0xe0 sub-action modify-vlan 2 user-
defined offset1 0x8864 0xffff
console(config-ext-nacl)# !
console(config)# interface gi 0/1
console(config-if)#ip access-group 1010 in
```

4.24 Конфигурация защиты от DOS-атак

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 161 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
firewall	-/включено	Перейти в режим конфигурирования модуля, отвечающего за функционал защиты от DoS-атак.

Вид запроса командной строки:

```
console(config-firewall)#
```

Таблица 162 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
enable	-/enable	Включение поддержки защиты от DOS-атак.

disable		Выключение поддержки защиты от DOS-атак.
ip inspect tcp enable	-/включено	Включение обнаружения synfin-пакетов
no inspect tcp		Выключение обнаружения synfin-пакетов
ip inspect tcp syn wait *sec*	sec: (1..65535)/1	Выставить таймер блокировки synfin-пакетов

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 163 – Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
sh run firewall	-	Отображает настройку модуля firewall
sh firewall stats	-	Отображает статистику по пакетам, обработанными модулем firewall
sh firewall logs	-	Отображает логи модуля firewall

4.25 Качество обслуживания – QoS

По умолчанию на всех портах коммутатора используется организация очереди пакетов по методу FIFO: первый пришел – первый ушёл (First In – First Out). Во время интенсивной передачи трафика при использовании данного метода могут возникнуть проблемы, поскольку устройством игнорируются все пакеты, не вошедшие в буфер очереди FIFO, и соответственно теряются безвозвратно. Решает данную проблему метод, организующий очереди по приоритету трафика. Механизм QoS (Quality of service – качество обслуживания), реализованный в коммутаторах, позволяет организовать восемь очередей приоритета пакетов в зависимости от типа передаваемых данных.

4.25.1 Настройка QoS

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 164 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
class-map *class_map_*num	class_map_num: (1..65535)	1. Создает список критериев классификации трафика. 2. Входит в режим редактирования списка критериев классификации трафика.
no class-map *class_map_num*		Удаляет список критериев классификации трафика.
policy-map *policy_map_num*	policy_map_num: (1..65535)	1. Создает стратегию классификации трафика. 2. Входит в режим редактирования стратегии классификации трафика.
no policy-map *policy_map_num*		Удаляет правило классификации трафика.

scheduler ***sched_num*** **interface {fastethernet fa_port | gigabitethernet *gi_port* | port-channel** *group***} sched-algo {strict-priority | strict-wrr | wrr}**	fa_port: (0/1..24); gi_port: (0/1..24); group: (1..8); sched_num: (1..65535)	Определить алгоритм работы планировщика на интерфейсе. **- strict-priority** – строгая очередь, имеет наивысший приоритет **- strict-wrr** – очередь по механизму wrr, имеющая приоритет выше очереди wrr **- wrr** – очередь, обрабатывающаяся по механизму wrr **- fa/gi_port** – исходящий интерфейс.
no scheduler *sched_num* **interface {fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| port-channel** *group***}**		Удаляет настройки планировщика.
queue *queue_num* **interface {fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| port-channel** *group***} weight** *weight*	fa_port: (0/1..24); gi_port: (0/1..24); group: (1..8); queue_num: (1..8); weight: (1..127)	Задать номер и вес очереди для исходящего интерфейса.
queue-map regn-priority {ipDscp *dscp_map* **| vlanPri** *cos_map***} queue-id** *queue_id*	dscp_map: (0..63); cas_map: (0..7); queue_id: (1..8)	Определить трафик с меткой CoS/DSCP в очередь
queue-map regn-priority {ipDscp *dscp_map* **| vlanPri** *cos_map***}**		Отменить определение трафика в очередь
qos interface {fastethernet *fa_port* **| gigabitethernet** *gi_port* **| port-channel** *group***} def-user-priority** *priority*	fa_port: (0/1..24); gi_port: (0/1..24); Priority: (0..7)/0	Указать очередь для интерфейса, при условии отсутствия меток CoS/DSCP у входящих пакетов
class-map *class_num*	class_num: (1..65535)	Создать и перейти в режим конфигурирования class-map
no class-map *class_num*		Удалить класс
policy-map *policy_num*	policy_num: (1..65535)	Создать и перейти в режим конфигурирования policy-map
no policy-map *class_num*		Удалить политику
logging service cpu rate-limit [queue]	-/выключено	Включить отправку трапов о превышении порога cpu-rate-limit в syslog
no logging service cpu rate-limit [queue]		Установит значение по умолчанию
snmp-server enable traps cpu rate-limit [queue]	-/выключена	Включение генерации уведомлений при превышении значения cpu-rate-limit
no snmp-server enable traps cpu rate-limit [queue]		Отключение генерации уведомления на устройстве.

Команды режима конфигурации VLAN

Вид запроса командной строки в режиме конфигурации VLAN:

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

Таблица 165 – Команды режима конфигурации VLAN

Команда	***Значение/Значение по умолчанию***	***Описание***
qos cos egress*cos_default*	cos_default: (0..7)/0	Устанавливает значение CoS для порта (CoS, применяемый для всего нетегированного трафика, проходящего через интерфейс).
no qos cos egress		Установит значение по умолчанию

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки:

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

Таблица 166 – Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
qos trust {cos | dscp | cos-dscp | none}	-/none	Устанавливает режим доверия коммутатора в базовом режиме QoS (CoS или DSCP). - **cos** – устанавливает классификацию входящих пакетов по значениям CoS. Для нетегированных пакетов используется значение CoS по умолчанию. - **dscp**– устанавливает классификацию входящих пакетов по значениям DSCP. - **cos-dscp** – устанавливает классификацию входящих пакетов по значениям DSCP для IP-пакетов и по значениям CoS для не IP-пакетов.
no qos trust		Устанавливает значения по умолчанию.

Команды режима редактирования списка критериев классификации трафика

Вид запроса командной строки режима редактирования списка критериев классификации трафика:

```
console# configure terminal
console(config)# class-map class-map-name
console(config-cls-map)#
```

Таблица 167 – Команды режима редактирования списка критериев классификации трафика

Команда	*Значение/Значение по умолчанию*	*Действие*
match access-group {ip-access-list | mac-access-list } *acl_num*	acl_num: (0..65535)	Добавляет критерий классификации трафика. Определяет правила фильтрации трафика по списку ACL для классификации.
set class *class_num*	class_num: (1..65535)	Активировать класс
no set class *class_num*		Отключить работу класса
set class *class_num* **regen-priority** *priority* **group-name** *name*	priority: (0..7); name: (1..31) символов	Задать внутренний приоритет для указанного класса

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-ply-map)#
```

Таблица 168 – Команды режима редактирования стратегии классификации трафика

Команда	*Значение/Значение по умолчанию*	*Действие*
set policy class *class_num* **default-priority-type {vlanPri** *new_cos_map* **| ipDscp** *new_dscp_map***}**	class_num : (0..65535); new_cos_map: (0..7); new_dscp_map: (0..63)	Устанавливает новое значение метки для пакета.
set policy class *class_num* **interace {fastethernet** *fa_port* **| gigabitethernet** *gi_port* **| port-channel** *group***} default-priority-type {vlanPri** *new_cos_map* **| ipDscp** *new_dscp_map***}**	class_num: (0..65535); new_cos_map: (0..7); new_dscp_map: (0..63)	Устанавливает новое значение метки для пакета на интерфейсе.

set meter {*meter***} violate-action drop**	-	Если скорость потока превышает указанную в соответсвующем meter, то пакеты, которые превысили ограничение, отбрасываются.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 169 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
meter *meter*	meter: (1..255)	Создать измеритель ограничения скорости для исходящего трафика.
no meter *meter*		Удалить измеритель ограничения скорости для исходящего трафика.

Команды режима конфигурации измерителя ограничения скорости для входящего трафика:

Вид запроса командной строки в режиме конфигурации:

```
console(config-meter)#
```

Таблица 170 – Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

Команда	*Значение/Значение по умолчанию*	*Действие*
meter-type avgRate cir {*cir_value***} {kbps | pps}**	-	Устанавливает ограничение скорости для исходящего трафика.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 171 – Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
show qos global info	-	Отображает глобальные настройки qos
show qos def-user-priority [fastethernet *fa_port* **| gigabitethernet** *gi_port* **| port-channel** *group***]**	-	Показывает в какую очередь определены интерфейсы
show queue-map	-	Отображает маппинг CoS и DSCP по умолчанию
show qos trust	-	Просмотр текущей настройки доверия меткам cosи dscp.

Пример применения сервисной политики:

Для трафика, имеющего DSCP 8, меняется VLAN на 100, p-bit меняется на 7, dscp меняется на 63, скорость потока ограничивается до 512 kbps.

```
console(config)# ip  access-list extended 1008
console(config-ext-nacl)# permit ip any any traffic-class 8 sub-action
modify-vlan 100
```

```
console(config-ext-nacl)# !
console(config)# interface gi 0/6
console(config-if)#  no shutdown
console(config-if)#  qos trust cos
console(config-if)#  switchport mode trunk
console(config-if)#  ip access-group 1008 in
console(config-if)# !
console(config)# interface gi 0/7
console(config-if)#  no shutdown
console(config-if)#  switchport mode trunk
console(config-if)#  qos map regen-priority-type vlanPri enable
console(config-if)# !
console(config)# class-map 1008
console(config-cls-map)#  match access-group ip-access-list 1008
console(config-cls-map)#  set class 1008 regen-priority 7 group-name QOS
console(config-cls-map)# !
console(config)# meter 10
console(config-meter)#  meter-type avgRate cir 512 kbps
console(config-meter)# !
console(config)# policy-map 1008
console(config-ply-map)#    set  policy  class  1008  default-priority-type
ipDscp 63
console(config-ply-map)# !
```

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

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

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

Таблица 172 – Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

Команда	*Значение/Значение по умолчанию*	*Действие*
rate-limit input *rate*	rate: (16..4194288) kbps	Устанавливает ограничение скорости для входящего трафика.
no rate-limit input		Установить значение по умолчанию
rate-limit output *rate*	rate: (16..4194288) kbps	Устанавливает ограничение скорости для исходящего трафика. **Значение rate должно быть кратно 16.**
no rate-limit output		Установить значение по умолчанию

Пример настройки ограничении скорости портаGigabitEthernet 0/4:

```
console# c t
console(config)# vlan 10
console(config-vlan)# vlan active
console(config-vlan)# !
console(config)# interface gigabitethernet 0/4
console(config-if)# no shutdown
console(config-if)# switchport acceptable-frame-type untaggedAndPriorityTagged
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 10
console(config-if)# rate-limit input 512
console(config-if)# rate-limit output 512
console(config-if)# !
console(config)# interface gigabitethernet 0/5
```

```
console(config-if)# no shutdown
console(config-if)# switchport mode trunk
console(config-if)# !
```

Пример настройки QoS:

Настроить планировщик по алгоритму wrr для исходящего интерфейса fa0/1. Распределить трафик согласно полю CoS в очереди 1-4. Назначить вес wrr для очередей согласно номеру очереди. Очередь 5 объявить приоритетной.

```
console(config)#scheduler 10 interface fastethernet 0/1 sched-algo wrr
console(config)#scheduler 20 interface fastethernet 0/1 sched-algo strict-
priority

console(config)#queue 1 interface fa 0/1 scheduler 10 weight 1
console(config)#queue 2 interface fa 0/1 scheduler 10 weight 2
console(config)#queue 3 interface fa 0/1 scheduler 10 weight 3
console(config)#queue 4 interface fa 0/1 scheduler 10 weight 4
console(config)#queue 5 interface fa 0/1 scheduler 20

console(config)#queue-map regn-priority vlanPri 1 queue-id 1
console(config)#queue-map regn-priority vlanPri 2 queue-id 2
console(config)#queue-map regn-priority vlanPri 3 queue-id 3
console(config)#queue-map regn-priority vlanPri 4 queue-id 4
console(config)#queue-map regn-priority vlanPri 5 queue-id 5
```

4.26 Обновление программного обеспечения с сервера TFTP

Сервер TFTP должен быть запущен и настроен на компьютере, с которого будет загружаться программное обеспечение. Сервер должен иметь разрешение на чтение файлов начального загрузчика и/или системного ПО. Компьютер с запущенным TFTP-сервером должен быть доступен для коммутатора (можно проконтролировать, выполнив на коммутаторе команду ping A.B.C.D, где A.B.C.D – IP-адрес компьютера).

Обновление программного обеспечения может осуществляться только привилегированным пользователем.

4.26.1 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.

Процедура обновления ПО:

Скопировать новый файл программного обеспечения на устройство в выделенную область памяти. Формат команды:

copy tftp://*tftp_ip_address*/*[directory]*/*filename image*

Или командой

```
Firmware upgrade tftp://tftp_ip_address/[directory]/filename
```

Пример команды для загрузки ПО через sftp:

```
copy sftp://username:password@Tftp_ip_address//[directory]/filename image
```

Новая версия программного обеспечения станет активной после перезагрузки коммутатора.

Для просмотра данных о версиях программного обеспечения и их активности введите команду **show bootvar**:

```
console#show bootvar
```

4.27 Режим отладки

Режим отладки позволяет снимать дополнительную диагностическую информацию с устройства.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 173 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
debug iss enable { init-shut | management-trc | data-path-trc | cntrl-plane-trc | dump-trc | os-resource-trc | all-fail}	-/disable	Включить генерацию отладочных сообщений для конкретного блока системного модуля iss.
debug iss disable { init-shut | management-trc | data-path-trc| cntrl-plane-trc | dump-trc | os-resource-trc | all-fail}		Выключить генерацию отладочных сообщений для конкретного блока системного модуля iss.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 174 – Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
no debug all	-	Отключить вывод всех отладочных сообщений.
dump sockets	-	Просмотр всех сокетов в системе.
dump mem *location* **[len** *byte***]**	location: (1..0xffffffff); byte: (1..256)	Отображение содержимого памяти из заданной области памяти.
dump {task | sem | que} name [*name***]**	-	Показать детали задачи, очереди или семафора при присвоении имени таска. - *name* – название таска
debug test mem alloc *bytes*	bytes: (1..4294967295)	Выделение блока памяти с заданным в байтах размером
debug test mem free	-	Освобождение выделенного блока памяти.
debug show sensor temprerature *index*	index: (0..1)	Отображение значения датчика температуры.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 175 – Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
debug np module { all | cfa | eth | igs | ip | iss | isspi | l2app | la | mau | mlds | mstp | pnac | qosx | rstp | tcam | vct | vlan } [level {all | errors | general | polling}]	-	Включает генерацию отладочных сообщений для NPAPI для указанного модуля.
no debug np module { all | cfa | eth | igs | ip | iss | isspi | l2app | la | mau | mlds | mstp | pnac | qosx | rstp | tcam | vct | vlan }		Выключает генерацию отладочных сообщений для NPAPI для указанного модуля.
debug show vlan np port	-	Отображает конфигурацию порта NPAPI
debug show ip arp np interfaces	-	Отображает дерево интерфейсов ARP в NPAPI

4.27.1 Команды отладки для интерфейсов

Данный режим отладки устанавливает трассировки для интерфейсов для указанного уровня severity.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 176 – Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
debug interface all *severity*	severity: (0..7)/-	Включить генерацию отладочных сообщений для всех видов трассировок.
no debug interface all		Выключить генерацию отладочных сообщений для интерфейсов.
debug interface arppktdump *severity*	severity: (0..7)/-	Включить трассировки дампа пакетов ARP.
no debug interface arppktdump		Выключить трассировки дампа пакетов ARP.
debug interface buffer *severity*	severity: (0..7)/-	Включить генерацию отладочных сообщений для пакетного буфера.
no debug interface buffer		Выключить генерацию отладочных сообщений для пакетного буфера.
debug interface enetpktdump *severity*	severity: (0..7)/-	Включить трассировки дампа пакетов Ethernet.
no debug interface enetpktdump		Выключить трассировки дампа пакетов Ethernet.
debug interface failall *severity*	severity: (0..7)/-	Включить генерацию отладочных сообщений при возникновении всех видов сбоев, включая валидацию пакетов.
no debug interface failall		Выключить генерацию отладочных сообщений при возникновении сбоев.
debug interface ippktdump *severity*	severity: (0..7)/-	Включить трассировки дампа пакетов IP.
no debug interface ippktdump		Выключить трассировки дампа пакетов IP.

debug interface os *severity*	severity: (0..7)/-	Генерирует отладочные сообщения для ресурсов ОС.
no debug interface os		Выключить генерацию отладочных сообщений для ресурсов ОС.
debug interface track *severity*	severity: (0..7)/-	Включить генерацию отладочных сообщений слежения интерфейса.
no debug interface track *severity*		Выключить генерацию отладочных сообщений слежения интерфейса.
debug interface trcerror *severity*	severity: (0..7)/-	Включить генерацию отладочных сообщений ошибок интерфейсов.
no debug interface trcerror *severity*		Выключить генерацию отладочных сообщений ошибок интерфейсов.

4.27.2 Отладка VLAN

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 177 – Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
debug vlan all-debug	-	Включить генерацию всех отладочных сообщений модуля VLAN.
no debug vlan all-debug		Выключить генерацию всех отладочных сообщений модуля VLAN.
debug vlan all-module	-	Включить генерацию отладочных сообщений, касающихся приоритета, избыточности, передачи трафика.
no debug vlan all-module		Выключить генерацию отладочных сообщений, касающихся приоритета, избыточности, передачи трафика.
debug vlan buffer	-	Включить генерацию отладочных сообщений буферов vlan.
no debug vlan buffer		Выключить генерацию отладочных сообщений буферов vlan.
debug vlan ctpl	-	Включить генерацию отладочных сообщений управления vlan.
no debug vlan ctpl		Выключить генерацию отладочных сообщений управления vlan.
debug vlan data	-	Включить генерацию отладочных сообщений обмена данными vlan.
no debug vlan data		Выключить генерацию отладочных сообщений обмена данными vlan.
debug vlan dump	-	Включить генерацию отладочных сообщений захвата пакетов vlan.
no debug vlan dump		Выключить генерацию отладочных сообщений захвата пакетов vlan.
debug vlan failall	-	Включить генерацию отладочных сообщений об ошибках vlan.
no debug vlan failall		Выключить генерацию отладочных сообщений об ошибках vlan.
debug vlan fwd	-	Включить генерацию отладочных сообщений передачи трафика vlan.
no debug vlan fwd		Выключить генерацию отладочных сообщений передачи трафика vlan.
debug vlan global	-	Включить генерацию отладочных сообщений глобально по модулю vlan
no debug vlan global		Выключить генерацию отладочных сообщений глобально по модулю vlan

debug vlan initshut	-	Включить генерацию отладочных сообщений изменения состояния модуля vlan.
no debug vlan initshut		Выключить генерацию отладочных сообщений изменения состояния модуля vlan.
debug vlan mgmt	-	Включить генерацию отладочных сообщений управления vlan.
no debug vlan mgmt		Выключить генерацию отладочных сообщений управления vlan.
debug vlan os	-	Включить генерацию отладочных сообщений для ресурсов модуля vlan, кроме буферов.
no debug vlan os		Выключить генерацию отладочных сообщений для ресурсов модуля vlan, кроме буферов.
debug vlan priority	-	Включить генерацию отладочных сообщений приоритетов vlan.
no debug vlan priority		Выключить генерацию отладочных сообщений приоритетов vlan.
debug vlan redundancy	-	Включить генерацию отладочных сообщений избыточности vlan.
no debug vlan redundancy		Выключить генерацию отладочных сообщений избыточности vlan.

4.27.3 Отладка Ethernet-oam

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 178 – Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
debug ethernet-oam all	-	Включить генерацию всех отладочных сообщений eoam.
no debug ethernet-oam all		Выключить генерацию всех отладочных сообщений eoam.
debug ethernet-oam buffer	-	Включить генерацию сообщений буферов eoam.
no debug ethernet-oam buffer		Выключить генерацию сообщений буферов eoam.
debug ethernet-oam config	-	Включить генерацию сообщений конфигурации eoam.
no debug ethernet-oam config		Выключить генерацию сообщений конфигурации eoam.
debug ethernet-oam ctrl	-	Включить генерацию сообщений управления eoam.
no debug ethernet-oam ctrl		Выключить генерацию сообщений управления eoam.
debug ethernet-oam discovery	-	Включить генерацию сообщений процесса обнаружения соседей eoam.
no debug ethernet-oam discovery		Выключить генерацию сообщений процесса обнаружения соседей eoam.
debug ethernet-oam failure	-	Включить генерацию сообщений ошибок eoam.
no debug ethernet-oam failure		Выключить генерацию сообщений ошибок eoam.
debug ethernet-oam func-entry	-	Включить генерацию сообщений входа в функции eoam.
no debug ethernet-oam func-entry		Выключить генерацию сообщений входа в функции eoam.
debug ethernet-oam func-exit	-	Включить генерацию сообщений выхода из функций eoam.
no debug ethernet-oam func-exit		Выключить генерацию сообщений выхода из функций eoam.
debug ethernet-oam init	-	Включить генерацию сообщений изменения состояния модуля eoam.
no debug ethernet-oam init		Выключить генерацию сообщений изменения состояния модуля eoam.

debug ethernet-oam lm	-	Включить генерацию сообщений link-monitor eoam.
no debug ethernet-oam lm		Выключить генерацию сообщений link-monitor eoam.
debug ethernet-oam loopback	-	Включить генерацию сообщений remote-loopback eoam.
no debug ethernet-oam loopback		Выключить генерацию сообщений remote-loopback eoam.
debug ethernet-oam mux-parser	-	Включить генерацию сообщений состояний mux-parser eoam.
no debug ethernet-oam mux-parser		Выключить генерацию сообщений состояний mux-parser eoam.
debug ethernet-oam pkt	-	Включить генерацию сообщений для пакета eoam.
no debug ethernet-oam pkt		Выключить генерацию сообщений для пакета eoam.
debug ethernet-oam redundancy	-	Включить генерацию сообщений избыточности eoam.
no debug ethernet-oam redundancy		Выключить генерацию сообщений избыточности eoam.
debug ethernet-oam resource	-	Включить генерацию сообщений для ресурсов eoam, кроме буферов
no debug ethernet-oam resource		Выключить генерацию сообщений для ресурсов eoam, кроме буферов
debug ethernet-oam rfi	-	Включить генерацию сообщений удаленного обнаружения аварий eoam.
no debug ethernet-oam rfi		Выключить генерацию сообщений удаленного обнаружения аварий eoam.
debug ethernet-oam var-reqresp	-	Включить генерацию сообщений для значений запросов-ответов eoam.
no debug ethernet-oam var-reqresp		Выключить генерацию сообщений для значений запросов-ответов eoam.

4.27.4 Журналирование отладочных сообщений

С помощью данного блока команд настраиваются параметры ведения журнала отладки в системе.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 179 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
debug-logging {*flash_url* **| console | file | flash} [standy]**	-/console	Перенаправить вывод отладочных сообщений в конкретное расположение.
no debug-logging [standby]		Установить значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 180 – Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
show debug-logging	-	Отобразить содержимое журнала отладки, хранящиеся в файле.
show debugging	-	Отобразить статус включенных опций отладки

4.27.5 Команды для отладки функций управления

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 181 – Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
debug radius {all | errors | events | packets | responses | timers}	-/выключено	Включить генерацию отладочных сообщений для протокола RADIUS.
no debug radius		Выключить генерацию отладочных сообщений для протокола RADIUS.
debug tacacs {all | dumprx | dumptx | errors | info}	-/выключено	Включить генерацию отладочных сообщений для протокола TACACS .
no debug tacacs		Выключить генерацию отладочных сообщений для протокола TACACS.
debug ssh {all | duffer | ctrl | data | dump | mgmt| resource | server | shut}	-/выключено	Включить генерацию отладочных сообщений для SSH.
no debug ssh {all | duffer | ctrl | data | dump | mgmt | resource | server | shut}		Выключить генерацию отладочных сообщений для SSH.
debug terminal take	-/выключено	Включить вывод отладочных сообщений в текущей SSH-/Telnet-сессии.
no debug terminal take		Выключает вывод отладочных сообщений в текущей SSH-/Telnet-сессии.

4.27.6 Команды для отладки протокола DHCP

Команды данного блока включают отслеживание модуля DHCP.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 182 – Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
debug ip dhcp snooping {all | entry | exit | debug | fail}	-/выключено	Включить генерацию сообщений отладки функции DHCP Snooping.
no debug ip dhcp snooping {all | entry | exit | debug | fail}		Выключить генерацию сообщений отладки функции DHCP Snooping.

debug ip dhcp client all	-/выключено	Включить генерацию всех сообщений отладки функции DHCP client.
no debug ip dhcp client all		Выключить генерацию всех сообщений отладки функции DHCP client.
debug ip dhcp client {bind | errors | event | packets}	-/выключено	Включить генерацию выборочных сообщений отладки функции DHCP client.
no debug ip dhcp client {bind | errors | event | packets}		Выключить генерацию выборочных сообщений отладки функции DHCP client.
debug ip dhcp relay {all | errors}	-/выключено	Включить генерацию сообщений отладки функции DHCP relay: - **all** – все отладочные сообщения; - **errors** – отладочные сообщения при ошибках.
no debug ip dhcp relay {all | errors}		Выключить генерацию сообщений отладки функции DHCP relay.
debug show ip dhcp np interfaces	-	Показывает конфигурацию функции контроля протокола DHCP.

4.27.7 Отладка функции PPPoE-IA

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 183 – Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
debug pppoe intermediate-agent all	-	Включить генерацию всех отладочных сообщений PPPoE-IA.
no debug pppoe intermediate-agent		Выключить генерацию всех отладочных сообщений PPPoE-IA.
debug pppoe intermediate-agent entry	-	Включить генерацию отладочных сообщений о входе в функции PPPoE-IA.
no debug pppoe intermediate-agent		Выключить генерацию всех отладочных сообщений PPPoE-IA.
debug pppoe intermediate-agent exit	-	Включить генерацию отладочных сообщений о выходе из функций PPPoE-IA.
no debug pppoe intermediate-agent		Выключить генерацию всех отладочных сообщений PPPoE-IA.
debug pppoe intermediate-agent fail	-	Включить генерацию отладочных сообщений об ошибках PPPoE-IA.
no debug pppoe intermediate-agent		Выключить генерацию всех отладочных сообщений PPPoE-IA.
debug pppoe intermediate-agent pkt	-	Включить генерацию отладочных сообщений о пакетах PPPoE-IA.
no debug pppoe intermediate-agent		Выключить генерацию всех отладочных сообщений PPPoE-IA.

4.27.8 Отладка функции DCS

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 184 – Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
debug dcs all	-	Включить генерацию всех отладочных сообщений dcs.
no debug dcs		Выключить генерацию всех отладочных сообщений dcs.
debug dcs entry	-	Включить генерацию отладочных сообщений о входе в функции dcs.
no debug dcs		Выключить генерацию всех отладочных сообщений dcs.
debug dcs exit	-	Включить генерацию отладочных сообщений о выходе из функций dcs.
no debug dcs		Выключить генерацию всех отладочных сообщений dcs.
debug dcs fail	-	Включить генерацию отладочных сообщений об ошибках dcs.
no debug dcs		Выключить генерацию всех отладочных сообщений dcs.

4.27.9 Отладка функций QoS

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 185 – Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
debug qos buffer	-	Включить генерацию отладочных сообщений для буферов QoS.
no debug qos buffer		Выключить генерацию отладочных сообщений для буферов QoS.
debug qos ctrl	-	Включить генерацию отладочных сообщений для управления QoS.
no debug qos ctrl		Выключить генерацию отладочных сообщений для управления QoS.
debug qos dump	-	Включить генерацию отладочных сообщений по пакетам QoS.
no debug qos dump		Выключить генерацию отладочных сообщений по пакетам QoS.
debug qos failall	-	Включить генерацию отладочных сообщений по ошибкам QoS.
no debug qos failall		Выключить генерацию отладочных сообщений по ошибкам QoS.
debug qos init-shut	-	Включить генерацию отладочных сообщений по изменению состояния модуля QoS.
no debug qos init-shut		Выключить генерацию отладочных сообщений по изменению состояния модуля QoS.
debug qos mgmt	-	Включить генерацию отладочных сообщений для управления QoS.
no debug qos mgmt		Выключить генерацию отладочных сообщений для управления QoS.
debug qos os	-	Включить генерацию отладочных сообщений для ресурсов QoS, кроме буферов.
no debug qos os		Выключить генерацию отладочных сообщений для ресурсов QoS, кроме буферов.

4.27.10 Команды для отладки протокола SNTP

Команды данного блока позволяют снимать дополнительную диагностическую информациюдля протокола SNTP.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 186 – Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
debugsntp {all | all-fail | buff | control | data-path | init-shut | mgmt| resource}	-/выключено	Включить генерацию отладочных сообщения блока SNTP
no debugsntp {all | all-fail | buff | control | data-path | init-shut | mgmt| resource}		Выключить генерацию отладочных сообщения блока SNTP

4.27.11 Команды для отладки протокола STP

Команды данного блока позволяют снимать дополнительную диагностическую информацию для протокола STP.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 187 – Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
debug spanning-tree global	-/выключено	Включить генерацию отладочных сообщений для протокола STP глобально.
no debug spanning-tree global		Установить значение по умолчанию.
debug spanning-tree all	-/выключено	Включить генерацию всех отладочных сообщений для протокола STP.
no debug spanning-tree all		Установить значение по умолчанию.
debug spanning-tree errors	-/выключено	Включить генерацию сообщений отладки для протокола STP для диагностики ошибок.
no debug spanning-tree errors		Установить значение по умолчанию.
debug spanning-tree init-shut	-/выключено	Включить генерацию сообщений отладки для протокола STP для init и shutdown. Эта трассировка генерируется при неудачной или успешной инициализации или закрытии модуля STP.
no debug spanning-tree init-shut		Установить значение по умолчанию.
debug spanning-tree management	-/выключено	Включает генерацию сообщений отладки при управлении протоколом STP. Отладочные сообщения генерируются каждый раз, когда вы настраиваете какие-либо функции STP.
no debug spanning-tree management		Установить значение по умолчанию.

debug spanning-tree memory	-/выключено	Включить генерацию отправки отладочных сообщений при неудачном и успешном выделении памяти для STP-процесса.
no debug spanning-tree memory		Установить значение по умолчанию.
debug spanning-tree bpdu	-/выключено	Включает генерацию сообщений отладки для протокола STP при неудачном и успешном приеме, передаче и обработке пакетов BPDU.
no debug spanning-tree bpdu		Установить значение по умолчанию.
debug spanning-tree events	-/выключено	Включает генерацию сообщений отладки для событий конфигурации протокола STP. Сообщения генерируются при настройке функций STP.
no debug spanning-tree events		Установить значение по умолчанию.
debug spanning-tree timers	-/выключено	Включает генерацию сообщений отладки при неудачном, успешном запуске, при остановке или перезапуске таймеров протокола STP.
no debug spanning-tree timers		Установить значение по умолчанию.
debug spanning-tree {port-info-state-machine | port-receive-state-machine | port-role-selection-state-machine | port-transmit-state-machine }	-/выключено	Включает генерацию сообщений отладки для портов, задействованных в построении дерева STP.
no debug spanning-tree {port-info-state-machine | port-receive-state-machine | port-role-selection-state-machine | port-transmit-state-machine| pseudoInfo-state-machine}		Установить значение по умолчанию.
debug spanning-tree redundancy	-/выключено	Включает генерацию сообщений отладки в резервном узле STP при выполнении резервного копирования информации о конфигурации от активного узла.
no debug spanning-tree redundancy		Установить значение по умолчанию.
debug spanning-tree sem-variables	-/выключено	Включает генерацию сообщений отладки для протокола STP при неудачном и успешном создании и удаление семафора.
no debug spanning-tree		Установить значение по умолчанию.
debug show spanning-tree port-state {gigabitethernet *gi_port* **| fastethernet** *fa_port***}**	-	Отобразить STP-состояния порта во всех существующих инстансах.
debug show spanning-tree vlan-mapping [instance]	instance: (0..63)	Отобразить маппинг VLAN по инстансам. Если указан опциональный параметр instance, то выводится маппинг только для этого инстанса.
debug spanning-tree bridge-detection-state-machine	-/выключено	Включить отладочные сообщения для механизма обнаружения соседей.
debug spanning-tree topology-change-state-machine	-/выключено	Включить отладочные сообщения для механизма обнаружения изменений топологии.

4.27.12 Команды для отладки протокола LLDP

Команды данного блока позволяют снимать дополнительную диагностическую информацию для протокола LLDP.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 188 – Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
debug lldp all	-/выключено	Включить генерацию всех отладочных сообщений для протокола LLDP.
no debug lldp all		Установить значение по умолчанию.
debug lldp all-fail	-/выключено	Включает генерацию сообщений отладки для протокола LLDP для диагностики ошибок.
no debug lldp all-fail		Установить значение по умолчанию.
debug lldp {buf | critical | ctrl | data-path | init-shut | mgmt | pkt-dump | redundancy | resourve}	-/выключено	Включить генерацию выборочных отладочных сообщений протокола LLDP. - *buf* – отладочные сообщения, связанные с буфером LLDP; - *critical* –отладочные сообщения критического уровня; - *ctrl* – отладочные сообщения при сбое при изменении или получении записей LLDP; - *data-path* –отладочные сообщения, касающиеся пути передачи или получения записей LLDP; - *init-shut* – отладочные сообщения при неудачной инициализации и выключении модуля LLDP; - *mgmt* – отладочные сообщения при сбое в конфигурации любой из функций LLDP; - *pkt-dump* –отладочные сообщения для трассировки дампов пакетов; - *resource* – отладочные сообщения, связанные с ресурсами ОС. Эта трассировка генерируется при сбое в очередях сообщений.
no debug lldp {buf | critical | ctrl | data-path | init-shut | mgmt. | pkt-dump | redundancy | resourve}		Установить значение по умолчанию.
debug lldp tlvall	-/выключено	Генерирует отладочные сообщения для всех TLV-опций.
no debug lldp tlv all		Установить значение по умолчанию.
debug lldp tlv {chassis-id | inventory-management | lag | mac-phy | max-frame | med-capability | mgmt-addr | mgmt-vid | network-policy | port-vlan | ppvlan | proto-id | pwr-mdi | sys-capab | sys-descr | sys-name | ttl | vid-digest | vlan-name}	-/выключено	Генерирует отладочные сообщения для выборочных функций TLV-опций.
no debug lldp tlv		Установить значение по умолчанию.

4.27.13 Команды для отладки функции IGMP Snooping

Команды данного блока позволяют снимать дополнительную диагностическую информацию для протокола IGMP.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 189 – Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
debug ip igmp snooping all	-/выключено	Включить генерацию всех отладочных сообщений для функции IGMP Snooping.
no debug ip igmp snooping all		Установить значение по умолчанию.

debug ip igmp snooping {entry | exit}	-/выключено	Включить генерацию отладочных сообщений для диагностики входа-выхода в функцию IGMP Snooping.
no debug ip igmp snooping {entry | exit}		Установить значение по умолчанию.
debug ip igmp snooping fwd	-/выключено	Включить генерацию отладочных сообщений в случае пересылки базы данных IGMP.
no debug ip igmp snooping fwd		Установить значение по умолчанию.
debug ip igmp snooping grp	-/выключено	Включить генерацию отладочных сообщений, в случае задействования информации о IGMP-группах.
no debug ip igmp snooping grp		Установить значение по умолчанию.
debug ip igmp snooping init	-/выключено	Включить генерацию сообщения по событиям инициализации и shutdown, информация заносится в файл.
no debug ip igmp snooping init		Установить значение по умолчанию.
debug ip igmp snooping {mgmt | redundancy | resourses| vlan | src}	-/выключено	Включить генерацию выборочных отладочных сообщений для функции IGMP Snooping.
no debug ip igmp snooping mgmt		Установить значение по умолчанию.
debug ip igmp snooping pkt	-/выключено	Включить генерацию отладочных сообщений при возникновении ошибки при передаче или приеме пакетов IGMP.
no debug ip igmp snooping pkt		Установить значение по умолчанию.
debug ip igmp snooping qry	-/выключено	Включить генерацию пакетов при отправке или получении query-пакетов IGMP.
no debug ip igmp snooping qry		Установить значение по умолчанию.
debug ip igmp snooping tmr	-/выключено	Включить генерацию пакетов в тех случаях, когда задействованы таймеры.
no debug ip igmp snooping tmr		Установить значение по умолчанию.
debug ip igmp snooping trace {all | data-path | ctrl-path | Rx | Tx}	-/выключено	Включить генерацию отладочных сообщений для диагностики трассировок, связанных с протоколом IGMP. - all – включить генерацию всех отладочных сообщений; - Rx – включить генерацию отладочных сообщений для трассировки принимаемых пакетов; - Tx – включить генерацию отладочных сообщений для трассировки передаваемых пакетов; - ctrl-path – включить генерацию отладочных сообщений при прохождении контрольной управляющей информации; - data-path – включить генерацию отладочных сообщений при прохождении мультикаст-трафика.
no debug ip igmp snooping trace {all | data-path | ctrl-path | Rx | Tx}		Установить значение по умолчанию.

4.27.14 Отладка для port-channel

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 190 – Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
debug lacp all	-	Включить генерацию всех отладочных сообщенийя для LACP.
no debug lacp all		Выключить генерацию всех отладочных сообщенийя для LACP.
debug lacp buffer	-	Включить генерацию отладочных сообщений по буферам LACP.

no debug lacp buffer		Выключить генерацию отладочных сообщений по буферам LACP.
debug lacp data	-	Включить генерацию отладочных сообщений обмена данными LACP.
no debug lacp data		Выключить генерацию отладочных сообщений обмена данными LACP.
debug lacp events	-	Включить генерацию отладочных сообщений по событиям LACP.
no debug lacp events		Выключить генерацию отладочных сообщений по событиям LACP.
debug lacp failall	-	Включить генерацию отладочных сообщений по ошибкам LACP.
no debug lacp failall		Выключить генерацию отладочных сообщений по ошибкам LACP.
debug lacp init-shutdown	-	Включить генерацию отладочных сообщений изменения состояния LACP.
no debug lacp init-shutdown		Выключить генерацию отладочных сообщений изменения состояния LACP.
debug lacp mgmt	-	Включить генерацию отладочных сообщений по управляющим сообщениям LACP.
no debug lacp mgmt		Выключить генерацию отладочных сообщений по управляющим сообщениям LACP.
debug lacp os	-	Включить генерацию отладочных сообщений по ресурсам LACP, исключая буферы.
no debug lacp os		Выключить генерацию отладочных сообщений по ресурсам LACP, исключая буферы.
debug lacp packet	-	Включить генерацию отладочных сообщений по пакетам LACP.
no debug lacp packet		Выключить генерацию отладочных сообщений по пакетам LACP.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 191 – Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
debug etherchannel all	-	Включить генерацию всех отладочных сообщений для LAG.
no debug etherchannel all		Выключить генерацию всех отладочных сообщений для LAG.
debug etherchannel detail	-	Включить генерацию подробных отладочных сообщений для LAG.
no debug etherchannel detail		Выключить генерацию подробных отладочных сообщений для LAG.
debug etherchannel error	-	Включить генерацию отладочных сообщений об ошибках LAG.
no debug etherchannel error		Выключить генерацию отладочных сообщений об ошибках LAG.
debug etherchannel event	-	Включить генерацию отладочных сообщений по событиям LAG.
no debug etherchannel event		Выключить генерацию отладочных сообщений по событиям LAG.
debug etherchannel idb	-	Включить генерацию отладочных сообщений по дескрипторам интерфейсов LAG.
no debug etherchannel idb		Выключить генерацию отладочных сообщений по дескрипторам интерфейсов LAG.

4.27.15 Отладка loopback-detection

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 192 – Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
debug loopback-detection all	-	Включить генерацию всех отладочных сообщений LBD.
no debug loopback-detection all		Выключить генерацию всех отладочных сообщений LBD.
debug loopback-detection buffer-alloc	-	Включить генерацию отладочных сообщений для буферов LBD.
no debug loopback-detection buffer-alloc		Выключить генерацию отладочных сообщений для буферов LBD.
debug loopback-detection control	-	Включить генерацию отладочных сообщений управления LBD.
no debug loopback-detection control		Выключить генерацию отладочных сообщений управления LBD.
debug loopback-detection pkt-dump	-	Включить генерацию отладочных сообщений захвата пакетов LBD.
no debug loopback-detection pkt-dump		Выключить генерацию отладочных сообщений захвата пакетов LBD.
debug loopback-detection pkt-flow	-	Включить генерацию отладочных сообщений потоков трафика LBD.
no debug loopback-detection pkt-flow		Выключить генерацию отладочных сообщений потоков трафика LBD.

4.27.16 Отладка для протокола SNMP

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 193 – Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
debug snmp	-	Включить генерацию всех отладочных сообщений для SNMP.
no debug snmp		Выключить генерацию всех отладочных сообщений для SNMP.

4.27.17 Команды для диагностики параметров TCAM

Команды данного блока позволяют снимать дополнительную диагностическую информацию для TCAM.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 194 – Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
debug show tcam	-	Отобразить информацию о TCAM.
debug show tcam domains	-	Отобразить информацию о доменах TCAM.
debug show tcam block *block_index* **[all]**	-	Отобразить информацию о блоке TCAM и допустимые записи. - *block_index* – индекс блока TCAM. block_id: (0..11); - *all* – печать всех записей, включая недопустимые.
debug show tcam entry *entry_index*	-	Отобразить информацию о записи TCAM и ее полей. - entry_index – индекс записи TCAM; entry_id:(0..1535);
debug show tcam entry allocated	-	Отобразить информацию о зарезервированных и использованных записях TCAM и о их владельцах.
debug show tcam portmask	-	Отобразить таблицу масок портов TCAM.
debug set tcam entry *entry_id* **field** *f_type* **data** *f_data* **mask** *f_mask*	entry_id: (0..1535); f_type: (0..114); f_data: (0..65535); f_mask: (0..65535)	Указать тип поля TCAM.
debug unset tcam entry *entry_id* **field** *f_type*		Стереть данные поля указанного entry_id.
debug set tcam entry *entry_id* **enable**	entry_id: (0..1535)	Включить работу записи TCAM с заданным entry_id.
debug set tcam entry *entry_id* **disable**		Выключить работу записи TCAM с заданным entry_id.
debug set tcam entry *entry_id* **move** *move* **{number** *number***}**	entry_id: (0..1535)	Переместить указанную запись TCAM в назначенную.
debug set tcam entry *entry_id* **action drop [withdraw]**	entry_id: (0..1535)	Установить действие drop для пакетов, которые не попали ни под одно правило.
debug unset tcam entry *entry_id* **action drop**		Отключить действие удаления.
debug set tcam entry *entry_id* **action redirect { port_number | cpu }**	entry_id: (0..1535)	Перенаправить пакеты, попадающие под правило с указанным entry_id в заданный порт или на ЦПУ.
debug set tcam entry *entry_id* **action redirect**		Отключить перенаправление пакетов.
debug set tcam entry *entry_id* **action inner-tag assign { vlan-id | shift | shift-from-outer-tag | inner-pvid }** *assigned_val*	entry_id: (0..1535)	Добавляет внутренний тег к пакетам, попадающим под TCAM-запись с указанным enter_id.
debug unset tcam entry *entry_id* **action inner-tag assign**		Удалить внутренний тег.
debug set tcam entry *entry_id* **action inner-tag format { none | untag | tag | keep }**	entry_id: (0..1535)	Установите действие внутреннего тега форматирования для записи TCAM. - *none* – не выполнять никакое действие; - *untag* – удалить внутренний тег; - *tag* – вставить внутренний тег; - *keep* – сохранить содержимое тега.
debug unset tcam entry *entry_id* **action inner-tag format**		Удалить действие тега.
debug set tcam entry *entry_id* **action outer-tag assign { vlan-id | shift | shift-from-inner-tag | outer-pvid }** *assigned_val*	entry_id: (0..1535)	Добавляет внешний тег к пакетам, попадающим под TCAM-запись с указанным enter_id.
debug unset tcam entry *entry_id* **action outer-tag assign**		Удалить внешний тег с пакетов с заданным entry_id записи TCAM.

debug set tcam entry *entry_id* **action outer-tag format { none | untag | tag | keep }**	entry_id: (0..1535)	Установите действие внешнего тега форматирования для записи TCAM. - *none* – не выполнять никакое действие; - *untag* – удалить внешний тег; - *tag* – вставить внешний тег; - *keep* – сохранить содержимое тега.
debug unset tcam entry *entry_id* **action outer-tag format**		Удалить действие тега.
debug set tcam entry *entry_id* **action {inner-tpid** *inner-tpid* **| outer-tpid** *outer-tpid***}**	entry_id: (0..1535)	Добавить внутренний или внешний TPID к указанной записи TCAM.
debug set tcam entry *entry_id* **action {inner-tpid | outer-tpid}**		Удалить внутренний или внешний TPID к указанной записи TCAM
debug set tcam entry *entry_id* **action remark { inner-user-pri | other-user-pri | dscp | ip-precedence | copy-ipri-to-opri | copy-opri-to-ipri | keep-inner-pri | keep-outer-pri }** *rem_val*	entry_id: (0..1535)	Настроить перезапись параметров QoS для указанной записи TCAM. - *copy-ipri-to-opri* – скопировать приоритет из внутреннего тега во внешний; - *copy-opri-to-ipri* – скопировать приоритет из внешнего тега во внутренний; - *dscp* – перезаписать поле DSCP в заголовке IP; - *inner-user-pri* – перезаписать приоритет 802.1p во внутренний тег VLAN; - *ip-precedence* -перезаписать поле ToS в заголовке IP; - *keep-inner-pri* – сохранить приоритет внутреннего тега; - *keep-outer-pri* – сохранить приоритет внешнего тега; - *outer-user-pri* – перезаписать приоритет 802.1p во внешнем тега VLAN.
debug set tcam entry *entry_id* **action remark**		Удалить перезапись параметров QoS для указанной записи TCAM.
debug show tcam applications	-	Отобразить общую информацию о TCAM.
debug show tcam range	-	Отобразить таблицу сравнения диапазона.
debug show tcam udb	-	Показать таблицу выбора полей (смещения UDB).

ПРИЛОЖЕНИЕ А. КОНСОЛЬНЫЙ КАБЕЛЬ

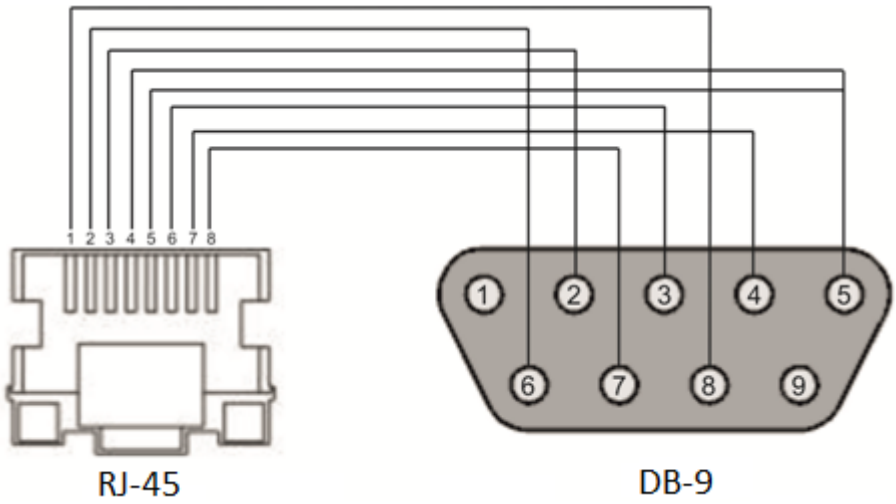

Рисунок А.1 – Подключение консольного кабеля

ПРИЛОЖЕНИЕ Б. ПОДДЕРЖИВАЕМЫЕ ЗНАЧЕНИЯ ETHERTYPE

Таблица Б.1 – Поддерживаемые значения EtherType

0x22DF	0x8145	0x889e	0x88cb	0x88e0	0x88f4	0x8808	0x881d	0x8832	0x8847
0x22E0	0x8146	0x88a8	0x88cc	0x88e1	0x88f5	0x8809	0x881e	0x8833	0x8848
0x22E1	0x8147	0x88ab	0x88cd	0x88e2	0x88f6	0x880a	0x881f	0x8834	0x8849
0x22E2	0x8203	0x88ad	0x88ce	0x88e3	0x88f7	0x880b	0x8820	0x8835	0x884A
0x22E3	0x8204	0x88af	0x88cf	0x88e4	0x88f8	0x880c	0x8822	0x8836	0x884B
0x22E6	0x8205	0x88b4	0x88d0	0x88e5	0x88f9	0x880d	0x8824	0x8837	0x884C
0x22E8	0x86DD	0x88b5	0x88d1	0x88e6	0x88fa	0x880f	0x8825	0x8838	0x884D
0x22EC	0x86DF	0x88b6	0x88d2	0x88e7	0x88fb	0x8810	0x8826	0x8839	0x884E
0x22ED	0x885b	0x88b7	0x88d3	0x88e8	0x88fc	0x8811	0x8827	0x883A	0x884F
0x22EE	0x885c	0x88b8	0x88d4	0x88e9	0x88fd	0x8812	0x8828	0x883B	0x8850
0x22EF	0x8869	0x88b9	0x88d5	0x88ea	0x88fe	0x8813	0x8829	0x883C	0x8851
0x22F0	0x886b	0x88ba	0x88d6	0x88eb	0x88ff	0x8814	0x882A	0x883D	0x8852
0x22F1	0x8881	0x88bf	0x88d7	0x88ec	0x8800	0x8815	0x882B	0x883E	0x9999
0x22F2	0x888b	0x88c4	0x88d8	0x88ed	0x8801	0x8816	0x882C	0x883F	0x9c40
0x22F3	0x888d	0x88c6	0x88d9	0x88ee	0x8803	0x8817	0x882D	0x8840	
0x22F4	0x888e	0x88c7	0x88db	0x88ef	0x8804	0x8819	0x882E	0x8841	
0x0800	0x8895	0x88c8	0x88dc	0x88f0	0x8805	0x881a	0x882F	0x8842	
0x8086	0x8896	0x88c9	0x88dd	0x88f1	0x8806	0x881b	0x8830	0x8844	
0x8100	0x889b	0x88ca	0x88de	0x88f2	0x8807	0x881c	0x8831	0x8846	

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) 274-47-87
+7(383) 272-83-31
E-mail: **techsupp@eltex.nsk.ru**

На официальном сайте компании Вы можете найти техническую документацию и программное обеспечение для продукции ООО «Предприятие «ЭЛТЕКС», обратиться к базе знаний, оставить интерактивную заявку или проконсультироваться у инженеров Сервисного центра на техническом форуме.

Официальный сайт компании: **http://eltex-co.ru/**
Технический форум: **http://eltex-co.ru/forum**
База знаний: **http://kcs.eltex.nsk.ru/**
Центр загрузок: **http://eltex-co.ru/support/downloads**