Комплексные решения для построения сетей

Ethernet-коммутаторы агрегации

MES5312, MES5316A, MES5324A, MES5332A

Руководство по эксплуатации, версия ПО 5.5.4

Версия документа	Дата выпуска	Содержание изменений
Версия 1.11	**15.10.2019**	**Добавлены разделы:** **5.9.5 Selective Q-in-Q** **5.15.6 Настройка протокола G.8032v2 (ERPS)** **Изменения в разделах:** **5.11 Группы агрегации каналов – Link Aggregation Group (LAG)** **5.19.4 Протокол управления сетью (SNMP)**
Версия 1.10	**20.05.2019**	**Добавлено описание моделей коммутаторов MES5316A, MES5324A, MES5332A**
Версия программного обеспечения	**5.5.4**	

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.

1 ВВЕДЕНИЕ

В последние годы наблюдается тенденция к осуществлению масштабных проектов по построению сетей связи в соответствии с концепцией NGN. Одной из основных задач при реализации крупных мультисервисных сетей является создание надежных и высокопроизводительных транспортных сетей, которые являются опорными в многослойной архитектуре сетей следующего поколения.

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

Коммутаторы серий MES5312, MES5316A, MES5324A, MES5332A могут использоваться на сетях крупных предприятий и предприятий малого и среднего бизнеса (SMB), в операторских сетях. Они обеспечивают высокую производительность, гибкость, безопасность, многоуровневое качество обслуживания (QoS). Коммутаторы MES5312, MES5316A, MES5324A, MES5332A обладают повышенной надежностью за счет резервирования узлов, определяющих бесперебойность функционирования – модулей питания и модулей вентиляции.

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

2 ОПИСАНИЕ ИЗДЕЛИЯ

2.1 Назначение

Коммутаторы агрегации серий MES5312, MES5316A, MES5324A, MES5332A – это высокопроизводительные устройства, оснащенные интерфейсами 10GBASE-R, 1000BASE-X и предназначенные для использования в операторских сетях в качестве устройств агрегации и в небольших центрах обработки данных (ЦОД).

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

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

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

2.2 Функции коммутатора

2.2.1 Базовые функции

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

Таблица 1 – Базовые функции устройства

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

2.2.2 Функции при работе с MAC–адресами

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

Таблица 2 – Функции работы с MAC-адресами

Таблица MAC-адресов	Коммутатор составляет в памяти таблицу, в которой устанавливается соответствие между MAC-адресами и узлами портов коммутатора.
Режим обучения	В отсутствие обучения, данные, поступающие на какой-либо порт, передаются на все остальные порты коммутатора. В режиме обучения коммутатор анализирует кадры и, определив MAC-адрес отправителя, заносит его в таблицу коммутации. Впоследствии кадр Ethernet, предназначенный для хоста, MAC-адрес которого уже есть в таблице, передается только через указанный в таблице порт.
Поддержка передачи на несколько MAC-адресов (MAC Multicast Support)	Данная функция позволяет устанавливать соединения «один ко многим» и «многие ко многим». Таким образом, кадр, адресованный многоадресной группе, передается на каждый порт, входящий в группу.
Автоматическое время хранения MAC-адресов (Automatic Aging for MAC Addresses)	Если от устройства с определенным MAC-адресом за определенный период времени не поступают пакеты, то запись для данного адреса устаревает и удаляется. Это позволяет поддерживать таблицу коммутации в актуальном состоянии.
Статические записи MAC (Static MAC Entries)	Сетевой коммутатор позволяет пользователю определить статические записи соответствий MAC-адресов, которые сохраняются в таблице коммутации.

2.2.3 Функции второго уровня сетевой модели OSI

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

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

Функция IGMP Snooping	Реализация протокола IGMP позволяет на основе информации, полученной при анализе содержимого IGMP-пакетов, определить, какие устройства в сети участвуют в группах многоадресной рассылки, и адресовать трафик на соответствующие порты.
Функция MLD Snooping	Реализация протокола MLD позволяет устройству минимизировать многоадресный IPv6 трафик.
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.
Private VLAN (light version)	Обеспечивает изоляцию между устройствами, находящимися в одном широковещательном домене, в пределах всей L2-сети. Реализованы только два режима работы порта Promiscuous и Isolated (Isolated-порты не могут обмениваться друг с другом).
Поддержка протокола STP (Spanning Tree Protocol)	Spanning Tree Protocol — сетевой протокол, основной задачей которого является приведение сети Ethernet с избыточными соединениями к древовидной топологии, исключающей петли. Коммутаторы обмениваются конфигурационными сообщениями, используя кадры специального формата, и выборочно включают и отключают передачу на порты.
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.
Протокол ERPS (Ethernet Ring Protection Switching)	Протокол предназначен для повышения устойчивости и надежности сети передачи данных, имеющей кольцевую топологию, за счет снижения времени восстановления сети в случае аварии. Время восстановления не превышает 1 секунды, что существенно меньше времени перестройки сети при использовании протоколов семейства spanning tree.
Поддержка VLAN	VLAN – это группа портов коммутатора, образующих одну широковещательную область (домен). Коммутатор поддерживает различные средства классификации пакетов для определения их принадлежности к определенной VLAN.
Поддержка GVRP (GARP VLAN)	Протокол регистрации GARP VLAN обеспечивает динамическое добавление/удаление групп VLAN на портах коммутатора. Если включен протокол GVRP, коммутатор определяет, а затем распространяет данные о принадлежности к VLAN на все порты, являющиеся частью активной топологии.
Поддержка VLAN на базе портов (Port-Based VLAN)	Распределение по группам VLAN выполняется по входящим портам. Данное решение позволяет использовать на каждом порту только одну группу VLAN.
Поддержка 802.1Q	IEEE 802.1Q – открытый стандарт, который описывает процедуру тегирования трафика для передачи информации о принадлежности к VLAN. Позволяет использовать несколько групп VLAN на одном порту.
Объединение каналов с использованием LACP	Протокол LACP обеспечивает автоматическое объединение отдельных связей между двумя устройствами (коммутатор–коммутатор или коммутатор–сервер) в единый канал передачи данных. В протоколе постоянно определяется возможность объединения каналов, и в случае отказа соединения, входящего в объединенный канал, его трафик автоматически перераспределяется по не отказавшим компонентам объединенного канала.

Создание групп LAG	В устройствах поддерживается функция создания групп каналов. Агрегация каналов (Link aggregation, trunking) или IEEE 802.3ad — технология объединения нескольких физических каналов в один логический. Это способствует не только увеличению пропускной способности магистральных каналов коммутатор—коммутатор или коммутатор—сервер, но и повышению их надежности. Возможны три типа балансировки – на основании MAC-адресов, на основании IP-адресов и на основании порта (socket) назначения. Группа LAG состоит из портов с одинаковой скоростью, работающих в дуплексном режиме.
Поддержка Auto Voice VLAN	Предоставляет возможность идентифицировать голосовой трафик на основании OUI (Organizationally Unique Identifier – первые 24 бита MAC-адреса). Если в MAC-таблице коммутатора присутствует MAC-адрес с OUI голосового шлюза или же IP-телефона, то данный порт автоматически добавляется в voice vlan (идентификация по протоколу SIP или же по MAC-адресу получателя не поддерживается).

2.2.4 Функции третьего уровня сетевой модели OSI

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

Таблица 4 – Описание функций третьего уровня (Layer 3)

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

2.2.5 Функции QoS

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

Таблица 5 – Основные функции качества обслуживания

Поддержка приоритетных очередей	Устройство поддерживает 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.

2.2.6 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.
UDP relay	Перенаправление широковещательного UDP-трафика на указанный IP-адрес
Функции DHCP-сервера	DHCP-сервер осуществляет централизованное управление сетевыми адресами и соответствующими конфигурационными параметрами, автоматически предоставляя их клиентам.
IP Source address guard	Функция коммутатора, которая ограничивает IP-трафик, фильтруя его на основании таблицы соответствий базы данных привязки DHCP – DHCP snooping и статически сконфигурированных IP-адресов. Функция используется для борьбы с подменой IP-адресов.
Dynamic ARP Inspection (Protection)	Функция коммутатора, предназначенная для защиты от атак с использованием протокола ARP. Сообщение, которое поступает с ненадежного порта, подвергается проверке – соответствует ли IP-адрес в теле принятого ARP-пакета IP-адресу отправителя. Если адреса не совпадают, то коммутатор отбрасывает пакет.
L2 – L3 – L4 ACL (Access Control List)	На основе информации, содержащейся в заголовках уровней 2, 3 и 4, у администратора есть возможность настроить до 1024 правил, согласно которым пакет будет обработан, либо отброшен.
Time-Based ACL	Позволяет сконфигурировать временные рамки, в течение которых данный ACL будет действовать.
Поддержка заблокированных портов	Основная функция блокировки – повысить безопасность сети, предоставляя доступ к порту коммутатора только для устройств имеющих MAC-адреса, закрепленные за этим портом.

Проверка подлинности на основе порта (802.1x)	Проверка подлинности IEEE 802.1x представляет собой механизм контроля доступа к ресурсам через внешний сервер. Прошедшие проверку подлинности пользователи получают доступ к ресурсам выбранной сети.

2.2.7 Функции управления коммутатором

Таблица 7 – Основные функции управления коммутаторами

Загрузка и выгрузка файла настройки	Параметры устройств сохраняются в файле настройки, который содержит данные конфигурации как всей системы в целом, так и определенного порта устройства.
Протокол TFTP (Trivial File Transfer Protocol)	Протокол TFTP используется для операций записи и чтения файлов. Протокол основан на транспортном протоколе UDP. Устройства поддерживают загрузку и передачу по данному протоколу файлов настройки и образов программного обеспечения.
Протокол SCP (Secure Copy)	Протокол SCP используется для операций записи и чтения файлов. Протокол основан на сетевом протоколе SSH. Устройства поддерживают загрузку и передачу по данному протоколу файлов настройки и образов программного обеспечения.
Удаленный мониторинг (RMON)	Удаленный мониторинг (RMON) – средство мониторинга компьютерных сетей, расширение SNMP. Совместимые устройства позволяют собирать диагностические данные с помощью станции управления сетью. RMON – это стандартная база MIB, в которой определены текущая и предыдущая статистика уровня MAC и объекты управления, предоставляющие данные в реальном времени.
Протокол SNMP	Протокол SNMP используется для мониторинга и управления сетевым устройством. Для управления доступом к системе определяется список записей сообщества, каждая из которых содержит привилегии доступа.
Интерфейс командной строки (CLI)	Управление коммутаторами посредством CLI осуществляется локально через последовательный порт RS-232, либо удаленно через telnet, ssh. Интерфейс командной строки консоли (CLI) является промышленным стандартом. Интерпретатор CLI предоставляет список команд и ключевых слов для помощи пользователю и сокращению объема вводимых данных.
Syslog	*Syslog* – протокол, обеспечивающий передачу сообщений о происходящих в системе событиях, а также уведомлений об ошибках удаленным серверам.
SNTP (Simple Network Time Protocol)	Протокол *SNTP* – протокол синхронизации времени сети, гарантирует точность синхронизации времени сетевого устройства с сервером до миллисекунды.
Traceroute	*Traceroute* – служебная функция, предназначенная для определения маршрутов передачи данных в IP-сетях.
Управление контролируемым доступом – уровни привилегий	Администратор может определить уровни привилегий доступа для пользователей устройства и характеристики для каждого уровня привилегий (только для чтения – 1 уровень, полный доступ – 15 уровень).
Блокировка интерфейса управления	Коммутатор способен устанавливать запрет доступа к каждому интерфейсу управления (SNMP, CLI). Запрет может быть установлен отдельно для каждого типа доступа: Telnet (CLI over Telnet Session) Secure Shell (CLI over SSH) SNMP
Локальная аутентификация	Для локальной аутентификации поддерживается хранение паролей в базе данных коммутатора.
Фильтрация IP-адресов для SNMP	Доступ по SNMP разрешается для определенных IP-адресов, являющихся членами SNMP-сообщества.

Клиент RADIUS	Протокол RADIUS используется для аутентификации, авторизации и учета. Сервер RADIUS использует базу данных пользователей, которая содержит данные проверки подлинности для каждого пользователя. Коммутаторы содержат клиентскую часть протокола RADIUS.
TACACS+ (Terminal Access Controller Access Control System)	Устройство предоставляет поддержку проверки подлинности клиентов посредством протокола TACACS+. Протокол TACACS+ обеспечивает централизованную систему безопасности для проверки пользователей, получающих доступ к устройству, а также централизованную систему управления при соблюдении совместимости с RADIUS и другими процессами проверки подлинности.
Сервер SSH	Функция сервера SSH позволяет клиенту SSH установить с устройством защищенное соединение для управления им.
Поддержка макрокоманд	Данная функция предоставляет возможность создавать макрокоманды, представляющие собой набор команд, и применять их для конфигурации устройства.

2.2.8 Дополнительные функции

В таблице 8 приведены дополнительные функции устройства.

Таблица 8 – Дополнительные функции устройства

Диагностика оптического трансивера	Устройство позволяет тестировать оптический трансивер. При тестировании отслеживаются такие параметры, как ток и напряжение питания, температура трансивера. Для реализации требуется поддержка этих функций в трансивере.
Green Ethernet	Данный механизм позволяет коммутатору снизить энергопотребление за счет отключения неактивных электрических портов.

2.3 Основные технические характеристики

Основные технические параметры коммутаторов приведены в таблице 9.

Таблица 9 – Основные технические характеристики

Общие параметры		
Пакетный процессор	MES5312	Marvell 98DX8212-A0 (Lewis)
	MES5316A	Marvell 98DX8316
	MES5324A	Marvell 98DX8324
	MES5332A	Marvell 98DX8332
Интерфейсы	MES5312	1x10/100/1000BASE-T (OOB) 12x10GBASE-R (SFP+)/1000BASE-X (SFP)
	MES5316A	1x10/100/1000BASE-T (OOB) 16x10GBASE-R (SFP+)/1000BASE-X (SFP)
	MES5324A	1x10/100/1000BASE-T (OOB) 24x10GBASE-R (SFP+)/1000BASE-X (SFP)
	MES5332A	1x10/100/1000BASE-T (OOB) 32x10GBASE-R (SFP+)/1000BASE-X (SFP)
Пропускная способность	MES5312	240 Гбит/с
	MES5316A	320 Гбит/с
	MES5324A	480 Гбит/с

	MES5332A	640 Гбит/с
Производительность на пакетах длиной 64 байта	MES5312	178 MPPS
	MES5316A	238 MPPS
	MES5324A	
	MES5332A	
Объем буферной памяти	MES5312	2 Мбайт
	MES5316A MES5324A MES5332A	3 Мбайт
Объем ОЗУ (DDR3)	MES5312 MES5316A MES5324A MES5332A	1 Гбайт
Объем ПЗУ (NAND Flash)	MES5312 MES5316A MES5324A MES5332A	1 Гбайт
Таблица MAC-адресов	MES5312 MES5316A MES5324A MES5332A	32K
Объем TCAM	MES5312	Для маршрутизации: 16K IPv4, 8K IPv6 Для обработки трафика: 18K x 10B
	MES5316A MES5324A MES5332A	Для маршрутизации: 16K IPv4, 8K IPv6 Для обработки трафика: 9K x 10B
Количество маршрутов L3 Unicast	MES5312 MES5316A MES5324A MES5332A	16K
Количество ARP-записей	MES5312 MES5316A MES5324A MES5332A	32K[1]
Количество групп L2 Multicast (IGMP snooping)	MES5312 MES5316A MES5324A MES5332A	4K
Количество маршрутов L3 Multicast (IGMP Proxy, PIM)	MES5312 MES5316A MES5324A MES5332A	8K
Скорость передачи данных	MES5312 MES5316A MES5324A MES5332A	Оптические интерфейсы 1/10 Гбит/с Электрические интерфейсы 10/100/1000 Мбит/с

[1] Для каждого хоста в ARP-таблице создается запись в таблице маршрутизации

Поддержка VLAN	MES5312 MES5316A MES5324A MES5332A	Согласно 802.1Q до 4K активных VLAN
Качество обслуживания QoS	MES5312 MES5316A MES5324A MES5332A	8 выходных очередей для каждого порта
Количество VRRP-маршрутизаторов	MES5312 MES5316A MES5324A MES5332A	255
Количество L3 интерфейсов	MES5312 MES5316A MES5324A MES5332A	2048
Количество виртуальных Loopback-интерфейсов	MES5312 MES5316A MES5324A MES5332A	64
Агрегация каналов (LAG)	MES5312 MES5316A MES5324A MES5332A	32 группы, до 8 портов в каждой
Количество экземпляров MSTP	MES5312 MES5316A MES5324A MES5332A	64
Количество DHCP pool	MES5312 MES5316A MES5324A MES5332A	16
Сверхдлинные кадры (jumbo frames)	MES5312 MES5316A MES5324A MES5332A	Максимальный размер пакетов 10K
Стекирование	MES5312 MES5316A MES5324A MES5332A	До 8 устройств
Соответствие стандартам	MES5312 MES5316A MES5324A MES5332A	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

Управление		
Локальное управление		Console
Удаленное управление		SNMP, Telnet, SSH, WEB
Физические характеристики и условия окружающей среды		
Источники питания	MES5312 MES5316A MES5324A MES5332A	сеть переменного тока: 220В+-20%, 50 Гц сеть постоянного тока: 36..72В варианты питания: - один источник питания постоянного или переменного тока; - два источника питания постоянного или переменного тока, с возможностью горячей замены.
Потребляемая мощность	MES5312	не более 40 Вт
	MES5316A	не более 57 Вт
	MES5324A	не более 68 Вт
	MES5332A	не более 75 Вт
Габаритные размеры	MES5312	430x230x44 мм
	MES5316A MES5324A MES5332A	430x275x44 мм
Интервал рабочих температур	MES5312 MES5316A MES5324A MES5332A	от -10 до +45 °С
Интервал температуры хранения	MES5312 MES5316A MES5324A MES5332A	Интервал температуры хранения от -50 до +70 °С **Перед первым включением после хранения при температуре меньшей, чем -20°С, или при большей, чем +50°С, требуется выдержать коммутатор при комнатной температуре не менее четырёх часов.**
Относительная влажность при эксплуатации (без образования конденсата)	MES5312 MES5316A MES5324A MES5332A	не более 80%
Относительная влажность при хранении (без образования конденсата)	MES5312 MES5316A MES5324A MES5332A	от 10% до 95%
Средний срок службы	MES5312 MES5316A MES5324A MES5332A	10 лет

Тип питания устройства определяется при заказе.

2.4 Конструктивное исполнение

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

Ethernet-коммутаторы серий MES5312, MES5316A, MES5324A, MES5332A выполнены в металлическом корпусе с возможностью установки в 19” каркас, высота корпуса 1U.

2.4.1 Внешний вид и описание передней панели устройства

Внешний вид передней панели устройств серий MES5312 показан на рисунке 1.

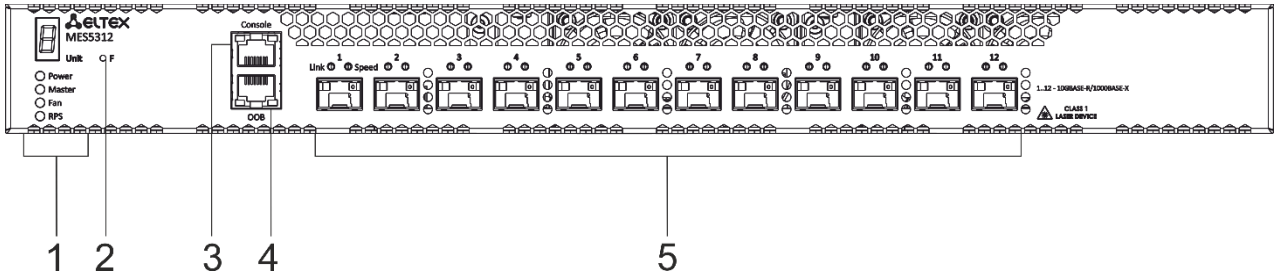


Рисунок 1 – Передняя панель MES5312

Внешний вид передней панели устройств серий MES5316A показан на рисунке 2.

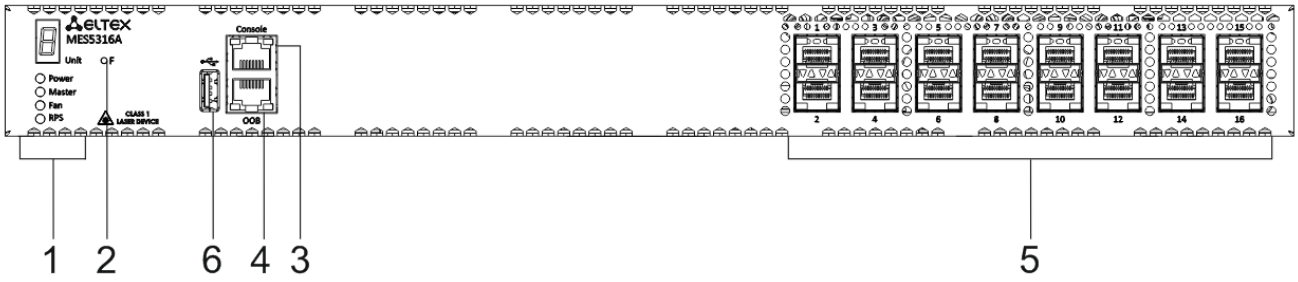


Рисунок 2 – Передняя панель MES5316A

Внешний вид передней панели устройств серий MES5324A показан на рисунке 3.

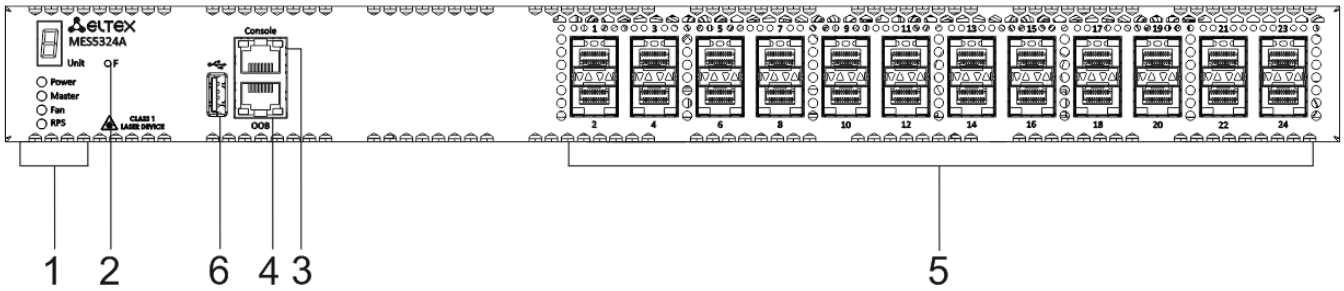


Рисунок 3 – Передняя панель MES5324A

Внешний вид передней панели устройств серий MES5332A показан на рисунке 4.

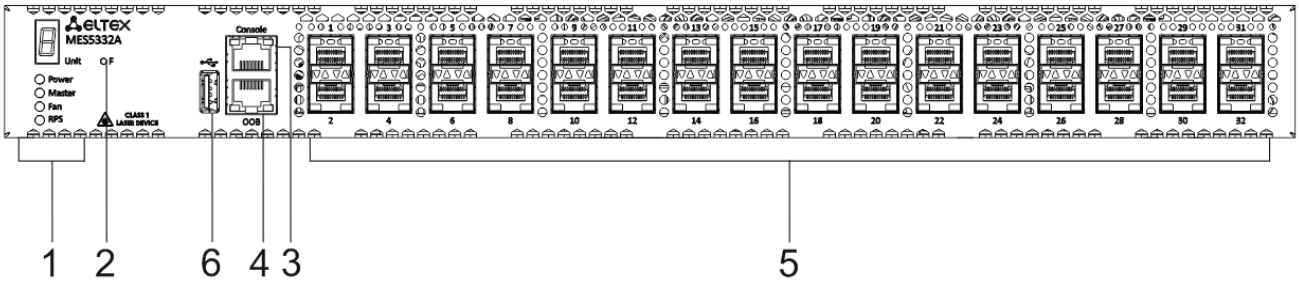


Рисунок 4 – Передняя панель MES5332A

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

Таблица 10 – Описание разъемов, индикаторов и органов управления передней панели MES5312, MES5316A, MES5324A, MES5332A

№	Элемент передней панели		Описание
1	Unit ID		Индикатор номера устройства в стеке.
	Power		Индикатор питания устройства.
	Master		Индикатор режима работы устройства (ведущий/ведомый).
	Fan		Индикатор работы вентиляторов.
	RPS		Индикатор резервного электропитания.
2	F		Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: - при нажатии на кнопку длительностью менее 10 с происходит перезагрузка устройства; - при нажатии на кнопку длительностью более 10 с происходит сброс настроек устройства до заводской конфигурации.
3	Console		Консольный порт для локального управления устройством. Распиновка разъема следующая: 1 не используется 2 не используется 3 RX 4 GND 5 GND 6 TX 7 не используется 8 не используется 9 не используется Распайка консольного кабеля приведена в приложении В
4	OOB		Порт (out-of-band) 10/100/1000BASE-T (RJ-45) для удаленного управления устройством. Управление осуществляется по сети, раздельно с каналом передачи данных.
5	[1-12]	MES5312	Слоты для установки трансиверов 10G SFP+/1G SFP.
	[1-16]	MES5316A	
	[1-24]	MES5324A	
	[1-32]	MES5332A	

6		MES5316A MES5324A MES5332A	USB-порт.

2.4.2 Задняя панель устройства

Внешний вид задней панели коммутаторов MES5312, MES5316A, MES5324A, MES5332A приведен на рисунках 5, 6.

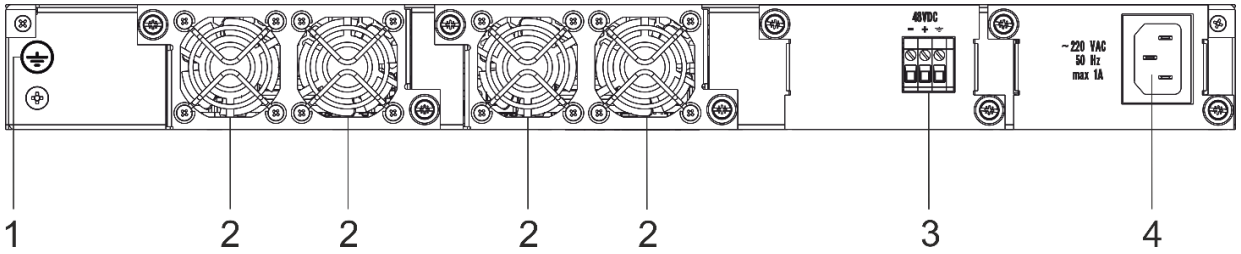


Рисунок 5 – Задняя панель MES5312, MES5324A, MES5332A

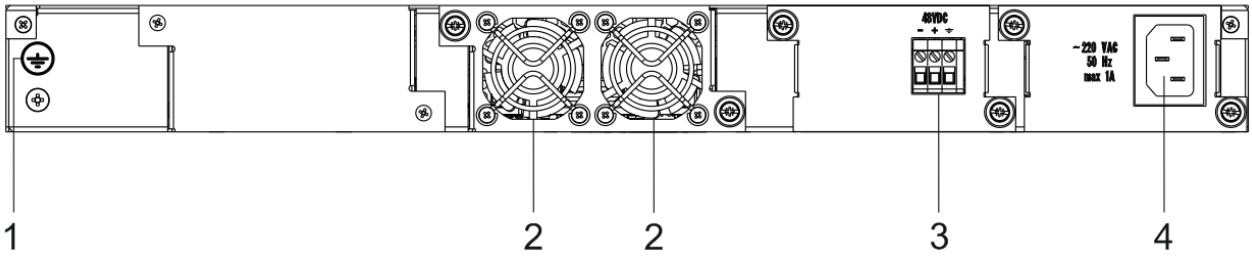


Рисунок 6 – Задняя панель MES5316A

В таблице 11 приведен перечень разъемов, расположенных на задней панели коммутаторов MES5312, MES5316A, MES5324A, MES5332A.

Таблица 11 – Описание разъемов задней панели коммутаторов MES5312, MES5316A, MES5324A, MES5332A

№	Элемент задней панели	Описание
1	Клемма заземления ⏚	Клемма для заземления устройства.
2	Вентиляторы	
3	48VDC	Разъем для подключения к источнику электропитания постоянного тока.
4	~220 VAC 50 Hz max 1A	Разъем для подключения к источнику электропитания переменного тока.

2.4.3 Боковые панели устройства

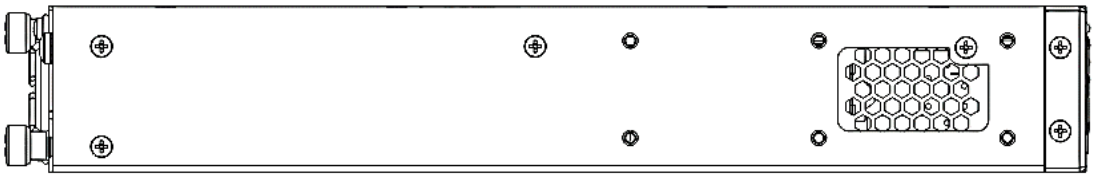


Рисунок 7 – Левая боковая панель Ethernet-коммутаторов MES5316A, MES5324A, MES5332A

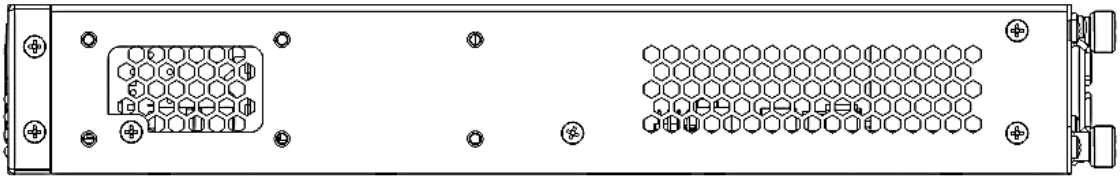


Рисунок 8 – Левая боковая панель Ethernet-коммутаторов MES5316A, MES5324A, MES5332A

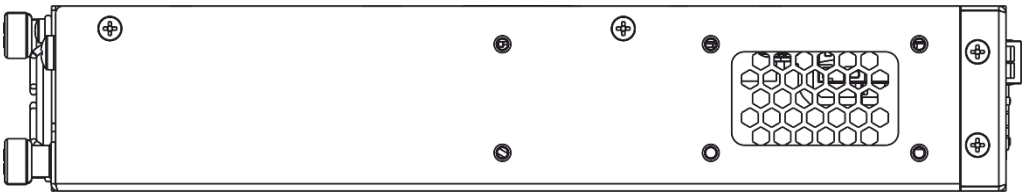


Рисунок 9 – Правая боковая панель Ethernet-коммутатора MES5312

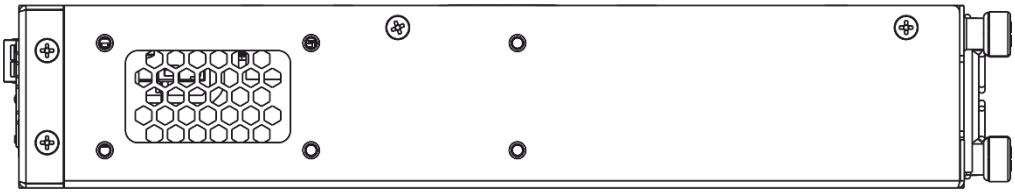


Рисунок 10 – Левая боковая панель Ethernet-коммутатора MES5312

На боковых панелях устройства расположены вентиляционные решетки, которые служат для отвода тепла. Не закрывайте вентиляционные отверстия посторонними предметами. Это может привести к перегреву компонентов устройства и вызвать нарушения в его работе. Рекомендации по установке устройства расположены в разделе «Установка и подключение».

2.4.4 Световая индикация

Состояние интерфейсов Ethernet индицируется двумя светодиодными индикаторами, *LINK/ACT* зеленого цвета и *SPEED* янтарного цвета. Расположение светодиодов показано на рисунках 11, 12.

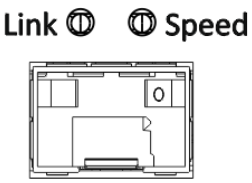


Рисунок 11 – Внешний вид разъема SFP/SFP+

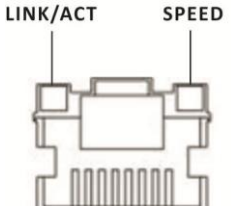


Рисунок 12 – Внешний вид разъема RJ-45

Таблица 12 – Световая индикация состояния XLG-портов

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 1 Гбит/с
Горит постоянно	Горит постоянно	Установлено соединение на скорости 10 Гбит/с
X	Мигание	Идет передача данных

Таблица 13 – Световая индикация состояния Ethernet-портов 10/100/1000BASE-T (OOB)

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

Индикатор *Unit ID* (1-8) служит для обозначения номера устройства в стеке.

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

Таблица 14 – 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
		Оранжевый	Отсутствие первичного питания основного источника (при питании устройства от резервного источника) или авария основного источника
Master	Признак ведущего устройства при работе в стеке	Зеленый, горит постоянно	Устройство является «мастером» стека
		Выключен	Устройство не является «мастером» в стеке или не задан режим стекирования
Fan	Состояние вентилятора охлаждения	Зеленый, горит постоянно	Все вентиляторы исправны
		Красный, горит постоянно	Отказ одного или более вентиляторов

RPS	Режим работы резервного источника питания	Зеленый, горит постоянно	Резервный источник подключен и работает нормально
		Красный, горит постоянно	Отсутствие первичного питания резервного источника или его неисправность.
		Выключен	Резервный источник не подключен

2.5 Комплект поставки

В базовый комплект поставки входят:

- Ethernet-коммутатор;
- Комплект крепежа в стойку;
- Руководство по эксплуатации (поставляется на CD-диске);
- Сертификат соответствия;
- Паспорт.

При наличии, в заказе также могут быть поставлены:

- Модуль питания PM160-220/12 или PM100-48/12 (опционально);
- Шнур питания (в случае комплектации модулем питания PM160-220/12).

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

3 УСТАНОВКА И ПОДКЛЮЧЕНИЕ

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

3.1 Крепление кронштейнов

В комплект поставки устройства входят кронштейны для установки в стойку и винты для крепления кронштейнов к корпусу устройства. На кронштейнах расположены шесть крепежных отверстий для разных вариантов крепления, что позволяет регулировать расстояние между передней панелью и дверцей серверного шкафа (рисунки 13, 14). Для установки кронштейнов выберите один из вариантов крепления:

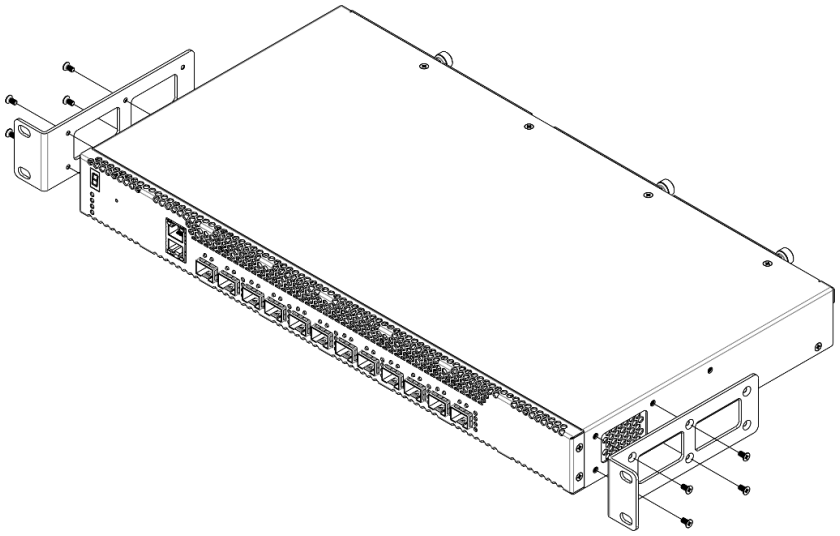


Рисунок 13 – Вариант крепления кронштейнов №1

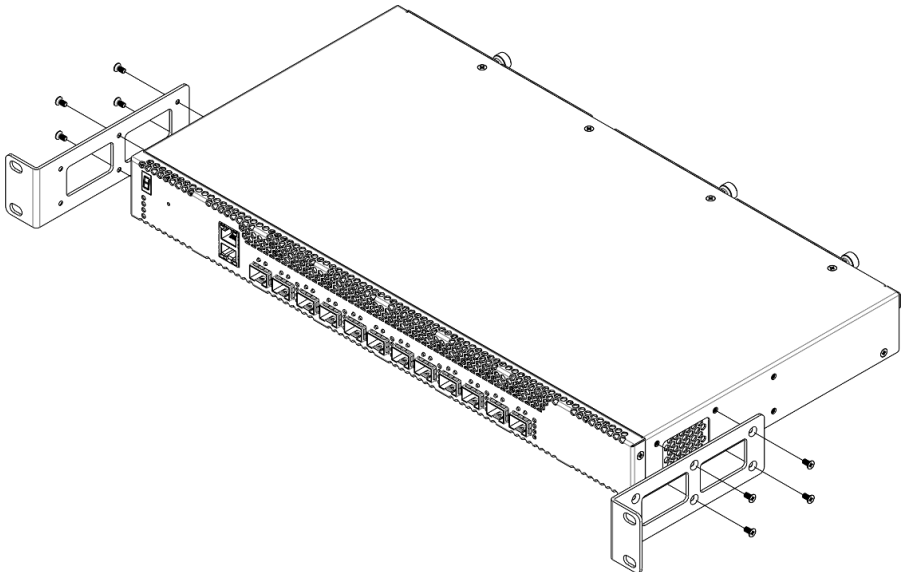


Рисунок 14 – Вариант крепления кронштейнов №2

1. Совместите выбранные четыре отверстия для винтов на кронштейне с такими же отверстиями на боковой панели устройства.

2. С помощью отвертки прикрепите кронштейн винтами к корпусу.
3. Повторите действия 1, 2 для второго кронштейна.

3.2 Установка устройства в стойку

Для установки устройства в стойку:

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

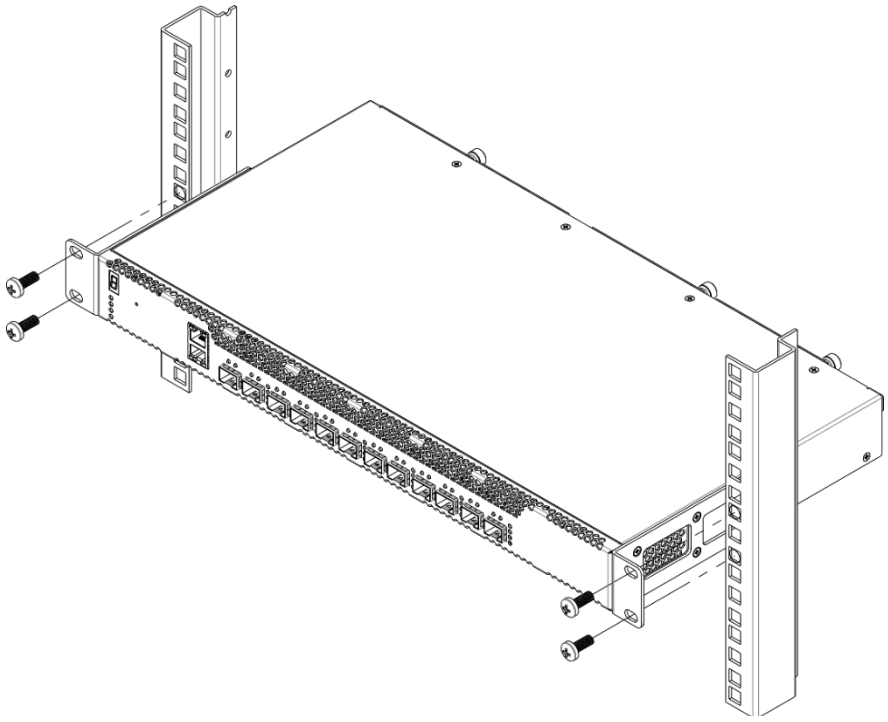


Рисунок 15 – Установка устройства в стойку

На рисунке 16 приведен пример размещения коммутаторов MES5312 в стойке.

Рисунок 16 – Размещение коммутаторов MES5312 в стойке

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

3.3 Установка модулей питания

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

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

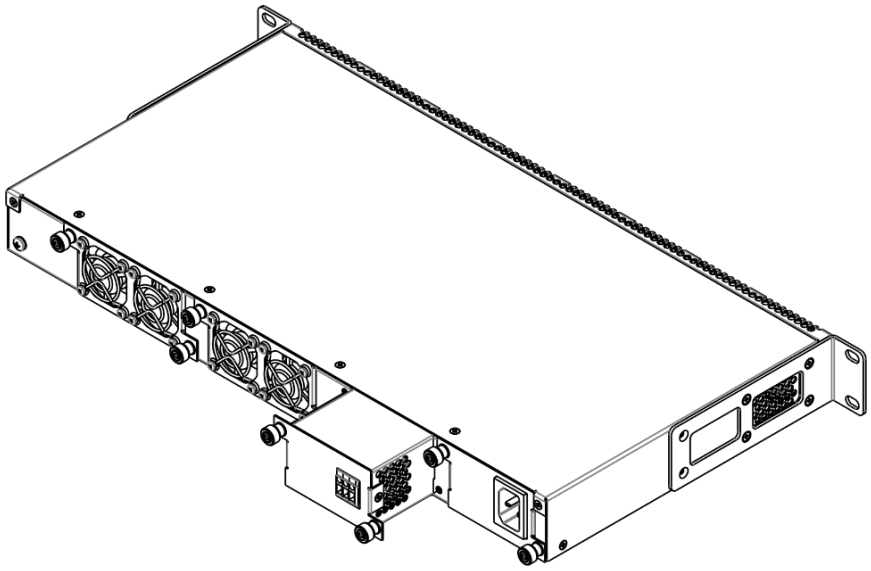


Рисунок 17 – Установка модулей питания

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

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

3.4 Подключение питающей сети

1. Прежде, чем к устройству будет подключена питающая сеть, необходимо заземлить корпус устройства. Заземление необходимо выполнять изолированным многожильным проводом. Устройство заземления и сечение заземляющего провода должны соответствовать требованиями ПУЭ.
2. Если предполагается подключение компьютера или иного оборудования к консольному порту коммутатора, это оборудование также должно быть надежно заземлено.
3. Подключите к устройству кабель питания. В зависимости от комплектации устройства, питание может осуществляться от сети переменного тока, либо от сети постоянного

тока. При подключении сети переменного тока следует использовать кабель, входящий в комплект устройства. Для подключения к сети постоянного тока используйте провод сечением не менее 1 мм^2.

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

3.5 Установка и удаление SFP-трансиверов

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

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

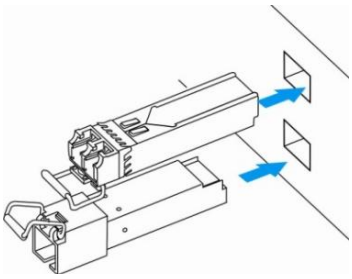


Рисунок 18 – Установка SFP-трансиверов

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

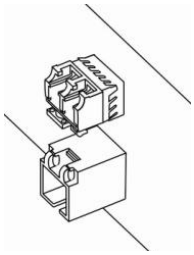


Рисунок 19 – Установленные SFP-трансиверы

Для удаления трансивера:

1. Откройте защелку модуля.

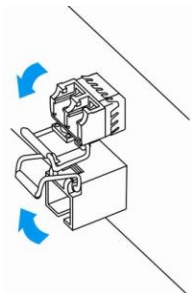


Рисунок 20 – Открытие защелки SFP-трансиверов

2. Извлеките модуль из слота.

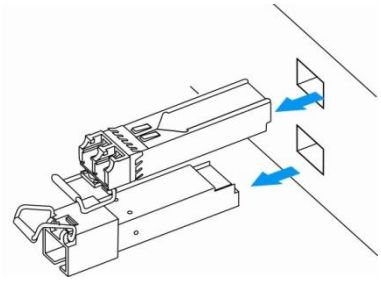


Рисунок 21 – Извлечение SFP-трансиверов

4 НАЧАЛЬНАЯ НАСТРОЙКА КОММУТАТОРА

4.1 Настройка терминала

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

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

4.2 Включение устройства

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

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

Отображение хода выполнения процедуры POST на коммутаторах MES5312:

```
BootROM 1.43
Booting from SPI flash


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


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

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

Running UBOOT...


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

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

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

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

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

```
 >lcli

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



User Name:
Detected speed: 115200


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

console#
```

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

4.3 Загрузочное меню

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

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

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

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

Вид загрузочного меню:

```
      Startup Menu
[1]  Restore Factory Defaults
[2]  Password Recovery Procedure
[3]  Back
 Enter your choice or press 'ESC' to exit:
```

Таблица 15 – Функции интерфейса загрузочного меню

Функция	***Описание***
Restore Factory Defaults	Восстановить заводские настройки
Password Recovery Procedure	Сбросить настройки аутентификации
Back	Продолжить загрузку

4.4 Режим работы коммутатора

Коммутаторы MES5312, MES5316A, MES5324A, MES5332A работают в режиме стекирования.

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

- *Master* (UID устройства 1 или 2), с него происходит управление всеми устройствами в стеке.

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

В режиме стекирования коммутаторы используют XG порты для синхронизации. При этом указанные порты не участвуют в передаче данных. Возможны две топологии синхронизирующихся устройств – кольцевая и линейная. Рекомендуется использовать кольцевую топологию для повышения отказоустойчивости стека.

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

Настройка коммутатора для работы в режиме стекирования

Запрос командной строки имеет следующий вид:

```
console(config)#
```

Таблица 16 – Базовые команды

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

Пример

- Настроить MES5312 для работы в режиме стекирования. Назначить вторым юнитом, использовать интерфейсы te1-2 в качестве стекирующих.

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

Команды режима privileged EXEC

Запрос командной строки имеет следующий вид:

```
console#
```

Таблица 17 – Базовые команды, доступные в режиме EXEC

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

- Пример использования команды **show stack links**:

```
console# show stack links
```

```
Topology is Chain

Unit Id     Active Links        Neighbor Links    Operational     Down/Standby
                                                  Link Speed      Links
------- -------------------- -------------------- ----------- --------------------
1       te1/0/1              te2/0/2              40G         te1/0/2
2       te2/0/2              te1/0/1              40G         te2/0/1
```

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

4.5 Настройка функций коммутатора

Функции по начальному конфигурированию устройства можно разделить на два типа.

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

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

```
console# write
```

4.5.1 Базовая настройка коммутатора

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

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

Базовая настройка включает следующее:

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

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

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

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

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

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

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

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

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

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

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

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

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

  Параметры интерфейса:

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

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

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

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

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

4.5.1.3 Получение IP-адреса от сервера DHCP

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

По умолчанию DHCP-клиент включен на интерфейсе VLAN 1.

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

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

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

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

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

4.5.1.4 Настройка параметров протокола SNMP для доступа к устройству

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

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

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

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

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

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

Для просмотра созданных строк сообщества и настроек SNMP используется команда:

```
console# show snmp
```

```
SNMP is enabled.


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

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

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

Traps are enabled.
Authentication-failure trap is enabled.

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


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

System Contact:
System Location:
```

4.5.2 Настройка параметров системы безопасности

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

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

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

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

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

4.5.2.1 Установка пароля для консоли

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

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

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

4.5.2.2 Установка пароля для Telnet

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

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

4.5.2.3 Установка пароля для SSH

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

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

4.5.3 Настройка баннера

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

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

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

5 УПРАВЛЕНИЕ УСТРОЙСТВОМ. ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ

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

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

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

```
console>
```

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

```
console#
```

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

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

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

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

5.1 Базовые команды

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 18 – Базовые команды, доступные в режиме *EXEC*

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

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

Команды режима privileged EXEC

Запрос командной строки имеет следующий вид:

```
console#
```

Таблица 19 – 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.
debug-mode	-	Перейти в режим отладки.

Команды, доступные во всех режимах конфигурации

Запрос командной строки имеет один из следующих видов:

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

Таблица 20 – Базовые команды, доступные во всех режимах конфигурации

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

Команды режима глобальной конфигурации

Запрос командной строки имеет следующий вид:

```
console(config)#
```

Таблица 21 – Базовые команды, доступные в режиме конфигурации

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

Команды режима конфигурации терминала

Запрос командной строки в режиме конфигурации терминала имеет следующий вид:

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

Таблица 22 – Базовые команды, доступные в режиме конфигурации терминала

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

5.2 Фильтрация сообщений командной строки

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

Таблица 23 – Команды режима глобальной конфигурации

Метод	*Значение/Значение по умолчанию*	*Действие*
begin *pattern*	-	Показывает строки, первые символы которых соответствуют шаблону *pattern*.
include *pattern*		Выводит все строки, содержащие шаблон.
exclude *pattern*		Выводит все строки, не содержащие шаблон.

5.3 Настройка макрокоманд

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 24 – Команды режима глобальной конфигурации

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 25 – Команды режима EXEC

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

Команды режима конфигурации интерфейса

Вид запроса командной строки режима конфигурации интерфейса:

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

Таблица 26 – Команды режима конфигурации интерфейса

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

5.4 Команды управления системой

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 27 – 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*] **[source** *A.B.C.D*]	host: (1..158) символов; size: (64..1518)/64 байт; count: (0..65535)/4; timeout: (50..65535)/2000 мс	Команда служит для передачи запросов (ICMP Echo-Request) протокола ICMP указанному узлу сети, а также для контроля поступающих ответов (ICMP Echo-Reply). - *A.B.C.D* – IPv4-адрес узла сети; - *host* – доменное имя узла сети; - *size* – размер пакета для отправки, количество байт в пакете; - *count* – количество пакетов для передачи; - *timeout* – время ожидания ответа на запрос.
ping ipv6 {*A.B.C.D.E.F* **|** *host*} **[size** *size*] **[count** *count*] **[timeout** *timeout*] **[source** A.B.C.D.E.F]	host: (1..158) символов; size: (68..1518)/68 байт; count: (0..65535)/4; timeout: (50..65535)/2000 мс	Команда служит для передачи запросов (ICMP Echo-Request) протокола ICMP указанному узлу сети, а так же, для контроля поступающих ответов (ICMP Echo-Reply). - *A.B.C.D.E.F* – IPv6-адрес узла сети; - *host* – доменное имя узла сети; - *size* – размер пакета для отправки, количество байт в пакете; - *count* – количество пакетов для передачи; - *timeout* – время ожидания ответа на запрос.
traceroute ip {*A.B.C.D* **|** *host*} **[size** *size*] **[ttl** *ttl*] **[count** *count*] **[timeout** *timeout*] **[source** *ip_address*]	host: (1..158) символов; size: (64..1518)/64 байт; ttl: (1..255)/30; count: (1..10)/3; timeout: (1..60)/3 с;	Определение маршрута трафика до узла назначения. - *A.B.C.D* – IPv4-адрес узла сети. - *host* – доменное имя узла сети; - *size* – размер пакета для отправки, количество байт в пакете; - *ttl* – максимальное количество участков в маршруте; - *count* – количество попыток передачи пакета на каждом участке; - *timeout* – время ожидания ответа на запрос; - *IP_address* – IP-адрес интерфейса коммутатора, используемый для передачи пакетов; **Описание ошибок при выполнении команд и результатов приведено в таблицах 29,30.**
traceroute ipv6 {*A.B.C.D.E.F* **|** *host*} **[size** *size*] **[ttl** *ttl*] **[count** *count*] **[timeout** *timeout*] **[source** *ip_address*]	host: (1..158) символов; size: (66..1518)/66 Байт; ttl: (1..255)/30; count: (1..10)/3; timeout: (1..60) /3 с;	Определение маршрута трафика до узла назначения. - *A.B.C.D.E.F* – IPv6-адрес узла сети. - *host* – доменное имя узла сети; - *size* – размер пакета для отправки, количество байт в пакете; - *ttl* – максимальное количество участков в маршруте; - *count* – количество попыток передачи пакета на каждом участке; - *timeout* – время ожидания ответа на запрос; - *IP_address* – IP-адрес интерфейса коммутатора, используемый для передачи пакетов. **Описание ошибок при выполнении команд и результатов приведено в таблицах 29, 30**.
telnet {*A.B.C.D* **|** *host*} **[***port***]** **[***keyword1***…]**	host: (1..158) символов; port: (1..65535)/23	Открытие TELNET-сессии для узла сети. - *A.B.C.D* – IPv4-адрес узла сети; - *host* – доменное имя узла сети; - *port* – TCP-порт, по которому работает служба Telnet; - *keyword* – ключевое слово. **Описание специальных команд Telnet и ключевых слов приведено в таблицах 31, 32.**

ssh {*A.B.C.D* **|** *host***} [***port***] [***keyword1...***]**	host: (1..158) символов; port: (1..65535)/22;	Открытие SSH-сессии для узла сети. - *A.B.C.D* – IPv4-адрес узла сети; - *host* – доменное имя узла сети; - *port* – TCP-порт, по которому работает служба SSH; - *keyword* – ключевое слово. **Описание ключевых слов приведено в таблице 32**.
resume [*connection***]**	connection: (1..5)/последняя установленная сессия	Переключение на другую установленную TELNET-сессию. - *connection* – номер установленной telnet-сессии.
show users [accounts]	-	Отображение информации о пользователях, использующих ресурсы устройства.
show sessions	-	Отображение информации об открытых сессиях к удаленным устройствам.
show system	-	Вывод системной информации.
show system id [unit *unit***]**	unit: (1..8)/-	Отображение серийного номера устройства. - *unit* – номер устройства в стеке.
show system [unit *unit***]**	unit: (1..8)/-	Отображение системной информации коммутатора. - *unit* – номер устройства в стеке.
show system fans [unit *unit***]**	unit: (1..8)/-	Отображение информации о состоянии вентиляторов. - *unit* – номер устройства в стеке.
show system power-supply	-	Отображение информации о состоянии источников питания.
show system sensors	-	Отображение информации температурных датчиков.
show version	-	Отображение текущей версии системного программного обеспечения устройства.
show hardware version	-	Отображает информацию об аппаратной версии платы
show system router resources		Отображение размера и занятости аппаратных таблиц устройства (маршрутизации, соседей, интерфейсов).
show system tcam utilization [unit *unit***]**	unit: (1..8)/-	Отображение загрузки ресурсов памяти TCAM (определенно адресуемая память). - *unit* – номер устройства в стеке.
show tasks utilization	-	Отображение уровня загрузки ресурсов центрального процессора коммутатора для каждого системного процесса.
show tech-support [config | memory]	-	Отображение информации об устройстве, необходимой для начальной диагностики проблем.

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

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

Команды режима privileged EXEC

Запрос командной строки в режиме privileged EXEC имеет следующий вид:

```
console#
```

Таблица 28 – Команды управления системой в режиме privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
reload [unit *unit_id***]**	unit_id: (1..8)/-	Команда служит для перезапуска устройства. - *unit_id* – номер устройства в стеке.
reload in {*minutes* **|** *hh:mm***}**	minutes: (1..999); hh: (0..23), mm: (0..59).	Установка промежутка времени, через который произойдет отложенная перезагрузка устройства.
reload at *hh:mm*	hh: (0..23), mm: (0..59).	Установка времени перезагрузки устройства.
reload cancel	-	Отмена отложенного перезапуска.
show cpu utilization	-	Отображение статистики по уровню загрузки ресурсов центрального процессора.
show cpu input rate	-	Отображение статистики по скорости входящих фреймов, обрабатываемых процессором.
show cpu input-rate detailed	-	Отображение статистики по скорости входящих фреймов, обрабатываемых процессором по типу трафика.

- Пример использования команды **traceroute**:

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

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

Таблица 29 – Описание результатов выполнения команды traceroute

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

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

Таблица 30 – Ошибки при выполнении команды traceroute

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

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

Таблица 31 – Специальные команды Telnet

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

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

Таблица 32 – Ключевые слова, используемые при открытии Telnet и SSH-сессий

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

Команды режима глобальной конфигурации

Запрос командной строки в режиме глобальной конфигурации имеет следующий вид:

```
console(config)#
```

Таблица 33 – Команды управления системой в режиме глобальной конфигурации

Команда	***Значение/Значение по умолчанию***	***Действие***
hostname *name*	name: (1..160) символов/-	Команда служит для задания сетевого имени устройства.
no hostname		Вернуть сетевое имя устройства в значение по умолчанию.
service tasks-utilization	-/включено	Разрешить устройству программно измерять уровень загрузки ресурсов центрального процессора коммутатора для каждого системного процесса.
no service tasks-utilization		Запретить устройству программно измерять уровень загрузки ресурсов центрального процессора коммутатора для каждого системного процесса.
service cpu-utilization	-/включено	Разрешить устройству программно измерять уровень загрузки ресурсов центрального процессора коммутатора.
no service cpu-utilization		Запретить устройству программно измерять уровень загрузки ресурсов центрального процессора коммутатора.

service cpu-input-rate	-/выключено	Разрешить устройству программно измерять скорость входящих фреймов, обрабатываемых центральным процессором коммутатора.
no service cpu-input-rate		Запретить устройству программно измерять скорость входящих фреймов, обрабатываемых центральным процессором коммутатора.
service cpu-rate-limits *traffic pps*	traffic: (http, telnet, ssh, snmp, ip, link-local, arp, arp-inspection, stp-bpdu, routing, ip-options,other-bpdu, dhcp-snooping, igmp-snooping, mld-snooping, sflow, ace, ip-error, other, vrrp); pps: 8..2048	Установка ограничений скорости входящих фреймов для определенного типа трафика. - *pps* - пакетов в секунду.
no service cpu-rate-limits *traffic*		Восстанавливает значение *pps* по умолчанию для определенного трафика.
service password-recovery	-/enabled	Разрешить восстановление пароля через загрузочное меню «password recovery procedure» с сохранением конфигурации.
no service password-recovery		Разрешить восстановление пароля через загрузочное меню «password recovery procedure» с удалением конфигурации.
link-flap prevention enable	-/enabled	Включить предотвращение флаппинга линка.
link-flap prevention disable		Отключить предотвращение флаппинга линка.
service mirror-configuration	-/enabled	Создавать резервную копию текущей конфигурации.
no service mirror-configuration		Отключить копирование текущей конфигурации.
system router resources [ip-entries *ip_entries* **| ipv6-entries** *ipv6_entries* **| ipm-entries** *ipm_entries* **| ipmv6-entries** *ipmv6_entries* **| policy-ip-entries** *ip_policy_routing_entries* **| policy-ipv6-entries** *ipv6_policy_routing_entries* **| vlan-mapping-entries** *vlan_mapping_entries***]**	ip_entries: (8..8024)/5120; ipv6_entries: (32..8048)/1024; ipm_entries: (8..8024)/512; ipmv6_entries: (32..8048)/512; ip_policy_routing_entries: (0..128)/64; ipv6_policy_routing_entries:(0..128)/64; vlan_mapping_entries: (0..16272)/0	Установка размера таблицы маршрутизации.

5.5 Команды для настройки параметров для задания паролей

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

Команды режима глобальной конфигурации

Запрос командной строки в режиме глобальной конфигурации имеет следующий вид:

```
console(config)#
```

Таблица 34 – Команды управления системой в режиме глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
passwords aging *age*	age: (0..365)/180 дней	Задает время жизни паролей. По истечении заданного срока будет предложено сменить пароль. Значение 0 говорит о том, что время жизни паролей не задано.
no password aging		Восстанавливает значение по умолчанию.
passwords complexity enable	-/выключено	Включает ограничение на формат пароля.
passwords complexity min-classes *value*	value: (0..4)/3	Включает ограничение, задающее минимальное количество классов символов (строчные буквы, заглавные буквы, цифры, символы).
no passwords complexity min-classes		Восстанавливает значение по умолчанию.
passwords complexity min-length *value*	value: (0..64)/8	Включает ограничение на минимальную длину пароля.
no passwords complexity min-length		Восстанавливает значение по умолчанию.
passwords complexity no-repeat *number*	number: (0..16)/3	Включает ограничение, задающее максимальное количество последовательно повторяющихся символов в новом пароле.
no password complexity no-repeat		Восстанавливает значение по умолчанию.
passwords complexity not-current	-/enabled	Запрещает при смене пароля использовать в качестве нового старый.
no passwords complexity not-current		Разрешает использовать старый пароль при смене.
passwords complexity not-username	-/enabled	Запрещает использовать в качестве пароля имя пользователя.
no passwords complexity not-username		Разрешает использовать в качестве пароля имя пользователя.

Таблица 35 – Команды управления системой в режиме Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show passwords configuration	-	Отображает информацию об ограничениях на пароли.

5.6 Работа с файлами

5.6.1 Описание аргументов команд

При осуществлении операций над файлами, в качестве аргументов команд выступают адреса URL – определители местонахождения ресурса. Описание ключевых слов, используемых в операциях, приведено в таблице 36.

Таблица 36 – 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.
mirror-config	Копия файла текущей конфигурации.
startup-config	Файл первоначальной конфигурации.
active-image	Файл с активным образом.
inactive-image	Файл с неактивным образом.

tftp://	Исходный адрес или адрес места назначения для TFTP-сервера. Синтаксис: **tftp://host/[directory/] filename.** - *host* – IPv4-адрес или сетевое имя устройства; - *directory* – каталог; - *filename* – имя файла.
scp://	Исходный адрес или адрес места назначения для SSH-сервера. Синтаксис: **scp://[username[:password]@]host/[directory/] filename** - *username* – имя пользователя; - *password* – пароль пользователя; - *host* – IPv4-адрес или сетевое имя устройства; - *directory* – каталог; - *filename* – имя файла.
logging	Файл с историей команд.

5.6.2 Команды для работы с файлами

Запрос командной строки в режиме Privileged EXEC имеет следующий вид:

```
console#
```

Таблица 37 – Команды для работы с файлами в режиме Privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
copy *source_url destination_url* **[exclude | include-encrypted | include-plaintext]**	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. Следующие опции доступны только при копировании из файла конфигурации: - **exclude** – информация, критичная для безопасности, не будет включена в конечный файл; - **include-encrypted** – информация, критичная для безопасности, будет включена в конечный файл в зашифрованном виде; - **include-plaintext** – информация, критичная для безопасности, будет включена в конечный файл в незашифрованном виде.
copy *source_url* **running-config**		Копирование файла конфигурации с сервера в текущую конфигурацию.
copy running-config *destination_url* **[exclude | include-encrypted | include-plaintext]**		Сохранение текущей конфигурации на сервере. - **exclude** – исключить из копируемых данных информацию о ключах, паролях и т.п; - **include-encrypted** – сохранять данные о ключах, паролях в шифрованном виде; - **include-plaintext** – сохранять данные о ключах, паролях в явном виде.
copy startup-config *destination_url*		Сохранение первоначальной конфигурации на сервере.
copy running-config startup-config	-	Сохранение текущей конфигурации в первоначальную конфигурацию.
copy running-config *file*	-	Сохранение текущей конфигурации в заданный резервный файл конфигурации.
copy startup-config *file*	-	Сохранение первоначальной конфигурации в заданный резервный файл конфигурации.
boot config *source_url*	-	Копирование файла конфигурации с сервера в файл первоначальной конфигурации.
dir [flash:*path* **|** *dir_name***]**	-	Отображает список файлов в указанном каталоге.

more {flash:*file* **| startup-config | running-config | mirror-config | active-image | inactive-image | logging |** *file***}**	file: (1..160) символов	Отображает содержимое файла. - **startup-config** – отображает содержимое файла первоначальной конфигурации; - **running-config** – отображает содержимое файла текущей конфигурации; - **flash:** – отображает файлы с флеш-памяти устройства; - **mirror-config** – отображает содержимое файла текущей конфигурации с зеркала; - **active-image** – отображает версию текущего файла образа ПО. - **inactive-image** – отображает версию неактивного файла образа ПО. - **logging** – отображает содержимое файла журнала. - *file* – имя файла. **Файлы отображаются в формате ASCII.**
delete *url*	-	Удаление файла.
delete startup-config	-	Удаления файла первоначальной конфигурации.
boot system inactive-image	-	Загрузиться с неактивного образа ПО.
show {startup-config | running-config} [brief | detailed | interfaces {tengigabitethernet *te_port* **| oob | port-channel** *group* **| vlan** *vlan_id* **| tunnel** *tunnel_id* **| loopback** *loopback_id***}]**	te_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094); tunnel_id: (1..16); loopback_id: (1..64)	Отображает содержимое файла первоначальной конфигурации (startup-config) или текущей конфигурации (running-config). - **interfaces** – конфигурация интерфейсов коммутатора - физических интерфейсов, групп интерфейсов (port-channel), VLAN-интерфейсов, oob-порта, интерфейса замыкания на себя, тунелей. Следующие опции доступны при выводе текущей конфигурации: - **brief** – вывод конфигурации без двоичных данных, например, SSH и SSL ключей. - **detailed** – вывод конфигурации с включением двоичных данных
show bootvar	-	Показывает активный файл системного ПО, который устройство загружает при запуске.
write [memory]	-	Сохранение текущей конфигурации в файл первоначальной конфигурации.
rename *url new_url*	url, new_url: (1..160) символов	Изменение имени файла. - *url* – текущее имя файла; - *new-url* – новое имя файла.

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

Примеры использования команд

- Удалить файл *test* из энергонезависимой памяти:

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

Результат выполнения команды: после подтверждения файл будет удален.

5.6.3 Команды для автоматического обновления и конфигурации

Процесс автоматического обновления

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

Процесс автоматического обновления состоит из следующих этапов:

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

Процесс автоматического конфигурирования

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

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

Полученный файл конфигурации добавляется к текущей (running) конфигурации.

Команды режима глобальной конфигурации

Запрос командной строки в режиме глобальной конфигурации имеет следующий вид:

```
console(config)#
```

Таблица 38 – Команды управления системой в режиме глобальной конфигурации

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

Команды режима privileged EXEC

Запрос командной строки в режиме privileged EXEC имеет следующий вид:

```
console#
```

Таблица 39 – Команды управления системой в режиме privileged EXEC

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

- Пример конфигурации ISC DHCP Server:

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

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

5.7 Настройка системного времени

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

Команды режима Privileged EXEC

Запрос командной строки в режиме Privileged EXEC имеет следующий вид:

```
console#
```

Таблица 40 – Команды настройки системного времени в режиме Privileged EXEC

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

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 41 – Команды настройки системного времени в режиме «EXEC»

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

Команды режима глобальной конфигурации

Запрос командной строки в режиме глобальной конфигурации имеет следующий вид:

```
console(config)#
```

Таблица 42 – Список команд для настройки системного времени в режиме глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
clock source {sntp | browser}	-/внешний источник не используется	Использование внешнего источника для установки системного времени.
no clock source {sntp | browser}		Запрещает использование внешнего источника для установки системного времени.
clock timezone *zone hours_offset* **[minutes** *minutes_offset***]**	zone: (1..4) символов/ нет описания зоны; hours_offset: (-12..+13)/0; minutes_offset: (0..59)/0;	Устанавливает значение часового пояса. - *zone* – слово, сформированное из первых букв словосочетания, которое оно заменяет (описание зоны); - *hours-offset* – часовое смещение относительно нулевого меридиана UTC; - *minutes-offset* – минутное смещение относительно нулевого меридиана UTC.
no clock timezone		Устанавливает значение по умолчанию.
clock summer-time *zone* **date** *date month year hh:mm date month year hh:mm* **[***offset***]**	zone: (1..4) символа/ нет описания зоны; date: (1..31); month: (Jan..Dec); year: (2000 ..2037); hh: (0..23); mm: (0..59); week: (1-5); day: (sun..sat); offset: (1..1440)/60 мин; По умолчанию переход на летнее время выключен	Задает дату и время для автоматического перехода на летнее время и возврата обратно (для определенного года). Первым в команде указывается описание зоны, вторым время для перехода на летнее время и третьим время для возврата. - *zone* – слово, сформированное из первых букв словосочетания, которое оно заменяет (описание зоны); - *date* – число; - *month* – месяц; - *year* – год; - *hh* – часы, *mm* – минуты; - *offset* – количество минут, добавляемых при переходе на летнее время.
clock summer-time *zone* **date** *month date year hh:mm month date year hh:mm* **[***offset***]**		
clock summer-time *zone* **recurring {usa | eu | {first | last |** *week***}** *day month hh:mm* **{first | last |** *week***}** *day month hh:mm***} [***offset***]**		Задает дату и время для автоматического перехода на летнее время и возврата обратно в режиме ежегодно. - *zone* – слово, сформированное из первых букв словосочетания, которое оно заменяет (описание зоны); - **usa** – установить правила перехода на летнее время, используемые в США (переход во второе воскресенье марта, обратно в первое воскресенье ноября, в 2 часа утра по местному времени); - **eu** – установить правила перехода на летнее время, используемые Евросоюзом (переход в последнее воскресенье марта, обратно в последнее воскресенье октября, в 1 час утра по Гринвичу); - *hh* – часы, *mm* – минуты; - *week* – неделя месяца; - *day* – день недели; - *month* – месяц; - *offset* – количество добавляемых минут при переходе на летнее время.
no clock summer-time		Отключает автоматический переход на летнее время.
sntp authentication-key *number* **md5** *value*	number: (1..4294967295); value: (1..32) символов; По умолчанию проверка подлинности отключена	Устанавливает ключ проверки подлинности для протокола SNTP. - *number* – номер ключа; - *value* – значение ключа; - encrypted – задать значение ключа в зашифрованном виде.
encrypted sntp authentication-key *number* **md5** *value*		
no sntp authentication-key *number*		Удаляет ключ проверки подлинности для протокола SNTP.
sntp authenticate	-/проверка подлинности не требуется	Требует проверку подлинности для получения информации от NTP-серверов.
no sntp authenticate		Устанавливает значение по умолчанию.

sntp trusted-key *key_number*	key_number: (1..4294967295); По умолчанию проверка подлинности отключена	Осуществляет проверку подлинности системы, от которой синхронизируется с помощью SNTP по заданному ключу. - *key_number* – номер ключа.
no sntp trusted-key *key_number*		Устанавливает значение по умолчанию.
sntp broadcast client enable {both | ipv4 | ipv6}	-/запрещено	Разрешает работу широковещательных SNTP-клиентов.
no sntp broadcast client enable		Устанавливает значение по умолчанию.
sntp anycast client enable {both | ipv4 | ipv6}	-/запрещено	Разрешает работу SNTP-клиентам, поддерживающим метод рассылки пакетов, позволяющий посылать данные ближайшему устройству из группы получателей.
no sntp anycast client enable		Устанавливает значение по умолчанию.
sntp client poll timer *seconds*	seconds: (60…86400)/24	Устанавливает время опроса для SNTP-сервера.
no sntp client poll timer		Устанавливает значение по умолчанию.
sntp client enable {tengigabitethernet *te_port* **| port-channel** *group* **| oob | vlan** *vlan_id***}**	te_port: (1..32); group: (1..32); vlan_id (1..4094) /запрещено	Разрешает работу SNTP-клиентам, поддерживающим метод рассылки пакетов, позволяющий посылать данные ближайшему устройству из группы получателей, а также широковещательным SNTP-клиентам для выбранного интерфейса. - подробное описание интерфейсов изложено в разделе «Конфигурация интерфейсов».
no sntp client enable {tengigabitethernet *te_port* **| port-channel** *group* **| oob | vlan** *vlan_id***}**		Устанавливает значение по умолчанию.
sntp unicast client enable	-/запрещено	Разрешает работу одноадресных SNTP-клиентов.
no sntp unicast client enable		Устанавливает значение по умолчанию.
sntp unicast client poll	-/запрещено	Разрешает последовательный опрос заданных одноадресных SNTP-серверов.
no sntp unicast client poll		Устанавливает значение по умолчанию.
sntp server {*ipv4_address* **|** *ipv6_address* **|** *ipv6_link_local_address%***{***vlan {integer}* **|** *ch {integer}* **|** *isatap {integer}* **|** *{physical_port_name}***} |** *hostname***} [poll] [key** *keyid***]**	hostname: (1..158) символов; keyid: (1..4294967295)	Задает адрес SNTP-сервера. - *ipv4_address* – IPv4-адрес узла сети; - *ipv6_address* – IPv6-адрес узла сети; - *ipv6z-address* – IPv6z-адрес узла сети для ping. Формат адреса *ipv6_link_local_address%interface_name*: *ipv6_link_local_address* – локальный IPv6 адрес канала; *interface_name* – имя исходящего интерфейса задается в следующем формате: *vlan {integer}* **|** *ch {integer}* **|** *isatap {integer}* **|** *{physical_port_name}* - *hostname* – доменное имя узла сети; - poll – включает опрос; - *keyid* – идентификатор ключа.
no sntp server {*ipv4_address* **|** *ipv6_address* **|** *ipv6_link_local_address%***{***vlan {integer}* **|** *ch {integer}* **|** *isatap {integer}* **|** *{physical_port_name}***} |** *hostname***}**		Удаление сервера из списка NTP-серверов.
clock dhcp timezone	-/запрещено	Разрешает получение таких данных как часовой пояс и летнее время от DHCP-сервера.
no clock dhcp timezone		Запрещает получения таких данных как часовой пояс и летнее время от DHCP-сервера.

Команды режима конфигурации интерфейса

Запрос командной строки в режиме конфигурации интерфейса имеет следующий вид:

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

Таблица 43 – Список команд для настройки системного времени в режиме конфигурации интерфейса

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

Примеры выполнения команд

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

```
console# show clock detail
```

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

Time zone:
Acronym is PST
Offset is UTC-8

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

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

Пример:

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

Используются следующие обозначения:

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

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

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

- Отобразить статус протокола SNTP:

```
console# show sntp status
```

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

Unicast servers:

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


Anycast server:


Broadcast:
```

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

5.8 Конфигурация временных интервалов time-range

Команды режима конфигурации временных интервалов

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

range_name – символьный (1...32) идентификатор временного интервала

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

Таблица 44 – Команды режима конфигурации временного интервала

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

5.9 Конфигурация интерфейсов и VLAN

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

Команды режима конфигурации интерфейса (диапазона интерфейсов)

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

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

Выбор интерфейса осуществляется при помощи команд:

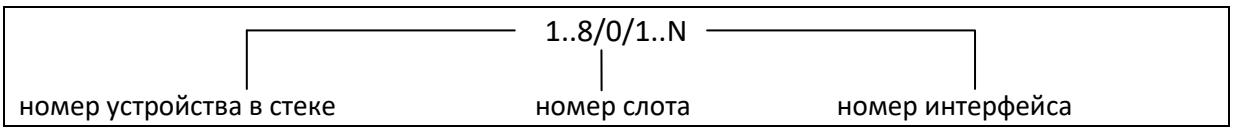
Таблица 45 – Команды выбора интерфейса для коммутаторов

Команда	*Назначение*
interface tengigabitethernet *te_port*	для настройки 10G-интерфейсов
interface port-channel *group*	для настройки групп каналов
interface oob	для настройки интерфейса управления (интерфейс управления присутствует не на всех коммутаторах)
interface loopback *loopback_id*	для настройки виртуальных интерфейсов

где:

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

Запись интерфейса



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

Ниже приведены команды для входа в режим настройки десятого Ethernet-интерфейса (для MES5312) первого устройства в стеке и входа в режим настройки группы каналов 1.

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

Выбор диапазона интерфейсов осуществляется при помощи команд:

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

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

Ниже приведены команды для входа в режим настройки диапазона Ethernet интерфейсов с 1 по 10 (для MES5312) и для входа в режим настройки всех групп портов.

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

console# configure
console(config)# interface range port-channel 1-32
console(config-if)#
```

Таблица 46 – 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, 10000)	Задать скорость передачи данных (Ethernet).
no speed		Установить значение по умолчанию.
duplex *mode*	mode: (full, half)/full	Задать режим дуплекса интерфейса (полнодуплексное соединение, полудуплексное соединение, Ethernet).
no duplex		Установить значение по умолчанию.
negotiation *[cap1 [cap2…cap5]]*	cap: (10f, 10h, 100f, 100h, 1000f, 10000f)	Включает автосогласование для скорости и дуплекса на настраиваемом интерфейсе. Можно указать определенные совместимости параметра автосогласования, если параметры не заданы, то поддерживаются все совместимости (Ethernet, port-channel).
no negotiation		Выключает автосогласование для скорости и дуплекса на настраиваемом интерфейсе.
flowcontrol *mode*	mode: (on, off, auto)/off	Задать режим управления потоком flowcontrol (включить, отключить или автосогласование). Автосогласование flowcontrol работает только в случае, если режим автосогласования negotiation включен на настраиваемом интерфейсе (Ethernet, port-channel).
no flowcontrol		Отключить режим управления потоком.
back-pressure	-/выключен	Включает функцию «обратного давления» на настраиваемом интерфейсе (Ethernet).
no back-pressure		Выключает функцию «обратного давления» на настраиваемом интерфейсе.
load-average *period*	period: (5..300)/15	Установить период, в течение которого собирается статистика о нагрузке на интерфейсе.
no load-average		Установить значение по умолчанию.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 47 – Команды режима общих настроек интерфейса Ethernet и Port-Channel

Команда	*Значение/Значение по умолчанию*	*Действие*
port jumbo-frame	-/запрещено	Разрешает коммутатору работать с фреймами большого размера. **Значение maximum transmission unit (MTU) по умолчанию 1500 байт.** **Настройка вступит в силу только после перезагрузки устройства.** **Значение maximum transmission unit (MTU) при настройке port jumbo-frame 10200 байт.**
no port jumbo-frame		Запрещает коммутатору работать с фреймами большого размера.
errdisable recovery cause {all | loopack-detection | port-security | dot1x-src-address | acl-deny | stp-bpdu-guard | stp-loopback-guard | udld | storm-control | link-flapping}	-/запрещено	Включить автоматическую активацию интерфейса после его отключения в следующих случаях: - **loopback-detection** — обнаружение петель; - **port-security** — нарушение безопасности для port security; - **dot1x-src-address** —непрохождение аутентификации, основанной на MAC-адресах пользователей; - **acl-deny** —несоответствие спискам доступа (ACL); - **stp-bpdu-guard** — активация защиты BPDU Guard (передача несанкционированного пакета BPDU через интерфейс); - **stp-loopback-guard** — обнаружение петель протоколом STP; - **udld** - активация защиты UDLD; - **storm-control –**широковещательный шторм; - **link-flapping –**флаппинга линка.
no errdisable recovery cause {all | loopack-detection | port-security | dot1x-src-address | acl-deny | stp-bpdu-guard | stp-loopback-guard | udld | storm-control | link-flapping}		Установить значение по умолчанию.
errdisable recovery interval *seconds*	seconds: (30..86400)/300 секунд	Установить временной интервал для автоматического повторного включения интерфейса.
no errdisable recovery interval		Установить значение по умолчанию.
snmp trap link-status	-/включено	Включает отправку SNMP trap-сообщений о состоянии интерфейсных линков.
no snmp trap link-status		Отключает отправку SNMP trap-сообщений.

Команды режима EXEC

Вид запроса командной строки в режиме EXEC:

```
console#
```

Таблица 48 – Команды режима EXEC

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

clear counters {oob | tengigabitethernet *te_port* **| port-channel** *group*	te_port: (1..8/0/1..32); group: (1..32)	Сброс статистики для интерфейса.
set interface active { tengigabitethernet *te_port* **| port-channel** *group*}	te_port: (1..8/0/1..32); group: (1..32)	Активирует порт или группу портов, выключенных командой **shutdown**.
show interfaces configuration {oob | tengigabitethernet *te_port* **| port-channel** *group* **| detailed}**	te_port: (1..8/0/1..32); group: (1..32)	Показать конфигурацию интерфейсов.
show interfaces status	-	Показать состояние всех интерфейсов.
show interfaces status {oob | tengigabitethernet *te_port* **| port-channel** *group* **| detailed}**	te_port: (1..8/0/1..32); group: (1..32)	Показать состояние Ethernet-порта, группы портов.
show interfaces advertise	-	Показать параметры автосогласования, объявленные для всех интерфейсов.
show interfaces advertise {oob | tengigabitethernet *te_port* **| port-channel** *group* **| detailed}**	te_port: (1..8/0/1..32); group: (1..32)	Показать параметры автосогласования, объявленные для Ethernet-порта, группы портов.
show interfaces description	-	Показать описания всех интерфейсов.
show interfaces description {oob | tengigabitethernet *te_port* **| port-channel** *group* **| detailed}**	te_port: (1..8/0/1..32); group: (1..32)	Показать описание Ethernet-порта, группы портов.
show interfaces counters	-	Показать статистику для всех интерфейсов.
show interfaces counters {oob | tengigabitethernet *te_port* **| port-channel** *group* **| detailed}**	te_port: (1..8/0/1..32); group: (1..32)	Показать статистику для интерфейса.
show interfaces utilization	-	Показать статистику по нагрузке для всех интерфейсов.
show interfaces utilization {tengigabitethernet *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Показать статистику по нагрузке для Ethernet-интерфейса.
show ports jumbo-frame	-	Показать настройку jumbo-frames в коммутаторе.
show errdisable recovery	-	Показать настройки для автоматической повторной активации порта.
show errdisable interfaces { tengigabitethernet *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Показать причину отключения порта, группы портов и состояние автоматической активации.

Примеры выполнения команд.

- Показать состояние интерфейсов:

```
console# show interfaces status
```

```
                                                Flow Link          Back   Mdix
Port     Type         Duplex  Speed Neg      ctrl State       Pressure Mode    Port Mode
-------- ------------ ------  ----- -------- ---- ----------- -------- ------- --------------------
----
te1/0/3  10G-Fiber    Full    1000  Disabled Off  Up          Disabled Off     Access
te1/0/4  10G-Fiber      --      --      --     --  Down           --     --     Access
te1/0/5  10G-Fiber      --      --      --     --  Down           --     --     Access
te1/0/6  10G-Fiber      --      --      --     --  Down           --     --     Access
te1/0/7  10G-Fiber      --      --      --     --  Down           --     --     Access
te1/0/8  10G-Fiber      --      --      --     --  Down           --     --     Access
te1/0/9  10G-Fiber      --      --      --     --  Down           --     --     Access
te1/0/10 10G-Fiber      --      --      --     --  Down           --     --     Access
te1/0/11 10G-Fiber      --      --      --     --  Down           --     --     Access
te1/0/12 10G-Fiber      --      --      --     --  Down           --     --     Access
```

```
                                          Flow    Link
Ch       Type    Duplex  Speed  Neg      control  State
-------- ------- ------  -----  -------- -------  -----------
Po1         --     --      --      --       --    Not Present
Po2         --     --      --      --       --    Not Present
Po3         --     --      --      --       --    Not Present
Po4         --     --      --      --       --    Not Present
Po5         --     --      --      --       --    Not Present
Po6         --     --      --      --       --    Not Present
Po7         --     --      --      --       --    Not Present
Po8         --     --      --      --       --    Not Present
Po9         --     --      --      --       --    Not Present
Po10        --     --      --      --       --    Not Present
Po11        --     --      --      --       --    Not Present
Po12        --     --      --      --       --    Not Present
Po13        --     --      --      --       --    Not Present
Po14        --     --      --      --       --    Not Present
Po15        --     --      --      --       --    Not Present
Po16        --     --      --      --       --    Not Present
Po17        --     --      --      --       --    Not Present
Po18        --     --      --      --       --    Not Present
Po19        --     --      --      --       --    Not Present
Po20        --     --      --      --       --    Not Present
Po21        --     --      --      --       --    Not Present
Po22        --     --      --      --       --    Not Present
Po23        --     --      --      --       --    Not Present
Po24        --     --      --      --       --    Not Present
Po25        --     --      --      --       --    Not Present
Po26        --     --      --      --       --    Not Present
Po27        --     --      --      --       --    Not Present
Po28        --     --      --      --       --    Not Present
Po29        --     --      --      --       --    Not Present
Po30        --     --      --      --       --    Not Present
Po31        --     --      --      --       --    Not Present
Po32        --     --      --      --       --    Not Present

                                                  Link
Oob       Type          Duplex  Speed Neg      State
--------  ------------ ------  ----- -------- -----------
oob       1G-Copper       --     --     --    Down
```

Показать параметры авто-согласования:

```
console# show interfaces advertise
```

```
Port       Type          Neg      Preferred   Operational Link Advertisement
---------- ------------ -------- ----------  -------------------------------------
te1/0/3    10G-Fiber    Disabled   --                          --
te1/0/4    10G-Fiber    Disabled   --                          --
te1/0/5    10G-Fiber    Disabled   --                          --
te1/0/6    10G-Fiber    Disabled   --                          --
te1/0/7    10G-Fiber    Disabled   --                          --
te1/0/8    10G-Fiber    Disabled   --                          --
te1/0/9    10G-Fiber    Disabled   --                          --
te1/0/10   10G-Fiber    Disabled   --                          --
te1/0/11   10G-Fiber    Disabled   --                          --
te1/0/12   10G-Fiber    Disabled   --                          --

Ch         Type          Neg      Preferred   Operational Link Advertisement
---------- ------------ -------- ----------  -------------------------------------
Po1        Unknown      Enabled  Slave                       --
Po2        Unknown      Enabled  Slave                       --
Po3        Unknown      Enabled  Slave                       --
Po4        Unknown      Enabled  Slave                       --
Po5        Unknown      Enabled  Slave                       --
Po6        Unknown      Enabled  Slave                       --
Po7        Unknown      Enabled  Slave                       --
Po8        Unknown      Enabled  Slave                       --
Po9        Unknown      Enabled  Slave                       --
Po10       Unknown      Enabled  Slave                       --
Po11       Unknown      Enabled  Slave                       --
Po12       Unknown      Enabled  Slave                       --
Po13       Unknown      Enabled  Slave                       --
Po14       Unknown      Enabled  Slave                       --
Po15       Unknown      Enabled  Slave                       --
Po16       Unknown      Enabled  Slave                       --
```

```
Po17       Unknown       Enabled  Slave                          --
Po18       Unknown       Enabled  Slave                          --
Po19       Unknown       Enabled  Slave                          --
Po20       Unknown       Enabled  Slave                          --
Po21       Unknown       Enabled  Slave                          --
Po22       Unknown       Enabled  Slave                          --
Po23       Unknown       Enabled  Slave                          --
Po24       Unknown       Enabled  Slave                          --
Po25       Unknown       Enabled  Slave                          --
Po26       Unknown       Enabled  Slave                          --
Po27       Unknown       Enabled  Slave                          --
Po28       Unknown       Enabled  Slave                          --
Po29       Unknown       Enabled  Slave                          --
Po30       Unknown       Enabled  Slave                          --
Po31       Unknown       Enabled  Slave                          --
Po32       Unknown       Enabled  Slave                          --

Oob        Type          Neg      Operational Link Advertisement
---------- ------------- -------- ---------------------------------
```

- oob 1G- Enabled --

Показать статистику по интерфейсам:

```
console# show interfaces counters
```

```
  Port       InUcastPkts  InMcastPkts  InBcastPkts    InOctets
---------------- ------------ ------------ ------------ ------------
    te1/0/1            0            0            0            0
    te1/0/2            0            0            0            0
.....................................................................

    te1/0/5            0            0            0            0
    te1/0/6            0            2            0         2176
    te1/0/7            0            1            0         4160
    te1/0/8            0            0            0            0
.....................................................................

      Port       OutUcastPkts OutMcastPkts OutBcastPkts  OutOctets
---------------- ------------ ------------ ------------ ------------
    te1/0/1            0            0            0            0
    te1/0/2            0            0            0            0
    te1/0/3            0            0            0            0
    te1/0/4            0            0            0            0
    te1/0/5            0            0            0            0
    te1/0/6            0          545           83        62186
    te1/0/7            0         1424          216       164048
    te1/0/8            0            0            0            0
    te1/0/9            0            0            0            0
.....................................................................


      OOB        InUcastPkts  InMcastPkts  InBcastPkts    InOctets
---------------- ------------ ------------ ------------ ------------
      oob              0           13            0          1390

      OOB        OutUcastPkts OutMcastPkts OutBcastPkts  OutOctets
---------------- ------------ ------------ ------------ ------------
      oob              3          616            0         39616
```

- Показать статистику по группе каналов 1:

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

```
       Ch         InUcastPkts  InMcastPkts  InBcastPkts    InOctets
---------------- ------------ ------------ ------------ ------------
      Po1             111          0            0          9007
```

```
       Ch         OutUcastPkts OutMcastPkts OutBcastPkts  OutOctets
---------------- ------------ ------------ ------------ ------------
      Po1              0            6            3           912

Alignment Errors: 0
FCS Errors: 0
Single Collision Frames: 0
Multiple Collision Frames: 0
SQE Test Errors: 0
Deferred Transmissions: 0
Late Collisions: 0
Excessive Collisions: 0
Carrier Sense Errors: 0
Oversize Packets: 0
Internal MAC Rx Errors: 0
Symbol Errors: 0
Received Pause Frames: 0
Transmitted Pause Frames: 0
```

- Показать настройку jumbo-frames в коммутаторе:

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

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

Таблица 49 – Описание счетчиков

Счетчик	***Описание***
InOctets	Количество принятых байтов.
InUcastPkts	Количество принятых одноадресных пакетов.
InMcastPkts	Количество принятых многоадресных пакетов.
InBcastPkts	Количество принятых широковещательных пакетов.
OutOctets	Количество переданных байтов.
OutUcastPkts	Количество переданных одноадресных пакетов.
OutMcastPkts	Количество переданных многоадресных пакетов.
OutBcastPkts	Количество переданных широковещательных пакетов.
Alignment Errors	Количество принятых фреймов с нарушенной целостностью (с количеством байт не соответствующим длине) и не прошедших проверку контрольной суммы (FCS).
FCS Errors	Количество принятых фреймов с количеством байт, соответствующим длине, но не прошедших проверку контрольной суммы (FCS).
Single Collision Frames	Количество фреймов, вовлеченных в единичную коллизию, но впоследствии переданных успешно.
Multiple Collision Frames	Количество фреймов, вовлеченных более чем в одну коллизию, но впоследствии переданных успешно.
Deferred Transmissions	Количество фреймов, для которых первая попытка передачи отложена из-за занятости среды передачи.
Late Collisions	Количество случаев, когда коллизия зафиксирована после того, как в канал связи уже были переданы первые 64 байт (slotTime) пакета.
Excessive Collisions	Количество фреймов, которые не были переданы из-за избыточного количества коллизий.
Carrier Sense Errors	Количество случаев, когда состояние контроля несущей было потеряно, либо не утверждено при попытке передачи фрейма.
Oversize Packets	Количество принятых пакетов, размер которых превышает максимальный разрешенный размер фрейма.

Internal MAC Rx Errors	Количество фреймов, которые не были приняты успешно из-за внутренней ошибки приема на уровне MAC.
Symbol Errors	Для интерфейса, работающего в режиме 100Мб/с – количество случаев, когда имелся недопустимый символ данных, в то время как правильная несущая была представлена. Для интерфейса, работающего в полудуплексном режиме 1000Мб/с – количество случаев, когда средства приема заняты в течение времени, равному или большему чем размер слота (slotTime), и в течение которого имелось хотя бы одно событие, которое заставляет PHY выдавать ошибку приема данных (Data reception error) или ошибку несущей (Carrier extend error) на GMII. Для интерфейса, работающего в полном дуплексном режиме 1000Мб/с – количество случаев, когда средства приема заняты в течение времени, равному или большему чем минимальный размер фрейма (minFrameSize), и в течение которого имелось хотя бы одно событие, которое заставляет PHY выдавать ошибку приема данных (Data reception error) на GMII.
Received Pause Frames	Количество принятых управляющих MAC-фреймов с кодом операции PAUSE.
Transmitted Pause Frames	Количество переданных управляющих MAC-фреймов с кодом операции PAUSE.

5.9.2 Настройка VLAN и режимов коммутации интерфейсов

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 50 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
vlan database	-	Перейти в режим конфигурации VLAN
vlan prohibit-internal-usage {add *VLANlist* **| remove** *VLANlist* **| except** *VLANlist* **| none}**	VLANlist: (2..4094)	- **add** – добавить указанные VLAN ID в перечень запрещенных для внутреннего использования; **- remove –** удалить указанные VLAN ID из перечня запрещенных для внутреннего использования; - **except** – добавить в перечень запрещенных для внутреннего использования все VLAN ID, за исключением указанных в качестве параметра; - **none** – очистить перечень VLAN ID, запрещенных для внутреннего использования.

Команды режима конфигурации VLAN

Вид запроса командной строки в режиме конфигурации VLAN:

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

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

Таблица 51 – Команды режима конфигурации VLAN

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

Команды режима конфигурации интерфейса (диапазона интерфейсов) VLAN

Вид запроса командной строки в режиме конфигурации интерфейса VLAN:

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

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

Выбор интерфейса осуществляется при помощи команды:

```
interface vlan vlan_id
```

Выбор диапазона интерфейсов осуществляется при помощи команды:

```
interface range vlan VLANlist
```

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

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

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

Таблица 52 – Команды режима конфигурации интерфейса VLAN

Команда	*Значение/Значение по умолчанию*	*Действие*
name *name*	name: (1..32)	Добавить имя VLAN.

no name	символов/имя соответствует номеру VLAN	Установить значение по умолчанию.

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

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

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

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

Порт может работать в четырех режимах:

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

Таблица 53 – Команды режима конфигурации интерфейса Ethernet

Команда	***Значение/Значение по умолчанию***	***Действие***
switchport mode *mode*	mode: (access, trunk, general, customer)/access	Задать режим работы порта в VLAN. - *mode* – режим работы порта в VLAN.
no switchport mode		Установить значение по умолчанию.
switchport access vlan *vlan_id*	vlan_id: (1..4094)/1	Добавить VLAN для интерфейса доступа. - *vlan_id* – идентификационный номер VLAN.
no switchport access vlan		Установить значение по умолчанию.
switchport general acceptable-frame-type {untagged-only | tagged-only | all}	-/принимать все типы фреймов	Принимать на интерфейсе только фреймы определенного типа: - **untagged-only** – только нетегированные; - **tagged-only** – только тегированные; - **all** – все фреймы.
switchport trunk allowed vlan add *vlan_list*	vlan_list: (2..4094, all)	Добавить список VLAN для интерфейса. - *vlan_list* – список VLAN ID. Диапазон номеров VLAN можно задать перечислением через запятую или указать начальное и конечное значения диапазона через дефис "-".
switchport trunk allowed vlan remove *vlan_list*		Удалить список VLAN для интерфейса.
switchport trunk native vlan *vlan_id*	vlan_id: (1..4094)/1	Добавляет номер VLAN в качестве Default VLAN для данного интерфейса. Весь нетегированный трафик, поступающий на данный порт, определяется в данную VLAN. - *vlan_id* – идентификационный номер VLAN.
no switchport trunk native vlan		Установить значение по умолчанию.

switchport general allowed vlan add *vlan_list* **[tagged | untagged]**	vlan_list: (2..4094, all)	Добавить список VLAN для интерфейса. - **tagged** – порт будет передавать тегированные пакеты для VLAN; - **untagged** – порт будет передавать нетегированные пакеты для VLAN. - *vlan_list* – список VLAN ID. Диапазон VLAN можно задать перечислением через запятую или указать начальное и конечное значения диапазона через дефис "-".
switchport general allowed vlan remove *vlan_list*		Удалить список VLAN для интерфейса.
switchport general pvid *vlan_id*	vlan_id: (1..4094)/1 – если установлен VLAN по умолчанию	Добавить идентификатор VLAN порта (PVID) для основного интерфейса. - *vlan_id* – идентификационный номер VLAN порта.
no switchport general pvid		Установить значение по умолчанию.
switchport general ingress-filtering disable	-/фильтрация включена	Выключить для основного интерфейса фильтрацию входящих пакетов на основе присвоенного им значения VLAN ID.
no switchport general ingress-filtering disable		Включить для основного интерфейса фильтрацию входящих пакетов на основе присвоенного им значения VLAN ID. Если фильтрация включена, и пакет не входит в группу VLAN с присвоенным пакету значением VLAN ID, то пакет отбрасывается.
switchport general acceptable-frame-type {tagged-only | untagged-only | all}	-/принимать все типы фреймов	Принимать на основном интерфейсе только фреймы определенного типа: - **tagged-only** – только тегированные; - **untagged-only** – только не тегированные; - **all** – все фреймы.
no switchport general acceptable-frame-type		Принимать на основном интерфейсе все типы фреймов.
switchport general map protocols-group *group* **vlan** *vlan_id*	vlan_id: (1..4094) group: (1.. 2147483647)	Установить правило классификации VLAN для интерфейса, основанное на привязке к протоколу. - *group* – идентификационный номер группы; - *vlan_id* – идентификационный номер VLAN.
no switchport general map protocols-group *group*		Удалить правило классификации.
switchport general map macs-group *group* **vlan** *vlan_id*	vlan_id: (1..4094) group: (1..2147483647)	Установить правило классификации VLAN для интерфейса, основанное на привязке к MAC-адресу. - *group* – идентификационный номер группы; - *vlan_id* – идентификационный номер VLAN.
no switchport general map macs-group *group*		Удалить правило классификации.
switchport general map protocols-group *group* **vlan** *vlan_id*	vlan_id: (1..4094) group: (1.. 2147483647)	Установить правило классификации VLAN для интерфейса, основанное на привязке к протоколу. - *group* – идентификационный номер группы; - *vlan_id* – идентификационный номер VLAN.
no switchport general map protocols-group *group*		Удалить правило классификации.
switchport general map subnets-group *group* **vlan** *vlan_id*	vlan_id: (1..4094) group: (1.. 2147483647)	Установить правило классификации VLAN для интерфейса, основанное на привязке к IP-адресу.
no switchport general map subnets-group *group*		Удалить правило классификации.
switchport customer vlan *vlan_id*	vlan_id: (1..4094)/1	Добавить VLAN для пользовательского интерфейса. - *vlan_id* – идентификационный номер VLAN.
no switchport customer vlan		Установить значение по умолчанию.
switchport customer multicast-tv vlan add *vlan_list*	vlan_list: (2..4094, all)	Разрешает принимать многоадресный трафик из указанных VLAN (не являющихся VLAN пользовательского интерфейса) на настраиваемом интерфейсе, совместно с пользователями других пользовательских портов, принимающих многоадресный трафик из данных VLAN. - *vlan_list* – список VLAN ID. Диапазон VLAN можно задать перечислением через запятую или указать начальное и конечное значения диапазона через дефис "-".

switchport customer multicast-tv vlan remove *vlan_list*		Запрещает принимать многоадресный трафик на настраиваемом интерфейсе.
switchport protected-port	-	Переводит порт в режим изоляции внутри группы портов.
no switchport protected-port		Восстанавливает значение по умолчанию.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 54 – Команды режима Privileged EXEC

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 55 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show vlan multicast-tv vlan *vlan_id*	vlan_id: (1..4094)	Показать порты-источники и приемники многоадресного трафика в данной VLAN. Порты источники могут как передавать, так и принимать многоадресный трафик.
show vlan protocols-groups	-	Показать информацию о группах протоколов.
show vlan macs-groups	-	Показать информацию о группах MAC-адресов.
show interfaces switchport {tengigabitethernet *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Показать конфигурацию порта, группы портов.
show interfaces protected-ports [tengigabitethernet *te_port* **| port-channel** *group* **| detailed]**	te_port: (1..8/0/1..32); group: (1..32)	Показать состояние портов: в режиме Private VLAN Edge, в private-vlan-edge-сообществе.

Примеры выполнения команд

- Показать информацию о всех VLAN:

```
console# show vlan
```

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

Vlan       Name            Tagged Ports      UnTagged Ports      Created by
---- ----------------- ------------------ ------------------ ----------------
 1           1                             te1/0/1-12                D

                                           Po1-16
 2           2                                                       S
 3           3                                                       S
 4           4                                                       S
 5           5                                                       S
```

```
 6           6                                                    S
 8           8                                                    S
```

Показать порты источники и приемники многоадресного трафика в VLAN 4:

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

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

- Показать информацию о группах протоколов:

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

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

- Показать конфигурацию порта TenGigabitEthernet 1/0/1:

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

```
Gathering information...

Name: te1/0/1
Switchport: enable
Administrative Mode: access
Operational Mode: not present
Access Mode VLAN: 1
Access Multicast TV VLAN: none
Trunking Native Mode VLAN: 1
Trunking VLANs: 1-3
                        4-4094 (Inactive)
General PVID: 1
General VLANs: none
General Egress Tagged VLANs: none
General Forbidden VLANs: none
General Ingress Filtering: enabled
General Acceptable Frame Type: all
General GVRP status: disabled
Customer Mode VLAN: none
Customer Multicast TV VLANs: none
Private-vlan promiscuous-association primary VLAN: none
Private-vlan promiscuous-association Secondary VLANs: none
Private-vlan host-association primary VLAN: none
Private-vlan host-association Secondary VLAN: none



Classification rules:

Classification type Group ID VLAN ID
------------------- -------- -------
```

5.9.3 Настройка Private VLAN

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

- На коммутаторах может быть сконфигурировано три типа PVLAN портов: promiscuous – порт, который способен обмениваться данными между любыми интерфейсами, включая isolated и community-порты PVLAN;
- isolated – порт, который полностью изолирован от других портов внутри одного и того же PVLAN, но не от promiscuous-портов. PVLANы блокируют весь трафик, идущий в сторону isolated-портов, кроме трафика со стороны promiscuous-портов; пакеты со стороны isolated-портов могут передаваться только в сторону promiscuous-портов;
- community – группа портов, которые могут обмениваться данными между собой и promiscuous-портами, эти интерфейсы отделены на втором уровне модели OSI от всех остальных community интерфейсов, а также isolated-портов внутри PVLAN.

Процесс выполнения функции дополнительного разделения портов с помощью технологии Private VLAN представлен на рисунке 22.

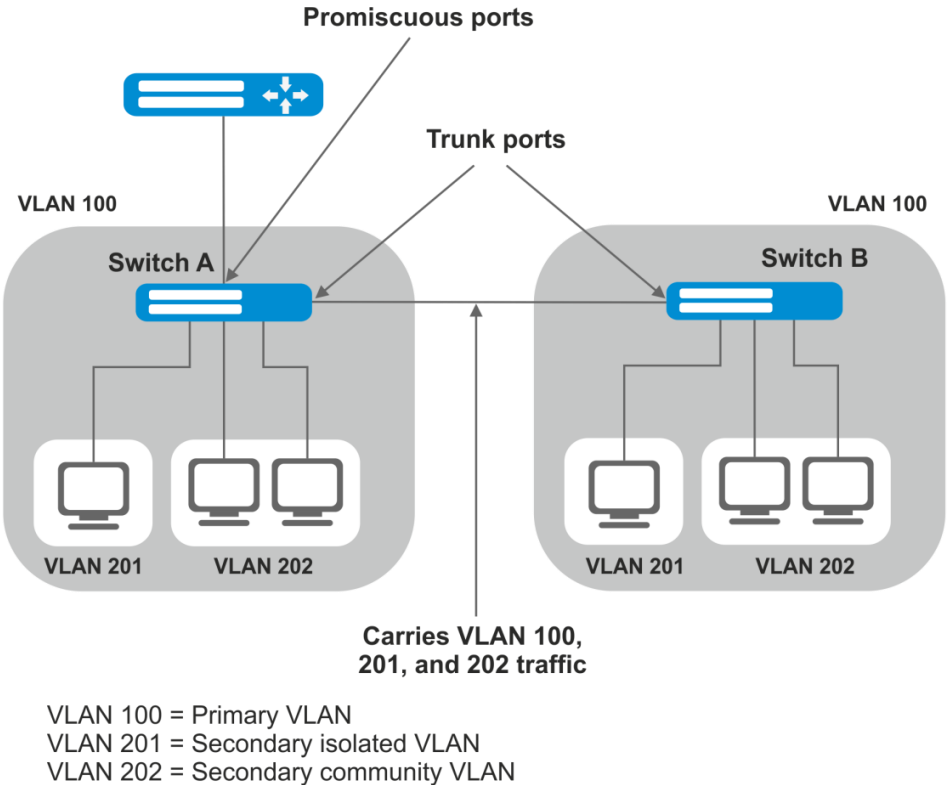


Рисунок 22 – Пример работы технологии Private VLAN

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

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

Таблица 56 – Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
switchport mode private-vlan {promiscuous | host}	-	Задать режим работы порта в VLAN.
no switchport mode		Установить значение по умолчанию.
switchport private-vlan mapping *primary_vlan* **[add | remove** *secondary_vlan]*	primary_vlan: (1..4094); secondary_vlan: (1..4094)	Добавить (удалить) основную и второстепенные VLAN на promiscuous интерфейс. **На один promiscuous интерфейс нельзя добавить больше одной primary vlan.**
no switchport private-vlan mapping		Удалить основную и второстепенные VLAN.
switchport private-vlan host-association *primary_vlan secondary_vlan*	primary_vlan: (1..4094) secondary_vlan: (1..4094)	Добавить primary и secondary vlan на host интерфейс. **На один host интерфейс нельзя добавить больше одной secondary vlan.**
no switchport private-vlan host-association		Удалить основную и второстепенные VLAN.

Таблица 57 – Команды режима конфигурации интерфейса VLAN

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

Максимальное количество второстепенных VLAN – 256
Максимальное количество community VLAN, которые могут быть ассоциированы с одной основной VLAN – 8.

5.9.4 Настройка интерфейса IP

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

Вид запроса командной строки в режиме конфигурации интерфейса IP .

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

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

Таблица 58 – Команды режима конфигурации интерфейса IP

Команда	*Значение/Значение по умолчанию*	*Действие*
directed-broadcast	-/выключено	Включает функцию перевода IP directed-broadcast пакета в стандартный широковещательный пакет и разрешает передачу через выбранный интерфейс.

no directed-broadcast		Запрещает трансляцию IP directed-broadcast пакетов.
helper-address *ip_address*	ip_address: A.B.C.D	Включает переадресацию широковещательных UDP-пакетов на определенный адрес. - *ip_address* – IP-адрес назначения, на который будут перенаправляться пакеты.
no helper-address *ip_address*		Отключает переадресацию широковещательных UDP-пакетов.

Примеры выполнения команд

- Включить функцию directed-broadcast:

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

5.9.5 Selective Q-in-Q

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

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

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

Вид запроса командной строки режима конфигурации интерфейса конфигурации:

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

Таблица 59 – Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
selective-qinq list ingress add_vlan vlan_id **[ingress_vlan** ingress_vlan_id**]**	vlan_id: (1..4094) ingress_vlan_id: (1..4094)	Создает правило, на основании которого к входящему пакету с внешней меткой ingress_vlan_id будет добавляться вторая метка vlan_id. Если ingress_vlan_id не указывать – правило будет применяться ко всем входящим пакетам, к которым не были применены другие правила («правило по умолчанию»).
selective-qinq list ingress deny [ingress_vlan ingress_vlan_id**]**	ingress_vlan_id: (1..4094)	Создает запрещающее правило, на основании которого входящие пакеты с внешней меткой тега ingress_vlan_id будут отбрасываться. Если ingress_vlan_id не указывается – будут отбрасываться все входящие пакеты.
selective-qinq list ingress permit [ingress_vlan ingress_vlan_id**]**	ingress_vlan_id: (1..4094)	Создает разрешающее правило, на основании которого входящие пакеты с внешней меткой тега ingress_vlan_id будут передаваться без изменений. Если ingress_vlan_id не указывается – будут передаваться все входящие пакеты без изменений.

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 60 – Команды режима EXEC

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

Примеры выполнения команд

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

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

5.10 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 конфигурации интерфейса Ethernet

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

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

Таблица 61 – Команды режима конфигурации интерфейса Ethernet

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 62 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show storm-control interface [tengigabitethernet *te_port***]**	te_port: (1..8/0/1..32)	Показывает конфигурацию функции контроля широковещательного «шторма» для указанного порта, либо всех портов.

Примеры выполнения команд

- Включить контроль широковещательного, многоадресного и одноадресного трафика на 3-м интерфейсе Ethernet. Установить скорость для контролируемого трафика – 5000 Кб/с: для широковещательного, 30% полосы пропускания для всего многоадресного, 70% для неизвестного одноадресного.

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

5.11 Группы агрегации каналов – Link Aggregation Group (LAG)

Коммутаторы обеспечивают поддержку групп агрегации каналов LAG в количестве согласно таблице (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 63 – Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
channel-group *group* **mode** *mode*	group: (1..32); mode: (on, auto)	Добавить ethernet-интерфейс в группу портов. - *on* – добавить порт в канал без LACP; - *auto* – добавить порт в канал с LACP в режиме «active».
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 64 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
port-channel load-balance {src-dst-mac-ip | src-dst-mac} [mpls-aware]	-/src-dst-mac	Задает механизм балансировки нагрузки для группы агрегированных портов. - **src-dst-mac-ip –** механизм балансировки основывается на MAC-адресе и IP-адресе; - **src-dst-mac –** механизм балансировки основывается на MAC-адресе; - **mpls-aware –** задает механизм балансировки MPLS-трафика для группы агрегированных портов, основанный на MAC-адресе.
no port-channel load-balance		Установить значение по умолчанию

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 65 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show interfaces port-channel [*group*]	group: (1..32)	Показывает информацию по группе каналов.

5.11.1 Статические группы агрегации каналов

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

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

5.11.2 Протокол агрегации каналов LACP

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

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 66 – Команды режима глобальной конфигурации

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

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

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

Таблица 67 – Команды режима конфигурации интерфейса Ethernet

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 68 – Команды режима EXEC

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

Примеры выполнения команд

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

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

5.12 Настройка IPv4-адресации

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

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

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

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

Таблица 69 – Команды режима конфигурации интерфейса

Команда	*Значение/Значение по умолчанию*	*Действие*
ip address *ip_address* **{***mask* **|** *prefix_length***}**	prefix_length: (8..32)	Назначение заданному интерфейсу IP-адреса и маски подсети. **Значение маски может быть записано либо в формате X.X.X.X, либо в формате /N, где N – количество единиц в двоичном представлении маски.**
no ip address [*IP_address***]**		Удаление IP-адреса интерфейса.
ip address dhcp	-	Получение IP-адреса для настраиваемого интерфейса от DHCP-сервера. **Не используется для loopback–интерфейса.**
no ip address dhcp		Запрет использования протокола DHCP для получения IP-адреса выбранным интерфейсом.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 70 – Команды режима глобальной конфигурации

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

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 71 – Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
clear host {* | *word***}**	word: (1..158) символов	Удаляет из памяти полученные по протоколу DHCP записи соответствий имен интерфейсов и их IP-адресов. * – удалить все соответствия.
renew dhcp { tengigabitethernet *te_port* **| vlan** *vlan_id* **| port-channel** *group* **| oob} [force-autoconfig]**	te_port: (1..8/0/1..32); group: (1..32) vlan_id: (1..4094)	Отправляет запрос к DHCP-серверу на обновление IP-адреса. - **force-autoconfig** – при обновлении IP-адреса загружается конфигурация с TFTP-сервера.
show ip helper-address	-	Отображает таблицу переадресации широковещательных UDP-пакетов.

Команды режима EXEC

Вид запроса командной строки в режиме Exec:

```
console>
```

Таблица 72 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip interface [tengigabitethernet *te_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan_id* **| tunnel** *tunnel* **| oob]**	te_port: (1..8/0/1..32); group: (1..32); loopback_id : (1…64); tunnel: (1..16); vlan_id: (1..4094)	Показывает конфигурацию IP-адресации для указанного интерфейса.

5.13 Настройка Green Ethernet

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

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 73 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
green-ethernet energy-detect	-/выключен	Включает энергосберегающий режим для неактивных портов.

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

Команды режима конфигурации интерфейса

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

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

Таблица 74 – Команды режима конфигурации интерфейса Ethernet

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

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 75 – Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show green-ethernet [tengigabitethernet *te_port* **| detailed]**	te_port: (1..8/0/1..32);	Отображает статистику green-ethernet.
green-ethernet power-meter reset	-	Сбрасывает счетчик измерителя мощности.

Примеры выполнения команд

- Отобразить статистику green-ethernet:

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

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

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

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

5.14 Настройка IPv6-адресации

5.14.1 Протокол IPv6

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

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

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

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

где:
interface-name – имя интерфейса:
interface-name = vlan<integer> | ch<integer> |<physical-port-name>
integer = <decimal-number> | <integer><decimal-number>
decimal-number = 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9
physical-port-name = **tengigabitethernet** (1..8/0/1..32)

Если значение группы или нескольких групп подряд в адресе протокола IPv6 равно нулю – 0000, то данные группы могут быть опущены. Например, адрес FE40:0000:0000:0000:0000:0000:AD21:FE43 может быть сокращен до FE40::AD21:FE43. Сокращению не могут быть подвергнуты 2 разделенные нулевые группы из-за возникновения неоднозначности.

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 76 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ipv6 default-gateway *ipv6_address*		Задает значение локального адреса IPv6-шлюза по умолчанию.
no ipv6 default-gateway *ipv6_address*		Удаляет настройки IPv6-шлюза по умолчанию.
ipv6 neighbor *ipv6_address* **{ tengigabitethernet** *te_port* **| port-channel** *group* **| vlan** *vlan_id***}** *mac_address*	te_port: (1..8/0/1..12); group: (1..32); vlan_id: (1..4094)	Создает статическое соответствие между MAC-адресом соседнего устройства и его IPv6-адресом. - *ipv6_address* – IPv6-адрес; - *mac_address* – MAC-адрес.
no ipv6 neighbor [*ipv6_address***] [tengigabitethernet** *te_port* **| port-channel** *group* **| vlan** *vlan_id***]**		Удаляет статическое соответствие между MAC-адресом соседнего устройства и его IPv6-адресом.
ipv6 icmp error-interval *milliseconds* **[***bucketsize***]**	milliseconds**:** (0..2147483647)/100; bucketsize: (1..200)/10	Задает ограничение скорости для ICMPv6-сообщений об ошибках.
no ipv6 icmp error-interval		Устанавливает значение по умолчанию.
ipv6 route *prefix***/***prefix_length* **{***gateway***} [***metric***]**	prefix: X:X:X:X::X; prefix_length: (0..128); metric: (1..65535)/1	Добавление статического маршрута IPv6 - *prefix* – сеть назначения; - *prefix_length* – префикс маски сети (количество единиц в маске); - *gateway* – шлюз для доступа к сети назначения;
no ipv6 route *prefix***/***prefix_length* **[***gateway***]**		Удаление статического маршрута IPv6.
ipv6 unicast-routing	-/выключено	Включает перенаправление одноадресных пакетов.
no ipv6 unicast-routing		Отключает перенаправление одноадресных пакетов.

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

Вид запроса командной строки режима конфигурации интерфейса:

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

Таблица 77 – Команды режима конфигурации интерфейса (Ethernet, VLAN, Port-channel)

Команда	*Значение/Значение по умолчанию*	*Действие*
ipv6 enable	-/выключено	Включает поддержку IPv6 на интерфейсе.
no ipv6 enable		Отключает поддержку IPv6 на интерфейсе.
ipv6 address autoconfig	По умолчанию автоматическая конфигурация включена, адреса не назначены.	Включение автоматической конфигурации IPv6-адресов на интерфейсе. Адреса настраиваются в зависимости от префиксов, которые получены в сообщениях «Router Advertisement».
no ipv6 address autoconfig		Устанавливает значение по умолчанию.
ipv6 address *ipv6_address/prefix_length* **link-local**	По умолчанию значение локального адреса: (FE80::EUI64)	Задает локальный IPv6-адрес интерфейса. Старшие биты локальных IP-адресов в IPv6 – FE80::
no ipv6 address [*ipv6_address/prefix-length* **link-local]**		Удаляет локальный IPv6-адрес.
ipv6 nd dad attempts *attempts_number*	(0..600)/1	Задает количество сообщений-требований, передаваемых интерфейсом взаимодействующему устройству в случае обнаружения дубликации (коллизии) IPv6-адреса.
no ipv6 nd dad attempts		Возвращает значение по умолчанию.
ipv6 unreachables	-/enabled	Включение ICMPv6 сообщений о недостижимости адресата при передаче пакетов на определенный интерфейс.
no ipv6 unreachables		Устанавливает значение по умолчанию.

ipv6 mld version *version*	version: (1..2)/2	Определение версии протокола MLD для интерфейса.
no ipv6 mld version		Устанавливает значение по умолчанию

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 78 – Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ipv6 neighbors {*ipv6_address* **| tengigabitethernet** *te_port* **| port-channel** *group* **| vlan** *vlan_id***}**	te_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094)	Показывает информацию о соседних IPv6 устройствах, содержащуюся в кэше.
clear ipv6 neighbors	-	Очищает кэш, содержащий информацию о соседних устройствах, работающих по протоколу IPv6. Информация о статических записях сохраняется.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 79 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ipv6 interface [brief | tengigabitethernet *te_port* **| port-channel** *group* **| loopback | vlan** *vlan_id***]**	te_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094)	Показывает настройки протокола IPv6 для указанного интерфейса.
show ipv6 route [summary | local |connected | static | ospf | icmp | nd | *ipv6_address***/***ipv6_prefix* **| interface { tengigabitethernet** *te_port* **| port-channel** *group* **| loopback | vlan** *vlan_id***}]**	te_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094)	Показывает таблицу IPv6-маршрутов.

5.15 Настройка протоколов

5.15.1 Настройка протокола DNS – системы доменных имен

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

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 80 – Команды режима глобальной конфигурации

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

Команды режима EXEC

Вид запроса командной строки в режиме EXEC:

```
console#
```

Таблица 81 – Команды режима EXEC

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

Примеры использования команд

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

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

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

```
console# configure
```

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

5.15.2 Настройка протокола ARP

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

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 82 – Команды режима глобальной конфигурации

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

Команды режима privileged EXEC

Вид запроса командной строки в режиме privileged EXEC:

```
console#
```

Таблица 83 – Команды режима privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
clear arp-cache	-	Удаляет все динамические записи из ARP-таблицы (команда доступна только для привилегированного пользователя).
show arp [ip-address *ip_address***] [mac-address** *mac_addres***] [tengigabitethernet** *te_port* **| port-channel** *group* **| oob**]	формат *ip_address*: A.B.C.D формат *mac_address*: H.H.H или H:H:H:H:H:H или H-H-H-H-H-H; te_port: (1..8/0/1..32); group: (1..32)	Показывает записи ARP-таблицы: все записи, фильтр по IP-адресу; фильтр по MAC-адресу; фильтр по интерфейсу. - *ip_address* – IP-адрес; - *mac_address* – MAC-адрес.
show arp configuration	-	Показывает глобальную конфигурацию ARP и конфигурацию ARP для интерфейсов.

Команды режима конфигурации интерфейса

Вид запроса командной строки в режиме interface configuration:

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

Таблица 84 – Команды режима interface configuration

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

Примеры использования команд

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

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

- Показать содержимое ARP-таблицы:

```
console# show arp
```

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

5.15.3 Настройка протокола GVRP

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 85 – Команды режима глобальной конфигурации

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

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

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

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

Таблица 86 – Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

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

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 87 – Команды режима privileged EXEC

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 88 – Команды режима EXEC

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

show gvrp error-statistics [tengigabitethernet *te_port* **| port-channel** *group***]**		Показывает статистику по ошибкам при работе протокола GVRP для указанного интерфейса, либо для всех интерфейсов.

5.15.4 Механизм обнаружения петель (loopback-detection)

Данный механизм позволяет устройству отслеживать закольцованные порты. Петля на порту обнаруживается путём отсылки коммутатором фрейма с адресом назначения, совпадающим с одним из MAC-адресов устройства.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 89 – Команды режима глобальной конфигурации

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

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

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

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

Таблица 90 – Команды режима конфигурации интерфейса Ethernet, группы интерфейсов, интерфейса VLAN

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 91 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show loopback-detection [tengigabitethernet te_port **| port-channel** *group* **| detailed]**	te_port: (1..8/0/1..32); group: (1..32).	Отображает состояние механизма loopback-detection.

5.15.5 Семейство протоколов STP (STP, RSTP, MSTP)

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

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

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

Максимально допустимое количество экземпляров MSTP указано в таблице 9.

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

5.15.5.1 Настройка протокола STP, RSTP

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 92 – 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 {stp | rstp | mstp}	-/RSTP	Устанавливает режим работы протокола STP: - **stp** – IEEE 802.1D Spanning Tree Protocol; - **rstp** – IEEE 802.1W Rapid Spanning Tree Protocol; - **mstp** – IEEE 802.1S Multiple Spanning Tree Protocol.
no spanning-tree mode		Устанавливает значение по умолчанию.

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

При задании 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 93 – 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 94	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 94
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 [auto]	-/auto	Включает режим, в котором порт при поднятии на нем линка сразу становится в состояние передачи, не дожидаясь истечения таймера. - **auto** – добавляет задержку 3 секунды перед переходом в состояние передачи.
no spanning-tree portfast		Выключает режим моментального перехода в состояние передачи по поднятию «линка».
spanning-tree guard {root | 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}	-/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 bpdu {filtering | flooding}	-	Определяет режим обработки пакетов BPDU-интерфейсом, на котором выключен протокол STP. - **filtering** – на интерфейсе с выключенным протоколом STP BPDU пакеты фильтруются; - **flooding** – на интерфейсе с выключенным протоколом STP нетегированные BPDU-пакеты передаются, тегированные – фильтруются.
no spanning-tree bpdu		Устанавливает значение по умолчанию.

Таблица 94 – Ценность пути, установленная по умолчанию (spanning-tree cost)

Интерфейс	***Метод определения ценности пути***	
	Long	***Short***
Port-channel	20000	4
TenGigabit Ethernet (10000 Mbps)	2000000	100

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 95 – Команды режима privileged EXEC

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 96 – Команды режима EXEC

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

5.15.5.2 Настройка протокола MSTP

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 97 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
spanning-tree	-/разрешено	Разрешает использование коммутатором протокола STP.
no spanning-tree		Запрещает использование коммутатором протокола STP.
spanning-tree mode {stp | rstp | mstp}	-/RSTP	Устанавливает режим работы протокола STP.
no spanning-tree mode		Устанавливает значение по умолчанию.
spanning-tree pathcost method {long | short}	-/short	Устанавливает метод определения ценности пути. - **long** – значение ценности в диапазоне 1..200000000; - **short** – значение ценности в диапазоне 1..65535.
no spanning-tree pathcost method		Устанавливает значение по умолчанию.
spanning-tree mst *instance_id* **priority** *priority*	instance_id: (1..15); 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: (1..40)/20	Устанавливает максимальное количество транзитных участков для пакета BPDU, необходимых для формирования дерева и удержания информации о его строении. Если пакет уже прошел максимальное количество транзитных участков, то на следующем участке он отбрасывается. - *hop_count* – максимальное количество транзитных участков для пакета BPDU.
no spanning-tree mst max-hops		Устанавливает значение по умолчанию.
spanning-tree mst configuration	-	Вход в режим конфигурации протокола MSTP.

Команды режима конфигурации протокола MSTP

Вид запроса командной строки в режиме конфигурации протокола MSTP:

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

Таблица 98 – Команды режима конфигурации протокола MSTP

Команда	*Значение/Значение по умолчанию*	*Действие*
instance *instance_id* **vlan** *vlan_range*	instance_id:(1..15); vlan_range: (1..4094)	Создает соответствие между экземпляром протокола MSTP и группами VLAN. - *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*).
show {current | pending}	-	Показывает текущую (**current**) либо ожидающую (**pending**) конфигурацию MST.
exit	-	Выход из режима конфигурации протокола MSTP с сохранением конфигурации.
abort	-	Выход из режима конфигурации протокола MSTP без сохранения конфигурации.

Команды режима конфигурации интерфейса Ethernet, интерфейса группы портов

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

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

Таблица 99 – 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..15); 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..15); 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 94

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.

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 100 – Команды режима EXEC

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

Примеры выполнения команд

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

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

console# show spanning-tree
```

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

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

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

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

5.15.6 Настройка протокола G.8032v2 (ERPS)

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 101 – Команды режима глобальной конфигурации

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

Команды режима конфигурации кольца

Вид запроса командной строки в режиме конфигурации кольца:

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

Таблица 102 – Команды режима конфигурации ERPS-кольца

Команда	*Значение/Значение по умолчанию*	*Действие*
protected vlan add *vlan_list*	vlan_list:(2..4094, all)	Добавляет диапазон VLAN в список защищенных VLAN. - *vlan_list* – список VLAN. Диапазон VLAN можно задать перечислением через запятую или указать начальное и конечное значения диапазона через дефис "-".
protected vlan remove *vlan_list*	vlan_list:(2..4094, all)	Удаляет диапазон VLAN из списка защищенных VLAN. - *vlan_list* – список VLAN для удаления.
port {west | east} { tengigabitethernet *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..24); group: (1..32)	Выбор west (east)-порта коммутатора, включенного в кольцо.

no port {west | east}		Удаление west (east)-порта коммутатора, включенного в кольцо.
rpl {west | east} {owner | neighbor}	-/no rpl	Выбор RPL-порта коммутатора и его роли. - **west** – RPL-портом будет назначен west-порт; - **east** – RPL-портом будет назначен west-порт; - **owner** – коммутатор будет являться владельцем RPL-порта; - **neighbor** – коммутатор будет являться соседом владельца RPL-порта.
no rpl		Удаление RPL-порта коммутатора.
level *level*	level: (0..7)/1	Настройка уровня сообщений R-APS. Необходимо для прохождения сообщений через CFM MEP. - *level* – уровень сообщений R-APS.
no level		Установка значения по умолчанию.
ring enable	-/выключено	Включение функционирования кольца.
no ring enable		Выключение функционирования кольца.
version version	version: (1..2)/2	Выбор режима совместимости с другими версиями протокола G.8032. - *version* – версия протокола G.8032.
no version		Установка значения по умолчанию.
revertive	-/revertive	Выбор режима работы кольца.
no revertive		Установка значения по умолчанию.
sub-ring vlan *vlan_id*	vlan_id:(1..4094)	Указание подкольца для данного кольца. - *vlan_id* – номер VLAN.
no sub-ring vlan *vlan_id*		Удаление подкольца.
sub-ring vlan *vlan_id* **[tc-propogation]**	vlan_id:(1..4094)	Включить отправку сигнала очистки MAC-таблицы в основное кольцо при перестроении подкольца.
no sub-ring vlan *vlan_id*		Отключить отправку сигнала очистки MAC-таблицы в основное кольцо при перестроении подкольца.
timer guard *value*	value:(10..2000) мс, кратное 10/500 мс	Установка таймера блокирующего устаревшие R-APS сообщения.
no timer guard		Установка значения по умолчанию.
timer holdoff *value*	value:(0..10000) мс, кратное 100 с точностью 5 мс/0 мс	Установка таймера задержки реакции коммутатора на изменение в состоянии. Вместо реакции на событие включается таймер, по истечении которого коммутатор информирует о своем состоянии. Предназначен для уменьшения флуда пакетов при флаппинге портов.
no timer holdoff		Установка значения по умолчанию.
timer wtr *value*	value:(1..12) мин/5 мин	Установка таймера, который запускается на RPL Owner коммутаторе в revertive-режиме. Используется для предотвращения частых защитных переключений из-за сигналов о неисправностях.
no timer wtr		Установка значения по умолчанию.
switch forced {west | east}	-/no	Форсирует запуск защитного переключения кольца, при этом блокируется указанный порт.
no switch forced		Отмена форсирования переключения кольца.
switch manual {west | east}	-/no	Ручное блокирование указанного west (east)-порта и разблокирование east (west).
no switch manual		Отмена ручной блокировки.
abort	-	Откатить изменения, внесенные с момента входа в режим конфигурации кольца.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 103 – Команды режима EXEC

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

5.15.7 Настройка протокола LLDP

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

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

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 104 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
lldp run	-/разрешено	Разрешает коммутатору использование протокола LLDP.
no lldp run		Запрещает коммутатору использование протокола LLDP.
lldp timer *seconds*	seconds: (5..32768)/30 сек	Определяет, как часто устройство будет отправлять обновление информации LLDP.
no lldp timer		Устанавливает значение по умолчанию.
lldp hold-Multiplier *number*	number: (2..10)/4	Задает величину времени для принимающего устройства, в течение которого нужно удерживать принимаемые пакеты LLDP перед их сбросом. Данная величина передается на принимаемую сторону в LLDP update пакетах (пакетах обновления), является кратностью для таймера LLDP (lldp timer). Таким образом, время жизни LLDP пакетов рассчитывается по формуле TTL = min (65535, LLDP-Timer * LLDP-HoldMultiplier)
no lldp hold-Multiplier		Устанавливает значение по умолчанию.
lldp reinit *seconds*	seconds: (1..10)/2 сек	Минимальное время, которое LLDP-порт будет ожидать перед повторной инициализацией LLDP.
no lldp reinit		Устанавливает значение по умолчанию.
lldp tx-delay *seconds*	seconds: (1..8192)/2 сек	Устанавливает задержку между последующими передачами пакетов LLDP, инициированными изменениями значений или статуса в локальных базах данных MIB LLDP. **Рекомендуется, чтобы данная задержка была меньше, чем значение 0.25* LLDP-Timer.**
no lldp tx-delay		Устанавливает значение по умолчанию.

lldp lldpdu {filtering | flooding}	-/filtering	Определяет режим обработки пакетов LLDP, когда протокол LLDP выключен на коммутаторе: - *filtering* – указывает, что LLDP-пакеты фильтруются, если протокол LLDP выключен на коммутаторе; - *flooding* – указывает, что LLDP-пакеты передаются, если протокол LLDP выключен на коммутаторе.
no lldp lldpdu		Устанавливает значение по умолчанию.
lldp med fast-start repeat-count *number*	number: (1..10)/3	Устанавливает число повторений PDU LLDP для быстрого запуска, определяемого посредством LLDP-MED.
no lldp med fast-start repeat-count		Устанавливает значение по умолчанию.
lldp med network-policy *number application* **[vlan** *vlan_id***] [vlan-type {tagged | untagged}] [up** *priority***] [dscp** *value***]**	number: (1..32); application*:* (voice, voice-signaling, guest-voice, guest-voice-signaling, softphone-voice, video-conferencing, streaming-video, video-signaling); vlan_id: (0..4095); priority: (0..7); value*:* (0..63)	Определяет правило для параметра network-policy (сетевая политика устройства). Данный параметр является опциональным для расширения протокола LLDP MED. - *number* – порядковый номер правила network policy; - *application* – главная функция, определенная для данного правила network policy. - *vlan_id* – идентификатор VLAN для данного правила; - **tagged**/**untagged** – определяет тегированной или нетегированной будет VLAN, используемая данным правилом. - *priority* – приоритет данного правила (используется на втором уровне модели OSI); - *value* – значение DSCP, используемое данным правилом.
no lldp med network-policy *number*		Удаляет созданное правило для параметра network-policy.
lldp notifications interval *seconds*	seconds: (5..3600)/5 сек	Устанавливает максимальную скорость передачи уведомлений LLDP. - *seconds* – период времени, в течение которого устройство может отправить не более одного уведомления.
no lldp notifications interval		Устанавливает значение по умолчанию.

Команды режима конфигурации интерфейсов Ethernet

Вид запроса командной строки в режиме конфигурации интерфейсов Ethernet:

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

Таблица 105 – Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
lldp transmit	По умолчанию разрешено использование в обоих направлениях.	Разрешает передачу пакетов по протоколу LLDP на интерфейсе.
no lldp transmit		Запрещает передачу пакетов по протоколу LLDP на интерфейсе.
lldp receive		Разрешает прием пакетов по протоколу LLDP на интерфейсе.
no lldp receive		Запрещает прием пакетов по протоколу LLDP на интерфейсе.
lldp optional-tlv *tlv_list*	tvl_list: (port-desc, sys-name, sys-desc, sys-cap, 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size, 802.3-power-via-mdi)/По умолчанию опциональные TLV не включены в пакет.	Определяет, какие опциональные TLV-поля (Type, Length, Value) будут включены устройством в передаваемый LLDP-пакет. В команду можно включить от одного до пяти опциональных TLV. **TLV 802.3-power-via-mdi доступна только на устройствах с поддержкой PoE.**
no lldp optional-tlv		Устанавливает значение по умолчанию.
lldp optional-tlv 802.1 {pvid [enable | disable] | ppvid {add | remove} *ppv_id* **| vlan-name {add | remove}** *vlan_id***}**	ppvid: (1-4094); vlan_id: (2-4094); По умолчанию опциональные TLV не включены.	Определяет, какие опциональные TLV-поля будут включены устройством в передаваемый LLDP-пакет: - **pvid** – PVID интерфейса; - **ppvid** – добавить/удалить PPVID; - **vlan-name** – добавить/удалить номер VLAN;

lldp optional-tlv 802.1 protocol {add | remove} {stp | rstp | mstp | pause | 802.1x | lacp | gvrp}		- **protocol** – добавить/удалить определенный протокол.
no lldp optional-tlv 802.1 pvid		Устанавливает значение по умолчанию.
lldp management-address {*ip_address* **| none | automatic [tengigabitethernet** *te_port* **| port-channel** *group* **| vlan** *vlan_id***]}**	формат ip-address: A.B.C.D; te_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094). По умолчанию управляющий адрес определяется автоматически.	Определяет управляющий адрес, объявленный на интерфейсе. - *ip_address* – задается статический IP-адрес; - **none** – указывает, что адрес не объявлен; - **automatic** – указывает, что система автоматически выбирает управляющий адрес из всех IP-адресов коммутатора; - **automatic** – указывает, что система автоматически выбирает управляющий адрес, из сконфигурированных адресов заданного интерфейса. Если интерфейс ethernet или интерфейс группы портов принадлежат VLAN, то данный адрес VLAN не будет включен в список возможных управляющих адресов. **В случае наличия нескольких IP-адресов система выбирает начальный IP-адрес из диапазона динамических IP-адресов. Если динамические адреса отсутствуют, то система выбирает начальный IP-адрес из диапазона возможных статических IP-адресов.**
no lldp management-address		Удаляет управляющий IP-адрес.
lldp notification {enable | disable}	По умолчанию отправка уведомлений LLDP запрещена.	Разрешает/запрещает отправку уведомлений LLDP на интерфейсе. - **enable** – разрешает; - **disable** – запрещает.
no lldp notifications		Устанавливает значение по умолчанию.
lldp med enable [*tlv_list*]	tvl_list: (network-policy, location, inventory)/запрещено использование расширения протокола LLDP MED.	Разрешает использование расширения протокола LLDP MED. В команду можно включить от одного до трех специальных TLV.
lldp med network-policy {add | remove} *number*	number: (1-32)	Назначает правило network-policy данному интерфейсу. - **add** – назначает правило; - **remove** – удаляет правило; - *number* – номер правила.
no lldp med network-policy		Удаляет правило network-policy с данного интерфейса.
lldp med location {coordinate *coordinate* **| civic-address** *civic_address_data* **| ecs-elin** *ecs_elin_data***}**	coordinate: 16 байт; civic_address_data: (6..160) байт; ecs_elin_data: (10..25) байт.	Задает местоположение устройства для протокола LLDP (значение параметра location протокола LLDP MED). - *coordinate* – адрес в системе координат; - *civic_address_data* – административный адрес устройства; - *ecs-elin_data* – адрес в формате, определенном ANSI/TIA 1057.
no lldp med location {coordinate | civic-address | ecs-elin}		Удаляет настройки параметра местоположения location.
lldp med notification topology-change {enable | disable}	-/запрещено	Разрешает/запрещает отправку уведомлений LLDP MED об изменении топологии. - **enable** – разрешает отправку уведомлений; - **disable** – запрещает отправку уведомлений.
no lldp med notifications topology-change		Устанавливает значение по умолчанию.

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

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

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 106 – Команды режима privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
clear lldp table [tengigabitethernet *te_port* **| oob]**	te_port: (1..8/0/1..32);	Очищает таблицу адресов обнаруженных соседних устройств и начинает новый цикл обмена пакетами по протоколу LLDP MED.
show lldp configuration [tengigabitethernet *te_port* **| oob | detailed]**	te_port: (1..8/0/1..32);	Показывает LLDP-конфигурации всех физических интерфейсов устройства, либо заданных интерфейсов.
show lldp med configuration [tengigabitethernet *te_port* **| oob | detailed]**	te_port: (1..8/0/1..32);	Показывает конфигурации расширения протокола LLDP – MED для всех физических интерфейсов, либо заданных интерфейсов.
show lldp local { tengigabitethernet *te_port* **| oob}**	te_port: (1..8/0/1..32);	Показывает LLDP-информацию, которую анонсирует данный порт.
show lldp local tlvs-overloading [tengigabitethernet *te_port* **| oob]**	te_port: (1..8/0/1..32);	Показывает статус перезагрузки TLVs LLDP.
show lldp neighbors [tengigabitethernet *te_port* **| oob]**	te_port: (1..8/0/1..32);	Показывает информацию о соседних устройствах, на которых работает протокол LLDP.
show lldp statistics [tengigabitethernet *te_port* **| oob | detailed]**	te_port: (1..8/0/1..32);	Показывает статистику LLDP.

Примеры выполнения команд

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

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

- Посмотреть конфигурацию LLDP:

```
console# show lldp configuration
```

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

Таблица 107 – Описание результатов

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

Показать информацию о соседних устройствах

```
console# show lldp neighbors
```

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

Таблица 108 – Описание результатов

Поле	*Описание*
Port	Номер порта.
Device ID	Имя или MAC-адрес соседнего устройства.
Port ID	Идентификатор порта соседнего устройства.
System name	Системное имя устройства.
Capabilities	Данное поле описывает тип устройства: B – Мост (Bridge); R – Маршрутизатор (Router); W – Точка доступа WI-FI (WLAN Access Point); T – Телефон (Telephone); D – DOCSIS-устройство (DOCSIS cable device); H – Сетевое устройство (Host); r – Повторитель (Repeater); O – Тип неизвестен (Other).
System description	Описание соседнего устройства.
Port description	Описание порта соседнего устройства.

Management address	Адрес управления устройством.
Auto-negotiation support	Определяет, поддерживается ли автоматическое определение режима порта.
Auto-negotiation status	Определяет, включена ли поддержка автоматического определения режима порта.
Auto-negotiation Advertised Capabilities	Определяет режимы, поддерживаемые функцией автоматического определения порта.
Operational MAU type	Рабочий MAU-тип устройства.

5.16 Voice VLAN

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

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

Список OUI производителей VoIP-оборудования, доминирующих на рынке.

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

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 109 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
voice vlan aging-timeout *timeout*	timeout: (1..43200)/1440	Устанавливает таймаут для порта, принадлежащего к voice-vlan. Если с порта в течение заданного времени не было фреймов с OUI VoIP-оборудования, то voice vlan удаляется с данного порта.
no voice vlan aging-timeout		Восстанавливает значение по умолчанию.

voice vlan cos *cos* **[remark]**	cos: (0-7)/6	Устанавливает COS, которым маркируются фреймы, принадлежащие Voice VLAN.
no voice vlan cos		Восстанавливает значение по умолчанию.
voice vlan id *vlan_id*	vlan_id: (1..4094)	Устанавливает идентификатор VLAN для Voice VLAN
no voice vlan id		Удаляет идентификатор VLAN для Voice VLAN **Для удаления идентификатора VLAN требуется предварительно отключить функцию voice vlan на всех портах.**
voice vlan oui-table {add *oui* **| remove** *oui***} [***word***]**	word: (1..32) символов	Позволяет редактировать таблицу OUI. - *oui* – первые 3 байта MAC-адреса; - *word* – описание oui.
no voice vlan oui-table		Удаляет все пользовательские изменения OUI-таблицы.

Команды режима конфигурации интерфейса Ethernet

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

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

Таблица 110 – Команды режима конфигурации интерфейса Ethernet

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

5.17 Групповая адресация

5.17.1 Функция посредника протокола IGMP (IGMP Snooping)

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

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

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

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

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 111 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip igmp snooping	По умолчанию функция выключена	Разрешает использование функции IGMP Snooping коммутатором.
no ip igmp snooping		Запрещает использование функции IGMP Snooping коммутатором.
ip igmp snooping vlan *vlan_id*	vlan_id: (1..4094) По умолчанию функция выключена	Разрешает использование функции IGMP Snooping коммутатором для данного интерфейса VLAN. - *vlan_id* – идентификационный номер VLAN.
no ip igmp snooping vlan *vlan_id*		Запрещает использование функции IGMP Snooping коммутатором для данного интерфейса VLAN.
ip igmp snooping vlan *vlan_id* **static** *ip_multicast_address* **[interface { tengigabitethernet** *te_port* **| port-channel** *group***}]**	vlan_id: (1..4094); te_port: (1..8/0/1..32); group: (1..32)	Регистрирует групповой IP-адрес в таблице групповой адресации и статически добавляет интерфейсы из группы для текущей VLAN. - *vlan_id* – идентификационный номер VLAN; - *ip_multicast_address* – групповой IP-адрес. Перечисление интерфейсов осуществляется через «–» и «,».
no ip igmp snooping vlan *vlan_id* **static** *ip_address* **[interface { tengigabitethernet** *te_port* **| port-channel** *group***}]**		Удаляет групповой IP-адрес из таблицы.
ip igmp snooping vlan *vlan_id* **mrouter learn pim-dvmrp**	vlan_id: (1..4094) По умолчанию разрешено	Разрешает для данной группы VLAN автоматическое распознавание портов, к которым подключены многоадресные маршрутизаторы. - *vlan_id* – идентификационный номер VLAN.
no ip igmp snooping vlan *vlan_id* **mrouter learn pim-dvmrp**		Запрещает для данной группы VLAN автоматическое распознавание портов, к которым подключены многоадресные маршрутизаторы.
ip igmp snooping vlan *vlan_id* **mrouter interface { tengigabitethernet** *te_port* **| port-channel** *group***}**	vlan_id: (1..4094); te_port: (1..8/0/1..32); group: (1..32)	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 { tengigabitethernet** *te_port* **| port-channel** *group***}**		Указывает, что к порту не подключен маршрутизатор многоадресной рассылки.
ip igmp snooping vlan *vlan_id* **forbidden mrouter interface { tengigabitethernet** *te_port* **| port-channel** *group***}**	vlan_id: (1..4094); te_port: (1..8/0/1..32); group: (1..32)	Устанавливает запрет на определение порта (статически, динамически) как порта, к которому подключен маршрутизатор многоадресной рассылки. - *vlan_id* – идентификационный номер VLAN.
no ip igmp snooping vlan *vlan_id* **forbidden mrouter interface {tengigabitethernet** *te_port* **| port-channel** *group***}**		Снимает запрет на определение порта как порта, к которому подключен маршрутизатор многоадресной рассылки.
ip igmp snooping vlan *vlan_id* **querier**	vlan_id: (1..4094); -/выдача запросов отключена	Включает поддержку выдачи запросов igmp-query коммутатором в данной VLAN.
no ip igmp snooping vlan *vlan_id* **querier**		Отключает поддержку выдачи запросов igmp-query коммутатором в данной VLAN.
ip igmp snooping vlan *vlan_id* **querier version {2 | 3}**	-/IGMPv3	Устанавливает версию IGMP-протокола, на основании которой будут формироваться IGMP-query запросы.
no ip igmp snooping vlan *vlan_id* **querier version**		Устанавливает значение по умолчанию
ip igmp snooping vlan *vlan_id* **querier address** *ip_address*	vlan_id: (1..4094)	Определяет исходный IP-адрес, который будет использоваться IGMP querier-ом. Querier – устройство, которое отправляет IGMP-запросы.
no ip igmp snooping vlan *vlan_id* **querier address**		Устанавливает значение по умолчанию. По умолчанию если IP-адрес настроен для VLAN, он используется в качестве адреса источника IGMP Snooping Querier.

ip igmp snooping vlan *vlan_id* **immediate-leave [host-based]**	vlan_id: (1..4094); -/выключено	Включить процесс IGMP Snooping Immediate-Leave на текущей VLAN. Означает, что порт должен быть немедленно удален из группы IGMP после получения сообщения IGMP leave. - **host-based** – механизм fast-leave срабатывает только в том случае, когда все пользователи, подключенные к данному порту отписались от группы (счетчик пользователей ведется на основании Source MAC-адресов в заголовках IGMP-report'ов).
no ip igmp snooping vlan *vlan_id* **immediate-leave**		Отключить процесс IGMP Snooping Immediate-Leave на текущей VLAN.

Команды режима конфигурации интерфейса VLAN

Вид запроса командной строки режима конфигурации VLAN:

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

Таблица 112 – Команды режима конфигурации интерфейса VLAN

Команда	*Значение/Значение по умолчанию*	*Действие*
ip igmp robustness *count*	count: (1..7)/2	Устанавливает значение устойчивости для IGMP. Если на канале наблюдается потеря данных, значение устойчивости должно быть увеличено.
no ip igmp robustness		Устанавливает значение по умолчанию.
ip igmp query-interval *seconds*	seconds: (30..18000)/125 с	Устанавливает таймаут, по которому система отправляет основные запросы всем участникам группы многоадресной передачи для проверки их активности.
no ip igmp query-interval		Устанавливает значение по умолчанию.
ip igmp query-max-response-time *seconds*	seconds: (5..20)/10 с	Устанавливает максимальное время ответа на запрос.
no ip igmp query-max-response-time		Устанавливает значение по умолчанию.
ip igmp last-member-query-count *count*	count: (1..7)/значение переменной robustness	Устанавливает количество запросов, после рассылки которых, коммутатор определяет, что на данном порту нет желающих участвовать в многоадресной рассылке.
no ip igmp last-member-query-count		Устанавливает значение по умолчанию.
ip igmp last-member-query-interval *milliseconds*	*milliseconds*: (100..25500)/1000 мс	Устанавливает интервал запроса для последнего участника.
no ip igmp last-member-query-interval		Устанавливает значение по умолчанию.
ip igmp version *version*	version: (1-3)/2	Установить версию протокола **IGMP.**
no ip igmp version		Установить значение по умолчанию.

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet

Вид запроса командной строки режима конфигурации интерфейса:

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

Таблица 113 – 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».

Команды режима EXEC

Все команды доступны только для привилегированного пользователя.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 114 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip igmp snooping mrouter [interface *vlan_id***]**	vlan_id: (1..4094)	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 [vlan *vlan_id***] [ip-multicast-address** *ip_multicast_address***] [ip-address** *IP_address***]**	vlan_id: (1..4094)	Показывает информацию об изученных многоадресных группах, участвующих в групповой рассылке.
show ip igmp snooping cpe vlans [vlan *vlan_id***]**	vlan_id: (1..4094)	Показывает таблицу соответствий между VLAN оборудования, установленного у пользователя, и VLAN для телевещания.

Примеры выполнения команд

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

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

5.17.2 Правила групповой адресации (multicast addressing)

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

Команды режима конфигурации интерфейса VLAN

Вид запроса командной строки в режиме конфигурации интерфейса VLAN:

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

Таблица 115 – Команды режима конфигурации интерфейса VLAN

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

bridge multicast forbidden ip-address *ip_multicast_address* **{add | remove} { tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Запрещает порту динамически добавляться к многоадресной группе. - *ip_multicast_address* – групповой IP-адрес; - **add** – добавление порта/портов к списку запрещенных; - **remove** – удаление порта/портов из списка запрещенных. Перечисление интерфейсов осуществляется через «–» и «,» **Прежде чем определить запрещенные порты, группы многоадресной рассылки должны быть зарегистрированы.**
no bridge multicast forbidden ip-address *ip_multicast_address*		Восстанавливает значение по умолчанию.
bridge multicast source *ip_address* **group** *ip_multicast_address* **{add | remove} { tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Устанавливает соответствие между IP-адресом пользователя и групповым адресом в таблице групповой адресации, и статически добавляет/удаляет интерфейсы из группы. - *ip_address* – исходный IP-адрес; - *ip_multicast_address* – групповой IP-адрес; - **add** – добавить порты в группу исходного IP-адреса; - **remove** – удалить порты из группы исходного IP-адреса.
no bridge multicast source *ip_address* **group** *ip_multicast_address*		Восстанавливает значение по умолчанию.
bridge multicast forbidden source *ip_address* **group** *ip_multicast_address* **{add | remove} { tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Устанавливает запрет на добавление/удаление соответствия между IP-адресом пользователя и групповым адресом в таблице групповой адресации для определенного порта. - *ip_address* – исходный IP-адрес; - *ip_multicast_address* – групповой IP-адрес; - **add** – запрет на добавление порта в группу исходного IP-адреса; - **remove** – запрет на удаление порта из группы исходного IP-адреса.
no bridge multicast forbidden source *ip_address* **group** *ip_multicast_address*		Восстанавливает значение по умолчанию.
bridge multicast ipv6 mode {mac-group | ip-group | ip-src-group}	-/mac-group	Задает режим групповой передачи данных для IPv6-пакетов многоадресной рассылки. **- mac-group** – многоадресная передача, основанная на VLAN и MAC-адресах; - **ip-group** – многоадресная передача с типом фильтрации, основанным на VLAN и адресе приемника в формате IPv6; - **ip-src-group** – многоадресная передача с типом фильтрации, основанным на VLAN и адресе отправителя в формате IPv6.
no bridge multicast ipv6 mode		Устанавливает значение по умолчанию.
bridge multicast ipv6 ip-address *ipv6_multicast_address* **{add | remove} { tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Регистрирует групповой IPv6-адрес в таблице групповой адресации, и статически добавляет/удаляет интерфейсы из группы. - *ipv6_multicast_address* – групповой IP-адрес; - **add** – добавляет порты к группе; - **remove** – удаляет порты из группы; Перечисление интерфейсов осуществляется через «–» и «,».
no bridge multicast ipv6 ip-address *ipv6_multicast_address*		Удаляет групповой IP-адрес из таблицы.
bridge multicast ipv6 forbidden ip-address *ipv6_multicast_address* **{add | remove} { tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Запрещает подключение настраиваемого порта/портов к групповому IPv6-адресу. - *ipv6_multicast_address* – групповой IP-адрес; - **add** – добавление порта/портов в список запрещенных; - **remove** – удаление порта/портов из списка запрещенных. Перечисление интерфейсов осуществляется через «–» и «,»
no bridge multicast ipv6 forbidden ip-address *ipv6_multicast_address*		Восстанавливает значение по умолчанию.

bridge multicast ipv6 source *ipv6_address* **group** *ipv6_multicast_address* **{add | remove} { tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Устанавливает соответствие между IPv6-адресом пользователя и групповым адресом в таблице групповой адресации, и статически добавляет/удаляет интерфейсы из группы. - *ipv6_address* – исходный IP-адрес; - *ipv6_multicast_address* – групповой IP-адрес; - **add** – добавить порты в группу исходного IP-адреса; - **remove** – удалить порты из группы исходного IP-адреса.
no bridge multicast ipv6 source *ipv6_address* **group** *ipv6_multicast_address*		Восстанавливает значение по умолчанию.
bridge multicast ipv6 forbidden source *ipv6_address* **group** *ipv6_multicast_address* **{add | remove} { tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Устанавливает запрет на добавление/удаление соответствия между IPv6-адресом пользователя и групповым адресом в таблице групповой адресации для определенного порта. - *ipv6_address* – исходный IPv6-адрес; - *ipv6_multicast_address* – групповой IPv6-адрес; - **add** – запрет на добавление порта в группу исходного IPv6-адреса; - **remove** – запрет на удаление порта из группы исходного IPv6-адреса.
no bridge multicast ipv6 forbidden source *ipv6_address* **group** *ipv6_multicast_address*		Восстанавливает значение по умолчанию.

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

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

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

Таблица 116 – Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 117 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Описание*
bridge multicast filtering	-/отключено	Включает фильтрацию групповых адресов.
no bridge multicast filtering		Отключает фильтрацию групповых адресов.
mac address-table aging-time *seconds*	seconds: (10..400)/300 секунд	Задает время хранения MAC-адреса в таблице глобально.

no mac address-table aging-time		Устанавливает значение по умолчанию.
mac address-table learning vlan *vlan_id*	vlan_id: (1..4094, all)/По умолчанию включено	Включить изучение MAC-адресов в данном VLAN.
no mac address-table learning vlan *vlan_id*		Отключить изучение MAC-адресов в данном VLAN.
mac address-table static *mac_address* **vlan** *vlan_id* **interface { tengigabitethernet** *te_port* **| port-channel** *group***} [permanent | delete-on-reset | delete-on-timeout | secure]**	vlan_id: (1..4094); te_port: (1..8/0/1..32); group: (1..32)	Добавляет исходный MAC-адрес в таблицу групповой адресации. - *mac_address* – MAC-адрес; - *vlan_id* – номер VLAN; - **permanent** – данный MAC-адрес можно удалить только с помощью команды **no bridge address;** - **delete-on-reset** – данный адрес удалится после перезагрузки устройства; - **delete-on-timeout** – данный адрес удалится по тайм-ауту; - **secure** – данный адрес удалится только с помощью команды **no bridge address** или после возвращения порта в режим обучения (**no port security**).
no mac address-table static [*mac_address***] vlan** *vlan_id*		Удаляет MAC-адрес из таблицы групповой адресации.
bridge multicast reserved-address *mac_multicast_address* **{ethernet-v2** *ethtype* **| llc** *sap* **| llc-snap** *pid* **] {discard | bridge}**	ethtype: (0x0600..0xFFFF); sap: (0..0xFFFF); pid: (0..0xFFFFFFFFFF)	Определяет действие для пакетов многоадресной рассылки с зарезервированного адреса. - *mac_multicast_address* – групповой MAC-адрес; - *ethtype* – тип пакета Ethernet v2; - *sap* – тип пакета LLC; - *pid* – тип пакета LLC-Snap; - **discard** – сброс пакетов; - **bridge** – пакеты передаются в режиме bridge.
no bridge multicast reserved-address *mac_multicast_address* **[ethernet-v2** *ethtype* **| llc** *sap* **| llc-snap** *pid***]**		Устанавливает значение по умолчанию.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 118 – Команды режима Privileged EXEC

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 119 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Описание*
show mac address-table [dynamic | static | secure] [vlan *vlan_id***] [interface { tengigabitethernet** *te_port* **| port-channel** *group***}] [address** *mac_address***]**	te_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094)	Показывает таблицу MAC-адресов для указанного интерфейса либо всех интерфейсов. - **dynamic** – просмотр только динамических записей; - **static** – просмотр только статических записей; - **secure** – просмотр только безопасных записей; - *vlan_id* – идентификационный номер VLAN; - mac-address – MAC-адрес.
show mac address-table count [vlan *vlan_id***] [interface { tengigabitethernet** *te_port* **| port-channel** *group***}]**	te_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094)	Показывает количество записей в таблице MAC-адресов для указанного интерфейса либо для всех интерфейсов. - *vlan_id* – идентификационный номер VLAN.
show bridge multicast address-table [vlan *vlan_id***] [address {***mac_multicast_address* **|** *ipv4_multicast_address* **|** *ipv6_multicast_address***}] [format {ip | mac}] [source {***ipv4_source_address* **|** *ipv6_source_address***}]**	vlan_id: (1..4094)	Показывает таблицу групповых адресов для указанного интерфейса либо всех интерфейсов VLAN (команда доступна только для привилегированного пользователя). - *vlan_id* – идентификационный номер VLAN; - *mac_multicast_address* – групповой MAC-адрес; - *ipv4_multicast_address* – групповой IPv4-адрес; - *ipv6_multicast_address* – групповой IPv6-адрес; - **ip** – просмотр по IP-адресам; - **mac** – просмотр по MAC-адресам; - *ipv4_source_address* – IPv4-адрес источника; - *ipv6_source_address* – IPv6-адрес источника.
show bridge multicast address-table static [vlan *vlan_id***] [address {***mac_multicast_address* **|** *ipv4_multicast_address* **|** *ipv6_multicast_address***} [source** *ipv4_source_address* **|** *ipv6_source_address***] [all | mac | ip]**	vlan_id: (1..4094)	Показывает таблицу статических групповых адресов для указанного интерфейса либо всех интерфейсов VLAN. - *vlan_id* – идентификационный номер VLAN; - *mac_multicast_address* – групповой MAC-адрес; - *ipv4_multicast_address* – групповой IPv4-адрес; - *ipv6_multicast_address* – групповой IPv6-адрес; - *ipv4_source_address* – IPv4-адрес источника; - *ipv6_source_address* – IPv6-адрес источника; - **ip** – просмотр по IP-адресам; - **mac** – просмотр по MAC-адресам; - **all** – просмотр полной таблицы.
show bridge multicast filtering *vlan_id*	vlan_id: (1..4094)	Показывает конфигурацию фильтра групповых адресов для указанного VLAN. - *vlan_id* – идентификационный номер VLAN.
show bridge multicast unregistered [tengigabitethernet *te_port* **| port-channel** *group***]**	te_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094)	Показывает конфигурацию фильтра для незарегистрированных групповых адресов.
show bridge multicast mode [vlan *vlan_id***]**	vlan_id: (1..4094)	Показывает режим групповой адресации для указанного интерфейса либо всех интерфейсов VLAN. - *vlan_id* – идентификационный номер VLAN.
show bridge multicast reserved-addresses	-	Отображает правила, установленные для групповых зарезервированных адресов.

Примеры выполнения команд

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

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

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

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

Forbidden ports for multicast addresses:

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

5.17.3 MLD snooping – протокол контроля многоадресного трафика в IPv6

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 120 – Команды глобального режима конфигурации

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

no ipv6 mld snooping vlan *vlan_id* **mrouter interface {tengigabitethernet** *te_port* **| port-channel** *group***}**		Удаляет mrouter-порты.
ipv6 mld snooping vlan *vlan_id* **immediate-leave**	vlan_id: (1..4094) -/выключено	Включить процесс MLD Snooping Immediate-Leave на текущей VLAN.
no ipv6 mld snooping vlan *vlan_id* **immediate-leave**		Отключить процесс MLD Snooping Immediate-Leave на текущей VLAN.
ipv6 mld snooping querier	-/выключено	Включает поддержку выдачи запросов igmp-query.
no ipv6 mld snooping querier		Отключает поддержку выдачи запросов igmp-query.

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

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

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

Таблица 121 – Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet, интерфейса группы портов, интерфейса VLAN

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 122 – Команды режима EXEC

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

5.17.4 Функция многоадресной маршрутизации IGMP Proxy

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

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

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

IGMP Proxy поддерживает до 512 downlink-интерфейсов.

Ограничения реализации функции IGMP Proxy:

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 123 – Команды режима глобальной конфигурации

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

Команды режима конфигурации интерфейсов Ethernet, VLAN, интерфейса группы портов

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

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

Таблица 124 – Команды режима конфигурации интерфейсов Ethernet, VLAN, группы портов

Команда	*Значение/Значение по умолчанию*	*Действие*
ip igmp-proxy {tengigabitethernet *te_port* **| port-channel** *group* **| vlan** *vlan_id***}**	te_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094)	Конфигурируемый интерфейс является интерфейсом к нижестоящей сети. Команда назначает связанный uplink-интерфейс, участвующий в маршрутизации.
ip igmp-proxy downstream protected interface { enable | disable }	-	Включить защиту по нисходящему интерфейсу. IPv4 multicast-трафик, поступающий на интерфейс, не будет перенаправлен.
no ip igmp-proxy downstream protected interface		Отключить защиту по нисходящему интерфейсу.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 125 – Команды режима EXEC

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

Примеры выполнения команд

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

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

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


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

5.18 Многоадресная маршрутизация – протокол PIM

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

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

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 126 – Команды глобального режима конфигурации

Команда	***Значение/Значение по умолчанию***	***Действие***
ip multicast-routing pim	-/По умолчанию функция выключена	Включить многоадресную маршрутизацию, протокол PIM на всех интерфейсах.
no ip multicast-routing pim		Отключить многоадресную маршрутизацию и протокол PIM.
ipv6 multicast-routing pim	-/По умолчанию функция выключена	Включить для IPv6 многоадресную маршрутизацию, протокол PIM на всех интерфейсах.
no ipv6 multicast-routing pim		Отключить для IPv6 многоадресную маршрутизацию и протокол PIM.
ip pim accept-register list *acc_list*	acc_list: (0..32) символа	Применение фильтрации регистрационных сообщений PIM. - *acc_list* – список многоадресных префиксов, задаваемый с помощью стандартного ACL.
no ip pim accept-register list		Отключение данного параметра.
ipv6 pim accept-register list *acc_list*	acc_list: (0..32) символа	Применение фильтрации регистрационных сообщений PIM для IPv6. - *acc_list* – список многоадресных префиксов, задаваемый с помощью стандартного ACL.
no ipv6 pim accept-register list		Отключение данного параметра.
ip pim bsr-candidate *ip_address* **[***mask***] [priority** *priority_num***]**	mask: (8..32)/30; priority_num: (0..192)/0	Указать устройство как кандидата в BSR (bootstrap router). - *ip_address* – валидный IP-адрес коммутатора; - *mask* – маска подсети; - *priority_num* – приоритет.
no ip pim bsr-candidate		Отключение данного параметра.
ipv6 pim bsr-candidate *ipv6_address* **[***mask***] [priority** *priority_num***]**	mask: (8..128)/126; priority_num: (0..192)/0	Указать устройство как кандидата в BSR (bootstrap router). - *ipv6_address* – валидный IPv6-адрес коммутатора; - *mask* – маска подсети; - *priority_num* – приоритет.
no ipv6 pim bsr-candidate		Отключение данного параметра.
ip pim rp-address *unicast_address* **[***multicast_subnet***]**	-	Создание статической Rendezvous Point (RP), дополнительно можно указать многоадресную подсеть для данной RP. - *unicast_addr* – IP-адрес; - *multicast_subnet* – многоадресная подсеть.

no ip pim rp-address *unicast_address* [*multicast_subnet*]		Удаление статической RP или удаление RP для указанной подсети.
ipv6 pim rp-address *ipv6_unicast_address* [*ipv6_multicast_subnet*]	-	Создание статической Rendezvous Point (RP), дополнительно можно указать многоадресную подсеть для данной RP. - *ipv6_unicast_ addr* – IPv6-адрес; - *ipv6_multicast_ subnet* – многоадресная подсеть.
no ipv6 pim rp-address *ipv6_unicast_address* [*ipv6_multicast_subnet*]		Удаление статической RP или удаление RP для указанной подсети.
ip pim rp-candidate *unicast_address* **[group-list** *acc_list*] **[priority** *priority*] **[interval** *secs*]	acc_list: (0..32) символа priority: (0..192)/192; secs: (1..16383)/60 секунд	Создание кандидата для Rendezvous Point (RP) - *unicast_addr* – IP-адрес; - *acc_list* – список многоадресных префиксов, задаваемый с помощью стандартного ACL; - *priority* – приоритетность кандидата; - *secs* – период отправки сообщений.
no ip pim rp-candidate *unicast_address*		Отключение данного параметра.
ipv6 pim rp-candidate *ipv6_unicast_address* **[group-list** *acc_list*] **[priority** *priority*] **[interval** *secs*]	acc_list: (0..32) символа priority: (0..192)/192; secs: (1..16383)/60 секунд	Создание кандидата для Rendezvous Point (RP) - *ipv6_unicast_addr* –IPv6-адрес; - *acc_list* – список многоадресных префиксов, задаваемый с помощью стандартного ACL; - *priority* – приоритетность кандидата; - *secs* – период отправки сообщений.
no ipv6 pim rp-candidate *ipv6_unicast_address*		Отключение данного параметра.
ip pim ssm {range *multicast_subnet* **| default}**	-	Указать многоадресную подсеть - **range** – указать многоадресную подсеть; - *multicast_subnet* – многоадресная подсеть; - **default** – указать диапазон в 232.0.0.0/8.
no ip pim ssm [range *multicast_subnet* **| default]**		Отключение данного параметра.
ipv6 pim ssm {range *ipv6_multicast_subnet* **| default}**	-	Указать многоадресную подсеть - **range** – указать многоадресную подсеть; - *ipv6_multicast_subnet* – многоадресная подсеть; - **default** – указать диапазон в FF3E::/32.
no ipv6 pim ssm [range *ipv6_multicast_subnet* **| default]**	-	Отключение данного параметра.
ipv6 pim rp-embedded	-/включено	Включить расширенный функционал rendezvous point (RP).
no ipv6 pim rp-embedded		Отключить расширенный функционал rendezvous point (RP).

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки:

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

Таблица 127 – Команды режима конфигурации интерфейса Ethernet

Команда	***Значение/ Значение по умолчанию***	***Действие***
ip (ipv6) pim	-/включено	Включение PIM на интерфейсе.
no ip (ipv6) pim		Выключение PIM на интерфейсе.
ip (ipv6) pim bsr-border	-/отключено	Прекратить передачу BSR-сообщений с интерфейса.
no ip pim bsr-border		Отключение данного параметра.
ip (ipv6) pim dr-priority *priority*	priority: (0..4294967294)/1	Указание приоритета для выбора DR-роутера. - *priority* – приоритет DR-роутера определяющий, кто из коммутаторов станет DR-роутером. Коммутатор с наибольшим значением станет DR-роутером.
no ip (ipv6) pim dr-priority		Возвращает значение по умолчанию.

ip ip (ipv6) pim hello-interval *secs*	secs: (1..18000)/30 сек	Указание периода отправки hello-пакетов. - *sec* – период отправки hello-пакетов.
no ip (ipv6) pim hello-interval		Возвращает значение по умолчанию.
ip (ipv6) pim join-prune-interval *interval*	interval: (1..18000)/60 секунд	Указать интервал, в течение которого коммутатор отсылает join или prune-сообщения. - *interval* – период времени отправки join, prune сообщений.
no ip (ipv6) pim join-prune-interval		Возвращает значение по умолчанию.
ip (ipv6) pim neighbor-filter *acc_list*	acc_list: (0..32) символа	Фильтрация входящих PIM-сообщений. - *acc_list* – список адресов, на основе которых производится фильтрация.
no ip (ipv6) pim neighbor-filter		Отключение данного параметра.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 128 – Команды режима EXEC

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

Пример использования команд

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

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

5.19 Функции управления

5.19.1 Механизм AAA

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

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

Для шифрования данных используется *механизм SSH.*

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 129 – Команды режима глобальной конфигурации

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

		фикации; - *tacacs* – использовать список TACACS-серверов для аутентификации. **Если метод аутентификации не определен, то доступ к консоли всегда успешный.** **Создание списка осуществляется командой: aaa authentication login list-name method_list. Использование списка: aaa authentication login list-name** **Во избежание потери доступа следует вводить необходимый минимум настроек для указываемого метода аутентификации.**
no aaa authentication enable authorization {default | *list_name*}		Устанавливает значение по умолчанию.
enable password *password* **[encrypted] [level** *level***]**	level: (1..15)/1; password: (0..159) символов	Устанавливает пароль для контроля изменения привилегий доступа пользователей. - *level* – уровень привилегий; - *password* – пароль; - *encrypted* – задать зашифрованный пароль (например, пароль в зашифрованном виде, скопированный с другого устройства).
no enable password [level *level***]**		Удаляет пароль для соответствующего уровня привилегий.
username *name* **{nopassword | password** *password* **| password encrypted** *encrypted_password***} [priveliged** *level***]**	name: (1..20) символов; password: (1..64) символов; encrypted_password: (1..64) символов; level: (1..15)	Добавляет пользователя в локальную базу данных. - *level* – уровень привилегий; - *password* – пароль; - *name* – имя пользователя; - *encrypted_password* –зашифрованный пароль (например, пароль в зашифрованном виде, скопированный с другого устройства).
no username *name*		Удаляет пользователя из локальной базы данных
aaa accounting login start-stop group {radius | tacacs+}	-/По умолчанию ведение учета запрещено	Разрешает ведение учета (аккаунта) для сессий управления. **Ведение учета разрешено только для пользователей, вошедших в систему по имени и паролю, для пользователей, вошедших по паролю терминала, ведение учета запрещено.** **Ведение учета активируется и прекращается, когда пользователь входит и отключается от системы, что соответствует значениям start и stop в сообщениях протокола RADIUS (параметры, содержащиеся в сообщениях протокола RADIUS, приведены в таблице 130).**
no aaa accounting login start-stop		Запрещает ведение учета (аккаунта) для введенных в CLI команд.
aaa accounting dot1x start-stop group radius	-/По умолчанию ведение учета запрещено	Разрешает ведение учета (аккаунта) для сессий 802.1x. **Ведение учета активируется и прекращается, когда пользователь входит и отключается от системы, что соответствует значениям start и stop в сообщениях протокола RADIUS (параметры, содержащиеся в сообщениях протокола RADIUS приведены в таблице 130).** **В режиме Multiple sessions сообщения stat/stop посылаются для каждого пользователя, в режиме Multiple hosts – только для пользователя, прошедшего аутентификацию (см. раздел по 802.1x).**
no aaa accounting dot1x start-stop group radius		Устанавливает значение по умолчанию.
aaa accounting commands stop-only group tacacs+	-/По умолчанию ведение учета команд выключено	Включает ведение учета введенных в CLI команд по протоколу Tacacs+.
no aaa accounting commands stop-only group		Устанавливает значение по умолчанию.

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

Таблица 130 – Атрибуты сообщений ведения учета протокола RADIUS для сессий управления

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

Таблица 131 – 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

Вид запроса командной строки в режиме конфигурации терминала:

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

Таблица 132 – Команды режима конфигурации терминальных сессий

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

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 133 – Команды режима Privileged EXEC

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Все команды данного раздела доступны только для привилегированных пользователей.

Таблица 134 – Команды режима EXEC

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

5.19.2 Протокол RADIUS

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

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 135 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
radius-server host {*ipv4-address* **|** *ipv6-address* **|** *hostname*} **[auth-port** *auth_port*] **[acct-port** *acct_port*] **[timeout** *timeout*] **[retransmit** *retries*] **[deadtime** *time*] **[key** *secret_key*] **[priority** *priority*] **[usage** *type*]	hostname: (1..158) символов; auth_port: (0..65535)/1812; acct_port: (0..65535)/1813; timeout: (1..30) сек; retries: (1..15); time (0..2000) мин; secret_key: (0..128) символов; priority: (0..65535)/0; type: (login, dot1.x, all)/all	Добавляет указанный сервер в список используемых RADIUS-серверов. - *ip_address* – IPv4 или IPv6-адрес RADIUS-сервера; - *hostname* – сетевое имя RADIUS-сервера; - *auth_port* – номер порта для передачи аутентификационных данных; - *acct_port* – номер порта для передачи данных учета; - *timeout* – интервал ожидания ответа от сервера; - *retries* – количество попыток поиска RADIUS-сервера; - *time* – время в минутах, в течение которого недоступные сервера не будут опрашиваться RADIUS-клиентом коммутатора; - *secret_key* – ключ для аутентификации и шифрования всего обмена данными RADIUS; - *priority* – приоритет использования RADIUS-сервера (чем ниже значение, тем приоритетнее сервер); - *type* – тип использования RADIUS-сервера; - **encrypted** – задать ключ в зашифрованном виде. В случае отсутствия в команде параметров *timeout*, *retries*, *time*, *secret_key* для данного RADIUS-сервера используются значения настроенные с помощью команд указанных ниже.
encrypted radius-server host {*ipv4-address* **|** *ipv6-address* **|** *hostname*} **[auth-port** *auth_port*] **[acct-port** *acct_port*] **[timeout** *timeout*] **[retransmit** *retries*] **[deadtime** *time*] **[key** *secret_key*] **[priority** *priority*] **[usage** *type*]		
no radius-server host {*ipv4-address* **|** *ipv6-address* **|** *hostname*}		Удаляет указанный сервер из списка используемых RADIUS-серверов.
[encrypted] radius-server key [*key***]**	key: (0..128) символов/по умолчанию ключ – пустая строка	Устанавливает ключ, используемый по умолчанию, для аутентификации и шифрования всего обмена данными RADIUS между устройством и окружением RADIUS. - **encrypted** – задать ключ в зашифрованном вид.
no radius-server key		Устанавливает значение по умолчанию.
radius-server timeout *timeout*	timeout: (1..30)/3 сек	Устанавливает интервал ожидания ответа от сервера, используемый по умолчанию.
no radius-server timeout		Устанавливает значение по умолчанию.
radius-server retransmit *retries*	retries: (1..15)/3	Определяет количество попыток, используемое по умолчанию, поиска RADIUS-сервера из списка серверов. При отказе осуществляется поиск следующего по приоритету сервера из списка.
no radius-server retransmit		Устанавливает значение по умолчанию
radius-server deadtime *deadtime*	deadtime: (0..2000)/0 мин	Позволяет оптимизировать время опроса RADIUS-серверов, когда некоторые сервера недоступны. Устанавливает время в минутах, используемое по умолчанию, в течение которого недоступные сервера не будут опрашиваться RADIUS-клиентом коммутатора.
no radius-server deadtime		Устанавливает значение по умолчанию.

radius-server host source-interface {tengigabitethernet *te_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan id***}**	vlan_id: (1..4094); te_port: (1..8/0/1..32); loopback_id: (1…64); group: (1..32)	Задает интерфейс устройства, IP-адрес которого будет использоваться по умолчанию в качестве адреса источника передаваемого в сообщениях протокола RADIUS.
no radius-server host source-interface		Удаляет интерфейс устройства.
radius-server host source-interface-ipv6 {tengigabitethernet *te_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan id***}**	vlan_id: (1..4094); te_port: (1..8/0/1..32); loopback_id: (1…64); group: (1..32)	Задает интерфейс устройства, IPv6-адрес которого будет использоваться по умолчанию в качестве адреса источника передаваемого в сообщениях протокола RADIUS.
no radius-server host source-interface-ipv6		Удаляет интерфейс устройства.

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 136 – Команды режима Privileged EXEC

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

Примеры использования команд

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

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

- Показать параметры настройки RADIUS-серверов

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

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

```
Global values
--------------

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

5.19.3 Протокол TACACS+

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

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

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 137 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
tacacs-server host {*ip_address* | *hostname*} **[single-connection] [port-number** *port*] **[timeout** *timeout*] **[key** *secret_key*] **[priority** *priority*]	hostname: (1..158) символов; port: (0..65535)/49; timeout: (1..30) сек; secret_key: (0..128) символов; priority: (0..65535)/0;	Добавляет указанный сервер в список используемых TACACS серверов. - *ip_address* – IP-адрес TACACS-сервера; - *hostname* – сетевое имя TACACS-сервера; - *single-connection* – в каждый момент времени иметь не больше одного соединения для обмена данными с TACACS-сервером; - *port* – номер порта для обмена данными с TACACS-сервером; - *timeout* – интервал ожидания ответа от сервера; - *secret_key* – ключ для аутентификации и шифрования всего обмена данными TACACS; - *priority* – приоритет использования TACACS-сервера (чем ниже значение, тем приоритетнее сервер); - **encrypted** – значение *secret_key* в зашифрованном виде. В случае отсутствия в команде параметров *timeout, secret_key* для данного TACACS-сервера используются значения, настроенные с помощью команд, указанных ниже.
encrypted tacacs-server host {*ip_address* | *hostname*} **[single-connection] [port-number** *port*] **[timeout** *timeout*] **[key** *secret_key*] **[priority** *priority*]		
no tacacs-server host {*ip_address* | *hostname*}		Удаляет указанный сервер из списка используемых TACACS-серверов.
tacacs-server key *key*	key: (0..128) символов/по умолчанию ключ – пустая строка	Устанавливает ключ, используемый по умолчанию, для аутентификации и шифрования всего обмена данными TACACS между устройством и окружением TACACS; - **encrypted** – значение *secret_key* в зашифрованном виде.
encrypted tacacs-server key *key*		
no tacacs-server key		Устанавливает значение по умолчанию.
tacacs-server timeout *timeout*	timeout: (1..30)/5 сек	Устанавливает интервал ожидания ответа от сервера, используемый по умолчанию.
no tacacs-server timeout		Установить значение по умолчанию.

tacacs-server host source-interface { tengigabitethernet *te_port* **| port-channel** *group* **| loopback** *loopback_id* **| tunnel** *tunnel* **| vlan** *vlan id}*	vlan_id: (1..4094); te_port: (1..8/0/1..32); loopback_id (1..64); tunnel (1-16); group: (1..32)	Задает интерфейс устройства, IP-адрес которого будет использоваться по умолчанию в качестве адреса источника для обмена сообщениями с TACACS-сервером.
no tacacs-server host source-interface		Удаляет интерфейс устройства.

Команды режима EXEC

Вид запроса командной строки в режиме EXEC:

```
console#
```

Таблица 138 – Команды режима EXEC

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

5.19.4 Протокол управления сетью (SNMP)

SNMP – технология, призванная обеспечить управление и контроль над устройствами и приложениями в сети связи путём обмена управляющей информацией между агентами, расположенными на сетевых устройствах, и менеджерами, находящимися на станциях управления. SNMP определяет сеть как совокупность сетевых управляющих станций и элементов сети (главные машины, шлюзы и маршрутизаторы, терминальные серверы), которые совместно обеспечивают административные связи между сетевыми управляющими станциями и сетевыми агентами.

Коммутаторы позволяют настроить работу протокола SNMP для удаленного мониторинга и управления устройством. Устройство поддерживает протоколы версий SNMPv1, SNMPv2, SNMPv3.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 139 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
snmp-server server	По умолчанию поддержка протокола SNMP отключена	Включить поддержку протокола SNMP.
no snmp-server server		Отключает поддержку протокола SNMP.
snmp-server community *community* **[ro | rw | su] [***ipv4_address* **|** *ipv6_address* **|** *ipv6z_address***] [mask** *mask* **| prefix** *prefix_length***]] [view** *view_name***]**	community: (1..20) символов; encrypted_community: (1..20) символов; формат ipv4_address:	Устанавливает значение строки сообщества для обмена данными по протоколу SNMP. - *community* – строка сообщества (пароль) для доступа по протоколу SNMP; - **encrypted** – задать строку сообщества в зашифрованном виде; - **ro** – доступ только для чтения;

snmp-server community-group *community group_name* **[***ipv4_address* **|** *ipv6_address* **|** *ipv6z_address***] [mask** *mask* **| prefix** *prefix_length***]**	A.B.C.D; формат ipv6_address: X:X:X:X::X; формат ipv6z_address: X:X:X:X::X%<ID>; mask: -/255.255.255.255; prefix_length: (1..32)/32; view_name: (1..30) символов; group_name: (1..30) символо	- **rw** – доступ для чтения и записи; - **su** – доступ администратора; - *view_name* – определяет имя для правила обозрения SNMP, которое должно быть предварительно определено с помощью команды **snmp-server view**. Определяет объекты, доступные сообществу; - *ipv4*_address, *ipv6_address*, *ipv6z_address* – IP-адрес устройства; - *mask* – маска адреса IPv4, которая определяет, какие биты адреса источника пакета сравниваются с заданным IP-адресом; - *prefix_length* – число бит, которые составляют префикс IPv4-адреса; - *group_name* – определяет имя группы, которое должно быть предварительно определено с помощью команды **snmp-server group**. Определяет объекты, доступные сообществу.
snmp-server view *view_name OID* **{included | excluded}**	view_name: (1..30) символов	Создает или редактирует правило обозрения для SNMP – разрешающее правило, либо ограничивающее серверу-обозревателю доступ к OID. - *OID* – идентификатор объекта MIB, представленный в виде дерева ASN.1 (строка вида 1.3.6.2.4, может включать в себя зарезервированные слова, например: system, dod). С помощью символа * можно обозначить семейство поддеревьев: 1.3.*.2); - **include** – OID включена в правило для обозревания; - **exclude** – OID исключена из правила для обозревания.
no snmp-server view *viewname* **[***OID***]**		Удаляет правило обозрения для SNMP.
encrypted snmp-server user *username groupname* {v3 | remote *host* v3 *[encrypted] [auth {md5|sha} auth-password] }*	username: (1..20) символов groupname: (1..30) символов engineid-string: (5..32) символов password: (1..32) символа md5: 16 или 32 байт sha: 20 или 36 байт формат IPv4: A.B.C.D IPv6: X:X:X:X::X IPv6z: X:X:X:X::X%<ID>	Создает SNMPv3- пользователя. - *username* – имя пользователя; - *groupname* – имя группы; - *engineid-string* – идентификатор удаленного SNMP-устройства, которому пользователь принадлежит; - *auth–password* – пароль для аутентификации и генерации ключа; - *md5* – ключ md5; - *sha*–ключ sha; - *host* – IP-адрес/ имя хоста.
no snmp-server user *username* [remote *engineid-string**]***		Удаляет SNMP-v3-пользователя.
snmp-server group *group_name* **{v1 | v2 | v3 {noauth | auth | priv} [notify** *notify_view***]} [read** *read_view***] [write** *write_view***]**	group_name: (1..30) символов; notify_view: (1..32) символов; read_view: (1..32) символов; write_view: (1..32) символов	Создает SNMP-группу или таблицу соответствий SNMP-пользователей и правил обозрений SNMP. - **v1**, **v2**, **v3** – SNMP v1, v2, v3 модель безопасности; - **noauth**, **auth**, **priv** – тип аутентификации, используемый протоколом SNMP v3 (**noauth** – без аутентификации, **auth** – аутентификация без шифрования, **priv** – аутентификация с шифрованием); - *notify_view* – имя правила обозрения, которому разрешено определять сообщения SNMP-агента – inform и trap; - *read_view* – имя правила обозрения, которому разрешено только чтение содержимого SNMP-агента коммутатора; - *write_view* – имя правила обозрения, которому разрешено вводить данные и конфигурировать содержимое SNMP-агента коммутатора.
no snmp-server group *groupname* **{v1 | v2 | v3 [noauth | auth | priv]}**		Удаляет SNMP-группу
snmp-server user *user_name group_name* **{v1 | v2c | v3 [remote {***ip_address* **|** *host***}]}**	user_name: (1..20) символов; group_name: (1..30)	Создает SNMPv3-пользователя. - *user_name* – имя пользователя; - *group_name* – имя группы.

no snmp-server user *user_name* **{v1 | v2c | v3 [remote {***ip_address* **|** *host***}]}**	символов	Удаляет SNMPv3-пользователя.
snmp-server filter *filter_name OID* **{included | excluded}**	filter_name: (1..30) символов	Создает или редактирует правило SNMP-фильтра, которое позволяет фильтровать inform и trap-сообщения, передаваемые SNMP-серверу. - *filter_name* – имя SNMP-фильтра; - *OID* – идентификатор объекта MIB, представленный в виде дерева ASN.1 (строка вида 1.3.6.2.4, может включать в себя зарезервированные слова, например: system, dod. С помощью символа * можно обозначить семейство поддеревьев: 1.3.*.2); - **include** – OID включена в правило фильтрации; - **exclude** – OID исключена из правила фильтрации.
no snmp-server filter *filter_name* **[***OID***]**		Удаляет правило SNMP-фильтра.
snmp-server host {*ipv4_address* **|** *ipv6_address* **|** *hostname***} [traps | informs] [version {1 | 2c | 3 {noauth | auth | priv}] {***community* **|** *username***} [udp-port** *port***] [filter** *filter_name***] [timeout** *seconds***] [retries** *retries***]**	hostname: (1..158) символов; community: (1..20) символов; username: (1..20) символов port: (1..65535)/162; filter_name: (1..30) символов; seconds: (1..300)/15; retries: (0..255)/3	Определяет настройки для передачи сообщений уведомления inform и trap SNMP-серверу. - *community* – строка сообщества SNMPv1/2c для передачи сообщений уведомления; - *username* – имя пользователя SNMPv3 для аутентификации; - **version** – определят тип сообщений trap – trap SNMPv1, trap SNMPv2, trap SNMPv3; - **auth** – указывает подлинность пакета без шифрования; - **noauth** – не указывает подлинность пакета; - **priv** – указывает подлинность пакета с шифрованием; - *port* – UDP-порт SNMP-сервера; - *seconds* – период ожидания подтверждений перед повторной передачей сообщений inform; - *retries* – количество попыток передачи сообщений inform, при отсутствии их подтверждения.
no snmp-server host {*ipv4_address* **|** *ipv6_address* **|** *hostname***} [traps | informs]**		Удаляет настройки для передачи сообщений уведомления inform и trap SNMPv1/v2/v3-серверу.
snmp-server engineid local {*engineid_string* **| default}**	engineid_string: (5..32) символов	Создает идентификатор локального SNMP-устройства – engineID. - *engineid_string* – имя SNMP-устройства; - **default** – при использовании данной настройки engine ID будет автоматически создан на основе MAC-адреса устройства.
no snmp-server engineid local		Удаляет идентификатор локального SNMP-устройства – engine ID
snmp-server source-interface {traps | informs} { tengigabitethernet *te_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan id***}**	te_port: (1..8/0/1..32); loopback_id: (1..64) group: (1..32)	Задает интерфейс устройства, IP-адрес которого будет использоваться по умолчанию в качестве адреса источника для обмена сообщениями с SNMP-сервером.
no snmp-server source-interface [traps | informs]		Удаляет интерфейс устройства.
snmp-server source-interface-ipv6 {traps | informs} { tengigabitethernet *te_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan id***}**	te_port: (1..8/0/1..32); loopback_id: (1..64) group: (1..32)	Аналогично для IPv6.
no snmp-server source-interface-ipv6 [traps | informs]		Удаляет интерфейс устройства.
snmp-server engineid remote {*ipv4_address* **|** *ipv6_address* **|** *hostname***}** *engineid_string*	hostname: (1..158) символов; engineid_string: (5..32) символов	Создает идентификатор удаленного SNMP-устройства – engine ID. - *engineid_string* – идентификатор SNMP-устройства.
no snmp-server engineID remote {*ipv4_address* **|** *ipv6_address* **|** *hostname***}**		Удаляет идентификатор удаленного SNMP-устройства – engine ID.
snmp-server enable traps	-/включено	Включает поддержку SNMP trap-сообщений.

no snmp-server enable traps		Отключает поддержку SNMP trap-сообщений.
snmp-server enable traps ospf	-/включено	Включает отправку SNMP trap-сообщений протокола OSPF.
no snmp-server enable traps ospf		Отключает отправку SNMP trap-сообщений.
snmp-server enable traps ipv6 ospf	-/включено	Включает отправку SNMP trap-сообщений протокола OSPF (IPv6).
no snmp-server enable traps ipv6 ospf		Отключает отправку SNMP trap-сообщений.
snmp-server enable traps erps	-/включено	Включает отправку SNMP trap-сообщений протокола ERPS
no snmp-server enable traps erps		Отключает отправку SNMP trap-сообщений протокола ERPS
snmp-server trap authentication	-/разрешено	Разрешает передавать сообщения trap серверу, который не прошел аутентификацию.
no snmp-server trap authentication		Запрещает передавать сообщения trap серверу, который не прошел аутентификацию.
snmp-server contact *text*	text: (1..160) символов	Определяет контактную информацию устройства.
no snmp-server contact		Удаляет контактную информацию устройства.
snmp-server location *text*	text: (1..160) символов	Определяет информацию о местоположении устройства.
no snmp-server location		Удаляет информацию о местоположении устройства.
snmp-server set *variable_name name1 value1* **[***name2 value2* **[…]]**	variable_name, name, value должны задаваться в соответствии со спецификацией	Позволяет установить значения переменных в базе данных MIB коммутатора. - *variable_name* – имя переменной; - *name*, *value* – пары соответствий имя – значение.

Команды режима конфигурации интерфейса (диапазона интерфейсов) 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***
snmp trap link-status	-/включено	Включает отправку SNMP trap-сообщений при изменении состояния настраиваемого порта.
no snmp trap link-status		Выключает отправку SNMP trap-сообщений при изменении состояния настраиваемого порта.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

Таблица 141 – Команды режима Privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show snmp	-	Показывает статус SNMP-соединений.
show snmp engineID	-	Показывает идентификатор локального SNMP-устройства – engineID.
show snmp views [*view_name***]**	view_name: (1..30) символов	Показывает правила обозрения SNMP.
show snmp groups [*group_name***]**	group_name: (1..30) символов	Показывает SNMP-группы.
show snmp filters [*filter_name***]**	filter_name: (1..30) символов	Показывает SNMP-фильтры.
show snmp users [*user_name***]**	user_name: (1..30) символов	Показывает SNMP-пользователей.

5.19.5 Протокол удалённого мониторинга сети (RMON)

Протокол мониторинга сети (RMON) является расширением протокола SNMP, позволяя предоставить более широкие возможности контроля сетевого трафика. Отличие RMON от SNMP состоит в характере собираемой информации – данные собираемые RMON в первую очередь характеризуют трафик между узлами сети. Информация, собранная агентом, передается в приложение управления сетью.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 142 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
rmon event *index type* **[**community *com_text*] [**description** *desc_text*] [**owner** *name*]	index: (1..65535); type: (none, log, trap, log-trap); com_text: (0..127) символов; desc_text: (0..127) символов; **name: строка**	Настраивает события, используемые в системе удаленного мониторинга. - *index* – индекс события; - *type* – тип уведомления, генерируемого устройством по этому событию: none – не генерировать уведомления, log – генерировать запись в таблице, trap – отсылать SNMP trap, log-trap – генерировать запись в таблице и отсылать SNMP trap; - *com_text* - строка сообщества SNMP для пересылки trap; - *desc_text* – описание события; **-** *name* – имя создателя события.
no rmon event *index*		Удаляет событие, используемое в системе удаленного мониторинга.
rmon alarm *index mib_object_id interval rthreshold fthreshold revent fevent* **[type** *type***] [startup** *direction***] [owner** *name***]**	index: (1..65535); mib_object_id: корректный OID; interval: (1..2147483647) сек; rthreshold: (0..2147483647); fthreshold: (0..2147483647); revent: (1..65535); fevent: (0..65535); type: (absolute, delta)/absolute; startup: (rising, falling, rising-falling)/rising-falling; name: строка	Настраивает условия выдачи аварийных сигналов. - *index* – индекс аварийного события; - *mib_object_id* – идентификатор переменной части объекта OID; - *interval* – интервал, в течение которого данные отбираются и сравниваются с восходящей и нисходящей границами; - *rthreshold* – восходящая граница; - *fthreshold* – нисходящая граница; - *revent* – индекс события, которое используется при пересечении восходящей границы; - *fevent* – индекс события, которое используется при пересечении нисходящей границы; - *type* – метод отбора указанных переменных и подсчета значения для сравнения с границами: Метод **absolute** – абсолютное значение выбранной переменной будет сравнено с границей на конце исследуемого интервала; Метод **delta** – значение выбранной переменной при последнем отборе будет вычтено из текущего значения и разница будет сравнена с границами (разница между значениями переменной в конце и в начале контрольного интервала); - **startup** – инструкция для генерации событий на первом контрольном интервале. Определяет правила генерации аварийных событий для первого контрольного интервала путем сравнения отобранной переменной с одной, либо обеими границами: - **rising** – генерировать единичное аварийное событие по восходящей границе, если значение отобранной переменной на первом контрольном интервале больше либо равно этой границе; **- falling** – генерировать единичное аварийное событие по нисходящей границе, если значение отобранной переменной на первом контрольном интервале меньше либо равно этой границе;

		- **rising-falling** – генерировать единичное аварийное событие по восходящей и/или нисходящей границе, если значение отобранной переменной на первом контрольном интервале больше либо равно восходящей границе и/или меньше либо равно нисходящей границе; - **owner** – имя создателя аварийного события.
no rmon alarm *index*		Удаляет условие выдачи аварийных событий.
rmon table-size {history *hist_entries* **| log** *log_entries***}**	hist_entries: (20..32767)/270; log_entries: (20..32767)/100	Задает максимальный размер RMON-таблиц. - **history** – максимальное количество строк в таблице истории; - **log** – максимальное количество строк в таблице записей. **Значение вступит в силу только после перезагрузки устройства.**
no rmon table-size {history | log}		Устанавливает значение по умолчанию.

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

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

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

Таблица 143 – Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

Команда	*Значение/Значение по умолчанию*	*Действие*
rmon collection stats *index* **[owner** *name***] [buckets** *bucket_num***] [interval** *interval***]**	index: (1..65535); name: (0..160) символов; bucket-num: (1..50)/50; interval: (1..3600)/1800 сек	Включает формирование истории по группам статистики для базы данных (MIB) удаленного мониторинга. - *index* – индекс требуемой группы статистики; - *name* – владелец группы статистики; - *bucket_num* – значение, ассоциируемое с количеством ячеек для сбора истории по группе статистики; - *interval* – период опроса для формирования истории.
no rmon collection stats *index*		Выключает формирование истории по группам статистики для базы данных (MIB) удаленного мониторинга.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 144 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show rmon statistics { tengigabitethernet *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Показывает статистику интерфейса Ethernet, либо группы портов, используемую для удаленного мониторинга.
show rmon collection stats [tengigabitethernet *te_port* **| port-channel** *group***]**		Отображает информацию по запрашиваемым группам статистики.

show rmon history *index* **{throughput | errors | other} [period** *period***]**	index: (1..65535); period: (1..2147483647) сек	Показывает историю Ethernet статистики RMON. - *index* – запрошенная группа статистики; - **throughput** – показывает счетчики производительности (пропускной способности); - **errors** – показывает счетчики ошибок; - **other** – показывает счетчики обрывов и коллизий; - *period* – показывает историю за запрошенный период времени.
show rmon alarm-table	-	Показывает сводную таблицу аварийных событий.
show rmon alarm *index*	index: (1..65535)	Показывает конфигурацию настройки аварийных событий. -*index* – индекс аварийного события.
show rmon events	-	Показывает таблицу событий удаленного мониторинга RMON.
show rmon log [*index***]**	index: (0..65535)	Показывает таблицу записей удаленного мониторинга RMON. - *index*- индекс события.

Примеры выполнения команд

- Показать статистику 10 интерфейса Ethernet:

```
console# show rmon statistics tengigabitethernet 1/0/10
```

```
Port te0/10
Dropped: 8
Octets: 878128 Packets: 978
Broadcast: 7 Multicast: 1
CRC Align Errors: 0 Collisions: 0
Undersize Pkts: 0 Oversize Pkts: 0
Fragments: 0 Jabbers: 0
64 Octets: 98 65 to 127 Octets: 0
128 to 255 Octets: 0 256 to 511 Octets: 0
512 to 1023 Octets: 491 1024 to 1518 Octets: 389
```

Таблица 145 – Описание результатов

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

Jabbers	Количество принятых пакетов длиной больше 1518 байт (исключая фреймовые биты, но включая биты контрольной суммы), имеющих неверную контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы – FCS), либо с нецелым числом байт (ошибки выравнивания – Alignment).
64 Octet	Количество принятых пакетов (включая плохие пакеты) длиной 64 байта (исключая фреймовые биты, но включая биты контрольной суммы).
65 to 127 Octets	Количество принятых пакетов (включая плохие пакеты) длиной от 65 до 127 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы).
128 to 255 Octets	Количество принятых пакетов (включая плохие пакеты) длиной от 128 до 255 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы).
256 to 511 Octets	Количество принятых пакетов (включая плохие пакеты) длиной от 256 до 511 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы).
512 to 1023 Octets	Количество принятых пакетов (включая плохие пакеты) длиной от 512 до 1023 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы).
1024 to 1518 Octets	Количество принятых пакетов (включая плохие пакеты) длиной от 1024 до 1518 байт включительно (исключая фреймовые биты, но включая биты контрольной суммы).

- Показать информацию по группам статистики для порта 8:

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

Index Interface Interval Requested Samples Granted Samples        Owner
----- --------- -------- ----------------- --------------- -------------------
  1      te0/8     300           50               50               Eltex
```

Таблица 146 – Описание результатов

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

- Показать счетчики пропускной способности для группы статистики 1:

```
console# show rmon history 1 throughput

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

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

Таблица 147 – Описание результатов

Параметр	*Описание*
Time	Дата и время создания записи.
Octets	Количество байт данных (включая байты плохих пакетов) принятых из сети (исключая фреймовые биты, но включая биты контрольной суммы).

Packets	Количество принятых пакетов (включая плохие пакеты) в течение периода формирования записи.
Broadcast	Количество принятых хороших пакетов в течение периода формирования записи направленных на широковещательные адреса.
Multicast	Количество принятых хороших пакетов в течение периода формирования записи направленных на многоадресные адреса.
Utilization	Оценка средней пропускной способности физического уровня на данном интерфейсе в течение периода формирования записи. Пропускная способность оценивается величиной до тысячной процента.
CRC Align	Количество принятых в течение периода формирования записи пакетов длиной от 64 до 1518 байт включительно, имеющих неверную контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы – FCS), либо с нецелым числом байт (ошибки выравнивания – Alignment).
Collisions	Оценка количества коллизий на данном Ethernet сегменте в течение периода формирования записи.
Undersize Pkts	Количество принятых в течение периода формирования записи пакетов длиной меньше 64 байт (исключая фреймовые биты, но включая биты контрольной суммы), но в остальном правильно сформированных.
Oversize Pkts	Количество принятых в течение периода формирования записи пакетов длиной больше 1518 байт (исключая фреймовые биты, но включая биты контрольной суммы), но в остальном правильно сформированных.
Fragments	Количество принятых в течение периода формирования записи пакетов длиной меньше 64 байт (исключая фреймовые биты, но включая биты контрольной суммы), имеющих неверную контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы – FCS), либо с нецелым числом байт (ошибки выравнивания – Alignment).
Jabbers	Количество принятых в течение периода формирования записи пакетов длиной больше 1518 байт (исключая фреймовые биты, но включая биты контрольной суммы), имеющих неверную контрольную сумму либо с целым числом байт (ошибки проверки контрольной суммы – FCS), либо с нецелым числом байт (ошибки выравнивания – Alignment).
Dropped	Количество задетектированных событий, когда пакеты были отброшены в течение периода формирования записи.

- Показать сводную таблицу сигналов тревоги:

```
console# show rmon alarm-table
```

```
Index  OID                           Owner
-----  ----------------------------  -------
1      1.3.6.1.2.1.2.2.1.10.1        CLI
2      1.3.6.1.2.1.2.2.1.10.1        Manager
```

Таблица 148 – Описание результатов

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

- Показать конфигурацию аварийных событий с индексом 1:

```
console# show rmon alarm 1
```

```
Alarm 1
-------
OID: 1.3.6.1.2.1.2.2.1.10.1
Last sample Value: 878128
Interval: 30
Sample Type: delta
Startup Alarm: rising
Rising Threshold: 8700000
Falling Threshold: 78
Rising Event: 1
Falling Event: 1
Owner: CLI
```

Таблица 149 – Описание результатов

Параметр	*Описание*
OID	OID контролируемой переменной.
Last Sample Value	Значение переменной на последнем контрольном интервале. Если метод отбора переменных **absolute** – то это абсолютное значение переменной, если **delta** – то разница между значениями переменной в конце и в начале контрольного интервала.
Interval	Интервал в секундах, в течение которого данные отбираются и сравниваются с верхней и нижней границами.
Sample Type	Метод отбора указанных переменных и подсчета значения для сравнения с границами. Метод **absolute** – абсолютное значение выбранной переменной будет сравнено с границей на конце исследуемого интервала. Метод **delta** – значение выбранной переменной при последнем отборе будет вычтено из текущего значения, и разница будет сравнена с границами (разница между значениями переменной в конце и в начале контрольного интервала).
Startup Alarm	Инструкция для генерации событий на первом контрольном интервале. Определяет правила генерации аварийных событий для первого контрольного интервала путем сравнения отобранной переменной с одной, либо обеими границами. **rising** – генерировать единичное аварийное событие по восходящей границе, если значение отобранной переменной на первом контрольном интервале большем либо равном этой границе. **falling** – генерировать единичное аварийное событие по нисходящей границе, если значение отобранной переменной на первом контрольном интервале меньше либо равно этой границе. **rising-falling** – генерировать единичное аварийное событие по восходящей и/или нисходящей границе, если значение отобранной переменной на первом контрольном интервале больше либо равно восходящей границе, и/или меньше либо равно нисходящей границе.
Rising Threshold	Значение восходящей границы. Когда значение отобранной переменной на предыдущем контрольном интервале было меньше данной границы, а на текущем контрольном интервале большем либо равном значению границы, тогда единичное событие генерируется.
Falling Threshold	Значение нисходящей границы. Когда значение отобранной переменной на предыдущем контрольном интервале было больше данной границы, а на текущем контрольном интервале меньше либо равно значению границы, тогда единичное событие генерируется.
Rising Event	Индекс события использующегося, когда восходящая граница пересечена.
Falling Event	Индекс события использующегося, когда нисходящая граница пересечена.
Owner	Пользователь, создавший запись.

- Показать таблицу событий удаленного мониторинга RMON:

```
console# show rmon events
```

```
Index  Description    Type        Community    Owner      Last time sent
-----  -----------    ----------  ----------   --------   ------------------
1      Errors         Log                      CLI        Nov 10 2009 18:47:17
2      High Broadcast Log-Trap    router       Manager    Nov 10 2009 18:48:48
```

Таблица 150 – Описание результатов

Параметр	*Описание*
Index	Индекс, уникально идентифицирующий событие.
Description	Комментарий, описывающий событие.
Type	Тип уведомления, генерируемого устройством по этому событию: none – не генерировать уведомления, log – генерировать запись в таблице, trap – отсылать SNMP trap, log-trap – генерировать запись в таблице и отсылать SNMP trap.
Community	Строка сообщества SNMP для пересылки trap.
Owner	Пользователь, создавший событие.
Last time sent	Время и дата генерирования последнего события. Если не было сгенерировано событий, то это значение будет равно нулю.

Показать таблицу записей удаленного мониторинга RMON:

```
console# show rmon log
```

```
Maximum table size: 100
Event Description Time
----- ----------- --------------------
1     Errors      Nov 10 2009 18:48:33
```

Таблица 151 – Описание результатов

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

5.19.6 Списки доступа ACL для управления устройством

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 152 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
management access-list *name*	name: (1..32) символа	Создает список доступа для управления. Вход в режим конфигурации списка доступа для управления.
no management access-list *name*		Удаляет список доступа для управления.
management access-class {console-only | *name***}**	name: (1..32) символа	Ограничивает управление устройством по определенному списку доступа (access list). Активирует указанный список доступа. - **console-only** – управление устройством доступно только с консоли.
no management access-class		Отменяет ограничение на управление устройством по определенному списку доступа (access list).

Команды режима конфигурации списка доступа для управления

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

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

Таблица 153 – Команды режима конфигурации списка доступа для управления

Команда	*Значение/Значение по умолчанию*	*Действие*
permit [tengigabitethernet *te_port* **| port-channel** *group* **| oob | vlan** *vlan_id***] [service** *service* **]**	te_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094) service: (telnet, snmp, http, https, ssh);	Задает разрешающее условие для управляющего списка доступа. - *service* – тип доступа.
permit ip-source {*ipv4_address* **|** *ipv6_address/prefix_length***} [mask {***mask* **|** *prefix_length***}] [tengigabitethernet** *te_port* **| port-channel** *group* **| oob | vlan** *vlan_id***] [service** *service***]**		
deny [tengigabitethernet *te_port* **| port-channel** *group* **| oob | vlan** *vlan_id***] [service** *service***] [ace-priority** *index***]**	te_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094); service: (telnet, snmp, http, https, ssh);	Задает запрещающее условие для управляющего списка доступа. - *service* – тип доступа,
deny ip-source {*ipv4_address* **|** *ipv6_address/prefix_length***} [mask {***mask* **|** *prefix_length***}] [tengigabitethernet** *te_port* **| port-channel** *group* **| oob | vlan** *vlan_id***] [service** *service***]**		

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 154 – Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show management access-list [*name*]	name: (1..32) символа	Показывает списки доступа (access list) для управления.
show management access-class	-	Показывает информацию об активных списках доступа (access list) для управления.

5.19.7 Настройка доступа

5.19.7.1 Telnet, SSH, HTTP и FTP

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 155 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip telnet server	По умолчанию Telnet сервер включен	Разрешает удаленное конфигурирование устройства через Telnet.
no ip telnet server		Запрещает удаленное конфигурирование устройства через Telnet.
ip ssh server	По умолчанию SSH сервер отключен	Разрешает удаленное конфигурирование устройства через SSH. **До тех пор, пока ключ для шифрования не сгенерирован, SSH-сервер будет находиться в резерве. После генерации ключа (используемые команды crypto key generate rsa и crypto key generate dsa) сервер перейдет в рабочее состояние.**
no ip ssh server		Запрещает удаленное конфигурирование устройства через SSH.
ip ssh port *port_number*	port_number: (1..65535)/22	TCP-порт, используемый SSH-сервером.
no ip ssh port		Устанавливает значение по умолчанию.
ip ssh-client source-interface { tengigabitethernet *te_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan_id***}**	te_port: (1..8/0/1..32); loopback_id: (1..64) group: (1..32); vlan_id: (1..4094)	Задает интерфейс для SSH-сессий.
no ip ssh-client source-interface		Удаляет интерфейс.
ipv6 ssh-client source-interface { tengigabitethernet *te_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan_id***}**	te_port: (1..8/0/1..32); loopback_id: (1..64) group: (1..32); vlan_id: (1..4094)	Задает интерфейс для IPv6 SSH-сессий.
no ipv6 ssh-client source-interface		Удаляет интерфейс.
ip ssh pubkey-auth	По умолчанию использование публичного ключа запрещено	Разрешает использование публичного ключа для входящих SSH-сессий.
no ip ssh pubkey-auth		Запрещает использование публичного ключа для входящих SSH-сессий.
ip ssh password-auth	По умолчанию	Включение режима аутентификации по паролю

no ip ssh password-auth	включено	Отключение режима аутентификации по паролю
crypto key pubkey-chain ssh	По умолчанию ключ не создан	Вход в режим конфигурации публичного ключа.
crypto key generate dsa	-	Генерирует пару ключей DSA – частный и публичный для SSH-сервиса. **Если хотя бы один из пары ключей уже создан, то система предложит перезаписать ключ.**
crypto key generate rsa	-	Генерирует пару ключей RSA – частный и публичный для SSH-сервиса. **Если хотя бы один из пары ключей уже создан, то система предложит перезаписать ключ.**
crypto key import dsa **encrypted crypto key import dsa**	-	Импортирует пару ключей DSA - encrypted –в зашифрованном виде.
crypto key import rsa **encrypted crypto key import rsa**	-	Импортирует пару ключей RSA - encrypted –в зашифрованном виде.
crypto certificate {1 | 2} generate	-	Генерирует SSL-сертификат.
no crypto certificate {1 | 2}		Восстанавливает SSL-сертификат по умолчанию для указанного сертификата.

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

Команды режима конфигурации публичного ключа

Вид запроса командной строки в режиме конфигурации публичного ключа:

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

Таблица 156 – Команды режима конфигурации публичного ключа

Команда	*Значение/Значение по умолчанию*	*Действие*
user-key *username* **{rsa | dsa}**	username: (1..48) символов	Вход в режим создания индивидуального публичного ключа. - **rsa** – создать RSA-ключ; - **dsa** – создать DSA-ключ.
no user-key *username*		Удаляет публичный ключ для определенного пользователя.

Вид запроса командной строки в режиме создания индивидуального публичного ключа:

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

Таблица 157 – Команды режима создания индивидуального публичного ключа

Команда	*Значение/Значение по умолчанию*	*Действие*
key-string	-	Создает публичный ключ для определенного пользователя.

key-string row *key_string*	-	Создает публичный ключ для определенного пользователя. Ввод ключа осуществляется построчно. - *key_string* – часть ключа. **Для того чтобы система поняла, что ключ введен полностью, необходимо ввести команду key-string row без символов.**

Команды режима EXEC

Команды данного раздела доступны только для привилегированных пользователей.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 158 – Команды режима EXEC

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

Примеры выполнения команд

Включить сервер SSH на коммутаторе. Разрешить использование публичных ключей. Создать RSA-ключ для пользователя **eltex**:

```
console# configure
console(config)# ip ssh server
console(config)# ip ssh pubkey-auth
console(config)# crypto key pubkey-chain ssh
console(config-pubkey-chain)# user-key eltex rsa
console(config-pubkey-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWlAl4kpqIw9GBRonZQZxjHKcqKL6rMlQ+ZNXf
ZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1gkTwml75Q
R9gHujS6KwGN2QWXgh3ub8gDjTSqmuSn/Wd05iDX2IExQWu08licglk02LYciz+Z4TrEU/9FJx
wPiVQOjc+KBXuR0juNg5nFYsY0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA6w9o44t6+AINEICB
CCA4YcF6zMzaT1wefWwX6f+Rmt5nhhqdAtN/4oJfce166DqVX1gWmNzNR4DYDvSzg0lDnwCAC8
Qh
Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

5.19.7.2 Команды конфигурации терминала

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 159 – Команды режима глобальной конфигурации

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

Команды режима конфигурации терминала

Вид запроса командной строки в режиме конфигурации терминала

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

Таблица 160 – Команды режима конфигурации терминала

Команда	*Значение/Значение по умолчанию*	*Действие*
speed *bps*	bps: (4800, 9600, 19200, 38400, 57600, 115200)/115200 бод	Устанавливает скорость доступа по локальной консоли (команда доступна только в режиме конфигурации локальной консоли).
no speed		Устанавливает значение по умолчанию.
autobaud	-/включено	Включает автоматическое определение скорости доступа по локальной консоли (команда доступна только в режиме конфигурации локальной консоли).
no autobaud		Выключает автоматическое определение скорости доступа по локальной консоли.
exec-timeout *minutes* **[***seconds***]**	minutes*:* (0..65535)/10 мин; seconds*:* (0..59)/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.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 161 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show line [console | telnet | ssh]	-	Показывает параметры терминала.

5.20 Журнал аварий, протокол SYSLOG

Системные журналы позволяют вести историю событий, произошедших на устройстве, а также контролировать произошедшие события в реальном времени. В журнал заносятся события семи типов: чрезвычайные, сигналы тревоги, критические и не критические ошибки, предупреждения, уведомления, информационные и отладочные.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 162 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
logging on	-/регистрация включена	Включает регистрацию отладочных сообщений и сообщений об ошибках.
no logging on		Выключает регистрацию отладочных сообщений и сообщений об ошибках. **При выключенной регистрации отладочные сообщения и сообщения об ошибках будут передаваться на консоль.**
logging host {*ip_address* **|** *host***} [port** *port***] [severity** *level***] [facility** *facility***] [description** *text***]**	host: (1..158) символов; port: (1..65535)/514; level: (см.Таблица 163); facility: (local0..7)/local7; text: (1..64) символов	Включает передачу аварийных и отладочных сообщений на удаленный SYSLOG сервер. - ip_*address*– IPv4 или IPv6-адрес SYSLOG-сервера; - *host* – сетевое имя SYSLOG-сервера; - *port* – номер порта для передачи сообщений по протоколу SYSLOG; - *level* – уровень важности сообщений, передаваемых на SYSLOG-сервер; - *facility* – услуга, передаваемая в сообщениях; - *text* – описание SYSLOG-сервера.
no logging host {*ip_address* **|** *host***}**		Удаляет выбранный сервер из списка используемых SYSLOG-серверов.
logging console [*level***]**	level: (Таблица 163)/informational	Включает передачу аварийных или отладочных сообщений выбранного уровня важности на консоль.
no logging console		Выключает передачу аварийных или отладочных сообщений на консоль.
logging buffered [*severity_level***]**	severity_level: (Таблица 163)/informational	Включает передачу аварийных или отладочных сообщений выбранного уровня важности во внутренний буфер.
no logging buffered		Выключает передачу аварийных или отладочных сообщений во внутренний буфер.
logging buffered size *size*	size: (20..1000)/200	Изменяет количество сообщений, запоминаемых во внутреннем буфере. Новое значение размера буфера применится после перезагрузки устройства.
no logging buffered size		Устанавливает значение по умолчанию.
logging file [*level***]**	level: (Таблица 163) /errors	Включает передачу аварийных или отладочных сообщений выбранного уровня важности в файл журнала.
no logging file		Выключает передачу аварийных или отладочных сообщений в файл журнала.
aaa logging login	-/включено	Заносить в журналы события аутентификации, авторизации и учета (AAA).
no aaa logging login		Не заносить в журналы события аутентификации, авторизации и учета (AAA).
file-system logging {copy | delete-rename}	По умолчанию регистрация включена	Включает регистрацию событий файловой системы. -**copy** – регистрация сообщений, связанных с операциями копирования файлов; -**delete-rename** – регистрация сообщений, связанных с удалением файлов и переименованием операций.

no file-system logging {copy | delete-rename}		Выключает регистрацию событий файловой системы.
logging aggregation on	-/отключено	Включает контроль агрегации syslog-сообщений.
no logging aggregation on		Отключает агрегацию syslog-сообщений.
logging aggregation aging-time *sec*	sec: (15..3600)/300 секунд	Устанавливает время хранения сгруппированных syslog-сообщений.
no logging aggregation aging-time		Устанавливает значение по умолчанию.
logging service cpu-rate-limits *traffic*	traffic: (http, telnet, ssh, snmp, ip, link-local, arp-switch-mode, arp-inspection, stp-bpdu, other-bpdu, dhcp-snooping, dhcpv6-snooping, igmp-snooping, mld-snooping, sflow, log-deny-aces, vrrp)/-	Включает контроль ограничения скорости входящих фрейм-мов для определенного типа трафика.
no logging service cpu-rate-limits *traffic*		Отключает логирование.
logging origin-id {string | hostname | ip | ipv6}	-/нет	Задает параметр, который будет использоваться в качестве идентификатора хоста в syslog-сообщениях.
no logging origin-id		Использовать значение по умолчанию.
logging source-interface { tengigabitethernet *te_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan *vlan_id*}**	te_port: (1..8/0/1..32); loopback_id: (1..64) group: (1..32); vlan_id: (1..4094)	Использовать IP-адрес указанного интерфейса в качестве источника в IP-пакетах протокола SYSLOG.
no logging source-interface		Использовать IP-адрес исходящего интерфейса.
logging source-interface-ipv6 { tengigabitethernet *te_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan *vlan_id*}**	te_port: (1..8/0/1..32); loopback_id: (1..64) group: (1..32); vlan_id: (1..4094)	Использовать IPv6-адрес указанного интерфейса в качестве источника в IP-пакетах протокола SYSLOG.
no logging source-interface-ipv6		Использовать IPv6-адрес исходящего интерфейса.

Каждое сообщение имеет свой уровень важности; в таблице 163 приведены типы сообщений в порядке убывания их важности.

Таблица 163 – Типы важности сообщений

Тип важности сообщений	***Описание***
Чрезвычайные (emergencies)	В системе произошла критическая ошибка, система может работать неправильно.
Сигналы тревоги (alerts)	Необходимо немедленное вмешательство в систему.
Критические (critical)	В системе произошла критическая ошибка.
Ошибочные (errors)	В системе произошла ошибка.
Предупреждения (warnings)	Предупреждение, неаварийное сообщение.
Уведомления (notifications)	Уведомление системы, неаварийное сообщение.
Информационные (informational)	Информационные сообщения системы.
Отладочные (debugging)	Отладочные сообщения, предоставляют пользователю информацию для корректной настройки системы.

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 164 – Команда режима Privileged EXEC для просмотра файла журнала

Команда	*Значение/Значение по умолчанию*	*Действие*
clear logging	-	Удаляет все сообщения из внутреннего буфера.
clear logging file	-	Удаляет все сообщения из файла журнала.
show logging file	-	Отображает состояние журнала, аварийные и отладочные сообщения, записанные в файле журнала.
show logging	-	Отображает состояние журнала, аварийные и отладочные сообщения, записанные во внутреннем буфере.
show syslog-servers	-	Отображает настройки для удалённых syslog-серверов.

Примеры использования команд

- Включить регистрацию ошибочных сообщений на консоли:

```
console# configure
console (config)# logging on
console (config)# logging console errors
```

- Очистить файл журнала:

```
console# clear logging file
Clear Logging File [y/n]y
```

5.21 Зеркалирование (мониторинг) портов

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

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

К контролирующему порту применяются следующие ограничения:

- Порт не может быть контролирующим и контролируемым портом одновременно;
- Порт не может быть членом группы портов;
- IP-интерфейс должен отсутствовать для этого порта;
- Протокол GVRP должен быть выключен на этом порту.

К контролируемым портам применяются следующие ограничения:

- Порт не может быть контролирующим и контролируемым портом одновременно.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 165 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
monitor session *session_id* **destination interface tengigabitethernet** *te_port* **[network]**	session_id: (1..7); te_port: (1..8/0/1..32):	Указывает зеркалирующий порт для выбранной сессии мониторинга. network – позволяет вести обмен данными
no monitor session *session_id* **destination**		Выключает функцию мониторинга на настраиваемом интерфейсе.
monitor session *session_id* **destination remote vlan** *vlan_id* **reflector-port tengigabitethernet** *te_port* **network**	vlan_id: (1..4094); session_id: (1..7); te_port: (1..8/0/1..32):	Указывается служебный vlan для зеркалирования трафика с заданного рефлектор-порта для выбранной сессии. remote vlan – служебный vlan для зеркалирования трафика; reflector-port – физический порт для передачи зеркалируемого трафика, на этом интерфейсе не должен был прописан remote vlan.
no monitor session *session_id* **destination**		Выключает функцию мониторинга на настраиваемом интерфейсе.
monitor session *session_id* **source interface tengigabitethernet** *te_port* **[rx | tx | both]**	session_id: (1..7); te_port: (1..8/0/1..32):	Добавляет указанный зеркалируемый порт для выбранной сессии мониторинга. rx – копировать пакеты принятые контролируемым портом; tx – копировать пакеты, переданные контролируемым портом; both – копировать все пакеты с контролируемого порта.
monitor session *session_id* **source interface tengigabitethernet** *te_port*		Выключает функцию мониторинга на настраиваемом интерфейсе.
monitor session *session_id* **source vlan** *vlan_id*	vlan_id: (1..4094); session_id: (1..7)	Добавляет указанный зеркалируемый vlan для выбранной сессии мониторинга.
no monitor session *session_id* **source vlan** *vlan_id*		Выключает функцию мониторинга на настраиваемом интерфейсе.
monitor session *session_id* **source remote vlan** *vlan_id*	vlan_id: (1..4094); session_id: (1..7)	Добавляет в качестве источника vlan с уже ранее зеркалируемым трафиком для выбранной сессии мониторинга.
no monitor session *session_id* **source remote vlan** *vlan_id*		Выключает функцию мониторинга на настраиваемом интерфейсе.

5.22 Функция sFlow

sFlow – технология, позволяющая осуществлять мониторинг трафика в пакетных сетях передачи данных путем частичной выборки трафика для последующей инкапсуляции в специальные сообщения, передаваемые на сервер сбора статистики.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 166 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
sflow receiver *id* **{***ipv4_address* **|** *ipv6_address* **|** *ipv6z_address* **|** *url***} [port** *port***] [max-datagram-size** *byte***]**	id: (1..8); port: (1.. 5535)/6343; byte: положительное целое число/1400; формат ipv4_address: A.B.C.D; формат ipv6_address: X:X:X:X::X; формат ipv6z_address: X:X:X:X::X%<ID>; url: (1..158) символов	Задает адрес сервера сбора статистики sflow. - *id* – номер sflow-сервера; - *ipv4_address, ipv6_address, ipv6z_address* – IP-адрес; - *url* – доменное имя хоста; - *port* – номер порта; - *byte* – максимальное количество байт, которое может быть отправлено в один пакет данных.
no sflow receiver *id*		Удаляет адрес сервера сбора статистики sflow
sflow receiver {source-interface | source-interface-ipv6} { tengigabitethernet *te_port* **| port-channel l** *group* **| loopback** *loopback_id* **| vlan** *vlan_id* **| oob}**	vlan_id: (1..4094) te_port: (1..8/0/1..32); loopback_id: (1..64) group: (1..32)	Задает интерфейс устройства, IP-адрес которого будет использоваться по умолчанию в качестве адреса источника сбора статистики.
no sflow receiver source-interface		Удаляет явное задание интерфейса, с адреса которого будет отправляться статистика sflow

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

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

Таблица 167 – Команды режима конфигурации интерфейса Ethernet

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

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 168 – Команды, доступные в режиме EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show sflow configuration [tengigabitethernet *te_port* **|]**	te_port: (1..8/0/1..32);	Выводит настройки sflow.
clear sflow statistics [tengigabitethernet *te_port* **|]**		Очищает статистику sFlow. Если интерфейс не указан, команда очищает все счетчики статистики sFlow.
show sflow statistics [tengigabitethernet *te_port* **|]**		Отображает статистику sFlow.

Примеры выполнения команд

- Установить IP-адрес 10.0.80.1 сервера 1 для сбора статистики sflow. Для ethernet-интерфейсов te1/0/1-te1/0/24 установить среднюю скорость выборки пакетов – 10240 кбит/с и максимальный интервал между успешными выборками пакетов – 240 с.

```
console# configure
console(config)# sflow receiver 1 10.0.80.1
console(config)# interface range tengigabitethernet 1/0/1-24
console(config-if-range)# sflow flowing-sample 1 10240
console (config-if)# sflow counters-sampling 240 1
```

6.1 Функции диагностики физического уровня

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

Для электрических интерфейсов:
- длина кабеля;
- расстояние до места неисправности – обрыва или замыкания.

Для оптических интерфейсов 1G и 10 G:
- параметры питания – напряжение и ток;
- выходная оптическая мощность;
- оптическая мощность на приеме.

6.1.1 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 169 – Команда диагностики оптического трансивера

Команда	*Значение/Значение по умолчанию*	*Действие*
show fiber-ports optical-transceiver [interface tengigabitethernet *te_port* **|** *t***]**	te_port: (1..8/0/1..32);	Отображает результаты диагностики оптического трансивера.

Пример выполнения команды:

```
sw1# show fiber-ports optical-transceiver interface
TengigabitEthernet1/0/5

   Port      Temp  Voltage Current  Output         Input         LOS  Transceiver
             [C]   [Volt]  [mA]     Power          Power              Type
                                    [mW / dBm]     [mW / dBm]
----------- ------ ------- ------- -------------- ------------- --- -------------
  te1/0/5     33    3.28    11.45  0.28 / -5.52  0.24 / -6.11  No      Fiber

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

        Transceiver information:
Vendor name: OEM
Serial number: S1C53253701833
Connector type: SC
Type: SFP/SFP+
Compliance code: BaseBX10
Laser wavelength: 1550 nm
Transfer distance: 20000 m
Diagnostic: supported
```

Таблица 170 – 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.

6.2 Функции обеспечения безопасности

6.2.1 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 171 – Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

Команда	*Значение/Значение по умолчанию*	*Действие*
port security	-/выключено	Включает функцию защиты на интерфейсе. Блокирует функцию изучения новых адресов для интерфейса. Пакеты с неизученными MAC-адресами источника отбрасываются. Команда аналогична команде **port security discard.**
no port security		Отключает функцию защиты на интерфейсе.
port security max *num*	num: (0..256)/1	Задает максимальное количество адресов, которое может изучить порт.
no port security max		Устанавливает значение по умолчанию.
port security routed secure-address *mac_address*	Формат MAC-адреса: H.H.H, H:H:H:H:H:H, H-H-H-H-H-H	Устанавливает защищенный MAC-адрес.
no port security routed secure-address *mac_address*		Удаляет защищенный MAC-адрес.
port security {forward | discard | discard-shutdown} [trap *freq***]**	freq: (1..1000000) сек	Включает функцию защиты на интерфейсе. Блокирует функцию изучения новых адресов для интерфейса. - **forward** – пакеты с неизученными MAC-адресами источника пересылаются. - **discard** – пакеты с неизученными MAC-адресами источника отбрасываются. - **discard-shutdown** – пакеты с неизученными MAC-адресами источника отбрасываются, порт отключается. - *freq* – частота генерируемых сообщений протокола SNMP trap при поступлении несанкционированных пакетов.
port security trap *freq*	freq: (1..1000000) сек	Задает частоту генерируемых сообщений протокола SNMP trap при поступлении несанкционированных пакетов.

port security mode {secure | max-addresses | lock}	-/lock	Задает режим ограничения изучения MAC-адресов для настраиваемого интерфейса. - **secure –** настраивает статическое ограничение изучения MAC-адресов на порту. - **max-addresses** – удаляет текущие динамически изученные адреса, связанные с интерфейсом. Разрешено изучение максимального количества адресов на порту. Повторное изучение и старение разрешены. - **lock** – сохраняет в файл текущие динамически изученные адреса, связанные с интерфейсом и запрещает обучение новым адресам и старение уже изученных адресов.
no port security mode		Устанавливает значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 172 – Команды режима EXEC

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

Примеры выполнения команд

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

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

- Подключить клиента к порту и изучить MAC-адрес.

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

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

6.2.2.1 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 173 – Команды режима глобальной конфигурации

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

Команды режима 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 174 – Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
dot1x port-control {auto | force-authorized | force-unauthorized} [time-range *time***]**	-/force-authorized; time: (1..32)	Настраивает аутентификацию 802.1X на интерфейсе. Разрешает ручной контроль за состоянием авторизации порта. - **auto** – использовать 802.1X для изменения состояния клиента между авторизованным и неавторизованным; - **force-authorized** – выключает аутентификацию 802.1X на интерфейсе. Порт переходит в авторизованное состояние без аутентификации; - **force-unauthorized** – переводит порт в неавторизованное состояние. Игнорируются все попытки аутентификации клиента, коммутатор не предоставляет сервис аутентификации для этого порта; - *time* – интервал времени. Если данный параметр не определен, то порт не авторизован.
no dot1x port-control		Устанавливает значение по умолчанию.
dot1x reauthentication	-/периодические повторные проверки подлинности выключены	Включает периодические повторные проверки подлинности (переаутентификацию) клиента.
no dot1x reauthentication		Выключает периодические повторные проверки подлинности (переаутентификацию) клиента.
dot1x timeout eap-timeout *period*	period: (1..65535) /30	Задает интервал времени в секундах, в течение которого сервер EAP ожидает ответа от клиента EAP до повторной передачи запроса.

no dot1x timeout eap-timeout		Установить значение по умолчанию.
dot1x timeout supplicant-held-period *period*	period: (1..65535) /60	Задает период времени, в течение которого запрашивающий ждет до перезапуска аутентификации после получения ответа FAIL от сервера Radius.
No dot1x timeout supplicat-held-period		Установить значение по умолчанию.
Dot1x timeout reauth-period *period*	period: (300..4294967295)/ 3600 сек	Устанавливает период между повторными проверками подлинности.
No dot1x timeout reauth-period		Устанавливает значение по умолчанию.
Dot1x timeout quiet-period *period*	period: (10..65535)/60 сек	Устанавливает период, в течение которого коммутатор остается в состоянии молчания после неудачной проверки подлинности. В течение периода молчания коммутатор не принимает и не инициирует никаких аутентификационных сообщений.
No dot1x timeout quiet-period		Устанавливает значение по умолчанию
dot1x timeout tx-period *period*	period: (30..65535)/30 сек	Устанавливает период, в течение которого коммутатор ожидает ответ на запрос либо идентификацию по протоколу EAP от клиента, перед повторной отправкой запроса.
No dot1x timeout tx-period		Устанавливает значение по умолчанию.
Dot1x max-req *count*	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.
Dot1x timeout silence-period *period*	period: (60..65535) сек/не задано	Устанавливает период времени неактивности клиента, по истечение которого клиент становится неавторизованным.
No dot1x timeout silence-period		Устанавливает значение по умолчанию

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 175 – Команды режима Privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
dot1x re-authenticate [tengigabitethernet *te_port* **| oob]**	te_port: (1..8/0/1..24)	Вручную осуществляет повторную проверку подлинности указанного порта в команде, либо всех портов, поддерживающих 802.1X.
dot1x unlock client tengigabitethernet *te_port mac_address*	te_port: (1..8/0/1..32);	Заблокировать клиента с указанным MAC-адресом на порту при достижении порога максимально возможных попыток аутентификации.
show dot1x interface {tengigabitethernet *te_port* **| oob}**	te_port: (1..8/0/1..32);	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 { tengigabitethernet *te_port* **| oob}**	te_port: (1..8/0/1..32);	Показывает статистику по 802.1X для выбранного интерфейса.

Примеры выполнения команд

- Включить режим аутентификации 802.1x на коммутаторе. Использовать RADIUS-сервер для проверки подлинности клиентов на интерфейсах IEEE 802.1X. Для 8 интерфейса Ethernet использовать режим аутентификации 802.1x.

```
console# configure
console(config)# dot1x system-auth-control
console(config)# aaa authentication dot1x default radius
console(config)# interface tengigabitethernet 1/0/8
console(config-if)# dot1x port-control auto
```

- Показать состояние 802.1x для коммутатора, для 8 интерфейса Ethernet.

```
console# show dot1x interface tengigabitethernet 1/0/8
```

```
Authentication is enabled
Authenticating Servers: Radius
Unauthenticated VLANs:
Authentication failure traps are disabled
Authentication success traps are disabled
Authentication quiet traps are disabled

te1/0/8
 Host mode: multi-host
 Port Administrated Status: auto
 Guest VLAN: disabled
 Open access: disabled
 Server timeout: 30 sec
 Port Operational Status: unauthorized*
 * Port is down or not present
 Reauthentication is disabled
 Reauthentication period: 3600 sec
 Silence period: 0 sec
 Quiet period: 60 sec
 Interfaces 802.1X-Based Parameters
  Tx period: 30 sec
  Supplicant timeout: 30 sec
  Max req: 2
 Authentication success: 0
 Authentication fails: 0
```

Таблица 176 – Описание результатов выполнения команд

Параметр	***Описание***
Port	Номер порта.
Admin mode	Режим аутентификации 802.1X: Force-auth, Force-unauth, Auto.
Oper mode	Операционный режим порта: авторизованный, неавторизованный, либо выключенный (Authorized, Unauthorized, Down).
Reauth Control	Контроль переаутентификации.
Reauth Period	Период между повторными проверками подлинности.
Username	Имя пользователя при использовании 802.1X. Если порт авторизован, то отображается имя текущего пользователя. Если порт не авторизован, то отображается имя последнего успешно авторизованного пользователя на порту.
Quiet period	Период, в течение которого коммутатор остается в состоянии молчания после неудачной проверки подлинности.
Tx period	Период, в течение которого коммутатор ожидает ответ на запрос либо идентификацию по протоколу EAP от клиента, перед повторной отправкой запроса.
Max req	Максимальное число попыток передачи запросов протокола EAP клиенту перед новым запуском процесса проверки подлинности.

Supplicant timeout	Период между повторными передачами запросов протокола EAP клиенту.
Server timeout	Период, в течение которого коммутатор ожидает ответа от сервера аутентификации.
Session Time	Время подключения пользователя к устройству.
Mac address	MAC-адрес пользователя.
Authentication Method	Метод аутентификации установленной сессии.
Termination Cause	Причина закрытия сессии.
State	Текущее значение автомата состояний определителя подлинности и выходного автомата состояний.
Authentication success	Количество полученных сообщений об успешной аутентификации от сервера.
Authentication fails	Количество полученных сообщений о неуспешной аутентификации от сервера.
VLAN	Группа VLAN назначенная пользователю.
Filter ID	Идентификатор группы фильтрации.

- Показать статистику по 802.1x для интерфейса Ethernet 8.

```
console# show dot1x statistics interface tengigabitethernet 1/0/8
```

```
EapolFramesRx: 12
EapolFramesTx: 8
EapolStartFramesRx: 1
EapolLogoffFramesRx: 1
EapolRespIdFramesRx: 4
EapolRespFramesRx: 6
EapolReqIdFramesTx: 3
EapolReqFramesTx: 5
InvalidEapolFramesRx: 0
EapLengthErrorFramesRx: 0
LastEapolFrameVersion: 1
LastEapolFrameSource: 00:00:02:56:54:38
```

Таблица 177 – 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.

6.2.2.2 Расширенная проверка подлинности

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

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 178 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
dot1x traps authentication success [802.1x | mac | web]	-/выключено	Разрешает отправку trap-сообщений, когда клиент успешно проходит аутентификацию.
no dot1x traps authentication success		Устанавливает значение по умолчанию.
dot1x traps authentication failure [802.1x | mac | web]	-/выключено	Разрешает отправку trap-сообщений, когда клиент не прошел аутентификацию.
no dot1x traps authentication failure		Устанавливает значение по умолчанию.
dot1x traps authentication quiet	-/выключено	Включает отправку trap-сообщений при превышении пользователем максимально допустимого количества безуспешных попыток аутентификации.
no dot1x traps authentication quiet		Устанавливает значение по умолчанию.

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

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

Таблица 179 – Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
dot1x host-mode {multi-host | single-host | multi-sessions}	-/multi-host	Разрешает наличие одного/нескольких клиентов на авторизованном порту 802.1X. - **multi-host** – несколько клиентов; - **single-host** – один клиент; - **multi-sessions** – несколько сессий.

dot1x violation-mode {restrict | protect | shutdown} [trap *freq***]**	-/protect; freq: (1..1000000)/1 сек	Задает действие, которое необходимо выполнить, когда устройство, MAC-адрес которого отличается от MAC-адреса клиента, осуществляет попытку доступа к интерфейсу. **- restrict -** пакеты с MAC-адресом, отличным от MAC-адреса клиента, пересылаются, при этом адрес источника не изучается; **- protect** – пакеты с MAC-адресом, отличным от MAC-адреса клиента, отбрасываются; - **shutdown** – порт выключается, пакеты с MAC-адресом, отличным от MAC-адреса клиента, отбрасываются; - *freq* – частота генерируемых сообщений протокола SNMP trap при поступлении несанкционированных пакетов. **Команда игнорируется в режиме Multiple hosts.**
no dot1x single-host-violation		Устанавливает значение по умолчанию.
dot1x authentication [mac | 802.1x | web]	-/выключена	Включает аутентификацию - **mac** – включает аутентификацию, основанную на MAC-адресах; - **802.1x** – включает аутентификацию, основанную на 802.1x; - **web** -включает механизм Web-based аутентификации **- Не должно быть статических привязок MAC-адресов.** **- Функция повторной аутентификации должна быть включена.**
no dot1x authentication		Выключает аутентификацию, основанную на MAC-адресах пользователей.
dot1x max-hosts *hosts*	hosts: (1..4294967295)	Задает максимальное количество хостов прошедших аутентификацию.
no dot1x max-hosts		Возвращает значение по умолчанию.
dot1x max-login-attempts *num*	num: (0, 3..10)/0	Задает количество неудачных попыток ввода логина, после которых клиент блокируется. 0 – бесконечное число попыток
no dot1x max-login-attempts		Возвращает значение по умолчанию.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 180 – Команды режима Privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show dot1x interface { tengigabitethernet *te_port* **| oob}**	te_port: (1..8/0/1..32);	Настройки протокола 802.1x на интерфейсе (команда доступна только для привилегированного пользователя).
show dot1x detailed	-	Показывает расширенные настройки протокола 802.1x.
show dot1x credentials	-	Структура учета данных отображает параметры авторизованных клиентов.
show dot1x users [*username***]**	username: строка	Показывает авторизованных клиентов.
show dot1x locked clients	-	Показывает неавторизованных клиентов, заблокированных по тайм-ауту.
show dot1x statistics interface { tengigabitethernet *te_port* **| oob}**	te_port: (1..8/0/1..32);	Показывает статистику 802.1X на интерфейсах.

6.2.3 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 181 – Формат полей опции 82

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

Для использования опции 82 на устройстве должна быть включена функция DHCP relay агента. Для включения DHCP relay агента используется команда IP dhcp relay enable в режиме глобальной конфигурации (см. соответствующий раздел документации).

Для корректной работы функции DHCP Snooping все используемые DHCP-серверы должны быть подключены к «доверенным» портам коммутатора. Для добавления порта в список «доверенных» используется команда IP dhcp snooping trust в режиме конфигурации интерфейса. Для обеспечения безопасности все остальные порты коммутатора должны быть «недоверенными».

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 182 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip dhcp snooping	-/выключено	Включает контроль протокола DHCP путем ведения таблицы DHCP snooping и отправки клиентских широковещательных DHCP-запросов на «доверенные» порты.
no ip dhcp snooping		Выключает контроль протокола DHCP.
ip dhcp snooping vlan *vlan_id*	vlan_id: (1..4094)/выключено	Разрешает контроль протокола DHCP в пределах указанной VLAN.
no ip dhcp snooping vlan *vlan_id*		Запрещает контроль протокола DHCP в пределах указанной VLAN.
ip dhcp snooping information option allowed-untrusted	По умолчанию прием DHCP-пакетов с опцией 82 от «ненадежных» портов запрещен	Разрешает принимать DHCP-пакеты с опцией 82 от «ненадежных» портов.
no ip dhcp snooping information option allowed-untrusted		Запрещает принимать DHCP-пакеты с опцией 82 от «ненадежных» портов.
ip dhcp snooping verify	По умолчанию верификация включена	Включает верификацию MAC-адреса клиента и MAC-адреса источника, принятого в DHCP-пакете на «недоверенных» портах.
no ip dhcp snooping verify		Выключает верификацию MAC-адреса клиента и MAC-адреса источника, принятого в DHCP-пакете на «недоверенных» портах.
ip dhcp snooping database	Резервный файл не используется	Разрешает использование резервного файла (базы) контроля протокола DHCP.
no ip dhcp snooping database		Запрещает использование резервного файла (базы) контроля протокола DHCP.
ip dhcp information option	-/разрешено	Разрешает устройству добавление опции 82 при работе протокола DHCP.
no ip dhcp information option		Запрещает устройству добавление опции 82 при работе протокола DHCP.

Таблица 183 – Формат полей опции 82 согласно рекомендациям TR-101

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

Таблица 184 – Формат полей опции 82 режима custom

Поле	*Передаваемая информация*
Circuit ID	Длина (1 байт) Тип Circuit ID Длина (1 байт) VLAN (2 байта) Номер модуля (1 байт) Номер порта (1 байт)
Remote agent ID	Длина (1 байт) Тип Remote ID (1 байт) Длина (1 байт) MAC-адрес коммутатора

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

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

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

Таблица 185 – Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

Команда	*Значение/Значение по умолчанию*	*Действие*
ip dhcp snooping trust	По умолчанию интерфейс не является доверенным	Добавляет интерфейс в список «доверенных» при использовании контроля протокола DHCP. DHCP-трафик «доверенного» интерфейса считается безопасным и не контролируется.
no ip dhcp snooping trust		Удаляет интерфейс из списка «доверенных» при использовании контроля протокола DHCP.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 186 – Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
ip dhcp snooping binding *mac_address vlan_id ip_address* **{ tengigabitethernet** *te_port* **| port-channel** *group***} expiry {***seconds* **| infinite}**	te_port: (1..8/0/1..32); group: (1..32); seconds: (10..4294967295) сек	Добавляет в файл (базу) контроля протокола DHCP соответствие MAC-адреса клиента, группе VLAN и IP-адресу для указанного интерфейса. Данная запись будет действительна в течение указанного в команде времени жизни записи, если клиент не отправит запрос на DHCP-сервер на обновление. Таймер обнуляется в случае получения от клиента запроса на обновление (команда доступна только для привилегированного пользователя). - *seconds* – время жизни записи; - **infinity** – время жизни записи не ограничено.
no ip dhcp snooping binding *mac_address vlan_id*		Удаляет из файла (базы) контроля протокола DHCP соответствие MAC-адреса клиента и группы VLAN.
clear ip dhcp snooping database	-	Очищает файл (базу) контроля протокола DHCP.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 187 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip dhcp information option	-	Показывает информацию об использовании опции 82 протокола DHCP.

show ip dhcp snooping [tengigabitethernet *te_port* **| port-channel** *group***]**	te_port: (1..8/0/1..32); group: (1..32);	Показывает конфигурацию функции контроля протокола DHCP.
show ip dhcp snooping binding [mac-address *mac_address***] [ip-address** *ip_address* **] [vlan** *vlan_id***] [tengigabitethernet** *te_port* **|port-channel** *group***]**	te_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094)	Показывает соответствия из файла (базы) контроля протокола DHCP.

Примеры выполнения команд

- Разрешить использование DHCP опции 82:

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

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

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

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

Interface           Trusted
-----------    ------------
te0/17              yes
```

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

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

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

Функцию защиты IP-адреса (IP Source Guard) необходимо включить глобально и для интерфейса.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 188 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip source-guard	По умолчанию функция выключена	Включает функцию защиты IP-адреса клиента для всего коммутатора.

no ip source-guard		Выключает функцию защиты IP-адреса клиента для всего коммутатора.
ip source-guard binding *mac_address vlan_id ip_address* **{ tengigabitethernet** *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094);	Создание статической записи в таблице соответствия между IP-адресом клиента, его MAC-адресом и группой VLAN для указанного в команде интерфейса.
no ip source-guard binding *mac_address vlan_id*		Удаление статической записи в таблице соответствия.
ip source-guard tcam retries-freq {*seconds* **| never}**	seconds: (10..600)/60 сек	Задает частоту обращения устройства к внутренним ресурсам с целью записи в память неактивных защищенных IP-адресов. - **never** – запрещает запись в память неактивных защищенных IP-адресов.
no ip source-guard tcam retries-freq		Устанавливает значение по умолчанию.

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

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

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

Таблица 189 – Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

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

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 190 – Команды режима Privileged EXEC

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 191 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip source-guard configuration [tengigabitethernet *te_port* **| ort-channel** *group***]**	te_port: (1..8/0/1..32); group: (1..32);	Команда отображает настройку функции защиты IP-адреса на заданном, либо на всех интерфейсах устройства.
show ip source-guard statistics [vlan *vlan_id***]**	vlan_id: (1..4094);	Команда отображает статистику функции защиты IP-адреса на заданном, либо на всех VLAN.
show ip source-guard status [mac-address *mac_address***] [ip-address** *ip_address* **] [vlan** *vlan_id***] [tengigabitethernet** *te_port* **| port-channel** *group***]**	te_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094);	Команда отображает статус функции защиты IP-адреса для указанного интерфейса, IP-адреса, MAC-адреса или группы VLAN.
show ip source-guard inactive	-	Команда отображает не активные IP-адреса отправителя.

Примеры выполнения команд

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

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

```
IP source guard is globally enabled.

Interface        State
---------       ------
te0/4           Enabled
te0/21          Enabled
te0/22          Enabled
```

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

```
console# configure
console(config)# ip dhcp snooping
console(config)# ip source-guard
console(config)# ip source-guard binding 0060.704A.ABAF 3 192.168.16.14
tengigabitethernet 1/0/12
```

6.2.5 Контроль протокола ARP (ARP Inspection)

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

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

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 192 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip arp inspection	По умолчанию функция выключена	Включает контроль протокола ARP (функцию ARP Inspection).
no ip arp inspection		Выключает контроль протокола ARP (функцию ARP Inspection).
ip arp inspection vlan *vlan_id*	vlan_id: (1..4094); По умолчанию функция выключена	Разрешает проверку протокола ARP, основанную на базе соответствий DHCP snooping, в выбранной группе VLAN.
no ip arp inspection vlan *vlan_id*		Запрещает проверку протокола ARP, основанную на базе соответствий DHCP snooping, в выбранной группе VLAN.
ip arp inspection validate	-	Предоставляет специфичные проверки для контроля протокола ARP. MAC-адрес источника: Для ARP-запросов и ответов проверяется соответствие MAC-адреса в заголовке Ethernet MAC-адресу источника в содержимом протокола ARP. MAC-адрес назначения: Для ARP-ответов проверяется соответствие MAC-адреса в заголовке Ethernet MAC-адресу назначения в содержимом протокола ARP. IP-адрес: Проверяется содержимое ARP-пакета на наличие некорректных IP-адресов.
no ip arp inspection validate		Запрещает специфичные проверки для контроля протокола ARP.
ip arp inspection list create *name*	name: (1..32) символа	1. Создание списка статических ARP-соответствий. 2. Вход в режим конфигурации ARP-списков.
no ip arp inspection list create *name*		Удаление списка статических ARP-соответствий.
ip arp inspection list assign *vlan_id*	vlan_id: (1..4094)	Назначает список статических ARP-соответствий для указанной VLAN.
no ip arp inspection list assign *vlan_id*		Отменяет назначение списка статических ARP-соответствий для указанной VLAN.
ip arp inspection logging interval {*seconds* **| infinite}**	seconds: (0..86400)/5 сек	Задает минимальный интервал между сообщениями, содержащими информацию протокола ARP, передаваемыми в журнал. - значение 0 указывает на то, что сообщения будут генерироваться незамедлительно; - infinite – не генерировать сообщений в журнал.
no ip arp inspection logging interval		Устанавливает значение по умолчанию.

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

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

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

Таблица 193 – Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

Команда	*Значение/Значение по умолчанию*	*Действие*
ip arp inspection trust	По умолчанию интерфейс не является доверенным	Добавляет интерфейс в список «доверенных» при использовании контроля протокола ARP. ARP-трафик «доверенного» интерфейса считается безопасным и не контролируется.

no ip arp inspection trust		Удаляет интерфейс из списка «доверенных» при использовании контроля протокола ARP.

Команды режима конфигурации ARP-списков

Вид запроса командной строки в режиме конфигурации ARP-списков:

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

Таблица 194 – Команды режима конфигурации ARP-списков

Команда	*Значение/Значение по умолчанию*	*Действие*
ip *ip_address* **mac-address** *mac_address*	-	Добавляет статическое соответствие IP- и MAC-адресов.
no ip *ip_address* **mac-address** *mac_address*		Удаляет статическое соответствие IP- и MAC-адресов.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 195 – Команды режима EXEC

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

Примеры выполнения команд

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

```
console# configure
console(config)# ip arp inspection list create spisok
console(config-ARP-list)# ip 192.168.16.98 mac-address 0060.70AB.CCCD
console(config-ARP-list)# exit
console(config)# ip arp inspection list assign 11 spisok
```

- Показать списки статических соответствий IP- и MAC-адресов:

```
console# show ip arp inspection list
```

```
List name: servers
```

```
Assigned to VLANs: 11
IP                  ARP
-----------      -------------------------
192.168.16.98  0060.70AB.CCCD
```

6.3 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.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 196 – Команды режима глобальной конфигурации

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

Команды режима конфигурации интерфейса VLAN

Вид запроса командной строки в режиме конфигурации интерфейса VLAN:

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

Таблица 197 – Команды режима конфигурации интерфейса VLAN, интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
ip dhcp relay enable	По умолчанию агент выключен	Включение функций DHCP Relay агента на настраиваемом интерфейсе.
no ip dhcp relay enable		Выключение функций DHCP Relay агента на настраиваемом интерфейсе.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 198 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip dhcp relay	-	Отображает конфигурацию настроенной функции DHCP Relay агента для коммутатора и отдельно для интерфейсов, а также список доступных серверов.

Примеры выполнения команд

- Показать состояние функции DHCP Relay агента:

```
console# show ip dhcp relay
```

```
DHCP relay is Enabled
DHCP relay is not configured on any vlan.
Servers: 192.168.16.38
Relay agent Information option is Enabled
```

6.4 Конфигурация DHCP-сервера

DHCP-сервер осуществляет централизованное управление сетевыми адресами и соответствующими конфигурационными параметрами, автоматически предоставляя их клиентам. Это позволяет избежать ручной настройки устройств сети и уменьшает количество ошибок.

Ethernet-коммутаторы могут работать как DHCP-клиент (получение собственного IP-адреса от сервера DHCP), так и как DHCP-сервер. В случае если DHCP-сервер отключен, то коммутатор может работать с DHCP Relay.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 199 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip dhcp server	-/выключено	Включение функции DHCP-сервера на коммутаторе.
no ip dhcp server		Выключение функции DHCP-сервера на коммутаторе.
ip dhcp pool host *name*	name: (1..32) символов	Вход в режим конфигурации статических адресов DHCP-сервера.
no ip dhcp pool host *name*		Удаляет конфигурацию DHCP-клиента с заданным именем.
ip dhcp pool network *name*	name: (1..32) символов	Вход в режим конфигурации DHCP-пула адресов DHCP-сервера. - **name** – имя DHCP-пула адресов.
no ip dhcp pool network *name*		Удаляет DHCP-пул с заданным именем.
ip dhcp excluded-address *low_address* **[***high_address***]**	-	Указывает IP-адреса, которые DHCP-сервер не будет назначать для DHCP-клиентов. - *low-address* – начальный IP-адрес диапазона; - *high-address* – конечный IP-адрес диапазона.
no ip dhcp excluded-address *low_address* **[***high_address***]**		Удаление IP-адреса из списка исключений для назначения его DHCP-клиентам.

Команды режима конфигурации статических адресов DHCP-сервера

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

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

Таблица 200 – Команды режима конфигурации

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

Команды режима конфигурации пула DHCP-сервера

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

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

Таблица 201 – Команды режима конфигурации

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

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

Вид запроса командной строки:

```
console(config-dhcp)#
```

Таблица 202 – Команды режима конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
default-router *ip_address_list*	По умолчанию список маршрутизаторов не определен.	Определяет список маршрутизаторов по умолчанию для DHCP-клиента: - *ip_address_list* – список IP-адресов маршрутизаторов, может содержать до 8 записей, разделенных пробелом. **IP-адрес маршрутизатора должен быть в той же подсети, что и клиент.**
no default-router		Устанавливает значение по умолчанию.
dns-server *ip_address_list*	По умолчанию список DNS-серверов не определен.	Определяет список DNS-серверов, доступных для клиентов DHCP. - *ip_address_list* – список IP-адресов DNS-серверов, может содержать до 8 записей, разделенных пробелом.
no dns-server		Устанавливает значение по умолчанию.
domain-name *domain*	domain: (1..32) символов	Определяет доменное имя для DHCP-клиентов.
no domain-name		Устанавливает значение по умолчанию.
netbios-name-server *ip_address_list*	По умолчанию список WINS-серверов не определен.	Определяет список WINS-серверов, доступных для клиентов DHCP. - *ip_address_list* – список IP-адресов WINS-серверов, может содержать до 8 записей, разделенных пробелом.
no netbios-name-server		Устанавливает значение по умолчанию.
netbios-node-type {b-node | p-node | m-node | h-node}	По умолчанию тип узла NetBIOS не определен.	Определяет тип узла NetBIOS Microsoft для клиентов DHCP: - *b-node* – широковещательный; - *p-node* – точка-точка; - *m-node* – комбинированный; - *h-node* – гибридный.
no netbios-node-type		Устанавливает значение по умолчанию.
next-server *ip_address*	-	Используется для указания DHCP-клиенту адреса сервера (как правило, TFTP-сервера), с которого должен быть получен загрузочный файл.
no next-server		Устанавливает значение по умолчанию.
next-server-name *name*	name: (1..64) символов	Используется для указания DHCP-клиенту имя сервера, с которого должен быть получен загрузочный файл.
no next-server-name		Устанавливает значение по умолчанию.
bootfile *filename*	filename: (1..128) символов	Указывает имя файла, используемого для начальной загрузки DHCP-клиента.
no bootfile		Устанавливает значение по умолчанию.
time-server *ip_address_list*	По умолчанию список серверов не определен.	Определяет список серверов времени, доступных для клиентов DHCP. - *ip_address_list* – список IP-адресов серверов времени, может содержать до 8 записей, разделенных пробелом.
no time-server		Устанавливает значение по умолчанию.
option *code* **{boolean** *bool_val* **| integer** *int_val* **| ascii** *ascii_string* **| ip[-list]** *ip_address_list* **| hex {***hex_string* **| none}} [description** *desc***]**	code: (0..255); bool_val: (true, false); int_val: (0..4294967295); ascii_string: (1..160) символов; desc: (1..160) символов	Настраивает опции DHCP-сервера. - *code* – код опции DHCP-сервера; - *bool_val* – логическое значение; - *integer* – целое положительное число; - *ascii_string* – строка в формате ASCII; - *ip_address_list* – список IP-адресов; - *hex_string* – строка в 16-ом формате;
no option *code*		Удаляет опции для DHCP-сервера.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 203 – Команды режима Privileged EXEC

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

Примеры выполнения команд

- Настроить DHCP-пул с именем *test* и указать для DHCP-клиентов: имя домена – *test.ru*, шлюз по умолчанию – *192.168.45.1* и DNS-сервер – *192.168.45.112*.

```
console#
console# configure
console(config)# ip dhcp pool network test
console(config-dhcp)# address 192.168.45.0 255.255.255.0
console(config-dhcp)# domain-name test.ru
console(config-dhcp)# dns-server 192.168.45.112
console(config-dhcp)# default-router 192.168.45.1
```

6.5 Конфигурация ACL (списки контроля доступа)

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

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

IPv6- и IPv4-списки могут работать вместе на одном физическом интерфейсе. Список ACL на базе MAC-адресации не может совмещаться со списками для IPv4 или IPv6. Два списка одинакового типа не могут работать вместе на интерфейсе.

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

Команды режима глобальной конфигурации

Командная строка в режиме глобальной конфигурации имеет вид:

```
console (config)#
```

Таблица 204 – Команды для создания и конфигурации списков ACL

Команда	*Значение/Значение по умолчанию*	*Действие*
ip access-list *access_list* **{deny | permit} {any |** *ip_address* **[***ip_address_mask***]}**	access_list: (0..32) символа	Создание стандартного списка ACL. - **deny** – запретить прохождение пакетов с указанными параметрами; - **permit** – разрешить прохождение пакетов с указанными параметрами.
no ip access-list *access_list*		Удалить стандартный список ACL.
ip access-list extended *access_list*		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 *access_list* **{deny | permit} {any |** *ipv6_address* **[***ipv6_address_prefix***]}**		Создание нового стандартного списка ACL для адресации IPv6. - **deny** – запретить прохождение пакетов с указанными параметрами; - **permit** – разрешить прохождение пакетов с указанными параметрами.
no ipv6 access-list *access_list*		Удаление стандартного списка ACL для адресации IPv6.
ipv6 access-list extended *access_list*		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*		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 *access_list*		Удаление списка ACL на базе MAC-адресации.
time-range *time_name*	time_name: (0..32) символа	Вход в режим конфигурации time-range и определение временных интервалов для списка доступа. - *time_name* – имя профиля настроек time-range.
no time-range *time_name*		Удаление заданной конфигурации time-range.

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

Команды режима конфигурации интерфейса Ethernet, VLAN, группы портов

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

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

Таблица 205 – Команда назначения списка ACL-интерфейсу.

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

Команды режима Privileged EXEC

Командная строка в режиме Privileged EXEC имеет вид:

```
console#
```

Таблица 206 – Команды для просмотра списков ACL

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

Команды режима EXEC

Командная строка в режиме EXEC имеет вид:

```
console#
```

Таблица 207 – Команды для просмотра списков ACL

Команда	*Значение/Значение по умолчанию*	*Действие*
show time-range [*time_name***]**	-	Показывает конфигурацию time-range

6.5.1 Конфигурация ACL на базе IPv4

В данном разделе приведены значения и описания основных параметров, используемых в составе команд настройки списков ACL, основанных на адресации IPv4. Создание и вход в режим редактирования списков ACL, основанных на адресации IPv4, осуществляется по команде: **ip access-list extended** *access-list*. Например, для создания списка ACL под названием EltexAL необходимо выполнить следующие команды:

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

Таблица 208 – Основные параметры, используемые в командах

Параметр	*Значение*	*Действие*
permit	Действие ‘разрешить’	Создает разрешающее правило фильтрации в списке ACL.
deny	Действие ‘запретить’	Создает запрещающее правило фильтрации в списке ACL.

protocol	Протокол	Поле предназначено для указания протокола (или всех протоколов), на основе которого будет осуществляется фильтрация. При выборе протокола возможны следующие варианты: icmp, igmp, ip, tcp, egp, igp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis, ipip, либо числовое значение протокола, в диапазоне (0 – 255). Для соответствия любому протоколу используется значение **IP.**
source	Адрес источника	Определяет IP-адрес источника пакета.
source_wildcard	Маска адреса источника	Битовая маска, применяемая к IP-адресу источника пакета. Маска определяет биты IP-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Например, используя маску, можно определить для правила фильтрации IP-сеть. Чтобы добавить в правило фильтрации IP-сеть 195.165.0.0, необходимо задать значение маски 0.0.255.255, то есть согласно данной маске последние 16 бит IP-адреса будут игнорироваться.
destination	Адрес назначения	Определяет IP-адрес назначения пакета.
destination_wildcard	Маска адреса назначения	Битовая маска, применяемая к IP-адресу назначения пакета. Маска определяет биты IP-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Маска используется аналогично маске *source_wildcard.*
vlan	Идентификатор Vlan	Определяет Vlan, для которого будет применяться правило.
dscp	Поле DSCP в заголовке L3	Определяет значение DSCP-поля diffserv. Возможные коды сообщений поля **dscp:** (0 – 63).
precedence	Приоритет IP	Определяет приоритет IP-трафика: (0-7).
time_name	Имя профиля конфигурации time-range	Определяет конфигурацию временных интервалов.
icmp_type	-	Тип сообщений протокола ICMP, используемый для фильтрации ICMP-пакетов. Возможные типы сообщений поля *icmp_type***:** echo-reply, destination-unreachable, source-quench, redirect, alternate-host-address, echo-request, router-advertisement, router-solicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain_name-request, domain_name-reply, skip, photuris, либо числовое значение типа сообщения, в диапазоне (0 – 255).
icmp_code	Код сообщения протокола ICMP	Код сообщений протокола ICMP, используемый для фильтрации ICMP-пакетов. Возможные коды сообщений поля *icmp_code***:** (0 – 255).
igmp_type	Тип сообщения протокола IGMP	Тип сообщений протокола IGMP, используемый для фильтрации пакетов IGMP. Возможные типы сообщений поля *igmp_type***:** *host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3*, либо числовое значение типа сообщения, в диапазоне (0 – 255).
destination_port	UDP/TCP-порт назначения	Возможные значения поля TCP-порта: bgp (179), chargen (19),

source_port	UDP/TCP-порт источника	daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80); Для UDP-порта: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). Либо числовое значение (0 – 65535).
list_of_flags	Флаги протокола TCP	Если для условия фильтрации флаг должен быть установлен, то перед ним ставится знак «+», если не должен быть установлен, то «-». Возможные варианты флагов: **+urg**, **+ack**, **+psh**, **+rst**, **+syn**, **+fin**, **-urg**, **-ack**, **-psh**, **-rst**, **-syn** и **-fin**. При использовании нескольких флагов в условии фильтрации, флаги объединяются в одну строку без пробелов, например: **+fin-ack.**
disable_port	Отключение порта	Выключает порт, с которого был принят пакет, удовлетворяющий условиям любой из команд запрета **deny,** в составе которой было описано поле**.**
log_input	Отправка сообщений	Включает отправку информационных сообщений в системный журнал при получении пакета, который соответствует записи.
offset_list_name	Наименование списка шаблонов пользователя	Задает использование списка шаблонов пользователя для распознавания пакетов. Для каждого списка ACL может быть определен свой список шаблонов.
ace-priority	Приоритет записи	Индекс задает положение правила в списке и его приоритет. Чем меньше индекс – тем приоритетнее правило. Диапазон допустимых значений (1..2147483647).

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

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

Таблица 209 – Команды, используемые для настройки ACL-списков на основе IP-адресации

Команда	***Действие***
permit *protocol* **{any |** *source source_wildcard***} {any |** *destination destination_wildcard***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [ace-priority** *index***]**	Добавляет разрешающую запись фильтрации для протокола. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
no permit *protocol* **{any |** *source source_wildcard***} {any |** *destination destination_wildcard***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***]**	Удаляет созданную ранее запись.
permit ip **{any |** *source_ip source_ip_wildcard***} {any |** *destination_ip destination_ip_wildcard***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *range_name***] [ace priority** *index***]**	Добавляет разрешающую запись фильтрации для протокола IP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
no permit ip **{any |** *source_ip source_ip_wildcard***} {any |** *destination_ip destination_ip_wildcard***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *range_name***]**	Удаляет созданную ранее запись.
permit icmp {any | source *source_wildcard***} {any | destination** *destination_wildcard***} {any |** *icmp_type***} {any |** *icmp_code***} [dscp** *dscp* **| ip-precedence** *precedence***] [time-range** *time_name***] [ace-priority** *index***] [offset-list** *offset_list_name***] [vlan** *vlan_id***]**	Добавляет разрешающую запись фильтрации для протокола ICMP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.

no permit icmp {any | source *source_wildcard***} {any | destination** *destination_wildcard***} {any |** *icmp_type***} {any |** *icmp_code***} [dscp** *dscp* **| ip-precedence** *precedence***] [time-range** *time_name***] [offset-list** *offset_list_name***] [vlan** *vlan_id***]**	Удаляет созданную ранее запись.
permit igmp {any | *source source_wildcard***} {any |** *destination destination_wildcard***} [**igmp_type**] [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [ace-priority** *index***]**	Добавляет разрешающую запись фильтрации для протокола IGMP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
no permit igmp {any | *source source_wildcard***} {any |** *destination destination_wildcard***} [**igmp_type**] [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***]**	Удаляет созданную ранее запись.
permit tcp {any | *source source_wildcard***} {any |** *source_port***} {any |** *destination destination_wildcard***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [match-all** *list_of_flags***] [time-range** *time_name***] [ace-priority** *index***]**	Добавляет разрешающую запись фильтрации для протокола TCP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
no permit tcp {any | *source source_wildcard* **} {any |** *source_port***} {any |** *destination destination_wildcard***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [match-all** *list_of_flags***] [time-range** *time_name***]**	Удаляет созданную ранее запись.
permit udp {any | *source source_wildcard***} {any |** *source_port***} {any |** *destination destination_wildcard***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [ace-priority** *index***]**	Добавляет разрешающую запись фильтрации для протокола UDP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
no permit udp {any | *source source_wildcard***} {any |** *source_port***} {any |** *destination destination_wildcard***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***]**	Удаляет созданную ранее запись.
deny *protocol* **{any |** *source source_wildcard***} {any |** *destination destination_wildcard***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [disable-port | log-input] [ace-priority** *index***]**	Добавляет запрещающую запись фильтрации для протокола. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова **disable-port** физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова **log-input** будет отправлено сообщение в системный журнал.
no deny *protocol* **{any |** *source source_wildcard***} {any |** *destination destination_wildcard***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [disable-port | log-input]**	Удаляет созданную ранее запись.
deny ip {any | *source_ip source_ip_wildcard***} {any |** *destination_ip destination_ip_wildcard***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *range_name***] [disable-port | log-input] [ace-priority** *index***]**	Добавляет запрещающую запись фильтрации для протокола IP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова **disable-port** физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова **log-input** будет отправлено сообщение в системный журнал.
no deny ip {any | *source_ip source_ip_wildcard***} {any |** *destination_ip destination_ip_wildcard***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *range_name***] [disable-port | log-input]**	Удаляет созданную ранее запись.
deny icmp {any | *source source_wildcard***} {any |** *destination destination_wildcard***} {any |** *icmp_type***} {any |** *icmp_code***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [disable-port | log-input] [ace-priority** *index***]**	Добавляет запрещающую запись фильтрации для протокола ICMP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова **disable-port** физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова **log-input** будет отправлено сообщение в системный журнал.
no deny icmp {any | *source source_wildcard***} {any |** *destination destination_wildcard***} {any |** *icmp_type***} {any |** *icmp_code***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [disable-port | log-input]**	Удаляет созданную ранее запись.

deny igmp {any | *source source_wildcard***} {any |** *destination destination_wildcard***} [***igmp_type***] [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [ace-priority** *index***] [disable-port | log-input]**	Добавляет запрещающую запись фильтрации для протокола IGMP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова **disable-port** физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова **log-input** будет отправлено сообщение в системный журнал.
no deny igmp {any | *source source_wildcard***} {any |** *destination destination_wildcard***} [***igmp_type***] [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [disable-port | log-input]**	Удаляет созданную ранее запись.
deny tcp {any | *source source_wildcard***} {any |** *source_port***} {any |** *destination destination_wildcard***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [match-all** *list_of_flags***] [time-range** *time_name***] [ace-priority** *index***] [disable-port | log-input]**	Добавляет запрещающую запись фильтрации для протокола TCP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова **disable-port** физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова **log-input** будет отправлено сообщение в системный журнал.
no deny tcp {any | *source source_wildcard***} {any |** *source_port***} {any |** *destination destination_wildcard***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [match-all** *list_of_flags***] [time-range** *time_name***] [disable-port | log-input]**	Удаляет созданную ранее запись.
deny udp {any | *source source_wildcard***} {any |** *source_port***} {any |** *destination destination_wildcard***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [ace-priority** *index***] [disable-port | log-input]**	Добавляет запрещающую запись фильтрации для протокола UDP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова **disable-port** физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова **log-input** будет отправлено сообщение в системный журнал.
no deny udp {any | *source source_wildcard***} {any |** *source_port***} {any |** *destination destination_wildcard***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [disable-port | log-input]**	Удаляет созданную ранее запись.
offset-list *offset_list_name* **{***offset_base offset mask value***}** …	Создаёт список шаблонов пользователя с именем *name*. Имя может включать от 1 до 32 символов. В одной команде может содержаться до тринадцати шаблонов в зависимости от выбранного режима настройки списков доступа (команда **set system mode**), включающих следующие параметры: - *offset_base* – базовое смещение. Возможные значения: **l3** – начало смещения с начала IP-заголовка; **l4 –** начало смещения с конца IP-заголовка. - *offset* – смещение байта данных в пределах пакета. Базовое смещение принимается за начало отсчета; - *mask* – маска. В анализе пакета принимают участие только те разряды байта, для которых в соответствующих разрядах маски задана ‘1’; - *value* – искомое значение.
no offset-list *offset_list_name*	Удаляет созданный ранее список.

6.5.2 Конфигурация ACL на базе IPv6

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

Создание и вход в режим редактирования списков ACL, основанных на адресации IPv6, осуществляется по команде: **ipv6 access-list** *access-list*. Например, для создания списка ACL под названием MESipv6 необходимо выполнить следующие команды:

```
console#
console# configure
console(config)# ipv6 access-list MESipv6
console(config-ipv6-al)#
```

Таблица 210 – Основные параметры, используемые в командах

Параметр	*Значение*	*Действие*
permit	Действие разрешить	Создает разрешающее правило фильтрации в списке ACL.
deny	Действие запретить	Создает запрещающее правило фильтрации в списке ACL.
protocol	Протокол	Поле предназначено для указания протокола (или всех протоколов), на основе которого будет осуществляется фильтрация. При выборе протокола возможны следующие варианты: **icmp**, **tcp**, **udp**, либо числовое значение протокола – **icmp** (58), **tcp** (6), **udp** (17). Для соответствия любому протоколу используется значение **IPv6.**
source_prefix/length	Адрес отправителя и его длина	Определяет IPv6-адрес и длину префикса сети (0-128) (количество старших бит адреса) источника пакета.
destination_prefix/length	Адрес назначения и его длина	Определяет IPv6-адрес и длину префикса сети (0-128) (количество старших бит адреса) назначения пакета.
dscp	Поле DSCP в заголовке L3	Определяет значение DSCP-поля diffserv. Возможные коды сообщений поля **dscp: (**0 – 63).
precedence	Приоритет IP	Определяет приоритет IP-трафика:(0-7).
time_name	Имя профиля конфигурации time-range	Определяет конфигурацию временных интервалов.
icmp_type	Тип сообщения протокола ICMP	Используется для фильтрации ICMP-пакетов. Возможные типы и числовые значения сообщений поля **icmp_type:** destination-unreachable (1), packet-too-big (2), time-exceeded (3), parameter-problem (4), echo-request (128), echo-reply (129), mld-query (130), mld-report (131), mldv2-report (143), mld-done (132), router-solicitation (133), router-advertisement (134), nd-ns (135), nd-na (136).
icmp_code	Код сообщений протокола ICMP	Используется для фильтрации ICMP-пакетов. Возможные значения поля **(**0 – 255).
destination_port	UDP/TCP-порт назначения	Возможные значения поля TCP-порта: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80); Для UDP-порта: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). Либо числовое значение (0 – 65535).
source_port	UDP/TCP-порт источника	
list_of_flags	Флаги протокола TCP	Если для условия фильтрации флаг должен быть установлен, то перед ним ставится знак «+», если не должен быть установлен, то «-». Возможные варианты флагов: **+urg**, **+ack**, **+psh**, **+rst**, **+syn**, **+fin**, **-urg**, **-ack**, **-psh**, **-rst**, **-syn** и **-fin**.
disable-port	Отключение порта	Выключает порт, с которого был принят пакет, удовлетворяющий условиям любой из команд запрета **deny,** в составе которой, было описано поле**.**
log-input	Отправка сообщений	Включает отправку информационных сообщений в системный журнал при получении пакета, который соответствует записи.
ace-priority	Индекс правила	Индекс правила в таблице, чем меньше индекс – тем приоритетнее правило: (1..2147483647).

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

После того, как хотя бы одна запись добавлена в список ACL, последними в список добавляются записи
permit-icmp any any nd-ns any
permit-icmp any any nd-na any
deny ipv6 any any
Две первые из них разрешают поиск соседних IPv6-устройств с помощью протокола ICMPv6, а последняя означает игнорирование всех пакетов, не удовлетворяющих условиям ACL.

Таблица 211 – Команды, используемые для настройки ACL списков на основе IPv6-адресации

Команда	*Действие*
permit *protocol* **{any |** *source_prefix/length***} {any |** *destination_prefix/length***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [ace-priority** *index***]**	Добавляет разрешающую запись фильтрации для протокола. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
no permit *protocol* **{any |** *source_prefix/length***} {any |** *destination_prefix/length***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***]**	Удаляет созданную ранее запись.
permit icmp {any | *source_prefix/length***} {any |** *destination_prefix/length***} {any |** *icmp_type***} {any |** *icmp_code***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [ace-priority** *index***]**	Добавляет разрешающую запись фильтрации для протокола ICMP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
no permit icmp {any | *source_prefix/length***} {any |** *destination_prefix/length***} {any |** *icmp_type***} {any |** *icmp_code***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***]**	Удаляет созданную ранее запись.
permit tcp {any | *source_prefix/length***} {any |** *source_port***} {any |** *destination_prefix/length***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [match-all** *list_of_flags***] [ace-priority** *index***]**	Добавляет разрешающую запись фильтрации для протокола TCP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
no permit tcp {any | *source_prefix/length***} {any |** *source_port***} {any |** *destination_prefix/length***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [match-all** *list_of_flags***]**	Удаляет созданную ранее запись.
permit udp {any | *source_prefix/length***} {any |** *source_port***} {any |** *destination_prefix/length***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [ace-priority** *index***]**	Добавляет разрешающую запись фильтрации для протокола UDP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
no permit udp {any | *source_prefix/length***} {any |** *source_port***} {any |** *destination_prefix/length***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***]**	Удаляет созданную ранее запись.
deny *protocol* **{any |** *source_prefix/length***} {any |** *destination_prefix/length***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [disable-port | log-input] [ace-priority** *index***]**	Добавляет запрещающую запись фильтрации для протокола. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова **disable-port** физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова **log-input** будет отправлено сообщение в системный журнал.
no deny *protocol* **{any |** *source_prefix/length***} {any |** *destination_prefix/length***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [disable-port | log-input]**	Удаляет созданную ранее запись.
deny icmp {any | *source_prefix/length***} {any |** *destination_prefix/length***} {any |** *icmp_type***} {any |** *icmp_code***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [disable-port | log-input] [ace-priority** *index***]**	Добавляет запрещающую запись фильтрации для протокола ICMP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова **disable-port** физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова **log-input** будет отправлено сообщение в системный журнал.
no deny icmp {any | *source_prefix/length***} {any |** *destination_prefix/length***} {any |** *icmp_type***} {any |** *icmp_code***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *time_name***] [disable-port | log-input]**	Удаляет созданную ранее запись.

deny tcp {any | *source_prefix/length***} {any |** *source_port***} {any |** *destination_prefix/length***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [match-all** *list_of_flags***] [time-range** *time_name***] [disable-port | log-input] [ace-priority** *index***]**	Добавляет запрещающую запись фильтрации для протокола TCP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова **disable-port** физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова **log-input** будет отправлено сообщение в системный журнал.
no deny tcp {any | *source_prefix/length***} {any |** *source_port***} {any |** *destination_prefix/length***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [match-all** *list_of_flags***] [time-range** *time_name***] [disable-port | log-input]**	Удаляет созданную ранее запись.
deny udp {any | *source_prefix/length***} {any |** *source_port***} {any |** *destination_prefix/length***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [match-all** *list_of_flags***] [time-range** *time_name***] [disable-port | log-input] [ace-priority** *index***]**	Добавляет запрещающую запись фильтрации для протокола UDP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова **disable-port** физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова **log-input** будет отправлено сообщение в системный журнал.
no deny udp {any | *source_prefix/length***} {any |** *source_port***} {any |** *destination_prefix/length***} {any |** *destination_port***} [dscp** *dscp* **| precedence** *precedence***] [match-all** *list_of_flags***] [time-range** *time_name***] [disable-port | log-input]**	Удаляет созданную ранее запись.
offset-list *offset_list_name* **{***offset_base offset mask value***}** …	Создаёт список шаблонов пользователя с именем *name*. Имя может включать от 1 до 32 символов. В одной команде может содержаться до тринадцати шаблонов в зависимости от выбранного режима настройки списков доступа (команда **set system mode**), включающих следующие параметры: - *offset_base* – базовое смещение. Возможные значения: **l3** – начало смещения с начала IPv6-заголовка; **l4 –** начало смещения с конца IPv6-заголовка. - *offset* – смещение байта данных в пределах пакета. Базовое смещение принимается за начало отсчета; - *mask* – маска. В анализе пакета принимают участие только те разряды байта, для которых в соответствующих разрядах маски задана ‘1’; - *value* – искомое значение.
no offset-list *offset_list_name*	Удаляет созданный ранее список.

6.5.3 Конфигурация ACL на базе MAC

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

Создание и вход в режим редактирования списков ACL, основанных на MAC-адресации, осуществляется по команде: **mac access-list extended** *access-list*. Например, для создания списка ACL под названием MESmac необходимо выполнить следующие команды:

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

Таблица 212 – Основные параметры, используемые в командах

Параметр	*Значение*	*Действие*
permit	Действие разрешить	Создает разрешающее правило фильтрации в списке ACL.
deny	Действие запретить	Создает запрещающее правило фильтрации в списке ACL.
source	Адрес отправителя	Определяет MAC-адрес источника пакета.

source_wildcard	Битовая маска, применяемая к MAC-адресу источника пакета	Маска определяет биты MAC-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Например, используя маску, можно определить для правила фильтрации диапазона MAC-адресов. Чтобы добавить в правило фильтрации все MAC-адреса, начинающиеся на 00:00:02:AA.xx.xx, необходимо задать значение маски 0.0.0.0.FF.FF, то есть, согласно данной маске, последние 32 бита MAC-адреса будут не важны для анализа.
destination	Адрес назначения	Определяет MAC-адрес назначения пакета.
destination_wildcard	Битовая маска, применяемая к MAC-адресу назначения пакета	Маска определяет биты MAC-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Маска используется аналогично маске source_wildcard.
vlan_id	vlan_id: (0..4095)	Подсеть VLAN фильтруемых пакетов.
cos	cos: (0..7)	Класс обслуживания (CoS) фильтруемых пакетов.
cos_wildcard	Битовая маска, применяемая к классу обслуживания (CoS) фильтруемых пакетов	Маска определяет биты CoS, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Например, чтобы использовать в правиле фильтрации CoS 6 и 7, необходимо в поле CoS указать значение 6, либо 7, а в поле маски значение 1 (7 в двоичном представлении – 111, 1 – 001, получается, что последний бит, будет игнорироваться, то есть CoS может быть либо 110 (6), либо 111 (7)).
eth_type	eth_type: (0..0xFFFF)	Ethernet тип фильтруемых пакетов в шестнадцатеричной записи.
disable-port	-	Выключает порт, с которого был принят пакет, удовлетворяющий условиям команды запрета **deny.**
log-input	Отправка сообщений	Включает отправку информационных сообщений в системный журнал при получении пакета, который соответствует записи.
time_name	Имя профиля конфигурации time-range	Определяет конфигурацию временных интервалов.
offset_list_name	Побайтовое смещение от ключевой точки	Задает использование списка шаблонов пользователя для распознавания пакетов. Для каждого списка ACL может быть определен свой список шаблонов.
ace-priority	Индекс правила	Индекс правила в таблице, чем меньше индекс – тем приоритетнее правило 1-2147483647.

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

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

Таблица 213 – Команды, используемые для настройки ACL-списков на основе MAC-адресации

Команда	*Действие*
permit {any | *source source-wildcard***} {any |** *destination destination_wildcard***} [vlan** *vlan_id***] [cos** *cos cos_wildcard***] [***eth_type***] [time-range** *time_name***] [ace-priority** *index***] [offset-list** *offset_list_name***]**	Добавляет разрешающую запись фильтрации. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
no permit {any | *source source-wildcard***} {any |** *destination destination_wildcard***} [vlan** *vlan_id***] [cos** *cos cos_wildcard***] [***eth_type***] [time-range** *time_name***] [offset-list** *offset_list_name***]**	Удаляет созданную ранее запись.

deny {any | *source source-wildcard***} {any |** *destination destination_wildcard***} [vlan** *vlan_id***] [cos** *cos cos_wildcard***] [**_eth_type_**] [time-range** *time_name***] [disable-port | log-input] [ace-priority***index***] [offset-list** *offset_list_name***]**	Добавляет запрещающую запись фильтрации. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором. При использовании ключевого слова **disable-port**, физический интерфейс, принявший такой пакет, будет выключен. При использовании ключевого слова *log-input* будет отправлено сообщение в системный журнал.
no deny {any | *source source-wildcard***} {any |** *destination destination_wildcard***} [vlan** *vlan_id***] [cos** *cos cos_wildcard***] [**_eth_type_**] [time-range** *time_name***] [disable-port | log-input] [offset-list** *offset_list_name***]**	Удаляет созданную ранее запись.
offset-list *offset_list_name* **{***offset_base offset mask value***}** *…*	Создаёт список шаблонов пользователя с именем *name*. Имя может включать от 1 до 32 символов. В одной команде может содержаться до тринадцати шаблонов в зависимости от выбранного режима настройки списков доступа (команда **set system mode**), включающих следующие параметры: - *offset_base* – базовое смещение. Возможные значения: **l2** – начало смещения от EtherType; **outer-tag** – начало смещения от STAG; **inner-tag** – начало смещения от CTAG; **src-mac** – начало смещения с MAC-адреса источника; **dst-mac** – начало смещения с MAC-адреса назначения. - *offset* – смещение байта данных в пределах пакета. Базовое смещение принимается за начало отсчета; - *mask* – маска. В анализе пакета принимают участие только те разряды байта, для которых в соответствующих разрядах маски задана ‘1’; - *value* – искомое значение.
no offset-list *offset_list_name*	Удаляет созданный ранее список.

6.6 Конфигурация защиты от DoS-атак

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

Команды режима глобальной конфигурации

Командная строка в режиме глобальной конфигурации имеет вид:

```
console (config)#
```

Таблица 214 – Команды для настройки защиты от DoS-атак

Команда	*Значение/Значение по умолчанию*	*Действие*
security-suite deny martian-addresses [reserved] {add | remove} *ip_address*	*ip_address:* ip-адрес	Запрещает прохождение фреймов с недопустимыми («марсианскими») IP-адресами источника (loopback, broadcast, multicast).
security-suite deny syn-fin	-	Отбрасывает пакеты tcp с одновременно установленными SYN- и FIN- флагами**.**
security-suite dos protect {add | remove} {stacheldraht | invasor-trojan | back-orifice-trojan}	-	Запрещает/разрешает прохождение определенных типов трафика, характерных для вредоносных программ: **- stacheldraht** – отбрасывает TCP-пакеты с портом источника равным 16660; **- invasor-trojan** – отбрасывает TCP-пакеты с портом назначения равным 2140 и портом источника 1024; **- back-orifice-trojan** – отбрасывает UDP-пакеты с портом назначения 31337 и портом источника равным 1024.
security-suite enable	-/выключено	Включает класс команд security-suite.
no security-suite enable		Отключает класс команд security-suite.

Команды режима конфигурации интерфейса Ethernet, группы портов.

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

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

Таблица 215 – Команда конфигурации защиты от DoS-атак для интерфейсов

Команда	*Значение/Значение по умолчанию*	*Действие*
security-suite deny {fragmented | icmp | syn} {add | remove} {any | *ip_address* [*mask*]}	ip_address: IP-адрес; mask: маска в формате IP-адреса или префикса	Создает правило, запрещающее прохождение трафика, соответствующего критериям. - **fragmented** – фрагментированные пакеты - **icmp** – ICMP-трафик **- syn** – syn-пакеты
no security-suite deny {fragmented | icmp | syn}		Удаляет запрещающее правило.
security-suite dos syn-attack *rate* **{any |** *ip_address* **[***mask***]}**	rate: (199..2000) пакетов в секунду; *ip_address*: – IP-адрес; mask: маска в формате IP-адреса или префикса	Задает порог syn-запросов на определенный IP-адрес/сеть, при превышении которого лишние фреймы будут отбрасываться.
no security-suite dos syn-attack {any | *ip_address* **[***mask***]}**		Восстанавливает значение по умолчанию.

6.7 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.

6.7.1 Настройка QoS

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 216 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
qos [basic | advanced [ports-trusted | ports-not-trusted]]	-/basic	Разрешает коммутатору использовать QoS. - **basic** – базовый режим QoS; - **advanced** – расширенный режим конфигурации QoS, включающий полный перечень команд настройки QoS; - **ports-trusted** – в данном подрежиме пакеты направляются в выходную очередь на основании полей в этих пакетах; - **ports-not-trusted** – в данном подрежиме все пакеты направляются в нулевую выходную очередь по умолчанию, для отправки в другие очереди требуется назначать на входной интерфейс стратегию классификации трафика (policy-map).

qos advanced-mode trust {cos | dscp | cos-dscp}	-/отключен	Установить метод доверия на портах при работе в режиме расширенного конфигурации QoS и подрежиме ports-trusted. - cos – порт доверяет значению 802.1p User priority; - dscp – порт доверяет значению DSCP в IPv4/IPv6-пакетах; - cos-dscp – порт доверяет обоим уровням, однако DSCP имеет приоритет над 802.1p.
no qos advanced-mode trust		Устанавливает метод по умолчанию.
class-map *class_map_name* **[match-all | match-any]**	class_map_name: (1..32) символов; По умолчанию используется опция match-all	1. Создает список критериев классификации трафика. 2. Входит в режим редактирования списка критериев классификации трафика. - **match-all** – все критерии данного списка должны быть выполнены; - **match-any** – один, любой критерий данного списка должен быть выполнен. **В списке критериев может быть одно или два правила. Если правила два, и оба они указывают на разные типы ACL (IP, MAC), то классификация будет осуществляться по первому в списке верному правилу.** **Действует только для режима qos advanced**
no class-map *class_map_name*		Удаляет список критериев классификации трафика.
policy-map *policy_map_name*	policy_map_name: (1..32) символов	1. Создает стратегию классификации трафика. 2. Входит в режим редактирования стратегии классификации трафика. **В одном направлении поддерживается только одна стратегия классификации трафика.** **По умолчанию policy-map устанавливает DSCP = 0 для IP-пакетов и CoS = 0 для тегированных пакетов.** **Действует только для режима qos advanced.**
no policy-map *policy_map_name*		Удаляет правило классификации трафика.
qos aggregate-policer *aggregate_policer_name committed_rate_kbps excess_burst_byte* **[exceed-action {drop | policed-dscp-transmit}]**	aggregate_policer_name: (1..32) символа; committed_rate_kbps: (3..57982058) кбит/с; excess_burst_byte: (3000..19173960) байт	Определяет шаблон настроек, который позволяет ограничить полосу пропускания канала и в то же время гарантировать определенную скорость передачи данных. При работе с полосой пропускания используется алгоритм маркированной «корзины». Задачей алгоритма является принятие решения: передать пакет или отбросить. Параметрами алгоритма являются скорость поступления (CIR) маркеров в «корзину» и объём (CBS) «корзины». - *committed-rate-kbps* – среднее значение скорости трафика. Данная скорость гарантируется при передаче информации; - *committed-burst-byte* – размер сдерживающего порога в байтах; - **drop** – пакет будет отброшен, когда «корзина» переполнится; - **policed-dscp-transmit** – при переполнении «корзины» значение DSCP будет переопределено. **Нельзя удалить шаблон настроек, если он используется в стратегии policy map, перед удалением следует удалить назначение шаблона стратегии: no police aggregate** *aggregate-policer-name***.** **Действует только для режима qos advanced.**
no qos aggregate-policer *aggregate_policer_name*		Удаляет шаблон настроек регулирования скорости канала.
wrr-queue cos-map *queue_id cos1…cos8*	queue_id: (1..8); cos1…cos8: (0..7);	Определяет значения CoS для очередей исходящего трафика.

no wrr-queue cos-map [*queue_id*]	Значения CoS по умолчанию для очередей: CoS = 1 – очередь 1 CoS = 2 – очередь 2 CoS = 0 – очередь 3 CoS = 3 – очередь 4 CoS = 4 – очередь 5 CoS = 5 – очередь 6 CoS = 6 – очередь 7 CoS = 7 – очередь 8	Устанавливает значения по умолчанию.
wrr-queue bandwidth *weight1..weight8*	weight: (0..255)/1 По умолчанию вес каждой очереди равен 1	Присваивает вес исходящим очередям, используемый механизмом WRR (Weighted Round Robin – весовой механизм распределения нагрузки).
no wrr-queue bandwidth		Устанавливает значение по умолчанию.
priority-queue out num-of-queues *number_of_queues*	number_of_queues: (0..8) По умолчанию все очереди обрабатываются по алгоритму «strict priority».	Задает количество приоритетных очередей. **Для приоритетной очереди вес WRR будет игнорироваться.** **Если задается отличное от «0» значение *N*, то старшие N очередей будут приоритетными (не будут участвовать в WRR).** **Пример:** **0: все очереди равноправны;** **1: семь младших очередей участвуют в WRR, 8-ая не участвует;** **2: шесть младших очередей участвуют в WRR, 7, 8 не участвуют.**
no priority-queue out num-of-queues		Устанавливает значение по умолчанию.
qos wrr-queue wrtd	По умолчанию WRTD выключено	Включает WRTD (Weighted Random Tail Drop) весовой механизм удаления пакетов из очередей. **Изменения вступят в силу после перезагрузки устройства.**
no qos wrr-queue wrtd		Выключает WRTD.
qos map enable {cos-dscp | dscp-cos}	-	Использовать заданную таблицу перемаркировки для доверенных портов коммутатора.
no qos map enable {cos-dscp | dscp-cos}		Не использовать таблицу перемаркировки.
qos map dscp-mutation *in_dscp* **to** *out_dscp*	in_dscp: (0..63), out_dscp: (0..63) По умолчанию карта изменений является пустой, то есть значения DSCP для всех входящих пакетов остаются неизменными	Заполняет таблицу перемаркировки DSCP. Для входящих пакетов с указанными значениями DSCP задает новые значения DSCP. - *in-dscp* – определяет до 8 значений DSCP, значения разделяются знаком пробела. - *out-dscp* – определяет до 8 новых значений DSCP, значения разделяются знаком пробела. **Действует только для режима qos basic.**
no qos map dscp-mutation [*in_dscp*]		Устанавливает значения по умолчанию.
qos map policed-dscp *dscp_list* **to** *dscp_mark_down*	dscp_list: (0..63) dscp_mark_down: (0..63) По умолчанию таблица повторной маркировки является пустой, то есть значения DSCP для всех входящих пакетов остаются неизменными	Заполняет таблицу перемаркировки DSCP. Для входящих пакетов с указанными значениями DSCP задает новое значение DSCP. - *dscp_list* – определяет до 8 значений DSCP, значения разделяются знаком пробела. - *dscp_mark_down* – определяет новое значение dscp. **Действует только для режима qos advanced.**
no qos map policed-dscp [*dscp_list*]		Устанавливает значение по умолчанию.
qos map dscp-queue *dscp_list* **to** *queue_id*	dscp_list: (0..63) queue_id: (1..8) Значения по умолчанию:	Устанавливает соответствие между значениями DSCP входящих пакетов и очередями. - *dscp_list* – определяет до 8 значений DSCP, значения разделяются знаком пробела.

no qos map dscp-queue [*dscp_list*]	DSCP: (0-7), очередь 1 DSCP: (8-15), очередь 2 DSCP: (16-23), очередь 3 DSCP: (24-31), очередь 4 DSCP: (32-39), очередь 5 DSCP: (40-47), очередь 6 DSCP: (48-55), очередь 7 DSCP: (56-63), очередь 8	Устанавливает значения по умолчанию
qos trust {cos | dscp | cos-dscp}	-/cos	Устанавливает режим доверия коммутатора в базовом режиме QoS (CoS или DSCP). - **cos** – устанавливает классификацию входящих пакетов по значениям CoS. Для нетегированных пакетов используется значение CoS по умолчанию; - **dscp** – устанавливает классификацию входящих пакетов по значениям DSCP. - **cos-dscp** – устанавливает классификацию входящих пакетов по значениям DSCP для IP-пакетов и по значениям CoS для не IP-пакетов. **Действует только для режима qos basic.**
no qos trust		Устанавливает значения по умолчанию.
qos dscp-mutation	-	Позволяет применить таблицу изменений dscp к совокупности dscp-доверенных портов. Использование таблицы изменений позволяет перезаписать значения dscp в IP-пакетах на новые значения. **Применить таблицу изменений DSCP возможно только для входящего трафика доверенных портов.** **Действует только для режима qos basic.**
no qos dscp-mutation		Отменяет использование карты изменений dscp.
qos map dscp-mutation *in_dscp* **to** *out_dscp*	in_dscp: (0..63); out_dscp: (0..63) По умолчанию карта изменений является пустой, то есть значения DSCP для всех входящих пакетов остаются неизменными	Заполняет таблицу перемаркировки DSCP. Для входящих пакетов с указанными значениями DSCP задает новые значения DSCP. - *in-dscp* – определяет до 8 значений DSCP, значения разделяются знаком пробела. - *out-dscp* – определяет до 8 новых значений DSCP, значения разделяются знаком пробела. **Действует только для режима qos basic.**
no qos map dscp-mutation [*in_dscp*]	-	Устанавливает значения по умолчанию.
rate-limit vlan *vlan_id rate burst*	vlan_id: (1..4094); rate: (3..57982058) кбит/с; burst: (3000..19173960) байт/128 кбайт	Устанавливает ограничение скорости для входящего трафика для заданной VLAN. - *vlan_id* – номер VLAN: - *rate* – средняя скорость трафика (CIR); - *burst* – размер сдерживающего порога (ограничение скорости) в байтах.
no rate-limit vlan *vlan_id*		Снимает ограничение скорости входящего трафика.

Команды режима редактирования списка критериев классификации трафика

Вид запроса командной строки режима редактирования списка критериев классификации трафика:

```
console# configure
console(config)# class-map class-map-name [match-all | match-any]
console(config-cmap)#
```

Таблица 217 – Команды режима редактирования списка критериев классификации трафика

Команда	*Значение/Значение по умолчанию*	*Действие*
match access-group *acl_name*	acl_name: (1..32) символов	Добавляет критерий классификации трафика. Определяет правила фильтрации трафика по списку ACL для классификации. **Действует только для режима qos advanced.**
no match access-group *acl_name*		Удаляет критерий классификации трафика.

Команды режима редактирования стратегии классификации трафика

Вид запроса командной строки режима редактирования стратегии классификации трафика:

```
console# configure
console(config)# policy-map policy-map-name
console(config-pmap)#
```

Таблица 218 – Команды режима редактирования стратегии классификации трафика

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

Команды режима конфигурации правила классификации

Вид запроса командной строки режима конфигурации правила классификации:

```
console# configure
console(config)# policy-map policy-map-name
console(config-pmap)# class class-map-name [access-group acl-name]
console(config-pmap-c)#
```

Таблица 219 – Команды режима конфигурации правила классификации

Команда	*Значение/Значение по умолчанию*	*Действие*
trust	По умолчанию режим доверия не установлен	Определяет режим доверия к определенному типу трафика согласно глобальному режиму доверия.
no trust		Устанавливает значение по умолчанию.

set {dscp *new_dscp* **| queue** *queue_id* **| cos** *new_cos* **| vlan** *vlan_id***}**	new_dscp: (0..63); queue_id: (1..8); new_cos: (0..7); vlan_id: (1..4094)	Устанавливает новые значения для IP-пакета. **Команда set является взаимоисключающей с командой trust для одной и той же стратегии policy-map.** **Стратегии policy-map, использующие команды set, trust или имеющий классификацию ACL, назначаются только для исходящих интерфейсов.** **Действует только для режима qos advanced.**
no set		Удаляет новые значения для IP-пакета.
redirect { tengigabitethernet *te_port* **| port-channel** *group***}**	te_port: (1..8/0/1..32); group: (1..32)	Направляет пакеты, удовлетворяющие правилу классификации трафика, в указанный порт.
no redirect		Устанавливает значение по умолчанию.
police *committed_rate_kbps committed_burst_byte* [**exceed-action {drop | policed-dscp-transmit}]**	committed_rate_kbps: (3..12582912) кбит/с; committed_burst_byte: (3000..19173960) байт; aggregate_policer_name: (1..32) символов	Позволяет ограничить полосу пропускания канала и в то же время гарантировать определенную скорость передачи данных. При работе с полосой пропускания используется алгоритм маркированной «корзины». Задачей алгоритма является принятие решения: передать пакет или отбросить. Параметрами алгоритма являются скорость поступления (CIR) маркеров в «корзину» и объём (CBS) «корзины». - *committed_rate_kbps* – среднее значение скорости трафика. Данная скорость гарантируется при передаче информации; - *committed_burst_byte* – размер сдерживающего порога в байтах; - **drop** – пакет будет отброшен, когда «корзина» переполнится; - **policed-dscp-transmit** – при переполнении «корзины», значение DSCP будет переопределено. **Действует только для режима qos advanced.**
police aggregate *aggregate_policer_name*		Назначает правилу классификации трафика шаблон настроек, который позволяет ограничить полосу пропускания канала и в то же время гарантировать определенную скорость передачи данных. **Действует только для режима qos advanced.**
no police		Удаляет шаблон настроек регулирования скорости канала из правила классификации трафика.

Команды режима конфигурации интерфейса Ethernet, группы портов

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

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

Таблица 220 – Команды режима конфигурации интерфейса Ethernet, группы портов

Команда	***Значение/Значение по умолчанию***	***Действие***
service-policy {input | output} *policy_map_name* **[default-action {deny-any | permit-any}]**	policy_map_name: (1..32) символов	Назначает интерфейсу стратегию классификации трафика.
no service-policy {input | output}		Удаляет стратегию классификации трафика с интерфейса.

traffic-shape *committed_rate* **[***committed_burst***]**	committed_rate: (64..1000000) кбит/с; committed_burst: (4096..16762902) байт	Устанавливает ограничение скорости для исходящего трафика через интерфейс. - *committed_rate* – средняя скорость трафика, кбит/с; - *committed_burst* – размер сдерживающего порога (ограничение скорости) в байтах.
no traffic-shape		Снимает ограничение скорости исходящего трафика через интерфейс.
traffic-shape queue *queue_id committed_rate* [*committed_burst*]	queue_id: (0..8); committed_rate: (36..1000000) кбит/с; committed_burst: (4096..16769020) байт	Устанавливает ограничение скорости трафика через интерфейс для исходящей очереди. - *committed_rate* – средняя скорость трафика, кбит/с; - *committed_burst* – размер сдерживающего порога (ограничение скорости) в байтах.
no traffic-shape queue *queue_id*		Снимает ограничение скорости трафика через интерфейс для исходящей очереди.
qos trust [cos | dscp | cos-dscp]	-/включено	Включает базовый механизм qos для интерфейса. - **cos** – порт доверяет значению 802.1p User priority; - **dscp** – порт доверяет значению DSCP в IPv4/IPv6-пакетах; **- cos-dscp – порт доверяет обоим уровням, однако DSCP имеет приоритет над 802.1p.**
no qos trust		Выключает базовый механизм qos для интерфейса.
rate-limit *rate* **[burst** *burst***]**	rate: (64..10000000) кбит/с; burst: (3000..19173960) байт/128 кбайт	Устанавливает ограничение скорости для входящего трафика.
no rate-limit		Снимает ограничение скорости входящего трафика.
qos cos *default_cos*	default_cos: (0..7)/0	Устанавливает значение CoS по умолчанию для порта (CoS, применяемый для всего нетегированного трафика, проходящего через интерфейс).
no qos cos		Устанавливает значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 221 – Команды режима EXEC

Команда	***Значение/значение по умолчанию***	***Действие***
show qos	-	Показывает режим QOS, настроенный на устройстве. В базовом режиме показывает «доверенный» режим (trust mode).
show class-map [*class_map_name***]**	class_map_name: (1..32) символа	Показывает списки критериев классификации трафика. **Действует только для режима qos advanced.**
show policy-map [*policy_map_name***]**	policy_map_name: (1..32) символа	Показывает правила классификации трафика. **Действует только для режима qos advanced.**
show qos aggregate-policer [*aggregate_policer_name***]**	aggregate_policer_name: (1..32) символа	Показывает настройки средней скорости и ограничения полосы пропускания для правил классификации трафика. **Действует только для режима qos advanced.**

show qos interface [buffers | queuing | policers | shapers] [tengigabitethernet *te_port* **| port-channel** *group* **| vlan** *vlan_id***]**	te_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094)	Показывает QoS-параметры для интерфейса. - *vlan_id* – номер VLAN; - *te_port* – номер интерфейсов Ethernet XG1-XG12; - *group* – номер группы портов; - **buffers** – настройки буфера для очередей интерфейса; - **queueing** – алгоритм обработки очередей (WRR или EF), вес для WRR-очередей, классы обслуживания для очередей и приоритет для EF; - **policers** – сконфигурированные стратегии классификации трафика для интерфейса; - **shapers** – ограничение скорости для исходящего трафика.
show qos map [dscp-queue | dscp-dp | policed-dscp | dscp-mutation]	-	Показывает информацию о замене полей в пакетах, используемых QOS. - **dscp-queue** – таблица соответствия DSCP и очередей; - **dscp-dp** – таблица соответствия меток DSCP и приоритета сброса (DP); - **policed-dscp** – таблица перемаркировки DSCP; - **dscp-mutation** – таблица изменения DSCP-to-DSCP.

Примеры выполнения команд

- Включить режим QoS advanced. Распределить трафик по очередям, пакеты с DSCP 12 в первую очередь, пакеты с DSCP 16 во вторую. Восьмая очередь – приоритетная. Создать стратегию классификации трафика по списку ACL, разрешающему передачу TCP-пакетов с DSCP 12 и 16 и ограничивающую скорость – средняя скорость 1000 Кбит/с, порог ограничения 200000 байт. Использовать данную стратегию на интерфейсах Ethernet 14 и 16.

```
console#
console# configure
console(config)# ip access-list tcp_ena
console(config-ip-al)# permit tcp any any any any dscp 12
console(config-ip-al)# permit tcp any any any any dscp 16
console(config-ip-al)# exit
console(config)# qos advanced
console(config)# qos map dscp-queue 12 to 1
console(config)# qos map dscp-queue 16 to 2
console(config)# priority-queue out num-of-queues 1
console(config)# policy-map traffic
console(config-pmap)# class class1 access-group tcp_ena
console(config-pmap-c)# police 1000 200000 exceed-action drop
console(config-pmap-c)# exit
console(config-pmap)# exit
console(config)# interface tengigabitethernet 1/0/14
console(config-if)# service-policy input traffic
console(config-if)# exit
console(config)# interface tengigabitethernet 1/0/16
console(config-if)# service-policy input traffic
console(config-if)# exit
console(config)#
```

6.7.2 Статистика QoS

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 222 – Команды режима глобальной конфигурации.

Команда	*Значение/Значение по умолчанию*	*Действие*
qos statistics aggregate-policer *aggregate_policer_name*	aggregate_policer_name: (1..32) символов; По умолчанию QoS-статистика отключена	Включает QoS-статистику по ограничению полос пропускания.
no qos statistics aggregate-policer *aggregate_policer_name*		Отключает QoS-статистику по ограничению полос пропускания.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 223 – Команды режима EXEC.

Команда	*Значение/ Значение по умолчанию*	*Действие*
clear qos statistics	-	Очищает статистику QoS.
show qos statistics	-	Показывает статистику QoS.

6.8 Конфигурация протоколов маршрутизации

6.8.1 Конфигурация статической маршрутизации

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 224 – Команды режима глобальной конфигурации

Команда	*Значение/ Значение по умолчанию*	*Действие*
ip route *prefix* **{***mask* **|** *prefix_length***} {***gateway* **[metric** *distance***] | reject-route}**	prefix_length: (0..32); distance (1..255)/1	Создает статическое правило маршрутизации. - *prefix* – сеть назначения (например 172.7.0.0); - *mask* – маска сети (в формате десятичной системы исчисления); - *prefix_length* – префикс маски сети (количество единиц в маске); - *gateway* – шлюз для доступа к сети назначения; - *distance* – вес маршрута; - **reject-route** – запрещает маршрутизацию к сети назначения через все шлюзы.
ip route *prefix* **{***mask* **|** *prefix_length***} {***gateway* **| reject-route}**		Удаляет правило из таблицы статической маршрутизации.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 225 – Команды режима EXEC

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

Пример выполнения команды

- Показать таблицу маршрутизации:

```
console# show ip route
```

```
Maximum Parallel Paths: 2 (4 after reset)
Codes: C - connected, S - static
C 10.0.1.0/24 is directly connected, Vlan  1
S  10.9.1.0/24 [5/2]     via 10.0.1.2, 17:19:18, Vlan 12
S  10.9.1.0/24 [5/3]     via 10.0.2.2, Backup Not Active
S 172.1.1.1/32 [5/3]    via 10.0.3.1, 19:51:18, Vlan 12
```

Таблица 226 – Описание результата выполнения команды

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

6.8.2 Настройка протокола RIP

Протокол RIP (англ. Routing Information Protocol) — внутренний протокол, который позволяет маршрутизаторам динамически обновлять маршрутную информацию, получая ее от соседних маршрутизаторов. Это очень простой протокол, основанный на применении дистанционного вектора маршрутизации. Как дистанционно-векторный протокол, RIP периодически посылает обновления между соседями, строя, таким образом, топологию сети. В каждом обновлении передается информация о дистанции до всех сетей на соседний маршрутизатор. Коммутатор поддерживает протокол RIP версии 2.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 227 – Команды режима глобальной конфигурации

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

Команды режима конфигурации протокола RIP

Вид запроса командной строки:

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

Таблица 228 – Команды режима конфигурации протокола RIP

Команда	*Значение/Значение по умолчанию*	*Действие*
default-metric [*metric***]**	metric: (1..15)/1	Устанавливает значение метрики, с которой будут анонсироваться маршруты, полученные другими протоколами маршрутизации. Без параметра устанавливает значение по умолчанию.
no default-metric		Устанавливает значение по умолчанию.
network *A.B.C.D*	A.B.C.D: IP-адрес интерфейса	Устанавливает IP-адрес интерфейса, который будет участвовать в процессе маршрутизации.
no network *A.B.C.D*		Удаляет IP-адрес интерфейса, который будет участвовать в процессе маршрутизации.
redistribute {static | connected } [metric transparent]	-	Разрешает анонсирование маршрутов через RIP. - без параметров – означает, что будет использоваться **default-metric** при анонсировании маршрутов**;** - **metric transparent** – означает, что будет использоваться метрика из таблицы маршрутизации**.**
no redistribute {static | connected} [metric transparent]		Запрещает анонсирование статических маршрутов через RIP. - **metric transparent** – запрещает использовать метрику из таблицы маршрутизации**.**
redistribute ospf [metric *metric* **| match** *type* **| route-map** *route_map_name***]**	metric: (1..15, transparent)/1; match: (internal, external-1, external-2); route_map_name: (1..32) символа	Разрешает анонсирование OSPF маршрутов через RIP. - *type* – производить анонсирование только для указанных типов OSPF маршрутов; - *route-map_name* – производить анонсирование маршрутов после их фильтрации через указанную route-map;
shutdown	-/включено	Выключают процесс маршрутизации по протоколу RIP.
no shutdown		Включают процесс маршрутизации по протоколу RIP.
passive-interface	-/включено	Отключить обновления маршрутизации.
no passive-interface		Включить обновления маршрутизации.
default-information originate	-/маршрут не генерируется	Генерировать маршрут по умолчанию
no default-information originate		Восстановить значение по умолчанию.

Команды режима конфигурации интерфейса IP

Вид запроса командной строки:

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

Таблица 229 – Команды режима конфигурации интерфейса IP

Команда	*Значение/ Значение по умолчанию*	*Действие*
ip rip shutdown	-/включено	Выключают процесс маршрутизации по протоколу RIP на данном интерфейсе.
no ip rip shutdown		Включают процесс маршрутизации по протоколу RIP на данном интерфейсе.
ip rip passive-interface	По умолчанию отправка обновлений включена	Выключает отправку обновлений на интерфейсе.
no ip rip passive-interface		Устанавливает значение по умолчанию.
ip rip offset *offset*	offset: (1..15)/1	Добавляет смещение к метрике.
no ip rip offset		Устанавливает значение по умолчанию.
ip rip default-information originate *metric*	metric: (1..15)/1; По умолчанию функция отключена	Устанавливает метрику для маршрута по умолчанию транслируемого через RIP.
no ip rip default-information originate		Устанавливает значение по умолчанию.
ip rip authentication mode {text | md5}	По умолчанию аутентификация отключена.	Включает аутентификацию в RIP и определяет ее тип: - **text** – аутентификация открытым текстом; - **md5** – аутентификации MD5.
no ip rip authentication mode		Устанавливает значение по умолчанию.
ip rip authentication key-chain *key_chain*	key_chain: (1..32) символов	Определяет набор ключей, который может использоваться для аутентификации.
no ip rip authentication key-chain		Устанавливает значение по умолчанию.
ip rip authentication-key *clear_text*	clear_text: (1..16) символов	Определяет ключ для аутентификации открытым текстом.
no ip rip authentication-key		Устанавливает значение по умолчанию.
ip rip distribute-list access *acl_name*	acl_name: (1..32) символов	Устанавливает стандартный IP ACL для фильтрации анонсируемых маршрутов.
no ip rip distribute-list		Устанавливает значение по умолчанию.

Команды режима privileged EXEC

Вид запроса командной строки в режиме privileged EXEC:

```
console#
```

Таблица 230 – Команды режима privileged EXEC

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

Примеры использования команд

Включить протокол RIP для подсети 172.16.23.0 (IP-адрес на коммутаторе **172.16.23.1**) и аутентификацию MD5 через набор ключей mykeys:

```
console#
console# configure
console(config)# router rip
console(config-rip)# network 172.16.23.1
console(config-rip)# interface ip 172.16.23.1
console(config-if)# ip rip authentication mode md5
console(config-if)# ip rip authentication key-chain mykeys
```

6.8.3 Настройка протокола OSPF, OSPFv3

OSPF (*Open Shortest Path First*) — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути алгоритм Дейкстры. Протокол OSPF представляет собой протокол внутреннего шлюза (IGP). Протокол OSPF распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы.

Устройство поддерживает одновременную работу нескольких независимых экземпляров процессов OSPF. Настройка параметров экземпляра OSPF производится путем указания идентификатора экземпляра (**process_id**).

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 231 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
router ospf [*process_id***]**	process_id: (1..65535)/1	Включает маршрутизацию по протоколу OSPF. Задает идентификатор процесса.
no router ospf [*process_id***]**		Выключает маршрутизацию по протоколу OSPF.
ipv6 router ospf [*process_id***]**	process_id: (1..65535)/1	Включает маршрутизацию по протоколу OSPFv3. Задает идентификатор процесса.
no ipv6 router ospf [*process_id***]**		Выключает маршрутизацию по протоколу OSPFv3.
ipv6 distance ospf {inter-as | intra-as} *distance*	distance: (1..255)	Задает административную дистанцию для маршрутов OSPF, OSPFv3. - **inter-as –** для внешних автономных систем - **intra-as –** внутри автономной системы
no ipv6 distance ospf {inter-as | intra-as}		Возвращает значения по умолчанию.

Команды режима процесса OSPF

Вид запроса командной строки в режиме конфигурации процесса OSPF:

```
console(router_ospf_process)#
console(ipv6 router_ospf_process)#
```

Таблица 232 – Команды режима конфигурации процесса OSPF

Команда	*Значение/Значение по умолчанию*	*Действие*
redistribute connected [metric *metric***] [route-map** *name***] [subnets]**	metric: (1..65535); name: (1..255) символов	Разрешает анонсирование connected маршрутов: - *metric* – значение метрики для импортируемых маршрутов; - *name* – имя политики импорта, позволяющей фильтровать и вносить изменения в импортируемые маршруты; - **subnets** – позволяет импортировать подсети.
no redistribute connected [metric *metric***] [route-map** *name***] [subnets]**		Запрещает указанную функцию.

redistribute static [metric *metric*] **[route-map** *name*] **[subnets]**	metric: (1..65535); name: (1..255) символов	Импорт статических маршрутов в OSPF. - *metric* – устанавливает значение метрики для импортируемых маршрутов; - *name* – применяет политику импорта, позволяющую фильтровать и вносить изменения в импортируемые маршруты; - **subnets** – позволяет импортировать подсети.
no redistribute static [metric *metric* **] [route-map** *name*] **[subnets]**		Запрещает указанную функцию.
redistribute ospf *id* **[nssa-only] [metric** *metric*] **[metric-type {type-1 | type-2}] [route-map** *name*] **[match {internal | external-1 | external-2}] [subnets]**	id: (1..65535); metric: (1..65535); name: (0..32) символа.	Импорт маршрутов из процесса OSPF в процесс OSPF: - **nssa-only** – устанавливает значение nssa-only для всех импортируемых маршрутов; - **metric-type type-1** – импортирует с пометкой как OSPF external 1; - **metric-type type-2** импортирует с пометкой как OSPF external 2; - **match internal** – импортирует маршруты в пределах area; - **match external-1** – импортирует маршруты типа OSPF external 1; - **match external-2** – импортирует маршруты типа OSPF external 2; - **subnets** – позволяет импортировать подсети; - *name* – применяет указанную политику импорта, позволяющую фильтровать и вносить изменения в импортируемые маршруты; - *metric* – устанавливает значение метрики для импортируемых маршрутов.
no redistribute ospf [*id***] [nssa-only] [metric** *metric*] **[metric-type {type-1 | type-2}] [route-map** *name*] **[match {internal | external-1 | external-2}] [subnets]**		Запрещает указанную функцию.
redistribute rip [metric *metric*] **[route-map** *name*] **[subnets]**	metric: (1..65535); name: (1..255) символа	Импорт маршрутов из RIP в OSPF. - *metric* – значение метрики для импортируемых маршрутов; - *name* – имя политики импорта, позволяющей фильтровать и вносить изменения в импортируемые маршруты; - **subnets** – позволяет импортировать подсети.
no redistribute rip [metric *metric*] **[route-map** *name*] **[subnets]**		Запрещает указанную функцию.
router-id *A.B.C.D*	A.B.C.D: идентификатор маршрутизатора в формате ipv4-адреса	Устанавливает идентификатор маршрутизатора, который уникально идентифицирует маршрутизатор в пределах одной автономной системы.
no router-id *A.B.C.D*		Устанавливает значение по умолчанию.
network *ip_addr* **area** *A.B.C.D* **[shutdown]**	ip_addr: A.B.C.D	Включить (отключить) экземпляр OSPF на IP-интерфейсе (для IPv4).
no network *ip addr*		Удаляет IP-адрес интерфейса.
default-metric *metric*	metric: (1..65535)	Устанавливает метрику OSPF-маршрута.
no default-metric		Отключение функции.
area *A.B.C.D* **stub [no-summary]**	A.B.C.D: идентификатор маршрутизатора в формате IPv4-адреса	Устанавливает для указанной зоны тип stub. Зона – совокупность сетей и маршрутизаторов, имеющих один и тот же идентификатор. - **no-summary** – не отправлять информацию о суммированных внешних маршрутах.
no area *A.B.C.D* **stub**		Устанавливает значение по умолчанию.

area *A.B.C.D* **nssa [no-summary] [translator-stability-interval** *interval***] [translator-role {always | candidate}]**	A.B.C.D: идентификатор маршрутизатора в формате IPv4-адреса; interval: целое положительное число;	Устанавливает для указанной зоны тип NSSA. - **no-summary** – не принимать информацию о суммированных внешних маршрутах внутрь NSSA-зоны; - *interval* **–** определяет промежуток времени (в сек), в течение которого транслятор будет выполнять свои функции после того, как обнаружит, что транслятором стал другой граничный маршрутизатор. - **translator-role** – определяет, каким образом на маршрутизаторе будет функционировать режим транслятора (трансляции Type-7 LSA в Type-5 LSA): - **always** – в принудительном постоянном режиме; - **candidate** – в режиме участия в выборах транслятора.
no area *A.B.C.D* **nssa**		Устанавливает значение по умолчанию.
area *A.B.C.D* **virtual-link** *A.B.C.D* **[hello-interval** *secs***] [retransmit-interval** *secs***] [transmit-delay** *secs***] [dead-interval** *secs***] [null | message-digest] [key-chain** *word***]**	A.B.C.D: идентификатор маршрутизатора в формате IPv4-адреса; secs: (1..65535) секунд; word: (1..256) символов	Создание виртуального соединения между основной и другими удаленными областями, которые имеют между ними области. - **hello-interval** – указать hello-интервал; - **retransmit-interval** – указать интервал меду повторными передачами; - **transmit-delay** – указать время задержки; - **dead-interval** – указать dead-интервал; - **null** – без аутентификации; - **message-digest** – аутентификация с шифрованием; - *word* – пароль для аутентификации.
no area *A.B.C.D* **virtual-link** *A.B.C.D* **[hello-interval** *secs***] [retransmit-interval** *secs***] [transmit-delay** *secs***] [dead-interval** *secs***] [null | message-digest] [key-chain** *word***]**		Удаляет виртуальное соединение.
area *A.B.C.D* **default-cost** *cost*	A.B.C.D: идентификатор маршрутизатора в формате IPv4-адреса; cost: целое положительное число	Устанавливает значение стоимости суммарного маршрута, используемого для stub- и NSSA-зон (для IPv4).
no area *A.B.C.D* **default-cost**		Устанавливает значение по умолчанию.
area *A.B.C.D* **authentication [message-digest]**	A.B.C.D: идентификатор маршрутизатора в формате IPv4-адреса; -/выключено	Включает аутентификацию для всех интерфейсов данной зоны (для IPv4): - **message-digest** – с шифрованием MD5.
no area *A.B.C.D* **authentication [message-digest]**		Отключает аутентификацию.
area *A.B.C.D* **range** *network_address mask* **[advertise | not-advertise]**	A.B.C.D: идентификатор маршрутизатора в формате IPv4-адреса; network_address*:* A.B.C.D; mask: E.F.G.H	Создает суммарный маршрут на границе зоны (для IPv4). - **advertise** – анонсировать созданный маршрут; - **not-advertise** – не анонсировать созданный маршрут.
no area *A.B.C.D* **range** *network_address mask*		Удаляет суммарный маршрут.
area *A.B.C.D* **filter-list prefix** *prefix_list* **in**	A.B.C.D: идентификатор маршрутизатора в формате IPv4-адреса; prefix_list: (1..32) символа	Устанавливает фильтр на маршруты, анонсируемые в указанную зону из других зон (для IPv4).
no area *A.B.C.D* **filter-list prefix** *prefix_list* **in**		Удаляет фильтр на маршруты, анонсируемые в указанную зону из других зон (для IPv4).
area *A.B.C.D* **filter-list prefix** *prefix_list* **out**	A.B.C.D: идентификатор маршрутизатора в формате IPv4-адреса; prefix_list: (1..32) символа	Устанавливает фильтр на маршруты, анонсируемые из указанной зоны в другие зоны (для IPv4).
no area *A.B.C.D* **filter-list prefix** *prefix_list* **out**		Удаляет фильтр на маршруты, анонсируемые из указанной зоны в другие зоны (для IPv4).
area *A.B.C.D* **shutdown**	A.B.C.D:	Отключает процесс OSPF для зоны.

no area *A.B.C.D* **shutdown**	идентификатор маршрутизатора в формате IPv4-адреса; -/включено	Включает процесс OSPF для зоны.
shutdown	-/включено	Отключает процесс OSPF.
no shutdown		Включает процесс OSPF.

Команды режима конфигурации интерфейса IP

Вид запроса командной строки:

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

Таблица 233 – Команды режима конфигурации интерфейса IP

Команда	*Значение/Значение по умолчанию*	*Действие*
ip ospf shutdown	-/включено	Выключает маршрутизацию по протоколу OSPF на интерфейсе.
no ip ospf shutdown		Включает маршрутизацию по протоколу OSPF на интерфейсе.
ip ospf authentication [key-chain *key_chain* **| null | message-digest]**	key_chain: (1..32) символов; По умолчанию аутентификация отключена	Включает аутентификацию в OSPF и определяет ее тип: - *key_chain* – имя набора ключей, созданного командой key chain; - **null** – не использовать аутентификацию; - **message-digest** – аутентификация MD5.
no ip ospf authentication [key-chain]		Устанавливает значение по умолчанию.
ip ospf authentication-key *key*	key: (1..8) символов	Назначает пароль для аутентификации соседей, доступных через текущий интерфейс. Пароль, указанный таким образом, будет внедрен в заголовок каждого уходящего в эту сеть пакета OSPF в качестве ключа аутентификации.
no ip ospf authentication-key		Удаляет пароль.
ip ospf cost *cost*	cost: (1..65535)/10	Устанавливает метрику состояния канала, которая является условным показателем "стоимости" пересылки данных по каналу.
no ip ospf cost		Устанавливает значение по умолчанию.
ip ospf dead-interval {*interval* **| minimal}**	interval: (1..65535) секунд; minimal – 1сек	Устанавливает интервал времени в секундах, по истечении которого сосед будет считаться неактивным. Этот интервал должен быть кратным значению hello-interval. Как правило, dead-interval равен 4 интервалам отправки hello-пакетов.
no ip ospf dead-interval		Устанавливает значение по умолчанию.
ip ospf hello-interval *interval*	interval: (1..65535)/10 секунд	Устанавливает интервал времени в секундах, по истечении которого маршрутизатор отправляет следующий hello-пакет с интерфейса.
no ip ospf hello-interval		Устанавливает значение по умолчанию.
ip ospf mtu-ignore	-/enabled	Отключение проверки MTU.
no ip ospf mtu-ignore		Устанавливает значение по умолчанию.
ip ospf passive-interface	-/disabled	Запрещает IP-интерфейсу обмениваться протокольными сообщениями с соседями через указанный физический интерфейс.
no ip ospf passive-interface		Разрешает IP-интерфейсу обмениваться протокольными сообщениями с соседями.
ip ospf priority *priority*	priority: (0..255)/1	Устанавливает приоритет маршрутизатора, который используется для выбора DR и BDR.
no ip ospf priority		Устанавливает значение по умолчанию.

Команды режима конфигурации интерфейса Ethernet, VLAN:

Вид запроса командной строки:

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

Таблица 234 – Команды режима конфигурации интерфейса Ethernet, VLAN

Команда	*Значение/Значение по умолчанию*	*Действие*
ipv6 ospf shutdown	-/включено	Выключает маршрутизацию по протоколу OSPFv3 на интерфейсе.
no ipv6 ospf shutdown		Включает маршрутизацию по протоколу OSPFv3 на интерфейсе.
ipv6 ospf *process* **area** *area* **[shutdown]**	process: (1..65536); area: идентификатор маршрутизатора в формате IPv4-адреса	Включить (отключить) OSPF процесс для определенной зоны.
ipv6 ospf cost *cost*	cost: (1..65535)/10	Устанавливает метрику состояния канала, которая является условным показателем "стоимости" пересылки данных по каналу.
no ipv6 ospf cost		Устанавливает значение по умолчанию.
ipv6 ospf dead-interval *interval*	interval: (1**..**65535***)*** секунд	Устанавливает интервал времени в секундах, по истечении которого сосед будет считаться неактивным. Этот интервал должен быть кратным значению hello-interval. Как правило, dead-interval равен 4 интервалам отправки hello-пакетов.
no ipv6 ospf dead-interval		Устанавливает значение по умолчанию.
ipv6 ospf hello-interval *interval*	interval: (1..65535)/10 секунд	Устанавливает интервал времени в секундах, по истечении которого маршрутизатор отправляет следующий hello-пакет с интерфейса.
no ipv6 ospf hello-interval		Устанавливает значение по умолчанию.
ipv6 ospf mtu-ignore	-/disabled	Отключение проверки MTU**.**
no ipv6 ospf mtu-ignore		Устанавливает значение по умолчанию.
ipv6 ospf neighbor {*ipv6_address***}**	-	Задает IPv6 адрес соседа.
ipv6 ospf neighbor {*ipv6_address***}**		Удаляет IPv6 адрес соседа.
ipv6 ospf priority *priority*	priority: (0..255)/1	Устанавливает приоритет маршрутизатора, который используется для выбора DR и BDR.
no ipv6 ospf priority		Устанавливает значение по умолчанию.
ipv6 ospf retransmit-interval *interval*	interval: (1..65535)/5 секунд	Устанавливает интервал времени в секундах, по истечении которого маршрутизатор повторно отправит пакет, на который не получил подтверждения о получении (например, Database Description пакет или Link State Request пакеты).
no ipv6 ospf retransmit-interval		Устанавливает значение по умолчанию.
ipv6 ospf transmit-delay *delay*	delay: (1..65535)/1 секунд	Устанавливает примерное время в секундах, необходимое для передачи пакета состояния канала.
no ip ospf transmit-delay		Устанавливает значение по умолчанию.

Команды режима privileged EXEC

Вид запроса командной строки в режиме privileged EXEC:

```
console#
```

Таблица 235 – Команды режима privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show {ip | ipv6} ospf [*process_id***]**	process_id: (1..65536)	Отображает конфигурации OSPF.
show {ip | ipv6} ospf [*process_id***] neighbor**	process_id: (1..65536)	Отображает информации об OSPF-соседях.
show ip ospf [*process_id***] neighbor** *A.B.C.D*	process_id: (1..65536); A.B.C.D: IP-адрес соседа	Отображает информации об OSPF-соседе с указанным адресом.
show {ip | ipv6} ospf [*process_id***] interface**	process_id: (1..65536)	Отображает конфигурации всех OSPF-интерфейсов.
show {ip | ipv6} ospf [*process_id***] interface [***ip_int* **| brief]**	process_id: (1..65535);	Отображает конфигурации конкретного OSPF-интерфейса.
show {ip | ipv6} ospf [*process_id***] database**	process_id: (1..65535)	Отображает состояние базы данных протокола OSPF.
show {ip | ipv6} ospf virtual-links [*process_id***]**	process_id: (1..65535)	Отображает параметры и текущее состояние виртуальных линков.

6.8.4 Настройка Virtual Router Redundancy Protocol (VRRP)

Протокол VRRP предназначен для резервирования маршрутизаторов, выполняющих роль шлюза по умолчанию. Это достигается путём объединения IP-интерфейсов группы маршрутизаторов в один виртуальный, который будет использоваться как шлюз по умолчанию для компьютеров в сети. На канальном уровне резервируемые интерфейсы имеют MAC-адрес 00:00:5E:00:01:XX, где XX – номер группы VRRP (VRID).

Только один из физических маршрутизаторов может выполнять маршрутизацию трафика на виртуальном IP-интерфейсе (VRRP master), остальные маршрутизаторы в группе предназначены для резервирования (VRRP backup). Выбор VRRP master происходит в соответствии с RFC 5798. Если текущий master становится недоступным – выбор master'а повторяется. Наивысший приоритет имеет маршрутизатор с собственным IP-адресом, совпадающим с виртуальным. В случае доступности он всегда становится VRRP master. Максимальное количество VRRP-процессов – 50.

Команды режима конфигурации интерфейсов Ethernet, VLAN, интерфейса группы портов

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

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

Таблица 236 – Команды режима конфигурации интерфейса Ethernet, VLAN, интерфейса группы портов

Команда	*Значение/Значение по умолчанию*	*Действие*
vrrp *vrid* **description** *text*	vrid: (1..255); text: (1..160 символов).	Добавление описания цели или использования для VRRP маршрутизатора с идентификатором *vrid.*
no vrrp *vrid* **description**		Удаление описания VRRP-маршрутизатора.
vrrp *vrid* **ip** *ip_address*	vrid: (1..255)	Определение IP-адреса VRRP-маршрутизатора
no vrrp *vrid* **ip [***ip_address***]**		Удаление IP-адреса VRRP с маршрутизатора. Если в качестве параметра не указан IP-адрес, то удалятся все IP-адреса виртуального маршрутизатора, вследствие чего удалится и сам виртуальный маршрутизатор *vrid* на данном устройстве.

vrrp *vrid* **preempt**	vrid: (1..255); По умолчанию включено	Включение режима, при котором backup-маршрутизатор с более высоким приоритетом будет пытаться перехватить на себя роль master у текущего master-маршрутизатора с более низким приоритетом. **Маршрутизатор, который является владельцем IP-адреса маршрутизатора, будет перехватывать на себя роль master независимо от настроек данной команды.**
no vrrp *vrid* **preempt**		Установка значения по умолчанию.
vrrp *vrid* **priority** *priority*	vrid: (1..255); priority: (1..254); По умолчанию: 255 для владельца IP-адреса,100 для остальных	Назначение приоритета VRRP-маршрутизатора.
no vrrp *vrid* **priority**		Установка значения по умолчанию.
vrrp *vrid* **shutdown**	vrid: (1..255); По умолчанию: выключен	Выключение VRRP протокола на данном интерфейсе.
no vrrp *vrid* **shutdown**		Включение VRRP протокола на данном интерфейсе.
vrrp *vrid* **source-ip** *ip_address*	vrid: (1..255); По умолчанию: 0.0.0.0	Определение реального VRRP-адреса, который будет использоваться в качестве IP-адреса отправителя для VRRP-сообщений.
no vrrp *vrid* **source-ip**		Установка значения по умолчанию.
vrrp *vrid* **track** *track_number* **[decrement** *decrement_priority***]**	vrid: (1..255); track_number: (1..64); decrement: (1..253)	Установить количество tracking-ов для указанной группы VRRP. - *decrement_priority* – понижение приоритета маршрутизатора когда объект наблюдения становится недоступен
no vrrp *vrid* **track**		Отменить заданное количество tracking-ов для указанной группы VRRP.
vrrp *vrid* **timers advertise {***seconds* **| msec** *milliseconds***}**	seconds: (1..40); milliseconds: (50..40950); По умолчанию: 1 сек	Определение интервала между анонсами master-маршрутизатора. Если интервал задан в миллисекундах, то происходит округление вниз до ближайшей секунды для VRRP Version 2 и до ближайших сотых долей секунды (10 миллисекунд) для VRRP Version 3.
no vrrp ***vrid*** **timers advertise [msec]**		Установка значения по умолчанию.
vrrp *vrid* **version {2 | 3 | 2&3}**	-/3	Определение поддерживаемой версии VRRP протокола. - **2** – поддерживается VRRPv2, определенный в RFC3768. Получаемые VRRPv3 сообщения отбрасываются маршрутизатором. Отправляются только VRRPv2 анонсы. - **3** – поддерживается VRRPv3, определенный в RFC5798, без совместимости с VRRPv2 (8.4, RFC5798). Получаемые VRRPv2 сообщения отбрасываются маршрутизатором. Отправляются только VRRPv3 анонсы. - **2&3** – поддерживается VRRPv3, определенный в RFC5798 с обратной совместимостью с VRRPv2. Получаемые VRRPv2 сообщения обрабатываются маршрутизатором. Отправляются VRRPv2 и VRRPv3 анонсы. Поддерживается только VRRP версии 3. Режимы 2 и 2&3 будут поддерживаться в будущих версиях ПО.
no vrrp *vrid* **version**		Установка значения по умолчанию.

Команды режима privileged EXEC

Все команды доступны для привилегированного пользователя.

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 237 – Команды режима privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show vrrp [all | brief | counters interface { tengigabitethernet *te_port* **| port-channel** *group* **| vlan** *vlan_id***}]**	te_port: (1..8/0/1..32); group: (1..32); vlan_id: (1..4094)	Просмотр краткой или детальной информации для всех или одного настроенного виртуального маршрутизатора VRRP. - **all** — просмотр информации о всех виртуальных маршрутизаторах, включая отключенные; - **brief** — просмотр краткой информации о всех виртуальных маршрутизаторах; - **counters** - отображает счетчики для VRRP.

Примеры выполнения команд

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

```
console(config-vlan)# interface vlan 10
console(config-if)# ip address 10.10.10.1 /24
console(config-if)# vrrp 1 ip 10.10.10.1
console(config-if)# no vrrp 1 shutdown
```

- Посмотреть конфигурацию VRRP:

```
console# show vrrp
```

```
Interface: vlan 10
Virtual Router 1
Virtual Router name
Supported version VRRPv3
State is Initializing
Virtual IP addresses are 10.10.10.1(down)
Source IP address is 0.0.0.0(default)
Virtual MAC address is 00:00:5e:00:01:01
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 255
```

7 СЕРВИСНОЕ МЕНЮ, СМЕНА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

7.1 Меню Startup

Меню ***Startup*** используется для выполнения специальных процедур, таких как восстановление заводских настроек и восстановление пароля.

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

```
      Startup Menu
[1]  Restore Factory Defaults
[2]  Password Recovery Procedure
[3]  Back
 Enter your choice or press 'ESC' to exit:
```

Для выхода из меню и загрузки устройства нажмите клавишу **<5>**, либо **<Esc>**.

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

Таблица 238 – Описание меню Startup

№	*Название*	*Описание*
<1>	**Restore Factory Defaults** Восстановление заводских настроек	Данная процедура используется для удаления конфигурации устройства. Восстановление конфигурации по умолчанию.

<2>	**Password Recovery Procedure**
	Восстановление пароля
		Данная процедура используется для восстановления утраченного пароля, она позволяет подключиться к устройству без пароля.
		Для восстановления пароля нажать клавишу **<2>**, при последующем подключении к устройству пароль будет проигнорирован.
		`Current password will be ignored!`
		Для возврата в меню Startup нажмите клавишу **[enter].**
		`==== Press Enter To Continue ====`

<3>	**Back** Выход из меню	Для выхода из меню и загрузки устройства нажмите клавишу **<Enter>**, либо **<Esc>**.

7.2 Обновление программного обеспечения с сервера TFTP

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

Обновление программного обеспечения может осуществляться только привилегированным пользователем.

7.2.1 Обновление системного программного обеспечения

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

Если номер устройства не задан, данная команда применяется к ведущему устройству.

Для просмотра текущей версии системного программного обеспечения, работающего на устройстве, введите команду **show version**:

```
console# show version
```

```
Active-image: flash://system/images/image1.ros
  Version: 5.5.4
  Commit: 25503143
  MD5 Digest: 6f3757fab5b6ae3d20418e4d20a68c4c
  Date: 03-Jun-2016
  Time: 19:54:26
Inactive-image: flash://system/images/_image1.ros
  Version: 5.5.4
  Commit: 16738956
  MD5 Digest: d907f3b075e88e6a512cf730e2ad22f7
  Date: 10-Jun-2016
  Time: 11:05:50
```

Процедура обновления ПО:

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

boot system tftp://*tftp_ip_address*/*[directory/]filename*

Пример выполнения команды:

```
console# boot system tftp://10.10.10.1/image1.ros
```

```
26-Feb-2016 11:07:54 %COPY-I-FILECPY: Files Copy - source URL
tftp://10.10.10.1/image.ros destination URL flash://
system/images/mes5324-401.ros
26-Feb-2016 11:08:53 %COPY-N-TRAP: The copy operation was completed successfully

Copy: 20644469 bytes copied in 00:00:59 [hh:mm:ss]
```

Новая версия программного обеспечения станет активной после перезагрузки коммутатора.

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

```
console#show bootvar
```

```
Active-image: flash://system/images/image1.ros
  Version: 5.5.4
  MD5 Digest: 0534f43d80df854179f5b2b9007ca886
  Date: 01-Mar-2016
  Time: 17:17:31
  Inactive-image: flash://system/images/_image1.ros
  Version: 5.5.4
```

```
  MD5 Digest: b66fd2211e4ff7790308bafa45d92572
  Date: 26-Feb-2016
  Time: 11:08:56
```

```
console# reload
```

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

Подтвердите перезагрузку вводом '**y**'.

ПРИЛОЖЕНИЕ А. ПРИМЕРЫ ПРИМЕНЕНИЯ И КОНФИГУРАЦИИ УСТРОЙСТВА

Настройка протокола множества связующих деревьев (MSTP)

Протокол MSTP позволяет строить множество связующих деревьев для отдельных групп VLAN на коммутаторах локальной сети, что позволяет балансировать нагрузку. Для простоты рассмотрим случай с тремя коммутаторами, объединенными в кольцевую топологию.

Пусть vlan 10, 20, 30 объединяются в первом экземпляре MSTP, vlan 40, 50, 60 объединяются во втором экземпляре. Необходимо, чтобы трафик VLAN-ов 10, 20, 30 между первым и вторым коммутаторами передавался напрямую, а трафик VLAN-ов 40, 50, 60 передавался транзитом через коммутатор 3. Коммутатор 2 назначим корневым для внутреннего связующего дерева (IST – Internal Spanning Tree) в котором передается служебная информация. Коммутаторы объединяются в кольцо, используя порты te1 и te2. Ниже приведена схема, изображающая логическую топологию сети.

Рисунок А.1 – Настройка протокола множества связующих деревьев

Когда один из коммутаторов выходит из строя, либо обрывается канал, множество деревьев MSTP перестраивается, что позволяет минимизировать последствия аварии. Ниже приведен процесс конфигурации коммутаторов. Для более быстрой настройки создается общий конфигурационный шаблон, который загружается на TFTP-сервер и используется впоследствии для настройки всех коммутаторов.

1. Создание шаблона и конфигурация первого коммутатора

```
console# configure
console(config)# vlan database
console(config-vlan)# vlan 10,20,30,40,50,60
console(config-vlan)# exit
console(config)# interface vlan 1
console(config-if)# ip address 192.168.16.1 /24
console(config-if)# exit
console(config)# spanning-tree mode mst
console(config)# interface range TengigabitEthernet 1/0/1-2
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk allowed vlan add 10,20,30,40,50,60
console(config-if)# exit
console(config)# spanning-tree mst configuration
console(config-mst)# name sandbox
```

```
console(config-mst)# instance 1 vlan 10,20,30
console(config-mst)# instance 2 vlan 40,50,60
console(config-mst)# exit
console(config)# do write
console(config)# spanning-tree mst 1 priority 0
console(config)# exit
console#copy running-config tftp://10.10.10.1/mstp.conf
```

Настройка multicast-TV VLAN

Функция *«Multicast-TV VLAN»* дает возможность использовать для передачи многоадресного трафика одну VLAN в сети оператора и доставлять этот трафик пользователям даже в том случае, если они не являются членами этой VLAN. С помощью функции «Multicast-TV VLAN» может быть сокращена нагрузка на сеть оператора за счет отсутствия дублирования многоадресных данных, например, при предоставлении услуги IPTV.

Схема применения функции предполагает, что порты пользователей работают в режиме «access» или «customer» и принадлежат к любой VLAN за исключением multicast-tv VLAN. Пользователи имеют возможность только получать многоадресный трафик из multicast-tv VLAN и не могут передавать данные в этой VLAN. Кроме того, в коммутаторе должен быть настроен порт-источник multicast-трафика, который должен быть участником multicast-tv VLAN.

Пример настройки для порта в режиме работы access

1. Включить фильтрацию многоадресных данных:

```
console(config)# bridge multicast filtering
```

2. Настроить VLAN пользователей (VID 100-124), multicast-tv VLAN (VID 1000), VLAN управления (VID 1200):

```
console(config)# vlan database
console(config-vlan)# vlan 100-124,1000,1200
console(config-vlan)# exit
```

3. Настроить порты пользователей:

```
console(config)# interface range te1/0/10-24
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 100
console(config-if)# switchport access multicast-tv vlan 1000
console(config-if)# bridge multicast unregistered filtering
console(config-if)# exit
```

4. Настроить uplink-порт, разрешив передачу многоадресного трафика, трафика пользователей и управление:

```
console(config)# interface te1/0/1
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk allowed vlan add 100-124,1000,1200
console(config-if)# exit
```

5. Настроить IGMP snooping глобально и на интерфейсах:

```
console(config)# ip igmp snooping
console(config)# ip igmp snooping vlan 1000
console(config)# ip igmp snooping vlan 1000 querier
console(config)# ip igmp snooping vlan 100
```

```
console(config)# ip igmp snooping vlan 101
console(config)# ip igmp snooping vlan 102
console(config)# ip igmp snooping vlan 103
…
console(config)# ip igmp snooping vlan 124
```

6. Настроить интерфейс управления:

```
console(config)# interface vlan 1200
console(config-if)# ip address 192.168.33.100 255.255.255.0
console(config-if)# exit
```

Настройка selective-qinq

Добавление SVLAN

Приведенный здесь пример конфигурации коммутатора демонстрирует как добавлять метку SVLAN 20 ко всему входящему трафику за исключением VLAN 27.

```
console# show running-config
```

```
vlan database
vlan 20,27
exit
!
interface tengigabitethernet1/0/5
 switchport mode general
 switchport general allowed vlan add 27 tagged
 switchport general allowed vlan add 20 untagged
 switchport general ingress-filtering disable
 selective-qinq list ingress permit ingress_vlan 27
 selective-qinq list ingress add_vlan 20
exit
!
!
end
```

Подмена CVLAN

В сетях передачи данных довольно часто возникают задачи, связанные с подменой VLAN (например, для коммутаторов уровня доступа существует типовая конфигурация, но пользовательский трафик, VOIP и трафик для управления требуется передавать в разных VLAN на различных направлениях). В этом случае было бы удобно воспользоваться функцией подмены CVLAN для замены типизированных VLAN на VLAN для требуемого направления. Ниже приведена конфигурация коммутатора, в котором осуществляется подмена VLAN 100, 101 и 102 на 200, 201 и 202. Обратная подмена должна осуществляться на этом же интерфейсе:

```
console# show running-config
```

```
vlan database
vlan 100-102,200-202
exit
!
interface tengigabitethernet 1/0/1
 switchport mode trunk
 switchport trunk allowed vlan add 200-202
 selective-qinq list egress override_vlan 100 ingress_vlan 200
 selective-qinq list egress override_vlan 101 ingress_vlan 201
 selective-qinq list egress override_vlan 102 ingress_vlan 202
 selective-qinq list ingress override_vlan 200 ingress_vlan 100
```

```
 selective-qinq list ingress override_vlan 201 ingress_vlan 101
 selective-qinq list ingress override_vlan 202 ingress_vlan 102
exit!end
```

ПРИЛОЖЕНИЕ Б. КОНСОЛЬНЫЙ КАБЕЛЬ

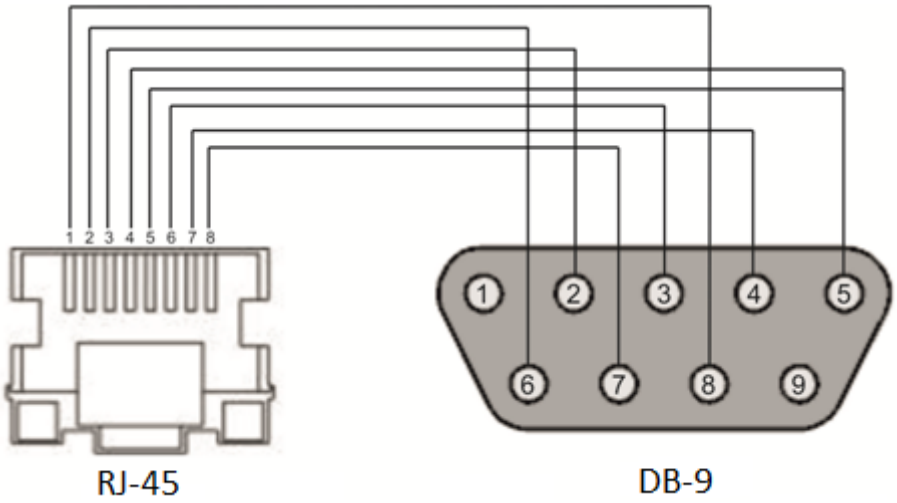


Рисунок Б.1 – Подключение консольного кабеля

ПРИЛОЖЕНИЕ В. ПОДДЕРЖИВАЕМЫЕ ЗНАЧЕНИЯ ETHERTYPE

Таблица В.1 – Поддерживаемые значения EtherType

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

ПРИЛОЖЕНИЕ Г. ОПИСАНИЕ ПРОЦЕССОВ КОММУТАТОРА

Таблица Г.1 – Описание процессов коммутатора

Имя процесса	Описание процесса
3SMA	Aging для IP-multicast
3SWF	Передача пакетов между уровнем 2 и сетевым уровнем
3SWQ	Программная обработка ACL перехваченных пакетов
AAAT	Управление и обработка методов AAA
AATT	Симулятор AAA для проверки методов AAA
ARPG	Реализация протокола ARP
B_RS	Управление перезагрузкой устройств в стеке
BFD	Реализация протокола BFD
BOXM	Дополнительные действия в стеке (получение сведений о стеке, индикация, обмен сообщениями, смена Unit ID)
BOXS	Обработка команд состояния стека: добавление Master/Slave, изучение топологии, обновление версии ПО ведомого устройства (slave)
BRGS	Bridge Security – ARP Inspection, DHCP Snooping, DHCP Relay Agent, IP Source Guard
BRMN	Bridge Management: STP, операции с FDB (добавление, удаление записей), зеркалирование, конфигурация портов/VLAN, GVRP, GARP, LLDP, IGMP Snooping, IP multicast
BSNC	Автомат синхронизации ведущего и ведомого устройств в стеке
BTPC	Клиент BOOTP
CDB_	Копирование конфигурационных файлов
CNLD	Загрузка/выгрузка конфигурации
COPY	Управление копированием файлов
CPUT	Утилизация CPU
D_LM	Link Manager – отслеживание состояния стек-линков
D_SP	Stacking Protocol
DDFG	Работа с файловой системой
DFST	Распределенная файловая система (DFS). Используется в работе стека
DH6C	DHCPv6-клиент
DHCP	Сервер и Relay Agent DHCP
DHCp	Ping
DMNG	Dinstant Manager – получение информации с удаленных юнитов (версия ПО, uptime, установка активного образа ПО)
DNSC	Клиент DNS
DNSS	Сервер DNS
DSND	Data Set Delays Report
DSPT	Dispatcher – обработка событий от удаленных юнитов об изменении состояния вентиляторов, источников питания, термодатчиков, SFP-трансиверов. Получение сообщений от удаленных юнитов об их версии ПО, серийном номере, MD5 сумме ПО.
DSYN	Stack application
DTSA	Stack application
ECHO	Протокол ECHO
EPOE	PoE (взаимодействие с пользователем)
ESTC	Логирование событий о превышении порогов трафика на CPU (cpu input-rate detailed)
EVAP	TRX Training – автоматическая настройка параметров SERDES
EVAU	Обработка событий Address Update, нижний уровень, передача выше

EVFB	Опрос состояния SFP
EVLC	Обработка событий о смене состояния порта, нижний уровень, передача выше
EVRT	RX Training
EVRX	Обработка событий приёма пакета из коммутатора в CPU, нижний уровень, передача пакета на уровень 2
EVTX	Обработка событий окончания отправки пакета из CPU в коммутатор, нижний уровень
exRX	Обработка выхода пакетов с нижнего уровня 2
FFTT	Управление таблицей маршрутизации и маршрутизация пакетов
FHSF	IPv6 First Hop Security (Обработка таймеров)
GOAH	Реализация web-сервера GoAhead
GRN_	Реализация Green Ethernet
HCLT	Получение и обработка команд настройки устройства нижнего уровня
HCPT	PoE (взаимодействие с контроллером)
HLTX	Отправка пакетов из CPU в коммутатор
HOST	Основной host-поток, холостой ход
HSCS	Stack Config – настройка функций коммутатора на удаленном юните
HSES	Stack Events – обработка событий link changed, address update с удаленных юнитов на мастере
HSEU	Обработка событий стека
ICMP	Реализация протокола ICMP
IOTG	Управление терминалами ввода-вывода
IOTM	Управление терминалами ввода-вывода
IOUR	Управление терминалами ввода-вывода
IP6C	Счётчики IPv4 и IPv6
IP6M	Маршрутизация IPv4 и IPv6
IPAT	Управление базой данных IP-адресов
IPG	Обработка перехваченных фрагментированных IP-пакетов
IPRD	Вспомогательная задача для ARP, RIP, OSPF
IPMT	Управление IP multicast маршрутизацией и IGMP Proxy
IT60	Задачи для работы с прерываниями
IT61	
IT64	
IT99	
IV11	Задача для работы с виртуальными прерываниями
L2HU	Передача пакетов на уровень 3
L2PS	Обработка событий смены состояния/настроек интерфейсов и передача сообщений зарегистрированным службам
L2UT	Утилизация портов (show interfaces utilization)
LBDR	Реализация функции Loopback Detection
LBDT	Отправка пакетов Loopback Detection
LTMR	Общая задача для всех таймеров
MACT	Обработка события об окончании действия в FDB (aging MAC-адресов)
MLDP	Marvell Link Layer Reliable Datagram Protocol, stack transport
MNGT	Автотесты
MRDP	Marvell Reliable Datagram Protocol, stack transport
MROR	Резервирование конфигурационного файла в энергонезависимой памяти
MSCm	Менеджер для работы с терминальными сессиями
MSRP	Передача событий в стеке пользовательским задачам
MSSS	Прослушивание IP-сокетов
MUXT	Отслеживание изменений структуры стека
NACT	Виртуальное тестирование кабеля (VCT)
NBBT	N-Base

NINP	Работа с комбо-портами
NSCT	Настройка ограничения скорости перехвата пакетов на CPU, ведение статистики по перехваченным пакетам
NSFP	Отслеживание событий, связанных с SFP, на сетевом уровне
NSTM	Storm Control
NTPL	Периодическая генерация сигнала для опроса таблиц MAC, VLAN, портов, мультикаста, маршрутизации, приоритезации
NTST	Добавление и удаление юнитов в стеке, сброс на дефолт состояния юнита, на сетевом уровне
NVCT	Вспомогательная задача для VCT. Запуск теста и отслеживание изменения состояния порта.
OBSR	Задача для отслеживания и уведомления об изменениях специфических параметров интерфейсов, необходимых для LLDP, CDP и других протоколов.
PLCR	Обработка событий смены состояния портов устройств стека
PLCT	Обработка событий смены состояния портов
PNGA	Реализация ping
POLI	Policy Management
PTPT	Precise Time Protocol
RADS	RADUIS-сервер
RCDS	Клиент Remote CLI
RCLA	Сервер Remote CLI
RCLB	
RELY	DHCPv6 Relay
ROOT	Родительский таск для всех задач
RPTS	Routing protocol
SCLC	Отслеживание состояния OOB-порта
SCPT	Автообновление и автоконфигурация
SCRX	Получение трафика с OOB-порта
SEAU	Получение событий Address Update, нижний уровень
SELC	Получение событий о смене состояния порта, нижний уровень
SERT	Отслеживание событий на порту для начала процедуры RX Training
SERX	Получение событий приёма пакета из коммутатора в CPU, нижний уровень
SETX	Получение событий окончания отправки пакета из CPU в коммутатор, нижний уровень
SFMG	sFlow Manager – обработка событий изменения IP-адреса, CLI/SNMP запросов, таймеров
SFSM	sFlow Sampler
SFTR	Протокол Sflow
SNAD	База данных SNA
SNAE	Обработка событий SNA
SNAS	Сохранение базы данных SNA в ПЗУ
SNMP	Реализация протокола SNMP
SNTP	Реализация протокола SNTP
SOCK	Управление работой сокетов
SQIN	Настройка Selective QinQ
SS2M	Slave To Master – передача сообщений с ведомого устройства (slave) на ведущее (master)
SSHP	Сервер SSH – настройка, обработка команд, таймер
SSHU	Сервер SSH – протокол
SSLP	Реализация SSL
SSTC	Логирование событий о превышении порогов трафика на CPU (cpu input-rate detailed)
STMB	Обработка SNMP-запросов о статусе стека
STSA	CLI-сессия через COM-порт
STSB	CLI-сессия через VLAN
STSC	CLI-сессия через VLAN

STSD	CLI-сессия через VLAN
STSE	CLI-сессия через VLAN
SW2M	Обработка событий Address Update от FDB, блокировка порта при возникновении ошибок на порту
SYLG	Вывод сообщений в syslog
TBI_	Таблица временных промежутков для ACL
TCPP	Реализация протокола TCP
TFTP	Реализация протокола TFTP
TMNG	Управление приоритетами задач
TNSL	Клиент TELNET
TNSR	Сервер TELNET
TRCE	Реализация traceroute
TRIG	Запуск действия в FDB (aging MAC-адресов)
TRMT	Управление юнитами в стеке с поддержкой транзакций
TRNS	File Transfer – копирование файлов между юнитами стека (ПО)
UDPR	UDP Relay
URGN	Обработка критических событий (например, перезагрузки)
VRRP	Реализация протокола VRRP
WBAM	Web-based Autentification
WBSO	Взаимодействие с web-клиентами, нижний уровень
WBSR	Управление и таймеры web-сервера
WNTT	Поддержка NAT для WBA
XMOD	Реализация протокола X-modem

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения технической консультации по вопросам эксплуатации оборудования ООО «Предприятие «ЭЛТЕКС» Вы можете обратиться в Сервисный центр компании.

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**