Ethernet-коммутаторы уровня доступа и агрегации серий RTT-A230, RTT-A330, RTT-A420

Руководство по эксплуатации

Версия ПО 4.0.25

СОДЕРЖАНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

[ ]	–	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	–	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

Коммутаторы серий RTT-A420, RTT-A330 и RTT-A230 могут использоваться в сетях крупных предприятий и предприятий малого и среднего бизнеса (SMB), в операторских сетях. Они обеспечивают высокую производительность, гибкость, безопасность, многоуровневое качество обслуживания (QoS). Коммутаторы серий RTT-A420 и RTT-A330 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 RTT-A420 и RTT-A330 – это высокопроизводительные устройства, оснащенные интерфейсами 10GBASE-X, 40GBASE-X и предназначенные для использования в операторских сетях в качестве устройств агрегации, а также в центрах обработки данных (ЦОД) – в роли коммутаторов Top-of-Rack или End-of-Row.

Порты устройств поддерживают работу на скоростях 40 Гбит/с (QSFP+) (RTT-A420), 10 Гбит/с (SFP+) или 1 Гбит/с (1000BASE-X и 1000BASE-T 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 (от лицевой панели в сторону тыльной) 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.

Коммутаторы доступа серии RTT-A230 – управляемые коммутаторы уровня L2+, которые позволяют подключить конечных пользователей и сетей предприятий малого и среднего бизнеса к сетям операторов связи с помощью интерфейсов 1/10Gigabit Ethernet.

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 (Jumbo frames). 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.
Передача на несколько MAC-адресов	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 (MAC Multicast Support).
Автоматическое время хранения MAC-адресов	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 (Automatic Aging for MAC Addresses).

Статические записи MAC	Сетевой коммутатор позволяет пользователю определить статические записи соответствий MAC-адресов, которые сохраняются в таблице коммутации (Static MAC Entries).

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 «шторма» (Broadcast, multicast, unknown unicast Storm Control)	«Шторм» — это размножение broadcast-, multicast-, unknown unicast-пакетов 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 (Port Mirroring). 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 (Protected ports).
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 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.
Поддержка VLAN	VLAN – это группа портов коммутатора, образующих одну широковещательную область (домен). Коммутатор поддерживает различные средства классификации пакетов для определения их принадлежности к определенной VLAN.
Поддержка протокола OAM (Operation, Administration, and Maintenance, IEEE 802.3ah)	Ethernet OAM (Operation, Administration, and Maintenance), IEEE 802.3ah – функции уровня канала передачи данных представляют собой протокол мониторинга состояния канала. В этом протоколе для передачи информации о состоянии канала между непосредственно подключенными устройствами Ethernet используются блоки данных протокола OAM (OAMPDU). Оба устройства должны поддерживать стандарт IEEE 802.3ah.
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 (Port-Based 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).
Selective Q-in-Q	Позволяет назначать внешний VLAN SPVLAN (Service Provider's VLAN) на основе сконфигурированных правил фильтрации по номерам внутренних VLAN (Customer VLAN). Применение Selective Q-in-Q позволяет разобрать трафик абонента на несколько VLAN, изменить метку SPVLAN у пакета в отдельном участке сети.

2.2.4 Функции третьего уровня сетевой модели OSI

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

Таблица 4 – Описание функций третьего уровня (Layer 3)

Клиенты BootP и DHCP	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 – 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	Протокол динамической маршрутизации Routing Information Protocol, 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 BGP	BGP (Border Gateway Protocol – протокол граничного шлюза) является протоколом маршрутизации между автономными системами (AS). Маршрутизаторы обмениваются информацией о маршрутах к сетям назначения.
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.
Протокол MSDP	Протокол для обмена информацией об источниках мультикаста между различными RP в PIM.

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	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	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	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+	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

Виртуальное тестирование кабеля (VCT)	Сетевые коммутаторы имеют в своём составе программные и аппаратные средства, позволяющие выполнять функции виртуального тестера кабеля – VCT. Тестер позволяет определить состояние медного кабеля связи.
Диагностика оптического трансивера	Устройство позволяет тестировать оптический трансивер. При тестировании отслеживаются такие параметры, как ток и напряжение питания, температура трансивера. Для реализации требуется поддержка этих функций в трансивере.
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	RTT-A420-24XG-4QXG	– Marvell 98CX8129-A1 (Hooper)
	RTT-A330-24T-4XG RTT-A330-24F-4XG RTT-A330-16F-4XG RTT-A330-8F-4XG RTT-A330-48T-4XG RTT-A330-48F-4XG	– Marvell 98DX3336-A1 (PonCat3)
	RTT-A230-24T-4XG RTT-A230-24P-4XG RTT-A230-24F-4XG RTT-A230-48T-4XG RTT-A230-48P-4XG	– Marvell 98DX3236-A1 (AlleyCat3)
	RTT-A230-8P-4G-AC RTT-A230-8T-2G-AC	– Marvell 98DX3233
Интерфейсы	RTT-A420-24XG-4QXG	– 24x10GBASE-R (SFP+)/1000BASE-X (SFP) – 4x40GBASE-SR4/LR4 (QSFP+) – 1x10/100/1000BASE-T (OOB RJ45) – 1x10/100/1000BASE-T (Management in-band) – 1xКонсольный порт RS-232 (RJ-45)

	RTT-A330-24T-4XG	– 20x10/100/1000BASE-T (RJ45) – 4x10GBASE-R (SFP+)/1000BASE-X (SFP) – 4x10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo – 1x10/100/1000BASE-T (OOB RJ45) – 1xКонсольный порт RS-232 (RJ-45)
	RTT-A330-24F-4XG	– 20x1000BASE-X/100BASE-FX (SFP) – 4x10GBASE-R (SFP+)/1000BASE-X (SFP) – 4x10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo – 1x10/100/1000BASE-T (OOB RJ45) – 1xКонсольный порт RS-232 (RJ-45)
	RTT-A330-16F-4XG	– 12x1000BASE-X/100BASE-FX (SFP) – 4x10GBASE-R (SFP+)/1000BASE-X (SFP) – 4x10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo – 1x10/100/1000BASE-T (OOB RJ45) – 1xКонсольный порт RS-232 (RJ-45)
	RTT-A330-8F-4XG	– 4x1000BASE-X/100BASE-FX (SFP) – 4x10GBASE-R (SFP+)/1000BASE-X (SFP) – 4x10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo – 1x10/100/1000BASE-T (OOB RJ45) – 1xКонсольный порт RS-232 (RJ-45)
	RTT-A230-24T-4XG	– 24x10/100/1000BASE-T (RJ45) – 4x10GBASE-R (SFP+)/1000BASE-X (SFP) – 1xКонсольный порт RS-232 (RJ-45)
	RTT-A230-24P-4XG	– 24x10/100/1000BASE-T PoE/PoE+ (RJ45) – 4x10GBASE-R (SFP+)/1000BASE-X (SFP) – 1xКонсольный порт RS-232 (RJ-45)
	RTT-A230-24F-4XG	– 20x1000BASE-X/100BASE-FX (SFP) – 4x10GBASE-R (SFP+)/1000BASE-X (SFP) – 4x10/100/1000BASE-T/1000BASE-X/100BASE-FX Combo – 1xКонсольный порт RS-232 (RJ-45)
	RTT-A230-48T-4XG RTT-A330-48T-4XG	– 48x10/100/1000BASE-T (RJ45) – 4x10GBASE-R (SFP+)/1000BASE-X (SFP) – 1xКонсольный порт RS-232 (RJ-45)
	RTT-A230-48P-4XG	– 48x10/100/1000BASE-T PoE/PoE+ (RJ45) – 4x10GBASE-R (SFP+)/1000BASE-X (SFP) – 1xКонсольный порт RS-232 (RJ-45)
	RTT-A330-48F-4XG	– 48x1000BASE-X/100BASE-FX (SFP) – 4x10GBASE-R (SFP+)/1000BASE-X (SFP) – 1xКонсольный порт RS-232 (RJ-45)
	RTT-A230-8P-4G-AC	– 8x10/100/1000BASE-T PoE/PoE+ (RJ45) – 2x10/100/1000BASE-T (RJ45) – 2x1000BASE-X (SFP) – 1xКонсольный порт RS-232 (RJ-45)
	RTT-A230-8T-2G-AC	– 8x10/100/1000BASE-T (RJ45) – 2x10/100/1000BASE-T/100/1000BASE-X Combo – 1xКонсольный порт RS-232 (RJ-45)
Пропускная способность	RTT-A420-24XG-4QXG	800 Гбит/с
	RTT-A230-24T-4XG RTT-A230-24P-4XG RTT-A230-24F-4XG RTT-A330-24T-4XG RTT-A330-24F-4XG	128 Гбит/с

	RTT-A230-48T-4XG RTT-A230-48P-4XG RTT-A330-48T-4XG RTT-A330-48F-4XG	176 Гбит/с
	RTT-A330-16F-4XG	112 Гбит/с
	RTT-A330-8F-4XG	96 Гбит/с
	RTT-A230-8P-4G-AC	24 Гбит/с
	RTT-A230-8T-2G-AC	20 Гбит/с
Производительность на пакетах длиной 64 байта (в режиме duplex)	RTT-A420-24XG-4QXG	1025,6 MPPS
	RTT-A230-24T-4XG RTT-A230-24P-4XG RTT-A230-24F-4XG RTT-A330-24T-4XG RTT-A330-24F-4XG	186,2 MPPS
	RTT-A230-48T-4XG RTT-A230-48P-4XG RTT-A330-48T-4XG RTT-A330-48F-4XG	261,8 MPPS
	RTT-A330-16F-4XG RTT-A330-8F-4XG	142 MPPS
	RTT-A230-8P-4G-AC RTT-A230-8T-2G-AC	35,4 MPPS
Объем буферной памяти	RTT-A420-24XG-4QXG	32 Мбит
	RTT-A330-24T-4XG RTT-A330-24F-4XG RTT-A330-16F-4XG RTT-A330-8F-4XG RTT-A230-24T-4XG RTT-A230-24P-4XG RTT-A230-24F-4XG RTT-A230-8T-2G-AC RTT-A230-8P-4G-AC	12 Мбит
	RTT-A230-48T-4XG RTT-A230-48P-4XG RTT-A330-48T-4XG RTT-A330-48F-4XG	24 Мбит
Объем ОЗУ (DDR3)	RTT-A420-24XG-4QXG	4 Гбайт
	Остальные модели	512 Мбайт
Объем ПЗУ (RAW NAND)	RTT-A420-24XG-4QXG	2 Гбайт
	Остальные модели	512 Мбайт
Таблица MAC-адресов	RTT-A420-24XG-4QXG	65536
	Остальные модели	16384
Количество правил ACL	RTT-A420-24XG-4QXG	1982
	Коммутаторы серии RTT-A330	3006
	Коммутаторы серии RTT-A230	958
Количество ACL	RTT-A420-24XG-4QXG	2048
	Коммутаторы серии RTT-A330	3072

	Коммутаторы серии RTT-A230	1024
Количество правил ACL в одном ACL	RTT-A420-24XG-4QXG Коммутаторы серии RTT-A330 Коммутаторы серии RTT-A230	256
Количество маршрутов L3 Unicast	RTT-A420-24XG-4QXG	IPv4 – 7744 IPv6 – 1942
	Коммутаторы серии RTT-A330	IPv4 – 12864 IPv6 – 3222
	Коммутаторы серии RTT-A230	IPv4 – 816 IPv6 – 210
Количество ARP-записей	RTT-A420-24XG-4QXG	7748
	Коммутаторы серии RTT-A330	4023
	Коммутаторы серии RTT-A230	820
Количество групп L2 Multicast (IGMP snooping)	RTT-A420-24XG-4QXG. Коммутаторы серии RTT-A330	4K
	Коммутаторы серии RTT-A230	2K
Количество маршрутов L3 Multicast (IGMP Proxy, PIM)	RTT-A420-24XG-4QXG, Коммутаторы серии RTT-A330	IPv4 – 4024 IPv4 IPv6 – 1006 IPv6
	Коммутаторы серии RTT-A230	IPv4 – 412 IPv4 IPv6 – 103 IPv6
Количество правил SQinQ	RTT-A420-24XG-4QXG	1982 (ingress/egress)
	Коммутаторы серии RTT-A330	3006 (ingress/egress)
	Коммутаторы серии RTT-A230	958 (ingress/egress)
Максимальное количество ECMP-маршрутов	RTT-A420-24XG-4QXG	64
	Остальные модели	8
Поддержка VLAN		Согласно 802.1Q, до 4K активных VLAN
Качество обслуживания QoS		Приоритизация трафика, 8 уровней, 8 выходных очередей с разными приоритетами для каждого порта
Количество VRRP-маршрутизаторов		255
Количество L3 интерфейсов	RTT-A420-24XG-4QXG	2048
	Остальные модели	130
Количество виртуальных Loopback-интерфейсов		64
Количество экземпляров процессов OSPF		20
Количество OSPF-соседств		64
Количество BGP-соседств		32
Агрегация каналов (LAG)		48 групп, до 8 портов в каждой
Количество экземпляров MSTP		64
Количество экземпляров PVST		63

Количество DHCP pool		32
Сверхдлинные кадры (jumbo frames)		Максимальный размер пакетов 10K
Стекирование		до 8 устройств
Соответствие стандартам		– IEEE 802.3 10BASE-T Ethernet – IEEE 802.3u 100BASE-T Fast Ethernet – IEEE 802.3ab 1000BASE-T Gigabit Ethernet – IEEE 802.3z Fiber Gigabit Ethernet – IEEE 802.3x Full Duplex, Flow Control – IEEE 802.3ad Link Aggregation (LACP) – IEEE 802.1p Traffic Class – IEEE 802.1q VLAN – IEEE 802.1v – IEEE 802.3 ac – IEEE 802.1d Spanning Tree Protocol (STP) – IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) – IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) – IEEE 802.1x Authentication – IEEE 802.3af PoE, IEEE 802.3at PoE+ (только RTT-A230-8P-4G-AC, RTT-A230-24P-4XG, только RTT-A230-48P-4XG)
Управление		
Локальное управление		Console
Удаленное управление		SNMP, Telnet, SSH, WEB
Физические характеристики и условия окружающей среды		
Источники питания	RTT-A420-24XG-4QXG RTT-A230-48P-4XG Коммутаторы серии RTT-A330	– Сеть переменного тока: 100 – 240 В, 50/60 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.
	RTT-A230-24T-4XG-AC RTT-A230-24P-4XG-AC RTT-A230-8T-2G-AC RTT-A230-8P-4G-AC	Сеть переменного тока: 110 – 250 В, 50/60 Гц
	RTT-A230-24T-4XG-ACA RTT-A230-24F-4XG-ACA RTT-A230-48T-4XG-ACA	– Сеть переменного тока: 110 – 250 В, 50/60 Гц и разъем под аккумуляторную батарею (АКБ). Характеристики зарядного устройства: – Ток заряда: – 2,7±0.2A - RTT-A230-24F-4XG-ACA и RTT-A230-48T-4XG-ACA; – 1.6±0.1A - RTT-A230-24T-4XG-ACA. – Напряжение срабатывания расцепителя нагрузки:10-10,5В; – Пороговое напряжение индикации низкого заряда: 11В **Сечение провода для подключения АКБ – не менее 1,5 мм. Использовать АКБ емкостью не менее 20Ah**
	RTT-A230-24F-4XG-DC	сеть постоянного тока: 36 – 72 В
Потребляемая мощность	RTT-A420-24XG-4QXG	не более 107 Вт
	RTT-A230-24T-4XG-ACA	не более 25 Вт
	RTT-A330-8F-4XG	не более 27 Вт

	RTT-A330-24T-4XG RTT-A330-16F-4XG RTT-A230-24F-4XG-DC	не более 35 Вт
	RTT-A230-24T-4XG-ACA	не более 26 Вт / не более 50 Вт (с учетом заряда АКБ)
	RTT-A230-24F-4XG-ACA	не более 45 Вт / не более 85 Вт (с учетом заряда АКБ)
	RTT-A330-48T-4XG RTT-A330-24F-4XG	не более 45 Вт
	RTT-A330-48F-4XG	не более 55 Вт
	RTT-A230-48T-4XG-ACA	не более 45 Вт / не более 85 Вт (с учетом заряда АКБ)
	RTT-A230-48P-4XG	не более 1600 Вт
	RTT-A230-8T-2G-AC	не более 15 Вт
	RTT-A230-8P-4G-AC	не более 275 Вт
	RTT-A230-24P-4XG-AC	не более 455 Вт
Бюджет мощности PoE	RTT-A230-24P-4XG-AC	380 Вт
	RTT-A230-48P-4XG	1450 Вт
	RTT-A230-8P-4G-AC	240 Вт
Габаритные размеры	RTT-A420-24XG-4QXG	430 x 44 x 298 мм
	RTT-A230-24T-4XG	430 x 44 x 158 мм
	RTT-A230-24P-4XG	440 x 44 x 203 мм
	RTT-A230-24F-4XG	430 x 44 x 243 мм
	RTT-A330-24T-4XG RTT-A330-24F-4XG RTT-A330-16F-4XG RTT-A330-8F-4XG	430 x 44 x 275 мм
	RTT-A230-48T-4XG	440 x 44 x 280 мм
	RTT-A330-48T-4XG	440 x 44 x 316 мм
	RTT-A330-48F-4XG	440 x 44 x 330 мм
	RTT-A230-48P-4XG	430 x 44 x 490 мм
	RTT-A230-8T-2G-AC	310 x 44 x 158 мм
	RTT-A230-8P-4G-AC	430 x 44 x 158 мм
Интервал рабочих температур	RTT-A420-24XG-4QXG	от 0 до +45 ºС
	RTT-A230-24T-4XG RTT-A230-24P-4XG RTT-A230-24F-4XG RTT-A230-8P-4G-AC RTT-A230-8T-2G-AC RTT-A230-48T-4XG RTT-A230-48P-4XG	от -20 до +50 ºС
	Все коммутатор серии RTT-A330	от -10 до +45 ºС
Масса	RTT-A420-24XG-4QXG	3,95 кг
	RTT-A330-24T-4XG	3,25 кг
	RTT-A330-24F-4XG	3,50 кг
	RTT-A330-16F-4XG	3,25 кг
	RTT-A330-8F-4XG	3,15 кг

	RTT-A230-24T-4XG	2,25 кг
	RTT-A230-24P-4XG-AC	3,16 кг
	RTT-A230-24F-4XG-ACA	3,55 кг
	RTT-A230-24F-4XG-DC	3,25 кг
	RTT-A230-48T-4XG	3,85 кг
	RTT-A330-48T-4XG	3,95 кг
	RTT-A230-48P-4XG	9,55 кг
	RTT-A330-48F-4XG	4 кг
	RTT-A230-8P-4G-AC	2,55 кг
	RTT-A230-8T-2G-AC	1,45 кг
Интервал температур хранения		от -40 до +70 ºС
Относительная влажность при эксплуатации (без образования конденсата)		не более 80%
Относительная влажность при хранении (без образования конденсата)		от 10% до 95%
Средний срок службы		10 лет

2.4 Конструктивное исполнение

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

Ethernet-коммутаторы выполнены в металлическом корпусе с возможностью установки в телекоммуникационную стойку или шкаф 19”, высота корпуса всех моделей коммутатороы составляет 1 Unit (44 мм).

2.4.1 Внешний вид и описание передней панели устройств

Внешний вид передней панели устройств показан на рисунках, приведенных ниже.

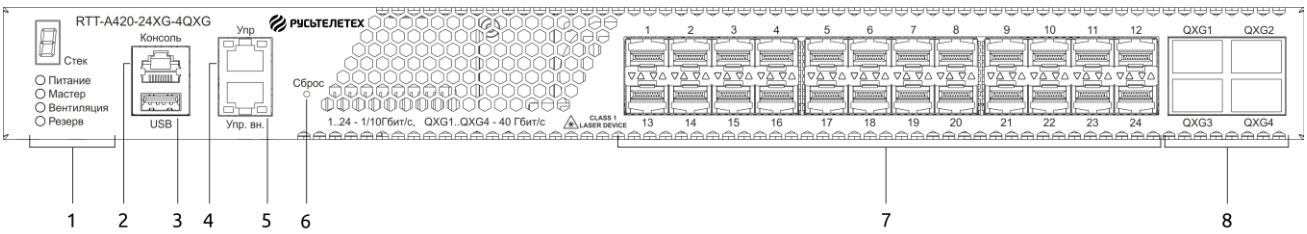


Рис. 1 – Передняя панель RTT-A420-24XG-4QXG

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

Таблица 10 – Описание разъемов, индикаторов и органов управления передней панели коммутатора RTT-A420-24XG-4QXG

№	Элемент передней панели	Описание
1	Стек	Индикатор номера устройства в стеке.
	Питание	Индикатор питания устройства.
	Мастер	Индикатор режима работы устройства (ведущий/ведомый).
	Вентиляция	Индикатор работы вентиляторов.
	Резерв	Индикатор резервного электропитания.
2	Консоль	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
3	USB	USB порт
4	Упр	Порт OOB (out-of-band) 10/100/1000 Base-T (RJ45) для удаленного управления устройством. Управление осуществляется по сети, отдельно от каналов передачи данных
5	Упр. вн.	Порт 10/100/1000 Base-T (RJ45) для удаленного управления устройством. Управление осуществляется по сети передачи данных (in-band)
6	Сброс	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам. Возможные действия: - при нажатии менее 10 с – перезагрузка устройства; - при нажатии на 10 с и более – перезагрузка устройства и сброс до заводской конфигурации
7	[1-24]	Интерфейсы для установки трансиверов SFP+, SFP
8	QXG1, QXG2 QXG3, QXG4	Интерфейсы для установки трансиверов QSFP+, SFP+

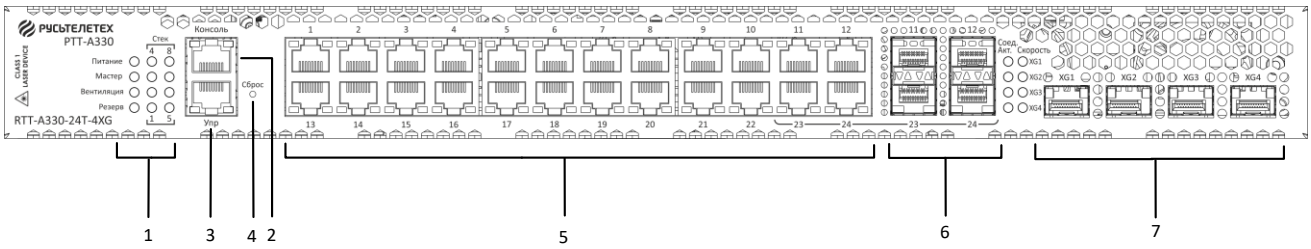


Рис. 2 – Передняя панель RTT-A330-24T-4XG

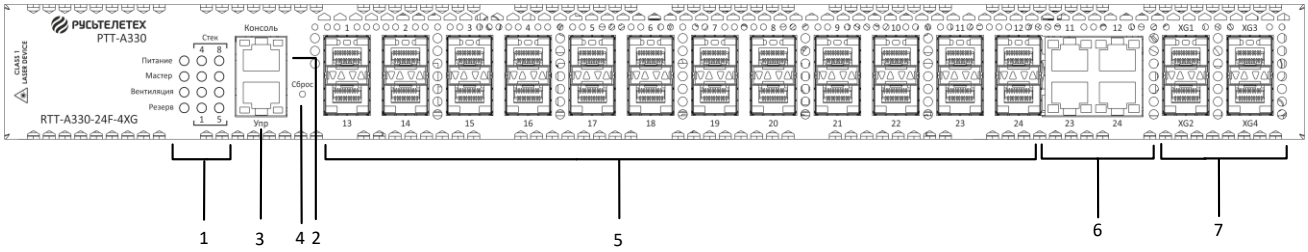


Рис. 3 – Передняя панель RTT-A330-24F-4XG

В таблице 11 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели коммутаторов RTT-A330-24T-4XG, RTT-A330-24F-4XG.

Таблица 11 – Описание разъемов, индикаторов и органов управления передней RTT-A330-24T-4XG, RTT-A330-24F-4XG

№	Элемент передней панели	Описание
1	Стек	Индикатор номера устройства в стеке
	Питание	Индикатор питания устройства
	Мастер	Индикатор режима работы устройства (ведущий/ведомый)
	Вентиляция	Индикатор работы вентиляторов
	Резерв	Индикатор резервного электропитания
2	Консоль	Консольный порт для локального управления устройством
3	Упр	Порт (out-of-band) 10/100/1000BASE-T (RJ45) для удаленного управления устройством. Управление осуществляется по сети, отдельно от каналов передачи данных
4	Сброс	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам. Возможные действия: - при нажатии менее 10 с – перезагрузка устройства; - при нажатии на 10 с и более – перезагрузка устройства и сброс до заводской конфигурации
5	[1-24]	Интерфейсы для установки трансиверов SFP Порты 10/100/1000BASE-T (RJ45)
6	[11-12, 23-24]	Комбинированные порты 10/100/1000BASE-T (RJ45)/1000BASE-X(SFP)
7	XG1, XG2, XG3, XG4	Интерфейсы для установки трансиверов SFP+/ SFP

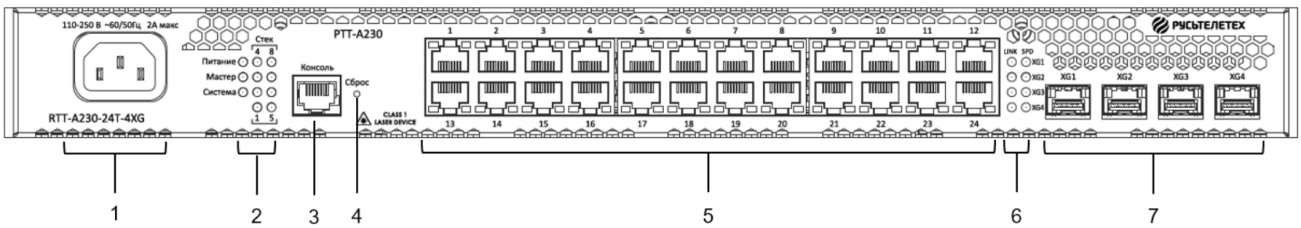


Рис. 4 – Передняя панель RTT-A230-24T-4XG-AC

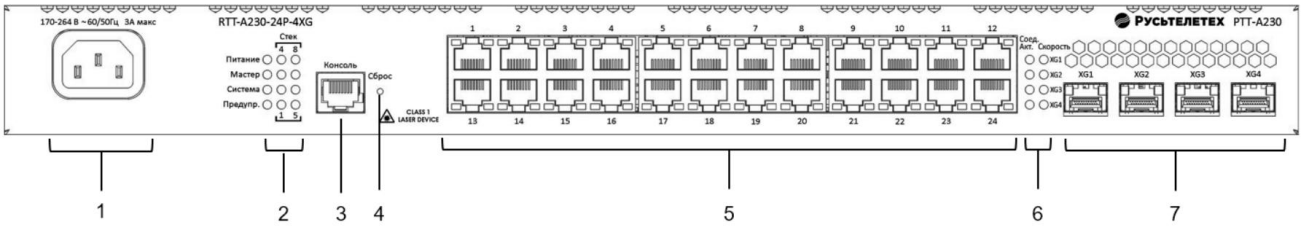


Рис. 5 – Передняя панель RTT-A230-24P-4XG-AC

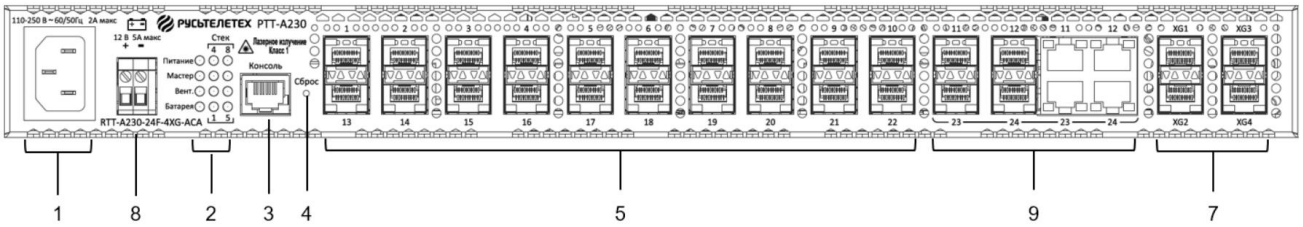


Рис. 6 – Передняя панель RTT-A230-24F-4XG-ACA

В таблице 12 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели коммутатора RTT-A230-24T-4XG-AC, RTT-A230-24P-4XG-AC, RTT-A230-24F-4XG-ACA.

Таблица 12 – Описание разъемов, индикаторов и органов управления передней панели RTT-A230-24T-4XG, RTT-A230-24P-4XG, RTT-A230-24F-4XG-ACA

№	Элемент передней панели	Описание
1	~110-250VAC, 60/50Hz max 2A	Разъем для подключения к источнику электропитания переменного тока
2	Стек	Индикатор номера устройства в стеке
	Питание	Индикатор питания устройства
	Мастер	Индикатор режима работы устройства (ведущий/ведомый)
	Система	Индикатор состояния устройства
	Вент.	Индикатор работы вентиляторов (для RTT-A230-24F-4XG-ACA)
	Батарея	Индикатор состояния батареи (для RTT-A230-24F-4XG-ACA)
	Предупр.	Индикатор аварии PoE
3	Консоль	Консольный порт для локального управления устройством
4	Сброс	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам. Возможные действия: - при нажатии менее 10 с – перезагрузка устройства; - при нажатии на 10 с и более – перезагрузка устройства и сброс до заводской конфигурации
5	[1-24]	Порты 10/100/1000BASE-T (RJ45) (для RTT-A230-24T-4XG-AC, RTT-A230-24P-4XG-AC)
	[1-10, 13-22]	Интерфейсы для установки трансиверов SFP (RTT-A230-24F-4XG-ACA)
6	Link/Speed	Световая индикация состояния оптических интерфейсов XG1- XG4
7	XG1, XG2, XG3, XG4	Слоты для установки трансиверов SFP+/SFP

8	12 В, 5 А Макс.	Клеммы для подключения внешнего источника постоянного тока
9	[11-12, 23-24]	Комбинированные порты 10/100/1000BASE-T (RJ45) / 1000BASE-X

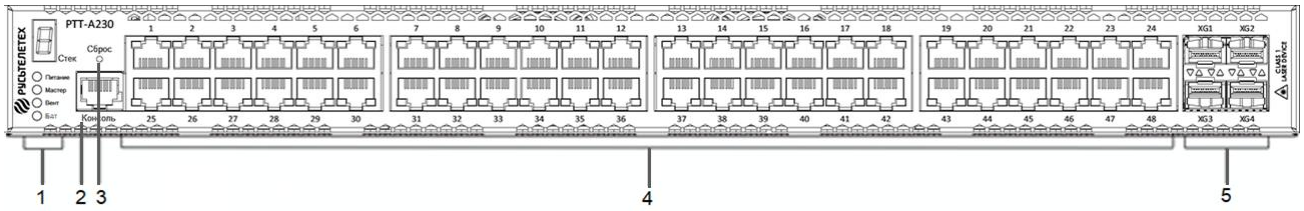


Рис. 7 – RTT-A230-48T-4XG-ACA, передняя панель

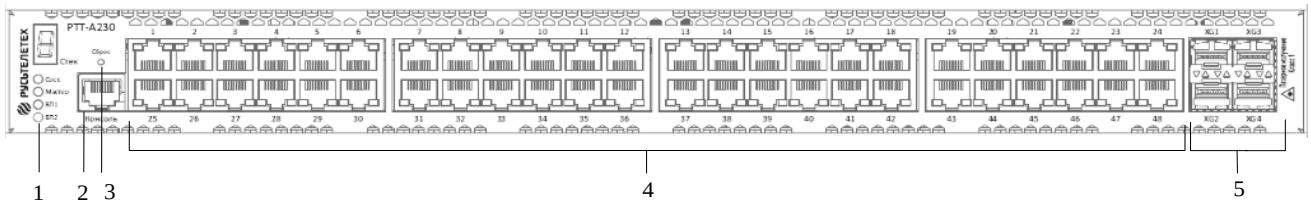


Рис. 8 – RTT-A230-48P-4XG, передняя панель

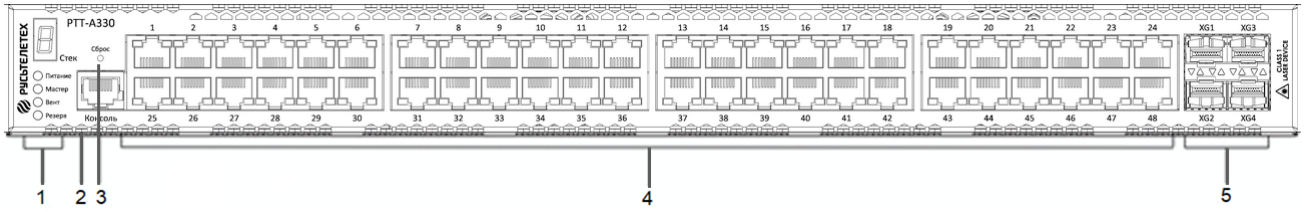


Рис. 9 – RTT-A330-48T-4XG, передняя панель

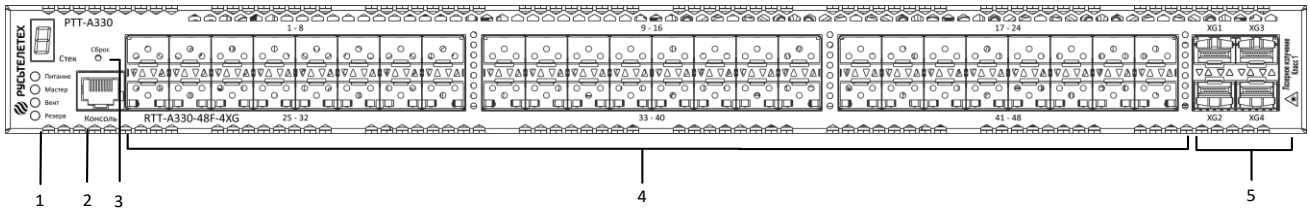


Рис. 10 – RTT-A330-48F-4XG, передняя панель

В таблице 13 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели коммутаторов RTT-A230-48T-4XG, RTT-A230-48P-4XG, RTT-A330-48T-4XG, RTT-A330-48F-4XG.

Таблица 13 – Описание разъемов, индикаторов и органов управления передней панели RTT-A230-48T-4XG, RTT-A230-48P-4XG, RTT-A330-48T-4XG, RTT-A330-48F-4XG

№	Элемент передней панели	Описание
1	Стек	Индикатор номера устройства в стеке
	Питание	Индикатор питания устройства
	Сост.	Индикатор состояния устройства (для RTT-A230-48P-4XG)

	Мастер		Индикатор режима работы устройства (ведущий/ведомый)
	Вент.		Индикатор работы вентиляторов
	Бат.		Индикатор состояния батареи (для RTT-A230-48T-4XG)
	БП1, БП2		Индикатор модулей питания (для RTT-A230-48P-4XG)
	Резерв		Индикатор резервного электропитания
2	Консоль		Консольный порт для локального управления устройством
3	Сброс		Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам. Возможные действия: - при нажатии менее 10 с – перезагрузка устройства; - при нажатии на 10 с и более – перезагрузка устройства и сброс до заводской конфигурации
4	[1-48]	RTT-A230-48T-4XG RTT-A330-48T-4XG	Порты 10/100/1000BASE-T (RJ45)
		RTT-A330-48F-4XG	Интерфейсы для установки трансиверов SFP
5	XG1, XG2, XG3, XG4		Интерфейсы для установки трансиверов SFP+/ SFP

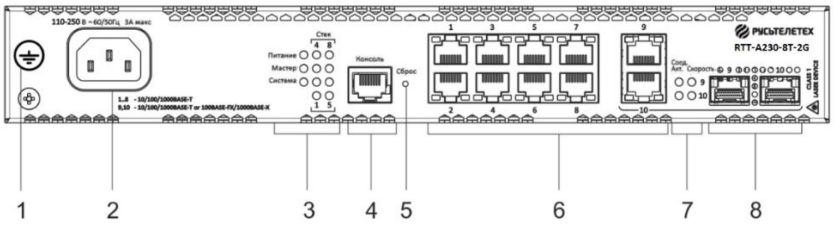


Рис. 11 – Передняя панель RTT-A230-8T-2G-AC

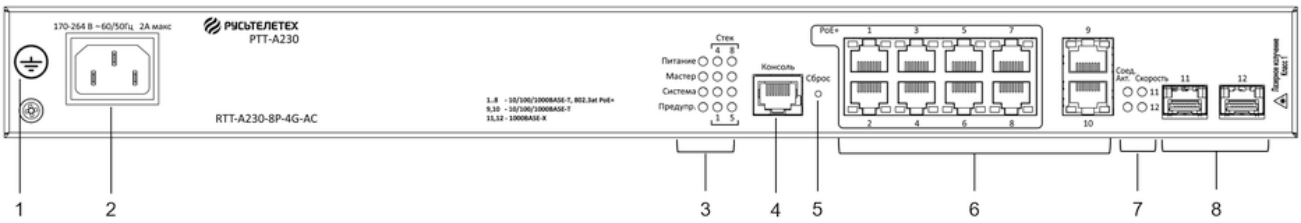


Рис. 12 – Передняя панель RTT-A230-8P-4G-AC

В таблице 14 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели коммутаторов RTT-A230-8T-2G-AC, RTT-A230-8P-4G-AC.

Таблица 14 – Описание разъемов, индикаторов и органов управления передней панели RTT-A230-8T-2G-AC, RTT-A230-8P-4G-AC

№	Элемент передней панели	Описание
1	Клемма заземления ⏚	Клемма для заземления устройства
2	~110-250VAC, 60/50Hz max 2A	Разъем для подключения к источнику электропитания переменного тока
3	Стек	Индикатор номера устройства в стеке

	Питание		Индикатор питания устройства
	Мастер		Индикатор режима работы устройства (ведущий/ведомый)
	Состояние		Индикатор состояния устройства
	Предупр.		Индикатор аварии PoE
4	Консоль		Консольный порт для локального управления устройством
5	Сброс		Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам. Возможные действия: - при нажатии менее 10 с – перезагрузка устройства; - при нажатии на 10 с и более – перезагрузка устройства и сброс до заводской конфигурации
6	[1-8]		Порты 10/100/1000BASE-T (RJ45) (для RTT-A230-8P-4G – с PoE+)
	[9-10]	RTT-A230-8P-4G	Порты 10/100/1000BASE-T (RJ45)
		RTT-A230-8T-2G	Комбинированные порты 10/100/1000BASE-T (RJ45)
7	Соед.Акт./Скорость		Световая индикация состояния оптических интерфейсов
8	[9-10]		Комбинированные порты 1000BASE-X (SFP) (для RTT-A230-8T-2G)
	[11-12]		Интерфейсы для установки трансиверов SFP (для RTT-A230-8P-4G)

2.4.2 Задняя панель устройств

Внешний вид задней панели коммутаторов RTT-A420-24XG-4QXG приведен на Рис. 13.

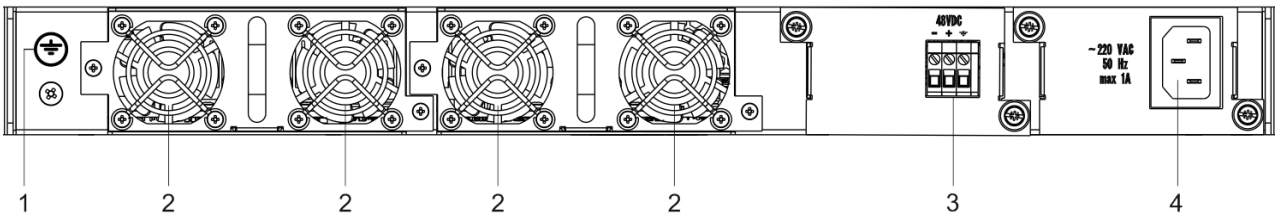


Рис. 13 – Задняя панель RTT-A420-24XG-4QXG

В таблице 15 приведен перечень разъемов, расположенных на задней панели коммутатора RTT-A420-24XG-4QXG.

Таблица 15 – Описание разъемов задней панели коммутатора RTT-A420-24XG-4QXG

№	Элемент задней панели	Описание
1	Клемма заземления ⏚	Клемма для заземления устройства
2	Съемные вентиляторы	Съемные вентиляционные модули с возможностью горячей замены
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

Внешний вид задней панели коммутаторов серии RTT-A330 приведен на Рис. 14.

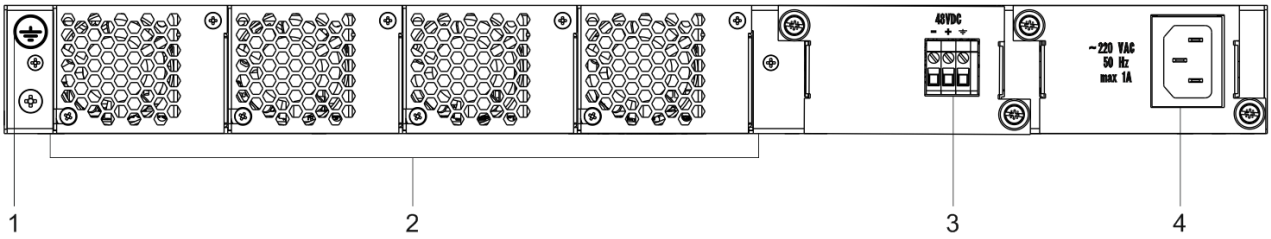


Рис. 14 – Задняя панель коммутаторов серии RTT-A330

Таблица 16 – Описание разъемов задней панели коммутаторов серии RTT-A330

№	Элемент задней панели	Описание
1	Клемма заземления ⏚	Клемма для заземления устройства
2	Съемные вентиляторы	Съемные вентиляционные модули с возможностью горячей замены
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

Внешний вид задней панели коммутаторов серии RTT-A230 приведен на Рис. 15 и Рис. 16.

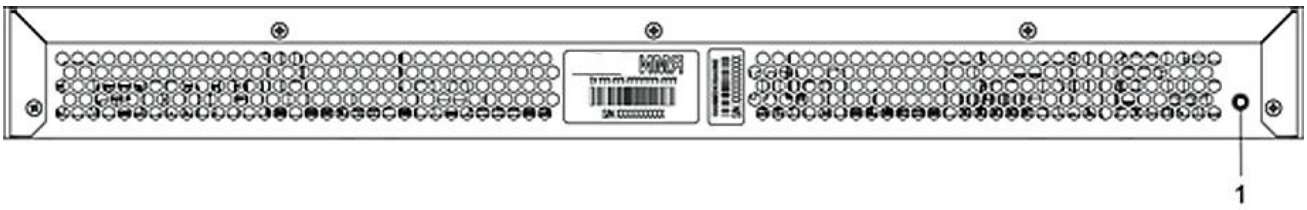


Рис. 15 – Задняя панель RTT-A230-24F-4XG, RTT-A230-24T-4XG, RTT-A230-24F-4XG

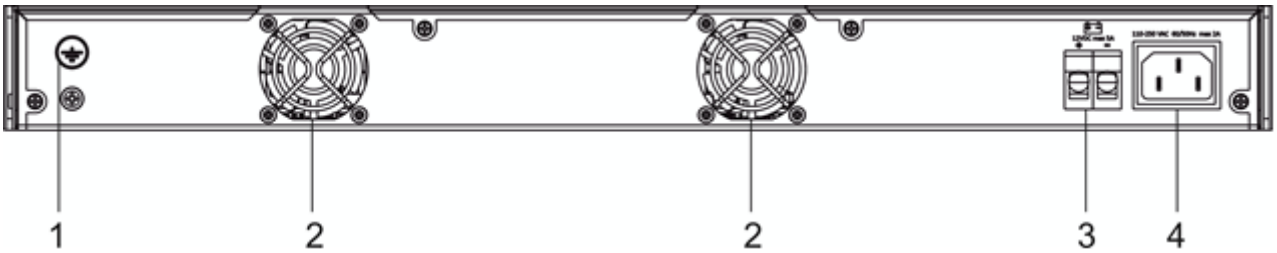


Рис. 16 – Задняя панель RTT-A230-48T-4XG

Таблица 17 – Описание разъемов задней панели коммутаторов RTT-A230

№	Элемент задней панели	Описание
1	Клемма заземления ⏚	Клемма для заземления устройства
2		Вентиляторы
3	12VDC max 5A	Клеммы для подключения аккумуляторной батареи 12V
4	~110-250VAC, 60/50Hz max 2A	Разъем для подключения к источнику электропитания переменного тока

Внешний вид задней панели коммутаторов RTT-A230-8T-2G-AC и RTT-A230-8P-4G-AC приведен на Рис. 17.

Рис. 17 – Задняя панель RTT-A230-8T-2G-AC, RTT-A230-8P-4G-AC

Внешний вид задней панели коммутатора RTT-A230-48P-4XG приведен на рисунке ниже.

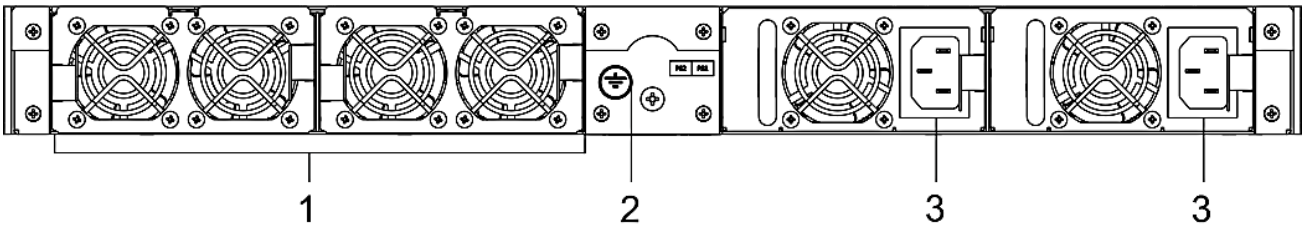


Рис. 18 – Задняя панель RTT-A230-48P-4XG

В приведен перечень разъемов, расположенных на задней панели коммутатора RTT-A230-48P-4XG

Таблица 18 – Описание разъемов задней панели коммутатора RTT-A230-48P-4XG

№	Элемент задней панели	Описание
1	Съемные вентиляторы	Съемные вентиляционные модули с возможностью горячей замены
2	Клемма заземления ⏚	Клемма для заземления устройства
3	~100-240VAC, 60/50Hz max 10A	Разъем для подключения к источнику электропитания переменного тока

2.4.3 Боковые панели устройства

Рис. 19 – Правая боковая панель Ethernet-коммутаторов

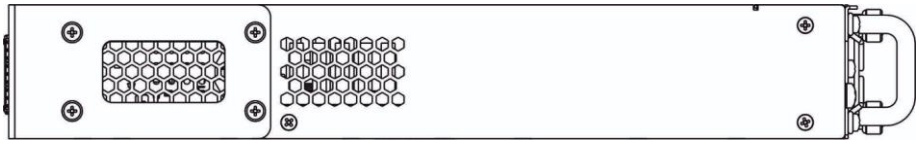


Рис. 20 – Левая боковая панель Ethernet-коммутаторов

На боковых панелях устройства расположены вентиляционные решетки, которые служат для отвода тепла. Не закрывайте вентиляционные отверстия посторонними предметами. Это может привести к перегреву компонентов устройства и вызвать нарушения в его работе. Рекомендации по установке устройства расположены в разделе 3.2.

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 ниже.

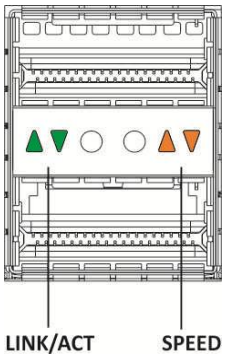


Рис. 21 – Внешний вид разъема с QSFP-трансиверами

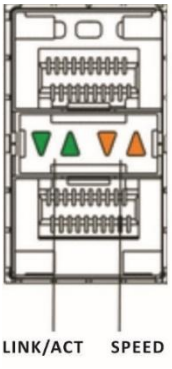


Рис. 22 – Внешний вид разъема SFP/SFP+

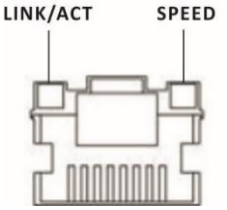


Рис. 23 – Внешний вид разъема RJ45

Таблица 19 – Световая индикация состояния QXG-портов

Свечение индикатора SPEED	Свечение индикатора LINK/ACT	Состояние интерфейса Ethernet
Выключен	Выключен	Порт выключен или соединение не установлено
Горит постоянно	Горит постоянно	Установлено соединение на скорости 40Gбит/с
Горит постоянно	Мигание	Идет передача данных

Таблица 20 – Световая индикация состояния XG-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 1Gбит/с
Горит постоянно	Горит постоянно	Установлено соединение на скорости 10Gбит/с
X	Мигание	Идет передача данных

Таблица 21 – Световая индикация состояния Ethernet-портов 10BASE-T

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

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

Системные индикаторы (Питание, Мастер, Вентиляция, Резерв) служат для определения состояния работы узлов коммутаторов.

Таблица 22 – Световая индикация системных индикаторов

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Питание	Состояние источников питания	Выключен	Питание выключено
		Зеленый, горит постоянно	Питание включено, нормальная работа устройства
		Зеленый, мерцает	Самотестирование устройства при старте (POST)
		Красный, горит постоянно	Отсутствие первичного питания от основного источника (при питании устройства от резервного источника)
Мастер	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
Вентиляция	Состояние вентилятора охлаждения	Зеленый, горит постоянно	Все вентиляторы исправны
		Красный, горит постоянно	Отказ одного или более вентиляторов
Состояние	Индикатор состояния устройства	Зеленый, горит постоянно	Нормальная работа устройства
		Красный, горит постоянно	Отказ одного или более вентиляторов, или авария PoE (RTT-A230-48P-4XG)
		Мигает, красный-зеленый	Загрузка устройства. Не назначен IP-адрес ни на один из интерфейсов, либо в стеке не обнаружен мастер (RTT-A230-24T-4XG)
PoE	Индикатор состояния PoE-портов	Зеленый, горит постоянно	Подключен потребитель PoE (горит индикатор, соответствующий порту)
		Выключен	Потребители PoE не подключены
Резерв	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
Батарея (RTT-A230-48T-4XG)	Индикатор состояния аккумуляторной батареи	Зеленый, горит постоянно	АКБ подключена, питание в норме
		Зеленый, мигание	АКБ заряжается
		Оранжевый, горит постоянно	Основное питание отключено, АКБ разряжается
		Мигает, красный-зеленый	Низкий уровень заряда АКБ
		Красный, горит постоянно	АКБ отключена
		Красный, мигание	Авария РТБ (расцепителя тока батареи)
	Индикатор состояния	Зеленый, горит постоянно	Блок питания установлен в слот, питание включено.

БП1, БП2 (RTT-A230-48P-4XG)	модулей питания	Красный, горит постоянно	Блок питания установлен в слот, но питание отключено; блок питания установлен в слот, питание включено, но имеется неисправность
		Выключен	Блок питания не установлен в слот
Предупр.	Световая индикация системных индикаторов	Оранжевый, горит постоянно	Нагрузка PoE выше настройки usage-threshold
		Красный, горит постоянно	Критическая ошибка в работе PoE, приведшая к отключению PoE на всех портах либо отказ одного или более вентиляторов
		Выключен	Нагрузка PoE ниже настройки usage-threshold

2.5 Комплект поставки

В базовый комплект поставки входят:

– Ethernet-коммутатор;

– модуль питания (в зависимости от модели коммутатора);

– шнур питания (в зависимости от модели коммутатора);

– консольный кабель;

– комплект крепежа в стойку;

– документация (в зависимости от модели коммутатора).

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

3. УСТАНОВКА И ПОДКЛЮЧЕНИЕ

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

3.1. Крепление кронштейнов

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

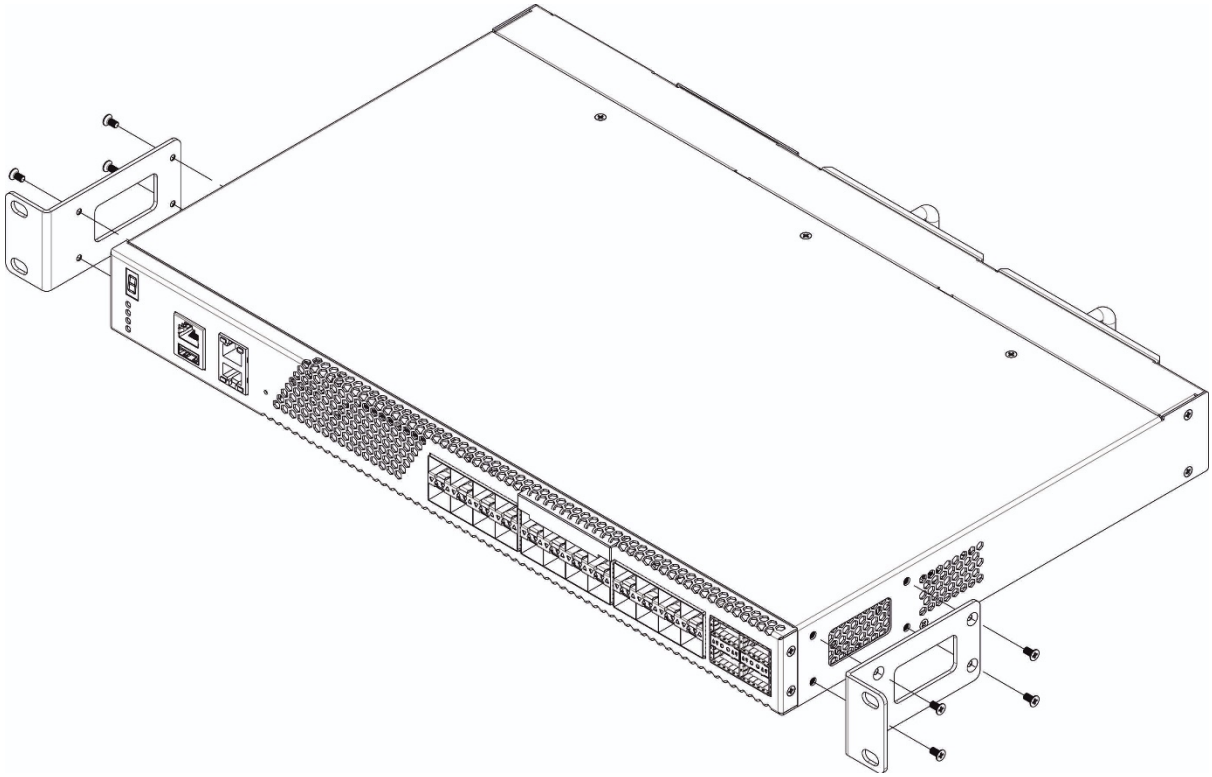


Рис. 24 – Крепление кронштейнов

– совместите четыре отверстия для винтов на кронштейне с такими же отверстиями на боковой панели устройства;

– с помощью отвертки прикрепите кронштейн винтами к корпусу.

– повторите действия предыдущие действия для второго кронштейна.

3.2. Установка устройства в стойку

Для установки устройства в стойку:

– приложите устройство к вертикальным направляющим стойки;

– 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;

– с помощью отвертки прикрепите коммутатор к стойке винтами.

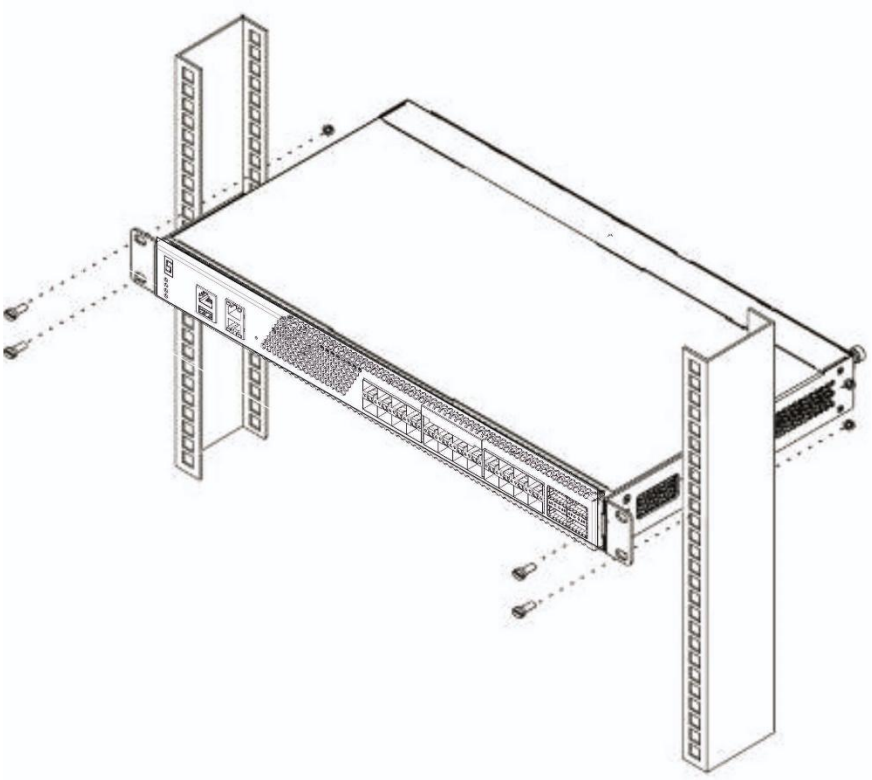


Рис. 25 – Установка устройства в стойку

На Рис. 26 приведен пример размещения коммутаторов RTT-A420 в стойке.

Рис. 26 – Размещение коммутаторов RTT-A420 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

В зависимости от модели коммутатора возможно использование съемных модулей питания. В таком случае коммутатор может работать с одним или двумя модулями питания. Установка второго модуля питания необходима в случае использования устройства в условиях, требующих повышенной надежности.

Слоты 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.

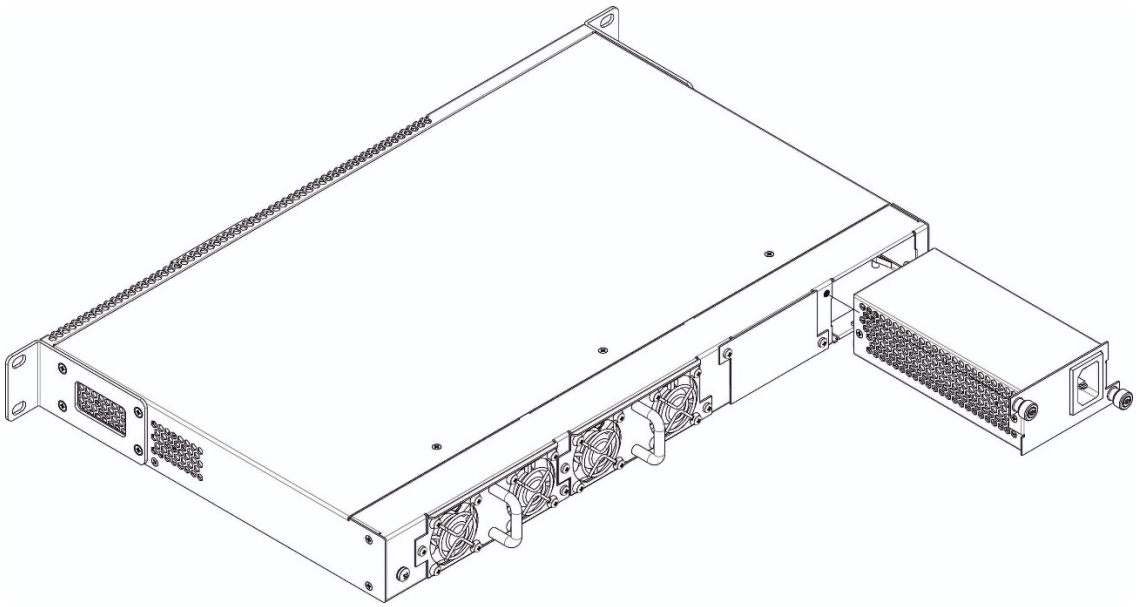


Рис. 27 – Установка модулей питания

Состояние модулей питания может быть проверено по индикации на передней панели коммутатора 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

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.

Если предполагается подключение компьютера или иного оборудования к консольному порту коммутатора, это оборудование также должно быть надежно заземлено.

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.

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

3.5. Подключение АКБ к коммутатору

Если модель коммутатора предусматривает использование АКБ, то его подключение осуществляется медным проводом сечением не менее 1,5 мм^2. При подключении АКБ необходимо соблюдать полярность. Ёмкость АКБ не менее 20 ампер часов.

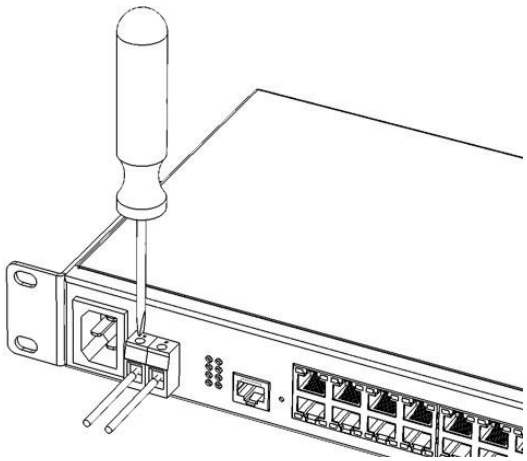


Рис. 28 – Подключение АКБ к устройству

3.6. Установка и удаление SFP-трансиверов

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

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

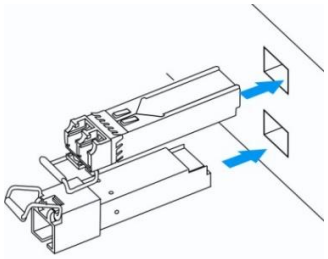


Рис. 29 – Установка SFP-трансиверов

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

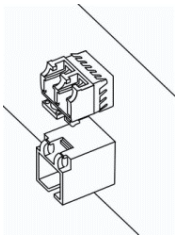


Рис. 30 – Установленные SFP-трансиверы

Для удаления трансивера:

Откройте защелку модуля.

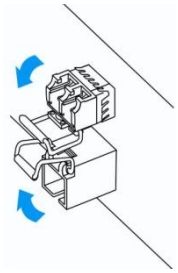


Рис. 31 – Открытие защелки SFP-трансиверов

Извлеките модуль из слота.

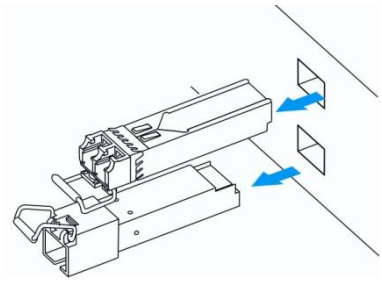


Рис. 32 – Извлечение SFP-трансиверов

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).

Пример отображения хода выполнения процедуры POST на коммутаторах:

```
BootROM 1.20
Booting from SPI flash
General initialization - Version: 1.0.0
High speed PHY - Version: 2.1.5 (COM-PHY-V20)
Update Device ID PEX0784611AB
Update Device ID PEX1784611AB
Update Device ID PEX2784611AB
Update Device ID PEX3784611AB
Update Device ID PEX4784611AB
Update Device ID PEX5784611AB
Update Device ID PEX6784611AB
Update Device ID PEX7784611AB
```

```
Update Device ID PEX8784611AB
Update PEX Device ID 0x78460
High speed PHY - Ended Successfully
DDR3 Training Sequence - Ver 5.3.0
DDR3 Training Sequence - Number of DIMMs detected: 1
DDR3 Training Sequence - Run with PBS.
DDR3 Training Sequence - Ended Successfully
BootROM: Image checksum verification PASSED
Starting U-Boot. Press ctrl+shift+6 to enable debug mode.


U-Boot 2018.12 (Feb 01 2018 - 14:45:42) Rustel version: v2018.12 2018_Q3.0 4.0.1

Loading system/images/active-image...

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 2018.12 (Feb 01 2018 - 14:45:42) Rustel version: v2018.12 2018_Q3.0 4.0.1

Loading system/images/active-image...

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

Вид загрузочного меню:

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

Таблица 23 – Функции интерфейса загрузочного меню

Функция	***Описание***
Restore Factory Defaults	Восстановить заводские настройки
Boot password	Установить / удалить пароль на bootrom
Image menu	Выбрать активный образа системного ПО
Password Recovery Procedure	Сбросить настройки аутентификации
Back	Продолжить загрузку

4.4. Режим работы коммутатора

Коммутаторы 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 от 1 до 8), ведущее устройство, с которого происходит управление всеми устройствами в стеке. Роль можно назначить всем устройствам, но активный master при этом будет один, остальные будут функционировать в роли Backup.
- *Backup* (UID устройства от 1 до 8) – устройство, подчиняющееся master. Дублирует все настройки и в случае выхода управляющего устройства из строя берет на себя функции управления стеком. Роль можно назначить максимум семи устройствам.
- *Slave* (UID устройств от 1 до 8) – устройство, подчиняющееся master. Не может работать в автономном режиме (если отсутствует master).

Роль можно назначить максимум шести устройствам. Допустима корректная работа стека без устройств с данной ролью.

Для корректной работы стека необходим хотя бы один юнит с ролью master и один юнит с ролью backup.

Интерфейсы в режиме стекирования работают только на максимальной скорости интерфейса.

По умолчанию коммутатор находится в роли master, порты XLG (XG) участвуют в передаче данных.

Для соединения в стек коммутатор RTT-A420-24XG-4QXG использует XLG-порты для синхронизации, модели RTT-A230-8T-2G и RTT-A230-8P-4G используют оптические порты 1G, остальные коммутаторы используют порты XG. При этом использованные для стека порты не участвуют в передаче данных.

Возможны две топологии синхронизирующихся устройств — кольцевая и линейная. Для повышения отказоустойчивости стека рекомендуется использовать кольцевую топологию. При использовании линейной топологии в схеме из двух юнитов стековые порты объединяются в LAG, что позволяет повысить пропускную способность канала. При использовании кольцевой топологии один стековый линк блокируется для Broadcast, Multicast, Unknown Unicast-трафика и не блокируется для обученного Unicast-трафика, что позволяет повысить пропускную способность стековых линков.

Для коммутаторов RTT-A230-48P-4XG, RTT-A230-48T-4XG, RTT-A330-48T-4XG, RTT-A330-48F-4XG для объединения в линейной топологии стековых портов в LAG необходимо использовать интерфейсы te1-8/0/1, te1-8/0/4 или te1-8/0/2, te1-8/0/3. При любых других комбинациях стековых портов один из них будет находиться в резерве и иметь статус Standby.

Коммутаторы всех серий поддерживают функционал NSF (Non-Stop Forwarding) в стеке. Данный функционал позволяет минимизировать потери для транзитного немаршрутизируемого трафика в момент передачи мастерства от master к backup.

Принцип работы NSF: в момент, когда backup берет управление на себя и запускает процесс доинициализации до роли master, запускается таймер NSF и фиксируются STP-статусы портов, порты в LACP, членство портов во VLAN,

скорость портов и т.д. Остальные настройки применяются на коммутаторе, ставшем master, в реальном времени.

При этом во время процесса NSF изменение статуса портов в STP на стеке полностью игнорируется. Также запрещается выполнение команд просмотра конфигурации (команды «show running-config, show startup-config» в режиме EXEC), изменение состояния портов (команды «shutdown, no shutdown» в контекстном меню конфигурации интерфейса) и VLAN (команда «vlan 2» в контекстном меню «vlan database»), скорости портов (“negotiation, speed” в контекстном меню конфигурации интерфейса), очистка FDB («clear mac address-table dynamic» в режиме EXEC), перезагрузка устройства («reload» в режиме EXEC), изменение имени устройства («hostname» в режиме глобальной конфигурации), включение/выключение STP («no spanning-tree» в режиме глобальной конфигурации).

Когда истекает таймер NSF, все ранее зафиксированные настройки применяются к стеку в реальном времени.

Таблица 24 — Матрица стекирования для RTT-A230

	RTT-A230-8T-2G-AC	*RTT-A230-8P-4G-AC*	*RTT-A230-24T-4XG*	*RTT-A230-24F-4XG*	*RTT-A230-48T-4XG*	*RTT-A230-24F-4XG*	*RTT-A230-24P-4XG*	*RTT-A230-48P-4XG*
RTT-A230-8T-2G-AC	+	-	-	-	-	-	-	-
RTT-A230-8P-4G-AC	-	+	-	-	-	-	-	-
RTT-A230-24T-4XG	-	-	+	+	-	+	-	-
RTT-A230-24F-4XG	-	-	+	+	-	+	-	-
RTT-A230-48T-4XG	-	-	-	-	+	-	-	-
RTT-A230-24F-4XG	-	-	+	+	-	+	-	-
RTT-A230-24P-4XG	-	-	-	-	-	-	+	+

RTT-A230-48P-4XG	-	-	-	-	-	-	+	+

Таблица 25 — Матрица стекирования для RTT-A330 и RTT-A420-24XG-4QXG

	RTT-A330-24T-4XG	***RTT-A330-24F-4XG***	***RTT-A330-8F-4XG***	***RTT-A330-16F-4XG***	***RTT-A330-48T-4XG***	***RTT-A330-48F-4XG***	***RTT-A420-24XG-4QXG***
RTT-A330-24T-4XG	+	+	+	+	-	-	-
RTT-A330-24F-4XG	+	+	+	+	-	-	-
RTT-A330-8F-4XG	+	+	+	+	-	-	-
RTT-A330-16F-4XG	+	+	+	+	-	-	-
RTT-A330-48T-4XG	-	-	-	-	+	+	-
RTT-A330-48F-4XG	-	-	-	-	+	+	-
RTT-A420-24XG-4QXG	-	-	-	-	-	-	+

Настройка стекирования коммутаторов

Запрос командной строки имеет следующий вид:

```
console(config)#
```

Таблица 26 – Команды для настройки стека

Команда	***Значение/Значение по умолчанию***	***Действие***
stack configuration links {fo1-4| te1-4 | gi9-12}	—	Назначить интерфейсы для синхронизации работы коммутатора в стеке. Минимальное количество — 1, максимальное — 2.
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		Удалить настройки стека.
stack configuration master unit *unit_id*	unit_id: (1..8)/—	Принудительно назначить устройство мастером (мастерство будет всегда сохранено за юнитом в случае наличия его в стеке). Если в команде указать номер устройства, отличный от того, на котором выполняем ее, то текущий мастер принудительно перезагрузится для отдачи мастерства.
no stack configuration master		Вернуть выбор мастера к стандартному алгоритму (после перезагрузки мастером будет выбрано устройство с наибольшим uptime).

stack configuration fec {off|cl74}	—/off	Настроить режим Forward Error Correction (FEC) на интерфейсах стека. **Только для RTT-A420-24XG-4QXG.**
stack nsf	—/выключено	Разрешить непрерывную передачу данных (NSF) во время отдачи мастерства.
no stack nsf		Запретить непрерывную передачу данных (NSF) во время отдачи мастерства.
stack nsf timer *value*	value: (60..600) с/120 с	Задать время, в течение которого длится NSF.
no stack nsf timer		Установить значение по умолчанию.
stack unit *unit_id*	unit_id: (1..8)	Перейти к конфигурированию юнита в стеке.

Команды режима конфигурации юнита

Вид запроса командной строки в режиме конфигурации юнита:

```
console(unit)#
```

Таблица 27 — Команды для настройки отдельного юнита

Команда	***Значение/Значение по умолчанию***	***Действие***
stack configuration role {slave | master}	role: (master, backup, slave)/1 — master, 2 — backup, 3-8 — slave	Назначить роль коммутатора в стеке.
no stack configuration role		Установить значение по умолчанию.
stack configuration links {fo1-4 | te1-4 | gi9-12}	—	Назначить интерфейсы для синхронизации работы коммутатора в стеке.
stack configuration unit-id *unit_id*	unit_id: (1..8, auto)/auto	Назначить номер устройства «unit-id» конфигурируемому юниту. Смена номера устройства произойдет после перезагрузки коммутатора.
no stack configuration		Удалить настройки стека.

Для применения настроек стека необходима перезагрузка устройства.

Пример

- Настроить RTT-A420-24XG-4QXG для работы в режиме стекирования. Назначить вторым юнитом, использовать интерфейсы fo1-2 в качестве стекирующих.

```
console#config
console(config)#stack configuration unit-id 2 links fo1-2
console(config)#
```

Команды режима privileged EXEC

Запрос командной строки имеет следующий вид:

```
console#
```

Таблица 28 – 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       fo1/0/1              fo2/0/2              40G         fo1/0/2
2       fo2/0/2              fo1/0/1              40G         fo2/0/1
```

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 **«rustel»** и создания пользователя **«operator»** с паролем **«pass»** и уровнем привилегий 1:

```
console# configure
console(config)# username admin password rustel privilege 15
console(config)# username operator password pass privilege 1
console(config)# exit
console#
```

4.5.1.2. Расширенная настройка уровня доступа

На устройстве существует возможность распределения прав пользователей в зависимости от уровня привилегий, на котором каждый из пользователей был создан. Конкретному уровню привилегий присваивается набор команд, которые могут выполняться пользователями с уровнем не ниже заданного.

Коммутатор поддерживает систему наследования набора команд от более низких уровней привилегий.

Привилегии выстраиваются только для конкретно заданного узла. Каждую команду необходимо прописывать явно, не используя сокращенные формы.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console (config) #
```

Таблица 29 – Команды для настройки расширенного доступа

Команда	***Значение/значение по умолчанию***	***Действие***
privilege *context level command*	level: (1..15); /уровень привилегий команд режима EXEC – 1, всех остальных команд – 15	Присваивает указанному уровню привилегий заданную команду. - *context* – режим работы командной строки; - *level* – уровень привилегий, на котором будет доступна настраиваемая команда; - *command* – команда.
No privilege *context level command*		Удаляет доступ к команде с уровня, на котором команда была разрешена.

- Пример настройки набора команд для пользователя **«admin»** с 4 уровнем привилегий и набора команд для пользователя **«user»** с 10 уровнем привилегий

```
console#configure
console(config)#username admin password pass1 privilege 4
console(config)#username user password pass2 privilege 10
console(config)#privilege exec 4 configure terminal
console(config)#privilege exec 4 show running-config
console(config)#privilege config 10 vlan database
console(config)#privilege config-vlan 10 vlan
```

Теперь для локальных пользователей, чей уровень привилегий выше или равен 4, станет доступен вывод команды *show running-config*, но не будет доступна настройка *vlan*. Для пользователей, уровень привилегий которых соответствует 10 и выше, будет доступна и настройка *vlan*, и вывод команды *show running-config*.

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

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

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

IP-адрес 192.168.1.239 существует до тех пор, пока на любом интерфейсе статически или по DHCP не создан другой IP-адрес.

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
```

4.5.1.4. 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 admin/oper	Type	Directed Broadcast	Prec	Redirect	Status
10.10.10.3/24	vlan 1	UP/UP	DHCP	disable	No	enable	Valid

4.5.1.5. 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. Если пароль утрачен, то можно перезагрузить устройство и через серийный порт прервать загрузку, нажав клавишу **<*Esc*>** или **<*Enter*>**. В течении первых двух секунд после появления сообщения автозагрузки откроется меню ***Startup***, в котором нужно запустить процедуру восстановления пароля ([2] Password Recovery Procedure).

Пользователь по умолчанию (admin/admin) существует до тех пор, пока не создан любой другой пользователь с уровнем привилегий 15.

При удалении всех созданных пользователей с 15 уровнем привилегий доступ к коммутатору будет осуществляться под пользователем по умолчанию (admin/admin).

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 authorization 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 authorization 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 authorization 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: Ordzhonikidze 11, str. 40
```

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***) – 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***) – 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***) – 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***) – 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 30 – 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>).
terminal no datadump		Установить значение по умолчанию.
terminal prompt	—/функция включена	Включить подтверждение перед выполнением некоторых команд.
terminal no prompt		Отключить подтверждение перед выполнением некоторых команд.
show banner [login | exec]	—	Отображает конфигурацию баннеров.

Команды режима privileged EXEC

Запрос командной строки имеет следующий вид:

```
console#
```

Таблица 31 – 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.

set system mode {acl-sqinq | acl-sqinq-udb}	acl-sqinq	Установить режим настройки фильтрации трафика. **- acl-sqinq** — режим по умолчанию; - **acl-sqinq-udb** — вдвое уменьшено количество возмож- ных правил SQinQ; добавлена возможность фильтрации по тринадцати оффсетам (в режиме по умолчанию — пять).

Команды, доступные во всех режимах конфигурации

Запрос командной строки имеет один из следующих видов:

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

Таблица 32 – 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

```
console(config)#
```

Таблица 33 – 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 34 – 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 ниже.

Таблица 35 – 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. Перенаправление вывода команд CLI в произвольный файл на ПЗУ

Интерфейс командной строки предоставляет возможность перенаправления вывода команд в произвольный файл на ПЗУ.

Для того чтобы копировать вывод команды в файл (перезаписать файл, если такой уже существует), требуется после набора команды отображения информации добавить символ «>» и указать имя файла. Для того, чтобы копировать вывод команды в конец файла, после набора команды отображения информации добавить символ «>>» и указать имя файла. Пример использования:

```
console#show system >> flash://directory/filename
```

Перенаправлять вывод команд в файл может только пользователь с 15 уровнем привилегий.

5.4. Настройка макрокоманд

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

Команды режима глобальной конфигурации

Таблица 36 – Команды режима глобальной конфигурации

Команда	***Значение/Значение по умолчанию***	***Действие***
macro name *word [***track** object *[***state** *activation_state]]*	*word*: (1..32) символов object: (1..64); *activation_state*: (any, up, down)/any	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. В теле макроса можно использовать до трёх переменных в конфигурации. Если задан параметр **track**, макрос будет активирован при изменении TRACK объекта с номером object, в соответствии с параметром **state** (up — активация при переходе из состояния DOWN в состояние UP, down — активация при переходе из состояния UP в состояние DOWN, any — активация при любом изменении состояния). Макрос не может быть активирован изменением TRACK объекта при наличии переменных в теле.
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

Таблица 37 – Команды режима EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
macro apply *word* **[***pattern1 value1***] [***pattern2 value2***] [***pattern3 value3***]**	word: (1..32) символов	Применяет указанный макрос. ***pattern*** - шаблон, состоящий из объявления, например символа "$", и переменной, написанных слитно ***value*** – переменная конфигурации
macro trace *word*		Проверяет указанный макрос на валидность.
show parser macro [{brief | description [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}] | name** *word***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); word: (1..32) символов	Отображает параметры настроенных макросов на устройстве.

Команды режима конфигурации интерфейса

Таблица 38 – Команды режима конфигурации интерфейса

Команда	***Значение/Значение по умолчанию***	***Действие***
macro apply *word* **[***pattern1 value1***] [***pattern2 value2***] [***pattern3 value3***]**	word: (1..32) символов	Применяет указанный макрос. ***pattern*** - шаблон, состоящий из объявления, например символа "$", и переменной, написанных слитно ***value*** – переменная конфигурации
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.

5.5. Команды управления системой

Команды режима EXEC

Таблица 39 – Команды управления системой в режиме EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
ping [ip] {*A.B.C.D* **|** *host***}** [**vrf** *vrf-name*] **[size** *size***] [count** *count***] [timeout** *timeout***] [source** *A.B.C.D***] [df]**	vrf-name: (1..32) символа; 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). - vrf-name — имя виртуальной области маршрутизации; - *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; - **df** — отменить фрагментацию пакетов.
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 также 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***}** [**vrf** *vrf-name*] **[size** *size***] [ttl** *ttl***] [count** *count***] [timeout** *timeout***] [source** *ip_address***]**	vrf-name: (1..32) символа; host: (1..158) символов; size: (64..1518)/64 байт; ttl: (1..255)/30; count: (1..10)/3; timeout: (1..60)/3 с;	Определить маршрут трафика до узла назначения. - vrf-name — имя виртуальной области маршрутизации; - *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 41, 42.**

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;	Определить маршрут 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 41, 42.**
telnet {*A.B.C.D* **|** *host*} [*port*] [*keyword1…*]	host: (1..158) символов; port: (1..65535)/23	Открыть TELNET-сессию 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 таблице 43.**
ssh {*A.B.C.D* **|** *host*} [*port*] [*keyword1...*]	host: (1..158) символов; port: (1..65535)/22;	Открыть SSH-сессию 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 44.**
resume [*connection*]	connection: (1..5)/последняя установленная сессия	Переключиться на другую установленную telnet-сессию. - *connection* — номер установленной telnet-сессии.
show users [accounts]	—	Отобразить информацию о пользователях, использующих ресурсы устройства.
show sessions	—	Отобразить информацию об открытых сессиях к удаленным устройствам.
show system	—	Вывести системную информацию.
show system battery [unit *unit*]	unit: (1..8)/—	Отобразить информацию о батарее. - *unit* — номер устройства в стеке.
show system id [unit *unit*]	unit: (1..8)/—	Отобразить серийный номер устройства, ревизию платы и базовый MAC-адрес. - *unit* — номер устройства в стеке.
show system [unit *unit*]	unit: (1..8)/—	Отобразить системную информацию коммутатора. - *unit* — номер устройства в стеке.
show system fans [unit *unit*]	unit: (1..8)/—	Отобразить информацию о состоянии вентиляторов. - *unit* — номер устройства в стеке.
show system power-supply	—	Отобразить информацию о состоянии источников питания.
show system sensors	—	Отобразить информацию температурных датчиков.
show version	—	Отобразить текущую версию системного программного обеспечения устройства.
show system router resources		Отобразить размер и занятость аппаратных таблиц устройства (маршрутизации, соседей, интерфейсов).
show system tcam utilization [unit *unit*]	unit: (1..8)/—	Отобразить загрузку ресурсов памяти TCAM (определенно адресуемая память). - *unit* — номер устройства в стеке.
show tasks utilization	—	Отобразить уровень загрузки ресурсов центрального процессора коммутатора для каждого системного процесса.

show tech-support [config | memory]	—	Отобразить информацию об устройстве, необходимую для начальной диагностики проблем. **Вывод команды представляет собой комбинацию выводов перечисленных ниже команд:** • **show clock** • **show system** • **show version** • **show bootvar** • **show running-config** • **show ip interface** • **show ipv6 interface** • **show spanning-tree active** • **show stack** • **show stack configuration** • **show stack links details** • **show interfaces status** • **show interfaces counters** • **show interfaces utilization** • **show interfaces te1/0/xx** • **show fiber-ports optical-transceiver** • **show interfaces channel-group** • **show cpu utilization** • **show cpu input-rate detailed** • **show tasks utilization** • **show mac address-table count** • **show arp** • **show errdisable interfaces** • **show vlan** • **show ip igmp snooping groups** • **show ip igmp snooping mrouter** • **show ipv6 mld snooping groups** • **show ipv6 mld snooping mrouter** • **show logging file** • **show logging** • **show users** • **show sessions** • **show system router resource** • **show system tcam utilization**
show storage devices	—	Отобразить значения объема и свободной памяти ПЗУ.

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;**

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

Таблица 40 – Команды управления системой в режиме privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
reload [unit *unit_id***]**	unit_id: (1..8)/—	Перезапустить устройство. - *unit_id* — номер устройства в стеке.
reload in {*minutes* **|** *hh:mm***}**	minutes: (1..999); hh: (0..23), mm: (0..59).	Установить промежуток времени, через который произойдет отложенная перезагрузка устройства.
reload at *hh:mm*	hh: (0..23), mm: (0..59).	Установить время перезагрузки устройства.
boot password *password*	—	Установить пароль на bootrom.
no boot password		Удалить пароль на bootrom.
reload cancel	—	Отменить отложенный перезапуск.
show cpu utilization	—	Отобразить статистику по уровню загрузки ресурсов центрального процессора.
show cpu input rate	—	Отобразить статистику по скорости входящих кадров, обрабатываемых процессором.
show cpu input-rate detailed	—	Отобразить статистику по скорости входящих кадров, обрабатываемых процессором по типу трафика.
show cpu thresholds	—	Отобразить список настроенных порогов для CPU.
show memory thresholds	—	Отобразить список настроенных порогов для RAM.
show sensor thresholds	—	Отобразить список порогов для датчиков.
show storage thresholds	—	Отобразить список порогов для разделов устройств.
show system mode	—	Отобразить информацию о параметрах фильтрации трафика.

- Пример использования команды **traceroute**:

```
console# traceroute ip rusteletech.ru
```

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

Таблица 41 – Описание результатов выполнения команды *traceroute*

Поле	***Описание***
1	Порядковый номер маршрутизатора в пути к указанному узлу сети.
gateway.rusteletech	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 ниже.

Таблица 42 – 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 43 – 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 44 – 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

Таблица 45 – Команды управления системой в режиме глобальной конфигурации

Команда	***Значение/Значение по умолчанию***	***Действие***
hostname *name*		Задать сетевое имя устройства.

no hostname	name: (1..160) символов/—	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	—/включено	Разрешить устройству программно измерять скорость входящих кадров, обрабатываемых центральным процессором коммутатора.
no service cpu-input-rate		Запретить устройству программно измерять скорость входящих кадров, 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, multicast-routing, multicast-rpf-fail, tcp-syn); pps: 8..2048	Установить на CPU ограничения скорости входящих кадров для определенного типа трафика. - *pps* — пакетов в секунду. **Реализует функцию CoPP (Control Plane Protection).**
no service cpu-rate-limits *traffic*		Восстановить 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-flapping enable	—/enabled	Включить предотвращение флаппинга линка.
link-flapping 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***]**	ip_entries: (8..8024)/5120; ipv6_entries: (32..8048)/1024; ipm_entries: (8..8024)/512; ipmv6_entries: (32..8048)/512	Установить размер таблицы маршрутизации.

cpu threshold index *index interval* **relation** *value* **[flap-interval** *flap_interval*] **[severity** *level***] [notify {enable | disable}] [recovery-notify {enable | disable}]**	index: (0..4294967295); interval: (5sec, 1min, 5min); relation: (greater-than, greater-or-equal, less-than, less-or-equal, equal-to, not-equal-to); value: (0..100) процентов; flap_interval: (0..100)/0 процентов; severity: (emerg, alert, crit, err, warning, notice, info, debug)/alert	Задать порог для загрузки CPU. - *index* — произвольный индекс порога; - *interval* — интервал измерения загрузки CPU. Значение загрузки CPU за этот интервал будет сравниваться с пороговым; - *relation* — отношение между загрузкой CPU и пороговым значением, необходимое для срабатывания порога; - *value* — значение порога; - *flap_interval* — значение, определяющее момент восстановления порога после срабатывания; - *severity* — уровень важности трапов для этого порога; - **notify** — включает/отключает отправку трапов о срабатывании порога; - **recovery-notify** — включает/отключает отправку трапов о восстановлении порога.
no cpu threshold index *index*		Удалить порог с заданным индексом.
memory threshold index *index relation value* **[flap-interval** *flap_interval***] [severity** *level***] [notify {enable | disable}] [recovery-notify {enable | disable}]**	index: (0..4294967295); relation: (greater-than, greater-or-equal, less-than, less-or-equal, equal-to, not-equal-to); value: (0..100) процентов; flap_interval: (0..100)/0 процентов; severity: (emerg, alert, crit, err, warning, notice, info, debug)/alert	Задать порог для объема свободной памяти RAM. **-** *index* — произвольный индекс порога; - *relation* — отношение между объемом свободной памяти и пороговым значением, необходимое для срабатывания порога; - *value* — значение порога; - *flap_interval* — значение, определяющее момент восстановления порога после срабатывания; - *severity* — уровень важности трапов для этого порога; **- notify —** включает/отключает отправку трапов о срабатывании порога; **- recovery-notify —** включает/отключает отправку трапов о восстановлении порога.
no memory threshold index *index*		Удалить порог с заданным индексом.
sensor threshold fan *fan_num* **unit-id** *unit_id* **index** *index relation value* **[flap-interval** *flap_interval***] [severity** *level***] [notify {enable | disable}] [recovery-notify {enable | disable}]**	fan_num: (1..63); unit_id: (1..8); index: (0..4294967295); relation: (greater-than, greater-or-equal, less-than, less-or-equal, equal-to, not-equal-to); value: (0..1000000000) оборотов/мин; flap_interval: (0..1000000000)/0 оборотов/мин; severity: (emerg, alert, crit, err, warning, notice, info, debug)/alert	Задать порог для датчика скорости вращения вентилятора. - *fan_num* — номер вентилятора; - *unit_id* — номер юнита, на котором находится вентилятор; **-** *index* — произвольный индекс порога; - *relation* — отношение между скоростью вращения вентилятора и пороговым значением, необходимое для срабатывания порога; - *value* — значение порога; - *flap_interval* — значение, определяющее момент восстановления порога после срабатывания; - *severity* — уровень важности трапов для этого порога; **- notify —** включает/отключает отправку трапов о срабатывании порога; **- recovery-notify —** включает/отключает отправку трапов о восстановлении порога.
no sensor threshold fan *fan_num* **unit-id** *unit_id* **index** *index*		Удалить порог с заданным индексом для вентилятора *fan_num* на юните *unit_id.*

sensor threshold thermal-sensor *sensor_num* **unit-id** *unit_id* **index** *index relation value* **[flap-interval** *flap_interval***] [severity** *level***] [notify {enable | disable}] [recovery-notify {enable | disable}]**	sensor_num: (1..63); unit_id: (1..8); index: (0..4294967295); relation: (greater-than, greater-or-equal, less-than, less-or-equal, equal-to, not-equal-to); value: (-1000000000..1000000000) °C; flap_interval: (0..1000000000)/0 °C; severity: (emerg, alert, crit, err, warning, notice, info, debug)/alert	Задать порог для датчика температуры. - *sensor_num* — номер термодатчика; - *unit_id* — номер юнита, на котором находится термодатчик; - *index* — произвольный индекс порога; - *relation* — отношение между температурой и пороговым значением, необходимое для срабатывания порога; - *value* — значение порога; - *flap_interval* — значение, определяющее момент восстановления порога после срабатывания; - *severity* — уровень важности трапов для этого порога; - **notify —** включает/отключает отправку трапов о срабатывании порога; - **recovery-notify —** включает/отключает отправку трапов о восстановлении порога.
no sensor threshold thermal-sensor *sensor_num* **unit-id** *unit_id* **index** *index*		Удалить порог с заданным индексом для термодатчика *sensor_num* на юните *unit_id.*
storage threshold index *index interval relation value* **[flap-interval** *flap_interval***] [severity** *level***] [notify {enable | disable}] [recovery-notify {enable | disable}]**	index: (0..4294967295); relation: (greater-than, greater-or-equal, less-than, less-or-equal, equal-to, not-equal-to); value: (0..100) процентов; interval: (0..100)/0 процентов; severity: (emerg, alert, crit, err, warning, notice, info, debug)/alert;	Задать порог для объема свободной памяти на ПЗУ. - *index* — произвольный индекс порога; - *relation* — отношение между объема свободной памяти и пороговым значением, необходимое для срабатывания порога; - *value* — значение порога; - *flap_interval* — значение, определяющее момент восстановления порога после срабатывания; - *severity* — уровень важности трапов для этого порога; - **notify —** включает/отключает отправку трапов о срабатывании порога; - **recovery-notify —** включает/отключает отправку трапов о восстановлении порога.
no storage threshold index *index*		Удалить порог с заданным индексом.
reset-button {enable | disable | reset-only}	—/enable	Настроить реакцию коммутатора на нажатие кнопки F. - **enable** — при нажатии на кнопку длительностью менее 10 сек, происходит перезагрузка устройства; при нажатии на кнопку длительностью более 10 сек, происходит сброс устройства до заводской конфигурации; - **disable —** не реагировать (отключена); - **reset-only —** только перезагрузка.

5.6. 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

Таблица 46 – Команды управления системой в режиме глобальной конфигурации

Команда	***Значение/Значение по умолчанию***	***Действие***
passwords aging *age*	age: (0..365)/180 дней	Задать 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		Восстановить значение по умолчанию.

passwords complexity enable	—/выключено	Включить ограничение на формат пароля.
no passwords complexity enable		Выключить ограничение на формат пароля.
passwords complexity min-classes *value*	value: (0..4)/3	Включить ограничение, задающее минимальное количество классов символов (строчные буквы, заглавные буквы, цифры, символы).
no passwords complexity min-classes		Восстановить значение по умолчанию.
passwords complexity min-length *value*	value: (0..64)/8	Включить ограничение на минимальную длину пароля.
no passwords complexity min-length		Восстановить значение по умолчанию.
passwords complexity no-repeat *number*	number: (0..16)/3	Включить ограничение, задающее максимальное количество последовательно повторяющихся символов в новом пароле.
no password complexity no-repeat		Восстановить значение по умолчанию.
passwords complexity not-current	—/enabled	Запретить при смене пароля использовать в качестве нового старый.
no passwords complexity not-current		Разрешить использовать старый пароль при смене.
passwords complexity not-username	—/enabled	Запретить использовать в качестве пароля имя пользователя.
no passwords complexity not-username		Разрешить использовать в качестве пароля имя пользователя.
password lockout *value*	value: (1..5)/—	Установить количество идущих подряд попыток ввода пароля с ошибкой до блокировки локальной учетной записи пользователя.
no password lockout		Установить значение по умолчанию.
passwords time block seconds	seconds: (0..7200)/0	Установить время блокировки локальной учетной записи пользователя.
no passwords time block		Установить значение по умолчанию.

Таблица 47 – Команды управления системой в режиме Privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show passwords configuration	—	Отобразить информацию об ограничениях на пароли.
set username *username* **active**	—	Разблокировать пользователя, заблокированного по причине неверного ввода пароля.

5.7. Работа с файлами

5.7.1. 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 48.

Таблица 48 – 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.
ftp://	Исходный адрес или адрес места назначения для FTP-сервера. Синтаксис: **ftp://[username[:password]@host/[directory/] filename** - *username* — имя пользователя; - *password* — пароль пользователя; - *host* — IPv4-адрес или сетевое имя устройства; - *directory* — каталог; - *filename* — имя файла.
tftp://	Исходный адрес или адрес места назначения для TFTP-сервера. Синтаксис: **tftp://host[:port]/[directory/] filename.** - *host* — IPv4-адрес или сетевое имя устройства; - *port* — порт назначения; - *directory* — каталог; - *filename* — имя файла.
scp://	Исходный адрес или адрес места назначения для SSH-сервера. Синтаксис: **scp://[username[:password]@]host[:port]/[directory/] filename** - *username* — имя пользователя; - *password* — пароль пользователя; - *host* — IPv4-адрес или сетевое имя устройства; - *port* — порт назначения; - *directory* — каталог; - *filename* — имя файла.
sftp://	Исходный адрес или адрес места назначения для SSH-сервера. Синтаксис: **sftp://[username[:password]@]host[:port]/[directory/] filename** - *username* — имя пользователя; - *password* — пароль пользователя; - *host* — IPv4-адрес или сетевое имя устройства; - *port* — порт назначения; - *directory* — каталог; - *filename* — имя файла.
logging	Файл с историей команд.

5.7.2. Команды для работы с файлами

Команды режима глобальной конфигурации

Таблица 49 — Команды для настройки параметров копирования в режиме глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip tftp source-interface {fortygigabitethernet *fo_port* **| tengigabitethernet** *te_port* **| gigabitethernet** *gi_port* **| loopback** *lb_port* **| tunnel** *tn_port* **| port-channel group | vlan** *vlan_id}*	fo_port: (1..4); te_port: (1..24); gi_port: (1..24); lb_port: (1..64); tn_port: (1..16); group: (1..48); vlan_id: (1..4094)	Определить IP-интерфейс источника для пакетов TFTP IPv4.

no ip tftp source-interface	/выключено	Установить значение по умолчанию.
ip sftp source-interface {fortygigabitethernet *fo_port* **| tengigabitethernet** *te_port* **| gigabitethernet** *gi_port* **| loopback** *lb_port* **| tunnel** *tn_port* **| port-channel group | vlan** *vlan_id}*	fo_port: (1..4); te_port: (1..24); gi_port: (1..24); lb_port: (1..64); tn_port: (1..16); group: (1..48); vlan_id: (1..4094)	Определить IP-интерфейс источника для пакетов SFTP IPv4.
no ip sftp source-interface	/выключено	Установить значение по умолчанию.

Команды режима privileged EXEC

Таблица 50 – 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;	Копировать файл 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		Копировать файл конфигурации с сервера в текущую конфигурацию.
copy running-config *destination_url* **[exclude | include-encrypted | include-plaintext]**		Сохранить текущую конфигурацию 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*		Сохранить первоначальную конфигурацию на сервере.
copy running-config startup-config	—	Сохранить текущую конфигурацию в первоначальную.
copy running-config *file*	—	Сохранить текущую конфигурацию в заданный резервный файл конфигурации.
copy **startup-config** *file*	—	Сохранить первоначальную конфигурацию в заданный резервный файл конфигурации.
boot config *source_url*	—	Копировать файл конфигурации с сервера в файл первоначальной конфигурации.
dir [flash:*path* | *dir_name*]	—	Отобразить список файлов в указанном каталоге.

more {flash:*file* | startup-config | running-config | mirror-config | active-image | inactive-image | logging | *file*}	file: (1..160) символов	Отобразить 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*	—	Удалить файл.
delete startup-config	—	Удалить файл первоначальной конфигурации.
boot system *source_url*	—	Копировать файл ПО с сервера в неактивную область памяти на место резервного ПО.
boot system inactive-image	—	Загрузить с неактивного образа ПО.
show {startup-config | running-config} interface {ip *ip_addr* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob | port-channel** *group* **| vlan** *vlan_id* **| tunnel** *tunnel_id* **| loopback** *loopback_id***} ipv6 {router ospf** *process_id***} router {ospf** *process_id***} [brief | detailed]**	ip_addr: A.B.C.D, all); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4) group: (1..48); vlan_id: (1..4094); tunnel_id: (1..16); loopback_id: (1..64); process_id: (1..65535)/1, all	Отобразить содержимое файла первоначальной (startup-config) или текущей (running-config) конфигурации. - **interfaces** — конфигурация интерфейсов коммутатора — IP-интерфейсов, физических интерфейсов, групп интерфейсов (port-channel), VLAN-интерфейсов, OOB-порта, loopback-интерфейсов, туннелей. Следующие опции доступны при выводе текущей конфигурации: - **ipv6 router ospf** — конфигурация IPv6 OSPF процессов. - **router ospf** — конфигурация IPv4 OSPF процессов. - **brief** — вывод конфигурации без двоичных данных, например, SSH- и SSL-ключей; - **detailed** — вывод конфигурации с включением двоичных данных. **Вывод контекстов конфигурации IP-интерфейсов и процессов OSPF доступен только для файла текущей конфигурации (running-config).**
show bootvar	—	Показать активный файл системного ПО, который устройство загружает при запуске.
write [memory]	—	Сохранить текущую конфигурацию в файл первоначальной конфигурации.
boot license *source_url*	—	Загрузить на устройство файл лицензии.
delete license [*word***]**	—	Удалить с устройства все установленные файлы лицензий. - *word* — имя файла лицензии, который должен быть удален.
rename *url new_url*	url, new_url: (1..160) символов	Изменить имя файла. - *url* — текущее имя файла; - *new-url* — новое имя файла.

Сервер TFTP не может быть адресом источника 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.

Существует возможность просмотра конфигурации для текущего местоположения для следующих режимов конфигурации:

- **vlan database**
- **interface** { **gigabitethernet** gi_port | **tengigabitethernet** te_port | **fortygigabitethernet** fo_port | **port-channel** *group* | **loopback** *loopback_id* | **vlan** vlan_id | **ip** ip_addr}
- **interface range** { **gigabitethernet** gi_port | **tengigabitethernet** te_port | **fortygigabitethernet** *fo_port* | **port-channel** *group* | **vlan** vlan_id}

Таблица 51 – Команды просмотра конфигурации из текущего местоположения

Команда	*Значение/Значение по умолчанию*	*Действие*
show	-	Отобразить настройки для текущего режима конфигурации

5.7.3. Команды для резервирования конфигурации

В данном разделе описаны команды, предназначенные для настройки резервирования конфигурации по таймеру или при сохранении текущей конфигурации на flash-накопителе.

Команды режима глобальной конфигурации

Таблица 52 – Команды управления системой в режиме глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
backup server *server* **port** *port*	server: (1..22) символов port: (0..65535)/порт по умолчанию (tftp — 69, scp — 22)	Указать сервер, на который будет производиться резервирование конфигурации. - *server* — строка в формате «tftp://XXX.XXX.XXX.XXX» или «scp://username:password@XXX.XXX.XXX.XX» - *port* — порт назначения сервера, на который будет происходить резервация конфигурации.
no backup server		Удалить сервер для резервирования.
backup path *path*	path: (1..128) символов	Указать путь расположения файла на сервере и префикса файла. При сохранении к префиксу будет добавляться текущая дата и время в формате ггггммддччммсс.
no backup path		Удалить пути для резервирования.
backup history enable	—/выключено	Включить сохранение истории резервных копий.
no backup history enable		Отключить сохранение истории резервных копий.
backup time-period *timer*	timer: (1..35791394)/720 мин	Указать промежуток времени, по истечении которого будет осуществляться автоматическое резервирование конфигурации.
no backup time-period		Восстановить значение по умолчанию.
backup auto	—/выключено	Включить автоматическое резервирование конфигурации.
no backup auto		Установить значение по умолчанию.
backup write-memory	—/выключено	Включить резервирование конфигурации при сохранении пользователем конфигурации на flash-накопитель.
no backup write-memory		Установить значение по умолчанию.

backup reachability-check tftp	—/включено	Включить отправку пустого пакета для проверки наличия TFTP-сервера (значение по умолчанию).
no backup reachability-check tftp		Отключить отправку пустого пакета для проверки наличия TFTP-сервера.

Таблица 53 – Команды управления системой в режиме Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show backup	-	Отображает информацию о настройках резервирования конфигурации
show backup history	-	Отображает историю успешно сохраненных на сервер конфигураций.

5.7.4. 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 загружается в первоначальную (startup) конфигурацию. После загрузки конфигурации коммутатор перезагружается.

Команды режима глобальной конфигурации

Таблица 54 – 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

Таблица 55 – 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
                     37293(Rusteletech)
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 rustel420-test {
         hardware ethernet a8:f9:4b:85:a2:00;   #mac-адрес коммутатора
         filename " Rustel-XXX-test.cfg";             #имя конфигурации коммутатора
         option image-filename 37293 18 1 16 " rustel-x.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
}
```

5.8. 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

Таблица 56 – 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 [vrf {*vrf_name* **| all}]**	vrf_name: (1..32) символов	Показать конфигурацию протокола SNTP. - *vrf_name* — имя виртуальной области маршрутизации.
show sntp status [vrf {*vrf_name* **| all}]**	vrf_name: (1..32) символов	Показать статус протокола синхронизации времени SNTP по сети. - *vrf_name* — имя виртуальной области маршрутизации.
show ntp	—	Показать текущее состояние и статистику службы NTP.
show ntp status	—	Показать статус протокола синхронизации времени NTP по сети.
show ntp associations [detail]	—	Показать информацию о согласовании устройства с NTP-серверами и одноранговыми узлами.
show ntp statistics	—	Показать статистику работы протокола.

Команды режима EXEC

Таблица 57 – 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

Таблица 58 – Список команд для настройки системного времени в режиме глобальной конфигурации

Команда	***Значение/Значение по умолчанию***	***Действие***
clock source {sntp | ntp | browser}	—/внешний источник не используется	Использовать внешний источник для установки системного времени. **В случае назначения источником ntp, устройство будет по умолчанию выполнять роль ntp-server, отвечая на запросы клиентов.**
no clock source {sntp | ntp | browser}		Запретить 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;	Установить 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		Установить 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	Задать 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***]**		Задать 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		Отключить автоматический переход на летнее время.
sntp authentication-key *number* **md5** *value*	number: (1..4294967295); value: (1..32) символов; По умолчанию проверка подлинности отключена	Установить 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*		Удалить ключ проверки подлинности для протокола SNTP.
sntp authenticate	—/проверка подлинности не требуется	Требовать проверку подлинности для получения информации от NTP-серверов.
no sntp authenticate		Установить значение по умолчанию.
sntp source-interface {fortygigabitethernet *fo_port* **| tengigabitethernet** *te_port* **| gigabitEthernet** *gi_port* **| loopback** *lb_port* **| tunnel** *tn_port* **| port-channel** *group* **| oob | vlan** *vlan_id***} [vrf {***vrf_name* **| all}]**	fo_port: (1..4); te_port: (1..24); gi_port: (1..24); lb_port: (1..64); tn_port: (1..16); group: (1..48); vlan_id: (1..4094); vrf_name: (1..32) символов /выключено	Определить IP-интерфейс источника для пакетов NTP IPv4. - *vrf_name* — имя виртуальной области маршрутизации.
no sntp source-interface		Установить значение по умолчанию.
sntp source-interface-ipv6 {fortygigabitethernet *fo_port* **| tengigabitethernet** *te_port* **| gigabitEthernet** *gi_port* **| loopback** *lb_port* **| tunnel** *tn_port* **| port-channel** *group* **| oob | vlan** *vlan_id***}**	fo_port: (1..4); te_port: (1..24); gi_port: (1..24); lb_port: (1..64); tn_port: (1..16); group: (1..48); vlan_id: (1..4094) /выключено	Определить IPv6-интерфейс источника для пакетов NTP IPv6.

no sntp source-interface-ipv6		Установить значение по умолчанию.
sntp source-port *udp_port*	udp_port: (1..65535)/по умолчанию используется случайный порт	Установить SRC UDP-порт для пакетов NTP. **При использовании UDP-портов из диапазона 1-1024 предварительно нужно убедиться, что данный порт свободен и не используется другими сервисами. Порт 50000 является портом по умолчанию для функционала peer detection ipaddr.**
no sntp source-port		Установить значение по умолчанию.
sntp trusted-key *key_number*	key_number: (1..4294967295); По умолчанию проверка подлинности отключена	Осуществить проверку подлинности системы, от которой синхронизируется с помощью SNTP по заданному ключу. - *key_number* — номер ключа.
no sntp trusted-key *key_number*		Установить значение по умолчанию.
sntp broadcast client enable {both | ipv4 | ipv6}	—/запрещено	Разрешить работу широковещательных SNTP-клиентов.
no sntp broadcast client enable		Установить значение по умолчанию.
sntp anycast client enable {both | ipv4 | ipv6}	—/запрещено	Разрешить работу SNTP-клиентам, поддерживающим метод рассылки пакетов, позволяющий посылать данные ближайшему устройству из группы получателей.
no sntp anycast client enable		Установить значение по умолчанию.
sntp client poll timer *seconds*	seconds: (60…86400)/1024	Установить время опроса для SNTP-сервера.
no sntp client poll timer		Установить значение по умолчанию.
sntp client enable {fortygigabitethernet *fo_port* **| tengigabitethernet** *te_port* **| port-channel** *group* **| oob | vlan** *vlan_id***}**	fo_port: (1..4); te_port: (1..24); group: (1..48); vlan_id (1..4094) /запрещено	Разрешить 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 {fortygigabitethernet *fo_port* **| tengigabitethernet** *te_port* **| port-channel** *group* **| oob | vlan** *vlan_id***}**		Установить значение по умолчанию.
sntp unicast client enable	—/запрещено	Разрешить работу одноадресных SNTP-клиентов.
no sntp unicast client enable		Установить значение по умолчанию.
sntp unicast client poll	—/запрещено	Разрешить последовательный опрос заданных одноадресных SNTP-серверов.
no sntp unicast client poll		Установить значение по умолчанию.

sntp server {ipv4_address | ipv6_address | ipv6_link_local_address%{vlan {integer} | ch {integer} | isatap {integer} | {physical_port_name}} | *hostname*} **[poll] [priority *priority*] [key** *keyid*] **[vrf {*vrf_name* | all}]**	priority: (0..255)/0 hostname: (1..158) символов; keyid: (1..4294967295); vrf_name: (1..32) символов	Задать адрес SNTP-сервера. - *priority* — приоритет сервера: при условии равных значений стратумов синхронизация времени будет выполняться с сервером, у которого наибольшее значение приоритета; - **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; - *vrf_name* — имя виртуальной области маршрутизации.
no sntp server {ipv4_address | ipv6_address | ipv6_link_local_address%{vlan {integer} | ch {integer} | isatap {integer} | {physical_port_name}} | *hostname*} **[vrf {*vrf_name* | all}]**		Удалить сервер из списка SNTP-серверов.
ntp {server | peer} {ipv4_address | ipv6_address | *hostname*} [version *version*]	version: (1..4)/4 hostname: (1..158) символов	Задать адрес NTP-сервера или одноранговой узла. - **ipv4_address** — IPv4-адрес узла сети; - **ipv6_address** — IPv6-адрес узла сети; - *hostname* — доменное имя узла сети; - **version** — определить версию протокола ntp.
no ntp {server | peer} {ipv4_address | ipv6_address | *hostname*}		Удалить сервер из списка NTP-серверов.
clock dhcp timezone	—/запрещено	Разрешить получение таких данных как часовой пояс и летнее время от DHCP-сервера.
no clock dhcp timezone		Запретить получение таких данных как часовой пояс и летнее время от DHCP-сервера.

Команды режима конфигурации интерфейса

Таблица 59 – 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.

- Указать ntp-server:

```
console(config)#clock source ntp
console(config)#ntp server 10.10.10.1
```

- Указать ntp-peer:

```
console(config)#clock source ntp
console(config)#ntp peer 10.10.10.1
```

- Указать sntp-server для unicast-режима:

```
console(config)#clock source sntp
console(config)#sntp client poll timer 60
console(config)#sntp unicast client enable
console(config)#sntp unicast client poll
console(config)#sntp server 10.10.10.1 poll
```

Для NTP-клиента в версиях ниже 4.0.23.1 допустима следующая конфигурация:

```
console(config)#clock source ntp
console(config)#sntp server <IP-адрес> poll
```

Начиная с версии 4.0.23.1 конфигурация NTP-клиента изменена в связи с полной поддержкой протокола NTP:

```
console(config)#clock source ntp
console(config)#ntp server <IP-адрес> poll
```

5.9. 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 60 – 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.

5.10. Конфигурация интерфейсов и VLAN

5.10.1. Параметры Ethernet-интерфейсов, Port-Channel и Loopback- интерфейсов

Команды режима конфигурации интерфейса (диапазона интерфейсов)

```
console# configure
console(config)# interface { gigabitethernet gi_port | tengigabitethernet
te_port | fortygigabitethernet fo_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, указанных в таблице ниже (в зависимости от модели коммутатора).

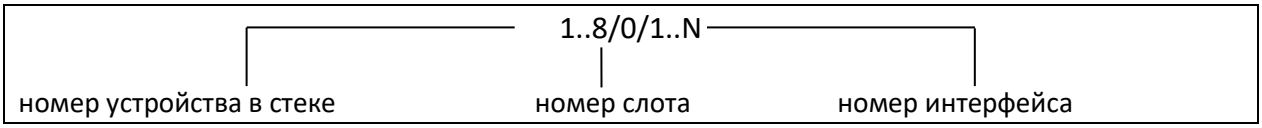
Таблица 61 – Команды выбора интерфейса в зависимости от модели коммутатора

Команда	*Назначение*	*Модель коммутатора*
interface fortygigabitethernet *fo_port*	для настройки 40G-интерфейсов	RTT-A420-24XG-4QXG
interface tengigabitethernet *te_port*	для настройки 10G-интерфейсов	RTT-A420-24XG-4QXG, все модели серии RTT-A330, все модели серии RTT-A230, кроме RTT-A230-8T-2G, RTT-A230-8P-4G
interface gigabitethernet *gi_port*	для настройки 1G-интерфейсов	все модели
interface port-channel *group*	для настройки групп каналов	все модели
interface oob	для настройки интерфейса управления	RTT-A420-24XG-4QXG, RTT-A330-24F-4XG, RTT-A330-24T-4XG
interface loopback *loopback_id*	для настройки виртуальных интерфейсов	все модели

где:

- *group* – порядковый номер группы, общее количество таблице 9 (строка «Агрегация каналов (LAG));
- *fo_port* – порядковый номер 40G-интерфейса, задается в виде: 1..8/0/1..N;
- *te_port* – порядковый номер 10G-интерфейса, задается в виде: 1..8/0/1..N;
- *gi_port* – порядковый номер 1G-интерфейса, задается в виде: 1..8/0/1..N;
- *loopback_id* – порядковый номер виртуального интерфейса, общее количество таблице 9 (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 RTT-A420-2XGF-4QXG) 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 fortygigabitethernet** *portlist* – для настройки диапазона fortygigabitethernet-интерфейсов;
- **interface range tengigabitethernet** *portlist* – для настройки диапазона tengigabitethernet-интерфейсов;
- **interface range gigabitethernet** *portlist* – для настройки диапазона gigabitethernet-интерфейсов;
- **interface range port-channel** *grouplist* – для настройки диапазона групп портов.

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

Пример команды для входа в режим настройки диапазона интерфейсов с 1 по 10:

```
console# configure
console(config)# interface range tengigabitethernet 1/0/1-10
console(config-if)#
console# configure
console(config)# interface range port-channel 1-8
console(config-if)#
```

Таблица 62 – 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.
no unidirectional		Установить значение по умолчанию.
negotiation *[cap1 [cap2…cap5]]*	cap: (10f, 10h, 100f, 100h, 1000f, 10000f)	Включить 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		Выключить автосогласование для скорости и дуплекса на настраиваемом интерфейсе.
negotiation bypass	—/включено	Выключить пропуск процедуры автосогласования, если партнер на встречной стороне не отвечает.
no negotiation bypass		Включить пропуск процедуры автосогласования, если партнер на встречной стороне не отвечает.
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	Включить функцию «обратного давления» на настраиваемом интерфейсе (Ethernet).
no back-pressure		Выключить функцию «обратного давления» на настраиваемом интерфейсе.
load-average *period*	period: (5..300)/15	Установить период, в течение которого собирается статистика о нагрузке на интерфейсе. **При этом интервал расчёта счётчиков не изменяется.**
no load-average		Установить значение по умолчанию.
media-type {force-fiber | force-copper | prefer-fiber} [auto-failover]	—/prefer-fiber	Выбрать тип комбо-порта в качестве основного носителя. **-force-fiber —** разрешена активность только оптической части комбо-порта; **-force-copper —** разрешена активность только медной части комбо-порта; **-prefer-fiber —** преимущество оптического линка.
no media-type		Установить значение по умолчанию.
mtu *size*	size: (128..1500)/1500 байт	Установить значение maximum transmission unit (MTU) **Настройка MTU не работает для транзитного трафика.** **Настройка применяется после перезагрузки устройства.**
no mtu		Установить значение по умолчанию.
snmp trap link-status	—/включено	Включить отправку SNMP trap-сообщений о состоянии интерфейсных линков.
no snmp trap link-status		Отключить отправку SNMP trap-сообщений.
hardware profile portmode {1x40g | 4x10g}	—/1x40g	Переключить режим портов XLG1-XLG4. **Команда доступна только для портов fortygigabitethernet устройства RTT-A420-24XG-4QXG.** **Настройка применяется после перезагрузки устройства.**
fec *cl74*	—/выключен	Включить режим прямой коррекции ошибок cl74 на настраиваемом интерфейсе (XLG1-XLG4). **Команда доступна только для портов fortygigabitethernet устройства RTT-A420-24XG-4QXG.** **Команда недоступна для стековых линков.**

fec off		Отключить режим прямой коррекции ошибок.
ip tcp adjust-mss *value*	value: (500..1460)/1460 байт	Назначить физическому интерфейсу Ethernet размер TCP Maximum segment size. **Используется при наличии IP address на интерфейсе.**
no ip tcp adjust-mss		Установить значение по умолчанию.

Команды режима глобальной конфигурации

Таблица 63 – Команды режима общих настроек интерфейса Ethernet и Port-Channel

Команда	*Значение/Значение по умолчанию*	*Действие*
port jumbo-frame	—/запрещено	Разрешить коммутатору работать с кадрами 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 10240 байт.**
no port jumbo-frame		Запретить коммутатору работать с кадрами большого размера.
errdisable recovery cause {all | loopack-detection | port-security | dot1x-src-address | acl-deny | stp-bpdu-guard | stp-loopback-guard | unidirectional-link | storm-control | link-flapping | l2pt-guard | pvst | vpc | arp-inspection | dhcp-rate-limit}	—/запрещено link-flapping/разрешено	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 — защита от «шторма» для различного трафика;** **- link-flapping — флаппинг линка;** **- l2pt-guard — превышение количества входящих пакетов функции L2PT;** **- pvst — ошибки протокола PVST;** **- vpc — ошибки протокола VPC;** **- arp-inspection — ошибки контроля протокола ARP;** **- dhcp-rate-limit — превышение количества принятых DHCP-пакетов на порту.**
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*		Установить временной интервал для автоматического повторного включения интерфейса.

no errdisable recovery interval	seconds: (30..86400)/300 секунд	Установить значение по умолчанию.
default interface [range] {gigabitethernet **gi_port** | fastethernet **fa_port** | port-channel **group** | loopback **loopback_id**}	gi_port: (1..8/0/1..28); fa_port: (1..8/0/1..24); group: (1..48); loopback_id: (1..64)	Сбросить настройки интерфейса или группы интерфейсов на значения, установленные по умолчанию.

Команды режима EXEC

Таблица 64 – Команды режима EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
clear counters	—	Сбросить статистику для всех интерфейсов.
clear counters {oob | gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group* **| vlan** *vlan_id***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48) vlan_id: (1..4094)	Сбросить статистику для интерфейса.
set interface active {gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Активировать порт или группу портов, выключенных командой **shutdown**.
show interfaces {gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Показать сводную информацию о состоянии, настройке и статистике порта.
show interfaces configuration {oob | gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group* **| detailed}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Показать конфигурацию интерфейсов.
show interfaces status	—	Показать состояние всех интерфейсов.
show interfaces status {oob | gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group* **| detailed}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Показать состояние Ethernet-порта, группы портов.
show interfaces advertise	—	Показать параметры автосогласования, объявленные для всех интерфейсов.
show interfaces advertise {oob | gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group* **| detailed}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Показать параметры автосогласования, объявленные для Ethernet-порта, группы портов.
show interfaces description	—	Показать описания всех интерфейсов.

show interfaces description {oob | gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group* **| detailed}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Показать описание Ethernet-порта, группы портов.
show interfaces counters	—	Показать статистику для всех интерфейсов.
show interfaces counters {oob | gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group* **| vlan** *vlan_id* **| detailed}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48) vlan_id: (1..4094)	Показать статистику для интерфейса.
show interfaces utilization	—	Показать статистику по нагрузке для всех интерфейсов.
show interfaces utilization {gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Показать статистику по нагрузке для Ethernet-интерфейса.
show interfaces mtu {gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group* **| vlan** *vlan_id* **| loopback** *loopback_id***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); loopback-id: (1..64); vlan_id: (1..4094)	Показать настройку MTU для интерфейса.
show ports jumbo-frame	—	Показать настройку jumbo-frames в коммутаторе.
show errdisable recovery	—	Показать настройки для автоматической повторной активации порта.
show errdisable interfaces {gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Показать причину отключения порта, группы портов и состояние автоматической активации.
show hardware profile portmode	—	Показать режим портов XLG1-XLG4. **Команда доступна только для RTT-A420-24XG-4QXG.**

Примеры выполнения команд.

- Показать состояние интерфейсов:

```
console# show interfaces status
```

```
                                                Flow Link          Uptime       Back    Mdix
Port     Type         Duplex  Speed Neg      ctrl State       (d,h:m:s)    Pressure Mode    Port
Mode
-------- ------------ ------  ----- -------- ---- ----------- ------------- -------- ------- --------
----------------
gi1/0/1  1G-Copper      --      --     --     --  Down             --          --      --     Access
gi1/0/2  1G-Copper      --      --     --     --  Down             --          --      --     Access
gi1/0/3  1G-Copper      --      --     --     --  Down             --          --      --     Access
gi1/0/4  1G-Copper      --      --     --     --  Down             --          --      --     Access
gi1/0/5  1G-Copper      --      --     --     --  Down             --          --      --     Access
gi1/0/6  1G-Copper      --      --     --     --  Down             --          --      --     Access
gi1/0/7  1G-Copper      --      --     --     --  Down             --          --      --     Access
gi1/0/8  1G-Copper      --      --     --     --  Down             --          --      --     Access
gi1/0/9  1G-Copper      --      --     --     --  Down             --          --      --     Access
```

```
gi1/0/10 1G-Copper      --      --     --     --  Down            --          --     --     Access
gi1/0/11 1G-Copper      --      --     --     --  Down            --          --     --     Access
gi1/0/12 1G-Copper      --      --     --     --  Down            --          --     --     Access
gi1/0/13 1G-Copper      --      --     --     --  Down            --          --     --     Access
gi1/0/14 1G-Copper      --      --     --     --  Down            --          --     --     Access
gi1/0/15 1G-Copper      --      --     --     --  Down            --          --     --     Access
gi1/0/16 1G-Copper      --      --     --     --  Down            --          --     --     Access
gi1/0/17 1G-Copper      --      --     --     --  Down            --          --     --     Access
gi1/0/18 1G-Copper      --      --     --     --  Down            --          --     --     Access
gi1/0/19 1G-Copper      --      --     --     --  Down            --          --     --     Access
gi1/0/20 1G-Copper      --      --     --     --  Down            --          --     --     Access
gi1/0/21 1G-Copper      --      --     --     --  Down            --          --     --     Access
gi1/0/22 1G-Copper      --      --     --     --  Down            --          --     --     Access
gi1/0/23 1G-Copper      --      --     --     --  Down            --          --     --     Access
gi1/0/24 1G-Copper      --      --     --     --  Down            --          --     --     Access
te1/0/1  10G-Fiber    Full   10000 Disabled Off  Up       00,04:37:36   Disabled Off     Trunk
te1/0/2  10G-Fiber    Full   10000 Disabled Off  Up       00,04:37:10   Disabled Off     Trunk
te1/0/3  10G-Fiber      --      --     --     --  Down            --          --     --     Access
te1/0/4  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
```

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

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

```
tengigabitethernet1/0/1 is down (not connected)
  Interface index is 1
  Hardware is tengigabitethernet, MAC address is a8:f9:4b:fd:00:41
  Description: RTT-A230-24T-4XG te 0/0/1
  Interface MTU is 9000
  Link is down for 0 days, 0 hours, 3 minutes and 28 seconds
  Flow control is off, MDIX mode is off
  15 second input rate is 0 Kbit/s
  15 second output rate is 0 Kbit/s
      0 packets input, 0 bytes received
      0 broadcasts, 0 multicasts
      0 input errors, 0 FCS, 0 alignment
      0 oversize, 0 internal MAC
      0 pause frames received
      0 packets output, 0 bytes sent
      0 broadcasts, 0 multicasts
      0 output errors, 0 collisions
      0 excessive collisions, 0 late collisions
      0 pause frames transmitted
      0 symbol errors, 0 carrier, 0 SQE test error
  Output queues: (queue #: packets passed/packets dropped)
      1: 0/0
      2: 0/0
      3: 0/0
      4: 0/0
      5: 0/0
      6: 0/0
      7: 0/0
```

```
      8: 0/0
```

- Показать параметры автосогласования:

```
console# show interfaces advertise
```

```
Port      Type          Neg      Preferred   Operational Link Advertisement
--------- ------------ -------- ----------  ----------------------------------
te1/0/1   10G-Fiber     Disabled   --                          --
te1/0/2   10G-Fiber     Disabled   --                          --
te1/0/3   10G-Fiber     Disabled   --                          --
te1/0/4   10G-Fiber     Disabled   --                          --

fo1/0/3   40G-Fiber     Disabled   --                          --
fo1/0/4   40G-Fiber     Disabled   --                          --
gi1/0/1   1G-Copper     Enabled  Slave                         --

Po1            --       Enabled  Slave                         --
Po2            --       Enabled  Slave                         --
Po8            --       Enabled  Slave                         --

Oob       Type          Neg      Operational Link Advertisement
--------- ------------ -------- ---------------------------------
oob       1G-Copper     Enabled  1000f, 100f, 100h, 10f, 10h
```

- 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 65 – 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 кадров с нарушенной целостностью (с количеством байт не соответствующим длине) и не прошедших проверку контрольной суммы (FCS).
FCS Errors	Количество принятых кадров с количеством байт, соответствующим длине, но не прошедших проверку контрольной суммы (FCS).
Single Collision Frames	Количество кадров, вовлеченных в единичную коллизию, но впоследствии переданных успешно.
Multiple Collision Frames	Количество кадров, вовлеченных более чем в одну коллизию, но впоследствии переданных успешно.
Deferred Transmissions	Количество кадров, 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 кадров, 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 кадра.
Oversize Packets	Количество принятых пакетов, размер которых превышает максимальный разрешенный размер кадра.
Internal MAC Rx Errors	Количество кадров, которые не были приняты успешно из-за внутренней ошибки приема на уровне MAC.
Symbol Errors	Для интерфейса, работающего в режиме 100 Мбит/с — количество случаев, когда имелся недопустимый символ данных, в то время как правильная несущая была представлена. Для интерфейса, работающего в полудуплексном режиме 1000 Мбит/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 1000 Мбит/с — количество случаев, когда средства приема заняты в течение времени, равному или большему чем минимальный размер кадра (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-кадров с кодом операции PAUSE.
Transmitted Pause Frames	Количество переданных управляющих MAC-кадров с кодом операции PAUSE.

5.10.2. Настройка VLAN и режимов коммутации интерфейсов

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 66 – 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.
vlan mode {basic | tr101}	—/basic	Включить возможность добавления на физическом интерфейсе в режиме customer сразу двух идентификаторов VLAN.

vlan statistics ingress {low | high}	—/выключено	Включить сбор статистики для диапазонов VLAN: - **low** — VLAN 1-2047; - **high** — VLAN 2048-4094.
no vlan statistics ingress {low | high}		Выключить сбор статистики для указанного диапазона.
vlan tr101 map inner-vlan *c_vlan_id* **interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	c_vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Снять на физическом интерфейсе сразу 2 идентификатора VLAN (в режиме customer), базируюсь как на s_vlan_id, так и на c_vlan_id. При этом действие выполняется только для трафика, идущего с интерфейса, указанного в данной настройке. - **c_vlan_id** — идентификационный номер внутренней VLAN. - **interface** — список интерфейсов, к входящему трафику которых возможно применение данного правила. Диапазон номеров интерфейсов можно задать перечислением через запятую или указать начальное и конечное значения диапазона через дефис. **Для работы данной команды необходима настройка режима «vlan mode tr101».**
no vlan tr101 map inner-vlan *c_vlan_id* **interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**		Удалить правило.

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 67 – 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.

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 68 – Команды режима конфигурации интерфейса VLAN

Команда	***Значение/Значение по умолчанию***	***Действие***
name *name*	name: (1..32) символов/имя соответствует номеру VLAN	Добавить имя VLAN.
no name		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 {fortygigabitethernet fo_port |
tengigabitethernet te_port | gigabitethernet gi_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 69 – 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 access acceptable-frame-type {untagged-only | all}	—/принимать все типы кадров	Принимать на интерфейсе только кадры определенного типа: - **untagged-only** — только нетегированные; - **all** — все кадры.
no switchport access acceptable-frame-type		Принимать на интерфейсе все типы кадров.
switchport trunk allowed vlan all	—/выключено	Автоматически добавить все доступные VLAN для данного интерфейса.
no switchport trunk allowed vlan all		Отключить автоматическое добавление VLAN.
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	Добавить 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 кадров	Принимать на интерфейсе только кадры определенного типа: - **tagged-only** — только тегированные; - **untagged-only** — только нетегированные; - **all** — все кадры.
no switchport general acceptable-frame-type		Принимать на интерфейсе все типы кадров.
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 dot1q ethertype egress stag *ethertype*	ethertype: **(**1..ffff) (hex)/8100	Заменить TPID (Tag Protocol ID) в 802.1q VLAN-тегах пакетов, исходящих с данного интерфейса. **Допустимые значения Ethertype представлены в Приложение В. Поддерживаемые значения Ethertype.**
no switchport dot1q ethertype egress stag		Заменить *ethertype* исходящего с интерфейса пакета на значение по умолчанию.
switchport dot1q ethertype ingress stag add *ethertype*	ethertype: (1..ffff) (hex)	Добавить TPID в таблицу классификаторов VLAN. Допустимые значения EtherType см. Приложение В. Поддерживаемые значения Ethertype.
switchport dot1q ethertype ingress stag remove *ethertype*		Удалить TPID из таблицы классификаторов VLAN.
switchport customer vlan *vlan_id*	vlan_id: (1..4094)/1	Добавить VLAN для пользовательского интерфейса. - *vlan_id* — идентификационный номер VLAN.

switchport customer vlan *vlan_id* **inner-vlan** *vlan_id*		Добавить к входящим нетегированным пакетам на клиентском порту внутренний 802.1q заголовок — C-VLAN (inner-vlan) и внешний 802.1q заголовок, содержащий pvid дополнительной VLAN (S-VLAN). **Для работы этой команды необходимо включить глобально режим «vlan mode tr101».**
no switchport customer vlan		Установить значение по умолчанию.
switchport customer multicast-tv vlan add *vlan_list*	vlan_list: (2..4094, all)	Разрешить 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*		Запретить принимать многоадресный трафик на настраиваемом интерфейсе.
switchport forbidden vlan add *vlan_list*	vlan_list: (2..4094, all)/все VLAN разрешены порту	Запретить добавление указанных VLAN порту. - *vlan_list* — список VLAN ID. Диапазон VLAN можно задать перечислением через запятую или указать начальное и конечное значения диапазона через дефис "-".
switchport forbidden vlan remove *vlan_list*		Разрешить добавление указанных VLAN порту.
switchport forbidden default-vlan	По умолчанию членство в default VLAN разрешено	Запретить добавление default VLAN порту.
no switchport forbidden default-vlan		Установить значение по умолчанию.
switchport protected-port	—	Перевести порт в режим изоляции внутри группы портов.
no switchport protected-port		Восстановить значение по умолчанию.
switchport protected-port isolate-group {*group***}**	group (1..8)	Перевести порт в указанную группу изоляции портов.
no switchport protected-port isolate-group {*group***}**		Удалить порт из указанной группы изоляции портов.
switchport protected {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48) По умолчанию используется маршрутизация по базе данных изученных MAC-адресов (FDB)	Перевести порт в режим Private VLAN Edge. Отменяет маршрутизацию по базе данных изученных MAC-адресов (FDB) и направляет весь одноадресный, многоадресный и широковещательный трафик на uplink-порт.
no switchport protected		Отключить отмену маршрутизации по базе данных изученных MAC-адресов (FDB).
switchport default-vlan tagged	—	Установить порт как тегирующий в дефолтной VLAN.
no switchport default-vlan tagged		Установить значение по умолчанию.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 70 – 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.
show default-vlan-membership [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Показать состав группы дефолтной VLAN.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 71 – 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 {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Показать конфигурацию порта, группы портов.
show interfaces protected-ports [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	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                             te1/0/1-24,              D
                                           fo1/0/1-4,gi1/0/1,
                                           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 0/1:

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

```
Added by: D-Default, S-Static, G-GVRP, R-Radius Assigned VLAN, T-Guest VLAN, V-Voice
VLAN
Port : te1/0/1
Port Mode: Trunk
Gvrp Status: disabled
Ingress Filtering: true
Acceptable Frame Type: admitAll
Ingress UnTagged VLAN ( NATIVE ): 1
Protected: Disabled

Port is member in:

Vlan               Name               Egress rule     Added by
---- -------------------------------- ----------- ----------------
 1                  1                  Untagged          D
 2                  2                    Tagged          S
 3                  3                    Tagged          S
 4                  4                    Tagged          S
 5                  5                    Tagged          S
 6                  6                    Tagged          S
 8                  8                    Tagged          S
 28                 28                   Tagged          S


Forbidden VLANS:
Vlan               Name
---- --------------------------------
Classification rules:

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

Mac based VLANs:
  Group ID   Vlan ID
------------ -------
```

5.10.3. 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 ниже.

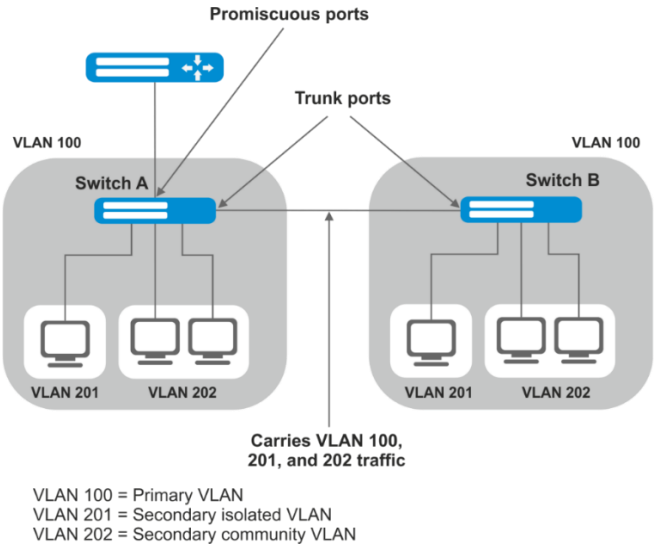


Рис. 33 – Пример работы технологии Private VLAN

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

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

Таблица 72 – 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 mode private-vlan trunk {promiscuous | secondary}	—	Задать режим работы порта в VLAN Trunk.
no switchport mode private-vlan trunk		Установить значение по умолчанию.
switchport private-vlan mapping [trunk] *primary_vlan* **add** *secondary_vlan*	primary_vlan: (1..4094); secondary_vlan: (1..4094)	Добавить основную и второстепенные VLAN на promiscuous интерфейс. **На один promiscuous-интерфейс нельзя добавить больше одной primary vlan.**
switchport private-vlan mapping [trunk] *primary_vlan* **remove** *secondary_vlan*		Удалить второстепенные VLAN на promiscuous интерфейс.
no switchport private-vlan mapping		Удалить основную и второстепенные VLAN.
switchport private-vlan hostassociation *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.
switchport private-vlan association trunk *primary_vlan secondary_vlan*	primary_vlan: (1..4094) secondary_vlan: (1..4094)	Добавить primary и secondary vlan на trunk-secondary интерфейс. **На один trunk-secondary интерфейс нельзя добавить больше одной secondary vlan.**
no switchport private-vlan association trunk		Удалить основную и второстепенные VLAN.
switchport private-vlan trunk allowed vlan add *vlan*	vlan: (1..4094)	Добавить на PVLAN Trunk-интерфейс VLAN, не учавствующую в PVLAN.
switchport private-vlan trunk allowed vlan remove *vlan*		Удалить на PVLAN Trunk-интерфейс VLAN, не учавствующую в PVLAN.
switchport private-vlan trunk native vlan *vlan*	vlan: (1..4094) / 1	Добавить номер VLAN, не учавствующую в PVLAN, в качестве Default VLAN для PVLAN Trunk-интерфейса.
no switchport private-vlan trunk native vlan		Установить значение по умолчанию.

Таблица 73 – 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.

Пример настройки интерфейсов коммутатора Switch A:

- promiscuous порт– interface gigabitethernet 1/0/4
- isolated порт- gigabitethernet 1/0/1
- community порт – gigabitethernet 1/0/2, 1/0/3.

```
interface gigabitethernet 1/0/1
 switchport mode private-vlan host
 description Isolate
 switchport forbidden default-vlan
 switchport private-vlan host-association 100 201
exit
!
interface gigabitethernet 1/0/2
 switchport mode private-vlan host
 description Community-1
 switchport forbidden default-vlan
 switchport private-vlan host-association 100 202
exit
!
interface gigabitethernet 1/0/3
 switchport mode private-vlan host
 description Community-2
 switchport forbidden default-vlan
 switchport private-vlan host-association 100 202
exit
!
interface gigabitethernet 1/0/4
 switchport mode private-vlan promiscuous
 description to_Router
 switchport forbidden default-vlan
 switchport private-vlan mapping 100 add 201-202
exit
!
interface tengigabitethernet 1/0/1
 switchport mode trunk
 switchport trunk allowed vlan add 100,201-202
 description trunk-sw1-sw2
 switchport forbidden default-vlan
exit
!
interface vlan 100
 name primary
```

```
 private-vlan primary
 private-vlan association add 201-202
exit
!
interface vlan 201
 name isolate
 private-vlan isolated
exit
!
interface vlan 202
 name community
```

Пример настройки интерфейсов при работе технологии Private VLAN Trunk

- trunk-isolated порт— gigabitethernet 1/0/1
- trunk-community порт — gigabitethernet 1/0/2, 1/0/3
- trunk-promiscous порт – interface gigabitethernet 1/0/4

```
interface gigabitethernet 1/0/1
 switchport mode private-vlan trunk secondary
 description Trunk-Isolated
 switchport private-vlan trunk allowed vlan add 301
 switchport private-vlan association trunk 100 201
exit
!
interface gigabitethernet 1/0/2
 switchport mode private-vlan trunk secondary
 description Trunk-Community
 switchport private-vlan trunk allowed vlan add 301
 switchport private-vlan association trunk 100 202
exit
!
interface gigabitethernet 1/0/3
 switchport mode private-vlan trunk secondary
 description Trunk-Community
 switchport private-vlan trunk allowed vlan add 301
 switchport private-vlan trunk native vlan 302
 switchport private-vlan association trunk 100 202
exit
!
interface gigabitethernet 1/0/4
 switchport mode private-vlan trunk promiscuous
 description Trunk-Promiscuous
 switchport private-vlan trunk allowed vlan add 301
 switchport private-vlan mapping trunk 100 add 201-202
exit
!
interface tengigabitethernet 1/0/1
 switchport mode trunk
 switchport trunk allowed vlan add 100,201-202
 description trunk-sw1-sw2
 switchport forbidden default-vlan
exit
!
interface vlan 100
 name primary
 private-vlan primary
 private-vlan association add 201-202
exit
!
interface vlan 201
 name isolate
 private-vlan isolated
exit
```

```
!
interface vlan 202
 name community
 private-vlan community
```

5.10.4. Настройка интерфейса IP

IP-интерфейс создаётся при назначении IP-адреса на любой из интерфейсов устройства gigabitethernet, tengigabitethernet, fortygigabitethernet, 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 74 – 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.
ip irdp	—/включено	Разрешает рассылку анонсов протокола IRDP (ICMP Router Discovery Protocol).
no ip rdp		Отключает рассылку анонсов.

Примеры выполнения команд

- Включить функцию directed-broadcast:

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

5.11. Selective Q-in-Q

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

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

Правила Selective Q-in-Q используют аппаратные ресурсы TCAM. Суммарный объем правил для сервисов Selective Q-in-Q, Security Suite, DHCP Snooping, ARP Inspection, IP Source Guard, Port ACL, VLAN ACL. Policy Based VLAN (MAC, Subnet, Protocol), Rate Limit per VLAN, PPPoE IA, VPC, L2PT, PIM Snooping равен размеру TCAM определенного устройства (за вычетом 66 правил по умолчанию). Максимальное количество SQinQ-правил для одиночного устройства приведено в таблице 9.

Если устройства объединены в стек, то сервисы DHCP Snooping, VLAN ACL, Security Suite, ARP Inspection, Rate Limit per VLAN, PPPoE IA, L2PT, PIM Snooping используют TCAM всех unit-ов стека, а сервисы Selective Q-in-Q, Port ACL, IP Source Guard, Policy Based VLAN (MAC, Subnet, Protocol), VPC используют TCAM определенного unit-а. Максимальное суммарное количество SQinQ-правил стека коммутатора RTT-A430-48XG-4QXG — 11600 правил. Максимальное суммарное количество SQinQ-правил стека коммутаторов серии RTT-A330 — 11136 правил. Максимальное суммарное количество SQinQ-правил стека коммутаторов серии RTT-A230 — 3456 правил.

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

Вид запроса командной строки режима конфигурации интерфейса конфигурации:

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

Таблица 75 – 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)	Создать 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)	Создать 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)	Создать 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)	Создать 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)	Удалтьб 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)	Создать 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)	Удалить список правил selective qinq для исходящих пакетов.

Команды режима конфигурации интерфейса VLAN

Вид запроса командной строки в режиме конфигурации интерфейса VLAN:

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

Таблица 76 — Команды режима конфигурации интерфейса Vlan

Команда	***Значение/Значение по умолчанию***	***Действие***
ip management outer-vlan *outer_vlan_id*	outer_vlan_id: (1-4094)	Создать правило для управления коммутатором с помощью Q-in-Q трафика. **В качестве outer_vlan_id используется внешний VLAN (S-VLAN). Для работы данного правила интерфейс Vlan (C-VLAN) должен быть в состоянии Up.**
no ip management		Удаляет данное правило.

Команды режима EXEC

Таблица 77 – Команды режима EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show selective-qinq	—	Отображает список правил selective qinq.
show selective-qinq interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Отображает список правил selective qinq для указанного порта.
show ip management [vlan *vlan_id***]**	vlan_id: (1-4094)	Отображает список правил для управления коммутатором с помощью Q-in-Q трафика.

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
```

- Отобразить список созданных правил selective qinq:

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

Direction	Interface	Rule type	Vlan ID	Classification	by Parameter
ingress	te0/1	override_vlan	10	ingress_vlan	11

5.12. Storm Control для различного трафика (broadcast, multicast, unknown, unicast)

«Шторм» возникает вследствие чрезмерного количества broadcast-, multicast-, unknown unicast-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 78 – 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 multicast [registered | unregistered] {pps *pps***} [trap] [shutdown]**	pps: (125.. 19531250)	Включает контроль многоадресного трафика: - **registered** — зарегистрированного; - **unregistered** — незарегистрированного. - *pps* — количество пакетов в секунду. 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 unicast { pps *pps***} [trap] [shutdown]**	pps: (125.. 19531250)	Включает контроль неизвестного одноадресного трафика. - *pps* — количество пакетов в секунду. 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.
storm-control broadcast {pps *pps***} [trap] [shutdown]**	pps: (125.. 19531250)	Включает контроль широковещательного трафика. - *pps* — количество пакетов в секунду. 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

Таблица 79 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show storm-control interface [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Показывает конфигурацию функции контроля «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 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
```

5.13. Группы агрегации каналов – Link Aggregation Group (LAG)

Коммутаторы обеспечивают поддержку групп агрегации каналов LAG в количестве, указанном в разделе «Основные технические характеристики» (Таблица 9) в строке «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.

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

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

Таблица 80 – Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
channel-group *group* **mode** *mode*	group: (1..48); 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 конфигурации интерфейса Port-Channel

Вид запроса командной строки в режиме конфигурации интерфейса Port-Channel:

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

Таблица 81 — Команды режима конфигурации интерфейса Port-Channel

Команда	*Значение/Значение по умолчанию*	*Действие*
lacp min-links *min-links*	min-links: (1..8)/1	Задать минимальное число активных линков в составе Port-Channel, при котором он переходит в состояние Up. **Настройка возможна только при работе Port-Channel в режиме LACP.**
no lacp min-links *min-links*		Установить значение по умолчанию.
lacp max-bundle max-bundle	max-bundle: (1..8)/8	Задать максимальное число активных линков в составе Port-Channel, остальные линки Port-Channel будут переведены в состояние inactive. **Активные порты выбираются по значению lacp приоритета порта или, при равнозначности приоритета — по номеру порта.** **Настройка возможна только при работе Port-Channel в режиме LACP.**
no lacp max-bundle		Установить значение по умолчанию.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

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

Таблица 82 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
port-channel load-balance {src-dst-mac-ip | src-dst-mac | src-dst-ip | src-dst-mac-ip-port | dst-mac | dst-ip | src-mac | src-ip} [mpls-aware]	—/src-dst-mac-ip	Задать механизм балансировки нагрузки для стратегии ECMP и для группы агрегированных портов. - **src-dst-mac-ip —** механизм балансировки основывается на MAC-адресе и IP-адресе; - **src-dst-mac —** механизм балансировки основывается на MAC-адресе; - **src-dst-ip —** механизм балансировки основывается на IP-адресе; - **src-dst-mac-ip-port —** механизм балансировки основывается на MAC-адресе, IP-адресе и TCP-порте назначения; - **dst-mac** — механизм балансировки основывается на MAC-адресе получателя; - **dst-ip** — механизм балансировки основывается на IP-адресе получателя. - **mpls-aware** — включение парсинга L3/L4-заголовков пакетов с MPLS-метками для всего устройства. Актуально только с режимами балансировки по L3/L4-заголовкам пакета.
no port-channel load-balance		Возврат к настройкам балансировки нагрузки по умолчанию.

Команды режима EXEC

Таблица 83 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show interfaces port –channel [*group*]	group: (1..48)	Показывает информацию по группе каналов.

5.13.1. 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.

5.13.2. 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 84 – 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 85 – Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
lacp timeout {long | short}	По умолчанию используется значение long	Установить административный таймаут протокола LACP: - **long** — длительное время таймаута; - **short** — малое время таймаута.
no lacp timeout		Установить значение по умолчанию.
lacp port-priority *value*	value: (1..65535)/1	Установить приоритет интерфейса Ethernet.
no lacp port-priority		Установить значение по умолчанию.
lacp force-up	—/выключено	Принудительно добавить интерфейс в LACP, вне зависимости от наличия lacp pdu с ответной стороны.
no lacp force-up		Отменить принудительное добавление интерфейса в LACP.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 86 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show lacp {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port*} **[parameters | statistics | protocol-state]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4);	Показывает информацию о протоколе LACP для интерфейса Ethernet. Если дополнительные параметры не используются, то будет показана вся информация. - **parameters** – показывает параметры настройки протокола; - **statistics** – показывает статистику работы протокола; - **protocol-state** – показывает состояние работы протокола.
show lacp port-channel [*group***]**	group: (1..48)	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
```

5.13.3. Настройка технологии Multi-Switch Link Aggregation Group (MLAG)

Как и LAG, виртуальные LAG позволяют объединить одну или несколько Ethernet-линий для увеличения скорости и обеспечения отказоустойчивости. MLAG так же известна как VPC (Virtual port-channel). При обычном LAG агрегированные линии должны быть на одном физическом устройстве, в случае же с VPC агрегированные линии находятся на разных физических устройствах. Функция VPC позволяет соединить два физических устройства в одно виртуальное.

При настройке VPC на одноранговых коммутаторах должна быть одинаковая версия программного обеспечения.

VPC Port-Channel контролируются только коммутатором с ролью Primary, коммутатор Secondary использует настройки Primary;

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 87 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
vpc domain *domain_id*	domain_id: (1..255)	Создает VPC-домен. **На одном устройстве может быть создан только один домен VPC. На парных устройствах должен быть одинаковый VPC-домен.**
no vpc domain *domain_id*		Удаляет VPC-домен с устройства.
vpc group *group_id*	group_id: (1..63)	Создает VPC-группу. Для каждого агрегированного интерфейса должна быть создана отдельная VPC-группа. На парных устройствах номера VPC-групп должны совпадать. **Суммарное количество VPC-групп не может превысить 48.**
no vpc group *group_id*		Удаляет VPC-группу с устройства.
vpc	—/выключено	Включает режим VPC. Используется после конфигурации VPC.
no vpc		Выключает режим VPC.

Команды режима конфигурации VPC

Вид запроса командной строки режима конфигурации VPC:

```
console(config)# vpc domain domain_id
console(config-vpcdomain)#
```

Таблица 88 – Команды режима конфигурации VPC

Команда	*Значение/Значение по умолчанию*	*Действие*
peer link *group*	group: (1..48)	Назначает Port-Channel в качестве peer-link.
no peer link		Исключает Port-Channel из участия в VPC.
peer detection	—/выключено	Включает peer detection protocol. **Peer-detection — дополнительный механизм, обеспечивающий функционирование VPC в случае обрыва peer-link. Поэтому запрещается использование peer-link для организации интерфейса peer-detection.**
no peer detection		Выключает peer detection protocol.
peer detection interval *msec*	msec: (200..4000)/700 ms	Задает интервал отправки сообщений peer detection protocol.
no peer detection interval		Устанавливает значение по умолчанию.

peer detection timeout *msec*	msec: (700..14000)/3500ms	Задать время ожидания ответа peer detection protocol.
no peer detection timeout		Устанавливает значение по умолчанию.
peer detection ipaddr *dest_ipaddress source_ipaddress* **[port** *udp_port***]**	udp_port: (1..65535)/50000	Настраивает IP-адрес получателя пакетов, IP-адрес отправителя и UDP порт для peer detection protocol
no peer detection ipaddr		Устанавливает значение по умолчанию
peer keepalive	—	Включает службу keepalive
no peer keepalive		Выключает службу keepalive
peer keepalive timeout *sec*	sec: (2..15)/5	Задать время ожидания ответа на запрос целостности peer-link
no peer keepalive timeout		Устанавливает значение по умолчанию
role priority *value*	value: (1..255)/100	Устанавливает приоритет устройства. Устройство с меньшим значением будет назначено Primary.
no role priority		Устанавливает значение по умолчанию
system mac-addr *mac_address*	—	Устанавливает MAC-адрес системы для отправки в VPC порты.
no system mac-addr		Устанавливает значение по умолчанию
system priority *value*	value: (1..65535)/32767	Устанавливает приоритет системы для отправки в VPC порты. Должен быть одинаковый на обоих устройствах.
no system		Устанавливает значение по умолчанию

Команды режима конфигурации VPC

Вид запроса командной строки режима конфигурации VPC-group:

```
console(config)# vpc group group-id
console(config-group)#
```

Таблица 89 – Команды режима конфигурации VPC

Команда	***Значение/Значение по умолчанию***	***Действие***
domain *domain_id*	domain_id: (1..255)	Устанавливает VPC-group членом VPC-домена.
no domain *domain_id*		Исключает VPC-group из VPC-домена.
vpc-port *group*	group: (1..48)	Добавляет Port-Channel в VPC-группу.
no vpc-port *group*		Исключает Port-Channel из VPC-группы

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 90 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show vpc	-	Отображает информацию о кофигурации VPC
show vpc group *id*	-	Отображает информацию о текущем состоянии VPC Group id
show vpc peer-detection	-	Отображает состояние службы peer detection protocol)
show vpc role	-	Отображает информацию о роли устройства
show vpc statistics peer { *keepalive* | *link* | *detection* **}**	-	Отображает состояние счетчиков службы VPC

5.14. 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 91 – 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.
ip unnumbered [vlan *vlan_id* **| loopback** *loopback_id***]**	vlan_id: (1..4094); loopback_id: (1..64)	Разрешает конфигурируемому интерфейсу заимствовать IP-адреса VLAN и Loopback-интерфейса.
no ip unnumbered		Отключает функцию заимствования адреса.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 92 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip default-gateway *ip_address*	—/шлюз по умолчанию не задан	Задать для коммутатора адрес шлюза по умолчанию.
no ip default-gateway		Удалить назначенный адрес шлюза по умолчанию.
ip helper-address {*ip_interface* **| all**} *ip_address* [*udp_port_list*]	—/выключено	Включить 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*		Отменить переадресацию на заданных интерфейсах.

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 93 – Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
clear host {* | *word*}	word: (1..158) символов	Удалить из памяти полученные по протоколу DHCP записи соответствий имен интерфейсов и их IP-адресов. * — удалить все соответствия.
renew dhcp {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| vlan** *vlan_id* **| port-channel** *group* **| oob} [force-autoconfig]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48) vlan_id: (1..4094)	Отправить запрос к DHCP-серверу на обновление IP-адреса. - **force-autoconfig** — при обновлении IP-адреса загружается конфигурация с TFTP-сервера.
show ip helper-address	—	Отобразить таблицу переадресации широковещательных UDP-пакетов.

Команды режима EXEC

Вид запроса командной строки в режиме Exec:

```
console>
```

Таблица 94 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip interface [vrf {*vrf-name* **| all} | gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan_id* **| oob]**	vrf-name: (1..32) символа; gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); loopback_id : (1…64) vlan_id: (1..4094)	Показать конфигурацию IP-адресации для указанного интерфейса или области виртуальной маршрутизации (vrf).

5.15. 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 95 – 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 96 – 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 97 – Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show green-ethernet [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4);	Отображает статистику green-ethernet.
green-ethernet power-meter reset	-	Сбрасывает счетчик измерителя мощности.

Примеры выполнения команд

- Отобразить статистику green-ethernet:

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

```
Energy-Detect mode: Disabled
Short-Reach mode: Disabled
Power Savings: 82% (0.07W out of maximum 0.40W)
Cumulative Energy Saved: 0 [Watt*Hour]
Short-Reach cable length threshold: 50m

Port        Energy-Detect           Short-Reach           VCT Cable
          Admin Oper Reason    Admin Force Oper Reason     Length
--------  ----- ---- -------   ----- ----- ---- -------   ----------
te1/0/1     on   off            on    off  off
te1/0/2     on   off            on    off  off
te1/0/3     on   off            on    off  off
te1/0/4     on   off            on    off  off
te1/0/5     on   off            on    off  off
te1/0/6     on   off            on    off  off
```

5.16. Настройка IPv6-адресации

5.16.1. 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 = **gigabitethernet** (1..8/0/1..48) | **tengigabitethernet** (1..8/0/1..24) **|** **fortygigabitethernet** (1..8/0/1..4)

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

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 98 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ipv6 default-gateway *ipv6_address*		Задать значение локального адреса IPv6-шлюза по умолчанию.
no ipv6 default-gateway *ipv6_address*		Удалить настройки IPv6-шлюза по умолчанию.

ipv6 neighbor *ipv6_address* **{gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id***}** *mac_address*	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Создать статическое соответствие между MAC-адресом соседнего устройства и его IPv6-адресом. - *ipv6_address* — IPv6-адрес; - *mac_address* — MAC-адрес.
no ipv6 neighbor [_ipv6_address_**] [gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id***]**		Удалить 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	Задать ограничение скорости для ICMPv6-сообщений об ошибках.
no ipv6 icmp error-interval		Установить значение по умолчанию.
ipv6 route *prefix***/***prefix_length* **{**_gateway_**}** **[**_metric_**]** **[distance** *distance***]**	prefix: X:X:X:X::X; prefix_length: (0..128); metric: (1..65535)/1; distance (1..255)/1	Добавить статический маршрут IPv6. - *prefix* — сеть назначения; - *prefix_length* — префикс маски сети (количество единиц в маске); - *gateway* — шлюз для доступа к сети назначения; - *distance* — административная дистанция маршрута.
no ipv6 route *prefix /prefix_length* **[**_gateway_**]**		Удалить статический маршрут IPv6.
ipv6 unicast-routing	—/выключено	Включить перенаправление одноадресных пакетов.
no ipv6 unicast-routing		Отключить перенаправление одноадресных пакетов.
ipv6 distance {ospf {inter-as | intra-as} | static} *distance*	distance (1.255)/static:1, OSPF intra-as:30, OSPF inter-as:110	Установить значение административной дистанции (AD) для всех маршрутов указанного типа. - **ospf inter-as** — установить значение AD для межзональных маршрутов, принятых по протоколу OSPF; - **ospf intra-as** — установить значение AD для внутризональных маршрутов, принятых по протоколу OSPF; - **static** — устанавливает значение AD для статических маршрутов.
no ipv6 distance {ospf {inter-as | intra-as} | static}		Установить значение по умолчанию.

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

Вид запроса командной строки режима конфигурации интерфейса:

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

Таблица 99 – Команды режима конфигурации интерфейса (Ethernet, VLAN, Port-channel)

Команда	***Значение/Значение по умолчанию***	***Действие***
ipv6 enable	—/выключено	Включить поддержку IPv6 на интерфейсе.
no ipv6 enable		Отключить поддержку IPv6 на интерфейсе.

ipv6 address *ipv6_address/prefix_length* **[eui-64] [anycast]**	prefix-length: (0..128) ((0..64) если используется параметр eui-64)	Задать IPv6-адрес на интерфейсе. - *ipv6_address* — IPv6-адрес, назначенный интерфейсу (8 блоков, разделенных двоеточием, в каждом блоке 16 бит, записанных в виде четырех шестнадцатеричных чисел); - *prefix_length* — длина префикса IPv6 — десятичное число — количество старших бит адреса составляющих префикс; - **eui-64** — идентификатор, созданный на базе MAC-адреса интерфейса, записывается в 64 младших бита IPv6-адреса; - **anycast** — указывает, что заданный адрес anycast-адрес.
no ipv6 address [*ipv6_address/prefix_length*] **[eui-64]**		Удалить IPv6-адрес с интерфейса.
ipv6 address autoconfig	По умолчанию автоматическая конфигурация включена, адреса не назначены.	Включить автоматическую конфигурацию IPv6-адресов на интерфейсе. Адреса настраиваются в зависимости от префиксов, которые получены в сообщениях «Router Advertisement».
no ipv6 address autoconfig		Установить значение по умолчанию.
ipv6 address *ipv6_address/prefix_length* **link-local**	По умолчанию значение локального адреса: (FE80::EUI64)	Задать локальный IPv6-адрес интерфейса. Старшие биты локальных IP-адресов в IPv6 — FE80::
no ipv6 address [*ipv6_address/prefix-length* **link-local]**		Удалить локальный IPv6-адрес.
ipv6 nd dad attempts *attempts_number*	(0..600)/1	Задать количество сообщений-требований, передаваемых интерфейсом взаимодействующему устройству в случае обнаружения дубликации (коллизии) IPv6-адреса.
no ipv6 nd dad attempts		Вернуть значение по умолчанию.
ipv6 unreachables	—/enabled	Включить ICMPv6-сообщения о недостижимости адресата при передаче пакетов на определенный интерфейс.
no ipv6 unreachables		Установить значение по умолчанию.
ipv6 mld version *version*	version: (1..2)/2	Определить версию протокола MLD для интерфейса.
no ipv6 mld version		Установить значение по умолчанию.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 100 – Команды режима Privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show ipv6 neighbors {*ipv6_address* | **gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **fortygigabitethernet** *fo_port* | **port-channel** *group* | **vlan** *vlan_id*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Показать информацию о соседних IPv6-устройствах, содержащуюся в кэше.
clear ipv6 neighbors	—	Очистить кэш, содержащий информацию о соседних устройствах, работающих по протоколу IPv6. Информация о статических записях сохраняется.
show ipv6 distance	—	Показать значение административной дистанции для различных источников маршрута.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 101 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ipv6 interface [brief | gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback | vlan** *vlan_id***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Показать настройки протокола IPv6 для указанного интерфейса.
show ipv6 route [summary | local |connected | static | ospf | icmp | nd | *ipv6_address***/***ipv6_prefix* **| interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback | vlan** *vlan_id***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Показать таблицу IPv6-маршрутов.

5.17. Настройка протоколов

5.17.1. 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 102 – 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 dns server	—/выключен	Включает работу DNS-сервера.

no ip dns server		Выключает работу DNS-сервера.
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 … address8*]	name: (1..158) символов	Определяет статические соответствия имен узлов сети IP-адресам, добавляет установленное соответствие в кэш. Функция локального DNS. Можно определить до восьми 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 103 – 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.
show ip dns server	—	Отображает статус DNS-сервера и список доступных серверов.
show ip dns server cache	—	Отображает кэш DNS-сервера.
show ip dns server cache *query_name query_type*	query_name: (1..158) символов: query_type: (1..255, a, ptr, aaaa)	Отображает подробный вывод записи, включающий в себя ответы RR на данный запрос *query_name* и *query_type.*
show ip dns server counters	—	Отображение общего числа запросов и общего числа ответов найденных в cache-hit.
clear ip dns server cache	—	Очистить кэш DNS-сервера.
clear ip dns server counters	—	Обнулить счетчики запросов и ответов.

Примеры использования команд

Использовать DNS-сервера по адресам 192.168.16.35 и 192.168.16.38, установить доменное имя по умолчанию – **rustel" - "console(config)# ip domain name rtt"**

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

Установить статическое соответствие: узел сети с именем rustel имеет IP-адрес 192.168.16.39:

```
console# configure
console(config)# ip host rustel 192.168.16.39
```

5.17.2. 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 104 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
arp *ip_address hw_address* **[gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_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; gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48) vlan_id: (1..4094)	Добавить статическую запись соответствия IP- и MAC-адресов в таблицу ARP для указанного в команде интерфейса. - *ip*_address — IP-адрес; - *hw_address* — MAC-адрес.
no arp *ip_address* **[gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***| port-channel** *group* **| vlan** *vlan_id* **| oob]**		Удалить статическую запись соответствия IP- и MAC-адресов из таблицы ARP для указанного в команде интерфейса.
arp timeout *sec*	sec: (1..40000000)/60000 сек	Настроить время жизни динамических записей в таблице ARP (с).
no arp timeout		Установить значение по умолчанию.
ip arp proxy disable	—/отключён	Отключить режим проксирования ARP-запросов для коммутатора.
no ip arp proxy disable		Включить режим проксирования ARP-запросов для коммутатора.

Команды режима privileged EXEC

Вид запроса командной строки в режиме privileged EXEC:

```
console#
```

Таблица 105 – Команды режима privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
clear arp-cache	—	Удалить все динамические записи из ARP-таблицы (команда доступна только для привилегированного пользователя).
show arp [ip-address *ip_address*] **[mac-address** *mac_address*] **[gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_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; gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Показать 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	—	Показать глобальную конфигурацию ARP и конфигурацию ARP для интерфейсов.

Команды режима конфигурации интерфейса

Вид запроса командной строки в режиме interface configuration:

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

Таблица 106 – Команды режима конфигурации интерфейса Ethernet, группы интерфейсов, интерфейса VLAN

Команда	*Значение/Значение по умолчанию*	*Действие*
ip proxy-arp	—/включено	Включить режим проксирования ARP-запросов на настраиваемом интерфейсе.
no ip proxy-arp		Отключить режим проксирования ARP-запросов на настраиваемом интерфейсе.
ip local-proxy-arp	—/выключено	Включить на интерфейсе функционал Local Proxy ARP (коммутатор будет отвечать на ARP-запросы к хостам, находящимся в том числе на этом же L3-интерфейсе). Для работы данной функции на порту необходимо включить обычный Proxy ARP (**IP proxy-arp**).
no ip local-proxy-arp		Отключить функционал Local Proxy ARP на интерфейсе.

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# 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
```

5.17.3. 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 107 – 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.
gvrp static-vlan	-	Полученные по GVRP vlan будут автоматически добавляться во vlan database.
no gvrp static-vlan		Отключить добавление vlan'ов, полученных по протоколу GVRP во vlan database.

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

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

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

Таблица 108 – 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 конфигурации интерфейса VLAN

Вид запроса командной строки в режиме конфигурации интерфейса VLAN:

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

Таблица 109 – Команды режима конфигурации интерфейса VLAN

Команда	***Значение/Значение по умолчанию***	***Описание***
gvrp advertisement-forbid	-	Запрещает анонсирование VLAN по протоколу GVRP.
no gvrp advertisement-forbid		Отменяет запрет на анонсирование VLAN по протоколу GVRP.

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 110 – Команды режима privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
clear gvrp statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Очищает накопленную статистику протокола GVRP.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 111 – Команды режима EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show gvrp configuration [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Показывает конфигурацию протокола GVRP для указанного интерфейса, либо для всех интерфейсов.

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

5.17.4. 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 112 – 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
loopback-detection mode {src-mac-addr | base-mac-addr | multicast-mac-addr | broadcast-mac-addr}	—/broadcast-mac-addr	Определяет MAC-адрес назначения, указываемый в LBD-фрейме. - **source-mac-addr** — в качестве адреса назначения используется MAC-адрес порта-источника; - **base-mac-addr** — в качестве адреса назначения используется MAC-адрес коммутатора; - **multicast-mac-addr** — в качестве адреса назначения используется групповой адрес; - **broadcast-mac-addr** — в качестве адреса назначения используется широковещательный адрес.
no loopback-detection mode		Восстанавливает значение по умолчанию
loopback-detection vlan- based	—/выключено	Включает режим обнаружения петли во VLAN. При нали- чии петли во VLAN данная VLAN будет заблокирована на порту, на котором была обнаружена петля.
no loopback-detection vlan-based		Отключает режим обнаружения петли во VLAN.
loopback-detection vlan- based recovery-time *value*	value: (30..1000000) /выключено	Задает время блокировки VLAN. - value — время, по истечение которого VLAN автоматиче- ски разблокируется.
no loopback-detection vlan-based recovery-time		Заблокированные VLAN не будут восстанавливаться автоматически.

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

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

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

Таблица 113 – 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 114 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show loopback-detection [gigabitethernet *gi_port* **| tengigabitethernet** te_port **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48).	Отображает состояние механизма loopback-detection.

5.17.5. Семейство протоколов STP (STP, RSTP, MSTP), PVSTP+, RPVSTP+

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.

5.17.5.1. Настройка протокола STP, RSTP

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 115 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
spanning-tree	—/включено	Разрешить использование коммутатором протокола STP.
no spanning-tree		Запретить использование коммутатором протокола STP.
spanning-tree mode {stp | rstp | mstp | pvst | rapid-pvst}	—/RSTP	Установить 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. - **pvst** — Per-Vlan Spanning Tree Protocol. - **rapid-pvst** — Rapid Per-Vlan Spanning Tree Protocol.
no spanning-tree mode		Установить значение по умолчанию.

spanning-tree forward-time *seconds*	seconds: (4..30)/15 сек	Установить интервал времени, затрачиваемый на прослушивание и изучение состояний перед переключением в состояние передачи.
no spanning-tree forward-time		Установить значение по умолчанию.
spanning-tree hello-time *seconds*	seconds: (1..10)/2 сек	Установить интервал времени между передачами широковещательных сообщений «Hello» к взаимодействующим коммутаторам.
no spanning-tree hello-time		Установить значение по умолчанию.
spanning-tree loopback-guard	—/запрещено	Разрешить защиту, выключающую интерфейс при получении своего BPDU.
no spanning-tree loopback-guard		Запретить защиту, выключающую интерфейс при получении своего BPDU.
spanning-tree loopguard default	—/отключено	Включить функцию Loop Guard для всех портов.
no spanning-tree loopguard default		Отключить функцию Loop Guard.
spanning-tree max-age *seconds*	seconds: (6..40)/20 сек	Установить время жизни связующего дерева STP.
no spanning-tree max-age		Установить значение по умолчанию.
spanning-tree priority *prior_val*	prior_val: (0..61440)/32768	Настроить приоритет связующего дерева STP. Значение приоритета должно быть кратно 4096.
no spanning-tree priority		Установить значение по умолчанию.
spanning-tree pathcost method {long | short}	—/long	Установить метод определения ценности пути. - **long** — значение ценности в диапазоне 1..200000000; - **short** — значение ценности в диапазоне 1..65535.
no spanning-tree pathcost method		Установить значение по умолчанию.
spanning-tree bpdu {filtering | flooding}	—/flooding	Определить 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		Установить значение по умолчанию.
spanning-tree process *id*	id: (1..31)/0	Создать отдельный процесс и перевести командный интерфейс в режим его конфигурации. **Внутри процесса применимы вышеуказанные команды:** **spanning-tree forward-time** *seconds;* **spanning-tree hello-time** *seconds;* **spanning-tree max-age** *seconds;* **spanning-tree priority** *prior_val.*
no spanning-tree process *id*		Удалить указанный процесс.
spanning-tree tc-protection		Включить ограничение на количество обрабатываемых TCN/TC BPDU за установленный интервал времени для STP, RSTP, нулевого экземпляра MSTP.
no spanning-tree tc-protection		Выключить ограничение на количество обрабатываемых TCN/TC BPDU.
spanning-tree tc-protection interval *seconds*	seconds: (1..10)/2 сек.	Установить интервал ограничения количества обрабатываемых TCN/TC BPDU.
no spanning-tree tc-protection interval		Установить значение по умолчанию.
spanning-tree tc-protection threshold *count*	count: (1..255)/1	Установить максимальное количество обрабатываемых TCN/TC BPDU за заданный интервал времени.
no spanning-tree tc-protection threshold		Установить 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 116 – Команды режима конфигурации интерфейса Ethernet, группы портов

Команда	*Значение/Значение по умолчанию*	*Действие*
spanning-tree disable	—/разрешено	Запретить работу протокола STP на конфигурируемом интерфейсе.
no spanning-tree disable		Разрешить работу протокола STP на конфигурируемом интерфейсе.
spanning-tree cost *cost*	cost: (1..200000000)/см. таблицу 117	Установить ценность пути через данный интерфейс. - *cost* — ценность пути.
no spanning-tree cost		Установить значение, определяемое на основании скорости порта и метода определения ценности пути, см. таблицу 117.
spanning-tree port-priority *priority*	priority: (0..240)/128	Установить приоритет интерфейса в связующем дереве STP. **Значение приоритета должно быть кратно 16.**
no spanning-tree port-priority		Установить значение по умолчанию.
spanning-tree portfast [auto]	—/auto	Включить 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		Выключить режим моментального перехода в состояние передачи по поднятию «линка».
spanning-tree guard {root | loop | none}	—/использование глобальной настройки	Включить 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	Разрешить защиту, выключающую интерфейс при приёме пакетов BPDU.
no spanning-tree bpduguard		Запретить защиту, выключающую интерфейс при приёме пакетов BPDU.
spanning-tree mac-address {dot1d | dot1ad}	—/dot1d	Изменить MAC-адрес, с которым отправляются и принимаются BPDU. - **dot1d** — отправляются и принимаются BPDU с MAC-адресом 01-80-C2-00-00-00; - **dot1ad** — отправляются и принимаются BPDU с MAC-адресом 01-80-C2-00-00-08.
no spanning-tree mac-address		Установить значение по умолчанию.
spanning-tree link-type {point-to-point | shared}	—/для дуплексного порта — «точка-точка», для полудуплексного — «разветвленный»	Установить протокол RSTP в передающее состояние и определить тип связи для выбранного порта: - **point-to-point —** точка-точка; - **shared —** разветвлённый.
no spanning-tree link-type		Установить значение по умолчанию.

spanning-tree restricted-tcn	—/прием BPDU с флагом TCN разрешен; vlan_list: (1..4094)	Запретить прием BPDU с флагом TCN.
no spanning-tree restricted- tcn		Разрешить прием BPDU с флагом TCN.
spanning-tree bpdu {filtering | flooding}	—	Определить 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		Установить значение по умолчанию.
spanning-tree binding-process *id*	id: (1..31)/0	Привязать порт к указанному процессу. По умолчанию все порты привязаны к нулевому процессу. - *id* — номер процесса.
no spanning-tree binding-process		Восстановить привязку порта по умолчанию.

Таблица 117 – Ценность пути, установленная по умолчанию (spanning-tree cost)

Интерфейс	***Метод определения ценности пути***	
	Long	***Short***
10M	2000000	100
100M	200000	19
1G	20000	4
10G	2000	2
40G	2000000	100
LAG 10M	20000	4
LAG 100M	20000	4
LAG 1G	20000	4
LAG 10G	2000	2
LAG 40G	500	2

Стоимость пути для группы каналов по методу long по умолчанию определяется делением стоимости интерфейса на количество линков в группе. Значение cost для LAG приведено с учётом членства в нём двух физических интерфейсов.

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 118 – Команды режима privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show spanning-tree [**gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group*]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Показать состояние протокола STP.
show spanning-tree detail [active | blockedports]	—	Показать подробную информацию о настройках протокола STP, информацию об активных или заблокированных портах.

clear spanning-tree detected-protocols [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48).	Перезапустить процесс миграции протокола. Заново происходит пересчёт дерева STP.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 119 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show spanning-tree bpdu [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48);	Показать режим обработки пакетов BPDU на интерфейсах.

5.17.5.2. Настройка протокола MSTP

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 120 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
spanning-tree	—/разрешено	Разрешить использование коммутатором протокола STP.
no spanning-tree		Запретить использование коммутатором протокола STP.
spanning-tree mode {stp | rstp | mstp | pvst | rapid-pvst}	—/RSTP	Установить режим работы протокола STP.
no spanning-tree mode		Установить значение по умолчанию.
spanning-tree pathcost method {long | short}	—/long	Установить метод определения ценности пути. - **long** — значение ценности в диапазоне 1..200000000; - **short** — значение ценности в диапазоне 1..65535.
no spanning-tree pathcost method		Установить значение по умолчанию.
spanning-tree mst *instance_id* **priority** *priority*	instance_id: (1..63); priority: (0..61440)/32768	Установить 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**		Установить значение по умолчанию.

spanning-tree mst max-hops *hop_count*	hop_count: (1..40)/20	Установить 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		Установить значение по умолчанию.
spanning-tree mst *instance_**id*** **tc-protection**	instance_id: (1..63)	Включить ограничение на количество обрабатываемых TC BPDU за установленный интервал времени.
no spanning-tree mst ***instance_id*** **tc-protection**		Выключить ограничение на количество обрабатываемых TC BPDU.
spanning-tree tc-protection mst *instance_id* **interval** *seconds*	instance_id: (1..63); seconds: (1..10)/2 сек.	Установить интервал ограничения количества обрабатываемых TC BPDU.
no spanning-tree tc-protection mst *instance_id* **interval**		Установить значение по умолчанию.
spanning-tree tc-protection mst *instance_id* **threshold** *count*	instance_id: (1..63); count: (1..255)/1	Установить максимальное количество обрабатываемых TC BPDU за заданный интервал времени.
no spanning-tree tc-protection mst *instance_id* **threshold**		Установить значение по умолчанию.
spanning-tree mst configuration	—	Войти 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 121 – Команды режима конфигурации протокола MSTP

Команда	***Значение/Значение по умолчанию***	***Действие***
instance *instance_id* **vlan** *vlan_range*	instance_id:(1..63); vlan_range: (1..4094)	Создать 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*		Удалить соответствие между экземпляром протокола MSTP и группами VLAN.
name *string*	string: (1..32) символа	Задать имя конфигурации MST. - *string* — имя конфигурации MST.
no name		Удалить имя конфигурации MST.
revision *value*	value: (0..65535)/0	Задать номер ревизии конфигурации MST. - *value* — номер ревизии конфигурации MST.
no revision		Установить значение по умолчанию (*value*).
show {current | pending}	—	Показать текущую (**current**) либо ожидающую (**pending**) конфигурацию MST.
exit	—	Выйти из режима конфигурации протокола MSTP с сохранением конфигурации.
abort	—	Выйти 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 122 – Команды режима конфигурации интерфейса Ethernet, группы портов

Команда	*Значение/Значение по умолчанию*	*Действие*
spanning-tree guard root	—/защита выключена	Включить защиту «корня» для всех связующих деревьев STP выбранного порта. Данная защита запрещает интерфейсу быть корневым портом коммутатора.
no spanning-tree guard root		Установить значение по умолчанию.
spanning-tree mst *instance_id* **guard root**	instance_id: (1..63); /защита выключена	Включить защиту «корня» указанного экземпляра MSTP для выбранного интерфейса. Данная защита запрещает интерфейсу быть корневым портом коммутатора. - *instance-id* — идентификатор экземпляра протокола MSTP.
no spanning-tree mst *instance_id* **guard root**		Установить значение по умолчанию.
spanning-tree mst *instance_id* **port-priority** *priority*	instance_id: (1..63); priority: (0..240)/128	Установить 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**		Установить значение по умолчанию.
spanning-tree mst *instance_id* **cost** *cost*	instance_id: (1..63); cost: (1..200000000)	Установить 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**		Установить значение, определяемое на основании скорости порта и метода определения ценности пути, см. таблицу 117.
spanning-tree port-priority *priority*	priority: (0..240)/128	Установить приоритет интерфейса в корневом связующем дереве MSTP. **Значение приоритета должно быть кратно 16.**
no spanning-tree port-priority		Установить значение по умолчанию.
spanning-tree restricted-tcn	–/прием BPDU с флагом TCN разрешен	Запретить прием BPDU с флагом TCN.
no spanning-tree restricted-tcn		Разрешить прием BPDU с флагом TCN.

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 123 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show spanning-tree [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***] [instance** *instance_id***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48) instance_id: (1..63).	Показать конфигурацию протокола STP. - *instance_id* — идентификатор экземпляра протокола MSTP.
show spanning-tree detail [active | blockedports] [instance *instance_id***]**	instance_id: (1..63)	Показать 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	—	Показать информацию о сконфигурированных экземплярах MSTP.
clear spanning-tree detected-protocols interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48).	Перезапустить 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            -
```

5.17.5.3. Настройка протоколов PVSTP+, RPVSTP+

PVSTP+ (Per-VLAN Spanning Tree Protocol Plus) – одна из разновидностей протокола Spanning Tree, расширяющая функциональность STP для использования в отдельных VLAN. Применение данного протокола позволяет в каждом VLAN создать отдельный экземпляр STP. PVSTP+ совместим с STP.

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

Всего поддерживается 64 PVST/RPVST-инстанса. При этом нулевой используется для всех VLAN, в которых отключен PVST/RPVST. Каждому VLAN с включенным PVST/RPVST соответствует один PVST/RPVST инстанс.

Порты, на которых активны более 64 VLAN, при переходе в режим PVST/RPVST временно блокируются, поэтому перед включением PVST/RPVST необходимо расчитать количество используемых VLAN на кольцевых портах коммутатора. Если данное значение превышает 63, то первоначально нужно отключить PVST/RPVST в избыточных VLAN/RPVST командой "no spanning-tree vlan <VLAN ID>".

При включенном режиме PVST/RPVST коммутаторы обрабатывают PVST bpdu во всех VLAN. Поэтому в случаях, когда в кольце используются коммутаторы с количеством PVST/RPVST VLAN, превышающем 63, следует расширить лимиты обработки PVST bpdu-трафика на CPU. Для этого используется команда "service cpu-rate-limits other-bpdu 1024".

Если в процесе эксплуатации понадобится убрать VLAN из PVST/RPVST-инстансов и добавить новые, нужно произвести следующие действия:

1) Отключить все порты на которых настроены VLAN, участвующие в PVST/RPVST (команда «shutdown» в режиме конфигурирования интерфейса);

2) Отключить STP в не нужных VLAN-ах (команда «no spanning-tree vlan *vlan_list*» в глобальном режиме конфигурирования);

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 124 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
spanning-tree vlan *vlan_list*	vlan_list: (1..4094)/ по умолчанию все инстансы включены	Включить работу протокола PVSTP+, RPVSTP+ в указанных VLAN.
spanning-tree vlan *vlan_list*		Отключить работу протокола PVSTP+, RPVSTP+ в указанных VLAN.
spanning-tree vlan *vlan_list* **bpdu {filtering | flooding}**	vlan_list: (1..4094)/ фильтрация отключена	Фильтрует или пропускает входящие кадры PVST/RPVST-BPDU. **Данная команда действует в том случае, если STP отключен либо включен в одном из режимов: STP/RSTP/MST. Если включен режим PVST/RPVST, то данная команда будет действовать только в том случае, если в указанной VLAN отключен STP.** **- filtering —** включить фильтрацию; - **flooding** — отключить фильтрацию.
no spanning-tree vlan *vlan_list* **bpdu**		Установить значение по умолчанию.
spanning-tree vlan *vlan_list* **forward-time** *seconds*	vlan_list: (1..4094); seconds: (4..30)/15 сек	Установить интервал времени, затрачиваемый на прослушивание и изучение состояний перед переключением в состояние передачи для указанных VLAN. **Таймеры должны соответствовать следующей формуле:** **2 * (Forward-Time - 1) ≥ Max-Age ≥ 2 * (Hello-Time + 1).**
no spanning-tree vlan *vlan_list* **forward-time**		Установить значение по умолчанию.
spanning-tree vlan *vlan_list* **hello-time** *seconds*	vlan_list: (1..4094); seconds: (1..10)/2 сек	Установить интервал времени между передачами широковещательных сообщений «Hello» к взаимодействующим коммутаторам для указанных VLAN.
no spanning-tree vlan *vlan_list* **hello-time**		Установить значение по умолчанию.
spanning-tree vlan *vlan_list* **max-age** *seconds*	vlan_list: (1..4094); seconds: (6..40)/20 сек	Установить время жизни связующего дерева STP для указанных VLAN.
no spanning-tree vlan *vlan_list* **max-age**		Установить значение по умолчанию.
spanning-tree vlan *vlan_list* **priority** *priority_value*	vlan_list: (1..4094); priority_value: (0..61440)/32768	Настроить приоритет связующего дерева STP. **Значение выбирается из диапазона с шагом 4096.**
spanning-tree vlan *vlan_list* **priority**		Установить значение по умолчанию.
spanning-tree vlan *vlan_list* **tc-protection**	vlan_list: (1..4094);	Включить ограничение на количество обрабатываемых TCN/TC BPDU за установленный интервал времени для STP, RSTP, нулевого экземпляра MSTP.
no spanning-tree vlan *vlan_list* **tc-protection**		Выключить ограничение на количество обрабатываемых TCN/TC BPDU.
spanning-tree vlan *vlan_list* **tc-protection interval** *seconds*	vlan_list: (1..4094); seconds: (1..10)/2 сек.	Установить интервал ограничения количества обрабатываемых TCN/TC BPDU.
no spanning-tree vlan *vlan_list* **tc-protection interval**		Установить значение по умолчанию.
spanning-tree vlan *vlan_list* **tc-protection threshold** *count*	vlan_list: (1..4094); count: (1..255)/1	Установить максимальное количество обрабатываемых TCN/TC BPDU за заданный интервал времени.
no spanning-tree vlan *vlan_list* **tc-protection threshold**		Установить значение по умолчанию.

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet

Вид запроса командной строки режима конфигурации интерфейса:

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

Таблица 125 – Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
spanning-tree vlan *vlan_list* **bpdu {filtering | flooding}**	vlan_list: (1..4094)/ фильтрация отключена	Фильтрует или пропускает входящие кадры PVST/RPVST-BPDU на заданном интерфейсе. **Данная команда действует в том случае, если STP отключен либо включен в одном из режимов: STP/RSTP/MST. Если включен режим PVST/RPVST, то данная команда будет действовать только в том случае, если в указанной VLAN отключен STP.** **- filtering —** включить фильтрацию; - **flooding** — отключить фильтрацию.
no spanning-tree vlan *vlan_list* **bpdu**		Установить значение по умолчанию.
spanning-tree vlan *vlan_list* **cost** *cost*	vlan_list: (1..4094); cost: (1..200000000)	Установить ценность пути через данный интерфейс для указанных VLAN. - *cost* — ценность пути.
no spanning-tree vlan *vlan_list* **cost**		Установить значение, определяемое на основании скорости порта и метода определения ценности пути для указанных VLAN.
spanning-tree vlan *vlan_list* **disable**	vlan_list: (1..4094)	Запретить работу протокола STP на конфигурируемом интерфейсе для указанных VLAN.
no spanning-tree vlan *vlan_list* **disable**		Разрешить работу протокола STP на конфигурируемом интерфейсе для указанных VLAN.
spanning-tree vlan *vlan_list* **port-priority** *priority_value*	vlan_list: (1..4094); priority_value: (0..240)/128	Установить приоритет интерфейса в корневом связующем дереве STP. **Значение выбирается из диапазона с шагом 16.**
no spanning-tree vlan *vlan_list* **port-priority**		Установить значение по умолчанию.
spanning-tree vlan *vlan_list* **guard {root | loop | none}**	vlan_list: (1..4094);	Включить защиту «корня» на данном интерфейсе для указанных VLAN. - **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 vlan *vlan_list* **guard**		Отключить все Guard-функции на интерфейсе.
spanning-tree *vlan* **vlan_list restricted-tcn**	—/выключено	Запретить прием BPDU с флагом TCN для указанных VLAN.
no spanning-tree *vlan* **vlan_list restricted-tcn**		Разрешить прием BPDU с флагом TCN для указанных VLAN.

5.17.6. 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 126 – 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 127 – 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} {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	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 128 – 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.

5.17.7. 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 129 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
lldp run	—/разрешено	Разрешить коммутатору использование протокола LLDP.
no lldp run		Запретить коммутатору использование протокола LLDP.
lldp timer *seconds*	seconds: (5..32768)/30 сек	Определить, как часто устройство будет отправлять обновление информации LLDP.
no lldp timer		Установить значение по умолчанию.
lldp hold-multiplier *number*	number: (2..10)/4	Задать величину времени для принимающего устройства, в течение которого нужно удерживать принимаемые пакеты LLDP перед их сбросом. Данная величина передается на принимающую 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		Установить значение по умолчанию.
lldp tx-delay *seconds*	seconds: (1..8192)/2 сек	Установить 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		Установить значение по умолчанию.

lldp lldpdu {filtering | flooding}	—/filtering	Определить 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		Установить значение по умолчанию.
lldp med fast-start repeat-count *number*	number: (1..10)/3	Установить число повторений PDU LLDP для быстрого запуска, определяемого посредством LLDP-MED.
no lldp med fast-start repeat-count		Установить 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)	Определить 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. Если не указывать значение DSCP, по умолчанию коммутатор будет отправлять параметр DSCP 0. **Изменение network-policy возможно только после снятия политики со всех интерфейсов, где она применена.**
no lldp med network-policy *number*		Удалить созданное правило для параметра network-policy.
lldp notifications interval *seconds*	seconds: (5..3600)/5 сек	Установить максимальную скорость передачи уведомлений LLDP. - *seconds* — период времени, в течение которого устройство может отправить не более одного уведомления.
no lldp notifications interval		Установить значение по умолчанию.

Команды режима конфигурации интерфейсов Ethernet

Вид запроса командной строки в режиме конфигурации интерфейсов Ethernet:

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

Таблица 130 – Команды режима конфигурации интерфейса Ethernet

Команда	***Значение/Значение по умолчанию***	***Действие***
lldp transmit	по умолчанию разрешено использование в обоих направлениях.	Разрешить передачу пакетов по протоколу LLDP на интерфейсе.
no lldp transmit		Запретить передачу пакетов по протоколу LLDP на интерфейсе.
lldp receive		Разрешить прием пакетов по протоколу LLDP на интерфейсе.
no lldp receive		Запретить 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.	Определить, 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		Установить 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.	Определить, какие опциональные TLV-поля будут включены устройством в передаваемый LLDP-пакет: - **pvid** — PVID интерфейса; - **ppvid** — добавить/удалить PPVID; - **vlan-name** — добавить/удалить номер VLAN; - **protocol** — добавить/удалить определенный протокол.
lldp optional-tlv 802.1 protocol {add | remove} {stp | rstp | mstp | pause | 802.1x | lacp | gvrp}		
no lldp optional-tlv 802.1 pvid		Установить значение по умолчанию.
lldp management-address {*ip_address* **| none | automatic [gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id***]}**	формат ip-address: A.B.C.D; gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094). По умолчанию управляющий адрес определяется автоматически.	Определить 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 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		Удалить управляющий IP-адрес.
lldp notification {enable | disable}	по умолчанию отправка уведомлений LLDP запрещена.	Разрешить/запретить отправку уведомлений LLDP на интерфейсе. - **enable** — разрешает; - **disable** — запрещает.
no lldp notifications		Установить значение по умолчанию.
lldp med enable [*tlv_list*]	tvl_list: (network-policy, location, inventory)/запрещено использование расширения протокола LLDP MED.	Разрешить 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)	Назначить правило network-policy данному интерфейсу. - **add** — назначает правило; - **remove** — удаляет правило; - *number* — номер правила.
no lldp med network-policy		Удалить 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.	Задать 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}		Удалить настройки параметра местоположения location.
lldp med notification topology-change {enable | disable}	—/запрещено	Разрешить/запретить отправку уведомлений LLDP MED об изменении топологии. - **enable** — разрешает отправку уведомлений; - **disable** — запрещает отправку уведомлений.
no lldp med notifications topology-change		Установить 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 131 – Команды режима privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
clear lldp table [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Очистить таблицу адресов обнаруженных соседних устройств и начать новый цикл обмена пакетами по протоколу LLDP MED.
show lldp configuration [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob | detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Показать LLDP-конфигурации всех физических интерфейсов устройства, либо заданных интерфейсов.
show lldp med configuration [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob | detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Показать конфигурации расширения протокола LLDP-MED для всех физических интерфейсов, либо заданных интерфейсов.
show lldp local {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Показать LLDP-информацию, которую анонсирует данный порт.
show lldp local tlvs-overloading [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Показать статус перезагрузки TLVs LLDP.

show lldp neighbors [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob | detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Показать информацию о соседних устройствах, на которых работает протокол LLDP.
show lldp statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob | detailed]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Показать 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 132 – Описание результатов

Поле	***Описание***
Timer	Определить, как часто устройство отправляет LLDP-обновления.
Hold Multiplier	Определить 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	Определить минимальное время, в течение которого порт будет ожидать перед посылкой следующего LLDP-сообщения.
Tx delay	Определить задержку между последующими передачами LLDP-кадров, инициированных изменениями значений либо статуса.
Port	Номер порта.
State	Режим работы порта для протокола LLDP.

Optional TLVs	Передаваемые TLV-опции. 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
---------     ----------------  -------- ----------    -------------
te0/1         0060.704C.73FE      1      ts-7800-2           B
te0/2         0060.704C.73FD      1      ts-7800-2           B
te0/3         0060.704C.73FC      9      ts-7900-1          B, R
te0/4         0060.704C.73FB      1      ts-7900-2           W
```

```
console# show lldp neighbors tengigabitethernet 1/0/20
```

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

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

Таблица 133 – 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.

5.17.8. Настройка протокола OAM

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

Команды режима конфигурации интерфейсов Ethernet

Вид запроса командной строки в режиме конфигурации интерфейсов Ethernet:

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

Таблица 134 – Команды режима конфигурации интерфейса Ethernet

Команда	***Значение/Значение по умолчанию***	***Действие***
ethernet oam	—/отключено	Включить поддержку Ethernet OAM на порту.
no ethernet oam		Отключить Ethernet OAM на конфигурируемом порту.
ethernet oam link-monitor frame threshold *count*	count: (1..65535)/1	Установить порог количества ошибок за указанный период (период устанавливается командой **ethernet oam link-monitor frame window**).
no ethernet oam link-monitor frame threshold		Восстановить значение по умолчанию.
ethernet oam link-monitor frame window *window*	window: (10..600)/100 мс	Установить временной промежуток для подсчета количества ошибок.
no ethernet oam link-monitor frame window		Восстановить значение по умолчанию.
ethernet oam link-monitor frame-period threshold *count*	count: (1..65535)/1	Установить порог для события «frame-period» (период устанавливается командой **ethernet oam link-monitor frame-period window**).
no ethernet oam link-monitor frame-period threshold		Восстановить значение по умолчанию.

ethernet oam link-monitor frame-period window *window*	window: (1..65535)/10000	Установить временной промежуток для события «frame-period» (в кадрах).
no ethernet oam link-monitor frame-period window		Восстановить значение по умолчанию.
ethernet oam link-monitor frame-seconds threshold *count*	count: (1..900)/1	Установить порог для события «frame-period» (период устанавливается командой **ethernet oam link-monitor frame-seconds window**), в секундах.
no ethernet oam link-monitor frame-seconds threshold		Восстановить значение по умолчанию.
ethernet oam link-monitor frame-seconds window *window*	window: (100..9000)/100 мс	Установить временной промежуток для события «frame-period».
no ethernet oam link-monitor frame-seconds window		Восстановить значение по умолчанию.
ethernet oam mode {active | passive}	—/active	Установить режим работы протокола OAM: - **active** — коммутатор постоянно отправляет OAMPDU; - **passive** — коммутатор начинает отправлять OAMPDU только при наличии OAMPDU со встречной стороны.
no ethernet oam mode		Восстановить значение по умолчанию.
ethernet-oam remote-failure	—/включено	Включить поддержку и обработку событий «remote-failure».
no ethernet oam remote-failure		Восстановить значение по умолчанию.
ethernet oam remote-loopback supported	—/отключено	Включить поддержку функции remote-loopback.
no ethernet oam remote-loopback supported		Восстановить значение по умолчанию.
ethernet oam uni-directional detection	—/отключено	Включить функцию обнаружения однонаправленных связей на базе протокола Ethernet OAM.
no ethernet oam uni-directional detection		Восстановить значение по умолчанию.
ethernet oam uni-directional detection action {log | error-disable}	—/log	Определить реакцию коммутатора на однонаправленную связь: - **log** — отправка SNMP trap и запись в журнал; - **error-disable** — перевод порта в состояние «error-disable», запись в журнал и отправка SNMP trap.
no ethernet oam uni-directional detection action		Восстановить значение по умолчанию.
ethernet oam uni-directional detection agressive	—/отключено	Включить агрессивный режим определения однонаправленной связи. Если от соседнего устройства перестают приходить Ethernet OAM-сообщения — линк помечается как однонаправленный.
no ethernet oam uni-directional detection aggressive		Восстановить значение по умолчанию.
ethernet oam uni-directional detection discovery time *time*	time: (5..300)/5 сек	Установить временной интервал для определения типа связи на порту.
no ethernet oam uni-directional detection discovery-time		Восстановить значение по умолчанию.

Команды режима privileged EXEC

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

```
console#
```

Таблица 135 – Команды режима privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
clear ethernet oam statistics [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4).	Очистить статистику Ethernet OAM для указанного интерфейса.
show ethernet oam discovery [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4).	Отобразить состояние протокола Ethernet OAM для указанного интерфейса.
show ethernet oam statistics [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4).	Отобразить статистику обмена протокольными сообщениями для указанного интерфейса.
show ethernet oam status [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Отобразить настройки Ethernet OAM для указанного интерфейса.
show ethernet oam uni-directional detection [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Отобразить состояние механизма определения однонаправленных связей для указанного интерфейса.
ethernet oam remote-loopback **{start/stop}** interface **{ gigabitethernet** gi_port **/tengigabitethernet** te_port **}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24)	Запустить процесс тестирования канала с помощью ethernet oam remote-loopback на указанном интерфейсе.

Примеры выполнения команд

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

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

```
gigabitethernet 1/0/3
Local client
------------
 Administrative configurations:
  Mode:              active
  Unidirection:      not supported
  Link monitor:      supported
  Remote loopback:   supported
  MIB retrieval:     not supported
  Mtu size:          1500
 Operational status:
  Port status:       operational
  Loopback status:   no loopback
```

```
  PDU revision:      3
Remote client
-------------
  MAC address: a8:f9:4b:0c:00:03
  Vendor(oui): a8 f9 4b
 Administrative configurations:
  PDU revision:      3
  Mode:              active
  Unidirection:      not supported
  Link monitor:      supported
  Remote loopback:   supported
  MIB retrieval:     not supported
  Mtu size:          1500
console#
```

5.17.9. Настройка протокола CFM (Connectivity Fault Management)

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

Протокол оперирует следующими понятиями:

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

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 136 – Команды режима глобальной конфигурации

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

Команды режима конфигурирования домена

Вид запроса командной строки в режиме конфигурирования домена:

```
console(config-cfm-md)#
```

Таблица 137 – Команды режима конфигурирования CFM-домена (MD)

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

Команды режима конфигурирования сервиса

Вид запроса командной строки в режиме конфигурирования домена:

```
console(config-cfm-ma)#
```

Таблица 138 – Команды режима конфигурирования CFM сервиса (MA)

Команда	***Значение/Значение по умолчанию***	***Действие***
continuity-check interval *interval*	interval: (1, 10, 100, 600) секунд/1 секунда	Установка интервала отправки Continuity Check сообщений.
no continuity-check interval		Установка значения по умолчанию
Direction down	-	Устанавливает направление конечной точкой сервиса (MEP) в нисходящее.
No direction down		Устанавливает направление конечной точки сервиса (MEP) в восходящее.
efd notify erps	-/выключено	Включает отправку уведомлений об обнаружении изменения состояния кольца ERPS на события events propagation link failure/restore и нарушение связности, детектированных с помощью Continuity Check Protocol (CCM)
no efd notify erps		Отключить отправку уведомлений.
mep *id*	id: (1..8191)	Добавление конечной точки сервиса (MEP) с идентификатором «id» к данному сервису.

		Данной командой осуществляется только привязка MEP к сервису. MEP создается в режиме конфигурирования интерфейса.
no mep *id*		Удаление конечной точки сервиса (MEP).
mip auto-create { lower-mep-only | none }	-/По умолчанию используется режим, сконфигурированный для домена, в котором находится сервис	Включение автоматического создания промежуточных точек сервиса (MIP). Промежуточные точки сервиса (MIP) создаются на всех портах, на которых прописан VLAN сервиса. Необязательные параметры: – lower-mep-only – исключает из списка порты, на которых уже создана конечная точка сервиса (MEP); – none – не создавать автоматически промежуточные точки сервиса (MIP).
no mip auto-create		Установка значения по умолчанию.

Команды режима конфигурирования интерфейса Ethernet

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

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

Таблица 139 – Команды режима конфигурирования интерфейса Ethernet

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

Команды режима конфигурирования конечной точки сервиса

Вид запроса командной строки в режиме конфигурирования домена:

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

Таблица 140 – Команды режима конфигурирования CFM конечной точки (MEP)

Команда	***Значение/Значение по умолчанию***	***Действие***
active	-/выключена	Включение конечной точки сервиса (MEP).
no active		Установка значения по умолчанию.
continuity-check enable	-/выключена	Включение отправки Continuity Check сообщений.
no continuity-check enable		Установка значения по умолчанию.
cos *cos*	cos: (0..7)/7.	Установка значения приоритета CoS, с которым будут отправляться Continuity Check сообщения.
no cos		Установка значения по умолчанию.
alarm delay *delay*	delay: (2500..10000) мс/2500 мс	Указание интервала задержки, по истечении которого будет генерироваться авария.
no alarm delay		Установка значения по умолчанию.

alarm reset ***interval***	interval: (2500..10000) мс/10000 мс	Указание промежутка времени, по истечении которого произойдет сброс аварии.
no alarm reset		Установка значения по умолчанию.
alarm notification { all | error-xcon | remote-error-xcon | mac-remote-error-xcon | xcon | none }	-/mac-remote-error-xcon	Включение уведомлений для определенных типов событий. Типы событий: - all – все события DefRDI, DefMACStatus, DefRemote, DefError, DefXcon; - error-xcon – только события DefError и DefXcon; - remote-error-xcon – только события DefRemote, DefError и DefXcon; - mac-remote-error-xcon – только события DefMACStatus, DefRemote, DefError и DefXcon; - xcon – только событие DefXcon; - none – уведомления отключены.
no alarm notification		Установка значения по умолчанию.

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 141 – Команды режима privileged EXEC

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

5.17.10. Настройка функции Flex-link

Flex-link – функция резервирования, предназначенная для обеспечения надежности канала передачи данных. В связке flex-link могут находиться ethernet и port-channel интерфейсы. Один из этих интерфейсов находится в

заблокированном состоянии и начинает пропускать трафик только в случае аварии на втором интерфейсе.

Команды режима конфигурирования интерфейса Ethernet, интерфейса группы портов

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

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

Таблица 142 – Команды режима конфигурирования интерфейса Ethernet, группы портов

Команда	*Значение/Значение по умолчанию*	*Действие*
flex-link backup { tengigabitethernet *te_port* **| gigabitethernet** *gi_port* **| port-channel** *port_channel}*	te_port: (1..8/0/1..4); gi_port: (1..8/0/1..24); port_channel (1..48)/-	Включает flex-link на интерфейсе и назначает выбранному интерфейсу роль backup-интерфейса в flex-link паре.
no flex-link backup { tengigabitethernet *te_port* **| gigabitethernet** *gi_port* **| port-channel** *port_channel}*		Выключает flex-link на интерфейсе и удаляет выбранный интерфейс из flex-link пары.
flex-link preemption mode [**forced | bandwidth| off**]	-/off	Задает действие при поднятии интерфейса, участвующего во flex-link: - **forced** – если поднявшийся интерфейс настроен как master, то он станет активным интерфейсом; - **bandwidth –** при поднятии интерфейса активным станет интерфейс с большей пропускной способностью; - **off** – поднявшийся интерфейс останется в заблокированном состоянии.
no flex-link preemption mode		Возвращает значение по умолчанию.
flex-link preemption delay *delay*	delay: (1..300)/35	Задает время от перехода отключенного порта в состояние «up», по прошествии которого выполняется действие, установленное командой **flex-link preemption mode**. - delay – период времени, в секундах.
no flex-link preemption delay		Возвращает значение по умолчанию.

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 143 – Команды режима EXEC

Команда	*Значение*	*Действие*
show interfaces flex-link [detailed] { tengigabitethernet *te_port* **| gigabitethernet** *gi_port* **| port-channel** *port-channel* **}**	te_port: (1..8/0/1..4); gi_port: (1..8/0/1..24); port_channel: (1..48)	Показывает конфигурацию функции flex-link.

5.17.11. Настройка функции Layer 2 Protocol Tunneling (L2PT)

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

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

Коммутаторы серии RTT-A420 предоставляют возможность инкапсулировать служебные пакеты протоколов STP, LACP, LLDP, IS-IS.

Пример

Если включить L2PT для протокола STP, то коммутаторы A, B, C и D будут объединены в одно связующее дерево несмотря на то, что коммутатор A не соединен напрямую с коммутаторами B, C и D (рис. 33). Информация об изменении топологии сети может быть передана сквозь сеть провайдера.

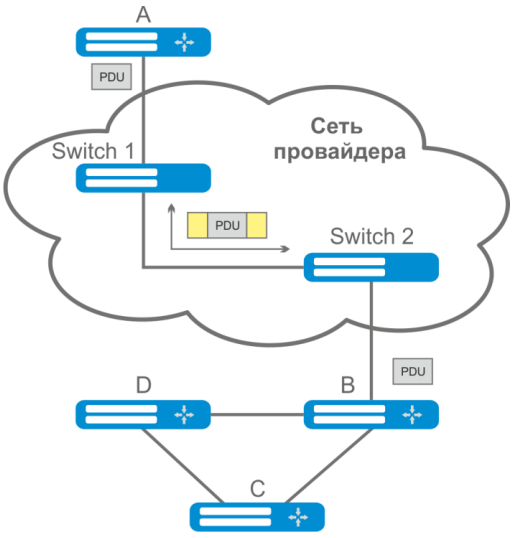


Рис. 34 – Пример работы функции L2PT

Алгоритм работы функции следующий:

Инкапсуляция:

1. Все L2 PDU перехватываются на CPU;

2. Подсистема L2PT определяет L2-протокол, которому соответствует принятый PDU, и проверяет, включена ли на порту, с которого принят этот PDU, настройка l2protocol-tunnel для данного L2-протокола.

Если настройка включена, то:

– во все порты VLAN, на которых включено туннелирование, отправляется PDU-фрейм;

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

Если настройка выключена, то:

– PDU-фрейм передается в обработчик соответствующего протокола.

Декапсуляция:

1. Реализован перехват на CPU Ethernet-кадров с MAC-адресом назначения, заданным при помощи команды l2protocol-tunnel address xx-xx-xx-xx-xx-xx. Перехват включается только тогда, когда хотя бы на одном порту включена настройка l2protocol-tunnel (независимо от протокола).
2. При перехвате пакета с MAC-адресом назначения xx-xx-xx-xx-xx-xx, он сначала попадает в подсистему L2PT, которая определяет L2-протокол для данного PDU по его заголовку, и проверяет, включена ли на порту, с которого принят инкапсулированный PDU, настройка l2protocol-tunnel для данного L2-протокола.

Если настройка включена, то:

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

Если настройка выключена:

– во все порты VLAN, на которых включено туннелирование, отправляется декапсулированный PDU-фрейм;

– во все порты VLAN, на которых выключено туннелирование, отправляется инкапсулированный PDU-фрейм.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 144 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
l2protocol-tunnel address {*mac_address***}**	mac_address: (01:00:ee:ee:00:00, 01:00:0c:cd:cd:d0, 01:00:0c:cd:cd:d1, 01:00:0c:cd:cd:d2, 01:0f:e2:00:00:03)/ 01:00:ee:ee:00:00	Задать MAC-адрес назначения для туннелируемых фреймов.
no l2protocol-tunnel address		Установить значение по умолчанию.

Команды режима конфигурации интерфейса Ethernet

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

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

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

Таблица 145 – Команды режима конфигурации интерфейса Ethernet

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

l2protocol-tunnel shutdown-threshold {stp | lacp | lldp | isis-l1 | isis-l2 | pvst | cdp | dtp | vtp | pagp} threshold	treshold: (1..4096)/выключено	Настройка порогового значения скорости входящих PDU-фреймов (в пакетах в секунду), полученных и подлежащих инкапсуляции. При превышении порога порт будет переведен в состояние Errdisable (отключен).
no l2protocol-tunnel shutdown-threshold {stp | lacp | lldp | isis-l1 | isis-l2 | pvst | cdp | dtp | vtp | pagp}		Отключает режим контроля скорости входящих PDU-фреймов.

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 146 – Команды режима privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show l2protocol-tunnel [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48).	Отображает информацию L2PT для указанного интерфейса или для всех интерфейсов, на которых включен L2PT, если интерфейс не указан.
clear l2protocol-tunnel statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port:(1..8/0/1..4); group: (1..48)	Очистка статистики L2PT для указанного интерфейса или для всех интерфейсов, на которых включен L2PT, если интерфейс не указан.

Примеры выполнения команд

- Установить туннельный MAC-адрес в значение 01:00:0c:cd:cd:d0, включить отправку SNMP traps от триггера l2protocol-tunnel (триггера на срабатывание drop-threshold и shutdown-threshold).

```
console(config)#l2protocol-tunnel address 01:00:0c:cd:cd:d0
console(config)#snmp-server enable traps l2protocol-tunnel
```

- Включить режим туннелирования STP на интерфейсе, установить значение CoS-пакетов BPDU равным 4, включить контроль скорости входящих пакетов BPDU.

```
console(config)# interface gigabitEthernet 1/0/1
console(config-if)# spanning-tree disable
console(config-if)# switchport mode customer
console(config-if)# switchport customer vlan 100
console(config-if)# l2protocol-tunnel stp
console(config-if)# l2protocol-tunnel cos 4
console(config-if)# l2protocol-tunnel drop-threshold stp 40
console(config-if)# l2protocol-tunnel shutdown-threshold stp 100
console#show l2protocol-tunnel
```

```
MAC address for tunneled frames: 01:00:0c:cd:cd:d0
```

```
Port     CoS Protocol Shutdown  Drop       Encaps    Decaps    Drop
                      Threshold Threshold  Counter   Counter   Counter
-------- --- -------- --------- ---------  --------- --------- ---------
gi1/0/1   4      stp       100        40         650         0       450
```

Примеры сообщений о срабатывании триггера:

```
12-Nov-2015 14:32:35 %-I-DROP: Tunnel drop threshold 40 exceeded for interface
gi1/0/1
12-Nov-2015 14:32:35 %-I-SHUTDOWN: Tunnel shutdown threshold 100 exceeded for
interface gi1/0/1
```

5.18. 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.

При назначении Voice VLAN на стороне оконечного оборудования необходимо использовать lldp-med политики или DHCP.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 147 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
voice vlan aging-timeout *timeout*	timeout: (1..43200)/1440	Установить таймаут для порта, принадлежащего к voice-vlan. Если с порта в течение заданного времени не было кадров с OUI VoIP-оборудования, то voice vlan удаляется с данного порта.
no voice vlan aging-timeout		Восстановить значение по умолчанию.
voice vlan cos *cos* **[remark]**	cos: (0-7)/6	Установить выходную очередь для трафика в Voice VLAN в соответствии с настроенным для Voice VLAN CoS без смены CoS. - **remark** — включает переназначение CoS на указанный для трафика в Voice VLAN.
no voice vlan cos		Восстановить значение по умолчанию.
voice vlan id *vlan_id*	vlan_id: (1..4094)	Установить идентификатор VLAN для Voice VLAN
no voice vlan id		Удалить 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	Позволить редактировать таблицу OUI. - *oui* — первые 3 байта MAC-адреса; - *word* — описание oui.
no voice vlan oui-table		Удалить все пользовательские изменения OUI-таблицы.
voice vlan state {oui-enabled | disabled}	-/выключено	Включить/отключить Voice VLAN.
no voice vlan state		Вернуть значение по умолчанию.

Команды режима конфигурации интерфейса Ethernet

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

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

Таблица 148 – Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
voice vlan enable	—/отключено	Включить Voice VLAN для порта.
no voice vlan enable		Отключить Voice VLAN для порта.
voice vlan authentication bypass enable	—/отключено	Разрешить трафику Voice VLAN игнорировать аутентификацию 802.1x. **Функционал работает для режимов dot1x host-mode single-host, multi-session.**

no voice vlan authentication bypass enable		Запретить трафику Voice VLAN игнорировать аутентификацию 802.1x.
voice vlan cos mode {src | all}	—/src	Включить маркировку трафика для всех кадров, либо только для источника.
no voice vlan cos mode		Восстановить значение по умолчанию.

5.19. Групповая адресация

5.19.1. 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 5.19.2 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 149 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip igmp snooping	по умолчанию функция выключена	Разрешить использование функции IGMP Snooping коммутатором.
no ip igmp snooping		Запретить использование функции IGMP Snooping коммутатором.
ip igmp snooping vlan *vlan_id*	vlan_id: (1..4094) по умолчанию функция выключена	Разрешить использование функции IGMP Snooping коммутатором для данного интерфейса VLAN. - *vlan_id* — идентификационный номер VLAN.
no ip igmp snooping vlan *vlan_id*		Запретить использование функции IGMP Snooping коммутатором для данного интерфейса VLAN.
ip igmp snooping vlan *vlan_id* **group-specific-query suppress**	vlan_id: (1..4094)	Включить перенаправление всех пакетов IGMP Group Specific Query в порты, привязанные к группе, согласно таблице ip igmp snooping groups.
no ip igmp snooping vlan *vlan_id*		Отключить перенаправление пакетов IGMP GroupSpecific Query в порты, привязанные к группе, согласно таблице ip igmp snooping groups.
ip igmp snooping vlan *vlan_id* **static** *ip_multicast_address* **[interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Зарегистрировать групповой IP-адрес в таблице групповой адресации и статически добавить интерфейсы из группы для текущей VLAN. - *vlan_id* — идентификационный номер VLAN; - *ip_multicast_address* — групповой IP-адрес. Перечисление интерфейсов осуществляется через «-» и «,».
no ip igmp snooping vlan *vlan_id* **static** *ip_address* **[interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**		Удалить групповой IP-адрес из таблицы.
ip igmp snooping vlan *vlan_id* **mrouter learn pim-dvmrp**	vlan_id: (1..4094) по умолчанию разрешено	Разрешить 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**		Запретить для данной группы VLAN автоматическое распознавание портов, к которым подключены многоадресные маршрутизаторы.
ip igmp snooping vlan *vlan_id* **mrouter interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Определить порт, к которому подключен маршрутизатор многоадресной рассылки для заданной VLAN. - *vlan_id* — идентификационный номер VLAN.
no ip igmp snooping vlan *vlan_id* **mrouter interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**		Указать, что к порту не подключен маршрутизатор многоадресной рассылки.
ip igmp snooping vlan *vlan_id* **forbidden mrouter interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Установить запрет на определение порта (статически, динамически) как порта, к которому подключен маршрутизатор многоадресной рассылки. - *vlan_id* — идентификационный номер VLAN.

no ip igmp snooping vlan *vlan_id* **forbidden mrouter interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**		Снять 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	Включить поддержку выдачи запросов igmp-query коммутатором в данной VLAN.
no ip igmp snooping vlan *vlan_id* **querier**		Отключить поддержку выдачи запросов igmp-query коммутатором в данной VLAN.
ip igmp snooping vlan *vlan_id* **replace source-ip** *ip_address*	vlan_id: (1..4094); ip_address: A.B.C.D/0.0.0.0	Включить замену IP-адреса источника на указанный IP-адрес во всех пакетах IGMP report в заданной VLAN. - *vlan_id* — идентификационный номер VLAN; - *A.B.C.D* — IP-адрес, на который будет произведена замена SRC IP. **Значение по умолчанию 0.0.0.0 говорит о том, что замена SRC IP IGMP report производиться не будет.**
no ip igmp snooping vlan *vlan_id* **replace source-ip**		Отключить замену IP-адреса источника в пакетах IGMP report в заданной VLAN.
ip igmp snooping vlan *vlan_id* **replace source-mac** *mac_address*	vlan_id: (1..4094); mac_address: (H.H.H или H:H:H:H:H:H или H-H-H-H-H-H —/выключено	Включить замену MAC-адреса источника на указанный MAC-адрес во всех пакетах IGMP report в заданной VLAN. - *vlan_id* — идентификационный номер VLAN; - *mac_address* — MAC-адрес, который будет подставлен в пакет IGMP report.
no ip igmp snooping vlan *vlan_id* **replace source-mac**		Отключить замену MAC-адреса источника в пакетах IGMP report в заданной VLAN.
ip igmp snooping vlan *vlan_id* **replace interface** *interfaces* *{***gigabitethernet** *gi_port |* **tengigabitethernet** *te_port |* **fortygigabitethernet** *fo_port |* **port-channel** *group}*	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48) —/разрешено	Разрешить подмену MAC-адреса источника или IP-адреса источника во всех пакетах IGMP report, поступающих в заданный порт в заданной VLAN. - *vlan_id* — идентификационный номер VLAN.
no ip igmp snooping vlan *vlan_id* **replace interface** *interfaces*		Запретить подмену MAC-адреса источника или IP-адреса источника во всех пакетах IGMP report, поступающих в заданный порт в заданной VLAN.
ip igmp snooping vlan *vlan_id* **querier version {2 | 3}**	—/IGMPv3	Установить версию IGMP-протокола, на основании которой будут формироваться IGMP-query запросы.
no ip igmp snooping vlan *vlan_id* **querier version**		Установить значение по умолчанию
ip igmp snooping vlan *vlan_id* **querier address** *ip_address*	vlan_id: (1..4094)	Определить исходный IP-адрес, который будет использоваться IGMP querier-ом. Querier — устройство, которое отправляет IGMP-запросы.
no ip igmp snooping vlan *vlan_id* **querier address**		Установить 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] [interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**	vlan_id: (1..4094); —/выключено gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	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); - **interface** — при использовании данного параметра механизм fast-leave срабатывает только на указанных интерфейсах (при условии, что процесс IGMP Snooping Immediate-Leave не включен глобально на текущей VLAN).

no ip igmp snooping vlan *vlan_id* **immediate-leave [host-based] [interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**		Отключить процесс IGMP Snooping Immediate-Leave на текущей VLAN или указанном физическом интерфейсе.
ip igmp snooping vlan *vlan_id* **proxy-report [version** *version***]**	vlan_id: (1..4094); version: (1..3)	Включить функцию proxy report в определенном VLAN. При включении этой функции коммутатор на пришедшие IGMP query будет отвечать от своего имени для статических групп. Клиентские IGMP report для статических групп при этом отбрасываются. - **version** — устанавливает версию IGMP для отправки пакетов. По умолчанию версия определяется по пришедшему на коммутатор пакету IGMP query.
no ip igmp snooping vlan *vlan_id* **proxy-report**		Выключить Proxy report в определенном VLAN.
ip igmp snooping map cpe untagged [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}] multicast-tv vlan** *vlan_id*	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Включить маппинг нетегированных IGMP-запросов для QinQ-интерфейсов на указанный vlan_id. ***interface*** — маппинг включается только на указанных интерфейсах.
no ip igmp snooping map cpe untagged [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}] multicast-tv vlan** *vlan_id*		Выключить маппинг нетегированных IGMP-запросов для указанных QinQ-интерфейсов. ***interface*** — маппинг выключается только на указанных интерфейсах.
ip igmp snooping map cpe vlan *cvlan_id* **[interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}] multicast-tv vlan** *vlan_id*	cvlan_id: (1..4094); vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Включить маппинг тегированных cvlan-id IGMP-запросов для QinQ-интерфейсов на указанный vlan_id. ***interface*** — маппинг включается только на указанных интерфейсах.
no ip igmp snooping map cpe vlan *cvlan_id* **[interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}] multicast-tv vlan** *vlan_id*		Выключить маппинг тегированных cvlan-id IGMP-запросов для указанных QinQ-интерфейсов. ***interface*** — маппинг выключается только на указанных интерфейсах.

Команды режима конфигурации интерфейса VLAN

Вид запроса командной строки режима конфигурации VLAN:

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

Таблица 150 – Команды режима конфигурации интерфейса VLAN

Команда	***Значение/Значение по умолчанию***	***Действие***
ip igmp robustness *count*	count: (1..7)/2	Установить значение устойчивости для IGMP. Если на канале наблюдается потеря данных, значение устойчивости должно быть увеличено.
no ip igmp robustness		Установить значение по умолчанию.

ip igmp version {2 / 3}	—/IGMPv3	Установить версию IGMP-протокола.
no ip igmp version		Установить значение по умолчанию.
ip igmp query-interval *seconds*	seconds: (30..18000)/125 с	Установить таймаут, по которому система отправляет основные запросы всем участникам группы многоадресной передачи для проверки их активности.
no ip igmp query-interval		Установить значение по умолчанию.
ip igmp query-max-response-time *seconds*	seconds: (5..20)/10 с	Установить максимальное время ответа на запрос.
no ip igmp query-max-response-time		Установить значение по умолчанию.
ip igmp last-member-query-count *count*	count: (1..7)/значение переменной robustness	Установить количество запросов, после рассылки которых, коммутатор определяет, что на данном порту нет желающих участвовать в многоадресной рассылке.
no ip igmp last-member-query-count		Установить значение по умолчанию.
ip igmp last-member-query-interval *milliseconds*	*milliseconds*: (100..25500)/1000 мс	Установить интервал запроса для последнего участника.
no ip igmp last-member-query-interval		Установить значение по умолчанию.

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet

Вид запроса командной строки режима конфигурации интерфейса:

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

Таблица 151 – Команды режима конфигурации интерфейса Ethernet

Команда	***Значение/Значение по умолчанию***	***Действие***
switchport access multicast-tv vlan *vlan_id*	vlan_id: (1..4094)	Включить перенаправление IGMP-запросов с клиентских VLAN в Multicast VLAN для интерфейса в режиме «access». **Для работы данной функции требуется включение ip igmp snooping не только глобально и в Multicast VLAN, но и в клиентских VLAN.**
no switchport access multicast-tv vlan		Выключить перенаправление IGMP-запросов с клиентских VLAN в Multicast VLAN для интерфейса в режиме «access».
switchport trunk multicast-tv vlan *vlan_id* **[tagged]**	vlan_id: (1..4094)	Включить перенаправление IGMP-запросов из VLAN, участником которых является порт, в Multicast VLAN для интерфейса в режиме «trunk». Multicast-трафик передается на порт нетегированным или тегированным в зависимости от параметра tagged. Параметр tagged указывает на то, что Multicast-трафик должен отправляться в порт тегированным в Multicast VLAN.
no switchport trunk multicast-tv vlan		Выключить перенаправление IGMP-запросов в Multicast VLAN. Порт исключается из групп многоадресной рассылки в Multicast VLAN.
switchport general multicast-tv vlan *vlan_id* **[tagged]**	vlan_id: (1..4094)	Включить перенаправление IGMP-запросов из VLAN, участником которых является порт, в Multicast VLAN для интерфейса в режиме «general». Multicast-трафик передается на порт нетегированным или тегированным в зависимости от параметра tagged. Параметр tagged указывает на то, что Multicast-трафик должен отправляться в порт тегированным в Multicast VLAN.

no switchport general multicast-tv vlan		Выключить перенаправление IGMP-запросов в Multicast VLAN. Порт исключается из групп многоадресной рассылки в Multicast VLAN.

Команды режима EXEC

Все команды доступны только для привилегированного пользователя.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 152 – Команды режима EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show ip igmp snooping mrouter [interface *vlan_id***]**	vlan_id: (1..4094)	Показать информацию об изученных многоадресных маршрутизаторах в указанной группе VLAN.
show ip igmp snooping interface *vlan_id*	vlan_id: (1..4094)	Показать 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)	Показать информацию об изученных многоадресных группах, участвующих в групповой рассылке.
show ip igmp snooping cpe vlans [vlan *vlan_id***]**	vlan_id: (1..4094)	Показать таблицу соответствий между VLAN оборудования, установленного у пользователя, и VLAN для телевещания.
show ip igmp snooping authorization-cache [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Вывести перечень авторизованных IGMP-групп на всех интерфейсах коммутатора, либо только на заданном интерфейсе.
clear ip igmp snooping authorization-cache [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Очистить таблицу авторизованных IGMP-групп на всех интерфейсах коммутатора, либо только на заданном интерфейсе.

Примеры выполнения команд

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

```
console# configure
console (config)# ip igmp snooping
console (config-if)# ip igmp snooping vlan 6 mrouter learn pim-dvmrp
console (config)# interface vlan 6
console (config-if)# ip igmp snooping query-interval 100
console (config-if)# ip igmp robustness 4
console (config-if)# ip igmp query-max-response-time 15
```

5.19.2. 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 153 – Команды режима конфигурации интерфейса VLAN

Команда	*Значение/Значение по умолчанию*	*Описание*
bridge multicast mode {mac-group | ipv4-group | ipv4-src-group}	—/mac-group	Задать 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		Установить значение по умолчанию.
bridge multicast address {*mac_multicast_address* | *ip_multicast_address*} **[{add | remove} {gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **fortygigabitethernet** *fo_port* | **port-channel** *group*}]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Добавить 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* }		Удалить групповой MAC-адрес из таблицы.
bridge multicast forbidden address {*mac_multicast_address* | *ip_multicast_address*} **[{add | remove} {gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **fortygigabitethernet** *fo_port* | **port-channel** *group*}]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Запретить 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* }		Удалить запрещающее правило для группового MAC-адреса.
bridge multicast forward-all {add | remove} {gigabitethernet *gi_port* | **tengigabitethernet** *te_port* | **fortygigabitethernet** *fo_port* | **port-channel** *group*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48) По умолчанию передача всех	Разрешить 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	многоадресных пакетов запрещена.	Восстановить значение по умолчанию.
bridge multicast forbidden forward-all {add | remove} {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48). По умолчанию портам не запрещено динамически присоединяться к многоадресной группе.	Запретить 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		Восстановить значение по умолчанию.
bridge multicast ip-address *ip_multicast_address* **{add | remove} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Зарегистрировать 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*		Удалить групповой IP-адрес из таблицы.
bridge multicast forbidden ip-address *ip_multicast_address* **{add | remove} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Запретить 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*		Восстановить значение по умолчанию.
bridge multicast source *ip_address* **group** *ip_multicast_address* **{add | remove} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Установить 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*		Восстановить значение по умолчанию.
bridge multicast forbidden source *ip_address* **group** *ip_multicast_address* **{add | remove} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Установить 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*		Восстановить значение по умолчанию.

bridge multicast ipv6 mode {mac-group | ip-group | ip-src-group}	—/mac-group	Задать 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		Установить значение по умолчанию.
bridge multicast ipv6 ip-address *ipv6_multicast_address* **{add | remove} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Зарегистрировать 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*		Удалить групповой IP-адрес из таблицы.
bridge multicast ipv6 forbidden ip-address *ipv6_multicast_address* **{add | remove} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Запретить 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*		Восстановить значение по умолчанию.
bridge multicast ipv6 source *ipv6_address* **group** *ipv6_multicast_address* **{add | remove} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Установить 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*		Восстановить значение по умолчанию.
bridge multicast ipv6 forbidden source *ipv6_address* **group** *ipv6_multicast_address* **{add | remove} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Установить 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*		Восстановить значение по умолчанию.

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

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

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

Таблица 154 – Команды режима конфигурации интерфейса Ethernet, VLAN, 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 155 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Описание*
bridge multicast filtering	—/отключено	Включить фильтрацию групповых адресов.
no bridge multicast filtering		Отключить фильтрацию групповых адресов.
mac address-table aging-time *seconds* **{vlan** *vlan_id***}**	seconds: (10..1000000)/300 секунд	Задать время хранения MAC-адреса в таблице глобально или для определенного VLAN.
no mac address-table aging-time {*seconds***} [vlan** *vlan_id***]**		Установить 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 {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***} [permanent | delete-on-reset | delete-on-timeout | secure]**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Добавить 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*		Удалить 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)	Определить 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***]**		Установить значение по умолчанию.
mac address-table lookup-length *length*	length: (1..8)/3	Задать размер области MAC-адресов в алгоритме хеширования. Изменения вступают в действие после рестарта коммутатора.
no mac address-table lookup-length		Установить значение по умолчанию. Изменения вступают в действие после рестарта коммутатора.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 156 – Команды режима Privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Описание***
clear mac address-table {dynamic | secure} [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	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 157 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Описание*
show mac address-table [dynamic | static | secure] [vlan *vlan_id***] [interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}] [address** *mac_address***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Показать таблицу MAC-адресов для указанного интерфейса либо всех интерфейсов. - **dynamic** — просмотр только динамических записей; - **static** — просмотр только статических записей; - **secure** — просмотр только безопасных записей; - *vlan_id* — идентификационный номер VLAN; - mac-address — MAC-адрес.
show mac address-table count [vlan *vlan_id***] [interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Показать 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)	Показать 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)	Показать конфигурацию фильтра групповых адресов для указанного VLAN. - *vlan_id* — идентификационный номер VLAN.
show bridge multicast unregistered [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Показать конфигурацию фильтра для незарегистрированных групповых адресов.
show bridge multicast mode [vlan *vlan_id***]**	vlan_id: (1..4094)	Показать режим групповой адресации для указанного интерфейса либо всех интерфейсов VLAN. - *vlan_id* — идентификационный номер VLAN.
show bridge multicast reserved-addresses	—	Отобразить правила, установленные для групповых зарезервированных адресов.

Примеры выполнения команд

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

```
console # configure
console(config) # mac address-table aging-time 450
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
```

5.19.3. 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 158 – 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 {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Регистрирует групповой IPv6-адрес в таблице групповой адресации и статически добавляет/удаляет интерфейсы из группы для текущей VLAN. - *ipv6_multicast_address* – групповой IPv6-адрес; Перечисление интерфейсов осуществляется через «–» и «,».

no ipv6 mld snooping vlan *vlan_id* **static** *ipv6_multicast_address* **[interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**		Удаляет групповой IP-адрес из таблицы.
ipv6 mld snooping vlan *vlan_id* **forbidden mrouter interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Добавляет правило, запрещающее портам из списка регистрироваться как MLD-mrouter.
no ipv6 mld snooping vlan *vlan_id* **forbidden mrouter interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_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 {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Добавляет список mrouter-портов.
no ipv6 mld snooping vlan *vlan_id* **mrouter interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**		Удаляет mrouter-порты.
ipv6 mld snooping vlan *vlan_id* **immediate-leave [interface {gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group*}]**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); -/выключено	Включить процесс MLD Snooping Immediate-Leave на текущей VLAN. - **interface** – при использовании данного параметра механизм fast-leave срабатывает только на указанных интерфейсах (при условии, что процесс MLD Snooping Immediate-Leave не включен глобально на текущей VLAN).
no ipv6 mld snooping vlan *vlan_id* **immediate-leave [interface {gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* | port-channel *group*}]**		Отключить процесс MLD Snooping Immediate-Leave на текущей VLAN или указанном интерфейсе.
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 159 – 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 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 160 – 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.

5.19.4. Функции ограничения multicast-трафика

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 161 – Команды режима глобальной конфигурации

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

Команды режима конфигурации multicast-профиля

Вид запроса командной строки режима конфигурации multicast-профиля:

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

Таблица 162 – Команды режима конфигурации multicast-профиля

Команда	*Значение/Значение по умолчанию*	*Действие*
match ip *low_ip* **[***high_ip***]**	*low_ip:* валидный multicast-адрес; *high_ip:* валидный multicast-адрес	Задает соответствие профиля указанному диапазону IPv4 multicast-адресов.
no match ip *low_ip* **[***high_ip***]**		Удаляет соответствие профиля указанному диапазону IPv4 multicast-адресов.
match ipv6 *low_ipv6* **[***high_ipv6***]**	*low_ipv6:* валидный IPv6 multicast-адрес; *high_ipv6:* валидный IPv6 multicast-адрес	Задает соответствие профиля указанному диапазону IPv6 multicast-адресов.
no match ipv6 *low_ipv6* **[***high_ipv6***]**		Удаляет соответствие профиля указанному диапазону IPv6 multicast-адресов.
permit	-/no permit	В случае несоответствия одному из заданных диапазонов, IGMP-report будут пропускаться.
no permit		В случае несоответствия одному из заданных диапазонов, IGMP-report будут отбрасываться.

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet

Вид запроса командной строки режима конфигурации интерфейса:

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

Таблица 163 – Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
multicast snooping max-groups *number*	number (1..1000)/-	Ограничивает количество одновременно просматриваемых multicast-групп для интерфейса.
no multicast snooping max-groups		Снимает ограничение на количество одновременно просматриваемых групп для интерфейса.
multicast snooping add *profille_name*	profile name: (1..32) символов	Привязывает указанный multicast-профиль к интерфейсу.
multicast snooping remove {*profille_name* **| all}**		Удаляет соответствие multicast-профиля (всех multicast-профилей) интерфейсу.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 164 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show multicast snooping groups count	-	Отображает информацию для всех портов о текущем количестве зарегистрированных групп, а также максимальное возможное количество.
show multicast snooping profile [*profille_name***]**	profile name: (1..32) символов	Отображает информацию о сконфигурированных multicast-профилях.

5.19.5. RADIUS авторизация запросов IGMP

Данный механизм позволяет производить авторизацию запросов протокола IGMP с помощью RADIUS-сервера. Для обеспечения надежности и распределения нагрузки может использоваться несколько RADIUS-серверов. Выбор сервера для отправки очередного запроса авторизации происходит случайным образом. Если сервер не ответил, он помечается как временно нерабочий, и перестает участвовать в механизме опроса на определенный период, а запрос отсылается на следующий сервер.

Полученные авторизационные данные хранятся в кэш-памяти коммутатора в течение заданного периода времени. Это позволяет ускорить повторную обработку IGMP-запросов. Параметры авторизации включают в себя:

- MAC-адрес клиентского устройства;
- Идентификатор порта коммутатора;
- IP-адрес группы;
- Решение о доступе - deny/permit.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 165 – Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
ip igmp snooping authorization cache-timeout *timeout*	timeout: (0..10000) мин/0	Установить время жизни в кэше. Если значение равно нулю — отсчёт времени жизни отключен (запись не удаляется со временем).

no ip igmp snooping authorization cache-timeout		Установить значение по умолчанию.

Команды режима конфигурирования интерфейса (диапазона интерфейсов) Ethernet

Вид запроса командной строки режима конфигурирования интерфейса:

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

Таблица 166 – Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
multicast snooping authorization radius [required]	—/отключена	Включить авторизацию через RADIUS-сервер. Если указан параметр **required**, то в случае недоступности всех RADIUS-серверов IGMP-запросы игнорируются. В противном случае IGMP-запрос будет обработан даже при отсутствии ответа сервера.
no multicast snooping authorization		Отключить авторизацию.
multicast snooping authorization forwarding-first	—/отключена	Включить предварительную обработку IGMP-запросов на порту до ответа RADIUS-сервера. При получении ответа от сервера в случае положительного ответа подписка остается, в случае отрицательного — удаляется, если дополнительно настроена функция **ip igmp snooping immediate-leave**.
no multicast snooping authorization forwarding-first		Восстановить значение по умолчанию.

Команды режима EXEC

Все команды доступны только для привилегированного пользователя.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 167 – Команды режима EXEC

Команда	*Значение*	*Действие*
show ip igmp snooping authorization-cache [gigabitethernet *gi_port* **| tengigabitethernet te**_*port* **]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Отобразить содержимое кэша авторизации IGMP. Если в команде указан интерфейс — то отображаются только те группы, которые зарегистрированы на указанном интерфейсе.
clear ip igmp snooping authorization-cache [gigabitethernet *gi_port* **| tengigabitethernet te**_*port* **]**	gi_port: (1..8/0/1..24); te_port: (1..8/0/1..4).	Очистить кэш авторизации. Если в команде указан интерфейс — очищаются записи кэш для указанного интерфейса. Если интерфейс не указан — кэш очищается полностью.

5.20. Маршрутизация многоадресного трафика

5.20.1. 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 168 – 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	Применить фильтрацию регистрационных сообщений PIM. - *acc_list* — список многоадресных префиксов, задаваемый с помощью стандартного ACL.
no ip pim accept-register list		Отключить фильтрацию.
ipv6 pim accept-register list *acc_list*	acc_list: (0..32) символа	Применить фильтрацию регистрационных сообщений PIM для IPv6. - *acc_list* — список многоадресных префиксов, задаваемый с помощью стандартного ACL.
no ipv6 pim accept-register list		Отключить фильтрацию.
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		Отключить данный параметр.

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		Отключить данный параметр.
ip pim dm {range *multicast_subnet* **| default}**	—	Включить маршрутизацию заданного диапазона мультикастных групп в режиме PIM-DM. - *multicast_subnet* — многоадресная подсеть; - **default** — указать диапазон в 224.0.1.0/24. **Команду можно ввести несколько раз, задав несколько диапазонов.**
no ip pim dm {range *multicast_subnet* **| default}**		Отключить данный параметр.
ip pim rp-address *unicast_address* **[***multicast_subnet***]**	—	Создать статическую 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***]**		Удалить статическую RP или удалить RP для указанной подсети.
ipv6 pim rp-address *ipv6_unicast_address* **[***ipv6_multicast_subnet***]**	—	Создать статическую 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***]**		Удалить статическую RP или удалить 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	Создать 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*		Отключить данный параметр.
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	Создать 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*		Отключить данный параметр.
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]		Отключить данный параметр.
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]**	—	Отключить данный параметр.
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 169 – Команды режима конфигурации интерфейса Ethernet, VLAN, группы портов

Команда	***Значение/ Значение по умолчанию***	***Действие***
ip (ipv6) pim	—/включено	Включить PIM на интерфейсе.
no ip (ipv6) pim		Выключить PIM на интерфейсе.
ip (ipv6) pim bsr-border	—/отключено	Прекратить передачу BSR-сообщений с интерфейса.
no ip pim bsr-border		Отключить данный параметр.
ip (ipv6) pim dr-priority *priority*	priority: (0..4294967294)/1	Указать приоритет 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		Вернуть значение по умолчанию.
ip ip (ipv6) pim hello-interval *secs*	secs: (1..18000)/30 сек	Указать период отправки hello-пакетов. - *sec* — период отправки hello-пакетов.
no ip (ipv6) pim hello-interval		Вернуть 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		Вернуть значение по умолчанию.
ip (ipv6) pim neighbor-filter *acc_list*	acc_list: (0..32) символа	Фильтровать входящие PIM-сообщения. - *acc_list* — список адресов, на основе которых производится фильтрация.
no ip (ipv6) pim neighbor-filter		Отключить данный параметр.
ip pim passive	—/disable	Включить пассивный режим на интерфейсе. Этот интерфейс не будет отправлять и принимать сообщения PIM от других маршрутизаторов PIM. Настройка никак не влияет на сообщения IGMP.
no ip pim passive		Выключить пассивный режим.
ip igmp static-group *group_address* **[source** *source_addr***]**	—	Включить статический запрос multicast-группы на интерфейсе. - *group-address* — IP-адрес группы; - *source-addr* — IP-адрес источника группы. **На интерфейсе должен быть включен PIM.**
no ip igmp static-group *group_addr* **[source** *source_addr***]**		Выключить статический запрос multicast-группы.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 170 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip (ipv6) pim rp mapping [*RP_addr***]**	—	Отобразить активные RP, связанные с маршрутной информацией. - *RP_addr* — IP-адрес.
show ip (ipv6) pim neighbor [detail] [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***| vlan** *vlan_id***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094).	Отобразить информацию о PIM-соседях.
show ip (ipv6) pim interface [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id* **|state-on | state-off]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Отобразить 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***]**	—	Отобразить таблицу привязки многоадресных групп. - *group-address* — адрес группы.
show ip (ipv6) pim counters	—	Отобразить содержимое PIM-счетчиков.
show ip (ipv6) pim bsr election	—	Отобразить информацию о BSR.
show ip (ipv6) pim bsr rp-cache	—	Отобразить информацию об изученных кандидатах в RP.
show ip (ipv6) pim bsr candidate-rp	—	Отобразить состояние кандидатов в RP.
clear ip (ipv6) pim counters	—	Обнулить 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
```

5.20.2. Функция PIM Snooping

Функция PIM Snooping используется в сетях, где коммутатор испольняет роль L2 устройства между PIM-маршрутизаторами.

Основной задачей PIM Snooping является предоставление многоадресного трафика только для тех портов, с которых были получен PIM Join, PIM Register.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 171 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip pim snooping	-/disabled	Разрешить использование функции PIM Snooping коммутатором.
no ip pim snooping		Запретить использование функции
ip pim snooping vlan *vlan_id*	vlan_id: (1..4094)	Разрешает использование функции PIM Snooping коммутатором для данного интерфейса VLAN. *vlan_id* – идентификационный номер VLAN.
no ip pim snooping vlan *vlan_id*		Запрещает использование функции PIM Snooping коммутатором для данного интерфейса VLAN.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 172 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip pim snooping	-	Показывает общую информацию о настройках
show ip pim snooping vlan *vlan_id*	vlan_id: (1..4094)	Показывает статистику контроля многоадресного трафика в данной vlan
show ip pim snooping groups	-	Показывает список зарегистрированный групп
sh ip pim snooping neighbors	-	Показывает список зарегистрированных участников PIM

5.20.3. Протокол MSDP

Протокол обнаружения источников многоадресной рассылки (MSDP) используется для обмена информацией об источниках мультикаста между разными PIM-доменами. MSDP-соединение обычно устанавливается между RP каждого домена.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 173 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
router msdp	-	Включает протокол MSDP и переходит в режим его конфигурации.
no router msdp		Останавливает протокол MSDP и удаляет всю его конфигурацию.

Команды режима конфигурации протокола MSDP

Вид запроса командной строки в режиме конфигурации протокола MSDP:

```
console(config-msdp)#
```

Таблица 174 – Команды режима конфигурации протокола MSDP

Команда	*Значение/Значение по умолчанию*	*Действие*
connect-source *ip_address*	-	Назначить IP-адрес, который будет использован в качестве исходящего при соединении с MSDP-пиром.
no connect-source		Установить значение по умолчанию.
description *text*	text: (1..160) символа	Задать описание MSDP-пира.
no description		Удалить описание.
mesh-group *name*	name: (1..31) символа	Добавить соседа к MESH-группе.
no mesh-group		Удалить соседа.
sa-filter { in | out } *sec_num* **{ permit | deny } [rp-address** *ip_addr_rp* **| group-address** *ip_addr_gr* **| source-address** *ip_addr_src* **]**	sec_num: (0..4294967294)	Создать правило фильтрации SA-сообщений: - **permit –** разрешающее правило фильтрации; - **deny –** запрещающее правило фильтрации; - sec_num **–** номер секции правила; - ip_addr_rp – фильтрация по адресу RP; - ip_addr_gr – фильтрация по адресу группы; - ip_addr_src - фильтрация по адресу источника мультикаста.
no sa-filter { in | out } *sec_num*		Удаляет созданную секцию правила.
shutdown	-/disable	Административно выключает сессию с MSDP-пиром, не удаляя его конфигурации.
no shutdown		Установить значение по умолчанию.

Команды режима конфигурации MSDP-пира

Вид запроса командной строки в режиме конфигурации MSDP-пира:

```
console(config-msdp)#
```

Таблица 175 – Команды режима конфигурации MSDP-пира

Команда	*Значение/Значение по умолчанию*	*Действие*
connect-source *ip_address*	-	Назначить IP-адрес, который будет использован в качестве исходящего при соединении с MSDP-пиром
no connect-source		Установить значение по умолчанию
description *text*	text: (1..160) символа	Задать описание MSDP-пира
no description		Удалить описание
mesh-group *name*	name: (1..31) символа	Добавить соседа к MESH-группе
no mesh-group		Удалить соседа
sa-filter { in | out } *sec_num* **{ permit | deny } [rp-address** *ip_addr_rp* **| group-address** *ip_addr_gr* **| source-address** *ip_addr_src* **]**	sec_num: (0..4294967294)	Создать правило фильтрации SA-сообщений - **permit –** разрешающее правило фильтрации - **deny –** запрещающее правило фильтрации - sec_num **–** номер секции правила - ip_addr_rp – фильтрация по адресу RP - ip_addr_gr – фильрация по адресу группы - ip_addr_src - фильрация по адресу источника мультикаста

no sa-filter { in | out } *sec_num*		Удаляет созданную секцию правила
shutdown	-/disable	Административно выключает сессию с MSDP-пиром, не удаляя его конфигурации
no shutdown		Установить значение по умолчанию

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 176 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip msdp peers [*ip_addr* **]**	-	Показывает информацию о настроенных пирах, статусе соединения, настройках пиров, а также статистику обмена сообщениями протокола MSDP - ip_addr – IP-адрес пира
show ip msdp source-active	-	Показывает содержимое кэша SA.
show ip msdp summary	-	Показывает суммарную информацию протокола MSDP.
clear ip msdp counters	-	Обнуляет счетчики.
clear ip msdp peers [*ip_add* **]**	-	Переустанавливает соединения с MSDP-пирами - *ip_addr* – IP-адрес пира

5.20.4. Функция 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.

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).

Во VLAN-е, в который осуществляется проксирование, IGMP Snooping должен быть отключен.

IGMP Proxy для QinQ трафика:

Для корректной работы функционала необходимо включить Proxy в SVLAN и CVLAN, а также настроить IP-адреса на данных интерфейсах.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 177 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip multicast-routing igmp-proxy	—/по умолчанию функция выключена	Разрешить работу маршрутизации многоадресных данных на сконфигурированных интерфейсах.
no ip multicast-routing igmp-proxy		Запретить 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 178 – Команды режима конфигурации интерфейсов Ethernet, VLAN, группы портов

Команда	*Значение/Значение по умолчанию*	*Действие*
ip igmp-proxy {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel group | vlan** *vlan_id***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Конфигурируемый интерфейс является интерфейсом к нижестоящей сети. Команда назначает связанный uplink-интерфейс, участвующий в маршрутизации.
ip igmp static-group *group-address* **[source** *source-addr***]**	—	Включить статический запрос multicast-группы на интерфейсе. - *group-address* — IP-адрес группы; - *source-addr* — IP-адрес источника группы. **На интерфейсе должен быть включен IGMP Proxy.**

no ip igmp static-group *group-address* **[source** *source-addr***]**		Выключить статический запрос multicast-группы.

Команды режима конфигурации интерфейса VLAN

Вид запроса командной строки режима конфигурации VLAN:

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

Таблица 179 – Команды режима конфигурации интерфейсов VLAN

Команда	***Значение/Значение по умолчанию***	***Действие***
ip igmp-proxy dscp *dscp*	dscp: (0..63)/0	Установить значение DSCP в IP-заголовке для пакетов протокола IGMP, которое будет использоваться коммутатором на интерфейсе VLAN.
no ip igmp-proxy dscp		Установить значение по умолчанию.
ip igmp-proxy cos *cos*	cos: (0..7)/0	Установить значение 802.1p в IP для пакетов протокола IGMP, которое будет использоваться коммутатором на интерфейсе VLAN.
no ip igmp-proxy cos		Установить значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 180 – Команды режима EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show ip mroute [*ip_multicast_address* **[***ip_address***]] [summary]**	—	Просмотреть списки 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* **| gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Показать информацию 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                -    -
```

5.21. Функции управления

5.21.1. 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 181 – 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)	Установить 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***}**		Установить 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 enable)	Установить 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 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 enable authorization {default | *list_name*}		Установить значение по умолчанию.
enable password *password* **[encrypted] [level** *level***]**	level: (1..15)/1; password: (0..159) символов/admin	Установить 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***]**		Установить пароль по умолчанию.
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)	Добавить 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*		Удалить пользователя из локальной базы данных
aaa accounting login start-stop group {radius | tacacs+}	—/по умолчанию ведение учета запрещено	Разрешить ведение учета (аккаунта) для сессий управления. **Разрешено только для пользователей, вошедших в систему по имени и паролю. Для 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 182).**
no aaa accounting login start-stop		Запретить ведение учета (аккаунта) для введенных в CLI команд.

aaa accounting dot1x start-stop group radius	—/по умолчанию ведение учета запрещено	Разрешить 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 182).** **В режиме Multiple sessions сообщения start/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		Установить значение по умолчанию.
ip http authentication aaa login-authentication [login-authorization] [http | https] *method_list*	method_list: (local, none, tacacs, radius)	Определить метод аутентификации при доступе к HTTP-серверу. При установке списка методов дополнительный метод будет применяться только в том случае, когда по основному методу аутентификации возвращена ошибка. - ***method_list* — метод аутентификации:** *local* — по имени из локальной базы данных; *none* — не используется; *tacacs* — использование списков всех серверов TACACS+; *radius* — использование списков всех RADIUS-серверов.
no ip http authentication aaa login-authentication		Установить значение по умолчанию.
aaa authentication mode {chain | break}	—/chain	Установить алгоритм опроса методов аутентификации. - **chain** — после неудачной попытки аутентификации по первому методу в списке следует попытка аутентификации по следующему методу в цепочке; - **break** — после неудачной аутентификации по первому методу процесс аутентификации останавливается. Аутентификация по следующему методу допустима только в случае невозможности аутентификации по предыдущему методу.
aaa accounting commands stop-only group tacacs+	—/по умолчанию ведение учета команд выключено	Включить ведение учета введенных в CLI команд по протоколу Tacacs+.
no aaa accounting commands stop-only group		Установить значение по умолчанию.
aaa accounting update	—/по умолчанию выключено	Включение отправки Interim-Update через регулярные промежутки времени.
no aaa accounting update		Выключение отправки Interim-Update через регулярные промежутки времени.
aaa accounting update periodic *minutes*	minutes: (1..300)/ 1 минута	Указание промежутка времени, через который будет производиться отправка Interim-update.
no aaa accounting update periodic		Установить значение по умолчанию.
aaa authorization commands {default | *list_name*} group *method_list*	list_name: (1..15) символов; method_list: (tacacs, local); —/по умолчанию активен список default и авторизация не осуществляется	Установить способ авторизации вводимых команд. - **default** — редактировать список с именем default, который по умолчанию есть в системе; - *list_name* — имя списка методов авторизации, создаваемого и редактируемого пользователем: - tacacs — метод, позволяющий использовать список TACACS серверов для авторизации; - local — метод, при котором авторизация не осуществляется.

no aaa authorization commands {default | *list_name*}		Восстановить значение по умолчанию. - **default** — сброс списка с именем default к значению по умолчанию; - *list_name* — удалить пользовательский список с именем list_name. **Список с именем default не может быть удален из системы**.
aaa authorization commands {default | *list_name*}	list_name: (1..15) символов; —/default	Активировать список методов авторизации вводимых команд. - **default** — сделать активным список с именем default; - *list_name* — сделать активным соответствующий пользовательский список.
no aaa authorization commands		Восстановить 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 182 – 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	MAC-адрес порта NAS, используемый для сессий с RADIUS-сервером.
Calling-Station-ID (31)	Есть	Есть	MAC-адрес пользователя.
Framed-IP-Address (8)	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 183 – 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.
RTT-Data-Filter	Нет	Есть	Список правил, содержащий в себе ключевые слова ACL (таблица 184)
RTT-Data-Filter-Name	Нет	Есть	Имя ACL. Если не задано, то имеет значение «RADIUS_ACL»

Таблица 184 – Ключевые слова ACL

Ключевое слово	***Описание***
prot	Тип или id протокола. Допустимые значения: - для ***IPV4***: icmp, igmp, ip, tcp, udp, ipinip, egp, igp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipip, pim, l2tp, isis; - для ***IPV6***: icmpv6, tcpv6, udpv6.
mac_src	MAC-адрес источника.
mac_dst	MAC-адрес назначения.
ip_src	IP-адрес источника.
ip_dst	IP-адрес назначения.
ipv6_src	IPv6-адрес источника.
ipv6_dst	IPv6-адрес назначения.
dscp	Значение DCSP-поля (0..63).
ip_precedence	Приоритет IP-трафика (0..7).
tcp_flags	TCP-флаг.
vlan	Порядковый номер VLAN.
icmp_type	Тип сообщений протокола ICMP, используемый для фильтрации ICMP-пакетов (0..255).
icmp_code	Код сообщений протокола ICMP, используемый для фильтрации ICMP-пакетов (0..255).
igmp_type	Тип протокола IGMP.
udp_port_src	UDP-порт источника.
udp_port_dst	UDP-порт назначения.
tcp_port_src	TCP-порт источника.
tcp_port_dst	TCP-порт назначения.
udp_src_start	Начальное значение UDP-порта из диапазона UDP-портов источника.
udp_src_end	Конечное значение UDP-порта из диапазона UDP-портов источника.

udp_dst_start	Начальное значение UDP-порта из диапазона UDP-портов назначения.
udp_dst_end	Конечное значение UDP-порта из диапазона UDP-портов назначения.
tcp_src_start	Начальное значение TCP-порта из диапазона TCP-портов источника.
tcp_src_end	Конечное значение TCP-порта из диапазона TCP-портов источника.
tcp_dst_start	Начальное значение TCP-порта из диапазона TCP-портов назначения.
tcp_dst_end	Конечное значение TCP-порта из диапазона TCP-портов назначения.

Формат записи IPv4 ACL, IPv6 ACL формируется следующим образом: первые четыре слова должны быть записаны через пробел в строгом порядке: acl_type, action (permit или deny), ip_precedence, prot. После записи обязательных параметров остальные параметры записываются в произвольном порядке.

Формат записи MAC ACL формируется следующим образом: первые три слова должны быть записаны через пробел в строгом порядке: acl_type, action (permit или deny), ip_precedence. После записи обязательных параметров остальные параметры записываются в произвольном порядке.

Маска для IP-адреса записывается через «/» без пробелов.

Протокол можно указать как в числовом виде, так и строкой.

Команды режима конфигурации терминала

Вид запроса командной строки в режиме конфигурации терминала:

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

Таблица 185 – Команды режима конфигурации терминальных сессий

Команда	***Значение/Значение по умолчанию***	***Действие***
login authentication {default | *list_name***}**	list_name: (1..12) символов	Задать 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		Установить значение по умолчанию.
enable authentication {default | *list_name***}**	list_name: (1..12) символов	Задать 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		Установить значение по умолчанию.
commands authorization	—/включено	Включить авторизацию команд для терминальной сессии.
no commands authorization		Отключить авторизацию команд для терминальной сессии.

password *password* **[encrypted]**	password: (0..159) символов	Задать пароль для терминала. - **encrypted** — задать зашифрованный пароль (например, пароль в зашифрованном виде, скопированный с другого устройства).
no password		Удалить пароль для терминала.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 186 – Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show authentication methods	—	Показывает информацию об аутентификационных методах на коммутаторе.
show authorization methods	—	Показывает информацию о созданных на коммутаторе методах авторизации команд. Указывает на активный метод.
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 187 – Команды режима EXEC

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

5.21.2. 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 188 – 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, dot1x, igmp-auth, coa, dot1x-eapol, dot1x-mac, all)/all	Добавить 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*}		Удалить указанный сервер из списка используемых RADIUS-серверов.
radius-server attributes framed-ip-address include-in-access-req	—/выключено	Добавить атрибут framed-ip-address (Опция 8) в access-request пакеты. **Значение атрибута заполняется на основе таблиц dhcp snooping или arp. Поиск идет в таблице dhcp-snooping, а затем, если запись не была найдена, в таблице arp.**
no radius-server attributes framed-ip-address include-in-access-req		Установить значение по умолчанию.
radius-server attributes nas-id include-in-access-req [format *word*]	word: (3..32)/%h	Добавить атрибут NAS-Id (опция №32) в Access-Request пакеты. Символы "%h", встречающиеся в форматной строке, заменяются на текущее имя хоста (hostname).
no radius-server attributes nas-id include-in-access-req [format]		Установить значение по умолчанию.
[encrypted] radius-server key [*key***]**	key: (0..128) символов/по умолчанию ключ — пустая строка	Установить ключ, используемый по умолчанию, для аутентификации и шифрования всего обмена данными RADIUS между устройством и окружением RADIUS. - **encrypted** — задать ключ в зашифрованном виде.
no radius-server key		Установить значение по умолчанию.
radius-server timeout *timeout*	timeout: (1..30)/3 сек	Установить интервал ожидания ответа от сервера, используемый по умолчанию.
no radius-server timeout		Установить значение по умолчанию.
radius-server retransmit *retries*	retries: (1..15)/3	Определить количество попыток поиска RADIUS-сервера из списка серверов, используемое по умолчанию. При отказе осуществляется поиск следующего по приоритету сервера из списка.

no radius-server retransmit		Установить значение по умолчанию.
radius-server deadtime *deadtime*	deadtime: (0..2000)/0 мин	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		Установить значение по умолчанию.
radius-server host source-interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan id***}**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id: (1…64); group: (1..48)	Задать интерфейс устройства, IP-адрес которого будет использоваться по умолчанию в качестве адреса источника передаваемого в сообщениях протокола RADIUS.
no radius-server host source-interface		Удалить интерфейс устройства.
radius-server host source-interface-ipv6 {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan id***}**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id: (1…64); group: (1..48)	Задать 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		Удалить интерфейс устройства.
radius server accounting-port *port*	port: (1-65535)	Установить порт регистрации учётных записей на RADIUS-сервере.
no radius server accounting-port		Отменить использование UDP-порта для регистрации учётных записей.
radius server authentication-port *port*	port: (1-65535)	Установить UDP-порт для отправки запросов на аутентификацию учётных записей.
no radius server autentification-port		Отменить использование UDP-порта для запросов на аутентификацию учётных записей.
radius server enable	—	Включить RADIUS-сервер на коммутаторе.
no radius server enable		Выключить RADIUS-сервер на коммутаторе.
radius server group *word*	word: (1-32)	Задать название для группы сервера и перейти в режим ее конфигурирования.
radius server secret key *key* **{ipv4 | ipv6 | default}**	формат ipv4_address: A.B.C.D; формат ipv6_address: X:X:X:X::X; key: (1-128) символа	Установить ключ для использования radius server. default — ключ назначается для использования клиентами, не имеющих определенного ключа.
no radius server secret [ipv4 | ipv6 | default]		Удалить ключ для использования radius server.
radius server secret {ipv4 | ipv6}	формат ipv4_address: A.B.C.D; формат ipv6_address: X:X:X:X::X;	Использовать зашифрованный ключ доступа к серверу для конкретного хоста.
no radius server secret {ipv4 | ipv6}		Удалить ключ для использования radius server.
radius server traps accouting	—	Включить поддержку trap-сообщений на события учётных записей.
no radius server traps accouting		Отключить поддержку trap-сообщений.
radius server traps authentication {failure | success}	—	Включить поддержку trap-сообщений, отображающих результат аутентификации на RADIUS-сервере. **failure —** сбой при попытке аутентификации. **success —** успешно пройденная аутентификация.
no radius server traps authentication		Отключить поддержку trap-сообщений.

radius server user username *username* **group password** *pass*	—	Создать пользователя и назначить для него группу на сервере с заданным паролем использования.
no radius server user username *username*		Удалить пользователя на сервере.

Команды режима конфигурирования radius server группы

Вид запроса командной строки в режиме конфигурирования radius server группы:

```
console(config-radius-server-group)#
```

Таблица 189 – Команды режима конфигурирования radius server группы:

Команда	***Значение/Значение по умолчанию***	***Действие***
acl *acl_name*	acl_name: (1-32) символа	Назначить использование указанного ACL в данной группе.
no acl		Отключить использование указанного ACL в данной группе.
allowed-time-range *range_name*	range_name: (1..32) символа	Назначить период времени time-range на использование группы.
no allowed-time-range		Отключить использование time-range на использование группы.
privilege-level *level*	level: (1-15)/1	Назначить уровень привилегий, на котором будет исполнима конфигурируемая группа.
no privilege-level		Установить значение по умолчанию.

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 190 – Команды режима Privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show radius-servers status	—	Показать статус серверов RADIUS.
show radius-servers [key]	—	Отобразить параметры настройки RADIUS-серверов (команда доступна только для привилегированных пользователей).
show radius server {statistics | group | accounting | configuration | rejected | secret | user}	—	Отобразить 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 :
```

5.21.3. 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 191 – 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*] **[vrf** *vrf_name*]	hostname: (1..158) символов; port: (0..65535)/49; timeout: (1..30) сек; secret_key: (0..128) символов; priority: (0..65535)/0; vrf_name: (1..32) символов	Добавить 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; - *vrf_name* — имя виртуальной области маршрутизации. 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*] **[vrf** *vrf_name*]		
no tacacs-server host {*ip_address* **|** *hostname*} **[vrf** *vrf_name*]		Удалить указанный сервер из списка используемых TACACS-серверов.
tacacs-server key *key*	key: (0..128) символов/по умолчанию ключ — пустая строка	Установить 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*		Установить значение по умолчанию.
no tacacs-server key		Установить значение по умолчанию.
tacacs-server timeout *timeout*	timeout: (1..30)/5 сек	Установить интервал ожидания ответа от сервера, используемый по умолчанию.
no tacacs-server timeout		Установить значение по умолчанию.
tacacs-server host source-interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan id***}** **[vrf** *vrf_name*]	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id (1..64); group: (1..48); vrf_name: (1..32) символов	Задать 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 [vrf *vrf_name*]		Удалить интерфейс устройства.
tacacs-server host source-interface-ipv6 {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan id***}**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id (1..64); group: (1..48)	Задать 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 [vrf *vrf_name*]		Удалить интерфейс устройства.

tacacs-server attributes port {console | telnet | ssh} word	word: (1..160) символов	Настроить формат поля *port*. Используются следующие шаблоны: - %n — номер текущей сессии; - % % — символ %.
no tacacs-server attributes port {console | telnet | ssh}		Удалить формат поля *port*.

Команды режима EXEC

Вид запроса командной строки в режиме EXEC:

```
console#
```

Таблица 192 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show tacacs [*ip_address* **|** *hostname***] [vrf {***vrf_name* **|** *all}***]**	host_name: (1..158) символов; vrf_name: (1..32) символов	Отобразить настройку и статистику для сервера TACACS+. - *ip_address* — IP-адрес TACACS+ сервера; - *hostname* — имя сервера; - *vrf_name* — имя виртуальной области маршрутизации.
show tacacs key [vrf {*vrf_name* **|** *all***]**	vrf_name: (1..32) символов	Отобразить параметры настройки tacacs-серверов.

5.21.4. 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 193 – 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		Отключить поддержку протокола SNMP.
snmp-server community *community* **[ro | rw | su]** [*ipv4_address* **|** *ipv6_address* **|** *ipv6z_address*] **[mask** *mask* **| prefix** *prefix_length*]] **[view** *view_name*] **[vrf** *vrf_name*]	community: (1..20) символов; encrypted_community *:* (1..20) символов; формат ipv4_address: 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) символов vrf-name: (1..32) символов	Установить 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; - **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; - *vrf_name* — имя области виртуальной маршрутизации.
snmp-server community-group *community group_name* [*ipv4_address* **|** *ipv6_address* **|** *ipv6z_address* **[vrf** *vrf_name*]] **[mask** *mask* **| prefix** *prefix_length*]		
encrypted snmp-server community *encrypted_community* **[ro | rw | su]** [*ipv4_address* **|** *ipv6_address* **|** *ipv6z_address*] **[mask** *mask* **| prefix** *prefix_length*]] **[view** *view_name*] **[vrf** *vrf_name*]		
encrypted snmp-server community-group *encrypted_community group_name* [*ipv4_address* **|** *ipv6_address* **|** *ipv6z_address* **[vrf** *vrf_name*]] **[mask** *mask* **| prefix** *prefix_length*]		
no snmp-server community *community* **[***ipv4_address* **|** *ipv6_address* **|** *ipv6z_address*] **[vrf** *vrf_name*]		Удалить параметры для строки сообщества.
no encrypted snmp-server community *community* [*ipv4_address* **|** *ipv6_address* **|** *ipv6z_address*] **[vrf** *vrf_name*]		
snmp-server view *view_name OID* **{included | excluded}**	view_name: (1..30) символов	Создать или редактировать 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***]**		Удалить правило обозрения для SNMP.
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	Создать 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]}**		Удалить SNMP-группу.
snmp-server user *user_name group_name* **{v1 | v2c | v3 | remote {***ip_address* **|** *host***} [vrf** *vrf_name***]}**	user_name: (1..20) символов; group_name: (1..30) символов vrf-name: (1..32) символов	Создать SNMPv3-пользователя. - *user_name* — имя пользователя; - *group_name* — имя группы; - *vrf_name* — имя области виртуальной маршрутизации.
no snmp-server user *user_name* **{v1 | v2c | v3 | remote {***ip_address* **|** *host***} [vrf** *vrf_name***] }**		Удалить SNMPv3-пользователя.
snmp-server filter *filter_name OID* **{included | excluded}**	filter_name: (1..30) символов	Создать или редактировать 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***]**		Удалить правило SNMP-фильтра.
snmp-server host {*ipv4_address* **|** *ipv6_address* **|** *hostname***} [traps | informs] [version {1 | 2c | 3 {noauth | auth | priv}] {***community* **|** *username***} [vrf** *vrf_name***] [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; vrf-name: (1..32) символов	Определить 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; - *vrf_name* — имя области виртуальной маршрутизации.
no snmp-server host {*ipv4_address* **|** *ipv6_address* **|** *hostname***} [vrf** *vrf_name***] [traps | informs]**		Удалить настройки для передачи сообщений уведомления inform и trap SNMPv1/v2/v3-серверу.

snmp-server engineid local {*engineid_string* **| default}**	engineid_string: (5..32) символов	Создать 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		Удалить идентификатор локального SNMP-устройства — engine ID
snmp-server source-interface {traps | informs} {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan_id***} [vrf** *vrf_name* **]**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id: (1..64) group: (1..48) vrf_name: (1..32) символов	Задать интерфейс устройства, IP-адрес которого будет использоваться по умолчанию в качестве адреса источника для обмена сообщениями с SNMP-сервером. - *vrf_name* — определяет имя области виртуальной маршрутизации.
no snmp-server source-interface [traps | informs] [vrf *vrf_name* **]**		Удалить интерфейс устройства.
snmp-server source-interface-ipv6 {traps | informs} {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan id***}**	vlan_id: (1..4094); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id: (1..64); group: (1..48)	Задать интерфейс устройства, IPv6-адрес которого будет использоваться по умолчанию в качестве адреса источника для обмена сообщениями с SNMP-сервером.
no snmp-server source-interface-ipv6 [traps | informs]		Удалить интерфейс устройства.
snmp-server engineid remote {*ipv4_address* **|** *ipv6_address* **|** *hostname***}** *engineid_string* **[vrf** *vrf_name***]**	hostname: (1..158) символов; engineid_string: (5..32) символов; vrf-name: (1..32) символов	Создать идентификатор удаленного SNMP-устройства — engine ID. - *engineid_string* — идентификатор SNMP-устройства; - *vrf_name* — имя области виртуальной маршрутизации.
no snmp-server engineID remote {*ipv4_address* **|** *ipv6_address* **|** *hostname***} [vrf** *vrf_name***]**		Удалить идентификатор удаленного SNMP-устройства — engine ID.
snmp-server enable traps	—/включено	Включить поддержку SNMP trap-сообщений.
no snmp-server enable traps		Отключить поддержку SNMP trap-сообщений.
snmp-server enable traps authentication	—/включено	Включить отправку SNMP trap-сообщений при неудачной попытке аутентификации.
no snmp-server enable traps authentication		Отключить отправку SNMP trap-сообщений.
snmp-server enable traps [erps | link-status]	—/включено	Включить отправку SNMP trap-сообщений: **- erps** протокола ERPS; - **link-status —** состояния интерфейсных линков.
no snmp-server enable traps [erps | link-status]		Отключить отправку SNMP trap-сообщений: **- erps** протокола ERPS; - **link-status —** состояния интерфейсных линков.
snmp-server enable traps flex-link	—/ включено	Включить отправку SNMP trap-сообщений при изменении состояния пары flex-link интерфейсов**.**
no snmp-server enable traps flex-link		Отключить отправку SNMP trap сообщений при изменении состояния пары flex-link-интерфейсов.
snmp-server enable traps mac-notification change	—/отключено	Включить отправку SNMP trap-сообщений при изменении в таблице изученных MAC-адресов.

no snmp-server enable traps mac-notification change		Отключить отправку SNMP trap-сообщений при изменении в таблице изученных MAC-адресов.
snmp-server enable traps mac-notification flapping	—/включено	Включить отправку SNMP trap-сообщений при обнаружении флаппинга MAC-адресов.
no snmp-server enable traps mac-notification flapping		Отключить отправку SNMP trap-сообщений при обнаружении флаппинга MAC-адресов.
snmp-server enable traps ospf	—/включено	Включить отправку SNMP trap-сообщений протокола OSPF.
no snmp-server enable traps ospf		Отключить отправку SNMP trap-сообщений.
snmp-server enable traps ipv6 ospf	—/включено	Включить отправку SNMP trap-сообщений протокола OSPF (IPv6).
no snmp-server enable traps ipv6 ospf		Отключить отправку SNMP trap-сообщений.
snmp-server enable traps dhcp-snooping limit clients	—/отключено	Включить отправку SNMP trap-сообщений при достижении предельного количества подключенных DHCP-клиентов.
no snmp-server enable traps dhcp-snooping limit clients		Отключить отправку SNMP trap-сообщений.
snmp-server enable traps transceiver-alarm	—/отключено	Включить отправку SNMP trap-сообщений на регистрацию события изменений параметров SFP с DDM. **Состояние считывается раз в 60 секунд. Может принимать значения W — Warning, E — Error, OK.**
no snmp-server enable traps transceiver-alarm		Установить значение по умолчанию.
snmp-server trap authentication	—/разрешено	Разрешить передавать сообщения trap-серверу, который не прошел аутентификацию.
no snmp-server trap authentication		Запретить передавать сообщения trap-серверу, который не прошел аутентификацию.
snmp-server contact *text*	text: (1..160) символов	Определить контактную информацию устройства.
no snmp-server contact		Удалить контактную информацию устройства.
snmp-server location *text*	text: (1..160) символов	Определить информацию о местоположении устройства.
no snmp-server location		Удалить информацию о местоположении устройства.
snmp-server set *variable_name name1 value1* **[***name2 value2* **[…]]**	variable_name, name, value должны задаваться в соответствии со спецификацией	Установить значения переменных в базе данных MIB коммутатора. - *variable_name* — имя переменной; - *name*, *value* — пары соответствий имя — значение.
snmp-server enable traps cpu notification	—/отключено	Включить отправку SNMP trap-сообщений о срабатывании порога загрузки CPU.
no snmp-server enable traps cpu notification		Отключить отправку SNMP trap-сообщений о срабатывании порога загрузки CPU.
snmp-server enable traps cpu recovery-notification	—/отключено	Включить отправку SNMP trap-сообщений о восстановлении порога загрузки CPU.
no snmp-server enable traps cpu recovery-notification		Отключить отправку SNMP trap-сообщений о восстановлении порога загрузки CPU.
snmp-server enable traps memory notification	—/отключено	Включить отправку SNMP trap-сообщений о срабатывании порога для объема свободного места в RAM.
no snmp-server enable traps memory notification		Отключить отправку SNMP trap-сообщений о срабатывании порога для объема свободного места в RAM.
snmp-server enable traps memory recovery-notification	—/отключено	Включить отправку SNMP trap-сообщений о восстановлении порога для объема свободного места в RAM.
no snmp-server enable traps memory recovery-notification		Отключить отправку SNMP trap-сообщений о восстановлении порога для объема свободного места в RAM.

snmp-server enable traps sensor notification	—/отключено	Включить отправку SNMP trap-сообщений о срабатывании порога для значения датчиков.
no snmp-server enable traps sensor notification		Отключить отправку SNMP trap-сообщений о срабатывании порога для значения датчиков.
snmp-server enable traps sensor recovery-notification	—/отключено	Включить отправку SNMP trap-сообщений о восстановлении порога для значения датчиков.
no snmp-server enable traps sensor recovery-notification		Отключить отправку SNMP trap-сообщений о восстановлении порога для значения датчиков.
snmp-server enable traps storage notification	—/отключено	Включить отправку SNMP trap-сообщений о срабатывании порога для объема свободного места на встроенной флеш-памяти.
no snmp-server enable traps storage notification		Отключить отправку SNMP trap-сообщений о срабатывании порога для объема свободного места на встроенной флеш-памяти.
snmp-server enable traps storage recovery-notification	—/отключено	Включить отправку SNMP trap-сообщений о восстановлении порога для объема свободного места на встроенной флеш-памяти.
no snmp-server enable traps storage recovery-notification		Отключить отправку SNMP trap-сообщений о восстановлении порога для объема свободного места на встроенной флеш-памяти.
snmp-server description *description*	description: (1..160) символов;	Изменить значение поля sysDescr для внешнего SNMP-запроса.
no snmp-server description		Вернуть значение по умолчанию поля sysDescr.

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

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

Таблица 194 – Команды режима конфигурации интерфейса Ethernet

Команда	***Значение/Значение по умолчанию***	***Действие***
snmp trap link-status	—/включено	Включить отправку SNMP trap-сообщений при изменении состояния настраиваемого порта.
no snmp trap link-status		Выключить отправку SNMP trap-сообщений при изменении состояния настраиваемого порта.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 195 – Команды режима Privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show snmp	—	Показать статус SNMP-соединений.
show snmp engineID	—	Показать идентификатор локального SNMP-устройства — engineID.

show snmp views [*view_name*]	view_name: (1..30) символов	Показать правила обозрения SNMP.
show snmp groups [*group_name*]	group_name: (1..30) символов	Показать SNMP-группы.
show snmp filters [*filter_name*]	filter_name: (1..30) символов	Показать SNMP-фильтры.
show snmp users [*user_name*]	user_name: (1..30) символов	Показать SNMP-пользователей.
show snmp vrf {name | all}	VRF name: (1..32) символов	Показать настройки SNMP для указанного VRF.

5.21.5. 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 196 – 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 197 – 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 198 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show rmon statistics {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Показывает статистику интерфейса Ethernet, либо группы портов, используемую для удаленного мониторинга.
show rmon collection stats [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_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 199 – 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               Rustel
```

Таблица 200 – 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: Rustel
Interface: gi0/1             Interval: 1800
Requested samples: 50        Granted samples: 50

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

Таблица 201 – 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 202 – 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 203 – 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 204 – 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 205 – Описание результатов

Параметр	*Описание*
Index	Индекс, уникально идентифицирующий запись.

Description	Комментарий, описывающий событие.
Time	Время создания записи.

5.21.6. 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.

ACL per VLAN работает только в режиме «acl-sqinq»

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 206 – 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 rustel_manag
console (config-macl)#
```

Таблица 207 – Команды режима конфигурации списка доступа для управления

Команда	*Значение/Значение по умолчанию*	*Действие*
permit [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| oob | vlan** *vlan_id*] **[service** *service* **] [ace-priority** *index*]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094) service: (telnet, snmp, http, https, ssh); index: (1..65535)	Задает разрешающее условие для управляющего списка доступа. - *service* – тип доступа. - *index* – приоритет правила.
permit ip-source {*ipv4_address* **|** *ipv6_address/prefix_length***} [mask {***mask* **|** *prefix_length***}] [gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| oob | vlan** *vlan_id*] **[service** *service*] **[ace-priority** *index*]		
deny [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| oob | vlan** *vlan_id*] **[service** *service*] **[ace-priority** *index*]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094); service: (telnet, snmp, http, https, ssh); index: (1..65535)	Задает запрещающее условие для управляющего списка доступа. - *service* – тип доступа, - *index* – приоритет правила.
deny ip-source {*ipv4_address* **|** *ipv6_address/prefix_length***} [mask {***mask* **|** *prefix_length***}] [gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| oob | vlan** *vlan_id*] **[service** *service*] **[ace-priority** *index*]		
remove ace-priority *index*	index: (1..65535)	Удалить условие из списка доступа.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 208 – 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.

5.21.7. Настройка доступа

5.21.7.1. 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 209 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip telnet server	по умолчанию Telnet-сервер включен	Разрешить удаленное конфигурирование устройства через Telnet.
no ip telnet server		Запретить удаленное конфигурирование устройства через Telnet.
ip ssh server	по умолчанию SSH-сервер отключен	Разрешить 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		Запретить удаленное конфигурирование устройства через SSH.
ip scp server	по умолчанию SCP-сервер отключен	Разрешить копирование файлов из файлового хранилища коммутатора и на него через SCP. **SSH-сервер должен быть включен.**
no ip scp server		Выключить SCP-сервер.
ip ssh port *port_number*	port_number: (1..65535)/22	TCP-порт, используемый SSH-сервером.
no ip ssh port		Установить значение по умолчанию.
ip ssh-client source-interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan_id***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id: (1..64) group: (1..48); vlan_id: (1..4094)	Задать интерфейс для SSH-сессий.
no ip ssh-client source-interface		Удалить интерфейс.
ipv6 ssh-client source-interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan_id***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id: (1..64) group: (1..48); vlan_id: (1..4094)	Задать интерфейс для IPv6 SSH-сессий.
no ipv6 ssh-client source-interface		Удалить интерфейс.

ip ssh pubkey-auth	по умолчанию использование публичного ключа запрещено	Разрешить использование публичного ключа для входящих SSH-сессий.
no ip ssh pubkey-auth		Запретить использование публичного ключа для входящих SSH-сессий.
ip ssh cipher *algorithms*	algorithms: (3des, aes128, aes192, aes256, arcfour, none)/разрешены все алгоритмы, кроме none	Задать список разрешенных алгоритмов шифрования для сервера.
no ip ssh cipher		Восстановить список разрешенных алгоритмов обмена ключами по умолчанию.
ip ssh kex *methods*	methods: (dh-group-exchange-sha1, dh-group1-sha1)/ разрешены все методы	Задать список разрешенных методов обмена ключами для сервера.
no ip ssh kex		Восстановить список разрешенных алгоритмов обмена ключами по умолчанию.
ip ssh password-auth	по умолчанию включено	Включить режим аутентификации по паролю.
no ip ssh password-auth		Отключить режим аутентификации по паролю.
crypto key pubkey-chain ssh	по умолчанию ключ не создан	Войти в режим конфигурации публичного ключа.
crypto key generate dsa	—	Генерировать 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	—	Генерировать 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	—	Импортировать пару ключей DSA. - encrypted — в зашифрованном виде.
encrypted crypto key import dsa		
crypto key import rsa	—	Импортировать пару ключей RSA. - encrypted — в зашифрованном виде.
encrypted crypto key import rsa		
crypto certificate {1 | 2} generate	—	Генерировать SSL-сертификат.
ip http server	по умолчанию HTTP-сервер включен	Разрешить удаленное конфигурирование устройства через web.
no ip http server		Запретить удаленное конфигурирование устройства через web.
ip http port *port*	1..65535/80	Задать порт HTTP-сервера.
no ip http port		Восстановить значение по умолчанию.
ip http secure-server	по умолчанию HTTPS-сервер выключен	Включить HTTPS-сервер.
no ip http secure-server		Выключить HTTPS-сервер.
ip http timeout-policy *seconds* **[http-only | https-only]**	seconds: (0..86400)/600	Задать таймаут HTTP-сессии.
no ip http timeout-policy		Восстановить значение по умолчанию.
ip https certificate {1 | 2}	—/1	Определить активный HTTPS-сертификат.
no ip https certificate		Восстановить значение по умолчанию.
crypto certificate {1 | 2} generate	—	Генерировать SSL-сертификат.
crypto certificate {1 | 2} import		Импортировать SSL-сертификат, назначенный центром сертификации.
no crypto certificate {1 | 2}		Восстановить 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 210 – 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 rustel rsa
console(config-pubkey-key)#
```

Таблица 211 – 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 212 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip ssh	—	Показать 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.	Показать 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]	—	Показать публичные ключи SSH-коммутатора.
show crypto certificate [1 | 2]	—	Отобразить SSL-сертификаты для HTTPS-сервера.

Примеры выполнения команд

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

```
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 rustel rsa
console(config-pubkey-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWlAl4kpqIw9GBRonZQZxjHKcqKL6rMlQ+ZNXfZS
kvHG+QusIZ/76ILmFT34v7u7ChFAE+Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1gkTwml75QR9gH
ujS6KwGN2QWXgh3ub8gDjTSqmuSn/Wd05iDX2IExQWu08licglk02LYciz+Z4TrEU/9FJxwPiVQO
jc+KBXuR0juNg5nFYsY0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA6w9o44t6+AINEICBCCA4YcF6
zMzaT1wefWwX6f+Rmt5nhhqdAtN/4oJfce166DqVX1gWmNzNR4DYDvSzg0lDnwCAC8Qh
Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

5.21.7.2. 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 213 – 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 214 – Команды режима конфигурации терминала

Команда	***Значение/Значение по умолчанию***	***Действие***
speed *bps*	bps: (2400, 9600, 19200, 38400, 57600, 115200)/115200 бод	Установить скорость доступа по локальной консоли (команда доступна только в режиме конфигурации локальной консоли).
no speed		Установить значение по умолчанию.
autobaud	—/включено	Включить автоматическое определение скорости доступа по локальной консоли (команда доступна только в режиме конфигурации локальной консоли).
no autobaud		Выключить автоматическое определение скорости доступа по локальной консоли.
exec-timeout *minutes* [*seconds*]	minutes*:* (0..65535)/10 мин; seconds*:* (0..59)/0 сек	Задать интервал, в течение которого система ожидает ввода пользователя. Если в течение данного интервала пользователь ничего не вводит, то консоль отключается.
no exec-timeout		Установить значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 215 – Команды режима EXEC

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

5.21.7.3. Удаленный запуск команд посредством SSH

Функция позволяет удаленно осуществить выполнение команд на коммутаторе через сессию SSH. Для работы данной функции необходимо, чтобы на коммутаторе был включен SSH-сервер (команда ip ssh server в глобальном режиме конфигурирования).

Ниже показан пример использования функции удаленного запуска команд через SSH.

Выполнить команду `show clock` для коммутатора с IP-адресом 192.168.1.239:

```
username@username-system:~$ ssh -l admin 192.168.1.239 "show clock"
admin@192.168.1.239's password:
*10:12:59 UTC Jun 10 2019
No time source
Time from Browser is disabled
```

Команды, требующие подтверждения (например: write, reload и др.), ждут ввода подтверждений и только потом соединение SSH разрывается.

5.22. 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 216 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
logging on	—/регистрация включена	Включить регистрацию отладочных сообщений и сообщений об ошибках.
no logging on		Выключить 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. таблицу 217); facility: (local0..7)/local7; text: (1..64) символов	Включить 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***}**		Удалить выбранный сервер из списка используемых SYSLOG-серверов.

logging console [*level***]**	level: (см. Таблицу 217)/informational	Включить передачу аварийных или отладочных сообщений выбранного уровня важности на консоль.
no logging console		Выключить передачу аварийных или отладочных сообщений на консоль.
logging buffered [*severity_level***]**	severity_level: (см. Таблицу 217)/informational	Включить передачу аварийных или отладочных сообщений выбранного уровня важности во внутренний буфер.
no logging buffered		Выключить передачу аварийных или отладочных сообщений во внутренний буфер.
logging buffered size *size*	size: (20..1000)/200	Изменить количество сообщений, запоминаемых во внутреннем буфере. Новое значение размера буфера применится после перезагрузки устройства.
no logging buffered size		Установить значение по умолчанию.
logging file [*level***]**	level: (см. таблицу 217)/errors	Включить передачу аварийных или отладочных сообщений выбранного уровня важности в файл журнала.
no logging file		Выключить 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).
logging events spanning-tree port-state-change	—/включено	Включить регистрацию изменения статуса интерфейсов в STP.
no logging events spanning-tree port-state-change		Отключить регистрацию изменения статуса интерфейсов в STP.
logging events spanning-tree topology-change	—/выключено	Включить регистрацию изменений топологии в STP.
no logging events spanning-tree topology-change		Отключить регистрацию изменений топологии в STP.
logging events spanning-tree root-bridge-change	—/выключено	Включить регистрацию смены root bridge.
no logging events spanning-tree root-bridge-change		Выключить регистрацию смены root bridge.
logging cli-commands	—/отключено	Включить логирование введенных в CLI команд.
no logging cli-commands		Отключить логирование введенных в CLI команд.
file-system logging {copy | delete-rename}	По умолчанию регистрация включена	Включить 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}		Выключить регистрацию событий файловой системы.
management logging deny	По умолчанию регистрация включена	Включить регистрацию событий о запрете доступа к управлению коммутатором.
no management logging deny		Выключить регистрацию событий о запрете доступа к управлению коммутатором.
logging aggregation on	—/отключено	Включить контроль агрегации syslog-сообщений.
no logging aggregation on		Отключить агрегацию syslog-сообщений.
logging aggregation aging-time *sec*	sec: (15..3600)/300 секунд	Установить время хранения сгруппированных syslog-сообщений.
no logging aggregation aging-time		Установить значение по умолчанию.
logging service cpu-rate-limits *traffic*	traffic: (http, telnet, ssh, snmp, ip, link-local, arp-	Включить контроль ограничения скорости входящих фреймов для определенного типа трафика.

no logging service cpu-rate-limits *traffic*	switch-mode, arp-inspection, stp-bpdu, other-bpdu, dhcp-snooping, dhcpv6-snooping, igmp-snooping, mld-snooping, sflow, log-deny-aces, vrrp)/—	Отключить логирование.
logging origin-id {string | hostname | ip | ipv6}	—/нет	Задать параметр, который будет использоваться в качестве идентификатора хоста в syslog-сообщениях.
no logging origin-id		Использовать значение по умолчанию.
logging source-interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan *vlan_id*}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id: (1..64) group: (1..48); 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 {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback_id* **| vlan** *vlan_id*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id: (1..64) group: (1..48); 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 217 приведены типы сообщений в порядке убывания их важности.

Таблица 217 – 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 218 – Команда режима Privileged EXEC для просмотра файла журнала и

аварийных событий

Команда	*Значение/Значение по умолчанию*	*Действие*
clear logging	—	Удалить все сообщения из внутреннего буфера.
clear logging file	—	Удалить все сообщения из файла журнала.
show logging file	—	Отобразить состояние журнала, аварийные и отладочные сообщения, записанные в файле журнала.
show logging	—	Отобразить состояние журнала, аварийные и отладочные сообщения, записанные во внутреннем буфере.
show syslog-servers	—	Отобразить 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
```

5.23. Зеркалирование (мониторинг) портов

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

К контролирующему порту применяются следующие ограничения:

– Порт не может быть контролирующим и контролируемым портом одновременно;
– 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;
– Существует ограничение на 7 сессий зеркалирования, по 8 зеркалируемых интерфейсов (портов или VLAN) в каждой.

Зеркалирование VLAN возможно только в первой сессии.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 219 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
port monitor mode {monitor-only | network}	—/monitor-only	Задать режим работы порта - monitor-only — кадры, поступающие на порт, отбрасываются; - network — позволяет вести обмен данными.
no port monitor mode		Вернуть значение по умолчанию.
port monitor remote vlan *vlan_id* **[cos** *priority***] [tx | rx]**	vlan_id: (1..4094); priority: (0..7)/0	Назначить VLAN для удаленного мониторинга (RSPAN), в которую будут помещаться пакеты с контролируемых интерфейсов.
no port monitor remote vlan *vlan_id*		Удалить VLAN для удаленного мониторинга.

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

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

Данные команды нельзя выполнять в режиме конфигурации диапазона интерфейсов Ethernet.

Таблица 220 – Команды доступные в режиме конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
port monitor {remote | gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***} [rx | tx]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4);	Включить функцию мониторинга на настраиваемом интерфейсе. Данный интерфейс будет контролирующим портом для указанного в команде контролируемого порта. - *gi_port, te_port,* fo_port — контролируемый порт; - **rx** — копировать пакеты, принятые контролируемым портом; - **tx** — копировать пакеты, переданные контролируемым портом; При отсутствии параметра rx/tx с контролируемого порта копируются все пакеты. **Функция мониторинга может быть настроена на двух портах одновременно.** **Конфигурация PortChannel в качестве контролирующего интерфейса производится после перевода интерфейса в состояние UP.**
no port monitor {remote | gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **}**		Выключить функцию мониторинга на настраиваемом интерфейсе.

port monitor vlan *vlan_id*	vlan_id: (1..4094)	Включить функцию мониторинга на настраиваемом интерфейсе. Данный интерфейс будет контролирующим портом для указанной VLAN. **Порт мониторинга не должен принадлежать к настраиваемой VLAN.** **Мониторинг VLAN может быть включен лишь в том случае, если в системе настроено не более одного контролирующего порта.** **Если контролирующий порт настроен ранее, то только этот порт может быть использован для мониторинга VLAN.**
no port monitor vlan *vlan_id*		Удалить указанную VLAN из мониторинга.
port monitor remote	—	Включить функцию удаленного мониторинга (RSPAN) на настраиваемом интерфейсе.
no port monitor remote		Выключить функцию удаленного мониторинга (RSPAN) на настраиваемом интерфейсе.

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 221 – Команды, доступные в режиме EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show ports monitor	-	Выводит информацию по контролирующим и контролируемым портам.

Примеры выполнения команд

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

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

- Вывести информацию по контролирующим и контролируемым портам.

```
console# show ports monitor
```

```
Port monitor mode: monitor-only
    RSPAN configuration
RX: VLAN 5, user priority 0
TX: VLAN 5, user priority 0

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

5.24. 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 222 – 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} {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel l** *group* **| loopback** *loopback_id* **| vlan** *vlan_id* **| oob}**	vlan_id: (1..4094) gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); loopback_id: (1..64) group: (1..48)	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 {gigabitethernet gi_port | tengigabitethernet
te_port | fortygigabitethernet fo_port}
console(config-if)#
```

Таблица 223 – Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
sflow flow-sampling *rate id* **[max-header-size** *bytes***]**	rate: (1024..107374823); id: (0..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 224 – Команды, доступные в режиме EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show sflow configuration [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Выводит настройки sflow.
clear sflow statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***]**		Очищает статистику sFlow. Если интерфейс не указан, команда очищает все счетчики статистики sFlow.
show sflow statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_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 flow-sampling 10240 1
console (config-if)# sflow counters-sampling 240 1
```

5.25. 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.

5.25.1. Диагностика медного кабеля

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 225 – Команды диагностики медного кабеля

Команда	*Значение/Значение по умолчанию*	*Действие*
test cable-diagnostics tdr [all | interface gigabitethernet *gi_port* **]**	gi_port: (1..8/0/1..48)	Выполняет виртуальное тестирование кабеля для указанного интерфейса. - **all** – для всех интерфейсов
show cable-diagnostics tdr [interface gigabitethernet *gi_port* **]**	gi_port: (1..8/0/1..48)	Отображает результаты последнего виртуального тестирования кабеля для указанного интерфейса.
test cable-diagnostics tdr-fast [all | interface gigabitethernet *gi_port* **]**	gi_port: (1..8/0/1..48)	Выполняет виртуальное тестирование кабеля с низкой точностью для указанного интерфейса. - **all** – для всех интерфейсов
show cable-diagnostics cable-length [interface gigabitethernet *gi_port***]**	gi_port: (1..8/0/1..48)	Отображает предположительную длину кабеля, подключенного к указанному интерфейсу (если номер порта не задан, то команда выполняется для всех портов). **Интерфейс должен быть активным и работать в режиме 1000Мбит/с или 100Мбит/с. Диагностика поддерживается только на интерфейсах GigabitEthernet.**

Примеры выполнения команд:

- Протестировать порт gi 1/0/1:

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

```
5324#test cable-diagnostics tdr interface gi0/1
..
Cable on port gi1/0/1 is good
```

5.25.2. *Диагностика оптического трансивера*

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

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

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 226 – Команда диагностики оптического трансивера

Команда	***Значение/Значение по умолчанию***	***Действие***
show fiber-ports optical-transceiver [detailed] [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4).	Отображает результаты диагностики оптического трансивера.

Пример выполнения команды:

```
sw1# show fiber-ports optical-transceiver interfaceFortygigabitEthernet1/0/1
```

```
   Port       Temp  Voltage Current Output Input LOS     Transceiver
                                    Power  Power         Type
----------- ------ ------- ------- ------ ----- ---- -------------
  fo1/0/1     OK     OK      OK     N/S    OK    No      Fiber
                             OK            OK    No
                             OK            OK    No
                             OK            OK    No
 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
```

Таблица 227 – 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.

5.25.3. Диагностика индикации интерфейсов

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 228 — Команды диагностики индикации интерфейсов

Команда	*Значение/Значение по умолчанию*	*Действие*
test led port mode { force-on | force-off |force-blink | default [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| all]}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); **/default all**	Включить необходимый режим работы индикации интерфейса - *force-off* — выключен; - *force-on* — горит постоянно; - *force-blink* — мигание; - *default* — режим работы световой индикации портов, описанный в пункте 2.4.4. **Только для устройства RTT-A420-24XG-4QXG.**
show led port mode [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port***]**	—	Отобразить информацию о режиме работы индикации на интерфейсе.

5.26. IP Service Level Agreements (IP SLA)

IP SLA (соглашения об уровне обслуживания в IP-сетях) – технология активного мониторинга, использующаяся для измерения параметров быстродействия компьютерных сетей и качества передачи данных. Активный

мониторинг представляет собой продолжительную циклическую генерацию трафика, сбор информации о его прохождении по сети и ведение статистики.

На данный момент измерение параметров сети может осуществляться с использование протокола ICMP.

При каждом выполнении операции ICMP Echo устройство отправляет ICMP Echo request сообщение на адрес назначения, ожидает получения сообщения ICMP Echo reply в течении заданного интервала времени.

С одной IP SLA операцией можно связать несколько объектов TRACK. Состояние объекта TRACK изменяется в момент изменения состояния IP SLA операции, либо с заданной задержкой.

При изменении состояния трека возможно выполнение макрокоманд. Макрокоманды выполнятются в режиме глобального конфигурирования. Для выполнения команд режима privileged EXEC команды необходимо дополнить префиксом do. Команды создания набора макрокоманд приведены в таблице 36.

Для использования функции IP SLA необходимо выполнить следующие действия:

- Создать операцию icmp-echo и сконфигурировать её.
- Запустить выполнение операции.
- Создать TRACK объект, связанный с конкретной IP SLA операцией и сконфигурировать его.
- При необходимости, создать макросы, выполняемые при изменении состояния объекта TRACK.
- Просмотреть статистику, при необходимости, очистить ее.
- При необходимости, прекратить выполнение операции.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 229 — Команды режима глобальной конфигурации

Команда	*Значение*	*Действие*
ip sla *operation*	operation: (1..64)	Переходит в режим конфигурирования IP SLA операции - operation – номер операции.
no ip sla *operation*		Удаляет IPI SLA операцию. - operation — номер операции. - life – время, в течение которого операция будет выполняться. - start-time — время запуска.
ip sla schedule *operation* **life** *life* **start-time** *start-time*	operation: (1..64); life: (forever); start-time: (now)	Запускает на выполнение IP SLA операцию. - operation — номер операции. - life – время, в течение которого операция будет выполняться. - start-time — время запуска.
no ip sla schedule *operation*		Прекращает выполнение IP SLA операции. - operation — номер операции.
track *object* **ip sla** *operation* **state**	object: (1..64); operation: (1..64)	Создает TRACK объект, который будет отслеживать состояние IP SLA операции. - object — номер TRACK объекта. - operation — номер IP SLA операции.
no track *object* **ip sla**		Удаляет TRACK объект. - object — номер TRACK объекта.
logging events ip sla operation-state-change	-/включено	Включает вывод сообщений об изменении статуса IP SLA операции.
no logging events ip sla operation-state-change		Выключает вывод сообщений об изменении статуса IP SLA операции.
logging events ip sla track-state-change	-/включено	Включает вывод сообщений об изменении статуса трека.
no logging events ip sla track-state-change		Выключает вывод сообщений об изменении статуса трека.

Таблица 230 —Команды режима создания операций IP SLA

Команда	*Значение*	*Действие*
icmp-echo {*A.B.C.D* | *host* } [**source-ip** *A.B.C.D*]	host: (1..158) символов	Переходит в режим конфигурирования ICMP ECHO операции. - *A.B.C.D* — IPv4-адрес узла сети; - *host* — доменное имя узла сети.

Команды режима конфигурирования IP SLA ICMP ECHO операции

Вид запроса командной строки в режиме конфигурирования IP SLA ICMP ECHO:

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

Таблица 231 – Команды режима конфигурирования операции ICMP Echo

Команда	*Значение/Значение по умолчанию*	*Действие*
frequency *secs*	*secs*: (10..500)/10 сек	Устанавливает частоту повторения ICMP ECHO операции. - *secs* – частота, в секундах.
no frequency		Устанавливает значение частоты повторений по умолчанию.
timeout *msecs*	*msecs*: (50..5000)/2000 мс	Устанавливает длину таймаута, по истечении которого, если не пришел ICMP-ответ, операция будет считаться неудачной. - *msecs* – таймаут, в миллисекундах.
no timeout		Устанавливает значение таймаута по умолчанию.
request-data-size *bytes*	*bytes*: (28..1472)/28 байт	Установить количество байт, передаваемых в ICMP-пакете в качестве данных (*payload*). *- bytes – количество байт.*

no request-data-size		Установить значение количества байт по умолчанию.

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

Команды режима конфигурирования трека

Вид запроса командной строки режима конфигурирования трека:

```
console(config-track)#
```

Таблица 232 – Команды режима глобальной конфигурации

Команда	*Значение*	*Действие*
delay {up ***secs*** **down** ***secs*** **/** ***up secs*** **/** ***down secs}***	secs: (1..180)/0	Устанавливает задержку для смены состояния TRACK объекта, при изменении состояния IP SLA операции. - *secs* – задержка, в секундах. - **up** - задержка изменения состояния, при при изменении операции в состояние OK; - **down** — задержка изменения состояния, при изменении операции в состояние Error.
no delay [up] [down]		Удаляет задержку.

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 233 – Команды режима privileged EXEC

Команда	*Значение*	*Действие*
show ip sla operation *[operation]*	operation: (1..64)	Отображает информацию о настроенных IP SLA операциях. - *operation* — номер операции.
show track *[object]*	object: (1..64)	Отображает информацию о настроенных TRACK объектах. - *object* — номер объекта.
clear ip sla counters [operation]	operation: (1..64)	Обнуляет счетчики IP SLA операции. - *operation* — номер операции.

Пример настройки, предназначенной для контроля узла сети с адресом 10.9.2.65 с отправкой icmp запроса каждые 20 секунд, временем ответа на icmp запрос не превышающим 500 мс и размером данных 92 байта; задержка смены состояния TRACK объекта – 3 секунды; при изменении состояния TRACK объекта выполняются макросы TEST_DOWN и TEST_UP:

```
console# configure
console(config)# interface vlan 1
console(config-if)# ip address 10.9.2.80 255.255.255.192
console(config-if)#exit
console(config)#macro name TEST_DOWN track 1 state down
Enter macro commands one per line. End with the character '@'.
int gi1/0/11
no shutdown
@
console(config)#
```

```
console(config)#macro name TEST_UP track 1 state up
Enter macro commands one per line. End with the character '@'.
int gi1/0/11
shutdown
@
console(config)#
console(config)#ip sla 1
console(config-ip-sla)# icmp-echo 10.9.2.65
console(config-ip-sla-icmp-echo)# timeout 500
console(config-ip-sla-icmp-echo)# frequency 20
console(config-ip-sla-icmp-echo)# request-data-size 92
console(config-ip-sla-icmp-echo)# exit
console(config-ip-sla)# exit
console(config)#ip sla schedule 1 life forever start-time now
console(config)#track 1 ip sla 1 state
console(config-track)# delay up 3 down 3
console(config-track)# exit
console(config)#exit
console#
```

Пример вывода статистики для операции ICMP Echo:

```
IP SLA Operational Number: 1
   Type of operation: icmp-echo
   Target address: 10.9.2.65
   Source Address: 10.9.2.80
   Request size (ICMP data portion): 92
   Operation frequency: 20
   Operation timeout: 500
   Operation state: scheduled
   Operation return code: OK
   Operation Success counter: 254
   Operation Failure counter: 38
   ICMP Echo Request counter: 292
   ICMP Echo Reply counter: 254
   ICMP Error counter: 0
```

где

- *Operation state* – текущее состояние операции:
  - *scheduled* – операция выполняется;
  - *pending* – выполнение операции остановлено.
- *Operation return code* – код завершения последней выполненной операции:
  - *OK* – успешное завершение предыдущей операции;
  - *Error* – неудачное завершение последней попытки измерения.
- *Operation Success counter* – количество успешно законченных операций.

- *Operation Failure counter* – количество неудачно законченных операций.
- *ICMP Echo Request counter* – количество проведённых запусков операции.
- *ICMP Echo Request counter* – количество полученных ответов на ICMP запрос.
- *ICMP Error counter* – счётчик, отображающий количество измерительных операций, закончившихся с соответствующим кодом ошибки.

5.27. Электропитание по линиям Ethernet (PoE)

Отдельные модели коммутаторов поддерживают электропитание устройств по линии Ethernet в соответствии с рекомендациями IEEE 802.3af (PoE) и IEEE 802.3at (PoE+) по типу распиновки A.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 234 – Команды режима глобальной конфигурации

Команда	***Значение/ Значение по умолчанию***	***Действие***
power inline limit-mode {port | class}	-/class	Выбор режима ограничения мощности электропитания: - **port** –ограничение устанавливается на основании административных параметров порта; - **class** – ограничение устанавливается на основании класса подключенного устройства
no power inline limit-mode		Возвращает значение по умолчанию
power inline restart auto	-/включено	Включить автоматический рестарт PoE в случае отключения PoE-контроллера.
no power inline restart auto		Установить значение по умолчанию. Отключить автоматический рестарт PoE в случае отключения PoE-контроллера.
power inline usage-threshold *percent*	percent: (1..99)/95	Устанавливает порог потребляемой мощности, при котором формируется информационное сообщение (snmp trap) о превышении порога.
no power inline usage-threshold		Восстанавливает значение порога по умолчанию.
power inline traps enable	-/выключено	Разрешение формирование информационных сообщений для подсистемы PoE.
no power inline traps enable		Возвращает настройки к параметрам по умолчанию.

power inline inrush test disable	-/включено	Включает проверку inrush-тока.
no power inline inrush test disable		Отключает проверку inrush-тока.
power inline disable	-/выключено	Отключает использование PoE. **Настройка вступит в силу только после перезагрузки устройства.**
no power inline disable		Включает использование PoE.

Команды режима конфигурации интерфейса

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

```
console# configure
console(config)# interface gigabitethernet gi_port
console(config-if)#
```

Таблица 235 – Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
power inline {auto | never} [time-range *range_name***]**	range_name : (1..32) символа; -/auto	Команда управляет работой протокола обнаружения PoE-устройств на интерфейсе. -**auto** – разрешает работу протокола обнаружения PoE-устройств на интерфейсе и включает подачу электропитания на интерфейс; -**never** – запрещает работу протокола обнаружения PoE-устройств на интерфейсе и отключает подачу электропитания; -**time-range** – временной интервал, в течение которого питание будет подаваться на интерфейс.
power inline powered-device *pd_type*	pd_type:(1..24) символов/не задано	Добавляет произвольное описание PoE-устройства для помощи в администрировании оборудования.
no power inline powered-device		Удаляет ранее заданное описание PoE-устройства.
power inline priority {critical | high | low}	-/low	Задаёт приоритет интерфейса PoE при управлении электропитанием. - **critical** – устанавливает наивысший приоритет электропитания. Электропитание портов с таким приоритетом будет прекращаться в последнюю очередь при перегрузке системы PoE; - **high** – устанавливает высокий приоритет электропитания; - **low –** устанавливает низкий приоритет электропитания.
no power inline priority		Восстанавливает приоритет по умолчанию.
power inline limit *power*	power: (0..30000)/30000 мВт	Назначает предел мощности электропитания для выбранного порта.
no power inline limit		Восстанавливает предел мощности по умолчанию.

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 236 – Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show power inline [gigabitethernet *gi_port* **| unit** *unit_id***]**	gi_port: (1..8/0/1..8); unit_id : (1..8)	Отображает состояние электропитания интерфейсов, поддерживающих питание по линии PoE. - *unit_id* – номер юнита в стеке.
show power inline consumption [gigabitethernet *gi_port* **| unit** *unit_id***]**	gi_port: (1..8/0/1..8); unit_id : (1..8)	Отображает характеристики потребления мощности PoE-интерфейсов устройства. - *unit_id* – номер юнита в стеке.
show power inline version	-	Отображает версию программного обеспечения контроллера подсистемы PoE.

Примеры выполнения команд

- Показать состояние электропитания всех интерфейсов устройства:

```
console# show power inline
```

```
Power-limit mode: Class based
Usage threshold: 95%
Trap: Disable
Legacy Mode: Disable
Inrush Test: Disable
SW Version: 22.172.3
Unit    Module    Nominal   Consumed   Temp (C)
                  Power (W) Power (W)
---- ------------ --------- ---------- --------
1    RTT-A230-8P-4G-AC     240       219 (91%)  85
     12-port 1G
     Managed
     Switch with
     8 POE+ ports
2    RTT-A230-8P-4G-AC     240       0 (0%)     42
     12-port 1G
     Managed
     Switch with
     8 POE+ ports
Interface    Admin       Oper          Power (W)      Class     Device      Priority
---------- ---------- ----------- ----------------- ----- -------------- --------
gi1/0/1    Auto       On          31.800             4                    low
gi1/0/2    Auto       On          31.800             4                    low
gi1/0/3    Auto       On          31.0               4                    low
gi1/0/4    Auto       On          31.400             4                    low
gi1/0/5    Auto       On          31.500             4                    low
gi1/0/6    Auto       On          31.0               4                    low
gi1/0/7    Auto       On          31.600             4                    low
gi1/0/8    Auto       Fault       0.0                0                    low
```

- Показать состояние электропитания выбранного интерфейса:

```
console# show power inline gi1/0/1
```

```
Interface    Admin       Oper          Power (W)      Class     Device      Priority
---------- ---------- ----------- ----------------- ----- -------------- --------
gi1/0/1    Auto       Searching   0.0                0                    low


Port Status:               Port is off. Detection is in process
Port standard:             802.3AT
Admin power limit (for port power-limit mode): 30.0   watts
Time range:
Operational power limit:   30.0   watts
Spare pair:                Disabled
```

```
Negotiated power:           0 watts (None)
Current (mA):               0
Voltage(V):                 0.0
Overload Counter:           0
Short Counter:              0
Denied Counter:             0
Absent Counter:             0
Invalid Signature Counter: 0
```

Описание отображаемых параметров электропитания приведено в таблице 237.

Таблица 237 – Параметры статуса электропитания

Nominal Power	Номинальная мощность источника питания подсистемы PoE.
Consumed Power	Измеренное значение потребляемой мощности.
Usage Threshold	Пороговое значение потребляемой мощности, при котором формируется информационное сообщение (snmp trap) о превышении порога.
Traps	Отображает разрешение формирование информационных сообщений.
Port	Обозначение интерфейса коммутатора.
Admin	Административное состояние электропитания порта. Возможные значения – auto и never.
Priority	Приоритет управления электропитанием порта. Возможные значения – critical, high, low.
Oper	Оперативное состояние электропитания порта. Возможные значения: Off - питание порта выключено административно; Searching – питание порта включено, ожидание подключения PoE-устройства; On – питание порта включено и есть присоединенное PoE-устройство; Fault – авария питания порта. PoE-устройство запросило мощность большую, чем доступно или потребляемая PoE-устройством мощность превысила заданный предел.
Port standard	Классификация подключенного устройства в соответствии с IEEE 802.3af, IEEE 802.3at.
Overload Counter	Счетчик количества случаев перегрузки по электропитанию.
Short Counter	Счетчик случаев короткого замыкания.
Denied Counter	Счетчик случаев отказа в подаче электропитания.
Absent Counter	Счетчик случаев прекращения электропитания из-за отключения питаемого устройства.
Invalid Signature Counter	Счетчик ошибок классификации подключенных PoE-устройств.

5.28. Функции обеспечения безопасности

5.28.1. 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 238 – Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

Команда	***Значение/Значение по умолчанию***	***Действие***
port security	—/выключено	Включить 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		Отключить функцию защиты на интерфейсе.
port security max *num* **[*voice*]**	num: (0..65536)/1	Задать максимальное количество адресов, которое может изучить порт. При этом из общего лимита адресов вычитается лимит адресов в voice vlan. **- *voice*** — устанавливает максимальное количество адресов, которое может быть изучено в voice-vlan. Лимит адресов в voice-vlan не может превышать общий лимит.
no port security max		Установить 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	Разрешить только маршрутизацию пакетов с указанным MAC-адресом источника.
no port security routed secure-address *mac_address*		Установить значение по умолчанию.

port security {forward | discard | discard-shutdown | discard-shutdown-vlan} [trap *freq***]**	freq: (1..1000000) сек	Включить 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. - **discard-shutdown-vlan** — пакеты с неизученными MAC-адресами источника отбрасываются. Порт удаляется из соответствующей(их) VLAN. Возврат порта во VLAN осуществляется командой set interface active. - *freq* — частота генерируемых сообщений протокола SNMP trap при поступлении несанкционированных пакетов.
port security trap *freq*	freq: (1..1000000) сек	Задать частоту генерируемых сообщений протокола SNMP trap при поступлении несанкционированных пакетов.
port security mode {secure {permanent | delete-on-reset} | max-addresses | lock}	—/lock	Задать режим ограничения изучения MAC-адресов для настраиваемого интерфейса. - **max-addresses** — удаляет текущие динамически изученные адреса, связанные с интерфейсом. Разрешено изучение максимального количества адресов на порту. Повторное изучение и старение разрешены. - **lock** — сохраняет в конфигурацию текущие динамически изученные адреса, связанные с интерфейсом и запрещает обучение новым адресам и старение уже изученных адресов. - **secure** — настраивает статическое ограничение изучения MAC-адресов на порту. - **permanent** — данный MAC-адрес сохранится в таблице даже после перезагрузки устройства. - **delete-on-reset** — данный адрес удалится после перезагрузки устройства.
no port security mode		Установить значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 239 – Команды режима EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show ports security {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| detailed}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Показать настройки функции безопасности на выбранном интерфейсе.
show ports security addresses {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| detailed}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Показать текущее количество изученных адресов и возможный лимит для заблокированных портов.

set interface active {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Активировать интерфейс, отключенный функцией защиты порта (команда доступна только для привилегированного пользователя).
show ports security status	—	Показать текущий статус всех интерфейсов.

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 mode secure permanent
console(config-if)# port security max 1
console(config-if)# port security
```

5.28.2. Проверка подлинности клиента на основе порта (стандарт 802.1x)

5.28.2.1. 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 240 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
dot1x system-auth-control	—/выключено	Включить режим аутентификации 802.1X на коммутаторе.
no dot1x system-auth-control		Выключить режим аутентификации 802.1X на коммутаторе.

aaa authentication dot1x default {none | radius} [none | radius]	—/radius	Задать 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		Установить 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 241 – 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)	Настроить 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		Установить значение по умолчанию.
dot1x reauthentication	—/периодические повторные проверки подлинности выключены	Включить периодические повторные проверки подлинности (переаутентификацию) клиента.
no dot1x reauthentication		Выключить периодические повторные проверки подлинности (переаутентификацию) клиента.
dot1x timeout reauth-period *period*	period: (300..4294967295)/ 3600 сек	Установить период между повторными проверками подлинности.
no dot1x timeout reauth-period		Установить значение по умолчанию.
dot1x timeout quiet-period *period*	period: (10..65535)/60 сек	Установить 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		Установить значение по умолчанию.

dot1x timeout tx-period *period*	period: (30..65535)/30 сек	Установить 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		Установить значение по умолчанию.
dot1x max-req *count*	count: (1..10)/2	Установить максимальное число попыток передачи запросов протокола EAP-клиенту перед новым запуском процесса проверки подлинности.
no dot1x max-req		Установить значение по умолчанию.
dot1x timeout supp-timeout *period*	period: (1..65535)/30 секунд	Установить период между повторными передачами запросов протокола EAP-клиенту.
no dot1x timeout supp-timeout		Установить значение по умолчанию.
dot1x timeout server-timeout *period*	period: (1..65535)/30 секунд	Установить период, в течение которого коммутатор ожидает ответа от сервера аутентификации.
no dot1x timeout server-timeout		Установить значение по умолчанию.
dot1x timeout silence-period ***period***	period: (60..65535) сек/не задано	Установить период времени неактивности клиента, по истечение которого клиент становится неавторизованным.
no dot1x timeout silence-period		Установить значение по умолчанию.
dot1x multi-sessions monitor-mode	—/выключено	Включить отправку multicast Request Identity независимо от аутентифицированных сессий.
no dot1x multi-sessions monitor-mode		Выключить периодические отправки multicast Request Identity независимо от аутентифицированных сессий.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 242 – Команды режима Privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
dot1x re-authenticate [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4);	Вручную осуществить повторную проверку подлинности указанного порта в команде, либо всех портов, поддерживающих 802.1X.
show dot1x [interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4);	Показать состояние 802.1X для коммутатора либо для указанного интерфейса.
show dot1x users [username *username***]**	username: (1..160) символов	Показать активных аутентифицированных пользователей 802.1X коммутатора.
show dot1x statistics interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4);	Показать 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 243 – 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 244 – Описание результатов выполнения команд

Параметр	***Описание***
EapolFramesRx	Количество корректных пакетов любого типа протокола EAPOL (Extensible Authentication Protocol over LAN), принятых данным определителем подлинности.
EapolFramesTx	Количество корректных пакетов любого типа протокола EAPOL, переданных данным определителем подлинности.
EapolStartFramesRx	Количество пакетов Start протокола EAPOL, принятых данным определителем подлинности.
EapolLogoffFramesRx	Количество пакетов Logoff протокола EAPOL, принятых данным определителем подлинности.
EapolRespIdFramesRx	Количество пакетов Resp/Id протокола EAPOL, принятых данным определителем подлинности.
EapolRespFramesRx	Количество пакетов ответов (кроме Resp/Id) протокола EAPOL, принятых данным определителем подлинности.
EapolReqIdFramesTx	Количество пакетов Resp/Id протокола EAPOL, переданных данным определителем подлинности.
EapolReqFramesTx	Количество пакетов запросов (кроме Resp/Id) протокола EAPOL, переданных данным определителем подлинности.
InvalidEapolFramesRx	Количество пакетов протокола EAPOL с нераспознанным типом, принятых данным определителем подлинности.
EapLengthErrorFramesRx	Количество пакетов протокола EAPOL с некорректной длиной, принятых данным определителем подлинности.

LastEapolFrameVersion	Версия протокола EAPOL, принятая в самом последнем на данный момент пакете.
LastEapolFrameSource	MAC-адрес источника, принятый в самом последнем на данный момент пакете.

5.28.2.2. 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 245 – Команды режима глобальной конфигурации

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

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

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

Таблица 246 – Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
dot1x host-mode {multi-host | single-host | multi-sessions}	—/multi-host	Разрешить 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	Задать 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		Установить значение по умолчанию.
dot1x authentication [mac | 802.1x | web]	—/выключено	Включить 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		Выключить аутентификацию, основанную на MAC-адресах пользователей.
dot1x max-hosts *hosts*	hosts: (1..4294967295)	Задать максимальное количество хостов, прошедших аутентификацию.
no dot1x max-hosts		Вернуть значение по умолчанию.
dot1x max-login-attempts *num*	num: (0, 3..10)/0	Задать количество неудачных попыток ввода логина, после которых клиент блокируется. 0 — бесконечное число попыток.
no dot1x max-login-attempts		Вернуть значение по умолчанию.
dot1x guest-vlan enable	—/выключено	Включить функцию гостевой VLAN на текущем интерфейсе.
no dot1x guest-vlan enable		Выключить функцию гостевой VLAN на текущем интерфейсе.
dot1x critical-vlan enable	—/выключено	Включить функцию критического VLAN на текущем интерфейсе.
no dot1x critical-vlan enable		Выключить функцию критического VLAN на текущем интерфейсе.
dot1x radius-attributes filter-id	—/выключено	Включить проверку подлинности, основанную на ACL/ назначить QoS-Policy.
no dot1x radius-attributes filter-id		Установить значение по умолчанию.
dot1x radius-attributes vlan {reject | static}	—/выключено	Включить обработку опции Tunnel-Private-Group-ID (81) в сообщениях RADIUS-сервера.
no dot1x radius-attributes vlan		Выключить обработку опции Tunnel-Private-Group-ID (81) в сообщениях RADIUS-сервера.
dot1x radius-attributes vendor-specific data-filter	—/выключено	Включить функцию динамического добавления ACL на порт через сообщения от RADIUS-сервера.

no dot1x radius-attributes vendor-specific data-filter		Выключить функцию динамического добавления ACL на порт через сообщения от RADIUS-сервера.

Команды режима конфигурирования VLAN

Вид запроса командной строки в режиме конфигурирования интерфейса VLAN:

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

Таблица 247 – Команды режима конфигурирования интерфейса VLAN

Команда	***Значение/Значение по умолчанию***	***Действие***
dot1x guest-vlan	по умолчанию VLAN не определен как гостевой	Определить гостевой VLAN. Открывает неавторизованным пользователям интерфейса доступ к гостевому VLAN. Если гостевой VLAN определен и разрешен, порт будет автоматически присоединяться к нему, когда не авторизован, и покидать, когда пройдет авторизацию. Чтобы использовать данный функционал, порт не должен быть статическим членом гостевого VLAN.
no dot1x guest-vlan		Установить значение по умолчанию.
dot1x critical-vlan	по умолчанию VLAN не определен как критический	Определить VLAN в качестве критического. Открывает неавторизованным пользователям доступ в критический VLAN при недоступности серверов RADIUS. Если критический VLAN определен и разрешен, порт будет автоматически добавлен в него после активации и покинет критический VLAN при получении ответа от сервера.
no dot1x critical-vlan		Установить значение по умолчанию.
dot1x auth-not-req	по умолчанию авторизация для VLAN включена	Определить VLAN без авторизации. Открывает неавторизованным пользователям доступ к выделенному VLAN. Неавторизованный VLAN должен быть назначен на порт статически как tagged.
no dot1x auth-not-req		Установить значение по умолчанию.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 248 – Команды режима Privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show dot1x [interface {gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* **| oob}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Показать состояние 802.1X для коммутатора либо для указанного интерфейса.
show dot1x detailed	—	Показать расширенные настройки протокола 802.1x.
show dot1x users [*username***]**	username: строка	Показать авторизованных клиентов.
show dot1x locked clients	—	Показать неавторизованных клиентов, заблокированных по таймауту.

show dot1x statistics interface {gigabitethernet *gi_port* | tengigabitethernet *te_port* | fortygigabitethernet *fo_port* **| oob}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Показать статистику 802.1x на интерфейсах.
show dot1x advanced {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| oob}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4)	Показать режимы работы dot1x.

5.28.2.3. Настройка активного сеанса клиента (CoA)

RADIUS CoA (Change of Authorization) — это функция, которая позволяет серверу RADIUS настроить активный сеанс клиента, ранее аутентифицированного на основе стандарта 802.1x. Обработка сообщений CoA-Request происходит в соответствии с RFC 5176. Обрабатываются сообщения, пришедшие на UDP-порт 3799 от серверов, заданных командой radius-server hosts и с ключом, заданным командой radius-server key. Для идентификации сеанса клиента используются RADIUS атрибуты User-Name или Acct-Session-Id. Для настройки сеанса клиента поддерживаются RADIUS-атрибуты Tunnel-Private-Group-Id, Filter-Id, Calling-Station-Id.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 249 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
aaa authorization dynamic radius	-/выключено	Включает функцию настройки активного сеанса клиента (CoA).
no aaa authorization dynamic		Выключает функцию настройки активного сеанса клиента (CoA).

5.28.3. Настройка функции MAC Address Notification

Функция MAC Address Notification позволяет отслеживать появление и исчезновение активного оборудования на сети путем сохранения истории изучения MAC-адресов. При обнаружении изменений в составе изученных MAC-

адресов коммутатор сохраняет информацию в таблице и извещает об этом с помощью сообщений протокола SNMP. Функция имеет настраиваемые параметры – глубина истории о событиях и минимальный интервал отправки сообщений. Сервис MAC Address Notification отключен по умолчанию и может быть настроен выборочно для отдельных портов коммутатора.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 250 – Команды режима глобальной конфигурации

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

no snmp-server enable traps mac-notification change		Отключает отправку SNMP-уведомлений об изменении состояния таблицы MAC-адресов.
snmp-server enable traps mac-notification flapping	—/включена	Включить отправку трапов о флаппинге MAC-адресов.
no snmp-server enable traps mac-notification flapping		Отключить отправку трапов о флаппинге MAC-адресов.

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки:

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

Таблица 251 – Команды режима конфигурации интерфейса Ethernet

Команда	***Значение/Значение по умолчанию***	***Действие***
snmp trap mac-notification change [added | removed]	-/выключена	Включение генерации уведомлений на каждом интерфейсе о событиях изменения состояния MAC-адресов. Отдельно можно разрешить генерацию уведомлений только об изучении MAC-адресов, либо только об их удалении.
no snmp trap mac-notification change		Отключение генерации уведомлений на интерфейсе.

Команды режима privileged EXEC

Вид запроса командной строки в режиме privileged EXEC:

```
console#
```

Таблица 252 – Команды режима privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show mac address-table notification change history [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094).	Отображение всех уведомлений об изменении состояния MAC-адресов, сохраненных в истории.
show mac address-table notification change statistics	-	Отображение статистики сервиса: общее количество событий об изучении MAC-адресов, общее количество событий об удалении MAC-адресов, общее количество отправленных SNMP-сообщений.

Примеры использования команд

- Пример показывает как настроить передачу сообщений SNMP MAC Notification на сервер с адресом **172.16.1.5**. При настройке задается общее разрешение работы сервиса, настраивается минимальный интервал отправки сообщений, задается размер истории событий и настраивается сервис на выбранном порту.

```
console(config)#snmp-server host 172.16.1.5 traps private
console(config)#snmp-server enable traps mac-notification change
console(config)#mac address-table notification change
```

```
console(config)#mac address-table notification change interval 60
console(config)#mac address-table notification change history 100
console(config)#interface gigabitethernet 0/7
console(config-if)#snmp trap mac-notification change
console(config-if)#exit
console(config)#
```

5.28.4. 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.

Опция формируется с учетом приоритета (в порядке уменьшения): настройки интерфейса Ethernet → настройки интерфейса VLAN → настройки режима глобального конфигурирования.

Таблица 253 – 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 (без добавления IP-адреса на клиентский интерфейс) или функция DHCP Snooping (при условии включения команды ip dhcp information option).

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 254 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip dhcp snooping	—/выключено	Включить контроль протокола DHCP путем ведения таблицы DHCP Snooping и отправки клиентских широковещательных DHCP-запросов на «доверенные» порты.
no ip dhcp snooping		Выключить контроль протокола DHCP.
ip dhcp snooping vlan *vlan_id*	vlan_id: (1..4094)/выключено	Разрешить контроль протокола DHCP в пределах указанной VLAN.
no ip dhcp snooping vlan *vlan_id*		Запретить 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	Разрешить принимать DHCP-пакеты с опцией 82 от «ненадежных» портов.
no ip dhcp snooping information option allowed-untrusted		Запретить принимать DHCP-пакеты с опцией 82 от «ненадежных» портов.
ip dhcp snooping verify	по умолчанию верификация включена	Включить верификацию MAC-адреса клиента и MAC-адреса источника, принятого в DHCP-пакете на «недоверенных» портах.
no ip dhcp snooping verify		Выключить верификацию MAC-адреса клиента и MAC-адреса источника, принятого в DHCP-пакете на «недоверенных» портах.

ip dhcp snooping database	резервный файл не используется	Разрешить использование резервного файла (базы) контроля протокола DHCP, позволяющего восстановить записи в таблице в случае перезагрузки устройства. **Необходима настройка синхронизации системного времени (NTP/SNTP).**
no ip dhcp snooping database		Запретить использование резервного файла (базы) контроля протокола DHCP.
ip dhcp snooping port-down action clear	—/выключено	Разрешить очистку таблицы DHCP Snooping при падении интерфейса.
no ip dhcp snooping port-down action		Запретить очистку таблицы DHCP Snooping при падении интерфейса.
ip dhcp information option	—/выключено	Разрешить устройству добавление опции 82 при работе протокола DHCP.
no ip dhcp information option		Запретить устройству добавление опции 82 при работе протокола DHCP.
ip dhcp information option format-type access-node-id *node_id*	node_id: (1..32) символов	Установить идентификатор Access Node ID опции 82.
no ip dhcp information option format-type access-node-id		Установить значение по умолчанию.
ip dhcp information option format-type remote-id *remote_id*	remote_id*:* (1..128) символов/—	Установить идентификатор Remote agentID опции 82.
no ip dhcp information option format-type remote-id		Установить значение по умолчанию.
ip dhcp information option format-type option *format* **[delimiter** *delimiter***]**	format: (sp, sv, pv, spv, bin,); delimiter: (.,;#)/пробел	Настроить формат DHCP опции 82. Формат: - **sp** — номер слота и порта; - **sv** — номер слота и VLAN; - **pv** — номер порта и VLAN; - **spv** — номер слота, порта и VLAN; - **bin** — бинарный формат: VLAN, слот, порт; - **user-defined** — формат определяется пользователем. При определении используются следующие шаблоны: %h: hostname; %p: короткое имя порта, например gi1/0/1; %P: длинное имя порта, например, gigabitethernet 1/0/1; %t: тип порта (значение поля ifTable::ifType в шестнадцатеричном виде); %m: мак-адрес порта в формате H-H-H-H-H-H-H-H; %M: мак-адрес системы в формате H-H-H-H-H-H-H-H; %u: номер юнита; %s: номер слота; %n: номер порта (как на лицевой панели); %i: ifIndex порта; %v: идентификатор VLAN; %c: мак-адрес клиента в формате H-H-H-H-H-H-H; %a: IP адрес системы в формате A.B.C.D; %%: одиночный символ %.
no ip dhcp information option format-type option		Установить значение по умолчанию.
ip dhcp information option suboption type {tr101 | custom}	—/tr101	Установить формат опции 82. - **tr101** — устанавливает формат опции 82 согласно синтаксису, принятому в рекомендациях TR-101 в соответствии с форматом, который приведен в таблице 255. - **custom** — устанавливает формат опции 82 в соответствии с форматом, который приведен в таблице 255.
no ip dhcp information option suboption type		Установить значение по умолчанию.

ip dhcp route {connected | static}	–	Разрешить устройству создавать запись в таблице маршрутизации с маской /32 для каждого IP-адреса полученного клиентом от DHCP-сервера. Записи в таблице маршрутизации автоматически удаляются при истечении срока аренды IP-адресов. – **connected** — маршрут создается как подключенный; – **static** — маршрут создается как статический. **Функция работает только при включенных DHCP Snooping и DHCP Relay.**
no ip dhcp route		Запретить устройству создавать запись в таблице маршрутизации для каждого IP-адреса полученного от DHCP-сервера.

Таблица 255 – 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 256 – 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 257 – Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

Команда	***Значение/Значение по умолчанию***	***Действие***
ip dhcp snooping	–	Включить контроль протокола DHCP в пределах интерфейса.
no ip dhcp snooping		Выключить контроль протокола DHCP в пределах интерфейса.

ip dhcp snooping trust	по умолчанию интерфейс не является доверенным	Добавить интерфейс в список «доверенных» при использовании контроля протокола DHCP. DHCP-трафик «доверенного» интерфейса считается безопасным и не контролируется.
no ip dhcp snooping trust		Удалить интерфейс из списка «доверенных» при использовании контроля протокола DHCP.
ip dhcp snooping limit rate *rate*	rate: (1..2048) pps/выключено	Установить ограничение для данного порта на количество принимаемых DHCP-пакетов в секунду. При превышении установленного порога dhcp-пакетов интерфейс блокируется.
no ip dhcp snooping limit rate		Снять ограничение на количество принимаемых DHCP-пакетов в секунду.
ip dhcp snooping limit clients *value*	value: (1..2048)/не задан	Установить предельное количество подключенных клиентов.
no ip dhcp snooping limit clients		Установить значение по умолчанию.
ip dhcp information option [global]	—/global	Разрешить устройству добавление опции 82 на интерфейсе при работе протокола DHCP. - **global** — добавление опции 82 определяется настройками на интерфейсе VLAN.
no ip dhcp information option		Запретить устройству добавление опции 82 для данного интерфейса при работе протокола DHCP.
ip dhcp information option format-type access-node-id *node_id*	node_id: (1..32) символов/—	Установить идентификатор access-node_id опции 82 на интерфейсе.
no ip dhcp information option format-type access-node-id		Установить значение по умолчанию.
ip dhcp information option format-type circuit-id circuit_id	circuit_id: (1..63) символов/—	Установить специфичный **Circuit-id** на интерфейсе.
no ip dhcp information option format-type circuit-id		Установить значение по умолчанию.
ip dhcp information option format-type remote-id *remote_id*	remote_id: (1..63) символов/—	Установить специфичный **Remote-id** на интерфейсе.
no ip dhcp information option format-type remote-id		Установить значение по умолчанию.
ip dhcp information option format-type option *format* **[delimiter** *delimiter***]**	format: (sp, sv, pv, spv, bin, user-defined); delimiter: (.,;#)/пробел	Настроить формат DHCP-опции 82 на интерфейсе. Формат: - **sp** — номер слота и порта; - **sv** — номер слота и VLAN; - **pv** — номер порта и VLAN; - **spv** — номер слота, порта и VLAN; - **bin** — бинарный формат: VLAN, слот, порт; - **user-defined** — формат определяется пользователем. При определении используются следующие шаблоны: %h: hostname; %p: короткое имя порта, например gi1/0/1; %P: длинное имя порта, например, gigabitethernet 1/0/1; %t: тип порта (значение поля ifTable::ifType в шестнадцатеричном виде); %m: MAC-адрес порта в формате H-H-H-H-H-H-H-H; %M: MAC-адрес системы в формате H-H-H-H-H-H-H-H; %u: номер юнита; %s: номер слота; %n: номер порта (как на лицевой панели); %i: ifIndex порта; %v: идентификатор VLAN; %c: MAC-адрес клиента в формате H-H-H-H-H-H; %a: IP-адрес системы в формате A.B.C.D.

no ip dhcp information option format-type option		Установить значение по умолчанию.
ip dhcp information option suboption-type {global | tr101 | custom}	—/global	Настроить формат опции 82 на интерфейсе. - **global** — формат опции определяется настройками опции на интерфейсе VLAN; - **tr101** — устанавливает формат опции 82 согласно синтаксису, принятому в рекомендациях TR-101 в соответствии с форматом, который приведен в таблице 255; - **custom** — устанавливает формат опции 82 в соответствии с форматом, который приведен в таблице 256.
no ip dhcp information option suboption-type		Установить значение по умолчанию.

Команды режима конфигурирования интерфейса VLAN

Вид запроса командной строки в режиме конфигурирования интерфейса VLAN:

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

Таблица 258 – Команды режима конфигурирования интерфейса VLAN

Команда	***Значение/Значение по умолчанию***	***Действие***
ip dhcp information option [global]	—/global	Разрешить устройству добавление опции 82 на интерфейсе при работе протокола DHCP. - **global** — добавление опции 82 определяется глобальными настройками.
no ip dhcp information option		Запретить устройству добавление опции 82 для данного VLAN при работе протокола DHCP.
ip dhcp information option format-type access-node-id *node_id*	node_id: (1..32) символов/—	Установить идентификатор access-node_id опции 82 для данного VLAN.
no ip dhcp information option format-type access-node-id		Установить значение по умолчанию.
ip dhcp information option format-type remote-id	remote_id: (1..32) символов/—	Установить идентификатор remote_id опции 82 для данного VLAN.
no ip dhcp information option format-type remote-id		Установить значение по умолчанию.
ip dhcp information option format-type option *format* **[delimiter** *delimiter***]**	format: (sp, sv, pv, spv, bin, user-defined); delimiter: (.,;#)/пробел	Настроить формат DHCP-опции 82 для данного VLAN. Формат: - **sp** — номер слота и порта; - **sv** — номер слота и VLAN; - **pv** — номер порта и VLAN; - **spv** — номер слота, порта и VLAN; - **bin** — бинарный формат: VLAN, слот, порт; - **user-defined** — формат определяется пользователем. При определении используются следующие шаблоны: %h: hostname; %p: короткое имя порта, например gi1/0/1; %P: длинное имя порта, например, gigabitethernet 1/0/1; %t: тип порта (значение поля ifTable::ifType в шестнадцатеричном виде); %m: мак-адрес порта в формате H-H-H-H-H-H-H-H;

		%M: мак-адрес системы в формате H-H-H-H-H-H; %u: номер юнита; %s: номер слота; %n: номер порта (как на лицевой панели); %i: ifIndex порта; %v: идентификатор VLAN; %c: мак-адрес клиента в формате H-H-H-H-H-H; %a: IP адрес системы в формате A.B.C.D.
no ip dhcp information option format-type option		Установить значение по умолчанию.
ip dhcp information option suboption-type {global | tr101 | custom}	—/global	Настроить формат опции 82 для данного VLAN. - **global** — формат опции определяется глобальными настройками; - **tr101** — устанавливает формат опции 82 согласно синтаксису, принятому в рекомендациях TR-101 в соответствии с форматом, который приведен в таблице 255; - **custom** — устанавливает формат опции 82 в соответствии с форматом, который приведен в таблице 256.
no ip dhcp information option suboption-type		Установить значение по умолчанию.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 259 – Команды режима Privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
ip dhcp snooping binding *mac_address vlan_id ip_address* **{gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***} expiry {***seconds* **| infinite}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); seconds: (10..4294967295) с	Добавить 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*		Удалить из файла (базы) контроля протокола DHCP соответствие MAC-адреса клиента и группы VLAN.
clear ip dhcp snooping database {mac-address *mac_address***} {vlan** *vlan***} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan: (1..4094)	Очистить файл (базу) контроля протокола DHCP или отдельную запись в файле(базе) контроля DHCP.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 260 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip dhcp information option	—	Показать информацию об использовании опции 82 протокола DHCP.
show ip dhcp snooping [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Показать конфигурацию функции контроля протокола DHCP.
show ip dhcp snooping binding [mac-address *mac_address***] [ip-address** *ip_address* **] [vlan** *vlan_id***] [gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Показать соответствия из файла (базы) контроля протокола DHCP.

Примеры выполнения команд

- Разрешить использование DHCP опции 82 в 10 VLAN:

```
console# configure
console(config)# ip dhcp snooping
console(config)# ip dhcp snooping vlan 10
console(config)# ip dhcp information option
console(config)# interface gigabitethernet 1/0/24
console(config)# ip dhcp snooping trust
```

- Показать все соответствия из таблицы контроля протокола DHCP:

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

5.28.5. 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.

Функционал IP Source Guard не отслеживает смену MAC-адреса клиентом. Отслеживание происходит только для связки IP-VLAN-Port.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 261 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip source-guard	—/выключено	Включить функцию защиты IP-адреса клиента для всего коммутатора.
no ip source-guard		Выключить функцию защиты IP-адреса клиента для всего коммутатора.
ip source-guard binding *mac_address vlan_id ip_address* **{gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094).	Создать статическую запись 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*		Удалить статическую запись в таблице соответствия.
ip source-guard tcam retries-freq {*seconds* **| never}**	seconds: (10..600)/60 сек	Задать 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		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(config-if)#
```

Таблица 262 – Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

Команда	*Значение/Значение по умолчанию*	*Действие*
ip source-guard [vlan {*vlan-id*}**]**	—/выключено	Включить функцию защиты IP-адреса клиента для настраиваемого интерфейса. - **vlan** — опционально для отдельных vlan.
no ip source-guard [vlan {*vlan-id*}**]**		Выключить функцию защиты IP-адреса клиента для настраиваемого интерфейса.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 263 – 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 264 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip source-guard configuration [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Отобразить настройку функции защиты IP-адреса на заданном, либо на всех интерфейсах устройства.
show ip source-guard status [mac-address *mac_address***] [ip-address** *ip_address* **] [vlan** *vlan_id***] [gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094);	Отобразить статус функции защиты IP-адреса для указанного интерфейса, IP-адреса, MAC-адреса или группы VLAN.
show ip source-guard inactive	—	Отобразить неактивные 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
```

5.28.6. Контроль протокола ARP (ARP Inspection)

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

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

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 265 – 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 266 – 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.
ip arp inspection limit rate *rate*	rate:(0..2048)/0 pps	Настроить ограничение скорости разрешенных arp-пакетов в pps.

no ip arp inspection trust limit rate		Удалить ограничение скорости для разрешенных arp-пакетов.

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 267 – 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 268 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip arp inspection [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	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
```

5.28.7. Функционал First Hop Security

Пакет функций First Hop Security включает в себя анализатор DHCPv6-пакетов, IPv6 Source Guard, ND Inspection и RA Guard. Данный набор функций предназначен для обеспечения контроля и фильтрации IPv6 трафика в сети.

Анализатор DHCPv6 пакетов позволяет добавлять соседей в таблицу привязок IPv6 binding table при получении адреса по DHCP, а также позволяет бороться с недоверенными DHCPv6 серверами.

IPv6 Source Guard позволяет устройству отклонять трафик, если он исходит от адреса, который не сохранен в IPv6 binding table. Таблица привязок соседей IPv6 binding table, подключенных к устройству, создается из таких источников информации, как отслеживание по протоколу обнаружения соседей (NDP).

С помощью функции ND Inspection коммутатор проверяет сообщения NS (Neighbor Solicitation) и NA (Neighbor Advertisement) и сохраняет их в IPv6 binding table. На основании таблицы коммутатор отбрасывает любые поддельные сообщения NS / NA.

Функционал RA Guard позволяет блокировать или отклонять нежелательные или посторонние сообщения Router Advertisement (RA), поступающие на коммутатор от маршрутизатора.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 269 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ipv6 neighbor binding policy *policy_name*	policy_name: (1..32) символа	Создать политику привязки соседей (neighbor binding) и перейти в режим её конфигурирования.
no ipv6 neighbor binding policy *policy_name*		Удалить политику привязки соседей.
ipv6 first hop security logging packet drop	—/выключено	Активировать логирование дропа пакетов при несоответствии политикам безопасности служб RA Guard, ND Inspection, DHCPv6 Guard и IPv6 Source Guard.
no ipv6 first hop security logging packet drop		Установить значение по умолчанию.
ipv6 neighbor binding address-config {stateless | any | dhcp}	—/выключено	Включить добавление записей в таблицу привязки соседей на основании: **- stateless** —IPv6 RA-сообщений; **- dhcp** — пакета DHCPv6 Reply. При этом все Link-local IPv6-адреса вносятся в таблицу привязки соседей по умолчанию в результате анализа ICMPv6-пакетов; **- any** — добавлять все адреса.
no ipv6 neighbor binding address-config		Установить значение по умолчанию.
ipv6 neighbor binding address-prefix {vlan | X:X:X:X::X/<0-128>}	—	Добавить статическую запись с префиксом в таблицу Neighbor Prefix Table. **- vlan** — привязать запись к определенному VLAN.
no ipv6 neighbor binding address-prefix {vlan | X:X:X:X::X/<0-128>}		Удалить статическую запись с префиксом из таблицы Neighbor Prefix Table.
ipv6 neighbor binding address-prefix-validation	—/выключено	Включить проверку адресов в таблице привязки соседей.
no ipv6 neighbor binding address-prefix-validation		Установить значение по умолчанию.
ipv6 neighbor binding lifetime *minutes*	minutes: 1..60 / 5	Установить время жизни таблицы привязки соседей для записи в минутах.
no ipv6 neighbor binding lifetime		Установить значение по умолчанию.
ipv6 neighbor binding logging	—/выключено	Включить логирование основных событий по изменению таблицы привязки.
no ipv6 neighbor binding logging		Установить значение по умолчанию.
ipv6 neighbor binding max-entries {interface-limit | vlan-limit | mac-limit} {limit | disable}	limit: (0..65535)/выключено	Определить максимальное количество записей в таблице привязки соседей. **- interface-limit** — определить лимит для интерфейса; **- vlan-limit** — определить лимит VLAN; **- mac-limit** — определить лимит MAC-адресов; **- disable** — разрешить максимальное количество записей. Максимальное значение = 4294967294.
no ipv6 neighbor binding max-entries		Установить значение по умолчанию.
ipv6 neighbor binding static ipv6 {X:X:X:X::X} vlan vlan_id **interface** *interface* **mac** *mac-address*	—	Добавить статическую запись без префикса в таблицу Neighbor Prefix Table. **- vlan** — привязать запись к определенному VLAN; - **interface** — привязать запись к определенному интерфейсу; - **mac** — привязать запись к определенному MAC-адресу.
no ipv6 neighbor binding static ipv6 {X:X:X:X::X} vlan vlan_id		Удалить статическую запись.

ipv6 source guard policy *policy_name*	policy_name: (1..32) символа	Создать политику Source Guard и перейти в режим её конфигурирования.
no ipv6 source guard policy *policy_name*		Удалить политику Source Guard.
ipv6 dhcp guard policy *policy_name*	policy_name: (1..32) символа	Создать политику DHCP Guard и перейти в режим её конфигурирования.
no ipv6 dhcp guard policy *policy_name*		Удалить политику DHCP Guard.
ipv6 dhcp guard preference {minimum *minimum_value* **| maximum** *maximum_value***}**	minimum_value;maximum_value: (0..255)/выключено	Установить максимальный и минимальный пределы предпочтения для DHCPv6 сервера.
ipv6 dhcp guard preference		Установить значение по умолчанию.
ipv6 nd inspection policy *policy_name*	policy_name: (1..32) символа	Создать политику ND Inspection и перейти в режим её конфигурирования.
no ipv6 nd inspection policy *policy_name*		Удалить политику ND Inspection.
ipv6 nd inspection drop-unsecure	—/выключено	Включить отбрасывание пакетов с отсутствующими или недопустимыми параметрами или подписью.
no ipv6 nd inspection drop-unsecure		Установить значение по умолчанию.
ipv6 nd inspection sec-level minimum	minimum: (0..7)/выключено	Установить минимальное значение параметра уровня безопасности, при использовании опций криптографически сгенерированного адреса (CGA).
no ipv6 nd inspection sec-level minimum		Установить значение по умолчанию.
ipv6 nd inspection validate source-mac	—/выключено	Включить проверку MAC-адреса пакета по его link-layer адресу.
no ipv6 nd inspection validate source-mac		Установить значение по умолчанию.
ipv6 nd raguard policy	policy_name: (1..32) символа	Создать политику ND RA Guard и перейти в режим её конфигурирования.
no ipv6 nd raguard policy		Удалить политику ND RA Guard.
ipv6 nd raguard hop-limit {minimum *minimum_value* **| maximum** *maximum_value***}**	minimum_value;maximum_value: (1..255)/выключено	Установить пределы значения Cur Hop Limit в Router Advertisement-сообщениях.
no ipv6 nd raguard hop-limit		Установить значения по умолчанию.
ipv6 nd raguard managed-config-flag {off | on}	—/выключено	Включить проверку флага "**managed-config**" в сообщениях Router Advertisement. **- off —** значение флага должно быть 0; **- on —** значение флага должно быть 1.
no ipv6 nd raguard managed-config-flag		Установить значение по умолчанию.
ipv6 nd raguard other-config-flag {off | on}	—/выключено	Включить проверку флага "**other-config**" в сообщениях Router Advertisement. **- off —** значение флага должно быть 0; **- on —** значение флага должно быть 1.
no ipv6 nd raguard other-config-flag		Установить значение по умолчанию.
ipv6 nd raguard router-preference minimum {low | medium | high}	—/выключено	Установить минимальное объявляемое значение Default Router Preference в Router Advertisement-сообщениях. **- low —** низкое значение; **- medium —** среднее значение; **- high —** высокое значение.
no ipv6 nd raguard router-preference minimum		Установить значение по умолчанию.

ipv6 nd raguard router-preference maximum {low | medium | high}	—/выключено	Установить максимальное объявляемое значение Default Router Preference в Router Advertisement-сообщениях. - **low —** низкое значение; - **medium —** среднее значение; - **high —** высокое значение.
no ipv6 nd raguard router-preference maximum		Установить значение по умолчанию.

Команды режима конфигурации политики привязки соседей

Вид запроса командной строки:

```
console(config-nbr-binding)#
```

Таблица 270 – Команды режима политики привязки соседей

Команда	***Значение/Значение по умолчанию***	***Действие***
logging binding enable	—/выключено	Включить логирование добавления/удаления IPv6 в таблицу привязки соседей.
logging binding disable		Выключить логирование добавления/удаления IPv6 в таблицу привязки соседей.
max-entries {interface-limit | vlan-limit | mac-limit} {*limit* **| disable}**	limit: (0..65535)/отключено	Определить максимальное количество записей в таблице привязки соседей. - **interface-limit** — определить лимит для интерфейса, - **vlan-limit** — определить лимит VLAN, - **mac-limit** — определить лимит MAC-адресов, - **disable** — разрешить максимальное количество записей. Максимальное значение = 4294967294.
no max-entries		Установить значение по умолчанию.
address-config {dhcp | any | stateless}	—/address-config	Включить добавление записей в таблицу привязки соседей на основании: - **dhcp** — пакета DHCPv6 Reply. При этом все Link-local IPv6-адреса вносятся в таблицу привязки соседей по умолчанию в результате анализа ICMPv6-пакетов, - **any —** добавлять все адреса, - **stateless —** на основе IPv6 RA сообщений.
no address-config		Установить значение по умолчанию.
address-prefix-validation {enable | disable}	—/выключено	Включить проверку адресов в таблице привязки соседей.
no address-prefix-validation		Установить значение по умолчанию.
device-role {perimeter | internal}	—/выключено	Указать роль устройства, подключенного к интерфейсу. - **perimeter —** устройство периметра; - **internal —** внутреннее устройство.
no device-role		Убрать роль с устройства, подключенного к интерфейсу.

Команды режима конфигурации политики Source Guard

Вид запроса командной строки:

```
console(config-nbr-srcgrd)#
```

Таблица 271 – Команды режима ipv6 Source Guard политики

Команда	*Значение/Значение по умолчанию*	*Действие*
trusted-port	-/выключено	Определить доверенный порт. Данная политика навешивается на порт, на котором не должна применяться политика Source Guard.
no trusted-port		Установить значение по умолчанию

Команды режима конфигурации политики DHCP Guard

Вид запроса командной строки:

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

Таблица 272 — Команды режима ipv6 DHCP Guard политики

Команда	*Значение/Значение по умолчанию*	*Действие*
device-role {client | server}	—/выключено	Указать роль устройства, подключенного к интерфейсу. - **server** — установить роль сервера; - **client** — установить роль клиента.
no device-role		Убрать роль с устройства, подключенного к интерфейсу.
match reply {disable | prefix-list *prefix_list***}**	prefix_list: (0..32) символа/выключено	Включить проверку анонсируемых адресов, полученных в сообщениях DHCPv6. - **disable** — отключить проверку по DHCPv6-сообщениям. - **prefix-list** — префикс-маска, по которой будет осуществляться проверка.
no match reply		Установить значение по умолчанию
match server address {disable | prefix-list *prefix_list***}**	prefix_list: (0..32) символа/выключено	Включить проверку адреса источника сервера. - **disable** — отключить проверку адреса источника сервера. - **prefix-list** — префикс-маска, по которой будет осуществляться проверка.
no match server address		Установить значение по умолчанию.
preference minimum {*preference_value* | **disable}**	preference_value: (0..255)/выключено	Установить минимальный предел анонсируемых DHCPv6-сервером опций. - **disable** — выключить проверку опций.
no preference minimum		Установить значение по умолчанию.
preference maximum {*preference_value* | **disable}**	preference_value: (0..255)/выключено	Установить максимальный предел анонсируемых DHCPv6-сервером опций. - **disable** — выключить проверку опций.
no preference maximum		Установить значение по умолчанию.

Команды режима конфигурации политики ND Inspection

Вид запроса командной строки:

```
console(config-nd-inspection) #
```

Таблица 273 — Команды режима ipv6 ND Inspection политики

Команда	*Значение/Значение по умолчанию*	*Действие*
device-role {host | router}	—/выключено	Указать роль устройства, подключенного к интерфейсу. - **host** — установить роль хоста; - **router** — установить роль маршрутизатора.
no device-role		Установить значение по умолчанию.

drop-unsecure {enable |disable}	—/выключено	Включить отбрасывание пакетов с отсутствующими или недопустимыми параметрами или подписью.
no drop-unsecure		Установить значение по умолчанию.
sec-level minimum {*sec_level_minimum* **| disable}**	sec_level_minimum: (0..7)/выключено	Указывает минимальное значение параметра уровня безопасности при использовании опций криптографически сгенерированного адреса (CGA).
no sec-level minimum		Установить значение по умолчанию.
validate source-mac {enable | disable}	—/выключено	Включить проверку MAC-адреса пакета по его link-layer адресу. **- enable —** включить; **- disable —** выключить.
no validate source-mac		Установить значение по умолчанию.

Команды режима конфигурации политики RA Guard

Вид запроса командной строки:

```
console(config-ra-guard)#
```

Таблица 274 — Команды режима ipv6 RA Guard политики

Команда	***Значение/Значение по умолчанию***	***Действие***
device-role {host | router}	—/выключено	Указать роль устройства, подключенного к интерфейсу. **- host —** установить роль хоста; **- router —** установить роль маршрутизатора.
no device-role		Установить значение по умолчанию.
hop-limit {minimum *value_limit* **| maximum** *value_limit***}**	value_limit: (1..255)/выключено	Установить пределы значения Cur Hop Limit в Router Advertisement-сообщениях.
no hop-limit		Установить значения по умолчанию.
managed-config-flag {off | on}	—/выключено	Включить проверку флага "**managed-config**" в сообщениях Router Advertisement. **- off —** значение флага должно быть 0; **- on —** значение флага должно быть 1.
no managed-config-flag		Установить значение по умолчанию.
match ra address {disable | prefix-list *prefix_list***}**	prefix_list:(1-32)символа/выключено	Включить проверку адресов в Router Advertisement-сообщениях. **- disable —** отключить проверку адресов; **- prefix-list —** префикс-маска, по которой будет осуществляться проверка.
no match ra address		Установить значение по умолчанию.
match ra prefixes {disable | prefix-list *prefix_list***}**	prefix_list: (1-32)символа/выключено	Включить проверку префиксов в Router Advertisement-сообщениях. **- disable —** отключить проверку префиксов; **- prefix-list —** префикс-маска, по которой будет осуществляться проверка.
no match ra address		Установить значение по умолчанию.
other-config-flag {off | on}	—/выключено	Включить проверку флага "**other-config**" в сообщениях Router Advertisement. **- off —** значение флага должно быть 0; **- on —** значение флага должно быть 1.
no other-config-flag		Установить значение по умолчанию.
router-preference minimum {low | medium | high}	—/выключено	Установить минимальное объявляемое значение Default Router Preference в Router Advertisement-сообщениях. **- low —** низкое значение;

		- medium — среднее значение; **- high —** высокое значение.
no router-preference minimum		Установить значение по умолчанию.
router-preference maximum {low | medium | high}	—/выключено	Установить максимальное объявляемое значение Default Router Preference в Router Advertisement-сообщениях. **- low —** низкое значение; **- medium —** среднее значение; **- high —** высокое значение.
no router-preference maximum		Установить значение по умолчанию.

Команды режима конфигурации политики First Hop Security

Вид запроса командной строки:

```
console(config-ipv6-fhs)#
```

Таблица 275 — Команды режима ipv6 First Hop Security политики

Команда	***Значение/Значение по умолчанию***	***Действие***
logging packet drop {enable | disable}	—/выключено	Активировать логирование дропа пакетов при несоответствии политикам безопасности служб RA Guard, ND Inspection, DHCPv6 Guard и IPv6 Source Guard. **- enable —** включить логирование дропа пакетов для данной политики; **- disable —** отключить логирование дропа пакетов для данной политики.
no logging packet drop		Установить значение по умолчанию.

Команды режима конфигурации интерфейса VLAN

Вид запроса командной строки режима конфигурации интерфейса VLAN:

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

Таблица 276 – Команды режима конфигурации интерфейса VLAN

Команда	***Значение/Значение по умолчанию***	***Действие***
ipv6 first hop security	—/выключено	Включить ICMPv6 и DHCPv6 snooping во vlan.
no ipv6 first hop security		Выключить ICMPv6 и DHCPv6 snooping во vlan.
ipv6 first hop security attach-policy *policy_name*	policy_name: (1..32)символа/выключено	Добавить политику First Hop Security на интерфейс.
no ipv6 first hop security attach-policy		Удалить политику First Hop Security с интерфейса.
ipv6 neighbor binding	—/выключено	Включить привязку соседей и добавление записей в таблицу.
no ipv6 neighbor binding		Выключить привязку соседей и добавление записей в таблицу.
ipv6 neighbor binding attach-policy *policy_name*	policy_name: (1..32)символа/выключено	Добавить политику Neighbor Binding на интерфейс.
no ipv6 neighbor binding attach-policy		Удалить политику Neighbor Binding с интерфейса.
ipv6 source guard	—/выключено	Включить IPv6 Source Guard.
no ipv6 source guard		Выключить IPv6 Source Guard.

ipv6 dhcp guard	—/выключено	Включить DHCP Guard.
no ipv6 dhcp guard		Выключить DHCP Guard.
ipv6 dhcp guard attach-policy *policy_name*	policy_name: (1..32)символа/выключено	Добавить политику DHCP Guard на интерфейс.
no ipv6 dhcp guard attach-policy		Удалить политики DHCP Guard с интерфейса.
ipv6 nd inspection	—/выключено	Включить IPv6 ND Inspection.
no ipv6 nd inspection		Выключить IPv6 ND Inspection.
ipv6 nd inspection attach-policy *policy_name*	policy_name: (1..32)символа/выключено	Добавить политику ND Inspection на интерфейс.
no ipv6 nd inspection attach-policy		Удалить политику ND Inspection с интерфейса.
ipv6 nd raguard	—/выключено	Включить IPv6 ND RA Guard.
no ipv6 nd raguard		Выключить IPv6 ND RA Guard
ipv6 nd raguard attach-policy *policy_name*	policy_name: (1..32)символа/выключено	Добавить политику ND RA Guard на интерфейс.
no ipv6 nd raguard attach-policy		Удалить политику ND RA Guard с интерфейса.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 277 – Команды режима EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show ipv6 first hop security	—	Отобразить настройки функций IPv6 First Hop Security.
show ipv6 source guard	—	Отобразить состояние функции IPv6 source guard.
show ipv6 neighbor binding table	—	Отобразить таблицу привязок соседей.
show ipv6 dhcp guard	—	Отобразить состояние и настройки функции DHCP Guard.
show ipv6 nd inspection	—	Отобразить состояние и настройки функции ND Inspection.
show ipv6 nd raguard	—	Отобразить состояние и настройки функции RA Guard.

5.29. Функции DHCP Relay посредника

5.29.1. Функции DHCP Relay для IPv4

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 278 – Команды режима глобальной конфигурации

Команда	***Значение/Значение по умолчанию***	***Действие***
ip dhcp relay enable	по умолчанию агент выключен	Включить функции DHCP Relay-агента на коммутаторе.
no ip dhcp relay enable		Выключить функции DHCP Relay-агента на коммутаторе.
ip dhcp relay address *ip_address* [**vlan** *vlan_id*] [**vrf** *vrf_name*]	vlan_id: (1..4094) vrf_name: {1..32} символа **Может быть задано до 32 серверов (диапазоном или перечислением).**	Задать IP-адрес доступного DHCP-сервера для DHCP Relay-агента. - **vlan** — клиентский VLAN, запросы из которого будут направлены на IP-адрес конкретного сервера. **Несколько клиентских VLAN добавляются через запятую в случае перечисления и через дефис в случае указания диапазонов.**
no ip dhcp relay address [*ip_address*] [**vrf** *vrf_name*]		Удалить IP-адрес из списка DHCP-серверов для DHCP Relay-агента.
ip dhcp relay information option format-type option *format* **[delimiter** *delimiter***]**	format: (sp, sv, pv, spv, bin); delimiter: (.,;#)/пробел	Настроить формат DHCP-опции 82. Формат: - **sv** — номер слота и VLAN; - **pv** — номер порта и VLAN; - **spv** — номер слота, порта и VLAN; - **bin** — бинарный формат: VLAN, слот, порт.
no ip dhcp relay information option format-type option		Установить значение по умолчанию.
ip dhcp relay information option format-type remote-id *word*	word: (1..63) символов	Задать идентификатор remote-id .
no ip dhcp relay information option format-type remote-id		Удалить идентификатор remote-id.
ip dhcp relay information option format-type access-node-id *word*	word: (1..48) символов/ идентификатор устройства не назначен	Установить строку идентификации устройства доступа.
no ip dhcp relay information option format-type access-node-id		Восстановить настройки по умолчанию.

ip dhcp relay information option suboption-type {tr101 | custom}	—/tr101	Настроить формат опции 82. - **tr101** — устанавливает формат опции 82 согласно синтаксису, принятому в рекомендациях TR-101 (см. таблицу 255); - **custom** — устанавливает формат опции 82 в соответствии с форматом, приведенном в таблице 256.
no ip dhcp relay information option suboption-type		Вернуть значение по умолчанию.
ip dhcp relay information policy {keep | replace | drop}	—/keep	Определить режим обработки DHCP-пакетов с опцией 82: **- keep** – пропускает пакеты без изменений; **- replace** – замещает содержимое опции 82; **- drop** – отбрасывает пакеты с опцией 82.
no ip dhcp relay information policy		Установить режим по умолчанию.
ip dhcp relay source-port *port*	port: (0..65535)/67	Использовать в качестве источника заданный UDP-порт.
no ip dhcp relay source-port		Восстановить настройки по умолчанию.

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 279 – Команды режима конфигурации интерфейса VLAN, интерфейса Ethernet

Команда	***Значение/Значение по умолчанию***	***Действие***
ip dhcp relay enable	по умолчанию агент выключен	Включить функции DHCP Relay-агента на настраиваемом интерфейсе.
no ip dhcp relay enable		Выключить функции DHCP Relay-агента на настраиваемом интерфейсе.

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

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

Таблица 280 — Команды режима конфигурации интерфейса Ethernet

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 281 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip dhcp relay [vrf *vrf_name***]**	vrf_name: {1..32} символа	Отобразить конфигурацию настроенной функции DHCP Relay-агента для коммутатора и отдельно для интерфейсов, а также список доступных серверов.

Примеры выполнения команд

- Показать состояние функции DHCP Relay агента:

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

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

5.29.2. Функции DHCP Relay для IPv6 и Lightweight DHCPv6 Relay Agent (LDRA)

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

Функция LDRA позволяет вставить в клиентские DHCPv6-пакеты опции 18 и 37, не изменяя формат пакета. Полновесный DHCPv6 Relay позволяет осуществлять передачу DHCPv6-пакетов от клиента к серверу и обратно в случае, если DHCPv6-сервер находится в одной сети, а клиент в другой. Другой функцией является добавление опций 18 и 37 в DHCPv6-запросы клиента. Принцип работы

полновесного DHCPv6 Relay агента на коммутаторе: коммутатор принимает от клиента DHCP-запросы, передает эти запросы серверу от имени клиента (оставляя в запросе опции с требуемыми клиентом параметрами и, в зависимости от конфигурации, добавляя свои опции). Получив ответ от сервера, коммутатор передает его клиенту.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 282 – Команды режима глобального конфигурирования

Команда	***Значение/ Значение по умолчанию***	***Действие***
ipv6 dhcp relay destination {*ipv6_multicast_address* | gigabitethernet *gi_port* | tengigabitethernet *te_port* |port-channel *group* | tunnel *tunnel_id* | vlan *vlan_id* }	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..4); group: (1..48) tunnel_id: (1..16) vlan_id: (1..4094)	Указать адрес DHCP-сервера или настроить исходящий интерфейс.
no ipv6 dhcp relay destination {*ipv6_multicast_address* | gigabitethernet *gi_port* | tengigabitethernet *te_port* |port-channel *group* | tunnel *tunnel_id* | vlan *vlan_id* }		Удалить адрес DHCP-сервера или исходящий интерфейс.
ipv6 dhcp information option format-type interface-id *word*	word: (1..63) символов	Задать идентификатор порта (опция 18).
no ipv6 dhcp information option format-type interface-id		Удалить идентификатор порта.
ipv6 dhcp information option format-type remote-id *word*	word: (1..63) символов	Задать идентификатор remote-id (опция 37).
no ipv6 dhcp information option format-type remote-id		Удалить идентификатор remote-id.
Ivp6 dhcp guard policy *word*	word: (1..32) символов	Создать политику DHCPv6 Relay и войти в режим её конфигурирования.
no ipv6 dhcp guard policy *word*		Удалить политику DHCPv6 Relay.
ipv6 dhcp guard preference minimum *preference* **maximum** *preference*	preference: (0..255)	Настроить минимальную и максимальную границу для preference, отправляемого в Advertise dhcpv6 сообщении от сервера клиенту. Advertise dhcpv6 сообщения с выходящими за границу preference будут отброшены.
no ipv6 dhcp guard preference minimum maximum *preference*		Удалить минимальную и максимальную границу для preference.

Команды режима конфигурирования политики DHCPv6 Relay

Вид запроса командной строки:

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

Таблица 283 – Команды режима конфигурирования политики DHCPv6 Relay

Команда	***Значение/ Значение по умолчанию***	***Действие***
device-role {client | server}	word: (1..63) символов	Задать роль порта, к которому привязана политика. Порт может быть обозначен как доверенный — в сторону сервера и как недоверенный — в сторону клиента.
no device-role		Удалить роль порта, к которому привязана политика.
match reply disable	—/выключено	Отключить проверку выданных сервером адресов в полученных сообщениях DHCPv6.
no match reply		Включить проверку выданных сервером адресов в полученных сообщениях DHCPv6.
match reply prefix-list *word*	word: (1..32) символов	Настроить фильтрацию выданных сервером адресов в полученных сообщениях DHCPv6 согласно prefix-list.
no match reply		Отключить фильтрацию выданных сервером адресов в полученных сообщениях DHCPv6 согласно prefix-list.
match server address disable	—/выключено	Отключить проверку адреса сервера в полученных сообщениях DHCPv6.
no match server address		Включить проверку адреса сервера сервером адресов в полученных сообщениях DHCPv6.
match server address prefix-list word	word: (1..32) символов	Настроить фильтрацию адреса сервера в полученных сообщениях DHCPv6 согласно prefix-list.
no match server address		Отключить фильтрацию адреса сервера в полученных сообщениях DHCPv6 согласно prefix-list.

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки:

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

Таблица 284 – Команды режима конфигурирования интерфейса Ethernet

Команда	***Значение/ Значение по умолчанию***	***Действие***
ipv6 dhcp relay destination {*ipv6_multicast_address* | **gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* |**port-channel** *group* | **tunnel** *tunnel_id* | **vlan** *vlan_id* **}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..4); group: (1..48) tunnel_id: (1..16) vlan_id: (1..4094)	Указать адрес DHCP-сервера или настроить исходящий интерфейс.
no ipv6 dhcp relay destination {*ipv6_multicast_address* | **gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* |**port-channel** *group* | tunnel *tunnel_id* | vlan *vlan_id* **}**		Удалить адрес DHCP-сервера или исходящий интерфейс.
ipv6 dhcp relay information option format-type interface-id *word*	word: (1..63) символов	Задать идентификатор порта (опция 18)

no ipv6 dhcp relay information option format-type interface-id		Восстановить значение по умолчанию.
ipv6 dhcp relay information option format-type remote-id *word*	word: (1..63) символов	Задать идентификатор remote-id (опция 37)
no ipv6 dhcp relay information option format-type remote-id		Восстановить значение по умолчанию.
ipv6 dhcp guard attach-policy *word* **[vlan** *vlan_id***]**	word: (1..32) символов vlan_id: (1..4094)	Привязать политику к интерфейсу.
no ipv6 dhcp guard attach-policy *word*		Отвязать политику от интерфейса.
ipv6 dhcp guard preference minimum preference maximum preference	preference: (0..255)	Настроить минимальную и максимальную границу для preference, отправляемого в Advertise dhcpv6 сообщении от сервера клиенту. Advertise dhcpv6 сообщения с выходящими за границу preference будут отброшены.
no ipv6 dhcp guard preference minimum maximum preference		Удалить минимальную и максимальную границу для preference.

Команды режима конфигурирования интерфейса VLAN

Вид запроса командной строки:

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

Таблица 285 – Команды режима конфигурирования интерфейса VLAN

Команда	***Значение/ Значение по умолчанию***	***Действие***
ipv6 dhcp relay destination {*ipv6_multicast_address* | **gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* |**port-channel** *group* | **tunnel** *tunnel_id* | vlan *vlan_id* }	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..4); group: (1..48) tunnel_id: (1..16) vlan_id: (1..4094)	Указать адрес DHCP-сервера или настроить исходящий интерфейс.
no ipv6 dhcp relay destination {*ipv6_multicast_address* | **gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* |**port-channel** *group* | **tunnel** *tunnel_id* | **vlan** *vlan_id* }		Удалить адрес DHCP-сервера или исходящий интерфейс.
ipv6 dhcp relay information option format-type interface-id *word*	word: (1..63) символов	Задать идентификатор порта (опция 18).
no ipv6 dhcp relay information option format-type interface-id		Восстановить значение по умолчанию.
ipv6 dhcp relay information option format-type remote-id *word*	word: (1..63) символов	Задать идентификатор remote-id (опция 37).
no ipv6 dhcp relay information option format-type remote-id		Восстановить значение по умолчанию.
ipv6 dhcp guard [attach-policy *word***]**	word: (1..32) символов vlan_id: (1..4094)	Привязать политику к интерфейсу.
no ipv6 dhcp guard [attach-policy *word***]**		Отвязать политику от интерфейса.
ipv6 dhcp ldra	—/выключено	Включить Lightweight DHCPv6 Relay Agent (LDRA).

no ipv6 dhcp ldra		Включить Lightweight DHCPv6 Relay Agent (LDRA).
ipv6 first hop security [attach-policy *word***]**	—/выключено	Разрешить работу функций DHCPv6 guard, Relay, LDRA, ICMPv6, DHCPv6.
no ipv6 first hop security [attach-policy *word***]**		Запретить работу функций DHCPv6 guard, Relay, LDRA, ICMPv6, DHCPv6.

Пример настройки DHCPv6 LDRA:

```
console#
console# configure
console(config)#ipv6 dhcp guard policy DHCP_RELAY_TRUST
console(config-dhcp-guard)#device-role server
console(config-dhcp-guard)#exit
console(config)#!
console(config)#interface gigabitethernet1/0/12
console(config-if)#ipv6 dhcp relay information option format-type interface-
id Gi12
console(config-if)#ipv6 dhcp relay information option format-type remote-id
RTT-A230
console(config-if)#exit
console(config)#!
console(config)#interface gigabitethernet1/0/24
console(config-if)#ipv6 dhcp guard attach-policy DHCP_RELAY_TRUST
console(config-if)#exit
console(config)#!
console(config)#interface vlan 1
console(config-if)#ipv6 dhcp ldra
console(config-if)#ipv6 dhcp guard
console(config-if)#ipv6 first hop security
```

5.30. Конфигурация PPPoE Intermediate Agent

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

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

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 286 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
pppoe intermediate-agent	-/отключен	Разрешить работу PPPoE Intermediate Agent.
no pppoe intermediate-agent		Запретить работу PPPoE Intermediate Agent.
pppoe intermediate-agent timeout *seconds*	seconds :(0..600)/300	Установить лимит времени неактивности пользователя.
no pppoe intermediate-agent timeout		Восстановить настройки по умолчанию.
pppoe intermediate-agent format-type access-node-id *word*	word: (1..48) символа/ идентификатор устройства не назначен.	Установка строки идентификации устройства доступа.
no pppoe intermediate-agent format-type access-node-id		Восстановить настройки по умолчанию.
pppoe intermediate-agent format-type generic-error-message *word*	word: (1..128) символа/PPPoE Discover packet is too large to process.	Установка текста сообщения об ошибке превышения размера пакета (MTU), отправляемого PPPoE IA в PADO или PADS пакетах. **Примечание:** если сообщение содержит символы пробела, его необходимо заключить в кавычки.
no pppoe intermediate-agent format-type generic-error-message		Восстановить настройки по умолчанию.
pppoe intermediate-agent format-type option {sp | sv | pv | spv | user-defined} delimeter [.,:#/]	-/установлен формат в соответствии с TR-101: slot / port : vlan;	Настройка набора параметров и разделителя между ними, которые используются для формирования подопции circuit -id. В команде используются следующие условные обозначения: - **sp** – slot + port - **sv** – slot + vlan - **pv** – port + vlan - **spv** – slot + port + vlan - **user-defined** – формат определяется пользователем. При определении используются следующие шаблоны: %h: hostname; %p: короткое имя порта, например gi1/0/1; %P: длинное имя порта, например, gigabitethernet 1/0/1; %t: тип порта (значение поля ifTable::ifType в шестнадцатеричном виде); %m: MAC-адрес порта в формате H-H-H-H-H-H-H-H; %M: MAC-адрес системы в формате H-H-H-H-H-H-H-H; %u: номер юнита; %s: номер слота; %n: номер порта (как на лицевой панели); %i: ifIndex порта; %v: идентификатор VLAN. %c: MAC-адрес абонентского устройства; %a[vlan_id]: IP-адрес интерфейса VLAN. Если vlan_id не указан, то подставляется IP-адрес интерфейса default vlan. Если IP-адрес не найден, подставляется адрес 0.0.0.0.

no pppoe intermediate-agent format-type option		Восстановить настройки по умолчанию.
pppoe intermediate-agent format-type remote-id *remote_id*	remote_id: (1..128) символов	Назначение идентификатора remote-id, добавляемого коммутатором глобально.
no pppoe intermediate-agent format-type remote-id		Восстанавливает настройку по умолчанию.

Команды режима конфигурации интерфейса

Вид запроса командной строки в режиме конфигурации интерфейса:

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

Таблица 287 – Команды режима конфигурации интерфейса Ethernet, группы портов

Команда	***Значение/Значение по умолчанию***	***Действие***
pppoe intermediate-agent	-/запрет	Разрешение работы PPPoE Intermediate Agent на интерфейсе.
no pppoe intermediate-agent		Запрет работы PPPoE Intermediate Agent на интерфейсе.
pppoe intermediate-agent format-type circuit-id *circuit_id*	circuit_id: (1..63) символов	Назначение идентификатора circuit-id, добавляемого коммутатором. Идентификатор, заданный в команде, полностью переопределяет идентификатор, вычисляемый на основе глобальных параметров **access-node-id** и **option/delimeter**.
no pppoe intermediate-agent format-type circuit-id		Восстанавливает настройку на основе глобальных параметров access-node-id и option/delimeter.
pppoe intermediate-agent format-type remote-id *remote_id*	remote_id: (1..63) символов/MAC-адрес коммутатора.	Назначение идентификатора remote-id, добавляемого коммутатором. Идентификатор должен быть сконфигурирован на всех интерфейсах коммутатора, где работает PPPoE IA.
no pppoe intermediate-agent format-type remote-id		Восстанавливает настройку по умолчанию.
pppoe intermediate-agent trust	-/не является доверенным.	Управление режимом доверия к интерфейсу. Команда добавляет интерфейс к списку доверенных. Интерфейсы, к которым подключены PPPoE-серверы, настраиваются как доверенные. Интерфейсы, к которым подключены пользователи, настраиваются как недоверенные.
no pppoe intermediate-agent trust		Восстанавливает значение по умолчанию.
pppoe intermediate-agent vendor-tag strip	-/выключен	Разрешение удаления vendor-specific опции из пакетов PADO, PADS, PADT перед отправкой их в сторону пользователя. Функция удаления может быть использована только на интерфейсе, на котором разрешена работа PPPoE IA и который является доверенным интерфейсом. Обычно функция удаления настраивается на интерфейсе, обращенном в сторону PPPoE-сервера.
no pppoe intermediate-agent vendor-tag strip		Выключает режим удаления.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 288 – Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show pppoe intermediate-agent info [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Отображение настроек PPPoE Intermediate Agent. Если в команде явно не задан интерфейс, то команда выполняется для всех интерфейсов, где разрешена работа PPPoE IA и всех доверенных портов.
show pppoe intermediate-agent statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Отображение статистики работы PPPoE Intermediate Agent. Если в команде не задан явно интерфейс, то команда выполняется для всех интерфейсов с разрешенным PPPoE IA и всех доверенных портов.
clear pppoe intermediate-agent statistics [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Очистка статистики работы PPPoE Intermediate Agent. Если в команде не задан явно интерфейс, то команда выполняется для всех интерфейсов с разрешенным PPPoE IA и всех доверенных портов.
show pppoe intermediate-agent sessions [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Отображение всех зарегистрированных клиентских сессий. Если в команде не задан явно интерфейс, то отображаются все сессии с сортировкой по интерфейсам.
clear pppoe intermediate-agent sessions [*mac-address***]**	mac address: (H.H.H или H:H:H:H:H:H или H-H-H-H-H-H)	Закрывает клиентскую сессию. Если не указан mac address, то все сессии.

5.31. 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. Возможна одновременная работа DHCP-сервера и DHCP-relay.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 289 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip dhcp server	—/выключено	Включить функцию DHCP-сервера на коммутаторе. **Перед включением сервера должны быть отключены DHCP-клиенты во всех VLAN. В т.ч. включенный по умолчанию во VLAN 1.**
no ip dhcp server		Выключить функцию DHCP-сервера на коммутаторе.
ip dhcp pool host *name*	name: (1..32) символов	Войти в режим конфигурации статических адресов DHCP-сервера.
no ip dhcp pool host *name*		Удалить конфигурацию DHCP-клиента с заданным именем.
ip dhcp pool network *name*	name: (1..32) символов	Войти в режим конфигурации DHCP-пула адресов DHCP-сервера. - *name* — имя DHCP-пула адресов. **Максимально допустимое количество DHCP pool указано в Таблица 9**
no ip dhcp pool network *name*		Удалить DHCP-пул с заданным именем.
ip dhcp excluded-address *low_address* **[***high_address***]**	—	Указать IP-адрес, 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***]**		Удалить IP-адрес из списка исключений для назначения его DHCP-клиентам.
ip dhcp ping enable	—/выключена	Включить передачу ICMP-запросов на назначаемый IP-адрес, чтобы проверить занятость адреса, прежде чем он будет назначен DHCP-клиенту.
no ip dhcp ping enable		Установить значение по умолчанию.
ip dhcp ping count *number*	number: (1..10)/2	Определить количество отправляемых ICMP-запросов.
no ip dhcp ping count		Установить значение по умолчанию.
ip dhcp ping timeout *time*	time: (300..1000)/500 мс	Определить таймаут, в течение которого DHCP-сервер ожидает ответ с адреса, на который получен ICMP-запрос.
no ip dhcp ping timeout		Установить значение по умолчанию.

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 290 – Команды режима конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
address *ip_address* **{***mask* **|** *prefix_length***}** **{client-identifier** *id* **| hardware-address** *mac_address***}**	—	Зарезервировать IP-адреса для DHCP-клиента вручную. - *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		Удалить зарезервированные IP-адреса.
client-name *name*	name: (1..32) символов	Определить имя DHCP-клиента.
no client-name		Удалить 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 291 – Команды режима конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
address **{***network_number* **| low** *low_address* **high** *high_address***}** **{***mask* **|** *prefix_length***}**	—	Установить 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		Удалить конфигурацию DHCP - пула адресов
lease {*days* **[***hours* **[***minutes***]] | infinite}**	—/1 день	Время аренды IP-адреса, который назначен от DHCP. - **infinite** — время аренды не ограничено; - *days* — количество дней; - *hours* — количество часов; - *minutes* — количество минут.
no lease		Установить значение по умолчанию.
ping enable	—/выключена	Включить передачу ICMP-запросов на назначаемый IP-адрес, чтобы проверить занятость адреса, прежде чем он будет назначен DHCP-клиенту.
no ping enable		Установить значение по умолчанию.

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

Вид запроса командной строки:

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

Таблица 292 – Команды режима конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
default-router *ip_address_list*	По умолчанию список маршрутизаторов не определен.	Определить 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		Установить значение по умолчанию.
dns-server *ip_address_list*	По умолчанию список DNS-серверов не определен.	Определить 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		Установить значение по умолчанию.
domain-name *domain*	domain: (1..32) символов	Определить доменное имя для DHCP-клиентов.
no domain-name		Установить значение по умолчанию.
netbios-name-server *ip_address_list*	По умолчанию список WINS-серверов не определен.	Определить 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		Установить значение по умолчанию.
netbios-node-type {b-node | p-node | m-node | h-node}	По умолчанию тип узла NetBIOS не определен.	Определить тип узла NetBIOS Microsoft для клиентов DHCP: - *b-node* — широковещательный; - *p-node* — точка-точка; - *m-node* — комбинированный; - *h-node* — гибридный.
no netbios-node-type		Установить 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		Установить 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		Установить значение по умолчанию.
bootfile *filename*	filename: (1..128) символов	Указать имя файла, используемого для начальной загрузки DHCP-клиента.
no bootfile		Установить значение по умолчанию.
time-server *ip_address_list*	По умолчанию список серверов не определен.	Определить 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		Установить 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	Настроить 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*		Удалить опции для DHCP-сервера.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 293 – Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
clear ip dhcp binding {*ip_address* **|** ***}**	—	Удалить записи 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	—	Просмотреть конфигурации DHCP-сервера.
show ip dhcp excluded-addresses	—	Просмотреть IP-адреса, которые DHCP-сервер не будет назначать для DHCP-клиентов.
show ip dhcp pool host [*ip_address* **|** *name*]	name: (1..32) символов	Просмотреть конфигурацию 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	Просмотреть конфигурацию DHCP-пула адресов DHCP-сервера: - *name* — имя DHCP-пула адресов.
show ip dhcp binding [*ip_address*]	—	Просмотреть IP-адреса, которые сопоставлены с физическими адресами клиентов, а так же время аренды, способ назначения и состояние IP-адресов.
show ip dhcp server statistics	—	Просмотреть статистику DHCP-сервера.
show ip dhcp allocated	—	Просмотреть активные IP-адреса, выданные 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
```

5.32. 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 списком 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 294 – 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	Создать стандартный список 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*		Создать новый расширенный список ACL для адресации IPv4 и войти в режим его конфигурации (если список с данным именем еще не создан), либо войти в режим конфигурации ранее созданного списка.
no ip access-list extended *access_list*		Удалить расширенный список ACL для адресации IPv4.
ipv6 access-list *access_list* **{deny | permit} {any |** *ipv6_address* **[***ipv6_address_prefix***]}**		Создать новый расширенный список ACL для адресации IPv6. - **deny** — запретить прохождение пакетов с указанными параметрами; - **permit** — разрешить прохождение пакетов с указанными параметрами.
no ipv6 access-list *access_list*		Удалить стандартный список ACL для адресации IPv6.
ipv6 access-list extended *access_list*		Создать новый расширенный список ACL для адресации IPv6 и войти в режим его конфигурации (если список с данным именем еще не создан), либо войти в режим конфигурации ранее созданного списка.
no ipv6 access-list extended *access_list*		Удалить расширенный список ACL для адресации IPv6.
mac access-list extended *access_list*		Создать новый список на базе MAC-адресации и войти в режим его конфигурации (если список с данным именем еще не создан), либо войти в режим конфигурации ранее созданного списка.
no mac access-list extended *access_list*		Удалить список ACL на базе MAC-адресации.
access-list configuration mode {default | commit}	—/default	Установить режим конфигурирования ACL. - **default** — ACL можно редактировать только тогда, когда он не привязан ни к одному из интерфейсов. Настройки правил ACL применяются немедленно. - **commit** — ACL можно редактировать, когда он привязан к физическому или VLAN интерфейсу. Изменения вступают в силу после выполнения команды *access-list commit*.
access-list commit	—	Применить изменения во всех ACL-списках.
access-list commit {access_list}	access_list: (0..32) символа	Применить изменения в определенном ACL-списке.

access-lists statistics { port | vlan }	—/выключено	Включить статистику списков ACL - **port** — только для списков ACL, привязанных к физическим интерфейсам; - **vlan** — только для списков ACL, привязанных к интерфейсам VLAN. **Для коммутаторов серии RTT-230 возможно включение статистики списков ACL, привязанных только к физическим портам или только к интерфейсам VLAN.**
no access-lists statistics { port | vlan }		Выключить статистику списков ACL.
time-range *time_name*	time_name: (0..32) символа	Войти в режим конфигурации time-range и определить временные интервалы для списка доступа. - *time_name* — имя профиля настроек time-range.
no time-range *time_name*		Удалить заданную конфигурацию 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 295 – Команда назначения списка ACL-интерфейсу

Команда	***Значение/Значение по умолчанию***	***Действие***
service-acl {input | output} *access_list*	access_list: (0..32) символа	В настройках определённого физического интерфейса привязать указанный список к данному интерфейсу. **Привязка к интерфейсу VLAN возможна только для направления input.** **Под действие ACL, назначаемого на interface vlan, попадает не только маршрутизируемый трафик, но и трафик внутри сети.** **Под действие ACL, назначаемого на interface vlan, попадает весь входящий в порты трафик в данной VLAN.**
no service-acl {input | output}		Удалить список с интерфейса.

Команды режима Privileged EXEC

Командная строка в режиме Privileged EXEC имеет вид:

```
console#
```

Таблица 296 – Команды для просмотра списков ACL

Команда	*Значение/Значение по умолчанию*	*Действие*
show access-lists [*access_list*]	access_list: (0..32) символа	Показать списки ACL, созданные на коммутаторе.
show access-lists time-range-active [*access_list*]		Показать списки ACL, созданные на коммутаторе, которые в настоящее время являются активными.
show interfaces access-lists [**gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id*]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094);	Показать списки ACL, назначенные интерфейсам.
clear access-lists counters [**gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id*]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Обнулить все счетчики списков ACL, либо счетчики для списков ACL заданного интерфейса.
show interfaces access-lists trapped packets [**gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id*]	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Показать счетчики списков доступа.
clear access-lists statistics	—	Очистить статистику списков ACL.
show access-lists candidate-config	—	Показать состояние всех ACL-списков после выполнения команды *access-list commit.*
show access-lists candidate-config {access_list}	access_list: (0..32) символа	Показать состояние определенного ACL-списка после выполнения команды *access-list commit.*
show candidate-config access-list	—	Показать, как будут выглядеть ACL-списки в show running-config после выполнения команды *access-list commit*.

Команды режима EXEC

Командная строка в режиме EXEC имеет вид:

```
console#
```

Таблица 297 – Команды для просмотра списков ACL

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

5.32.1. 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 RustelAL необходимо выполнить следующие команды:

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

При одновременном использовании правил с параметром offset-list и правил с параметром UDP/TCP-порт (permit/deny tcp/udp any src_tcp/udp_port any dst_tcp/udp_port) существует аппаратное ограничение. Для их совместной работы необходимо при создании offset-листа, помимо нужных байтов, указать байты TCP/UDP-портов из L4-заголовка.

Таблица 298 – Основные параметры, используемые в командах

Параметр	*Значение*	*Действие*
permit	-	Создать разрешающее правило фильтрации в списке ACL.
deny	-	Создать 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	Определить IP-адрес источника пакета.
source_wildcard	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	Определить IP-адрес назначения пакета.
destination_wildcard	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	vlan: (1..4094)	Определить VLAN, для которого будет применяться правило.
dscp	dscp: (0..63)	Определить значение DSCP-поля diffserv.
precedence	precedence: (0..7)	Определить приоритет IP-трафика.
time_name	time_name: (0..32) символов	Определить конфигурацию временных интервалов.

icmp_type	тип сообщения протокола ICMP	Используется 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	icmp_code: (0..255)	Код сообщений протокола ICMP, используемый для фильтрации ICMP-пакетов.
igmp_type	тип сообщения протокола IGMP	Тип сообщений протокола IGMP, используемый для фильтрации пакетов IGMP. Возможные типы сообщений поля *igmp_type*: *host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3*, либо числовое значение типа сообщения, в диапазоне (0–255).
destination_port	UDP/TCP-порт назначения	Возможные значения поля TCP-порта: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110, syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80); Для UDP-порта: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177). Либо числовое значение (0– 65535).
source_port	UDP/TCP-порт источника	
list_of_flags	флаги протокола TCP	Если для условия фильтрации флаг должен быть установлен, то перед ним ставится знак «+», если не должен быть установлен, то «-». Возможные варианты флагов: **+urg**, **+ack**, **+psh**, **+rst**, **+syn**, **+fin**, **-urg**, **-ack**, **-psh**, **-rst**, **-syn** и **-fin**. При использовании нескольких флагов в условии фильтрации, флаги объединяются в одну строку без пробелов, например: **+fin-ack.**
disable_port	-	Выключить порт, с которого был принят пакет, удовлетворяющий условиям любой из команд запрета **deny,** в составе которой было описано поле**.**
log_input	-	Включить отправку информационных сообщений в системный журнал при получении пакета, который соответствует записи.
offset_list_name	offset_list_name: (0..32) символов	Задать использование списка шаблонов пользователя для распознавания пакетов. Для каждого списка ACL может быть определен свой список шаблонов.
ace-priority	ace-priority: (1..2147483647)	Индекс задает положение правила в списке и его приоритет. Чем меньше индекс — тем приоритетнее правило. Значение индекса должно быть уникальным в рамках списка правил в одном ACL.

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

Если пакет попадает под критерий правила в ACL, то над ним выполняется действие этого правила (permit/deny). Дальнейшая проверка не производится.

Если на интерфейс назначены IP и MAC ACL, то первоначально пакет будет проверен на соответствие правилам IP ACL, потом — MAC ACL (в случае, если не попадет под действие ни одного из правил IP ACL).

Если после проверки на соответствие правилам IP или MAC ACL (когда 1 ACL назначен на интерфейс) или IP и MAC ACL (когда 2 ACL назначены на интерфейс) пакет не попал под действие ни одного из правил, то к данному пакету будет применено действие “deny any any”.

Таблица 299 – 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***]**	Добавить 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***]**	Удалить созданную ранее запись.
permit ip **{any |** *source_mac source_mac_wildcard***} {any |** *destination_mac destination_mac_wildcard***} {any |** *source_ip source_ip_wildcard***} {any |** *destination_ip destination_ip_wildcard***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *range_name***] [ace priority** *index***]**	Добавить разрешающую запись фильтрации для протокола IP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
no permit ip **{any |** *source_mac source_mac_wildcard***} {any |** *destination_mac destination_mac_wildcard***} {any |** *source_ip source_ip_wildcard***} {any |** *destination_ip destination_ip_wildcard***} [dscp** *dscp* **| precedence** *precedence***] [time-range** *range_name***]**	Удалить 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***]**	Добавить 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***]**	Удалить 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***]**	Добавить 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***]**	Удалить 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***]**	Добавить 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***]**	Удалить 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***]**	Добавить 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***]**	Удалить 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***]**	Добавить 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]**	Удалить 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***]**	Добавить 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]**	Удалить 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***]**	Добавить 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]**	Удалить 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]**	Добавить 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]**	Удалить 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]**	Добавить 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]**	Удалить 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]**	Добавить 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]**	Удалить созданную ранее запись.
offset-list *offset_list_name* **{***offset_base offset mask value***}** …	Создать 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 задан ‘0’; - *value* — искомое значение.
no offset-list *offset_list_name*	Удалить созданный ранее список.
access-list commit	Применить изменения в ACL-списке.

5.32.2. 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 RTTipv6 необходимо выполнить следующие команды:

```
console#
console# configure
console(config)# ipv6 access-list extended RTTipv6
console(config-ipv6-al)#
```

Таблица 300 – Основные параметры, используемые в командах

Параметр	*Значение*	*Действие*
permit	-	Создать разрешающее правило фильтрации в списке ACL.
deny	-	Создать 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	Определить IPv6-адрес и длину префикса сети (0-128) (количество старших бит адреса) источника пакета.
destination_prefix/length	адрес назначения и его длина	Определить IPv6-адрес и длину префикса сети (0-128) (количество старших бит адреса) назначения пакета.
dscp	dhcp: (0..63)	Определить значение DSCP-поля diffserv.
precedence	precedence: (0..7)	Определить приоритет IP-трафика.
time_name	time_name: (1..32) символов	Определить 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	icmp_code: (0..255)	Используется для фильтрации ICMP-пакетов.
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	-	Выключить порт, с которого был принят пакет, удовлетворяющий условиям любой из команд запрета **deny,** в составе которой было описано поле**.**
log-input	-	Включить отправку информационных сообщений в системный журнал при получении пакета, который соответствует записи.
ace-priority	ace-priority: (1..2147483647)	Индекс правила в таблице. Чем меньше индекс — тем приоритетнее правило. Значение индекса должно быть уникальным в рамках списка правил в одном ACL.

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 301 – 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***]**	Добавить 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***]**	Удалить 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***]**	Добавить 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***]**	Удалить 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***]**	Добавить 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***]**	Удалить 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***]**	Добавить 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***]**	Удалить 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***]**	Добавить 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]**	Удалить 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***]**	Добавить 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]**	Удалить 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***]**	Добавить 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]**	Удалить 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***]**	Добавить 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]**	Удалить созданную ранее запись.
offset-list *offset_list_name* **{***offset_base offset mask value***}** …	Создать 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 задан ‘0’; - *value* — искомое значение.
no offset-list *offset_list_name*	Удалить созданный ранее список.
access-list commit	Применить изменения в ACL-списке.

5.32.3. 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 RTTmac необходимо выполнить следующие команды:

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

При одновременном использовании правил с параметром offset-list и правил с параметром EtherType (permit/deny any any EtherType) существует аппаратное ограничение. Для их совместной работы необходимо при создании offset-листа, помимо нужных байтов, указать байты EtherType.

Таблица 302 – Основные параметры, используемые в командах

Параметр	*Значение*	*Действие*
permit	-	Создать разрешающее правило фильтрации в списке ACL.
deny	-	Создать запрещающее правило фильтрации в списке ACL.
source	-	Определить MAC-адрес источника пакета.
source_wildcard	wildcard-маска адреса источника	Маска определяет биты MAC-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Например, используя маску, можно определить для правила фильтрации диапазон 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	MAC-адрес назначения пакета	Определить MAC-адрес назначения пакета.
destination_wildcard	wildcard-маска адреса назначения	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: (1..4094)	Подсеть VLAN фильтруемых пакетов.
cos	cos: (0..7)	Класс обслуживания (CoS) фильтруемых пакетов.
cos_wildcard	wildcard-маска класса 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	-	Выключить порт, с которого был принят пакет, удовлетворяющий условиям команды запрета **deny.**
log-input	-	Включить отправку информационных сообщений в системный журнал при получении пакета, который соответствует записи.
time_name	time_name: (1..32) символов	Определить конфигурацию временных интервалов.

offset_list_name	offset_list__name: (1..32) символов	Задать использование списка шаблонов пользователя для распознавания пакетов. Для каждого списка ACL может быть определен свой список шаблонов.
ace-priority	ace-priority: (1..2147483647)	Индекс правила в таблице. Чем меньше индекс — тем приоритетнее правило. Значение индекса должно быть уникальным в рамках списка правил в одном ACL.

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

Если пакет попадает под критерий правила в ACL, то над ним выполняется действие этого правила (permit/deny). Дальнейшая проверка не производится.

Если на интерфейс назначены IP и MAC ACL, то первоначально пакет будет проверен на соответствие правилам IP ACL, потом — MAC ACL (в случае, если не попадет под действие ни одного из правил IP ACL).

Если после проверки на соответствие правилам IP или MAC ACL (когда 1 ACL назначен на интерфейс) или IP и MAC ACL (когда 2 ACL назначены на интерфейс) пакет не попал под действие ни одного из правил, то к данному пакету будет применено действие "deny any any".

Таблица 303 – 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***]**	Добавить 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***]**	Удалить 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***]**	Добавить 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***]**	Удалить созданную ранее запись.
offset-list *offset_list_name* **{***offset_base offset mask value***}** …	Создать 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 задан '0'; - *value* — искомое значение.

no offset-list *offset_list_name*	Удалить созданный ранее список.
access-list commit	Применить изменения в ACL-списке.

5.33. 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 304 – Команды для настройки защиты от DoS-атак

Команда	*Значение/Значение по умолчанию*	*Действие*
ip martian-address filtering	—/включено	Включить фильтрацию пакетов с адресами источника и назначения из сети 0.0.0.0/8.
no ip martian-address filtering		Выключить фильтрацию пакетов с адресами источника и назначения из сети 0.0.0.0/8.
security-suite deny martian-addresses {add | remove} *ip_address*	ip_address:mask/—	Настроить или удалить диапазон IP-адресов. Пакеты с IP-адресом источника или назначения, попадающие под настроенный диапазон, будут отброшены.
security-suite deny martian-addresses reserved {add | remove}	add/—	Настроить или удалить фильтр для зарезервированных IP-адресов. Зарезервированными считаются следующие адреса: 0.0.0.0/8 — адреса источника и назначения (исключение — адрес источника 0.0.0.0); 127.0.0.0/8 — адреса источника и назначения; 192.0.2.0/24 — адреса источника и назначения; 224.0.0.0/4 — только адреса источника; 240.0.0.0/4 — адреса источника и назначения (исключение — адрес назначения 255.255.255.255).
security-suite deny syn-fin	—/включено	Отбросить TCP-пакеты с одновременно установленными SYN- и FIN- флагами**.**
no security-suite deny syn-fin		Выключить функцию отбрасывания TCP-пакетов с одновременно установленными SYN- и FIN- флагами.
security-suite dos protect {add | remove} {stacheldraht | invasor-trojan | back-orifice-trojan}	—	Запретить/разрешить 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 [global-rules-only]	—/выключено	Включить класс команд security-suite. - **global-rules-only** — отключает класс команд security-suite на интерфейсах. **Не влияет на работу команды security-suite deny syn-fin.**
no security-suite enable		Отключить класс команд security-suite.

security-suite syn protection mode {block | report | disabled}	—/block	Настроить режим защиты от SYN-атак: **- block** — отбрасывает предназначенные устройству TCP-пакеты с установленным флагом SYN и формирует предупреждающее сообщение; **- report** — формирует предупреждающее сообщение при приходе предназначенного устройству TCP-пакета с установленным флагом SYN; **- disable** — отключает защиту.
no security-suite syn protection mode		Настроить режим по умолчанию.
security-suite syn protection recovery *sec*	sec: (10..600) / 60	Определить интервал, по истечении которого будет разблокирован ранее заблокированный источник SYN-атаки.
no security-suite syn protection recovery		Установить значение по умолчанию.
security-suite syn protection threshold *rate*	rate: (20..200) / 80	Определить скорость (количество пакетов в секунду) от конкретного источника, при которой этот источник будет идентифицирован как атакующий.
no security-suite syn protection threshold		Установить значение по умолчанию.
security-suite syn protection statistics	—/выключено	Включить ведение статистики SYN-атак.
no security-suite syn protection statistics		Выключить ведение статистики SYN-атак.

Команды режима конфигурации интерфейса Ethernet, группы портов.

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

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

Таблица 305 – 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	Создать правило, запрещающее прохождение трафика, соответствующего критериям. - **fragmented** — фрагментированные пакеты - **icmp** — ICMP-трафик **- syn** — SYN-пакеты
no security-suite deny {fragmented | icmp | syn}		Удалить 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	Задать порог SYN-запросов на определенный IP-адрес/сеть, при превышении которого лишние кадры будут отбрасываться.
no security-suite dos syn-attack {any | *ip_address* [*mask*]}		Восстановить значение по умолчанию.

Команды режима privileged EXEC

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 306 — Команда режима privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show security-suite configuration		Отобразить настройки защиты от DoS-атак.
show security-suite syn protection {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Отобразить настройки защиты от SYN-атак и оперативное состояние интерфейсов.
show security-suite syn protection statistics [detailed] [source-ip *ip_address* **| interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Отобразить настройки статистики защиты от SYN-атак и информацию об источниках атаки. **- detailed** — отображает дополнительную информацию об источнике атаки; **- source-ip** — отображает информацию для указанного IP-адреса источника; **- interface** — отображает информацию для указанного интерфейса. **В статистике сохраняется информация о 512 последних источниках атак.**
clear security-suite syn protection statistics		Очистить статистику об источниках SYN-атак.

5.34. 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.

5.34.1. Настройка QoS

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 307 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip tx-dscp *value*	value: (0..64)/56	Установить значение поля DSCP для IP-пакетов, формируемых центральным процессором.
no ip tx-dscp		Установить значение по умолчанию.
ipv6 tx-user-priority *value*	value: (0..7)/7	Установить значение поля DSCP для пакетов, формируемых центральным процессором.
no ipv6 tx-user-priority		Установить значение по умолчанию.
ip tx-user-priority *value*	value: (0..7)/7	Установить значение поля CoS для тегированных пакетов, формируемых центральным процессором.
no ip tx-user-priority		Установить значение по умолчанию.
qos [basic | advanced [ports-trusted | ports-not-trusted]]	—/basic	Разрешить 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 очередь, которой соответствует cos=0 (соответствие можно посмотреть командой «show qos interface queuing»), для отправки в другие очереди требуется назначать на входной интерфейс стратегию классификации трафика (policy-map). Значения dscp не учитываются при выборе выходной очереди в этом подрежиме.
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		Установить 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. Создать список критериев классификации трафика. 2. Войти 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*		Удалить список критериев классификации трафика.
policy-map *policy_map_name*	policy_map_name: (1..32) символов	1. Создать стратегию классификации трафика. 2. Войти 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*		Удалить правило классификации трафика.
qos aggregate-policer *aggregate_policer_name committed_rate_kbps committed_burst_byte* **[exceed-action {drop | policed-dscp-transmit}] [peak peak_rate_kbps peak_burst_byte [violate-action {drop | policed-dscp-transmit}]]}]**	aggregate_policer_name: (1..32) символа; committed_rate_kbps: (3..57982058) кбит/с; committed_burst_byte: (3000..19173960) байт; peak_rate_kbps: (3..57982058) кбит/с; peak_burst_byte: (3000..19173960) байт	Определить шаблон настроек, который позволяет ограничить полосу пропускания канала. 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; - *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; - **peak** — установить пороговое значение скорости трафика с переопределенными значениями DSCP; - **violate-action** — установить действие над пакетом после превышения порогового значения. **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.** **Параметр policed-dscp-transmit позволяет при превышении значения** *commited_rate* **или** *peak_rate* **передать пакет дальше, изменив в нем метку dscp, которая настраивается командой qos map policed-dscp с дополнительным аргументом violation в случае с peak_rate. При этом при превышении** *commited_rate* **и** *peak_rate* **можно настраивать разные значения dscp.**
no qos aggregate-policer *aggregate_policer_name*		Удалить шаблон настроек регулирования скорости канала.

qos aggregate-policer *aggregate_policer_name* **pps** *committed_rate_pps committed_burst_packet* **[exceed-action {drop | policed-dscp-transmit [peak** *peak_rate_pps peak_burst_packet* **[violate-action {drop | policed-dscp-transmit}]]}]**	committed_rate_pps: (125..19531250) pps; committed_burst_packet: (1..19531250) пакетов; aggregate_policer_name: (1..32) символов; peak_rate_pps: (125..19531250) pps; peak_burst_packet: (1..19531250) пакетов	Определить 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_pps* — среднее значение скорости трафика в pps; - *excess_burst_packet* — размер сдерживающего порога в пакетах; - **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.** **Параметр policed-dscp-transmit позволяет при превышении значения** *commited_rate* **или** *peak_rate* **передать пакет дальше, изменив в нем метку dscp, которая настраивается командой qos map policed-dscp с дополнительным аргументом violation в случае с peak_rate. При этом при превышении** *commited_rate* **и** *peak_rate* **можно настраивать разные значения dscp.**
no qos aggregate-policer aggregate_policer_name		Удалить шаблон настроек регулирования скорости канала.
wrr-queue cos-map *queue_id cos1…cos8*	queue_id: (1..8); cos1…cos8: (0..7); Значения CoS по умолчанию для очередей: CoS = 1 — очередь 2 CoS = 2 — очередь 3 CoS = 0 — очередь 1 CoS = 3 — очередь 6 CoS = 4 — очередь 5 CoS = 5 — очередь 8 CoS = 6 — очередь 8 CoS = 7 — очередь 7	Определить значения CoS для очередей исходящего трафика.
no wrr-queue cos-map [*queue_id***]**		Установить значение по умолчанию.
wrr-queue bandwidth *weight1..weight8*	weight: (0..255); значение по умолчанию определяется количеством настроенных очередей WRR. Например, если настроено 5 очередей WRR, то настройка по умолчанию будет иметь вид: wrr-queue bandwidth 1 2 4 8 16	Присвоить вес исходящим очередям, используемый механизмом WRR (Weighted Round Robin — весовой механизм распределения нагрузки).
no wrr-queue bandwidth		Установить 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».	Задать 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		Установить значение по умолчанию.
qos wrr-queue wrtd	по умолчанию WRTD выключено	Включить WRTD (Weighted Random Tail Drop) весовой механизм удаления пакетов из очередей. **Изменения вступят в силу после перезагрузки устройства.**
no qos wrr-queue wrtd		Выключить WRTD.
qos map enable {cos-dscp | dscp-cos}	—/выключено	Использовать заданную таблицу перемаркировки для доверенных портов коммутатора.
no qos map enable {cos-dscp | dscp-cos}		Не использовать таблицу перемаркировки.
qos map dscp-dp *dscp_list* **to** *dp*	dscp_list: (0..63); dp: (0..2) По умолчанию все пакеты имеют приоритет сброса dp=0	Поставить в соответствие значению DSCP приоритет сброса (чем выше числовое значение приоритета, тем ниже вероятность того, что пакет будет отброшен; в первую очередь отбрасываются пакеты с приоритетом сброса 0, затем 1, затем 2). - *dscp_list* — определяет до 8 значений DSCP, значения разделяются знаком пробела. **Действует только для режима qos advanced.**
no qos map dscp-dp [*dscp_list*]		Установить значения по умолчанию.
qos map dscp-cos *dscp_list* **to** *cos*	dscp_list: (0..63); cos: (0..7)	Заполнить таблицу перемаркировки DSCP. Заменяет значение DSCP на CoS.
no qos map dscp-cos [*dscp_list*]		Вернуться к значениям по умолчанию.
qos map cos-dscp *cos* **to** *dscp_list*	dscp_list: (0..63); cos: (0..7)	Заполнить таблицу перемаркировки CoS. Заменяет значение CoS на DSCP.
no qos map cos-dscp [*cos*]		Вернуться к значениям по умолчанию.
qos map policed-dscp [violation] *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	Заполнить 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. - **violation** — задать новое значение DSCP в пакете при превышении значения *peak_rate*. **Действует только для режима qos advanced.**
no qos map policed-dscp [*dscp_list*]		Установить значение по умолчанию.
qos map dscp-queue *dscp_list* **to** *queue_id*	dscp_list: (0..63) queue_id: (1..8) Значения по умолчанию:	Установить 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	Установить значение по умолчанию.
qos trust {cos | dscp | cos-dscp}	—/dscp	Установить 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		Установить значение 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.**
no qos dscp-mutation		Отменить 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	Заполнить 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.
no qos map dscp-mutation [*in_dscp*]		Установить значение по умолчанию.
rate-limit vlan *vlan_id rate burst*	vlan_id: (1..4094); rate: (3..57982058) кбит/с; burst: (3000..19173960) байт/128 кбайт	Установить 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*		Снять ограничение скорости входящего трафика.
rate-limit vlan *vlan_id* **pps** *rate_pps burst_packet*	vlan_id: (1..4094); rate_pps: (125.. 19531250) pps burst_pps: (1..19531250) пакетов	Установить ограничение скорости для входящего трафика для заданной VLAN. - *vlan_id* — номер VLAN: - *rate_pps* — количество пакетов в секунду. - *burst_packet* — размер сдерживающего порога (ограничение скорости) в пакетах.
no rate-limit vlan *vlan_id*		Снять ограничение скорости входящего трафика.

qos tail-drop mirror-limit {rx | tx} limit	limit: (0..7000)/3500	Настроить распределение ресурсов буфера для скопированных пакетов в контролирующий порт. - **rx** — скопированные пакеты, принятые контролируемым портом; - **tx** — скопированные пакеты, переданные контролируемым портом.
no qos tail-drop mirror-limit {rx | tx}		Установить значение по умолчанию.
qos tail-drop multicast replication-limit	—/выключено	Включить ограничение репликации multicast-пакетов.
no qos tail-drop multicast replication-limit		Выключить ограничение репликации multicast-пакетов.
traffic-limiter mode {kbps | pps}	/kbps	Установить режим работы ограничения трафика. - **kbps** — ограничение входящих килобит в секунду; - **pps** — ограничение входящих пакетов в секунду; **Данная команда изменяет режим работы для следующего функционала: storm-control, rate-limit, rate-limit vlan, police, qos aggregate-policer.** **Выбранный режим должен соответствовать настройкам ограничения трафика иначе ограничения трафика не произойдет. Например: команда storm-control unicast kbps не будет ограничивать трафик, если введена команда traffic-limiter mode pps.**

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 308 – Команды режима редактирования списка критериев классификации трафика

Команда	*Значение/Значение по умолчанию*	*Действие*
match access-group *acl_name*	acl_name: (1..32) символов	Добавить критерий классификации трафика. Определяет правила фильтрации трафика по списку ACL для классификации. **Действует только для режима qos advanced.**
no match access-group *acl_name*		Удалить 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 309 – 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	Определить правило классификации трафика и войти 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*		Удалить 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 310 – Команды режима конфигурации правила классификации

Команда	*Значение/Значение по умолчанию*	*Действие*
mirror {*monitor_session*}	monitor_session: 1	Указать номер monitor сессии для зеркалирования трафика.
no mirror {*monitor_session*}		Отменить зеркалирование.
trust	По умолчанию режим доверия не установлен	Определить режим доверия к определенному типу трафика согласно глобальному режиму доверия.
no trust		Установить 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)	Установить 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		Удалить новые значения для IP-пакета.

redirect {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group***}**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48)	Направить пакеты, удовлетворяющие правилу классификации трафика, в указанный порт.
no redirect		Установить значение по умолчанию.
police *committed_rate_kbps committed_burst_byte* [**exceed-action {drop | policed-dscp-transmit [peak** ***peak_rate_kbps peak_burst_byte*** **[violate-action {drop | policed-dscp-transmit}]]}]**	committed_rate_kbps: (3..12582912) кбит/с; committed_burst_byte: (3000..19173960) байт; peak_rate_kbps: (3..57982058) кбит/с; peak_burst_byte: (3000..19173960) байт	Ограничить полосу пропускания канала. 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; - *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; - **peak** — установить пороговое значение скорости трафика с переопределенными значениями DSCP; - **violate-action** — установить действие над пакетом после превышения порогового значения. **Действует только для режима qos advanced.** **Параметр policed-dscp-transmit позволяет при превышении значения** *committed_rate* **или** *peak_rate* **передать пакет дальше, изменив в нем метку dscp, которая настраивается командой qos map policed-dscp с дополнительным аргументом violation в случае с** *peak_rate***. При этом при превышении** *committed_rate* **и** *peak_rate* **можно настраивать разные значения dscp.**
police aggregate *aggregate_policer_name*		Назначить правилу классификации трафика шаблон настроек, который позволяет ограничить полосу пропускания канала. **Действует только для режима qos advanced.**
no police		Удалить шаблон настроек регулирования скорости канала из правила классификации трафика.

police pps *committed_rate_pps committed_burst_packet***} [exceed-action {drop | policed-dscp-transmit [***peak peak_rate_pps peak_burst_packet* **[violate-action {drop | policed-dscp-transmit}]]}]**	committed_rate_pps: (125.. 19531250) pps; committed_burst_packet: (1.. 19531250) пакетов; peak_rate_pps: (125..19531250) pps; peak_burst_packet: (1..19531250) пакетов	Ограничить полосу пропускания канала. 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_pps* — среднее значение скорости трафика в pps; - *committed_burst_packet* — размер сдерживающего порога в пакетах; - **drop** — пакет будет отброшен, когда «корзина» переполнится; - **policed-dscp-transmit** — при переполнении «корзины» значение DSCP будет переопределено; - **peak** — установить пороговое значение скорости трафика с переопределенными значениями DSCP; - **violate-action** — установить действие над пакетом после превышения порогового значения. **Действует только для режима qos advanced.** **Параметр policed-dscp-transmit позволяет при превышении значения** *committed_rate* **или** *peak_rate* **передать пакет дальше, изменив в нем метку dscp, которая настраивается командой qos map policed-dscp с дополнительным аргументом violation в случае с** *peak_rate***. При этом при превышении** *committed_rate* **и** *peak_rate* **можно настраивать разные значения dscp.**
no police		Удалить шаблон настроек регулирования скорости канала из правила классификации трафика.

Команды режима конфигурации профиля qos tail-drop

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

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

Значения лимитов, близких к максимальным, можно использовать, только если расширение лимитов профиля до 400-1500 не помогает избавиться от дропов в выходных очередях.

Таблица 311 — Команды режима конфигурации профиля qos tail-drop

Команда	***Значение/Значение по умолчанию***	***Действие***
port-limit *limit*	RTT-A230, RTT-A330: limit: (0..5902)/88 RTT-A420: limit: (0..7640)/108	Задать размер пакетного разделяемого пула для порта.
no port-limit		Установить значение по умолчанию.

queue *queue_id* **[limit** *limit***] [without-sharing | with-sharing]**	RTT-A230, RTT-A330: limit: (0..5902)/18 RTT-A420: limit: (0..7640)/10 queue_id: (1..8)	Изменить параметры очереди: - *queue_id* — номер очереди; - *limit* — количество пакетов в очереди; - **without-sharing** — запретить доступ к общему пулу; - **with-sharing** — разрешить доступ к общему пулу.
no queue *queue_id*		Установить значение по умолчанию.

Пример настройки tail-drop profile и назначение его на порт:

Создание tail-drop profile:

```
console(config)# qos tail-drop profile 2
console(config-tdprofile)# queue 1 limit 400
console(config-tdprofile)# queue 2 limit 400
console(config-tdprofile)# queue 3 limit 400
console(config-tdprofile)# queue 4 limit 400
console(config-tdprofile)# queue 5 limit 400
console(config-tdprofile)# queue 6 limit 400
console(config-tdprofile)# queue 7 limit 400
console(config-tdprofile)# queue 8 limit 400
console(config-tdprofile)# port-limit 400
```

Назначение tail-drop profile на порт:

```
console(config)# interface Gigabit Ethernet 1/0/1
console(config-tdprofile)# qos tail-drop profile 2
```

Команды режима конфигурации интерфейса Ethernet, группы портов

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

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

Таблица 312 — 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	Назначить интерфейсу стратегию классификации трафика. - **deny-any** — отбросить трафик, не попадающий под действие политики; - **permit-any** — разрешить прохождение трафика, не попадающего под действие политики.
no service-policy {input | output}		Удалить стратегию классификации трафика с интерфейса.
traffic-shape *committed_rate* **[***committed_burst***]**	committed_rate: (64..10000000) кбит/с; committed_burst: (4096..16762902) байт	Установить 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		Снять ограничение скорости исходящего трафика через интерфейс.

traffic-shape queue *queue_id committed_rate* [*committed_burst*]	queue_id: (0..8); committed_rate: (64..10000000) кбит/с; committed_burst: (4096..16762902) байт	Установить 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*		Снять ограничение скорости трафика через интерфейс для исходящей очереди.
qos trust [cos | dscp | cos-dscp]	—/включено	Включить 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		Выключить базовый механизм qos для интерфейса.
rate-limit *rate* **[burst** *burst***]**	rate: (64..10000000) кбит/с; burst: (3000..19173960) байт/128 кбайт	Установить ограничение скорости для входящего трафика.
no rate-limit		Снять ограничение скорости входящего трафика.
rate-limit pps *rate_pps* **[burst** *burst_packet***]**	rate_pps: (125.. 19531250) pps burst_pps: (1.. 19531250) пакетов	Установить ограничение скорости для входящего трафика в pps.
no rate-limit		Снять ограничение скорости входящего трафика.
qos cos *default_cos*	default_cos: (0..7)/0	Установить значение CoS по умолчанию для порта (CoS, применяемый для всего нетегированного трафика, проходящего через интерфейс).
no qos cos		Установить значение по умолчанию.

Команды режима конфигурации интерфейса Vlan

Вид запроса командной строки режима конфигурации интерфейса Vlan:

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

Таблица 313 — Команды режима конфигурации интерфейса Vlan

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 314 — Команды режима EXEC

Команда	***Значение/значение по умолчанию***	***Действие***
show qos	—	Показать 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	Показать списки критериев классификации трафика. **Действует только для режима qos advanced.**
show policy-map [*policy_map_name*]	policy_map_name: (1..32) символа	Показать правила классификации трафика. **Действует только для режима qos advanced.**

show qos aggregate-policer [*aggregate_policer_name*]	aggregate_policer_name: (1..32) символа	Показать настройки средней скорости и ограничения полосы пропускания для правил классификации трафика. **Действует только для режима qos advanced.**
show qos interface [buffers | queuing | policers | shapers] [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Показать QoS-параметры для интерфейса. - *vlan_id* — номер VLAN; - *gi_port* — номер интерфейсов Ethernet g1; - *te_port* — номер интерфейсов Ethernet XG1-XG24; - *fo_port* — номер интерфейсов Ethernet XLG1-XLG4; - *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]	—	Показать информацию о замене полей в пакетах, используемых QOS. - **dscp-queue** — таблица соответствия DSCP и очередей; - **dscp-dp** — таблица соответствия меток DSCP и приоритета сброса (DP); - **policed-dscp** — таблица перемаркировки DSCP; - **dscp-mutation** — таблица изменения DSCP-to-DSCP.
show qos tail-drop	—	Просмотреть параметры tail-drop.
show qos tail-drop [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4);	Просмотреть tail-drop информацию по конкретному порту (всем портам).
show qos tail-drop unit *unit_id*	unit_id: (1..8)	Просмотреть tail-drop информацию по конкретному устройству в стеке.
show ip tx-priority	—	Просмотреть информацию о маркировке трафика, формируемого центральным процессором.

Примеры выполнения команд

- Включить режим QoS advanced. Распределить трафик по очередям, пакеты с DSCP 12 в первую очередь, пакеты с DSCP 16 во вторую. Восьмая очередь — приоритетная. Создать стратегию классификации трафика по списку ACL, разрешающему передачу TCP-пакетов с DSCP 12 и 16 и ограничивающую скорость — средняя скорость 1000 Кбит/с, порог ограничения 200000 байт. Использовать данную стратегию на интерфейсах Ethernet 14 и 16.

```
console#
console# configure
console(config)# ip access-list tcp_ena
console(config-ip-al)# permit tcp any any dscp 12
console(config-ip-al)# permit tcp any any dscp 16
console(config-ip-al)# exit
console(config)# qos advanced
console(config)# qos map dscp-queue 12 to 1
console(config)# qos map dscp-queue 16 to 2
console(config)# priority-queue out num-of-queues 1
console(config)# policy-map traffic
console(config-pmap)# class class1 access-group tcp_ena
console(config-pmap-c)# police 1000 200000 exceed-action drop
console(config-pmap-c)# exit
console(config-pmap)# exit
console(config)# interface tengigabitethernet 1/0/14
console(config-if)# service-policy input
```

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

5.34.2. Статистика QoS

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 315 – 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.
qos statistics queues *set* **{***queue* **| all} {***dp* **| all} {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| all}**	set: (1..2); queue: (1..8); dp: (high, low); gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); Значение по умолчанию: set 1: все приоритеты, все очереди, высокий приоритет сброса. set 2: все приоритеты, все очереди, низкий приоритет сброса.	Включает QoS -статистику для выходных очередей. - *set* – определяет набор счетчиков; - *queue* – определяет исходящую очередь; - *dp* – определяет приоритет сброса.
no qos statistics queues *set*		Отключает QoS-статистику для выходных очередей.

Команды режима конфигурации интерфейса Ethernet, группы портов

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

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

Таблица 316 – Команды режима конфигурации интерфейса Ethernet.

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 317 – Команды режима EXEC

Команда	*Значение/ Значение по умолчанию*	*Действие*
clear qos statistics	-	Очищает статистику QoS.
show qos statistics	-	Показывает статистику QoS.

5.35. Конфигурация протоколов маршрутизации

5.35.1. 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 318 – Команды режима глобальной конфигурации

Команда	*Значение/ Значение по умолчанию*	*Действие*
ip route *prefix prefix_length* **{reject-route |** *gateway* **[metric** *metric***] |name** *name***]** [**distance** *distance*]**}**	prefix: (A.B.C.D); prefix_length: (A.B.C.D или /n); gateway: (A.B.C.D) metric (1..255)/1; name: (1..32) символа; distance (1..255)/1	Создать статическое правило маршрутизации. - *prefix* — IP-адрес сети назначения; - *prefix_length* — маска префикса назначения или ее длина; - **reject-route** — запрещает маршрутизацию к сети назначения через все шлюзы; - *gateway* — IP-адрес шлюза для доступа к сети назначения; - metric — метрика для данного маршрута; - *name* — имя маршрута; - *distance* — административная дистанция маршрута.
no ip route *prefix prefix_length* **{reject-route | *gateway*}**		Удалить правило из таблицы статической маршрутизации.
distance {ospf {inter-as | intra-as} | static} ***distance***	distance (1..255)/static:1, OSPF intra-as:30, OSPF inter-as:110	Установить значение административной дистанции (AD) для всех маршрутов указанного типа. - **ospf inter-as** — установить значение AD для межзональных маршрутов, принятых по протоколу OSPF; - **ospf intra-as** — установить значение AD для внутризональных маршрутов, принятых по протоколу OSPF; - **static** — установить значение AD для статических маршрутов.
distance {ospf {inter-as | intra-as} | static}		Установить значение по умолчанию.

Команды режима конфигурации VRF

Вид запроса командной строки режима глобальной конфигурации:

```
console(config-vrf)#
```

Таблица 319 — Команды режима конфигурации vrf

Команда	***Значение/ Значение по умолчанию***	***Действие***
ip route prefix {*mask* **|** *prefix_length***} { reject-route |** *gateway* **[metric** *distance***] |name** *name***]}**	prefix_length: (0..32); distance: (1..255)/1	Создать 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; - *name* — имя маршрута; - **reject-route** — запрет маршрутизации к сети назначения через все шлюзы.
no ip route *prefix prefix_length***} { reject-route |** *gateway***}**		Удалить правило из таблицы статической маршрутизации.
ip default-gateway {*gateway*}	—/шлюз по умолчанию не задан	Задать для коммутатора адрес шлюза по умолчанию через vrf.
no ip default-gateway {*gateway*}		Удалить назначенный адрес шлюза по умолчанию.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 320 – Команды режима EXEC

Команда	***Значение/ Значение по умолчанию***	***Действие***
show ip route [connected | vrf [*vrf-name]* | static | address *ip_address* **[***mask* **|** *prefix_length***] [multicast] [longer-prefixes]]**	—	Показать 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; - **vrf** — область виртуальной маршрутизации, в которой находится маршрут; - **multicast** — маршруты, задействованные для передачи многоадресного трафика.
show distance	—	Показать значение административной дистанции для различных источников маршрута.

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 321 – Описание результата выполнения команды

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

5.35.2. 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 322 – 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 323 – 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 [id] [metric *metric* **| match** *type* **| route-map** *route_map_name***]**	id: (1-65536) metric: (1..15, transparent)/1; match: (internal, external-1, external-2); route_map_name: (1..32) символа	Разрешает анонсирование OSPF маршрутов через RIP. - *id* – идентификатор процесса OSPF; - *type* – производить анонсирование только для указанных типов OSPF маршрутов; - *route-map_name* – производить анонсирование маршрутов после их фильтрации через указанную route-map;
no redistribute ospf [id] [metric *metric* **| match** *type* **| route-map** *route_map_name***]**		Без параметров запрещает анонсирование маршрутов OSPF через RIP. В случае указания параметра возвращает его дефолтное значение.
redistribute bgp metric [*metric* **| transparent]**	*metric:* (1..15, transparent)/1	Разрешает анонсирование BGP маршрутов через RIP. - *metric* — значение метрики для импортируемых маршрутов; - **metric transparent** — означает, что будет использоваться метрика из таблицы маршрутизации.
no redistribute bgp metric [*metric* **| transparent]**		Без параметров запрещает анонсирование маршрутов BGP через RIP. В случае указания параметра возвращает его дефолтное значение.
redistribute isis [*level***] [match** *match***] [metric** *metric***] [transparent]**	*level:* (level-1, level-2, level-1-2)/level-2; *match:* (internal, external); *metric:* (1..15, transparent)/1	Разрешает анонсирование IS-IS маршрутов через RIP. - *level* — установить, из какого уровня IS-IS будут анонсироваться маршруты; - *match* — производить анонсирование только для указанных типов IS-IS маршрутов.
no redistribute isis [*level***] [match** *match***] [metric** *metric***] [transparent]**		Без параметров запрещает анонсирование маршрутов IS-IS через RIP. В случае указания параметра возвращает его дефолтное значение.
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-if)#
```

Таблица 324 – 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 325 – 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
```

5.35.3. 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 326 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
router ospf [*process_id*] [vrf *vrf_name*]	process_id: (1..65535)/1 vrf_name: (1..32) символа	Включить маршрутизацию по протоколу OSPF. Задать идентификатор процесса.
no router ospf [*process_id*] [vrf *vrf_name*]		Выключить маршрутизацию по протоколу OSPF.
ipv6 router ospf [*process_id*]	process_id: (1..65535)/1	Включить маршрутизацию по протоколу OSPFv3. Задать идентификатор процесса.
no ipv6 router ospf [*process_id*]		Выключить маршрутизацию по протоколу OSPFv3.
ipv6 distance ospf {inter-as | intra-as} *distance*	distance: (1..255)	Задать 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}		Вернуть 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 327 – Команды режима конфигурации процесса OSPF

Команда	*Значение/Значение по умолчанию*	*Действие*
redistribute connected [metric *metric*] **[metric-type {type-1 | type-2}] [route-map** *name_policy*] **[filter-list** *name_acl*] **[tag** *value*] **[subnets]**	metric: (1..65535); name_policy: (1..255) символов; name_acl: (1..32) символов; value: (0-4294967295)	Разрешить анонсирование connected-маршрутов: - **metric-type type-1** — импортирует с пометкой как OSPF external 1; - **metric-type type-2** — импортирует с пометкой как OSPF external 2; - **subnets** — позволяет импортировать подсети. - *metric* — значение метрики для импортируемых маршрутов; - *name-policy* — имя политики импорта, позволяющей фильтровать и вносить изменения в импортируемые маршруты; - *name-acl* — имя стандартного IP ACL, позволяющего фильтровать импортируемые маршруты; - *value* — значение атрибута tag для импортируемых маршрутов.
no redistribute connected [metric *metric*] **[metric-type {type-1 | type-2}] [route-map** *name_policy*] **[filter-list** *name_acl*] **[tag** *value*] **[subnets]**		Запретить анонсирование connected-маршрутов. В случае указания параметра вернуть его значение по умолчанию.
redistribute static [metric *metric*] **[metric-type {type-1 | type-2}] [route-map** *name_policy*] **[filter-list** *name_acl*] **[tag** *value*] **[subnets]**	metric: (1..65535); name_policy: (1..255) символов; name_acl: (1..32) символов; value: (0-4294967295)	Разрешить анонсирование статических маршрутов: - **metric-type type-1** — импортирует с пометкой как OSPF external 1; - **metric-type type-2** — импортирует с пометкой как OSPF external 2; - **subnets** — позволяет импортировать подсети; - *metric* — значение метрики для импортируемых маршрутов; - *name-policy* — имя политики импорта, позволяющей фильтровать и вносить изменения в импортируемые маршруты; - *name-acl* — имя стандартного IP ACL, позволяющего фильтровать импортируемые маршруты; - *value* — значение атрибута tag для импортируемых маршрутов.
no redistribute static [metric *metric*] **[metric-type {type-1 | type-2}] [route-map** *name_policy*] **[filter-list** *name_acl*] **[tag** *value*] **[subnets]**		Запретить анонсирование статических маршрутов. В случае указания параметра вернуть его значение по умолчанию.

redistribute ospf *id* **[nssa-only] [metric** *metric***] [metric-type {type-1 | type-2}] [route-map** *name***] [match {internal | external-1 | external-2 | nssa-external-1 | nssa-external-2}] [tag** *value***] [subnets]**	id: (1..65535); metric: (1..65535); name: (0..32) символа; value: (0-4294967295)	Импортировать маршруты 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; - **match nssa-external-1** — импортирует маршруты типа OSPF NSSA external 1; - **match nssa-external-2** — импортирует маршруты типа OSPF NSSA 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; - *value* — значение атрибута tag 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}] [tag** *value***] [subnets]**		Запретить импорт маршрутов из процесса OSPF в процесс OSPF. В случае указания параметра вернуть его значение по умолчанию.
redistribute rip [metric *metric***] [metric-type {type-1 | type-2}] [route-map** *name_policy***] [filter-list** *name_acl***] [tag** *value***] [subnets]**	metric: (1..65535); name_policy: (1..255) символов; name_acl: (1..32) символов; value: (0-4294967295)	Разрешить анонсирование маршрутов, полученных по протоколу RIP: - **metric-type type-1** — импортирует с пометкой как OSPF external 1; - **metric-type type-2** — импортирует с пометкой как OSPF external 2; - **subnets** — позволяет импортировать подсети; - *metric* — значение метрики для импортируемых маршрутов; - *name-policy* — имя политики импорта, позволяющей фильтровать и вносить изменения в импортируемые маршруты; - *name-acl* — имя стандартного IP ACL, позволяющего фильтровать импортируемые маршруты; - *value* — значение атрибута tag для импортируемых маршрутов.
no redistribute rip [metric *metric***] [metric-type {type-1 | type-2}] [route-map** *name_policy***] [filter-list** *name_acl***] [tag** *value***] [subnets]**		Запретить анонсирование маршрутов, полученных по протоколу RIP. В случае указания параметра вернуть его значение по умолчанию.

redistribute isis [*level*] **[match** *match*] **[metric** *metric*] **[metric-type {type-1 | type-2}] [route-map** *name_policy*] **[filter-list** *name_acl*] **[tag** *value*] **[subnets]**	level: (level-1, level-2, level-1-2)/level-2; match: (internal, external); metric: (1..65535); value: (0-4294967295)	Разрешить анонсирование маршрутов, полученных по протоколу IS-IS: - **metric-type type-1** — импорт с пометкой OSPF external 1; - **metric-type type-2** — импорт с пометкой OSPF external 2; - **subnets** — позволяет импортировать подсети; - *level* — уровень IS-IS, из которого будут анонсироваться маршруты; - *match* — производить анонсирование только для указанных типов IP-IS маршрутов; - *metric* — значение метрики для импортируемых маршрутов; - *name-policy* — имя политики импорта, позволяющей фильтровать и вносить изменения в импортируемые маршруты; - *value* — значение атрибута tag для импортируемых маршрутов.
no redistribute isis [*level*] **[match** *match*] **[metric-type {type-1 | type-2}] [route-map** *name_policy*] **[filter-list** *name_acl*] **[tag** *value*] **[subnets]**		Без параметров запретить анонсирование маршрутов, полученных по протоколу IS-IS. В случае указания параметра вернуть его значение по умолчанию.
redistribute bgp [metric *metric*] **[metric-type {type-1 | type-2}] [route-map** *name_policy*] **[filter-list** *name_acl*] **[tag** *value*] **[subnets]**	metric: (1..65535); name_policy: (1..255) символов; name_acl: (1..32) символов; value: (0-4294967295)	Разрешить анонсирование маршрутов, полученных по протоколу BGP: - **metric-type type-1** — импортирует с пометкой как OSPF external 1; - **metric-type type-2** — импортирует с пометкой как OSPF external 2; - **subnets** — позволяет импортировать подсети; - *metric* — значение метрики для импортируемых маршрутов; - *name-policy* — имя политики импорта, позволяющей фильтровать и вносить изменения в импортируемые маршруты; - *name-acl* — имя стандартного IP ACL, позволяющего фильтровать импортируемые маршруты; - *value* — значение атрибута tag для импортируемых маршрутов.
no redistribute bgp [metric *metric*] **[metric-type {type-1 | type-2}] [route-map** *name_policy*] **[filter-list** *name_acl*] **[tag** *value*] **[subnets]**		Запретить анонсирование маршрутов, полученных по протоколу BGP. В случае указания параметра вернуть его значение по умолчанию.
compatible rfc1583	—/enabled	Включить совместимость с RFC 1583 (только для IPv4).
no compatible rfc1583		Выключить совместимость с RFC 1583.
router-id *A.B.C.D*	A.B.C.D: идентификатор маршрутизатора в формате IPv4-адреса	Установить идентификатор маршрутизатора, который уникально идентифицирует маршрутизатор в пределах одной автономной системы.
no router-id *A.B.C.D*		Установить 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*		Удалить IP-адрес интерфейса.
default-metric *metric*	metric*:* (1..65535)	Установить метрику OSPF-маршрута.
no default-metric		Отключить функцию.

area *A.B.C.D* **stub [no-summary]**	A.B.C.D: идентификатор маршрутизатора в формате IPv4-адреса	Установить 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**		Установить 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;	Установить для указанной зоны тип NSSA. - **no-summary** — не принимать информацию о суммированных внешних маршрутах внутрь NSSA-зоны; - *interval* **—** определяет промежуток времени (в секундах), 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**		Установить 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	Создать виртуальное соединение 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***]**		Удалить виртуальное соединение.
area *A.B.C.D* **default-cost** *cost*	A.B.C.D: идентификатор маршрутизатора в формате IPv4-адреса; cost*:* целое положительное число	Установить значение стоимости суммарного маршрута, используемого для stub- и NSSA-зон (для IPv4).
no area *A.B.C.D* **default-cost**		Установить значение по умолчанию.
area *A.B.C.D* **authentication [message-digest]**	A.B.C.D: идентификатор маршрутизатора в формате IPv4-адреса; —/выключено	Включить аутентификацию для всех интерфейсов данной зоны (для IPv4): - **message-digest** — с шифрованием MD5.
no area *A.B.C.D* **authentication [message-digest]**		Отключить 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	Создать 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*		Удалить 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	Установить фильтр на маршруты, анонсируемые в указанную зону из других зон (для IPv4). **Фильтрация производится только для маршрутов LSA Type 3.**
no area *A.B.C.D* **filter-list prefix** *prefix_list* **in**		Удалить 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	Установить фильтр на маршруты, анонсируемые из указанной зоны в другие зоны (для IPv4). **Фильтрация производится только для маршрутов LSA Type 3.**
no area *A.B.C.D* **filter-list prefix** *prefix_list* **out**		Удалить фильтр на маршруты, анонсируемые из указанной зоны в другие зоны (для IPv4).
area *A.B.C.D* **shutdown**	A.B.C.D: идентификатор маршрутизатора в формате IPv4-адреса; —/включено	Отключить процесс OSPF для зоны.
no area *A.B.C.D* **shutdown**		Включить процесс OSPF для зоны.
auto-cost reference-bandwidth *reference*	reference: (0..400000)/ 0 Мбит/с	Установить автоматический расчет метрики интерфейса в зависимости от его скорости по формуле: *reference/ifSpeed*. - *reference* — базовая скорость. **Значение *reference*, равное 0, отключает автоматический расчет метрики.**
no auto-cost reference-bandwidth		Установить значение по умолчанию.
shutdown	—/включено	Отключить процесс OSPF.
no shutdown		Включить процесс OSPF.
summary-address *ipv4_addr mask* **[not-advertise]**	—/выключено	Включить суммирование маршрутов IPv4, которые были получены OSPF из других протоколов. **not-advertise** — просуммировать, но не анонсировать.
no summary-address *ip_addr mask* **[not-advertise]**		Отключить суммаризацию маршрутов.
neighbor *ip_add* **[priority** *priority***]**	priority: (0..255)/0	Задать IPv4-адрес для статического OSPF-соседа. - *ip_add* — IPv4-адрес. - *priority* — указать priority для соседа (учитывается только в состоянии attempt/down). **Настройка актуальна только для non-broadcast и point-to-multipoint non-broadcast типов сетей.**
no neighbor *ip_add*		Удалить конфигурацию для OSPF-соседа с указанным IPv4-адресом.
summary-prefix *ipv6* **[not-advertise]**	—/выключено	Включить суммирование маршрутов IPv6, которые были получены OSPF из других протоколов. **not-advertise** — просуммировать, но не анонсировать.
summary-prefix *ipv6* **[not-advertise]**		Отключить суммаризацию маршрутов.
timers spf delay *delay*	delay: (0..600000)/5000 мс	Установить величину задержки, производимой перед очередным последовательным расчетом SPF.
no timers spf delay		Установить значение по умолчанию.

timers lsa throttle *min_interval hold_interval max_interval*	min_interval: (0..60000)/5000 мс; hold_interval: (0..60000)/0 мс; max_interval: (0..60000)/0 мс	Задать временные параметры LSA-троттлинга. Троттлинг действует только на LSA, источником которых является локальное устройство. - *min_interval* — минимальный временной интервал между двумя последовательно отправляющимися одинаковыми LSA. - *hold_interval* — интервал, определяющий текущее время задержки. С каждой новой последовательной LSA этот интервал умножается на два, пока не достигнет значения *max_interval.* - *max_interval* — максимальный временной интервал между двумя последовательно отправляющимися одинаковыми LSA.
no timers lsa throttle		Установить значение по умолчанию.
timers lsa arrival *min_arrival*	min_arrival: (0..60000)/1000 мс	Установить минимальный временной интервал, с которым маршрутизатор обрабатывает принимаемые LSA.
no timers lsa arrival *min_arrival*		Установить значение по умолчанию.
passive-interface	/выключено	Запретить всем IP-интерфейсам, участвующим в процессе OSPF, обмениваться протокольными сообщениями с соседями (включить пассивный режим). **При применении данной команды настройка ip ospf passive-interface удаляется со всех ip-интерфейсов и становится для них значением по умолчанию.**
no passive-interface		Установить значение по умолчанию.

Команды режима конфигурации интерфейса IP

Вид запроса командной строки:

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

Таблица 328 – Команды режима конфигурации интерфейса IP

Команда	***Значение/Значение по умолчанию***	***Действие***
ip ospf shutdown	—/включено	Выключить маршрутизацию по протоколу OSPF на интерфейсе.
no ip ospf shutdown		Включить маршрутизацию по протоколу OSPF на интерфейсе.
ip ospf network {broadcast | non-broadcast | point-to-point | point-to-multipoint non-broadcast}	—/broadcast	Выбрать тип сети: - **broadcast** — широковещательная сеть с множественным доступом; - **non-broadcast** — нешироковещательная сеть с множественным доступом; - **point-to-point** — сеть «точка-точка»; - **point-to-multipoint non-broadcast** — нешироковещательная сеть с множественным доступом «точка-многоточка».
no ip ospf network		Установить значение по умолчанию.

ip ospf authentication [key-chain *key_chain* **| null | message-digest]**	key_chain: (1..32) символов; по умолчанию аутентификация отключена	Включить аутентификацию в OSPF и определить ее тип. Без указания параметров будет использоваться аутентификация с помощью пароля, заданного открытым текстом. - **keychain** — включает использование набора ключей. Работает в связке с режимом message-digest. - *key_chain* — имя набора ключей, созданного командой keychain; - **null** — не использовать аутентификацию; - **message-digest** — аутентификация MD5 с использование набора ключей.
no ip ospf authentication [keychain]		Установить значение по умолчанию.
ip ospf authentication-key *key*	key: (1..8) символов	Назначить 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		Удалить пароль.
ip ospf cost ***cost***	cost: (1..65535)/10	Установить метрику состояния канала, которая является условным показателем "стоимости" пересылки данных по каналу.
no ip ospf cost		Установить значение по умолчанию.
ip ospf poll-interval *interval*	interval: (1..255)/120	Установить интервал времени в секундах, по истечении которого маршрутизатор отправляет hello-пакеты с неактивного интерфейса (OSPF-соседство в статусе down). **Настройка актуальна только для non-broadcast и point-to-multipoint non-broadcast типов сетей.**
no ip ospf poll-interval		Установить значение по умолчанию.
ip ospf dead-interval {*interval* **| minimal}**	interval: (1..65535) секунд; minimal — 1сек	Установить 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		Установить значение по умолчанию.
ip ospf hello-interval *interval*	interval: (1..65535)/10 секунд	Установить интервал времени в секундах, по истечении которого маршрутизатор отправляет следующий hello-пакет с интерфейса.
no ip ospf hello-interval		Установить значение по умолчанию.
ip ospf mtu-ignore	—/включено	Отключить проверки MTU.
no ip ospf mtu-ignore		Установить значение по умолчанию.
ip ospf passive-interface	—/выключено	Запретить IP-интерфейсу обмениваться протокольными сообщениями с соседями (включить пассивный режим).
no ip ospf passive-interface		Установить значение по умолчанию. **Если применена настройка passive-interface в режиме конфигурации процесса OSPF, то данная команда выводит данный IP-интерфейс из пассивного режима.**
passive-interface	—/выключено	Выключить отправку протокольных сообщений для всех OSPF-интерфейсов.
no passive-interface		Включить отправку протокольных сообщений для всех OSPF-интерфейсов.
ip ospf priority ***priority***	priority: (0..255)/1	Установить приоритет маршрутизатора, который используется для выбора DR и BDR.
no ip ospf priority		Установить значение по умолчанию.
ip ospf retransmit-interval *interval*	interval: (1..65535)/5 секунд	Установить интервал времени в секундах, по истечении которого маршрутизатор повторно отправит пакет, на который не получил подтверждения о получении (например, Database Description или Link State Request пакеты).
no ip ospf retransmit-interval		Установить значение по умолчанию.

ip ospf transmit-delay *delay*	delay: (1..65535)/1 секунд	Установить примерное время в секундах, необходимое для передачи пакета состояния канала.
no ip ospf transmit-delay		Установить значение по умолчанию.
ip ospf bfd	—/выключено	Включить протокол BFD на OSPF-соседстве.
no ip ospf bfd		Выключить протокол BFD на OSPF-соседстве.

Команды режима конфигурации интерфейса Ethernet, VLAN:

Вид запроса командной строки:

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

Таблица 329 – Команды режима конфигурации интерфейса Ethernet, VLAN

Команда	***Значение/Значение по умолчанию***	***Действие***
ipv6 ospf shutdown	—/включено	Выключить маршрутизацию по протоколу OSPFv3 на интерфейсе.
no ipv6 ospf shutdown		Включить 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	Установить метрику состояния канала, которая является условным показателем "стоимости" пересылки данных по каналу.
no ipv6 ospf cost		Установить значение по умолчанию.
ipv6 ospf dead-interval *interval*	interval: (1..65535) секунд	Установить 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		Установить значение по умолчанию.
ipv6 ospf hello-interval interval	interval: (1..65535)/10 секунд	Установить интервал времени в секундах, по истечении которого маршрутизатор отправляет следующий hello-пакет с интерфейса.
no ipv6 ospf hello-interval		Установить значение по умолчанию.
ipv6 ospf mtu-ignore	—/выключено	Отключить проверку MTU.
no ipv6 ospf mtu-ignore		Установить значение по умолчанию.
ipv6 ospf neighbor {*ipv6_address*}	—	Задать IPv6-адрес соседа.
ipv6 ospf neighbor {*ipv6_address*}		Удалить IPv6-адрес соседа.
ipv6 ospf priority *priority*	priority: (0..255)/1	Установить приоритет маршрутизатора, который используется для выбора DR и BDR.
no ipv6 ospf priority		Установить значение по умолчанию.
ipv6 ospf retransmit-interval *interval*	interval: (1..65535)/5 секунд	Установить 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		Установить значение по умолчанию.
ipv6 ospf transmit-delay *delay*	delay: (1..65535)/1 секунд	Установить примерное время в секундах, необходимое для передачи пакета состояния канала.
no ip ospf transmit-delay		Установить значение по умолчанию.

Команды режима privileged EXEC

Вид запроса командной строки в режиме privileged EXEC:

```
console#
```

Таблица 330 – Команды режима privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show {ip | ipv6} ospf [*process_id* **| vrf** *vrf_name***]**	**process_id**: (1..65536) vrf_name: (1..32) символа	Отобразить конфигурацию OSPF.
show {ip | ipv6} ospf [*process_id***] neighbor [vrf** *vrf_name***]**	**process_id**: (1..65536) vrf_name: (1..32) символа	Отобразить информацию об OSPF-соседях.
show ip ospf [*process_id***] neighbor *A.B.C.D* [vrf** *vrf_name***]**	**process_id**: (1..65536); **A.B.C.D: IP-адрес соседа** vrf_name: (1..32) символа	Отобразить информацию об OSPF-соседе с указанным адресом.
show {ip | ipv6} ospf [*process_id***] interface [vrf** *vrf_name***]**	**process_id**: (1..65536) vrf_name: (1..32) символа	Отобразить конфигурацию всех OSPF-интерфейсов.
show {ip | ipv6} ospf [*process_id***] interface {gigabitethernet** *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id* **| tunnel** *tunnel_id | A.B.C.D* **[vrf *vrf_name*] [brief]}**	**process_id: (1..65535);** gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094); tunnel_id: (1..16); A.B.C.D: IP-адрес; vrf_name: (1..32) символа	Отобразить конфигурацию конкретного OSPF-интерфейса.
show {ip | ipv6} ospf [*process_id***] database [vrf** *vrf_name***] [router [vrf** *vrf_name***] | summary [vrf** *vrf_name***] | as-summary [vrf** *vrf_name***]]**	**process_id: (1..65535);** **vrf_name: (1..32) символа**	Отобразить состояние базы данных протокола OSPF.
show {ip | ipv6} ospf virtuallinks [*process_id***] | [vrf** *vrf_name***]**	**process_id: (1..65535);** **vrf_name: (1..32) символа**	Отобразить параметры и текущее состояние виртуальных линков.
clear ip ospf [*process id* **| vrf** *vrf_name* **process}**	**process_id: (1..65535);** **vrf_name: (1..32) символа**	Разорвать соседства и удалить соответствующие маршруты.

Примеры выполнения команд

- Показать OSPF-соседей для определенного VRF (vrf1):

```
console# show ip ospf neighbor vrf vrf1
```

- Перезапустить OSPF-процесс для определенного VRF (vrf1):

```
console# clear ip ospf vrf vrf1 process
```

5.35.4. Настройка протокола BGP (Border Gateway Protocol)

BGP (Border Gateway Protocol – протокол граничного шлюза) является протоколом маршрутизации между автономными системами (AS). Основной функцией BGP-системы является обмен информацией о доступности сетей с другими системами BGP. Информация о доступности сетей включает список автономных систем (AS), через которые проходит эта информация.

BGP является протоколом прикладного уровня и функционирует поверх протокола транспортного уровня TCP (порт 179). После установки соединения передаётся информация обо всех маршрутах, предназначенных для экспорта. В дальнейшем передаётся только информация об изменениях в таблицах маршрутизации.

Поддержка протокола BGP предоставляется по лицензии.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 331 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
router bgp [*as_plain_id_* **|** ***as_dot_id***]	as_plain_id: (1..4294967295)/1 as_dot_id: (1.0..65535.65535)	Включить маршрутизацию по протоколу BGP. Задать идентификатор AS и войти в режим его конфигурирования. - *as_plain_id* — идентификатор автономной системы, используемый маршрутизатором при установлении соседства и обмене маршрутной информацией. - *as_dot_id* — идентификатор автономной системы в 32-битном формате.
no router bgp [*as_plain_id_* **|** *as_dot_id*]		Остановить BGP-маршрутизатор, удалить всю конфигурацию протокола BGP.
ip community-list standard *name* **seq** *section_id* **{permit	deny}**	name: (1..32) символа; section_id: (1..4294967295); reg_exp: (1-127) символа	Создать стандартный список community и войти в режим его конфигурирования.
ip community-list expanded *name* **seq** *section_id* **{permit	deny}** *reg_exp*		Создать расширенный список community. - *reg_exp* — регулярное выражение. Данный список community используется как шаблон для поиска совпадений community в секции match в route-map.
**no ip community-list {standard	expanded}** ***name*** **seq** [*section_id*]		Удалить указанный список community целиком или только конкретную его секцию.
ip extcommunity-list standard *name* **seq** *section_id* **{permit	deny}**	name: (1..32) символа; section_id: (1..4294967295);	Создать стандартный список с расширенными community и войти в режим его конфигурирования.

ip extcommunity-list expanded *name* **seq** *section_id* **{permit | deny}** *reg_exp*	reg_exp: (1-127) символа	Создать расширенный список с расширенными community. - *reg_exp* — регулярное выражение. Данный список extcommunity используется как шаблон для поиска совпадений расширенных community в секции match в route-map.
no ip extcommunity-list {standard | expanded} *name* **seq [***section_id***]**		Удалить указанный список extcommunity целиком или только конкретную его секцию.
ip as-path access-list *name* **seq** *section_id* **{permit | deny}** *reg_exp*	name: (1..32) символа; section_id (1–4294967295); reg_exp: (1..160) символа	Создать список as-path. - *reg_exp* — регулярное выражение. Данный список as-path используется как шаблон для поиска совпадений as-path-filter в секции match в route-map.
no ip as-path access-list *name* **seq [***section_id***]**		Удалить указанный список as-path целиком или только конкретную его секцию.

Команды режима конфигурации AS

Вид запроса командной строки в режиме конфигурации AS:

```
console(router-bgp)#
```

Таблица 332 – Команды режима конфигурации AS

Команда	*Значение/Значение по умолчанию*	*Действие*
bgp router-id *ip_add*	—	Задать идентификатор BGP-маршрутизатора.
no bgp router-id		Удалить идентификатор BGP-маршрутизатора.
bgp asnotation dot	—/asplain	Задействовать систему обозначения номеров AS в формате asdot.
no bgp asnotation		Установить значение по умолчанию
bgp client-to-client reflection	—/включено	Включить пересылку маршрутов, полученных от reflector-клиента, другим BGP-соседям.
no bgp client-to-client reflection	—	Выключить пересылку маршрутов, полученных от reflector-клиента, другим BGP-соседям.
bgp cluster-id *ip_add*	—	Задать идентификатор кластера BGP-маршрутизатора. **В случае, если идентификатор кластера не настроен, в качестве идентификатора будет использоваться глобальный идентификатор BGP-маршрутизатора.**
no bgp cluster-id	—	Удалить идентификатор кластера BGP-маршрутизатора
bgp transport path-mtu-discovery	—	Включить процедуру Path MTU Discovery для автоматического определения Maximum Segment Size при установлении TCP-соединения между соседями. **Включение Path MTU Discovery на процессе включает его на всех соседях.**
no bgp transport path-mtu-discovery	—	Установить значение по умолчанию.
shutdown	—/no shutdown	Административно выключить протокол BGP, не удаляя его конфигурацию. **Это действие влечёт за собой разрыв всех сессий с BGP-соседями и очистку таблицы маршрутизации протокола BGP.**
no shutdown		Включить работу AS.
neighbor *ip_add*	—	Задать IPv4- или IPv6-адрес для BGP-соседа или перейти в режим конфигурирования существующего соседа. - ip_add — IPv4- или IPv6-адрес. **Возможно установление соседства в том числе и через IPv6 Link-local адреса.**

no neighbor *ip_add*		Удалить конфигурацию для BGP-соседа с указанным IPv4- или IPv6-адресом.
peer-group *name*	name: (1..32) символа	Создать Peer-группу - name — имя группы
no peer-group *name*		Удалить созданную Peer-группу.
address-family ipv4 {unicast | multicast}	—/unicast	Указать тип IPv4 Address Family и перевести коммутатор в режим конфигурации соответствующей Address Family.
no address-family ipv4 {unicast | multicast}		Выключить соответствующую Address-Family.
address-family ipv6 unicast	—	Указать тип IPv6 Address Family unicast и перевести коммутатор в режим конфигурации соответствующей Address-Family.
no address-family ipv6 unicast		Выключить соответствующую Address-Family.
vrf [*vrf_name***]**	vrf-name: (1..32) символа	Создание контекста VRF. - *vrf-name* — имя виртуальной области маршрутизации. **VRF должен быть создан в глобальной конфигурации комутатора.**
no vrf [*vrf_name***]**		Удаление контекста VRF.

Если соседство установлено на IPv4-адресах, то при отправке маршрутов IPv6 такому соседу в качестве next-hop будет установлен искусственный IPv6-адрес, основанный на IPv4-адресе. Чтобы это изменить, необходимо использовать route-map, в которой указать необходимый IPv6 next-hop. Пример данной настройки приведен ниже.

Пример создания route-map и привязки ее к BGP-соседу для изменения исходящих маршрутов IPv6

```
console(config)#ipv6 route-map test 10 permit
console(config-route-map)#set ipv6 next-hop 2030::1
console(config-route-map)#exit
console(config)#router bgp 65500
console(router-bgp)#neighbor 10.0.0.2
console(router-bgp-nbr)#address-family ipv6 unicast
console(router-bgp-nbr-af)#route-map test out
```

В результате выполнения команды при отправке IPv6-маршрутов соседу 10.0.0.2 значение поля next-hop будет 2030::1.

Команды режима конфигурации Address-Family

Вид запроса командной строки в режиме конфигурации Address-Family:

```
console(router-bgp-af)#
```

Таблица 333 – Команды режима конфигурации Address-Family

Команда	***Значение/Значение по умолчанию***	***Действие***
network *ipv4_add* **[mask** ***mask*****]**	—	Задать подсеть, которая анонсируется BGP-соседям. - *ipv4-add* — IPv4-адрес подсети. - *mask* — маска подсети. **Если маска не указана, по умолчанию она задается классовым методом адресации.**
no network *ipv4_add* **[mask** *mask*]		Удалить анонс данной подсети.

network *ipv6_add*	ipv6_add: X:X:X:X::X/(0-128)	Задать подсеть, которая анонсируется BGP-соседям. - *ipv6-add* — IPv6-адрес подсети.
no network *ipv6_add*		Удалить анонс данной подсети.
aggregate-address *ipv4_add mask* **[summary-only | as-set | advertise-map** *route_map_name* **| attribute-map** *route_map_name* **| suppress-map** *route_map_name***]**	—	Включить агрегацию более специфичных маршрутов, входящих в указанный префикс - ipv4_add — IPv4-адрес подсети. - mask — маска подсети. - route_map_name — имя route-map.
no aggregate-address *ipv4_add mask*		Удалить агрегацию более специфичных маршрутов, входящих в указанный префикс.
aggregate-address *ipv6_add* **[summary-only | as-set | advertise-map** *route_map_name* **| attribute-map** *route_map_name* **| suppress-map** *route_map_name***]**	—	Включить агрегацию более специфичных маршрутов, входящих в указанный префикс - ipv6_add — IPv6-адрес подсети. - route_map_name — имя route-map.
no aggregate-address *ipv6_add*		Удалить агрегацию более специфичных маршрутов, входящих в указанный префикс.
redistribute connected [metric *metric* **| filter-list** *name***]**	metric: (1-4294967295); name: (1..32) символа	Разрешить анонсирование connected-маршрутов. - *metric* — значение атрибута MED, которое будет присвоено импортированным маршрутам. - *name* — название access-list, который будет применен к маршрутам.
no redistribute connected		Запретить анонсирование connected-маршрутов.
redistribute rip [metric *metric* **| filter-list** *name***]**	metric: (1-4294967295); name: (1..32) символа	Импортировать маршруты RIP в BGP. - *metric* — значение атрибута MED, которое будет присвоено импортированным маршрутам**.** - *name* — название списка access-list, который будет применен к маршрутам. **Недоступно для address-family ipv6 unicast.**
no redistribute rip		Запретить импорт маршрутов из протокола RIP.
redistribute static [metric *metric* **| filter-list** *name***]**	metric: (1-4294967295); name: (1..32) символа	Разрешить анонсирование статических маршрутов. - *metric* — значение атрибута MED, которое будет присвоено импортированным маршрутам**.** - *name* — название access-list, который будет применен к маршрутам.
no redistribute static		Запретить анонсирование статических маршрутов.
redistribute ospf *id* **[metric** *metric* **| match** *type* **| metric-type** *mtype* **| nssa-only | filter-list** *name***]**	id: (1..65535); metric: (1-4294967295); type: (internal, external-1, external-2, nssa-external-1, nssa-external-2); name: (1..32) символов; mtype: (type-1, type-2); name: (1..32) символа	Импортировать маршруты OSPF в BGP. - *id* — идентификатор процесса OSPF. - *metric* — значение атрибута MED, которое будет присвоено импортированным маршрутам. - *type* — тип OSPF-маршрутов, анонсируемых в BGP. - *name* — название списка access-list, который будет применен к маршрутам. - *mtype* — тип метрики Ex1 или Ex2. **В случае с address-family ipv6 unicast подразумевается OSPF3.**
no redistribute ospf		Запретить импорт маршрутов из протокола OSPF.

redistribute isis [*level]* [match *match*] **[metric** *metric*] **[filter-list** *acl_name*]	level: (level-1, level-2, level-1-2)/level-2; *match:* (internal, external); *metric:* (1-65535); acl_name: (1..32) символа	Импортировать маршруты из IS-IS в BGP. - *level* — установить, из какого уровня IS-IS будут анонсироваться маршруты; - *match* — производить анонсирование только для указанных типов IS-IS маршрутов; - *metric* — значение метрики для импортируемых маршрутов; - *acl_name* — имя стандартного IP ACL, который будет использован для фильтрации импортируемых маршрутов. **Недоступно для address-family ipv6 unicast.**
no redistribute isis		Запретить импорт маршрутов из протокола IS-IS.

Команды режима конфигурации BGP-соседа

Вид запроса командной строки в режиме конфигурации BGP-соседа:

```
console(router-bgp-nbr)#
```

Таблица 334 – Команды режима конфигурации BGP-соседа

Команда	***Значение/Значение по умолчанию***	***Действие***
description *descr*	descr: (1..80) символов/нет описания	Добавить описание BGP-соседа.
no description		Удалить описание BGP-соседа.
maximum-prefix *value* **[threshold** *percent* **| hold-timer** *second* **| action** *type* **]**	value: (0-4294967295); percent: (0-100); second: (30-86400); type: (restart, warning-only)	Включить ограничение количества принимаемых маршрутов от BGP-соседа. - *value* — максимальное количество принимаемых маршрутов. - *percent* — процент от максимального количества маршрутов, по достижении которого отправляется предупреждение. - *second* — временной промежуток (в секундах), по истечению которого происходит переподключение, если сессия была разорвана из-за превышения количества маршрутов. - *type* — назначает действие выполняемое при достижении максимального значения — разрыв сессии <restart> или отправка предупреждения <warning-only>.
no maximum-prefix		Выключить ограничение количества принимаемых маршрутов от BGP-соседа.

advertisement-interval *adv_sec* **withdraw** *with_sec*	adv-sec: (0-65535)/30 секунд; with-sec: (0-65535)/30 секунд	Задать временные интервалы. - *adv-sec* — минимальный интервал между отправкой UPDATE сообщений одного и того же маршрута. - *with-sec* — минимальный интервал между анонсированием маршрута и его последующим де-анонсированием. Примечание: - advertisement-interval должен быть больше или равен withdraw-interval. - Маршруты, которые должны быть анонсированы соседним BGP-маршрутизаторам, распределяются по нескольким UPDATE-сообщениям. Между отправкой этих UPDATE-сообщений выдерживается случайный временной интервал таким образом, чтобы общее время между обновлением маршрутов в локальной таблице BGP и отправкой последнего UPDATE-сообщения не превышало advertisement-interval или as-origination-interval в случае отправки локальных (маршруты из локальной AS) маршрутов в eBGP-соединении. Таким образом, каждый из маршрутов может иметь случайную величину задержки анонсирования. - Точность работы таймеров advertisement-interval, withdraw-interval и as-origination-interval зависит от максимального значения любого из этих трёх таймеров, настроенных на BGP-маршрутизаторе (учитываются таймеры, настроенные для всех BGP-соседей). Все значения таймеров анонсирования и де-анонсирования маршрутов, сконфигурированных на устройстве, дискретизируются интервалом в 1/255 от наибольшего настроенного значения. Увеличение максимального значения будет приводить к увеличению частоты дискретизации таймеров и, соответственно, к понижению точности их работы.
no advertisement-interval		Установить значение по умолчанию.
ebgp-multihop	—/TTL равен 1	Установить TTL, равный 64, для eBGP-подключений.
no ebgp multihop		Установить значение по умолчанию.
as-origination-interval *seconds*	seconds: (0-65535)/15 секунд	Задать временной интервал между отправкой UPDATE сообщений одного и того же маршрута, используется для анонса локальных (маршруты из локальной AS) маршрутов eBGP соседям.
no as-origination-interval		Установить значение по умолчанию.
connect-retry-interval *seconds*	seconds: (1-65535)/120 секунд	Задать временной интервал, по истечении которого возобновляется попытка создать BGP-сессию с соседом.
no connect-retry-interval		Установить значение по умолчанию.
next-hop-self [all]	—/выключено	Включить подмену значения атрибута NEXT_HOP на локальный адрес маршрутизатора. - **all** —включает подмену значения атрибута NEXT_HOP на локальный адрес маршрутизатора также и для маршрутов, отражаемых от route-reflector.
no next-hop-self		Отключить подмену атрибута NEXT_HOP.
remote-as [*as_plain_id_***|** *as_dot_id***]**	as_plain_id: (1..4294967295)/1 as_dot_id: (1.0..65535.65535)	Задать номер автономной системы, в которой находится BGP-сосед. Установление соседства невозможно, пока соседу не назначен номер AS. **Это действие влечёт разрыв сессии с соседом и очистку всех принятых от него маршрутов.**
no remote-as		Удалить идентификатор соседней автономной системы.

timers *holdtime keepalive*	holdtime: (0 | 3-65535)/90 секунд; keepalive: (0-21845)/30 секунд	Задать временные интервалы. - *holdtime* — если в течение этого времени не будет принято keepalive-сообщение, то соединение с соседом сбрасывается. - *keepalive* — интервал между отправкой keepalive-сообщений. **Значения holdtime и keepalive должны быть либо оба равны нулю, либо оба больше нуля. holdtime должен быть больше или равен keepalive.** **- Если был выбран таймер hold, который настроен на локальном маршрутизаторе, то используется локальное значение таймера keepalive;** **- Если был выбран таймер hold, который настроен на соседнем маршрутизаторе, и значение локально настроенного таймера keepalive меньше чем 1/3 выбранного таймера hold, то используется локальное значение таймера keepalive;** **- Если был выбран таймер hold, который настроен на соседнем маршрутизаторе, и значение локально настроенного таймера keepalive больше чем 1/3 выбранного таймера hold, то используется целое число, которое меньше чем 1/3 выбранного таймера hold.**
no timers		Установить значение по умолчанию.
timers idle-hold *seconds*	seconds: (1..32747)/15	Задать временной интервал удержания соседа в состоянии Idle после того, как он был сброшен в это состояние. За этот интервал все попытки переустановить соединение с соседом будут отклонены.
no timers idle-hold		Установить значение по умолчанию.
timers open-delay *seconds*	seconds: (0-240)/0 секунд	Задать временной интервал между установкой TCP-соединения и отправкой первого OPEN-сообщения.
no timers open-delay		Установить значение по умолчанию.
shutdown	—/no shutdown	Административно выключить сессию с BGP-соседом и очистить принятые от него маршруты, не удаляя его конфигурации.
no shutdown		Административно включить сессию с BGP-соседом.
update-source [GigabitEthernet *gi_port* **TengigabitEthernet** *te_port* **FortygigabitEthernet** *fo_port* **Port-Channel** *group* **Loopback** ***loopback*** **Vlan** *vlan_id* **]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port(1..8/0/1..4); group: (1..48); loopback: (1-64); vlan-id: (1-4094)	Назначить интерфейс, который будет использован в качестве исходящего при соединении с соседом.
no update-source		Отменить ручную настройку исходящего интерфейса, включить автоматический выбор интерфейса.
route-reflector-client [meshed]	—/disabled	Назначить BGP-соседа Route-Reflector клиентом. - **meshed** — параметр выставляется если используется mesh-топология. При получении от такого клиента BGP-маршрутов они не будут пересылаться другим клиентам. **BGP-маршрутизатор является route-reflector-ом, если хотя бы один его сосед сконфигурирован как route-reflector клиент.**
no route-reflector-client		Установить значение по умолчанию.
soft-reconfiguration inbound	—/disabled	Сохранить полученные от соседа маршруты в отдельной области памяти. Метод позволяет применить входящую политику "route-map in" для соседа без сброса соседства и запроса маршрутов. **По умолчанию работает механизм Route Refresh.**

no soft-reconfiguration inbound		Отключить механизм сохранения маршрутов.
prefix-list *name* **{ in | out }**	name: (1..32) символа	- *name* — название IP prefix-list, который будет применен к анонсируемым или принимаемым маршрутам.
no prefix-list *name* **{ in | out }**		Отвязать IP prefix-list.
peer-group *name*	name: (1..32) символа	- *name* — имя Peer-группы, которая будет применена к соседу. **Настройки на Peer-группе имеют более высокий приоритет, чем настройки на самом соседе.**
no peer-group		Удалить соседа из группы.
address-family ipv4 { unicast | multicast }	—/unicast	Указать тип IPv4 Address Family и перевести коммутатор в режим конфигурации соответствующей address family для этого BGP-соседа.
no address-family ipv4 { unicast | multicast }		Выключить соответствующую IPv4 Address-Family.
transport path-mtu-discovery	—/disabled	Включить процедуру Path MTU Discovery для BGP-соседа. **Не поддерживается на IPv6-соседстве.**
no transport path-mtu-discovery		Выключить процедуру Path MTU Discovery для BGP-соседа.
fall-over bfd	—/выключено	Включить протокол BFD на соседе. **Не поддерживается на IPv6-соседстве.**
no fall-over bfd		Выключить протокол BFD на соседе.
as-path-filter *name* **{in | out}**	name: (1..32) символа	Задать фильтр as-path для BGP-соседа. - *name* — имя списка as-path; - **in** — для входящих маршрутов; - **out** — для исходящих маршрутов.
no as-path-filter *name* **{in | out}**		Удалить фильтр as-path.
password *word*	word: (1..128) символов; по умолчанию аутентификация отключена	Включить аутентификацию всех TCP-сегментов, принятых от BGP-соседа. Задать ключ аутентификации в текстовом виде. Данная настройка игнорируется, если для аутентификации указана key-chain. - *word* — ключ в текстовом виде.
no password		Установить значение по умолчанию.

password encrypted *encryptedword*	encryptedword: (1..128); по умолчанию аутентификация отключена	Включить аутентификацию всех TCP-сегментов, принятых от BGP-соседа. Задает ключ аутентификации в зашифрованном виде (например, пароль в зашифрованном виде, скопированный с другого устройства). Данная настройка игнорируется, если для аутентификации указана key-chain. - *encryptedword* — ключ в текстовом виде.
no password encrypted		Установить значение по умолчанию.
password key-chain *word*	word: (1..32) символов; по умолчанию аутентификация отключена	Задать имя связки ключей, которая будет использоваться для аутентификации всех TCP-сегментов, принятых от BGP-соседа. - *word* — имя связки ключей.
no password key-chain		Установить значение по умолчанию.
ip mroute prefix *prefix_length fw_router_address* **tunnel** *tunnel_id*	prefix: (A.B.C.D); prefix-length: (A.B.C.D или /n); fw_router_address: (A.B.C.D); tunnel_id: (1..16)	Создать статическое правило для многоадресной таблицы маршрутизации. - *prefix* — IP-адрес сети назначения; - *prefix_length* — маска префикса назначения или ее длина; - *fw_router_address* — IP-адрес маршрутизатора многоадресной рассылки; - *tunnel_id* — идентификатор туннеля.
no ip mroute prefix *prefix_length fw_router_address* **tunnel** *tunnel_id*		Удалить статическое правило из таблицы многоадресной маршрутизации.

Команды режима конфигурации Address Family BGP-соседа

Вид запроса командной строки в режиме конфигурации Address Family BGP-соседа:

```
console(router-bgp-nbr-af)#
```

Таблица 335 – Команды режима конфигурации Address Family BGP-соседа

Команда	***Значение/Значение по умолчанию***	***Действие***
maximum-prefix *value* **[threshold** *percent* **| hold-timer** *second* **| action** *type***]**	value: (0-4294967295); percent: (0-100); second: (30-86400); type: (restart, warning-only)	Включить ограничение количества принимаемых маршрутов от BGP-соседа. - value — максимальное количество принимаемых маршрутов. - percent — процент от максимального количества маршрутов, по достижении которого отправляется предупреждение. - second — временной промежуток (в секундах), по истечению которого происходит переподключение, если сессия была разорвана из-за превышения количества маршрутов. - type — назначает действие выполняемое при достижении максимального значения — разрыв сессии <restart> или отправка предупреждения <warning-only>.
no maximum-prefix		Выключить ограничение количества принимаемых маршрутов от BGP-соседа.

advertisement-interval *adv_sec* **withdraw** *with_sec*	adv-sec: (0-65535)/30 секунд; with-sec: (0-65535)/30 секунд	Задать временные интервалы. - *adv-sec* — минимальный интервал между отправкой UPDATE сообщений одного и того же маршрута. - *with-sec* — минимальный интервал между анонсированием маршрута и его последующим де-анонсированием. **- advertisement-interval должен быть больше или равен withdraw-interval.** **- Маршруты, которые должны быть анонсированы соседним BGP-маршрутизаторам, распределяются по нескольким UPDATE-сообщениям. Между отправкой этих UPDATE-сообщений выдерживается случайный временной интервал таким образом, чтобы общее время между обновлением маршрутов в локальной таблице BGP и отправкой последнего UPDATE-сообщения не превышало advertisement-interval или as-origination-interval в случае отправки локальных (маршруты из локальной AS) маршрутов в eBGP-соединении. Таким образом, каждый из маршрутов может иметь случайную величину задержки анонсирования.** **- Точность работы таймеров advertisement-interval, withdraw-interval и as-origination-interval зависит от максимального значения любого из этих трёх таймеров, настроенных на BGP-маршрутизаторе (учитываются таймеры, настроенные для всех BGP-соседей). Все значения таймеров анонсирования и де-анонсирования маршрутов, сконфигурированных на устройстве, дискретизируются интервалом в 1/255 от наибольшего настроенного значения. Увеличение максимального значения будет приводить к увеличению частоты дискретизации таймеров и, соответственно, к понижению точности их работы.**
no advertisement-interval		Установить значение по умолчанию.
as-origination-interval *seconds*	seconds: (0-65535)/15 секунд	Задать временной интервал между отправкой UPDATE сообщений одного и того же маршрута, используется для анонса локальных (маршруты из локальной AS) маршрутов eBGP соседям.
no as-origination-interval		Установить значение по умолчанию.
route-map *name* **{ in | out}**	name: (0..32) символа	- *name* — имя политики route-map, которая будет применена к соседу в данной Address Family. Позволяет фильтровать и вносить изменения в анонсируемые и принимаемые маршруты.
no route-map *name* **{ in | out }**		Удалить политики с данной Address Family.
next-hop-self	—/включено	Включить подмену значения атрибута NEXT_HOP на локальный адрес маршрутизатора.
no next-hop-self		Отключить подмену атрибута NEXT_HOP.
route-reflector-client [meshed]	—/disabled	Назначить BGP-соседа Route-Reflector клиентом. - **meshed** — параметр выставляется если используется mesh-топология. При получении от такого клиента BGP-маршрутов они не будут пересылаться другим клиентам. **BGP-маршрутизатор является route-reflector'ом, если хотя бы один его сосед сконфигурирован как route-reflector клиент.**
no route-reflector-client		Устанавливает значение по умолчанию.

Команды режима конфигурации Peer-групп

Вид запроса командной строки в режиме конфигурации Peer-групп:

```
console(router-bgp-nbrgrp)#
```

Таблица 336 – Команды режима конфигурации Peer-групп

Команда	*Значение/Значение по умолчанию*	*Действие*
maximum-prefix *value* **[threshold** *percent* **| hold-timer** *second* **| action** *type* **]**	value: (0-4294967295); percent: (0-100); second: (30-86400); type: (restart, warning-only)	Включить ограничение количества принимаемых маршрутов от BGP-соседа. - *value* — максимальное количество принимаемых маршрутов. - *percent* — процент от максимального количества маршрутов, по достижении которого отправляется предупреждение. - *second* — временной промежуток (в секундах), по истечению которого происходит переподключение, если сессия была разорвана из-за превышения количества маршрутов. - *type* — назначает действие выполняемое при достижении максимального значения — разрыв сессии <restart> или отправка предупреждения <warning-only>.
no maximum-prefix		Выключить ограничение количества принимаемых маршрутов от BGP-соседа.
advertisement-interval *adv_sec* **withdraw** *with_sec*	adv-sec: (0-65535)/30 секунд; with-sec: (0-65535)/30 секунд	Задать временные интервалы. - *adv-sec* — минимальный интервал между отправкой UPDATE сообщений одного и того же маршрута. - *with-sec* — минимальный интервал между анонсированием маршрута и его последующим де-анонсированием. **- advertisement-interval должен быть больше или равен withdraw-interval.** **- Маршруты, которые должны быть анонсированы соседним BGP-маршрутизаторам, распределяются по нескольким UPDATE-сообщениям. Между отправкой этих UPDATE-сообщений выдерживается случайный временной интервал таким образом, чтобы общее время между обновлением маршрутов в локальной таблице BGP и отправкой последнего UPDATE-сообщения не превышало advertisement-interval или as-origination-interval в случае отправки локальных (маршруты из локальной AS) маршрутов в eBGP-соединении. Таким образом, каждый из маршрутов может иметь случайную величину задержки анонсирования.** **- Точность работы таймеров advertisement-interval, withdraw-interval и as-origination-interval зависит от максимального значения любого из этих трёх таймеров, настроенных на BGP-маршрутизаторе (учитываются таймеры, настроенные для всех BGP-соседей). Все значения таймеров анонсирования и де-анонсирования маршрутов, сконфигурированных на устройстве, дискретизируются интервалом в 1/255 от наибольшего настроенного значения. Увеличение максимального значения будет приводить к увеличению частоты дискретизации таймеров и, соответственно, к понижению точности их работы.**
no advertisement-interval		Установить значение по умолчанию.
as-origination-interval *seconds*	seconds: (0-65535)/15 секунд	Задать временной интервал между отправкой UPDATE сообщений одного и того же маршрута, используется для анонса локальных (маршруты из локальной AS) маршрутов eBGP соседям.
no as-origination-interval		Установить значение по умолчанию.

connect-retry-interval *seconds*	seconds: (1-65535)/120 секунд	Задать временной интервал, по истечению которого возобновляется попытка создать BGP-сессию с соседом.
no connect-retry-interval		Установить значение по умолчанию.
next-hop-self [all]	—/выключено	Включить подмену значения атрибута NEXT_HOP на локальный адрес маршрутизатора. - **all** —включает подмену значения атрибута NEXT_HOP на локальный адрес маршрутизатора также и для маршрутов, отражаемых от route-reflector.
no next-hop-self		Отключить подмену атрибута NEXT_HOP.
remote-as [*as_plain_id***_|** *as_dot_id***]**	as_plain_id: (1..4294967295)/1 as_dot_id: (1.0..65535.65535)	Задать номер автономной системы, в которой находится BGP-сосед. Установление соседства невозможно, пока соседу не назначен номер AS. **Это действие влечёт разрыв сессии с соседом и очистку всех принятых от него маршрутов.**
no remote-as		Удалить идентификатор соседней автономной системы.
timers *holdtime keepalive*	holdtime: (0 | 3-65535)/90 секунд; keepalive: (0-21845)/30 секунд	Задать временные интервалы. - *holdtime* — если в течение этого времени не будет принято keepalive-сообщение, то соединение с соседом сбрасывается. - *keepalive* — интервал между отправкой keepalive-сообщений. **Значения holdtime и keepalive должны быть либо оба равны нулю, либо оба больше нуля. holdtime должен быть больше или равен keepalive.** **- Если был выбран таймер hold, который настроен на локальном маршрутизаторе, то используется локальное значение таймера keepalive;** **- Если был выбран таймер hold, который настроен на соседнем маршрутизаторе и значение локально настроенного таймера keepalive меньше чем 1/3 выбранного таймера hold, то используется локальное значение таймера keepalive;** **- Если был выбран таймер hold, который настроен на соседнем маршрутизаторе и значение локально настроенного таймера keepalive больше чем 1/3 выбранного таймера hold, то используется целое число, которое меньше чем 1/3 выбранного таймера hold.**
no timers		Установить значение по умолчанию.
timers idle-hold *seconds*	seconds: (1..32747)/15	Задать временной интервал удержания соседа в состоянии Idle после того, как он был сброшен в это состояние. За этот интервал все попытки переустановить соединение с соседом будут отклонены.
no timers idle-hold		Установить значение по умолчанию.
timers open-delay *seconds*	seconds: (0-240)/0 секунд	Задать временной интервал между установкой TCP-соединения и отправкой первого OPEN-сообщения.
no timers open-delay		Установить значение по умолчанию.
shutdown	—/no shutdown	Административно выключить сессии со всеми BGP-соседями, входящими в состав Peer-группы, и очищает принятые от них маршруты, не удаляя их конфигурации. В конфигурацию каждого соседа, входящего в peer-группу, в контекст (router-bgp-nbr) добавляется команда shutdown.
no shutdown		Административно включить сессии со всеми BGP-соседями, входящими в состав Peer-группы. Удаляет команду shutdown из конфигурации каждого соседа, входящего в peer-группу.

update-source [GigabitEthernet *gi_port* **TengigabitEthernet** *te_port* **FortygigabitEthernet** *fo_port* **Port-Channel** ***group*** **Loopback** *loopback* **Vlan** *vlan_id* **]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port(1..8/0/1..4); group: (1..48); loopback: (1-64); vlan-id: (1-4094)	Назначить интерфейс, который будет использован в качестве исходящего при соединении с соседом.
no update-source		Отменить ручную настройку исходящего интерфейса, включить автоматический выбор интерфейса.
route-reflector-client [meshed]	—/disabled	Назначить BGP-соседа Route-Reflector клиентом. - **meshed** — параметр выставляется, если используется mesh-топология. При получении от такого клиента BGP-маршрутов они не будут пересылаться другим клиентам. **BGP-маршрутизатор является route-reflector-ом, если хотя бы один его сосед сконфигурирован как клиент route-reflector.**
no route-reflector-client		Установить значение по умолчанию.
soft-reconfiguration inbound	—/disabled	Сохранить полученные от соседа маршруты в отдельной области памяти. Метод позволяет применить входящую политику "route-map in" для соседа без сброса соседства и запроса маршрутов. **По умолчанию работает механизм Route Refresh.**
no soft-reconfiguration inbound		Отключить механизм сохранения маршрутов
prefix-list *name* **{ in | out }**	name: (0..32) символа	- *name* — название IP prefix-list, который будет применен к анонсируемым или принимаемым маршрутам.
no prefix-list *name* **{ in | out }**		Отвязать IP prefix-list
fall-over bfd	—/выключено	Включить протокол BFD на peer-группе. **Не поддерживается на IPv6-соседстве.**
no fall-over bfd		Выключить протокол BFD на Peer-группе.
password *word*	word: (1..128) символов; по умолчанию аутентификация отключена	Включить аутентификацию всех TCP-сегментов, принятых от BGP-соседа. Задать ключ аутентификации в текстовом виде. Данная настройка игнорируется, если для аутентификации указана key-chain. Данная настройка игнорируется для входящих в настраиваемую группу пиров, для которых присутствуют собственные настройки аутентификации. - *word* — ключ в текстовом виде.
no password		Установить значение по умолчанию.
password encrypted *encryptedword*	encryptedword: (1..128); по умолчанию аутентификация отключена	Включить аутентификацию всех TCP-сегментов, принятых от BGP-соседа. Задает ключ аутентификации в зашифрованном виде (например, пароль в зашифрованном виде, скопированный с другого устройства). Данная настройка игнорируется, если для аутентификации указана key-chain. Данная настройка игнорируется для входящих в настраиваемую группу пиров, для которых присутствуют собственные настройки аутентификации. - encrypted*word* — ключ в текстовом виде.
no password encrypted		Установить значение по умолчанию.

password key-chain *word*	word: (1..32) символов; по умолчанию аутентификация отключена	Задать имя связки ключей, которая будет использоваться для аутентификации всех TCP-сегментов, принятых от BGP-соседа. Данная настройка игнорируется для входящих в настраиваемую группу пиров, для которых присутствуют собственные настройки аутентификации. - *word* — имя связки ключей.
no password key-chain		Установить значение по умолчанию.

Команды режима конфигурации стандартного community list

Вид запроса командной строки режима конфигурации стандартного community list:

```
console(ip-comm-list)#
```

Таблица 337 — Команды режима конфигурации стандартного community list

Команда	***Значение/Значение по умолчанию***	***Действие***
community {graceful-shutdown | internet | local-as | no-advertise | no-export | ASN2:NN}	—	Добавить community в список.
no community {graceful-shutdown | internet | local-as | no-advertise | no-export | ASN2:NN}		Удалить community из списка.

Команды режима конфигурации стандартного extcommunity_list

Вид запроса командной строки режима конфигурации стандартного extcommunity_list:

```
console(ip-extcomm-list)#
```

Таблица 338 — Команды режима конфигурации стандартного extcommunity list

Команда	***Значение/Значение по умолчанию***	***Действие***
ext-community {4byteas-generic {transitive | non-transitive} | cost [igp | pre-bestpath | rt | soo} *number*	number: (ASN2:NN, ASN4:NN, IPV4:NN)	Добавить расширенное community в список.
ext-community cost [igp | pre-bestpath] *value*	value: (0..255)	Добавит расширенное community в список.
no ext-community {4byteas-generic {transitive | non-transitive} | cost [igp | pre-bestpath | rt | soo}	—	Удалить расширенное community из списка.

Команды режима privileged EXEC

Все команды доступны для привилегированного пользователя.

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 339 – Команды режима privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
clear ip bgp [*ip_add***] vrf [***vrf-name***]**	ip_add: A.B.C.D; vrf-name: (1..32) символа, all	Переустановить соединения с BGP-соседями, очищая принятые от них маршруты. - *ip-add* — адрес соседнего BGP-спикера, с которым будет переустановлена сессия; - *vrf_name* — имя виртуальной области маршрутизации.
show ip bgp *afi safi* **vrf [***vrf-name***]**	afi: (all, ipv4, ipv6); safi: (all, unicast, multicast); vrf-name: (1..32) символа, all	Отобразить таблицу BGP-маршрутов (Loc-RIB), указанных AFI/SAFI. - *afi* — идентификатор Adress Family; - s*afi* — идентификатор Sub-Address Family; - *vrf_name* — имя виртуальной области маршрутизации.
show ip bgp [*ip_add*] **vrf [***vrf-name***]**	ip_add: A.B.C.D; vrf-name: (1..32) символа, all	Отобразить таблицу BGP-маршрутов (Loc-RIB). - *ip-add* — префикс подсети назначения, по которому будет отображена подробная информация о маршрутах до неё; - *vrf_name* — имя виртуальной области маршрутизации.
show ip bgp neighbor [*ip-add* **[detail | advertised-routes | received-routes]] vrf [***vrf-name***]**	ip_add: A.B.C.D; vrf-name: (1..32) символа, all	Отобразить информацию о настроенных BGP-соседях. - *ip-add* — адрес соседнего BGP-спикера, по которому будет отфильтрована информация. - detail — отобразить подробную информацию. - **advertised-routes** — отобразить таблицу маршрутов, анонсированных соседу. - **received-routes** — отобразить таблицу принимаемых маршрутов до применения к ним входящей политики; - *vrf_name* — имя виртуальной области маршрутизации.
show ip bgp peer-group *name* **vrf [***vrf-name***]**	name: (1..32 символа); vrf-name: (1..32) символа, all	Отобразить созданные peer-группы и их настройки. - *name* — отобразить настройки группы с именем name; - *vrf_name* — имя виртуальной области маршрутизации.
show ip bgp peer-group *name* **neighbors vrf [***vrf-name***]**	name: (1..32 символа); vrf-name: (1..32) символа, all	Отобразить состоящих в peer-группе соседей. - *name* — отобразить настройки группы с именем name; - *vrf_name* — имя виртуальной области маршрутизации.

5.35.5. Нстройка протокола IS-IS

IS-IS (intermediate system to intermediate system) — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути алгоритм Дейкстры. Протокол IS-IS представляет собой протокол внутреннего шлюза (IGP). Протокол IS-IS распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 340 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
router isis	-/ISIS маршрутизатор отключен	Запускает IS-IS маршрутизатор. Входит в режим конфигурации протокола IS-IS.
no router isis		Останавливает IS-IS маршрутизатор. Удаляет конфигурацию протокола IS-IS.

Команды режима конфигурации протокола IS-IS

Вид запроса командной строки в режиме конфигурации протокола IS-IS:

```
console(router-isis)#
```

Таблица 341 – Команды режима конфигурации протокола IS-IS

Команда	*Значение/Значение по умолчанию*	*Действие*
address-family ipv4 unicast	—	Перейти в режим конфигурации Address-Family.
authentication key *word* **[***level***]**	word: (1..20) символов; level: (level-1, level-2)/level-1-2	Задать ключ аутентификации в виде текста. Используется для аутентификации LSP, CSNP, PSNP PDU. Данная настройка игнорируется если для аутентификации указана key-chain. - *word* — ключ в текстовом виде; - *level* — уровень IS-IS, для которого применится настройка.
no authentication key		Удалить ключ аутентификации.
authentication key encrypted *encryptedword* **[***level***]**	encryptedword: (1..128) символов; level: (level-1, level-2)/level-1-2	Задает ключ аутентификации в зашифрованном виде (например, пароль в зашифрованном виде, скопированный с другого устройства). Используется для аутентификации LSP, CSNP, PSNP PDU. Данная настройка игнорируется если для аутентификации указана key-chain. - *encryptedword* — ключ в зашифрованном виде; - *level* — уровень IS-IS, для которого применится настройка.
no authentication key		Удалить ключ аутентификации.
authentication key-chain *word* **[***level***]**	word: (1..32) символа; level: (level-1, level-2)/level-1-2	Задать имя связки ключей, которая будет использоваться для аутентификации LSP, CSNP, PSNP PDU. - *word* — имя связки ключей; - *level* — уровень IS-IS, для которого применится настройка.
no authentication key-chain		Отключить режим использования связки ключей для аутентификации.
authentication mode {text | md5} [*level***]**	level: (level-1, level-2)/level-1-2; По умолчанию аутентификация отключена.	Включить аутентификацию в IS-IS и определить ее тип: - **text** — аутентификация открытым текстом; - **md5** — аутентификация MD5; - *level* — уровень IS-IS, для которого применится настройка.
no authentication mode		Установить значение по умолчанию.
hostname dynamic	—/включено	Включить поддержку динамических hostname.

no hostname dynamic		Выключить поддержку динамических hostname.
is-type {level-1 | level-2-only |level-1-2}	—/level-1-2	Задать тип маршрутизатора в IS-IS домене: - **level-1** — все взаимодействия с другими маршрутизаторами происходят на 1 уровне; - **level-2-only** — все взаимодействия с другими маршрутизаторами происходят на 2 уровне; - **level-1-2** — устройство поддерживает взаимодействия обоих уровней.
no is-type		Установить значение по умолчанию.
lsp-buff-size *size*	size (512-9000)/1500 байт	Установить максимально возможный размер отправляемых LSP и SNP. Значение lsp buffer size не должно превышать значение pdu buffer size.
no lsp-buff-size		Установить значение по умолчанию.
lsp-gen-interval second [**level**]	second: (1-65535000)/30000 миллисекунд; level: (level-1, level-2)/level-1-2	Задать минимальный интервал в мс, между генерацией одной и той же LSP. - *second* — значение интервала в миллисекундах, по истечении которого LSP может быть заново сгенерировано. - ***level*** — уровень для которого применим данный интервал. Если не указывать, интервал применится к обоим уровням.
no lsp-gen-interval		Установить значение по умолчанию.
lsp-refresh-interval second	second: (1-65235)/900 секунд;	Задать максимальный интервал в секундах, между генерацией LSP. - *second* — значение интервала в секундах, по истечении которого LSP будет заново сгенерировано.
no lsp-refresh-interval		Установить значение по умолчанию.
max-lsp-lifetime second	second: (350-65535)/1200 секунд;	Задать время жизни LSP. Значение должно быть хотя бы на 300 секунд больше, чем lsp-refresh-interval. - *second* — значение в секундах.
metric-style *style* **[***level***]**	style: (narrow, wide, both)/both level: (level-1, level-2)/level-1-2	Задать используемый стиль метрики. - narrow — поддерживать только стандартную (узкую) метрику. -wide — поддерживать только расширенную метрику. - both — поддерживать оба стиля метрики. - *level* — уровень, для которого применим указанный стиль метрики. Если не указывать, метрика применится к обоим уровням.
no metric-style		Установить значение по умолчанию.
net XX.XXXX.XXXX.XX	—	Установить так называемый NET (Network Entity Title) адрес — уникальный идентификатор маршрутизатора в пределах IS-IS домена. При записи NET используется шестнадцатеричная система счисления.
no net		Удалить идентификатор маршрутизатора.
shutdown	—/включено	Отключить процесс ISIS.
no shutdown		Включить процесс ISIS.
spf interval maximum-wait *second*	second: (0-4294967295)/5000	Установить интервал между двумя последовательными пересчетами алгоритма SPF в миллисекундах.
no spf interval maximum-wait		Установить значение по умолчанию.

spf threshold restart-limit *number*	number: (1-4294967295)/10	Установить, сколько раз алгоритм SPF может быть прерван обновлением LSDB.
no spf threshold restart-limit		Установить значение по умолчанию.
spf threshold updates-restart *number*	number: (1-4294967295)/4294967295	Задает количество обновлений LSDB, при которых алгоритм SPF останавливается и перезапускается
no spf threshold updates-restart		Установить значение по умолчанию.
spf threshold updates-start *number*	number: (1-4294967295)/4294967295	Установить количество обновлений LSDB, необходимое для немедленного запуска алгоритма SPF (spf interval maximum-wait при этом игнорируется).
no spf threshold updates-start		Установить значение по умолчанию.
no max-lsp-lifetime		Установить значение по умолчанию.

Команды режима конфигурации Address-Family

Вид запроса командной строки в режиме конфигурации Address-Family:

```
console(router-isis-af)#
```

Таблица 342 — Команды режима конфигурации Address-Family

Команда	***Значение/Значение по умолчанию***	***Действие***
redistribute connected [level *level*] **[metric-type** ***type***] **[metric** *metric*] **[filter-list** *name*]	level: (level-1, level-2); type: (internal, external); metric: (1-16777215); name: (1-32) символа.	Разрешить импорт connected-маршрутов: - *level* — уровень IS-IS, в который будет выполняться перераспределение маршрутов; - *type* — установить импортируемым маршрутам тип метрики; - *metric* — значение метрики для импортируемых маршрутов; - *name* — имя стандартного IP ACL, который будет использован для фильтрации импортируемых маршрутов. Если глобально включен стандартный (narrow) стиль метрики, все значения метрики больше 63 будут указаны в TLV как 63.
no redistribute connected [level *level]* **[metric-type** ***type]*** **[metric** *metric]* ***[*****filter-list** *name]*		Запретить импорт connected-маршрутов в IS-IS. В случае указания параметра вернуть его значение по умолчанию.
redistribute static [level *level*] **[metric-type** *type*] **[metric** *metric*] **[filter-list** *name*]	level: (level-1, level-2); type: (internal, external); metric: (1-16777215); name: (1-32) символа.	Разрешить импорт статических маршрутов в IS-IS. - *level* — уровень IS-IS, в который будет выполняться перераспределение маршрутов; - *type* — установить импортируемым маршрутам тип метрики; - *metric* — значение метрики для импортируемых маршрутов; - *name* — имя стандартного IP ACL, который будет использован для фильтрации импортируемых маршрутов. Если глобально включен стандартный (narrow) стиль метрики, все значения метрики больше 63 будут указаны в TLV как 63.

no redistribute static [level *level***] [metric-type** *type***] [metric** *metric***] [filter-list** *name***]**		Запретить импорт статических маршрутов в IS-IS. В случае указания параметра вернуть его значение по умолчанию.
redistribute rip [level *level***] [metric-type** *type***] [metric** *metric***] [filter-list** *name***]**	level: (level-1, level-2); type: (internal, external); metric: (1-16777215); name: (1-32) символа.	Разрешить импорт маршрутов из RIP в IS-IS. - *level* — уровень IS-IS, в который будет выполняться перераспределение маршрутов; - *type* — установить импортируемым маршрутам тип метрики; - *metric* — значение метрики для импортируемых маршрутов; - *name* — имя стандартного IP ACL, который будет использован для фильтрации импортируемых маршрутов. Если глобально включен стандартный (narrow) стиль метрики, все значения метрики больше 63 будут указаны в TLV как 63.
no redistribute rip [level *level***] [metric-type** *type***] [metric** *metric***] [filter-list** *name***]**		Запретить импорт маршрутов из RIP в IS-IS. В случае указания параметра вернуть его значение по умолчанию.
redistribute bgp [level *level***] [metric-type** *type***] [metric** *metric***] [filter-list** *name***]**	level: (level-1, level-2); type: (internal, external); metric: (1-16777215); name: (1-32) символа.	Разрешить импорт маршрутов из BGP в IS-IS. - *level* — уровень IS-IS, в который будет выполняться перераспределение маршрутов; - *type* — установить импортируемым маршрутам тип метрики; - *metric* — значение метрики для импортируемых маршрутов; - *name* — имя стандартного IP ACL, который будет использован для фильтрации импортируемых маршрутов. Если глобально включен стандартный (narrow) стиль метрики, все значения метрики больше 63 будут указаны в TLV как 63.
no redistribute bgp [level *level***] [metric-type** *type***] [metric** *metric***] [filter-list** name**]**		Запретить импорт маршрутов из BGP в IS-IS. В случае указания параметра вернуть его значение по умолчанию.
redistribute ospf [*id*] [level *level***] [metric-type** *type***] [match** *match***] [metric** *metric***] [filter-list** *name***]**	Id: (1-65536) level: (level-1, level-2); type: (internal, external); match:(internal, external-1, external-2, nssa-external-1, nssa-external-2); metric: (1-16777215); name: (1-32) символа.	Разрешить импорт маршрутов из OSPF в IS-IS. - *id* — идентификатор процесса OSPF; - *level* — уровень IS-IS, в который будет выполняться перераспределение маршрутов; - *type* — установить импортируемым маршрутам тип метрики; - *match* — тип маршрута OSPF, подлежащий импорту. - *metric* — значение метрики для импортируемых маршрутов; - *name* — имя стандартного IP ACL, который будет использован для фильтрации импортируемых маршрутов. Если глобально включен стандартный (narrow) стиль метрики, все значения метрики больше 63 будут указаны в TLV как 63.
no redistribute ospf [*id*] [level *level***] [metric-type** *type***] [match** *match***] [metric** *metric***] [filter-list** *name***]**		Запретить импорт маршрутов из OSPF в IS-IS. В случае указания параметра вернуть его значение по умолчанию.

Команды режима конфигурации интерфейса Ethernet, VLAN:

Вид запроса командной строки:

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

Таблица 343 — Команды режима конфигурации интерфейса Ethernet, VLAN

Команда	*Значение/Значение по умолчанию*	*Действие*
ip router isis	—/выключено	Включить протокол маршрутизации IS-IS на текущем интерфейсе.
no ip router isis		Выключить протокол маршрутизации IS-IS на текущем интерфейсе.
isis authentication key *word* **[***level***]**	word: (1..20) символов; level: (level-1, level-2)/level-1-2	Задать ключ аутентификации в виде текста. Используются для аутентификации HELLO PDU. Данная настройка игнорируется если для аутентификации указан key-chain. - *word* — ключ в текстовом виде; - *level — уровень IS-IS*
no isis authentication key		Удалить ключ аутентификации.
isis authentication key encrypted *encryptedword* **[***level***]**	encryptedword: (1..128) символов; level: (level-1, level-2)/level-1-2	Задать ключ аутентификации в зашифрованном виде (например, пароль в зашифрованном виде, скопированный с другого устройства). Используются для аутентификации HELLO PDU. Данная настройка игнорируется если для аутентификации указан key-chain. - *encryptedword* — ключ в зашифрованном виде.
no isis authentication key		Удалить ключ аутентификации.
isis authentication key-chain *word* **[***level***]**	word: (1..32) символа; level: (level-1, level-2)/level-1-2	Задать имя связки ключей, которая будет использоваться для аутентификации HELLO PDU. - *word* — имя связки ключей.
no isis authentication key-chain		Отключить режим использования связки ключей для аутентификации.
isis authentication mode {text | md5} [*level***]**	level: (level-1, level-2)/level-1-2; По умолчанию аутентификация отключена.	Включить аутентификацию в HELLO PDU на текущем интерфейсе и определить ее тип: - **text** — аутентификация открытым текстом; - **md5** — аутентификация MD5.
no isis authentication mode		Установить значение по умолчанию.
isis circuit-type {level-1 | level-2-only |level-1-2}	—/level-1-2	Указать, соседства какого уровня можно формировать на данном интерфейсе.
no isis circuit-type		Установить значение по умолчанию.
isis metric *metric* **[***level***]**	metric: (1-16777215)/10; level: (level-1, level-2)/level-1-2	Установить метрику для данного интерфейса. - *metric* — значение метрики. Если глобально включен стандартный (narrow) стиль метрики, все значения метрики больше 63 будут указаны в TLV как 63. - *level* — уровень IS-IS, для которого будет применяться метрика.
no isis metric		Установить значение по умолчанию.
isis passive-interface	—/пассивный режим отключен	Перевести интерфейс в пассивный режим. В этом режиме интерфейс не отправляет и не принимает HELLO PDU.
no isis passive-interface		Установить значение по умолчанию.
isis network point-to-point	—/broadcast	Установить тип интерфейса point-to-point.
no isis network point-to-point		Установить значение по умолчанию.

isis hello-padding *value*	value: (disable, enable, adaptive)/enable	Установить режим работы паддинга hello-сообщений. - disable — отключить паддинг во всех сообщениях hello; - enable — включить паддинг во всех сообщениях hello; - adaptive — включить паддинг до установления соседства.
no isis hello-padding		Установить значение по умолчанию.
isis pdu-buff-size ***size***	size (512-9000)/1500 байт	Установить размер hello PDU. Значение **pdu-buff-size должно быть больше значения lsp-buff-size.**
no isis pdu-buff-size		Установить значение по умолчанию.

Команды режима конфигурации интерфейса Loopback:

Вид запроса командной строки:

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

Таблица 344 — Команды режима конфигурации интерфейса Loopback

Команда	***Значение/Значение по умолчанию***	***Действие***
ip router isis	—/выключено	Включить протокол маршрутизации IS-IS на текущем интерфейсе.
no ip router isis		Выключить протокол маршрутизации IS-IS на текущем интерфейсе.
isis circuit-type {level-1 | level-2-only |level-1-2}	—/level-1-2	Указать, соседства какого уровня можно формировать на данном интерфейсе.
no isis circuit-type		Установить значение по умолчанию.
isis metric *metric* **[***level***]**	metric: (1-16777215)/10; level: (level-1, level-2)/level-1-2	Установить метрику для данного интерфейса. - *metric* — значение метрики. Если глобально включен стандартный (narrow) стиль метрики, все значения метрики больше 63 будут указаны в TLV как 63. - *level* — уровень IS-IS, для которого будет применяться метрика.
no isis metric		Установить значение по умолчанию.
isis passive-interface	—/пассивный режим отключен	Перевести интерфейс в пассивный режим. В этом режиме интерфейс не отправляет и не принимает HELLO PDU.
no isis passive-interface		Установить значение по умолчанию.

Команды режима privileged EXEC

Вид запроса командной строки имеет вид:

```
console#
```

Таблица 345 — Команды режима privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show isis database [level] **[detail] [lsp-id** lsp-id**]**	level: (level-1, level-2) lsp-id: 20 символов	Отобразить базу данных топологии протокола IS-IS. - **level** — указывает уровень протокола IS-IS, базу данных которого необходимо отобразить; - **detail** — отображение подробной информации о TLV; - **lsp-id** — отображение информации по выбранной LSP PDU.

show isis hostname	—	Отобразить известные соответствия *SystemID* и *Hostname.*
show isis interfaces [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback***| vlan** *vlan_id***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port(1..8/0/1..4; group: (1..48); loopback: (1-64); vlan-id: (1-4094)	Отобразить информацию об интерфейсах, участвующих в IS-IS.
show isis neighbors [detail] [gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| loopback** *loopback***| vlan** *vlan_id***]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port(1..8/0/1..4; group: (1..48); loopback: (1-64); vlan-id: (1-4094)	Отобразить информацию о соседях. - **detail** — использование данного параметра позволяет отобразить детальную информацию о соседях.
clear isis	—	Сбросить все соседства и очистить таблицу маршрутизации IS-IS.

5.35.6. Настройка Route-Map

Применение route-map позволяет изменять атрибуты у анонсируемых и принимаемых маршрутов BGP.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 346 – Команды режима глобальной конфигурации

Команда	***Значение/Значение по умолчанию***	***Действие***
route-map *name* **[** *section_id* **] [permit | deny]**	name: (0..32) символа; section_id: (1.. 4294967295).	Создать запись route-map. Переводит командную строку в режим конфигурирования route-map. - name — название route-map. - section_id — номер записи в этой route-map. - permit — применить set команды к маршрутам, - deny — отбросить маршруты. **Максимальное количество route-map = 32 (включая секции одного route-map).**
no route-map *name* **[** *section_id* **] [permit | deny]**		Удалить route-map - *section_id* — удаляет запись с номером section_id.

Команды режима конфигурации секции route-map

Вид запроса командной строки в режиме конфигурации секции route-map:

```
console(config-route-map)#
```

Таблица 347 – Команды режима конфигурации секции route-map

Команда	*Значение/Значение по умолчанию*	*Действие*
continue *section_id* **[and]**	section_id: (1.. 4294967295).	Задать номер следующей секции route-map, которая будет применена к маршрутам, после применения текущей. - **and** — указывает, что match установки в этой route-map должны быть логически объединены (AND) с match установками в route-map, обозначенных параметром section_id. **Создание цепочек route-map (без параметра and) возможно, если тип route-map выставлен в permit.** **Если при создании цепочки применяется параметр and, то все set установки должны находиться в последней секции этой цепочки.**
no continue		Сбросить установку.
match ip [address | next-hop | route-source] prefix-list *name*	name: (0..32) символа	Задать соответствие prefix-list и адреса маршрута. - **address** — соответствие prefix-list и ip адреса маршрута. - **next-hop** — соответствие prefix-list и next-hop ip адреса маршрута. - **route-source** — соответствие prefix-list и ip адреса источника маршрута. **Чтобы не отбрасывались остальные маршруты, не указанные в prefix-list, необходимо создать пустой route-map и привязать его к текущему через continue.**
no match ip [address | next-hop | route-source] prefix-list *name*		Сбросить соответствие.
match local-preference *value*	value: (1.. 4294967295).	Задать соответствие маршрута с атрибутом local-preference.
no match local-preference		Сбросить соответствие.
match metric *value*	value: (1.. 4294967295).	Задать соответствие маршрута с атрибутом metric.
no match metric		Сбросить соответствие.
match origin [igp |egp | incomplete]	—	Задать соответствие маршрута с атрибутом origin. - **igp** — маршрут был получен из протокола внутренней маршрутизации (например, командой **network**) - **egp** — маршрут был выучен по протоколу EGP. - **incomplete** — маршрут был выучен каким-то иным образом (например командой **redistribute**).
no match origin		Сбросить соответствие.
match {community | extcommunity} *name* **[exact-match]**	—	Задать соответствие, при котором community из списка с именем *name* должны содержаться в community маршрута. **exact-match** — требует точного совпадения всех community из списка с community маршрута.
no match {community | extcommunity}		Сбросить соответствие.
set community {add | replace | remove} {graceful-shutdown | internet | local-as | no-advertise | no-export | *number***}**	number: ASN2:NN	**add** — добавить к маршруту community; **replace** — удалить все community из маршрута и добавить указанное; **remove** — удалить из маршрута указанное community.
no set community		Сбросить действие set community.
set community-list {add | remove} *name*	name: (1..32) символа	**add** — добавить к маршруту все community из списка с именем *name*; **remove** — удалить из маршрута все community, содержащиеся в списке с именем *name*.

no set community-list {add | remove}		Сбросить действие set community-list.
set community-list remove all	—	Удалить из маршрута все community.
no set community-list remove all		Сбросить действие, удаляющее из маршрута все community.
set extcommunity {add | replace | remove} sub-type {rt | soo} *number*	number: (ASN2:NN, ASN4:NN, IPV4:NN)	**add** — добавить к маршруту расширенное community; **replace** — удалить все расширенные community из маршрута и добавить указанное; **remove** — удалить из маршрута указанное community.
set extcommunity {add | replace | remove} sub-type color *value*	value: (0..4294967295)	**add** — добавить к маршруту расширенное community; **replace** — удалить все расширенные community из маршрута и добавить указанное; **remove** — удалить из маршрута указанное community.
set extcommunity {add | replace | remove} *word*	word: (1..127)	**add** — добавить к маршруту расширенное community; **replace** — удалить все расширенные community из маршрута и добавить указанное; **remove** — удалить из маршрута указанное (или все попадающие под регулярное выражение) community. Для данной операции можно использовать в качестве параметра word регулярное выражение. *word: — имя* community в формате HEX.
no set extcommunity	—	Сбросить действие set extcommunity.
set extcommunity-list {add | remove} *name*	name: (1..32) символа	**add** — добавить к маршруту все расширенные community из списка с именем *name*; **remove** — удалить из маршрута все расширенные community, содержащиеся в списке с именем *name*.
no set extcommunity-list {add | remove}		Сбросить действие.
match tag *value*	value: (0-4294967295)	Задать соответствие маршрута с атрибутом tag.
no match tag		Сбросить соответствие.
set tag *value*	value: (0-4294967295)	Установить значение атрибута tag.
no set tag		Сбросить установку атрибута tag.
match as-number *reg_exp*	reg_exp: (1..127) символа	Задать соответствие пути маршрута и регулярного выражения *reg_exp*.
no match as-number		Сбросить соответствие.
match as-path-filter *name*	name: (1..32) символа	Задать соответствие пути маршрута и регулярного выражения *as-path* из списка с именем *name*.
no match as-path-filter		Сбросить соответствие.
set as-path path-limit *value*	value: (0-255)	Добавить к маршруту атрибут AS_PATHLIMIT. Нулевое значение ограничивает анонсирование локально сгенерированных маршрутов, только между iBGP соседями (не будут видны для eBGP). Значение больше 0 означает, что если AS_PATH атрибут имеет больше AS-номеров, чем значение AS_PATHLIMIT, то нужно его отбросить при выходе в eBGP.
no set as-path path-limit		Сбросить path-limit.
set as-path prepend *as_number*	as_number: (1-4294967295)	Добавить к атрибуту AS-Path введенные AS-номера.
no set as-path prepend		Сбросить добавление к AS-Path.
set as-path prepend local-as *value*	value: (0-10)	Добавить к атрибуту AS-Path *value* номеров Local AS (на выход eBGP соседу).
no set as-path prepend local-as		Сбросить добавление к AS-Path.
set as-path remove *as_number*	as_number: (0..127) символа	Удалить из атрибута AS-Path указанную AS.
no set as-path remove		Сбросить удаление.

set ip next-hop *ip_address*	—	Установить next-hop атрибут маршрута. - ip_address — IP-адрес next-hop.
no set ip next-hop		Сбросить установку атрибута next-hop.
set local-preference *value*	value: (1-4294967295)	Установить значение атрибута local-preference.
no set local-preference		Сбросить установку атрибута local-preference.
set metric *value*	value: (1-4294967295)	Установить значение атрибута metric.
no set metric		Сбросить установку атрибута metric.
set next-hop-peer	—/атрибут не установлен	Установить значение атрибута next-hop, как адрес соседа.
no set next-hop-peer		Сбросить установку атрибута.
set origin [igp |egp | incomplete]	—	Установить значение атрибута origin. - **igp** — маршрут был получен из протокола внутренней маршрутизации (например, командой **network**) - **egp** — маршрут был выучен по протоколу EGP. - **incomplete** — маршрут был выучен каким-то иным образом (например командой **redistribute**).
no set origin		Сбросить установку атрибута origin.
set weight *value*	value: (1-4294967295)	Установить значение атрибута weight.
no set weight		Сбросить установку атрибута weight.

Команды режима privileged EXEC

Все команды доступны для привилегированного пользователя.

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 348 – Команды режима privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show route-map [*name***]**	name: (0..32) символа	Просмотр информации о созданных route-map. - name – имя route-map.

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 349 – Команды режима конфигурации интерфейса Ethernet, VLAN, интерфейса группы портов

Команда	***Значение/Значение по умолчанию***	***Действие***
ip policy route-map *name*	*name: (0..32) символа*	Применить route-map с именем name для заданного интерфейса.
no ip policy route-map		Удалить route-map с интерфейса.

5.35.7. Настройка Prefix-List

Prefix-листы позволяют фильтровать принимаемые и анонсируемые маршруты протоколов динамической маршрутизации.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 350 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip prefix-list *list-name* **[seq** *seq_value***] [description** *text***] {deny | permit}** *ip_address* **[***mask***] [ge** *ge_value***] [le** *le_value***]**	list-name: (1..32); *seq_value: (1.. 4294967294);* text*:* (0..80) символа; ge_value: (1..32); le_value: (1..32)	Создать Prefix-list. **- permit –** разрешающее действие для маршрута **- deny** – запрещающее действие для маршрута - list-name – имя создаваемого prefix-листа - seq_value – номер записи в списке префиксов - text – описание списка префиксов - ge_value –соответствие длине префикса, равной или большей, чем настроенная длина префикса - le_value – соответствие длине префикса, которая равна или меньше настроенной длины префикса. Если не нашлось ни одного соответствия, то будет применена неявная политика по умолчанию **deny any.**
no ip prefix-list *list-name* **[seq** *seq_value***]**		Удалить созданный Prefix-List.

Команды режима privileged EXEC

Все команды доступны для привилегированного пользователя.

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 351 – Команды режима privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip prefix-list [*name***]**	name: (0..32) символа	Просмотр информации о созданных prefix-list. - name – имя prefix-list.

5.35.8. Настройка связки ключей

Связка ключей позволяет создать набор паролей (ключей) с последующей возможностью настройки времени действия каждого пароля. Созданные пароли могут использоваться протоколами RIP, OSPF, IS-IS для аутентификации.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 352 — Команды режима глобальной конфигурации

Команда	***Значение/Значение по умолчанию***	***Действие***
key chain *word*	word: (1..32) символа/-	Создает связку ключей с именем *word* и входит в режим конфигурации связки ключей.
no key chain *word*		Удаляет связку ключей с именем *word*.

Команды режима конфигурации связки ключей

Вид запроса командной строки в режиме конфигурации связки ключей:

```
console(config-keychain)#
```

Таблица 353 — Команды режима конфигурации связки ключей

Команда	***Значение/Значение по умолчанию***	***Действие***
key *key_id*	key_id: (1..255)/-	Создает ключ с идентификатором *key_id* и входит в режим конфигурации ключа.
no key *key_id*		Удаляет ключ с идентификатором *key_id*.

Команды режима конфигурации ключа

Вид запроса командной строки в режиме конфигурации ключа:

```
console(config-keychain-key)#
```

Данный режим доступен из режима конфигурации связки ключей и предназначен для задания самого ключа и его параметров.

Таблица 354 — Команды режима конфигурации ключа

Команда	***Значение/Значение по умолчанию***	***Действие***
key-string *word*	word: (1..16) символов/—	Задать значение ключа.
no key-string		Удалить значение ключа.
encrypted key-string *encryptedword*	encryptedword/—	Задать значение ключа в зашифрованном виде. - *encryptedword* — зашифрованный пароль (например, пароль в зашифрованном виде, скопированный с другого устройства).
no encrypted key-string		Удалить значение ключа.
accept-lifetime *time_to_start* **{***time_to_stop* **|** *duration* **|** *infinite***}**	—/всегда действителен	Задать время жизни ключа, в течение которого ключ будет действителен для сверки с ключом в принимаемых сообщениях. - *time_to_start* — время и дата начала действия ключа. Задается в формате *hh:mm:ss month day year* - *time_to_stop* — время и дата прекращения действия ключа. Задается в формате *hh:mm:ss month day year*

		- *duration* — задает продолжительность действия ключа в секундах - *infinite* — устанавливает бесконечное время действия ключа
no accept-lifetime		Удалить время жизни ключа
send-lifetime *time_to_start* {*time_to_stop* **|** *duration* **|** *infinite*}	—/всегда действителен	Задать время жизни ключа, в течение которого ключ будет действителен для отправки сообщений. - *time_to_start* — время и дата начала действия ключа. Задается в формате *hh:mm:ss month day year.* - *time_to_stop* — время и дата прекращения действия ключа. Задается в формате *hh:mm:ss month day year.* - *duration* — задает продолжительность действия ключа в секундах. - *infinite* — устанавливает бесконечное время действия ключа.
no send-lifetime		Удалить время жизни ключа.

Если в какой-то момент времени сразу несколько ключей будут являться действительными, то фактически использоваться будет ключ с наименьшим идентификатором.

Команды режима privileged EXEC

Вид запроса командной строки имеет вид:

```
console#
```

Таблица 355 — Команды режима privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show key chain *word*	word: (1..32) символа/-	Отображает информацию о связке ключей с именем *word*

Примеры выполнения команд

Создать связку ключей с именем name1 и поместить в неё два ключа. На ключе key 2 настроить временной интервал, в течение которого этот ключ может быть использован для сверки с ключом в принятых пакетах.

```
console(config)#key chain name1
console(config-keychain)#key 1
console(config-keychain-key)#key-string testkey1
console(config-keychain-key)#exit
console(config-keychain)#key 2
console(config-keychain-key)#key-string testkey2
console(config-keychain-key)#accept-lifetime 12:00:00 feb 20 2020 12:00:00 mar 20 2020
```

Показать информацию о созданной связке ключей:

```
console# show key chain name1
```

```
Key-chain name1:
   key 1 -- text (Encrypted) "y9nRgqddPOa7W3O4gfrNBeGhigRuwwp6mWCy69nLuQk="
       accept lifetime (always valid) - (always valid) [valid now]
       send lifetime (always valid) - (always valid) [valid now]
   key 2 -- text (Encrypted) "G7sTS+v5oGJwHBL6UxZyWVPzbqZ/6fIOF3h3NB6wYMM="
       accept lifetime (12:00:00 Feb 20 2020) - (12:00:00 Mar 20 2020)
       send lifetime (always valid) - (always valid) [valid now]
```

5.35.9. *Балансировка нагрузки Equal-Cost Multi-Path (ECMP)*

Балансировка нагрузки ECMP позволяет передавать пакеты одному получателю по нескольким «лучшим маршрутам». Данный функционал предназначен для распределения нагрузки и оптимизации пропускной способности сети. ECMP может работать как со статическими маршрутами, так и с протоколами динамической маршрутизации RIP, OSPF, BGP.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 356 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip maximum-paths *maximum_paths*	maximum_paths: (1..64)/1	Задать максимальное количество путей, которые могут быть установлены в FIB для каждого маршрута. **Настройка вступит в силу только после сохранения конфигурации и перезагрузки устройства.**
no ip maximum-paths		Установить значение по умолчанию.

5.35.10. *Настройка Virtual Router Redundancy Protocol (VRRP)*

Протокол VRRP предназначен для резервирования маршрутизаторов, выполняющих роль шлюза по умолчанию. Это достигается путём объединения IP-интерфейсов группы маршрутизаторов в один виртуальный, который будет использоваться как шлюз по умолчанию для компьютеров в сети. На канальном уровне резервируемые интерфейсы имеют MAC-адрес 00:00:5E:00:01:XX, где XX – номер группы VRRP (VRID).

Только один из физических маршрутизаторов может выполнять маршрутизацию трафика на виртуальном IP-интерфейсе (VRRP master), остальные маршрутизаторы в группе предназначены для резервирования (VRRP backup). Выбор VRRP master происходит в соответствии с RFC 5798. Если текущий master становится недоступным – выбор master'a повторяется. Наивысший приоритет имеет маршрутизатор с собственным IP-адресом,

совпадающим с виртуальным. В случае доступности он всегда становится VRRP master. Максимальное количество VRRP-процессов – 50.

Команды режима конфигурации интерфейсов Ethernet, VLAN, интерфейса группы портов

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

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

Таблица 357 – 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).	Добавить описание цели или использования для VRRP маршрутизатора с идентификатором *vrid.*
no vrrp *vrid* **description**		Удалить описание VRRP-маршрутизатора.
vrrp *vrid* **ip** *ip_address*	vrid: (1..255)	Определить IP-адрес VRRP-маршрутизатора.
no vrrp *vrid* **ip** [*ip_address*]		Удалить IP-адрес 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	Включить режим, 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**		Установить значение по умолчанию.
vrrp *vrid* **priority** *priority*	vrid: (1..255); priority: (1..254); По умолчанию: 255 для владельца IP-адреса,100 для остальных	Назначить приоритет VRRP-маршрутизатора.
no vrrp *vrid* **priority**		Установить значение по умолчанию.
vrrp *vrid* **shutdown**	vrid: (1..255); По умолчанию: выключен	Выключить VRRP-протокол на данном интерфейсе.
no vrrp *vrid* **shutdown**		Включить VRRP-протокол на данном интерфейсе.
vrrp *vrid* **source-ip** *ip_address*	vrid: (1..255); По умолчанию: 0.0.0.0	Определить реальный VRRP-адрес, который будет использоваться в качестве IP-адреса отправителя для VRRP-сообщений.
no vrrp *vrid* **source-ip**		Установить значение по умолчанию.
vrrp *vrid* **timers advertise** {*seconds* **|** **msec** *milliseconds*}	seconds: (1..40); milliseconds: (50..40950); По умолчанию: 1 сек	Определить интервал 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]**		Установить значение по умолчанию.

vrrp *vrid* **version {2 | 3 | 2&3}**	—/2	Определить поддерживаемую версию 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.
no vrrp *vrid* **version**		Установка значения по умолчанию.
vrrp *vrid* **checksum exclude pseudo-header**	По умолчанию: используется метод расчета контрольной суммы с псевдозаголовком	Включить метод расчета контрольной суммы в заголовке VRRP без учета псевдозаголовка. RFC 3768.
no vrrp *vrid* **checksum exclude pseudo-header**		Установить метод расчета контрольной суммы, определенный в RFC5798, по умолчанию.

Команды режима privileged EXEC

Все команды доступны для привилегированного пользователя.

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 358 – Команды режима privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show vrrp [all | brief | interface {gigabitethernet *gi_port* **| tengigabitethernet** *te_port* **| fortygigabitethernet** *fo_port* **| port-channel** *group* **| vlan** *vlan_id***}]**	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Просмотреть краткую или детальную информацию для всех или одного настроенного виртуального маршрутизатора VRRP. - **all** — просмотр информации о всех виртуальных маршрутизаторах, включая отключенные; - **brief** — просмотр краткой информации о всех виртуальных маршрутизаторах.

Примеры выполнения команд

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

```
console(config-vlan)# interface vlan 10
console(config-if)# ip address 10.10.10.1 /24
console(config-if)# vrrp 1 ip 10.10.10.1
console(config-if)# no vrrp 1 shutdown
```

- Посмотреть конфигурацию VRRP:

```
console# show vrrp
Interface: vlan 10
Virtual Router 1
Virtual Router name
Supported version VRRPv3
State is Initializing
Virtual IP addresses are 10.10.10.1(down)
```

```
Source IP address is 0.0.0.0(default)
Virtual MAC address is 00:00:5e:00:01:01
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 255
```

5.35.11. *Настройка протокола Bidirectional Forwarding Detection (BFD)*

Протокол BFD позволяет быстро обнаружить неисправности линков. BFD может работать как со статическими маршрутами, так и с протоколами динамической маршрутизации RIP, OSPF, BGP.

В текущей версии ПО реализована работа только с протоколом BGP.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 359 – Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
bfd neighbor *ip_addr* **[interval** *int* **] [min-rx** *min***] [multiplier** *mult_num***]**	int: (150..1000)/150 min: (150..1000)/150 mult_num: (1..255)/3	Задать BFD-соседа. - **int** – минимальный интервал передачи для обнаружения ошибки; - **min** – минимальный интервал приёма для обнаружения ошибки. - **mult_num** – количество потеряных пакетов до разрыва сессии
no bfd neighbor *ip_addr*		Установить значение по умолчанию.

Команды режима privileged EXEC

Все команды доступны для привилегированного пользователя.

Вид запроса командной строки режима privileged EXEC:

```
console#
```

Таблица 360 – Команды режима privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip bfd neighbors [*ip_addr***] [detail]**		Просмотр информации об активных BFD-соседях

5.35.12. Протокол GRE

GRE (Generic Routing Encapsulation) — протокол туннелирования сетевых пакетов. Его основное назначение — инкапсуляция пакетов сетевого уровня сетевой модели OSI в IP-пакеты. GRE может использоваться для организации VPN на 3-м уровне модели OSI. В коммутаторах RTT реализованы статические неуправляемые GRE-туннели, то есть туннели создаются вручную путем конфигурирования на локальном и удаленном узлах. Параметры туннеля для каждой из сторон должны быть взаимосогласованными или переносимые данные не будут декапсулироваться партнером.

Протокол GRE поддерживается на моделях серии RTT-A330 и на RTT-A420-24XG-4QXG.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 361 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
interface Tunnel *tunnel_id*	tunnel_id: (1..16)	Создает интерфейс туннеля.

Команды режима конфигурации интерфейса туннеля

Вид запроса командной строки в режиме конфигурации интерфейса туннеля:

```
console(config-tunnel)#
```

Таблица 362 — Команды режима конфигурации интерфейса туннеля

Команда	*Значение/Значение по умолчанию*	*Действие*
tunnel mode gre ip	—/выключено	Задает тип туннеля GRE с использованием IPv4.
no tunnel mode gre ip		Удаляет туннель.
tunnel source {ipv4_address | **gigabitethernet** *gi_port* | **tengigabitethernet** *te_port* | **fortygigabitethernet** *fo*_port | **port-channel** *group* | **tunnel** *tunnel*_id | **vlan** *vlan_id*}	gi_port: (1..8/0/1..48); te_port: (1..8/0/1..24); fo_port: (1..8/0/1..4); group: (1..48); vlan_id: (1..4094)	Назначает IP-адрес или интерфейс, который будет использоваться в качестве адреса отправителя внешнего IP-заголовка GRE туннеля.
no tunnel source		Удаляет IP-адрес отправителя.

tunnel destination {_URL_ | *ipv4_address***}**	—	Назначает IP-адрес получателя (конца туннеля).
no tunnel destination		Удаляет IP-адрес получателя.
ip address *ipv4_address*	—	Устанавливает IP-адрес интерфейса туннеля. С использованием этого адреса коммутатор доступен через туннель. Может использоваться в качестве шлюза на удаленном устройстве при маршрутизации в туннель.
no ip address		Удаляет IP-адрес интерфейса туннеля.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 363 — Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip tunnel [*tunnel-id***]**	tunnel_id: (1..16)	Отображает информацию туннеля.
show ip interface tunnel *tunnel_id*	tunnel_id: (1..16)	Отображает информацию об IP-интерфейсе туннеля.
show interfaces tunnel *tunnel-id*	tunnel_id: (1..16)	Отображает информацию интерфейса туннеля.

Пример настройки туннеля

Создание туннеля и настройка статического маршрута для сети, находящейся на противоположной стороне туннеля:

- в качестве локального адреса для туннеля используется IP-адрес 192.168.1.1;
- в качестве удаленного адреса для туннеля используется IP-адрес 192.168.1.2;
- IP-адрес туннеля на локальной стороне 172.16.0.1/30;
- сеть на противоположной стороне туннеля 10.10.1.0/24

```
console(config)#vlan database
console(config-vlan)#vlan 301
console(config-vlan)#exit
console(config)#interface tengigabitethernet1/0/1
console(config-if)#switchport mode trunk
console(config-if)#switchport trunk allowed vlan add 301
console(config-if)#exit
console(config)#interface vlan 301
console(config-if)#ip address 192.168.1.1 /24
console(config-if)#exit
console(config)#interface Tunnel 1
console(config-tunnel)#Tunnel mode gre ip
console(config-tunnel)#Tunnel source 192.168.1.1
console(config-tunnel)#Tunnel destination 192.168.1.2
console(config-tunnel)#ip address 172.16.0.1 /30
console(config-tunnel)#exit
console(config)#ip route 10.10.1.0 /24 Tunnel 1
```

На встречном устройстве необходимо выполнить взаимосогласованные настройки.

5.35.13. Конфигурация виртуальной области маршрутизации (VRF)

VRF (Virtual Routing and Forwarding) — это технология, которая позволяет нескольким экземплярам таблицы маршрутизации сосуществовать в одном маршрутизаторе одновременно.

Список поддержанных в VRF функций доступен в таблице 367.

Таблица 364 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip vrf [vrf-name**]**	vrf-name: (1..32) символа	Создание виртуальной области маршрутизации.
no ip vrf [vrf-name**]**		Удаление виртуальной области маршрутизации.

Таблица 365 — Команды режима конфигурации интерфейса

Команда	*Значение/Значение по умолчанию*	*Действие*
ip vrf [vrf-name**]**	vrf-name: (1..32) символа	Привязка интерфейса к области виртуальной маршрутизации. После ввода команды все созданные в дальнейшем IP-адреса будут ассоциироваться с vrf, к которому был привязан интерфейс.
no ip vrf		Отвязка интерфейса от области виртуальной маршрутизации.

Таблица 366 — Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip vrf [all | vrf-name**]**	vrf-name: (1..32) символа	Вывод информации о созданных виртуальных областях маршрутизации и об L3-интерфейсах, которые в них находятся.

Таблица 367 — Функции, поддержанные для работы в VRF

Функции	*Навигация*
Команды управления системой	5.5 Команды управления системой
Статическая маршрутизация	5.35 Конфигурация протоколов маршрутизации
DHCP-Relay	5.29.1 Функции DHCP Relay для IPv4
OSFP	5.35.3 Настройка протокола OSPF, OSPFv3
BGP	5.35.4 Настройка протокола BGP (Border Gateway Protocol)

6. СЕРВИСНОЕ МЕНЮ, СМЕНА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

6.1. 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]  Boot password
[3]  Password Recovery Procedure
[4]  Image menu
[5]  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 368 – Описание меню Startup

№	*Название*	*Описание*
<1>	**Restore Factory Defaults** Восстановление заводских настроек	Данная процедура используется для удаления конфигурации устройства. Восстановление конфигурации по умолчанию.
<2>	**Boot password** Установка / удаление пароля на начальный загрузчик	Данная процедура используется для установки/удаления пароля на **начальный загрузчик.**

<3>	**Password Recovery Procedure**
	Восстановление пароля
		Данная процедура используется для восстановления утраченного пароля, она позволяет подключиться к устройству без пароля.
		Для восстановления пароля нажать клавишу **<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 ====`

<4>	**Image menu** Выбор активного файла системного ПО	Данная процедура используется для выбора активного **файла системного ПО.** Если не выбран новый загруженный файл системного ПО активным, то устройство выполнит загрузку с использованием текущего активного образа Image menu [1] Show current image – просмотр данных о версиях ПО на устройстве [2] Set current image – выбор активного **файла системного ПО** [3] Back
<5>	**Back** Выход из меню	Для выхода из меню и загрузки устройства нажмите клавишу **<Enter>**, либо **<Esc>**.

6.2. Обновление программного обеспечения с сервера TFTP

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

Обновление программного обеспечения может осуществляться только привилегированным пользователем.

6.2.1. Обновление системного программного обеспечения

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

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/Rustel-XXX.ros
  Version: 4.0.3
  Commit: 25503143
  MD5 Digest: 6f3757fab5b6ae3d20418e4d20a68c4c
  Date: 03-Jun-2016
  Time: 19:54:26
Inactive-image: flash://system/images/Rustel-XXX.ros
  Version: 4.0.4
  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/Rustel-XXX.ros
```

```
26-Feb-2016 11:07:54 %COPY-I-FILECPY: Files Copy - source URL
tftp://10.10.10.1/ Rustel-XXX.ros destination URL flash://
system/images/RTT-XXX.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/Rustel-XXX.ros
  Version: X.X.X
  MD5 Digest: 0534f43d80df854179f5b2b9007ca886
  Date: XX-Xxx-20XX
  Time: 17:17:31
  Inactive-image: flash://system/images/Rustel-XXX.ros
  Version: X.X.X
  MD5 Digest: b66fd2211e4ff7790308bafa45d92572
  Date: XX-Xxx-20XX
  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.

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 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
```

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, добавить привязку групп:

```
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
```

Пример настройки для порта в режиме customer

Данный тип подключения может быть использован для того, чтобы помечать пользовательские IGMP-report'ы определенных VLAN (CVLAN) отдельными внешними метками (SVLAN).

1. Включить фильтрацию многоадресных данных:

```
console(config)# bridge multicast filtering
```

2. Настроить VLAN пользователей (VID 100), multicast-tv VLAN (VID 1000, 1001), VLAN управления (VID 1200):

```
console(config)# vlan database
console(config-vlan)# vlan 100,1000-1001,1200
console(config-vlan)# exit
```

3. Настроить порт пользователя:

```
console(config)# interface te1/0/1
console(config-if)# switchport mode customer
console(config-if)# switchport customer vlan 100
console(config-if)# switchport customer multicast-tv vlan add 1000,1001
console(config-if)# exit
```

4. Настроить uplink-порт, разрешив передачу многоадресного трафика, трафика пользователей и управление:

```
console(config)# interface te1/0/10
console(config-if)# switchport mode trunk
console(config-if)# switchport trunk allowed vlan add 100,1000-1001,1200
console(config-if)# exit
```

5. Настроить IGMP snooping глобально и на интерфейсах, добавить правила маркировки пользовательских IGMP-report'ов:

```
console(config)# ip igmp snooping
console(config)# ip igmp snooping vlan 100
console(config)# ip igmp snooping map cpe vlan 5 multicast-tv vlan 1000
console(config)# ip igmp snooping map cpe vlan 6 multicast-tv vlan 1001
```

6. Настроить интерфейс управления:

```
console(config)# interface vlan 1200
console(config-if)# ip address 192.168.33.100 255.255.255.0
console(config-if)# exit
```

ПРИЛОЖЕНИЕ Б. КОНСОЛЬНЫЙ КАБЕЛЬ

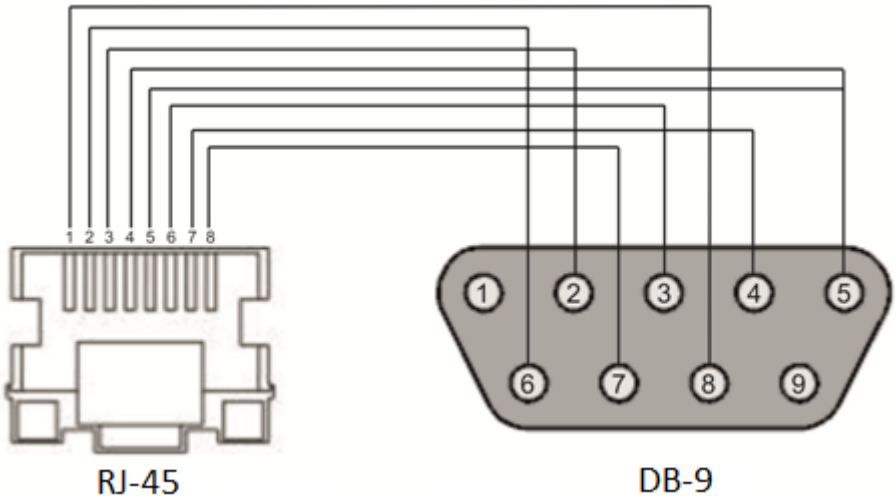


Рисунок Б.1 – Подключение консольного кабеля

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, PPPoE Intermediate Agent
BRMN	Bridge Management: EAPS, STP, операции с FDB (добавление, удаление записей), зеркалирование, конфигурация портов/VLAN, GVRP, GARP, LLDP, IGMP Snooping, IP multicast, OAM
BSNC	Автомат синхронизации ведущего и ведомого устройств в стеке
BTPC	Клиент BOOTP
CDB_	Копирование конфигурационных файлов
CEAU	Очистка очереди событий Address Update
CFM	Реализация Ethernet CFM
CNLD	Загрузка/выгрузка конфигурации
COPY	Управление копированием файлов
CPUM	Мониторинг загрузки CPU
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)
FHSS	Приложения IPv6 First Hop Security
FLNK	Flex Link
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
IP6L	Приём и отправка IPv6-пакетов
IP6M	Маршрутизация IPv4 и IPv6
IP6R	Приём и отправка IPv6-пакетов
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)
LACP	Менеджер LAG и LACP
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)
MEMV	Мониторинг утилизации оперативной памяти
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
SNPR	SNMP Proxy
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
STSF	CLI-сессия через VLAN
STUT	Мониторинг утилизации флеш-памяти
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
UNQt	Обработка платформозависимых событий
URGN	Обработка критических событий (например, перезагрузки)
UTST	Подсистема юнит-тестов
VPCB	VPC (работа с MAC-таблицей)
VPCM	VPC (основной процесс)
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

ПРИЛОЖЕНИЕ Д. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Версия документа	Дата выпуска	Содержание изменений
Версия 1.48	27.06.2025	Синхронизация с версией 4.0.25
Версия 1.47	07.05.2025	Синхронизация с версией 4.0.24.5
Версия 1.46	19.02.2025	Синхронизация с версией 4.0.24.1 Изменения в разделах: 4.4 Режим работы коммутатора 5.7.2 Команды для работы с файлами 5.8 Настройка системного времени 5.13.2 Протокол агрегации каналов LACP 5.21.1 Механизм AAA 5.21.3 Протокол TACACS+ 5.28.2.1 Базовая проверка подлинности 5.28.2.2 Расширенная проверка подлинности 5.28.4 Контроль протокола DHCP и опция 82 5.29.1 Функции DHCP Relay для IPv4 5.34.1 Настройка QoS 5.35.1 Конфигурация статической маршрутизации 5.35.3 Настройка протокола OSPF, OSPFv3 5.35.4 Настройка протокола BGP (Border Gateway Protocol) 5.35.5 Настройка протокола IS-IS 5.35.13 Конфигурация виртуальной области маршрутизации (VRF lite)
Версия 1.45	03.12.2024	Синхронизация с версией 4.0.23.6 Изменения в разделах: 5.7.1 Описание аргументов команд 5.7.3 Команды для резервирования конфигурации 5.10.1 Параметры Ethernet-интерфейсов, Port-Channel- и Loopback-интерфейсов 6.2.1 Обновление системного программного обеспечения
Версия 1.44	07.10.2024	Синхронизация с версией 4.0.23.5 Изменения в разделах: 5.17.5.2 Настройка протокола MSTP
Версия 1.43	12.08.2024	Синхронизация с версией 4.0.23.1 Изменения в разделах: 2.4 Конструктивное исполнение 4.4 Режим работы коммутатора 5.6 Команды для настройки параметров для задания паролей 5.7.1 Описание аргументов команд 5.8 Настройка системного времени 5.17.5.1 Настройка протокола STP, RSTP 5.18 Voice VLAN 5.21.4 Протокол управления сетью (SNMP) 5.22 Журнал аварий, протокол SYSLOG 5.23 Зеркалирование (мониторинг) портов 5.28.2.1 Базовая проверка подлинности 5.28.2.2 Расширенная проверка подлинности 5.28.7 Функционал First Hop Security

		5.29 Функции DHCP Relay-посредника 5.35.3 Настройка протокола OSPF, OSPFv3 5.35.4 Настройка протокола BGP (Border Gateway Protocol)
Версия 1.42	04.06.2024	Синхронизация с версией ПО 4.0.22.7 Изменения в разделах: 5.13 Группы агрегации каналов — Link Aggregation Group (LAG) 5.17.7 Настройка протокола LLDP 5.23 Зеркалирование (мониторинг) портов 5.33 Конфигурация защиты от DoS-атак 5.35.4 Настройка протокола BGP (Border Gateway Protocol)
Версия 1.41	07.03.2024	Синхронизация с версией ПО 4.0.22
Версия 1.40	19.12.2023	Синхронизация с версией ПО 4.0.21.7
Версия 1.39	20.10.2023	Синхронизация с версией ПО 4.0.21.5 Изменения в разделах: 2.3 Основные технические характеристики 5.19.1 Функция посредника протокола IGMP (IGMP Snooping) 5.21.1 Механизм AAA 5.29.1 Функции DHCP Relay для IPv4 5.32 Конфигурация ACL (списки контроля доступа) 5.35.10 Настройка Virtual Router Redundancy Protocol (VRRP) 5.35.13 Конфигурация виртуальной области маршрутизации (VRF lite)
Версия 1.38	09.08.2023	Синхронизация с версией ПО 4.0.21 Изменения в разделах: 2.3 Основные технические характеристики 5.5 Команды управления системой 5.8 Настройка системного времени 5.21.2 Протокол RADIUS 5.28.2.3 Настройка активного сеанса клиента (CoA) 5.33 Конфигурация защиты от DoS-атак 5.35.4 Настройка протокола BGP (Border Gateway Protocol) 5.35.6 Настройка Route-Map
Версия 1.37	28.04.2023	Синхронизация с версией ПО 4.0.20 Изменения в разделах: 5.7.1 Описание аргументов команд 5.10.2 Настройка VLAN и режимов коммутации интерфейсов 5.17.5 Семейство протоколов STP (STP, RSTP, MSTP), PVSTP+, RPVSTP+ 5.28.1 Функции обеспечения защиты портов 5.35.3 Настройка протокола OSPF, OSPFv3 5.35.4 Настройка протокола BGP (Border Gateway Protocol) 5.35.5 Настройка протокола IS-IS
Версия 1.36	23.01.2023	Синхронизация с версией ПО 4.0.19 Изменения в разделах: 4.4 Режим работы коммутатора

		5.10.1 Параметры Ethernet-интерфейсов, Port-Channel- и Loopback-интерфейсов 5.10.2 Настройка VLAN и режимов коммутации интерфейсов 5.16.1 Протокол IPv6 5.17.5.1 Настройка протокола STP, RSTP 5.18 Voice VLAN 5.19.1 Функция посредника протокола IGMP (IGMP Snooping) 5.20.1 Протокол PIM 5.20.4 Функция IGMP Proxy 5.21.2 Протокол RADIUS 5.21.4 Протокол управления сетью (SNMP) 5.23 Зеркалирование (мониторинг) портов 5.28.1 Функции обеспечения защиты портов 5.28.2.2 Расширенная проверка подлинности 5.34.1 Настройка QoS 5.35.1 Конфигурация статической маршрутизации 5.35.10 Настройка Virtual Router Redundancy Protocol (VRRP)
Версия 1.35	16.12.2022	Синхронизация с версией ПО 4.0.18.4
Версия 1.34	29.11.2022	Синхронизация с версией ПО 4.0.18.2 Изменения в разделах: 5.7.3 Команды для резервирования конфигурации 5.10.1 Параметры Ethernet-интерфейсов, Port-Channel- и Loopback-интерфейсов 5.17.2 Настройка протокола ARP 5.17.8 Настройка протокола OAM 5.17.5 Семейство протоколов STP (STP, RSTP, MSTP), PVSTP+, RPVSTP+ 5.17.5.3 Настройка протоколов PVSTP+, RPVSTP+ 5.21.4 Протокол управления сетью (SNMP) 5.34.1 Настройка QoS
Версия документа 1.33	29.07.2022	Синхронизация с версией ПО 4.0.18 Добавлены разделы: 5.35.13 Конфигурация виртуальной области маршрутизации (VRF) Изменения в разделах: 5.5 Команды управления системой 5.7.2 Команды для работы с файлами 5.10.1 Параметры Ethernet-интерфейсов, Port-Channel- и Loopback-интерфейсов 5.14 Настройка IPv4-адресации 5.17.5 Семейство протоколов STP (STP, RSTP, MSTP), PVSTP+, RPVSTP+ 5.21.7 Настройка доступа 5.23 Зеркалирование (мониторинг) портов 5.28.5 Защита IP-адреса клиента (IP source Guard) 5.29.1 Функции DHCP Relay для IPv4 5.34.1 Настройка QoS 5.35.1 Конфигурация статической маршрутизации 5.35.3 Настройка протокола OSPF, OSPFv3 5.35.4 Настройка протокола BGP (Border Gateway Protocol)

Версия документа 1.32	27.06.2022	Синхронизация с версией ПО 4.0.17 Изменения в разделах: 2.3 Основные технические характеристики 4.4 Режим работы коммутатора 5.10.2 Настройка VLAN и режимов коммутации интерфейсов 5.11 Selective Q-in-Q 5.13 Группы агрегации каналов — Link Aggregation Group (LAG) 5.17.7 Настройка протокола LLDP 5.19.1 Функция посредника протокола IGMP (IGMP Snooping) 5.19.5 RADIUS-авторизация запросов IGMP 5.21.2 Протокол RADIUS 5.32.1 Конфигурация ACL на базе IPv4 5.32.3 Конфигурация ACL на базе MAC 5.35.3 Настройка протокола OSPF, OSPFv3
Версия документа 1.31	01.04.2022	Синхронизация с версией ПО 4.0.16.14
Версия документа 1.30	28.02.2022	Синхронизация с версией ПО 4.0.16.13
Версия документа 1.29	12.01.2022	Изменения в разделах: 5.18 Voice VLAN 5.25.3 Диагностика индикации интерфейсов 5.32.1 Конфигурация ACL на базе IPv4 5.32.2 Конфигурация ACL на базе IPv6 5.32.3 Конфигурация ACL на базе MAC
Версия документа 1.28	12.11.2021	Изменения в разделах: 2.3 Основные технические характеристики 5.35.3 Настройка протокола OSPF, OSPFv3 5.35.4 Настройка протокола BGP (Border Gateway Protocol)
Версия документа 1.27	12.10.2021	Изменения в разделах: 2.3 Основные технические характеристики 5.19.2 Правила групповой адресации (multicast addressing) 5.23 Зеркалирование (мониторинг) портов
Версия документа 1.26	30.07.2021	Изменения в разделах: 4.4 Режим работы коммутатора 5.5 Команды управления системой 5.8 Настройка системного времени 5.17.5 Семейство протоколов STP (STP, RSTP, MSTP), PVSTP+, RPVSTP+ 5.22 Журнал аварий, протокол SYSLOG 5.31 Конфигурация DHCP-сервера 5.35.4 Настройка протокола BGP (Border Gateway Protocol) 5.35.6 Настройка Route-Map
Версия документа 1.25	30.04.2021	Добавлены разделы: 5.25.3 Диагностика индикации интерфейсов Изменения в разделах: 2.3 Основные технические характеристики 4.4 Режим работы коммутатора 5.10.4 Настройка интерфейса IP 5.11 Selective Q-in-Q 5.12 Storm Control для различного трафика (broadcast, multicast, unknown unicast)

		5.13.3 Настройка технологии Multi-Switch Link Aggregation Group (MLAG) 5.18 Voice VLAN 5.21.1 Механизм AAA 5.28.6 Контроль протокола ARP (ARP Inspection) 5.28.2 Проверка подлинности клиента на основе порта (стандарт 802.1x) 5.28.3 Настройка функции MAC Address Notification 5.33 Конфигурация защиты от DoS-атак 5.34.1 Настройка QoS
Версия документа 1.24	02.03.2021	Синхронизация с версией ПО 4.0.15.3
Версия документа 1.23 Версия ПО 4.0.15.2	10.02.2021	Изменения в разделах: 2.2.3 Функции второго уровня сетевой модели OSI 2.4.4 Световая индикация 4.5.1 Базовая настройка коммутатора 4.5.2 Настройка параметров системы безопасности 5.5 Команды управления системой 5.12 Storm Control для различного трафика (broadcast, multicast, unknown unicast)
Версия документа 1.22 Версия ПО 4.0.15.1	24.12.2020	Добавлены разделы: 5.35.12 Протокол GRE Изменения в разделах: 5.7.4 Команды для автоматического обновления и конфигурации 5.10.2 Настройка VLAN и режимов коммутации интерфейсов 5.10.3 Настройка Private VLAN 5.13.3 Настройка технологии Multi-Switch Link Aggregation Group (MLAG) 5.17.1 Настройка протокола DNS — системы доменных имен 5.21.3 Протокол TACACS+ 5.28.4 Контроль протокола DHCP и опция 82 5.33 Конфигурация защиты от DoS-атак 5.34.1 Настройка QoS Приложение Г. Описание процессов коммутатора
Версия документа 1.21 Версия ПО 4.0.14.3	27.10.2020	Изменения в разделах: 2.5 Комплект поставки 5.7.2 Команды для работы с файлами 5.33 Конфигурация защиты от DoS-атак
Версия документа 1.20 Версия ПО 4.0.14.2	16.10.2020	Изменения в разделах: 2.3 Основные технические характеристики 5.20.4 Функция IGMP Proxy 5.17.4 Механизм обнаружения петель (loopback-detection)
Версия документа 1.19 Версия ПО 4.0.14.1	14.09.2020	5.1 Базовые команды 5.10.1 Параметры Ethernet-интерфейсов, Port-Channel и Loopback- интерфейсов 5.17.11 Настройка функции Layer 2 Protocol Tunneling (L2PT) 5.21.4 Протокол управления сетью (SNMP) 5.28.1 Функции обеспечения защиты портов 5.28.5 Защита IP-адреса клиента (IP source Guard)
Версия документа 1.18	01.09.2020	Добавлены разделы:

Версия ПО 4.0.14.0		5.26 IP Service Level Agreements (IP SLA) 5.28.2.3 Настройка активного сеанса клиента (CoA) 5.35.5 Настройка протокола IS-IS 5.35.8 Настройка связки ключей Изменения в разделах: 2.3 Основные технические характеристики 2.4.4 Световая индикация 2.5 Комплект поставки 5.7.2 Команды для работы с файлами 5.10 Конфигурация интерфейсов и VLAN 5.10.1 Параметры Ethernet-интерфейсов, Port-Channel и Loopback- интерфейсов 5.19.1 Функция посредника протокола IGMP (IGMP Snooping) 5.20.4 Функция IGMP Proxy 5.21.1 Механизм AAA 5.27 Электропитание по линиям Ethernet (PoE) 5.28.1 Функции обеспечения защиты портов 5.28.4 Контроль протокола DHCP и опция 82 5.32 Конфигурация ACL (списки контроля доступа) 5.34 Качество обслуживания – QoS 5.35.2 Настройка протокола RIP 5.35.3 Настройка протокола OSPF, OSPFv3 5.35.4 Настройка протокола BGP (Border Gateway Protocol)
Версия 1.17 Версия ПО 4.0.13.3	23.01.2020	Изменения в разделах: 5.10.1 Параметры Ethernet-интерфейсов, Port-Channel и Loopback- интерфейсов 5.10.2 Настройка VLAN и режимов коммутации интерфейсов 5.17.5 Семейство протоколов STP (STP, RSTP, MSTP), PVSTP+, RPVSTP+ 5.19.1 Функция посредника протокола IGMP (IGMP Snooping) 5.19.3 MLD snooping – протокол контроля многоадресного трафика в IPv6 5.28.4 Контроль протокола DHCP и опция 82
Версия 1.16	22.10.2019	Добавлены разделы: 4.5.1.2 Расширенная настройка уровня доступа 5.13.3 Настройка технологии Multi-Switch Link Aggregation Group (MLAG) 5.21.7.3 Удаленный запуск команд посредством SSH 5.28.7 Функционал First Hop Security 5.35.11 Настройка протокола Bidirectional Forwarding Detection (BFD) Изменения в разделах: 5.7.2 Команды для работы с файлами 5.10.1 Параметры Ethernet-интерфейсов, Port-Channel и Loopback- интерфейсов 5.10.2 Настройка VLAN и режимов коммутации интерфейсов 5.17.5 Семейство протоколов STP (STP, RSTP, MSTP), PVSTP+, RPVSTP+

		5.17.5.3 Настройка протоколов PVSTP+, RPVSTP+ 5.27 Электропитание по линиям Ethernet (PoE) 5.28.2.2 Расширенная проверка подлинности 5.29.2 Функции DHCP Relay для IPv6 и Lightweight DHCPv6 Relay Agent (LDRA) 5.35.3 Настройка протокола OSPF, OSPFv3 5.35.4 Настройка протокола BGP (Border Gateway Protocol) 5.35.5 Настройка протокола IS-IS
Версия 1.15	16.09.2019	Добавлены разделы: 5.29.1 Функции DHCP Relay для IPv4 5.29.2 Функции DHCP Relay для IPv6 и Lightweight DHCPv6 Relay Agent (LDRA) Изменения в разделах: 2.3 Основные технические характеристики 2.5 Комплект поставки 4.5.1 Базовая настройка коммутатора 5.10 Конфигурация интерфейсов и VLAN 5.22 Журнал аварий, протокол SYSLOG 5.28.2.3 Настройка активного сеанса клиента (CoA) 5.32 Конфигурация ACL (списки контроля доступа)
Версия 1.14 Версия ПО 4.0.12	27.05.2019	Добавлены разделы: 5.17.10 Настройка функции Flex-link 5.19.5 RADIUS авторизация запросов IGMP 5.20.2 Функция PIM Snooping 5.20.3 Протокол MSDP 5.35.5 Настройка протокола IS-IS 5.35.7 Настройка Prefix-List Изменения в разделах: 2.2.4 Функции третьего уровня сетевой модели OSI 2.3 Основные технические характеристики 5.10 Конфигурация интерфейсов и VLAN 5.14 Настройка IPv4-адресации 5.19.4 Функции ограничения multicast-трафика 5.20.1 Протокол PIM 5.20.4 Функция IGMP Proxy 5.21.4 Протокол управления сетью (SNMP) 5.28.4 Контроль протокола DHCP и опция 82 5.32.1 Конфигурация ACL на базе IPv4 5.35 Конфигурация протоколов маршрутизации 5.35.4 Настройка протокола BGP (Border Gateway Protocol) 5.35.10 Настройка Virtual Router Redundancy Protocol (VRRP)
Версия 1.13 Версия ПО 4.0.11	05.02.2019	Изменения в разделах: 2.2.4 Функции третьего уровня сетевой модели OSI 4.4 Режим работы коммутатора 5.17.3 Настройка протокола GVRP 5.21.7.1 Telnet, SSH, HTTP и FTP 5.25.2 Диагностика оптического трансивера 5.27.2.2 Расширенная настройка подлинности 5.27.3 Контроль протокола DHCP и опции 82 5.28 Функции DHCP-Relay посредника 5.5 Команды управления системой Увеличено количество Port-Channel до 48

		Добавлены разделы: 5.17.9 Настройка протокола CFM (Connectivity Fault Management) 5.34.4 Настройка протокола BGP (Border Gateway Protocol)
Версия 1.12	01.11.2018	Изменения в разделах: 2.3 Основные технические характеристики 5.17.4 Механизм обнаружения петель (loopback-detection) 5.5 Команды управления системой 5.19.2 Правила групповой адресации (multicast addressing)
Версия 1.11	28.09.2018	Добавлен раздел: 5.17.5.3 Настройка протокола PVST+ Изменения в разделах: 2.4.1 Внешний вид и описание передней панели устройства. 4.4 Режим работы коммутатора 5.5 Команды управления системой 5.17.3 Настройка протокола GVRP 5.19.1 Функция посредника протокола IGMP (IGMP Snooping) 5.19.2 Правила групповой адресации (multicast addressing) 5.25.2 Диагностика оптического трансивера 5.25.1 Диагностика медного кабеля 5.21.2 Протокол RADIUS 5.26 Электропитание по линиям Ethernet (PoE) 5.27.1 Функция обеспечения защиты портов 5.30 Конфигурация DHCP-сервера 5.4 Настройка макрокоманд
Версия 1.10	28.06.2018	Изменения в разделах 5.13 Группы агрегации каналов – Link Aggregation Group (LAG)
Версия 1.9 Версия ПО 4.0.9	28.05.2018	Добавлены разделы: 5.3 Перенаправление вывода команд CLI в произвольный файл на ПЗУ 5.34.5 Настройка Equal-cost multi-path (ECMP) Изменения в разделах: 2.3 Основные технические характеристики 5.7.4 Команды для автоматического обновления и конфигурации 5.10.1 Параметры Ethernet-интерфейсов, Port-Channel и Loopback-интерфейсов 5.13 Группы агрегации каналов Large Aggregation Group 5.14 Настройка IPv4 адресации 5.17.1 Настройка протокола DNS – системы доменных имен 5.17.9 Настройка функции Layer 2 Protocol Tunneling (L2PT) 5.19.5 Функция многоадресной маршрутизации IGMP Proxy 5.20 Многоадресная маршрутизация – протокол PIM 5.30 Конфигурация DHCP-сервера 5.34.3 Настройка протокола OSPF, OSPFv3 ПРИЛОЖЕНИЕ А. ПРИМЕРЫ ПРИМЕНЕНИЯ И КОНФИГУРАЦИИ УСТРОЙСТВА

		ПРИЛОЖЕНИЕ Г. ОПИСАНИЕ ПРОЦЕССОВ КОММУТАТОРА
Версия 1.8 Версия ПО 4.0.8	12.12.2017	Изменения в разделах: 2.3 Основные технические характеристики 2.4 Конструктивное исполнение 2.4.4 Световая индикация 5.4 Команды управления системой 5.9.1 Параметры Ethernet-интерфейсов, Port-Channel и Loopback-интерфейсов 5.9.2 Настройка VLAN и режимов коммутации интерфейсов 5.16.7 Настройка протокола LLDP 5.18.1 Функция посредника протокола IGMP (IGMP Snooping) 5.20.4 Протокол управления сетью (SNMP) 5.20.6 Списки доступа ACL для управления устройством 5.24.2 Диагностика оптического трансивера 6.2 Журнал аварий, протокол Syslog. 6.9 Конфигурация PPPoE Intermediate Agent
Версия 1.7 Версия ПО 4.0.7	18.09.2017	Добавлены разделы: 5.9.3 Настройка Private VLAN Изменения в разделах: 2.3 Основные технические характеристики 5.4 Команды управления системой 5.9.2 Настройка VLAN и режимов коммутации интерфейсов 5.16.4 Механизм обнаружения петель (Loopback-detection) 5.18 Групповая адресация 5.20.6 Списки доступа ACL для управления устройством 5.20.2 Протокол RADIUS 5.20.4 Протокол управления сетью (SNMP) 5.21 Журнал аварий, протокол SYSLOG 5.26.3 Контроль протокола DHCP и опция 82 5.28 Конфигурация PPPoE Intermediate Agent 5.32.1 Настройка QoS
Версия 1.6 Версия ПО 4.0.6	25.05.2017	Добавлены разделы: 5.16.9 Настройка функции Layer 2 Protocol Tunneling (L2PT) Изменения в разделах: 2.2.4 Функции третьего уровня сетевой модели OSI 5.9 Конфигурация интерфейсов и VLAN 5.12 Группы агрегации каналов – Link Aggregation Group (LAG) 5.16.4 Механизм обнаружения петель (Loopback-detection) 5.16.6 Настройка протокола G.8032v2 (ERPS) 5.20.4 Протокол управления сетью (SNMP) 5.20.7.1 Telnet, SSH, HTTP и FTP 5.26.1 Функции обеспечения защиты портов 5.27 Функции DHCP Relay посредника 5.28 Конфигурация PPPoE Intermediate Agent 5.30.3 Конфигурация ACL на базе MAC 5.32.1 Настройка QoS 5.33.3 Настройка протокола OSPF, OSPFv3
Версия 1.5	23.03.2017	Добавлены разделы:

Версия ПО 4.0.5		5.6.3 Команды для резервирования конфигурации 5.26.6 Настройка функции MAC Address Notification ПРИЛОЖЕНИЕ Г ОПИСАНИЕ ПРОЦЕССОВ КОММУТАТОРА Изменения в разделах: 4.3 Загрузочное меню 5.4 Команды управления системой 5.6.2 Команды для работы с файлами 5.9 Конфигурация интерфейсов 5.18.2 Функция посредника протокола IGMP (IGMP Snooping) 5.16.2 Настройка протокола ARP 5.16.5.1 Настройка протокола STP, RSTP 5.20.1 Механизм AAA 5.26.3 Контроль протокола DHCP и опция 82 6.1 Меню Startup
Версия 1.4 Версия ПО 4.0.4	09.09.2016	Добавлены разделы: 5.8 Конфигурация временных интервалов time-range 5.15.8 Настройка протокола OAM 5.17.4 Функции ограничения multicast-трафика 5.24 Электропитание по линиям Ethernet (PoE) 5.27 Конфигурация PPPoE Intermediate Agent Изменения в разделах: 2.3 Основные технологические характеристики 5.4 Команды управления системой 5.7 Настройка системного времени 5.8 Конфигурация интерфейсов 5.12 Настройка IPv4-адресации 5.15.5 Семейство протоколов STP (STP, RSTP, MSTP) 5.17.1 Правила групповой адресации (multicast addressing) 5.17.2 Функция посредника протокола IGMP (IGMP Snooping) 5.19.1 Механизм AAA 5.19.2 Протокол RADIUS 5.19.4 Протокол TACACS+ 5.19.5 Протокол управления сетью (SNMP)
Версия 1.3	22.07.2016	Добавлены разделы: 5.15.6 Настройка протокола G.8032v2 (ERPS) Изменения в разделах: 2.2.3 Функции второго уровня сетевой модели OSI 5.4 Команды управления системой 5.8.2 Настройка интерфейса VLAN 5.19.1 Механизм AAA 5.19.8.1 Telnet, SSH, HTTP и FTP 5.20 Журнал аварий, протокол SYSLOG 5.27 Конфигурация ACL (списки контроля доступа)
Версия 1.2	25.05.2016	Добавлены разделы: 2.3 Основные технологические характеристики
Версия 1.1 Версия ПО 4.0.2	12.05.2016	Добавлены разделы: 2.3 Основные технологические характеристики
Версия 1.0	25.03.2016	Первая публикация

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения технической консультации по вопросам эксплуатации программного обеспечения ООО «Русьтелетех» можно обращаться в Сервисный центр компании:

Российская Федерация,115419, г. Москва, ул. Орджоникидзе, дом 11, стр. 40.

Телефон: +7(495) 234-9777

E-mail: support@rusteletech.ru

Официальный сайт компании: rusteletech.ru