Коммутатор Ethernet

MES2318U

Руководство по эксплуатации, версия ПО 10.3.3.1

Версия документа	Дата выпуска	Содержание изменений
Версия 1.0	09.2023	Синхронизация с версией ПО 10.3.3.1
Версия программного обеспечения 10.3.3.1		

СОДЕРЖАНИЕ

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

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

ПРИМЕЧАНИЯ И ПРЕДУПРЕЖДЕНИЯ

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

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

ВВЕДЕНИЕ

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

Для достижения высоких скоростей широко применяются технологии передачи информации Gigabit Ethernet (GE). Передача информации на высоких скоростях, особенно в сетях крупного масштаба, подразумевает выбор такой топологии сети, которая позволяет гибко осуществлять распределение высокоскоростных потоков.

Коммутатор MES2318U может использоваться на сетях крупных предприятий и предприятий малого и среднего бизнеса (SMB), в операторских сетях. Он обеспечивает высокую производительность, гибкость, безопасность, многоуровневое качество обслуживания (QoS).

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

1 ОПИСАНИЕ ИЗДЕЛИЯ

1.1 Назначение

Устройство MES2318U является управляемым коммутатором, выполняющим свои коммутационные функции на канальном и сетевом уровнях модели OSI.

Сетевые коммутаторы MES2318U имеют в своем составе 8 электрических портов 2,5 Gigabit Ethernet и 2 оптических порта TenGigabit Ethernet для установки SFP+-трансиверов.

1.2 Функции коммутатора

1.2.1 Базовые функции

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

Таблица 1 – Базовые функции устройства

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

1.2.2 Функции при работе с MAC-адресами

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

Таблица 2 – Функции работы с MAC-адресами

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

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

1.2.3 Функции второго уровня сетевой модели OSI

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

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

Функция IGMP Snooping	Реализация протокола IGMP позволяет на основе информации, полученной при анализе содержимого IGMP-пакетов, определить, какие устройства в сети участвуют в группах многоадресной рассылки, и адресовать трафик на соответствующие порты.
Функция MLD Snooping	Реализация протокола MLD позволяет устройству минимизировать многоадресный IPv6-трафик.
Функция MVR	Функция, позволяющая перенаправлять многоадресный трафик из одного 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. 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.
Поддержка протокола STP (Spanning Tree Protocol)	Spanning Tree Protocol – сетевой протокол, основной задачей которого является приведение сети Ethernet с избыточными соединениями к древовидной топологии, исключающей петли. Коммутаторы обмениваются конфигурационными сообщениями, используя кадры специального формата, и выборочно включают и отключают передачу на порты.
Поддержка протокола RSTP (IEEE 802.1w Rapid spanning tree protocol)	Rapid (быстрый) STP (RSTP) – является усовершенствованием протокола STP, характеризуется меньшим временем приведения сети к древовидной топологии и имеет более высокую устойчивость.
Поддержка протокола ERPS (Ethernet Ring Protection Switch)	Протокол предназначен для повышения устойчивости и надежности сети передачи данных, имеющей кольцевую топологию, за счет снижения времени восстановления сети в случае аварии. Время восстановления не превышает 1 секунды, что существенно меньше времени перестройки сети при использовании протоколов семейства spanning tree.
Поддержка VLAN	VLAN – это группа портов коммутатора, образующих одну широковещательную область (домен). Коммутатор поддерживает различные средства классификации пакетов для определения их принадлежности к определенного VLAN.

Поддержка протокола OAM (Operation, Administration and Maintenance, IEEE 802.3ah)	Ethernet OAM (Operation, Administration and Maintenance), IEEE 802.3ah – функции уровня канала передачи данных, представляющие собой протокол мониторинга состояния канала. В этом протоколе для передачи информации о состоянии канала между непосредственно подключенными устройствами Ethernet используются блоки данных протокола OAM (OAMPDU). Оба устройства должны поддерживать стандарт IEEE 802.3ah.
Поддержка VLAN на базе портов (Port-Based VLAN)	Распределение по группам VLAN выполняется по входящим портам. Данное решение позволяет использовать на каждом порту только одну группу VLAN.
Поддержка 802.1Q	IEEE 802.1Q — открытый стандарт, который описывает процедуру тегирования трафика для передачи информации о принадлежности к VLAN. Позволяет использовать несколько групп VLAN на одном порту.
Объединение каналов с использованием LACP	Протокол LACP обеспечивает автоматическое объединение отдельных связей между двумя устройствами (коммутатор–коммутатор или коммутатор–сервер) в единый канал передачи данных. В протоколе постоянно определяется возможность объединения каналов, и в случае отказа соединения, входящего в объединенный канал, его трафик автоматически перераспределяется по не отказавшим компонентам объединенного канала.
Создание групп LAG	В устройствах поддерживается функция создания групп каналов. Агрегация каналов (Link aggregation, trunking) или IEEE 802.3ad — технология объединения нескольких физических каналов в один логический. Это способствует не только увеличению пропускной способности магистральных каналов коммутатор—коммутатор или коммутатор—сервер, но и повышению их надежности. Возможны три типа балансировки – на основании MAC-адресов, на основании IP-адресов и на основании порта (socket) назначения. Группа LAG состоит из портов с одинаковой скоростью, работающих в дуплексном режиме.
Selective Q-in-Q	Позволяет назначать внешний VLAN SPVLAN (ServiceProvider's VLAN) на основе сконфигурированных правил фильтрации по номерам внутренних VLAN (Customer VLAN). Применение Selective Q-in-Q позволяет разобрать трафик абонента на несколько VLAN, изменить метку SPVLAN у пакета в отдельном участке сети.

1.2.4 Функции третьего уровня сетевой модели OSI

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

Таблица 4 – Описание функций третьего уровня (Layer 3)

Статические IP-маршруты	Администратор коммутатора имеет возможность добавлять и удалять статические записи в таблицу маршрутизации.
Клиенты BootP и DHCP (Dynamic Host Configuration Protocol)	Устройства способны автоматически получать IP-адрес по протоколу BootP/DHCP.
Протокол ARP (Address Resolution Protocol)	ARP – протокол сопоставления IP-адреса и физического адреса устройства. Соответствие устанавливается на основе анализа ответа от узла сети, адрес узла запрашивается в широковещательном пакете.
Функция IGMP proxy	IGMP Proxy — функция упрощенной маршрутизации многоадресных данных между сетями. Для управления маршрутизацией используется протокол IGMP.
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.

1.2.5 Функции QoS

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

Таблица 5 – Основные функции качества обслуживания

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

1.2.6 Функции обеспечения безопасности

Таблица 6 – Функции обеспечения безопасности

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

1.2.7 Функции управления коммутатором

Таблица 7 – Основные функции управления коммутаторами

Загрузка и выгрузка файла настройки	Параметры устройств сохраняются в файле настройки, который содержит данные конфигурации как всей системы в целом, так и определенного порта устройства.
Протокол TFTP (Trivial File Transfer Protocol)	Протокол TFTP используется для операций записи и чтения файлов. Протокол основан на транспортном протоколе UDP. Устройства поддерживают загрузку и передачу по данному протоколу файлов настройки и образов программного обеспечения.
Протокол SNMP	Протокол SNMP используется для мониторинга и управления сетевым устройством. Для управления доступом к системе определяется список записей сообщества, каждая из которых содержит привилегии доступа.

Интерфейс командной строки (CLI)	Управление коммутаторами посредством CLI осуществляется локально через последовательный порт RS-232, либо удаленно через Telnet. Интерфейс командной строки консоли (CLI) является промышленным стандартом. Интерпретатор CLI предоставляет список команд и ключевых слов для помощи пользователю и сокращению объема вводимых данных.
Syslog	*Syslog* – протокол, обеспечивающий передачу сообщений о происходящих в системе событиях, а также уведомлений об ошибках удаленным серверам.
SNTP (Simple Network Time Protocol)	Протокол *SNTP* – протокол синхронизации времени сети, гарантирует точность синхронизации времени сетевого устройства с сервером до миллисекунды.
Traceroute	*Traceroute* – служебная функция, предназначенная для определения маршрутов передачи данных в IP-сетях.
Управление контролируемым доступом – уровни привилегий	Администратор может определить уровни привилегий доступа для пользователей устройства и характеристики для каждого уровня привилегий (только для чтения – 1 уровень, полный доступ – 15 уровень).
Блокировка интерфейса управления	Коммутатор способен устанавливать запрет доступа к каждому интерфейсу управления (SNMP, CLI). Запрет может быть установлен отдельно для каждого типа доступа: • Telnet (CLI over Telnet Session); • SNMP; • SSH.
Локальная аутентификация	Для локальной аутентификации поддерживается хранение паролей в базе данных коммутатора.
Фильтрация IP-адресов для SNMP	Доступ по SNMP разрешается для определенных IP-адресов, являющихся членами SNMP-сообщества.
Функции DHCP-сервера	DHCP-сервер осуществляет централизованное управление сетевыми адресами и соответствующими конфигурационными параметрами, автоматически предоставляя их клиентам.
Клиент RADIUS	Протокол RADIUS используется для аутентификации, авторизации и учета. Сервер RADIUS использует базу данных пользователей, которая содержит данные проверки подлинности для каждого пользователя. Коммутаторы содержат клиентскую часть протокола RADIUS.
TACACS+ (Terminal Access Controller Access Control System)	Устройство предоставляет поддержку проверки подлинности клиентов посредством протокола TACACS+. Протокол TACACS+ обеспечивает централизованную систему безопасности для проверки пользователей, получающих доступ к устройству, а также централизованную систему управления при соблюдении совместимости с RADIUS и другими процессами проверки подлинности.

1.2.8 Дополнительные функции

В таблице 8 приведены дополнительные функции устройства.

Таблица 8 – Дополнительные функции устройства

Виртуальное тестирование кабеля (VCT)	Сетевые коммутаторы имеют в своём составе программные и аппаратные средства, позволяющие выполнять функции виртуального тестера кабеля – VCT. Тестер позволяет определить состояние медного кабеля связи.
Диагностика оптического трансивера	Устройство позволяет тестировать оптический трансивер. При тестировании отслеживаются такие параметры, как ток и напряжение питания, температура трансивера. Для реализации требуется поддержка этих функций в трансивере.
UDLD (Unidirectional Link Detection)	Протокол второго уровня, созданный для автоматического обнаружения потери двухсторонней коммуникации на оптических линиях связи.

Соответствие стандарту МЭК 61850	Коммутатор обладает всеми необходимыми характеристиками для работы с протоколами MMS, GOOSE, SV: • Малая величина задержки GOOSE-сообщения при передаче; • Умение распознавать Ethertype GOOSE-сообщения; • Умение работать с тегом виртуальной сети и тегом приоритета IEEE 802.1Q GOOSE-сообщения; • Поддержка передачи multicast-сообщений и возможность работы с определенным стандартом МЭК 61850 диапазоном групп вещания.

1.3 Основные технические характеристики

Основные технические параметры коммутатора приведены в таблице 9.

Таблица 9 – Основные технические характеристики

Общие параметры	
Интерфейсы	8 × 10/100/1000/2500BASE-T (PoE++) 2 × 1000BASE-X (SFP)/10GBASE-R (SFP+) 1 × Консольный порт RS-232 (RJ-45)
Пропускная способность	80 Гбит/с
Производительность на пакетах длиной 64 байта[1]	59,52 MPPS
Объем буферной памяти	1,5 Мбайт
Объем ОЗУ (DDR3)	1 Гбайт
Объем ПЗУ (SPI Flash)	64 Мбайт
Таблица MAC-адресов	16384
Количество ARP-записей	1000
Поддержка VLAN	согласно 802.1Q до 4094 активных VLAN
Количество групп L2 Multicast (IGMP snooping)	1023
Количество групп L3 Multicast (IGMP proxy)	512
Количество правил MAC-based VLAN	640[2]
Количество правил Protocol-based VLAN	8 на любое количество интерфейсов
Количество правил SQinQ	384 (ingress)/512 (egress)
Количество правил ACL	MAC – 509 IPv4/IPv6 – 384/192
Количество правил ACL в одном ACL	1
Количество маршрутов L3 IPv4 Unicast	406
Количество маршрутов L3 IPv6 Unicast	21
Количество VRRP-маршрутизаторов	32
Количество L3-интерфейсов	8 vlan, до 5 IPv4-адресов в каждом vlan, до 22 IPv6 GUA суммарно для всех vlan

[1] Значения указаны для односторонней передачи

[2] Добавление правила на каждый порт расходует аппаратные ресурсы общего пула

Количество виртуальных Loopback-интерфейсов	10
Агрегация каналов (LAG)	24 группы, до 8 портов в одном LAG
Количество экземпляров MSTP	64
Количество DHCP pool	5
Количество адресов, выдаваемых DHCP-сервером	4096
Количество статических записей DHCP-сервера	512, включая все статические записи для одного идентификатора
Качество обслуживания QoS	приоритизация трафика, 8 уровней 8 выходных очередей с разными приоритетами для каждого порта
Сверхдлинные кадры (jumboframes)	максимальный размер пакетов 12288 байт
Соответствие стандартам	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-T Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z Fiber Gigabit Ethernet IEEE 802.3x Full Duplex, Flow Control IEEE 802.3ad Link Aggregation (LACP) IEEE 802.1p Traffic Class IEEE 802.1q VLAN IEEE 802.1v IEEE 802.3 ac IEEE 802.1d Spanning Tree Protocol (STP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) IEEE 802.3af PoE, IEEE 802.3at PoE+ МЭК 61850
Управление	
Локальное управление	Console
Удаленное управление	SNMP, Telnet, SSH, Web
Физические характеристики и условия окружающей среды	
Источники питания	сеть переменного тока: 200–240 В, 50–60 Гц
Максимальная потребляемая мощность (с учетом нагрузки PoE)	810 Вт
Бюджет PoE	720 Вт
Тепловыделение	90 Вт
Аппаратная поддержка Dying Gasp	есть
Интервал рабочих температур	от -15 до +50 °С
Интервал температуры хранения	от -40 до +70 °С
Относительная влажность при эксплуатации (без образования конденсата)	не более 80 %
Относительная влажность при хранении (без образования конденсата)	от 10 % до 95 %
Габаритные размеры (Ш × В × Г)	430 x 44 x 243 мм
Масса	3,74 кг
Исполнение	19", 1U
Срок службы	не менее 15 лет

Тип питания устройства определяется при заказе.

1.4 Конструктивное исполнение

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

Ethernet-коммутатор MES2318U выполнен в металлическом корпусе с возможностью установки в 19” каркас, высота корпуса 1U.

1.4.1 Внешний вид и описание передней панели устройств

Внешний вид передней панели устройства MES2318U показан на рисунке 1.

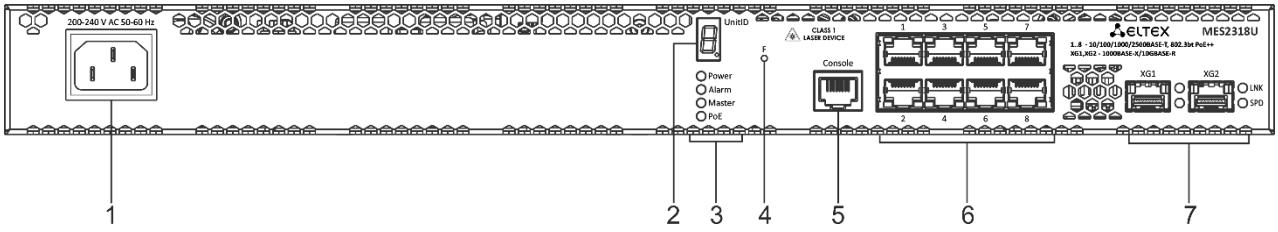

Рисунок 1 — Передняя панель MES2318U

Таблица 10 — Описание разъемов, индикаторов и органов управления передней панели коммутатора MES2318U

№	Элемент передней панели	Описание
1	200-240V AC, 50-60 Hz	Разъем для подключения к источнику электропитания переменного тока
2	UnitID	Индикатор номера устройства в стеке
3	Power	Индикатор питания устройства
	Alarm	Индикатор аварии
	Master	Индикатор режима работы устройства (ведущий/ведомый)
	PoE	Индикатор работы PoE
4	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: - при нажатии на кнопку длительностью менее 10 с происходит перезагрузка устройства; - при нажатии на кнопку длительностью более 10 с происходит сброс настроек устройства до заводской конфигурации.

5	Console	Консольный порт для локального управления устройством. Распиновка разъема следующая: 1 не используется 2 не используется 3 RX 4 GND 5 GND 6 TX 7 не используется 8 не используется 9 не используется Распайка консольного кабеля приведена в приложении А.
6	[1-8]	Порты 10/100/1000/2500BASE-T (RJ-45)
7	[XG1, XG2]	Слоты для установки трансиверов 1000BASE-X (SFP)/10GBASE-R (SFP+)

1.4.2 Задняя и верхняя панели устройств

Внешний вид задней панели коммутатора MES2318U приведен на рисунке 2.

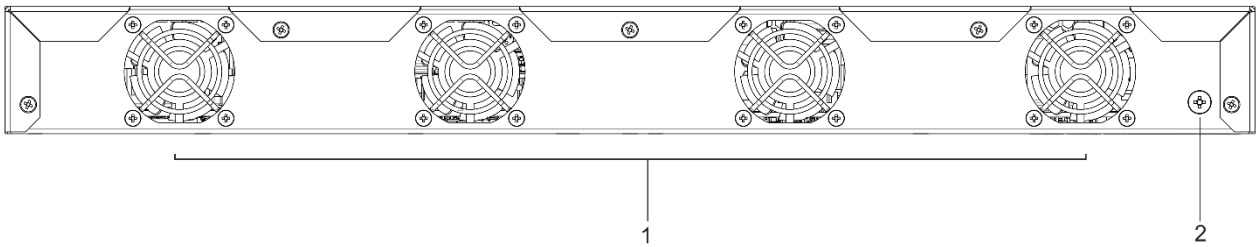

Рисунок 2 — Задняя панель MES2318U

В таблице 11 приведен перечень разъемов, расположенных на задней панели коммутатора.

Таблица 11 — Описание разъемов задней панели коммутатора MES2318U

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

1.4.3 Боковые панели устройства

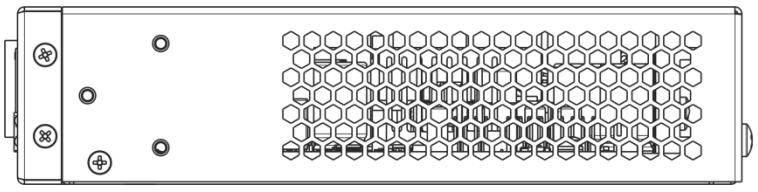

Рисунок 3 — Правая боковая панель MES2318U

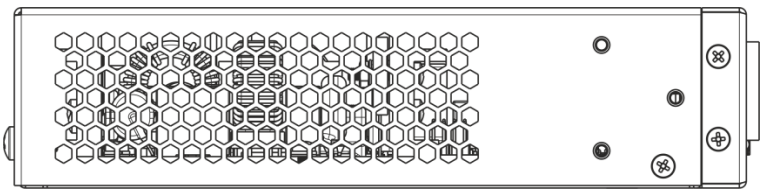

Рисунок 4 — Левая боковая панель MES2318U

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

1.4.4 Световая индикация

Состояние интерфейсов Ethernet индицируется двумя светодиодными индикаторами, *LINK/ACT* зеленого цвета и *SPEED* янтарного цвета. Расположение светодиодов показано на рисунках 5, 6.

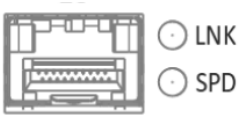

Рисунок 5 – Внешний вид одинарного разъема SFP/SFP+

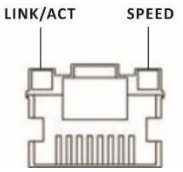

Рисунок 6 – Внешний вид разъема RJ-45

Таблица 12 — Световая индикация состояния Ethernet-портов 10/100/1000BASE-T

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

Таблица 13 — 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 1 Гбит/с.
Горит постоянно	Горит постоянно	Установлено соединение на скорости 10 Гбит/с.
X	Мигание	Идет передача данных.

Системные индикаторы (Power, Alarm) служат для определения состояния работы узлов коммутатора MES2318U.

Таблица 14 — Световая индикация системных индикаторов

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Power	Состояние источников питания	Выключен	Питание выключено.
		Зеленый, горит постоянно	Питание включено, нормальная работа устройства.
		Зеленый, мерцает	Самотестирование устройства при старте (POST).

		Красный, горит постоянно	Отсутствие первичного питания основного источника (при питании устройства от резервного источника) или авария вторичного источника.
Alarm	Состояние устройства	Не горит	Нормальная работа устройства.
		Красный, горит постоянно	Перегрев.
Master	Признак ведущего устройства при работе в стеке	Зеленый, горит постоянно	Устройство является «мастером» Стека.
		Выключен	Устройство не является «мастером» в стеке или не задан режим стекирования.
PoE	Индикатор состояния PoE-портов	Зеленый, горит постоянно	Подключен потребитель PoE (горит индикатор, соответствующий порту).
		Красный, горит постоянно	Ошибка PoE на порту.
		Выключен	Потребитель PoE не подключен.
		Выключен	Устройство не является «мастером» в стеке или не задан режим стекирования.

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

1.5 Комплект поставки

В базовый комплект поставки входят:

- Ethernet-коммутатор MES2318U;
- Комплект крепежа в стойку;
- Шнур питания Евровилка-C13, 1.8м;
- Памятка о документации;
- Сертификат/декларация соответствия;
- Паспорт.

По заказу покупателя в комплект поставки опционально могут быть включены:

- Руководство по эксплуатации на CD-диске;
- SFP/SFP+ трансиверы.

2 УСТАНОВКА И ПОДКЛЮЧЕНИЕ

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

2.1 Крепление кронштейнов

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

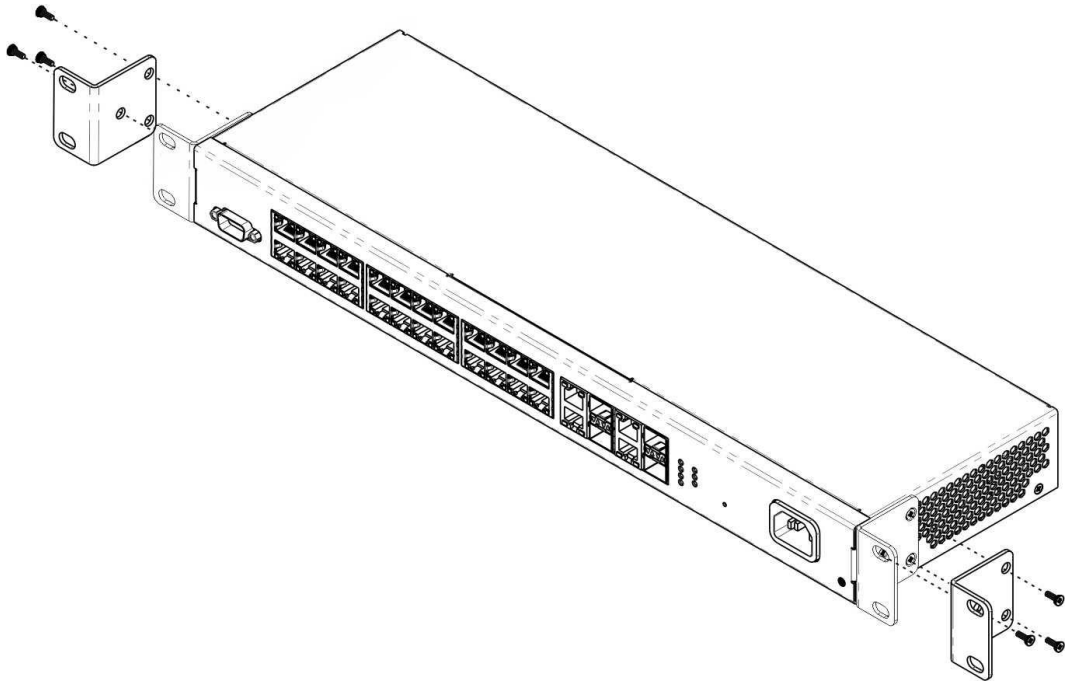

Рисунок 7 – Крепление кронштейнов

1. Совместите четыре отверстия для винтов на кронштейне с такими же отверстиями на боковой панели устройства.
2. С помощью отвертки прикрепите кронштейн винтами к корпусу.
3. Повторите действия 1, 2 для второго кронштейна.

2.2 Установка устройства в стойку

Для установки устройства в стойку:

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

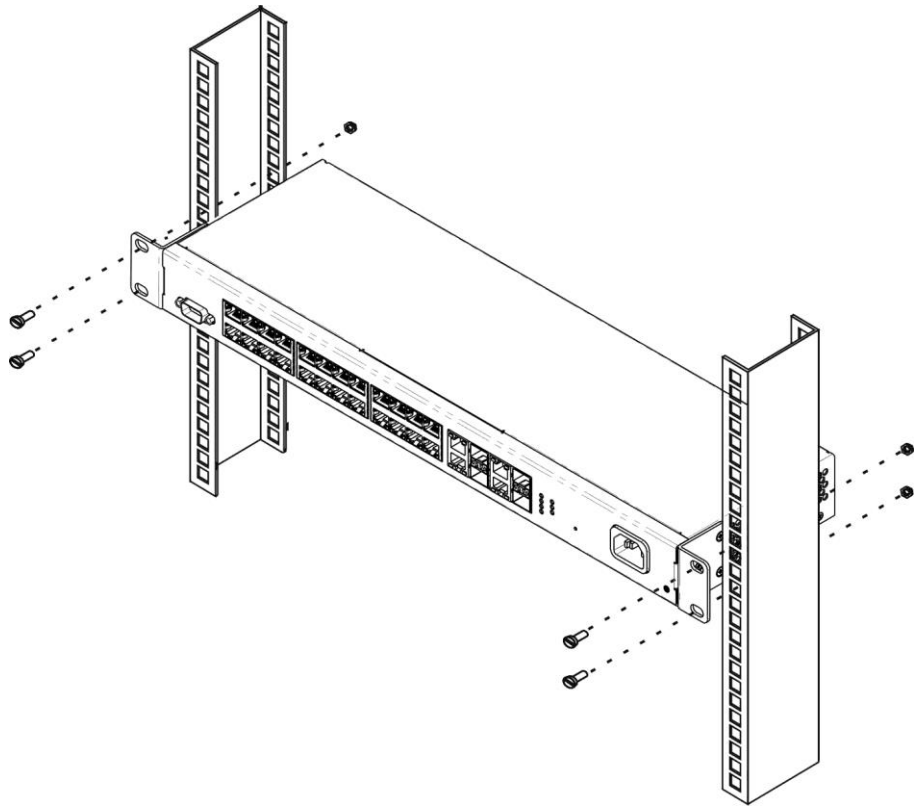

Рисунок 8 – Установка устройства в стойку

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

2.3 Подключение питающей сети

1. Прежде, чем к устройству будет подключена питающая сеть, необходимо заземлить корпус устройства. Заземление необходимо выполнять изолированным многожильным проводом. Устройство заземления и сечение заземляющего провода должны соответствовать требованиями ПУЭ.

Подключение должно осуществляться квалифицированным специалистом.

2. Если предполагается подключение компьютера или иного оборудования к консольному порту коммутатора, это оборудование также должно быть надежно заземлено.
3. Подключите к устройству кабель питания. В зависимости от комплектации устройства, питание может осуществляться от сети переменного тока, либо от сети постоянного тока. При подключении сети переменного тока следует использовать кабель, входящий в комплект устройства. Для подключения к сети постоянного тока используйте провод сечением не менее 1 мм^2.

Во избежание возникновения короткого замыкания при подключении к сети постоянного тока рекомендуется произвести зачистку провода на длину 9 мм.

Цепь питания постоянным током должна содержать устройство отключения питания с физическим разъединением соединения (выключатель, разъем, контактор, автоматический выключатель и т.п.).

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

2.4 Установка и удаление SFP-трансиверов

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

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

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

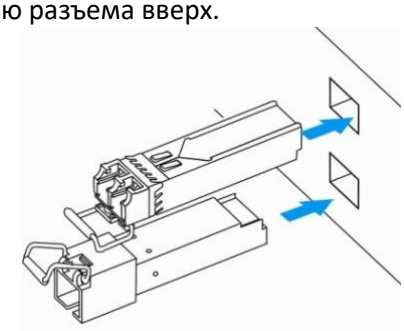

Рисунок 9 – Установка SFP-трансиверов

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

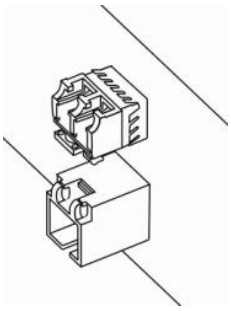

Рисунок 10 – Установленные SFP-трансиверы

Для удаления трансивера:

1. Откройте защелку модуля.

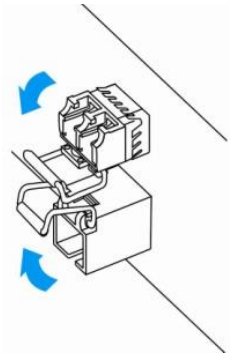

Рисунок 11 – Открытие защелки SFP-трансиверов

2. Извлеките модуль из слота.

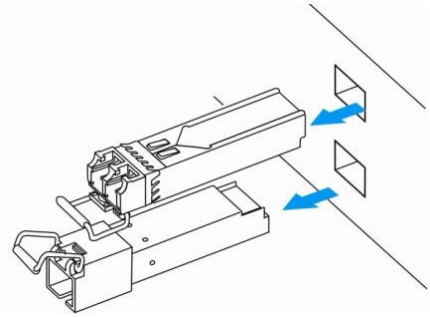

Рисунок 12 – Извлечение SFP-трансиверов

3 НАЧАЛЬНАЯ НАСТРОЙКА КОММУТАТОРА

3.1 Горячие клавиши

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

3.2 Настройка терминала

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

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

3.3 Включение устройства

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

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

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

console#
```

3.4 Загрузочное меню

Для входа в загрузочное меню следует подключиться к устройству через интерфейс RS-232, перезагрузить устройство и ввести пароль для загрузочного меню в течение 3-х секунд после появления строк:

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

CPU:500MHz LXB:200MHz MEM:300MHz
DRAM:  256 MB
SPI-F: 1x32 MB
Loading 65536B env. variables from offset 0x110000
chip_index=      23
Switch Model: MES2318U_board (Port Count: 28)
************************************************
Now External 8218B
************************************************
Now Internal PHY
************************************************
Now External 8218B
************************************************
Now External 8214FC
Net:   Net Initialization Skipped
Autobootin 3 seconds..
```

Пароль от загрузочного меню по умолчанию для всех устройств «eltex».

Вид загрузочного меню:

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

Таблица 15 — Функции интерфейса загрузочного меню

Функция	*Описание*
Restore Factory Defaults	Восстановить заводские настройки.
Boot password	Изменение пароля на загрузочное меню.
Password Pecovery Procedure	Восстановление утраченного пароля. При следующей загрузке основного ПО пользователь сразу попадет в режим Privileged EXEC без ввода пароля.
Image menu	Выбрать активный образ системного ПО. Если новый загруженный файл системного ПО не выбран активным, то устройство выполнит загрузку с использованием текущего активного образа. Image menu [1] Show current image – просмотр активного слота с образом ПО; [2] Set current image – выбор активного слота системного ПО; [3] Back.
Serial bandwidth	Выбор скорости последовательного интерфейса.

Для выхода из загрузочного меню и продолжения загрузки основного образа ПО необходимо нажать <Esc>.

Если в течение 1 минуты не выбран ни один из пунктов меню, загрузка устройства продолжится.

3.5 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 startup-config
```

3.5.1 Автоматическая настройка параметров коммутатора (Zero Touch Provisioning)

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 16 — Команды режима глобальной конфигурации

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

3.5.2 Базовая настройка коммутатора

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

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

Базовая настройка включает следующее:

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

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

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

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

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

Информация о локальных учетных записях хранится в энергонезависимой памяти и может быть очищена командой 'delete startup-config'.

Необходимо брать в кавычки имена учетных записей и пароли, содержащие спецсимволы.

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

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

IP-адрес 192.168.1.239 существует до тех пор, пока на любом интерфейсе статически или по DHCP не создан другой IP-адрес. При этом на interface vlan 1 должен быть включен dhcp-клиент.

При удалении всех IP-адресов коммутатора доступ к нему будет осуществляться по IP-адресу 192.168.1.239/24. При этом на interface vlan 1 должен быть включен dhcp-клиент.

Пример команд настройки IP-адреса для интерфейса VLAN 1

Параметры интерфейса:

IP-адрес, назначаемый для интерфейса VLAN 1 – 192.168.16.144
Маска подсети – 255.255.255.0
IP-адрес шлюза по-умолчанию – 192.168.1.1

```
console# configure terminal
console(config)# interface vlan 1
console(config-if)# ip address 192.168.16.144 255.255.255.0
```

```
console(config-if)# exit
console(config)#ip route 0.0.0.0 0.0.0.0 192.168.16.1
```

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

```
console# show ip interface
```

```
vlan1 is up, line protocol is up
Internet Address is 192.168.16.144/24
Broadcast Address  192.168.16.255
Vlan counters disabled
```

3.5.2.3 Настройка параметров протокола SNMP для доступа к устройству

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

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

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

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

3.5.3 Настройка параметров системы безопасности

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

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

При использовании настроек устройства по умолчанию имя пользователя – ***admin***, пароль – ***admin***.

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

Всегда должен существовать пользователь с уровнем привилегий 15.

3.5.3.1 Настройка доступа до серверов RADIUS и TACACS+

Для использования Radius и TACACS+ серверов необходимо выполнить следующие настройки на коммутаторе:

- Настроить IP-адрес сервера;
- Настроить ключ доступа, заданный для настраеваемого сервера (при наличии).

Пример команд для настройки RADIUS и TACACS+ серверов:

```
console# configure terminal
console(config)# radius-server host 192.168.16.3 key KEY
console(config)# tacacs-server host 192.168.16.3 key KEY
```

3.5.3.2 Настройка AAA для разных протоколов управления

Настроить список AAA по умолчанию. Список AAA по умолчанию применяется ко всем линиям (console, telnet, SSH), если для указанной линии не указано иного. В приведенном примере для линии console доступ будет осуществляться только через локальную базу данных.

Пример команд для настройки AAA:

```
console(config)# aaa authentication default radius tacacs local
console(config)# aaa authentication user-defined cons local
console(config)# line console
console(config-line)# aaa authentication login cons
console(config-line)# aaa authentication enable cons
```

4 УПРАВЛЕНИЕ УСТРОЙСТВОМ. ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ

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

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

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

```
console>
```

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

```
console#
```

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

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

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

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

4.1 Базовые команды

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 17 — Базовые команды, доступные в режиме EXEC

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

Команды режима Privileged EXEC

Запрос командной строки имеет следующий вид:

```
console#
```

Таблица 18 — Базовые команды, доступные в режиме Privileged EXEC

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

Команды, доступные во всех режимах конфигурации

Запрос командной строки имеет один из следующих видов:

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

Таблица 19 — 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	-	Вывести справку по используемым командам.

4.2 Фильтрация сообщений командной строки

Фильтрация сообщений позволяет уменьшить объем отображаемых данных в ответ на запросы пользователя и облегчить поиск необходимой информации. Для фильтрации требуется добавить в конец командной строки символ «|» и использовать одну из опций фильтрации, перечисленных в таблице 26. Фильтрация работает только для show-команд.

Команды режима Privileged EXEC

Запрос командной строки имеет следующий вид:

```
console#
```

Таблица 20 — Базовые команды, доступные в режиме Privileged EXEC

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

4.3 Настройка макрокоманд

Данная функция позволяет создавать унифицированные наборы команд – макросы, которые можно впоследствии применять в процессе конфигурации. Максимальное количество макросов – 15.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 21 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
macro name *word*	word: (1..32) символов	Создать новый набор команд, если набор с таким именем существует – перезаписать 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.
no macro name *word*		Удалить указанный макрос.
macro apply *word* [*pattern1 value1*] [*pattern2 value2*] [*pattern3 value3*]	word: (1..32) символов	Применить указанный макрос. - *pattern* – шаблон, состоящий из объявления, например символа "%", и переменной, написанных слитно; - *value* – переменная конфигурации.
macro trace *word* [*pattern1 value1*] [*pattern2 value2*] [*pattern3 value3*]	word: (1..32) символов	Отобразить процесс выполнения макроса. - *pattern* – шаблон, состоящий из объявления, например символа "%", и переменной, написанных слитно; - *value* – переменная конфигурации.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 22 — Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
macro apply *word* [*pattern1 value1*] [*pattern2 value2*] [*pattern3 value3*]	word: (1..32) символов	Применить указанный макрос. - *pattern* – шаблон, состоящий из объявления, например символа "%", и переменной, написанных слитно; - *value* – переменная конфигурации.
macro trace *word* [*pattern1 value1*] [*pattern2 value2*] [*pattern3 value3*]	word: (1..32) символов	Отобразить процесс выполнения макроса. - *pattern* – шаблон, состоящий из объявления, например символа "%", и переменной, написанных слитно; - *value* – переменная конфигурации.
show macro	-	Отобразить параметры настроенных макросов на устройстве.

Команды режима конфигурации интерфейса

Вид запроса командной строки режима конфигурации интерфейса:

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

Таблица 23 — Команды режима конфигурации интерфейса

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

Пример использования макрокоманд:

```
console(config)#macro name 1234
Enter macro commands, one per line. End with symbol '@'.
conf t
interface gi0/%1
switchport mode access
switchport access vlan %2
description %3
@
console#macro apply 1234 %1 6 %2 10 %3 "gi0/6"
```

4.4 Команды управления системой

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console>
```

Таблица 24 — Команды управления системой в режиме EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
ping [ip] {*A.B.C.D* **|** *host***} [size** *size***] [count** *count***] [timeout** *timeout***]**	host: (1..158) символов; size: (36..2080)/64 байт; count: (0..10)/3; timeout: (1..100)	Команда служит для передачи запросов (ICMP Echo-Request) протокола ICMP указанному узлу сети, а также для контроля поступающих ответов (ICMP Echo-Reply). - *A.B.C.D* – IPv4-адрес узла сети; - *host* – доменное имя узла сети; - *size* – размер пакета для отправки, количество байт в пакете; - *count* – количество пакетов для передачи; - *timeout* – время ожидания ответа на запрос.
traceroute{*A.B.C.D* **| ipv6** *AAAA::BBBB***} [size** *size***] [ttl** *ttl***] [count** *count***] [timeout** *timeout***]**	size: (64..1518)/64 байт; ttl: (1..255)/30; count: (1..10)/3; timeout: (1..60)/3 с	Определение маршрута трафика до узла назначения. - *A.B.C.D* – IPv4-адрес узла сети; - *AAAA::BBBB* – IPv6-адрес узла сети - *host* – доменное имя узла сети; - *size* – размер пакета для отправки, количество байт в пакете; - *ttl* – максимальное количество участков в маршруте; - *count* – количество попыток передачи пакета на каждом участке; - *timeout* – время ожидания ответа на запрос; **Описание ошибок при выполнении команд и результатов приведено в таблице 32.**
show users	-	Отобразить информацию о пользователях, использующих ресурсы устройства.
show system information	-	Вывод системной информации.
show nvram	-	Отобразить информацию об устройстве в энергонезависимой памяти.

show tech-support	-	Вывод команды представляет собой комбинацию выводов перечисленных ниже команд: - show clock - show system information - show bootvar - show running-config - show ip interface - show ip route - show ipv6 interface - show spanning-tree - show etherchannel summary - show etherchannel load-balance - show interfaces status - show interfaces counters - show interfaces utilization - show interfaces - show ip arp - show env all - show mac-address-table count summary - show fiber-ports optical-transceiver - show cpu rate limit - show errdisable interfaces - show vlan - show ip igmp snooping groups - show ip igmp snooping forward - show ip igmp snooping mrouter - show ipv6 mld snooping groups - show ipv6 mld snooping forward - show ipv6 mld snooping mrouter - show logging - show logging filename-one - show logging filename-two - show logging filename-three - show users - debug show tcam

Команды режима Privileged EXEC

Запрос командной строки в режиме Privileged EXEC имеет следующий вид:

```
console#
```

Таблица 25 — Команды управления системой в режиме Privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
reload	-	Команда служит для перезапуска устройства.
reload at *hh:mm:ss* **[***day month***]**	hh: (0..23); mm:(0..59); ss: (0..59); day: (1...31); month: (1..12)	Установка времени перезагрузки устройства.
reload in {*hours minutes***}**	hours: (0..168); minutes: (0..59)	Установка времени, через которое произойдет перезагрузка устройства.
reload cancel	-	Отмена отложенной перезагрузки.
show reload	-	Просмотр времени, на которое назначена переза-грузка.
show env {*CPU***}**	-	Мониторинг утилизации CPU.
show env {*tasks***}**	-	Мониторинг утилизации CPU по процессам.
show env {*RAM***}**	-	Мониторинг утилизации RAM.
show env {*temperature***}**	-	Мониторинг термодатчика.
show env {*flash***}**	-	Мониторинг flash-памяти.
show env {*power***}**	-	Мониторинг питания и АКБ.
show env {*all***}**	-	Мониторинг всех параметров окружения.

show env {*dry-contacts***}**	-	Мониторинг текущего состояния сухих контактов.
show env {*fan***}**	-	Мониторинг состояния вентиляторов.
show env {*fan thresholds***}**	-	Отобразить таблицу с допустимыми скоростями вращения вентиляторов.
telnet {*A.B.C.D* **|** *AAAA::BBBB* **|** *AAAA::BBBB%interface***} [-l** *name***]**	-	Открытие TELNET-сессии для узла сети. - *A.B.C.D* – IPv4-адрес узла сети; - *AAAA::BBBB* – IPv6-адрес узла сети - *interface* – интерфейс; - *name* – имя пользователя.
show telnet-client	-	Отобразить статус клиента Telnet и количество активных сессий.
ssh [@]{*A.B.C.D* | *AAAA::BBBB* | *AAAA::BBBB%interface***} [-l** *name***] [-1|-2] [-C] [-v] [command]**	-	Открытие SSH-сессии для узла сети. - *A.B.C.D* – IPv4-адрес узла сети; - *AAAA::BBBB* – IPv6-адрес узла сети - *interface* – интерфейс; - *name* – имя пользователя; - 1 – использовать только SSH версии 1; - 2 – использовать только SSH версии 2; - C – запросить сжатие данных; - v – подробно отображать процесс подключения; - command – команда, выполняемая на SSH-сервере.
show ssh-client	-	Отобразить статус клиента SSH и количество активных сессий.
create ssl crypto key rsa [1024 | 2048]	-	Сгенерировать приватный ключ для SSL-сервера на коммутаторе.
create ssl cert-req algo rsa sn [string]	-	Сгенерировать запрос на сертификат от коммутатора.
create ssl server-cert	-	Включить режим ввода сертификата.

При выполнении команды `traceroute` могут произойти ошибки, описание ошибок приведено в таблице 26.

Таблица 26 — Ошибки при выполнении команды `traceroute`

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

Команды режима глобальной конфигурации

Запрос командной строки в режиме глобальной конфигурации имеет следующий вид:

```
console(config)#
```

Таблица 27 — Команды управления системой в режиме глобальной конфигурации

Команда	***Значение/Значение по умолчанию***	***Действие***
hostname *name*		Команда служит для задания сетевого имени устройства.

no hostname	name: (1..128) символов/-	Вернуть сетевое имя устройства в значение по умолчанию.
system location *name*	name:(1..255) символов	Задать информацию о местоположении устройства.
system contact *name*	name:(1..255) символов	Задать контактную информацию устройства.
system description *name*	name:(1..255) символов	Задать описание устройства
cpu rate limit queue *queue* **maxrate** *pps*	queue: (1-8) -pps: 1..2000/128	Установить ограничение скорости входящих кадров (frame) для определенной очереди - *pps* – пакетов в секунду. **Реализует функцию CoPP (Control plane protection).** **Распределение очередей для принимаемого трафика на CPU приведено в Приложение В. Очереди для принимаемого на CPU трафика.**
cpu-rate limit queue *queue* **maxrate** *128*		Восстановить значение *pps* по умолчанию для определенной очереди.
reset-button {*enable* **|** *disable* **|** *reset-only***}**	-/enable	- *enable* – при нажатии кнопки F длительностью менее 10 секунд, происходит перезагрузка устройства; при нажатии на кнопку более 10 секунд, происходит сброс устройства до заводской конфигурации; - *disable* – кнопка F отключена (не реагирует на нажатие); - *reset-only* **–** только перезагрузка.
set telnet-client enable	-/включено	Включить работу TELNET-клиента.
set telnet-client disable		Выключить работу TELNET-клиента.
set ip http enable	-/включено	Включить HTTP-сервер на устройстве.
set ip http disable		Выключить HTTP-сервер на устройстве.
ip http port *port*	80	Назначить порт, прослушиваемый HTTP-сервером. **Требуется перезапуск HTTP-сервера для применения Настройки.**
set ssh-client enable	-/включено	Включить работу SSH-клиента.
set ssh-client disable		Выключить работу SSH-клиента.
env maximum CPU threshold percentage	percentage:1-100/100	Настроить логирование о превышении заданного в процентах порога утилизации CPU.
env maximum RAM threshold percentage	percentage:1-100/100	Настроить логирование о превышении заданного в процентах порога утилизации RAM.
env maximum flash threshold percentage	percentage:1-100/100	Настроить логирование о превышении заданного в процентах порога утилизации flash.
banner exec [*string***]**	-/выключено	Настроить приветствие для неавторизованных пользователей при подключении к коммутатору. *string* — текст приветствия длиной до 256 символов. При вводе команды без параметра string приветствие может иметь длину до 1023 символов. Ввод приветствия прерывается с помощью символа "@".
no banner exec		Удалить приветствие для неавторизованных пользователей.
banner login [*string***]**	-/выключено	Настроить приветствие для пользователей после авторизации. *string* — текст приветствия длиной до 256 символов. При вводе команды без параметра string приветствие может иметь длину до 1023 символов. Ввод приветствия прерывается с помощью символа "@".
no banner login		Удалить приветствие для авторизованных пользователей.
logging events reload	-/включено	Включить отправку snmp трапов и syslog сообщений при перезагрузке устройства по команде «reload» или через SNMP.
no logging events reload		Выключить отправку snmp трапов и syslog сообщений при перезагрузке устройства по команде «reload» или через SNMP.
ip http secure server	-/выключено	Включить HTTPS-сервер на устройстве.
no ip http secure server		Отключить HTTPS-сервер на устройстве.

Таблица 28 — Команды режима Privileged EXEC

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

4.5 Команды для настройки параметров для задания паролей

Данный раздел предназначен для настройки задания паролей для пользователей.

Команды режима глобальной конфигурации

Запрос командной строки в режиме глобальной конфигурации имеет следующий вид:

```
console(config)#
```

Таблица 29 — Команды управления системой в режиме глобальной конфигурации

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

Запрос командной строки в режиме Privileged EXEC имеет следующий вид:

```
console#
```

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

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

4.6 Работа с файлами

4.6.1 Описание аргументов команд

При осуществлении операций над файлами, в качестве аргументов команд выступают адреса URL – определители местонахождения ресурса. Описание ключевых слов, используемых в операциях, приведено в таблице 37.

Таблица 31 — Список ключевых слов и их описание

Ключевое слово	*Описание*
flash://	Исходный адрес или адрес места назначения для энергонезависимой памяти. Энергонезависимая память используется по умолчанию, если адрес URL определен без префикса (префиксами являются: flash:, tftp:, scp:…).
running-config	Файл текущей конфигурации.
startup-config	Файл первоначальной конфигурации.
active-image	Файл с активным образом.
inactive-image	Файл с неактивным образом.
tftp://	Исходный адрес или адрес места назначения для TFTP-сервера. Синтаксис: **tftp://host/[directory]/ filename.** - **host** – IPv4-адрес или сетевое имя устройства; - **directory** – каталог; - **filename** – имя файла.
logging	Файл с историей команд.

4.6.2 Команды для работы с файлами

Запрос командной строки в режиме Privileged EXEC имеет следующий вид:

```
console#
```

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

Команда	*Значение/Значение по умолчанию*	*Действие*
copy *source_url destination_url* **image**	source_url: (1..160) символов; destination_url: (1..160) символов	Копирование файла из местоположения источника в местоположение назначения. - *source_url* – местоположение копируемого файла; - *destination_url* – адрес места назначения, куда файл будет скопирован.
copy startup-config *destination_url*		Сохранение первоначальной конфигурации на сервере.
copy *source_url* **boot**		Копирование файла начального загрузчика из местоположения источника в систему.
dir [flash:path | dir_name]	-	Отобразить список файлов в указанном каталоге.
more [flash:path | file_name]	-	Отобразить содержимое файла.
pwd	-	Отобразить путь до текущей директории.
cd [flash:path | dir_name]	-	Изменить директорию на указанную.
mkdir [flash:path | dir_name]	-	Создать директорию с указанным названием.
rmdir [flash:path | dir_name]	-	Удалить директорию с указанным названием.
erase [flash_url]	-	Удалить файл
erase startup-config	-	Удалить файл первоначальной конфигурации.
erase nvram:	-	Сбросить до дефолтной энергонезависимую память.
erase flash:/LogDir/filename	-	Удалить файл записи аварийных и отладочных сообщений.
boot system inactive	-	Загрузиться с неактивного образа ПО.
boot system active	-	Загрузиться с активного образа ПО.
delete startup-config	-	Удалить файл первоначальной конфигурации вместе с очисткой глобальных настроек nvram и удалением пользователей.
show running-config [**interface {gigabitethernet** *gi_port* **|twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group* **| vlan** *vlan_id*]**[module]**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); group: (1..24); vlan: (2..4094); module: (igs, la, stp..)	Отобразить содержимое файла текущей конфигурации (running-config). - **interface** – конфигурация интерфейсов коммутатора - физических интерфейсов, групп интерфейсов (port-channel), VLAN-интерфейсов, интерфейса замыкания на себя; - **igs** – IGMP snooping; - **la** – link-aggregation; - **stp** – spanning-tree.
show startup-config	-	Отобразить содержимое файла первоначальной конфигурации.

show bootvar	-	Показать активный файл системного ПО, который устройство загружает при запуске.
write {*startup-config* **|** *url*}	-	Сохранить текущую конфигурацию в файл первоначальной конфигурации.
replace running-config [flash:path]	-	Заменить running-config конфигурацией из файла.
clear running-config	-	Очистить текущую конфигурацию (running-config).
diff [flash:path] [flash:path]	-	Сравнить две конфигурации.

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

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

```
MES2318U# bootimg print
```

Команда для смены активного образа из u-boot:

```
MES2318U# bootimg inactive
```

Команда «bootimg inactive» применяется без ожидания подтверждения.

При загрузке файла конфигурации с удаленного сервера в «startup-config» в начале файла необходимо добавить строку с символом «!».
Файл конфигурации должен иметь расширение «.conf».

4.6.3 Команды для резервирования конфигурации

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

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 33 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
backup server *dest_url*	-	Указать адрес сервера, на который будет производиться резервирование конфигурации. Строка в формате «tftp://XXX.XXX.XXX.XXX».
no backup server		Удалить адрес сервера.
backup path *path*	-	Указать путь расположения файла на сервере с префиксом имени файла. При сохранении к префиксу будет добавлена текущая дата и время в формате ггггммддччммсс.

no backup path		Удалить путь для резервирования.
backup auto	-	Включить автоматическое резервирование конфигурации.
no backup auto		Выключить автоматическое резервирование конфигурации.
backup history enable	-	Включить сохранение истории резервных копий.
no backup history enable		Выключить сохранение истории резервных копий.
backup time-period *timer*	timer: (1..35791394)/720 минут	Указать промежуток времени, по истечении которого будет осуществляться автоматическое резервирование конфигурации.
no backup time-period		Установить значение по умолчанию.
backup write-memory	-/выключено	Включение резервирования конфигурации при сохранении пользователем конфигурации на flash-накопитель.
no backup write-memory		Установить значение по умолчанию.

Команды режима Privileged EXEC

Запрос командной строки в режиме Privileged EXEC имеет следующий вид:

```
console#
```

Таблица 34 — Команды режима Privileged EXEC

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

4.7 Настройка системного времени

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

Команды режима Privileged EXEC

Запрос командной строки в режиме Privileged EXEC имеет следующий вид:

```
console#
```

Таблица 35 — Команды настройки системного времени в режиме Privileged EXEC

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

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console#
```

Таблица 36 — Команды режима Privileged EXEC

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

Команды режима глобальной конфигурации

Запрос командной строки в режиме глобальной конфигурации имеет следующий вид:

```
console(config)#
```

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

Команда	*Значение/Значение по умолчанию*	*Действие*
clock time source *ntp*	-	Установить sntp-сервер источником синхронизации времени для устройства.
no clock time source		Установить значение по умолчанию.
clock utc-offset *utc*	utc: (+00:00..+14:00)	Установить часовое смещение относительно нулевого меридиана.
no clock utc-offset		Установить значение по умолчанию.

Команды режима конфигурации SNTP

Для перехода в режим конфигурации SNTP необходимо использовать команду:

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

Запрос командной строки в режиме конфигурации интерфейса имеет следующий вид:

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

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

Команда	*Значение/Значение по умолчанию*	*Действие*
set sntp unicast-server auto-discovery enabled	-/disabled	Включить автоматический поиск sntp-сервера в режиме unicast.
set sntp unicast-server auto-discovery disabled		Выключить автоматический поиск sntp-сервера в режиме unicast.
set sntp unicast-server {ipv4 | ipv6} *ip_addr* **[priority** *priority***] [version** *version***] [port** *udp_port***]**	Может быть задано до 4 серверов priority: (1..15); port: (1025..36564); version: (3..4)	Указать ip-адрес SNTP-сервера.
no sntp unicast-server {ipv4 | ipv6} *ip_addr*		Удалить ip-адрес SNTP-сервера.
set sntp client enable	-/disabled	Включить работу SNTP-клиента.
set sntp client disable		Выключить работу SNTP-клиента.
set sntp client addressing-mode unicast	-/unicast	Указать режим работы SNTP-клиента.
set sntp client authentication-key *key* **md5** *parametrs*	key: (0..65535)	Установить ключ аутентификации для SNTP-клиента.
set sntp client clock-format {ampm | hours}	-/hours	Установить формат часов для SNTP.
set sntp client port *port_num*	port_num: (123, 1025-65535)	Установить udp-порт для sntp-клиента.
set sntp client time-zone *zone*	zone: (+00:00 to +14:00)	Задать значение часового пояса.
set sntp client version *version*	version: (v1,,v4)	Задать версию протокола для работы sntp-клиента.

Таблица 39 — Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show sntp statistics	-	Показать статистику протокола SNTP.
show sntp status	-	Показать статус протокола SNTP.

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Пример настройки SNTP-клиента для сервера 192.168.1.1:

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

4.8 Конфигурация интерфейсов и VLAN

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

Команды режима конфигурации интерфейса (диапазона интерфейсов)

```
console# configure terminal
console(config)# interface {gigabitethernet gi_port |
twopointfivegigabitethernet two_port |tengigabitethernet te_port | port-
channel group | range {…} | loopback loopback_id }
console(config-if)#
```

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

Выбор интерфейса осуществляется при помощи команд приведённых в таблице 40:

Таблица 40 — Команды выбора интерфейса

Команда	*Назначение*
interface gigabitethernet *gi_port*	Для настройки 1G-интерфейсов.
interface twopointfivegigabitethernet *two_port*	Для настройки 2,5G-интерфейсов.
Interface tengigabitethernet *te_port*	Для настройки 10G-интерфейсов.
interface port-channel *group*	Для настройки групп каналов.
interface loopback *loopback_id*	Для настройки виртуальных интерфейсов.

где:

- ***fa_port*** – порядковый номер 100MB-интерфейса, задается в виде: 0/1;
- ***gi_port*** – порядковый номер 1G-интерфейса, задается в виде: 0/1;
- ***two_port*** – порядковый номер 2,5G-интерфейса, задается в виде: 0/1;
- ***te_port*** – порядковый номер 10G-интерфейса, задается в виде 0/1;
- ***group*** – порядковый номер группы, общее количество согласно таблице 9 (строка «Агрегация каналов (LAG)»);

– ***loopback_id*** – порядковый номер виртуального интерфейса, общее количество согласно таблице 9 (строка «Количество виртуальных Loopback-интерфейсов»).

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

Таблица 41 — Команды режима конфигурации интерфейсов Ethernet и Port-Channel

Команда	*Значение/Значение по умолчанию*	*Действие*
shutdown	-/включено	Выключить конфигурируемый интерфейс (Ethernet, port-channel).
no shutdown		Включить конфигурируемый интерфейс.
description *description*	description: (1..128) символов/нет описания	Добавить описание интерфейса (Ethernet, port-channel).
no description		Удалить описание интерфейса.
speed *mode*	mode: (10, 100, 1000, 10000)	Задать скорость передачи данных (Ethernet).
no speed		Установить значение по умолчанию.
duplex *mode*	mode: (full, half)/full	Задать режим дуплекса интерфейса (полнодуплексное соединение, полудуплексное соединение, Ethernet).
no duplex		Установить значение по умолчанию.
negotiation [cap1 [cap2…cap5]]	cap: (10f, 10h, 100f, 100h, 1000f)	Включает автосогласование для скорости и дуплекса на настраиваемом интерфейсе. Можно указать определенные совместимости параметра автосогласования. Если параметры не заданы, то поддерживаются все совместимости. **Автосогласование настраивается только на интерфейсах Ethernet.**
no negotiation		Выключает автосогласование для скорости и дуплекса на настраиваемом интерфейсе.
flowcontrol *on*	mode: (on, off)/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).
flowcontrol *off*		Отключить режим управления потоком.
media-type { force-fiber | force-copper | prefer-fiber }	-/prefer-fiber	Выбор типа комбо-порта в качестве основного носителя. **- force-fiber** – разрешена активность только оптической части комбо-порта; **- force-cooper –** разрешена активность только медной части комбо-порта; **- prefer-fiber** – преимущество оптического линка.
mtu *size*	size: (128..12288)/ 12288 байт	Установить значение maximum transmission unit (MTU) для интерфейса *- size – размер пакета (количество байт в пакете)* **Если Ethernet-интерфейс входит в состав Port-Channel, то на нем нельзя изменять значение MTU.** **Дефолтное значение MTU для Ethernet и Port-Channel интерфейсов равно значению заданному командой system mtu в режиме глобальной конфигурации.**
no mtu		Установить значение по умолчанию.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 42 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
errdisable recovery interval *interval*	interval: (30..86400)/300	Установить временной интервал для автоматического повторного включения интерфейса. При смене интервала таймер обновляется для всех заблокированных портов, на которых включено автосогласование.
no errdisable recovery interval		Установить значение по умолчанию.
errdisable recovery cause {storm-control|loopback-detection | udld | port-security}	-/запрещено	Включить автоматическую активацию интерфейса после его отключения в следующих случаях: - **loopback-detection** – обнаружение петель; - **udld** – активация защиты UDLD; - **storm-control –** широковещательный шторм; - **port-security –** нарушение безопасности для port security.
no errdisable recovery cause {storm-control|loopback-detection | udld | port-security}		Установить значение по умолчанию.
system mtu *size*	size: (128..10000)/10000 байт size: (128..12288)/12288 байт	Установить значение системного maximum transmission unit (MTU) - *size* – размер пакета (количество байт в пакете).
no system mtu		Установить значение по умолчанию.
default interface [range] { gigabitethernet *gi_port* | **twopointfivegigabitethernet** *two_port* | **tengigabitethernet** *te_port* | **port-channel** *group* | **vlan** *vlan_id* | **loopback** *loopback_id* **}**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); group: (1..24); vlan_id: (1..4094); loopback_id: (1..10)	Сброс настроек интерфейса или группы интерфейсов на значения, установленные по умолчанию. **Во время выполнения команды интерфейс будет отключен.**

Команды режима EXEC

Вид запроса командной строки в режиме EXEC:

```
console#
```

Таблица 43 — Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
clear counters	-	Сброс статистики для всех интерфейсов.
clear counters { gigabitethernet *gi_port* | **twopointfivegigabitethernet** *two_port* | **tengigabitethernet** *te_port* | **port-channel** *group***}**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); group: (1..24)	Сброс статистики для интерфейса.
show interfaces { gigabitethernet *gi_port* | **twopointfivegigabitethernet** *two_port* | **tengigabitethernet** *te_port* | **port-channel** *group***}**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); group: (1..24)	Показать сводную информацию о состоянии, настройке и статистике порта.
show interfaces status	-	Показать состояние всех интерфейсов.
show interfaces description	-	Показать описания всех интерфейсов.
show interfaces counters	-	Показать статистику для всех интерфейсов.
show interfaces counters { gigabitethernet *gi_port* | **twopointfivegigabitethernet** *two_port* | **tengigabitethernet** *te_port* | **port-channel** *group* | **vlan** *vlan_id* **}**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); group: (1..24); vlan: (1..4094)	Показать статистику для интерфейса.

show errdisable interfaces { gigabitethernet *gi_port* | **twopointfivegigabitethernet** *two_port* | **tengigabitethernet** *te_port* **}**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11)	Показать причину отключения порта, группы портов, заблокированные порты.
show errdisable recovery	-	Показать настройки для автоматической повторной активации порта.
set interface active { gigabitethernet *gi_port* | **twopointfivegigabitethernet** *two_port* | **tengigabitethernet** *te_port* **}**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11)	Активировать интерфейс после errdisable.
show interfaces utilization { gigabitethernet *gi_port* | **twopointfivegigabitethernet** *two_port* | **tengigabitethernet** *te_port } {interval interval***}**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); interval: (5, 60, 300) сек	Показать статистику по нагрузке для интерфейса. - **Interval** – интервал в секундах.

4.8.2 Настройка VLAN и режимов коммутации интерфейсов

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 44 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
vlan *vlan_id*	vlan_id: (2..4094)	Перейти в режим конфигурирования указанного VLAN
map protocol {ip | other} {enet-v2 | llcOther | snap} protocols-group *group-id*	group-id: (1..*2147483647*)/-	Настроить группу протоколов, по которым будет производиться классификация кадров. В одну группу можно объединить несколько протоколов, указывая для них один и тот же Group ID. Номер протокола можно выбрать из списка предустановленных значений или задать вручную через параметр other в формате XX:XX. Расположение поля с номером протокола зависит от типа L2-заголовка и инкапсуляции: **- enet-v2** – кадр с заголовком Ethernet II, протокол определяется по полю EtherType. При наличии VLAN-тегов выбирается самый последний EtherType, с наибольшим оффсетом. **- llcOther** – кадр формата RFC1042 (IEEE 802). Двухбайтный номер протокола соответствует полям DSAP:SSAP в LLC-заголовке. **- snap** – кадр с LLC/SNAP-инкапсуляцией. Номер протокола соответствует полю Protocol ID в SNAP-заголовке.
no map protocol {ip | other} {enet-v2| llcOther | snap}		Удаляет protocol-group с коммутатора.
map mac {host | *mac-address mask***} macs-group** *group-id*	group-id: (1..*2147483647*)/-	Настроить диапазон MAC-адресов, по которым будет производиться классификация. Для разных MAC-адресов можно выбрать одну и ту же группу.
no map mac {host | *mac-address***}**		Удалить указанный MAC-адрес из macs-group.
shutdown garp	-/выключено	Отключить работу модуля GARP на устройстве. **Данная команда отключает работу модуля GARP с безвозвратным удалением всех настроек блока GARP.**
no shutdown garp		Включить модуль протокола GARP. **Для работы модуля GARP резервируется 15 Мбайт оперативной памяти.**

gvrp enable	-/выключено	Включить протокол GVRP глобально.
gvrp disable		Выключить протокол GVRP глобально.
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
voice vlan oui-table {add *oui* **| remove** *oui***} [descriprion** *word***]**	word:(1..32) символов	Разрешить редактировать таблицу OUI. - *oui* – первые 3 байта MAC-адреса; - *word* – описание oui.

Команды режима конфигурации VLAN (диапазон VLAN'ов)

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

Таблица 45 — Команды режима конфигурации VLAN

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

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

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

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

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

Порт может работать в четырех режимах:

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

Таблица 46 — Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
switchport mode {access |trunk | general}	mode: (access, trunk, general)/general	Задать режим работы порта в VLAN.
no switchport mode		Установить значение по умолчанию.
switchport access vlan *vlan_id*	vlan_id: (1..4094)/1	Добавить VLAN для интерфейса доступа. - *vlan_id* – идентификационный номер VLAN.
no switchport access vlan		Установить значение по умолчанию.
switchport dot1q tunnel	-	Перевести порт режим работы с внешним VLAN-тегом. Команда используется для настройки функции Q-in-Q.

switchport trunk native vlan *vlan_id*	vlan_id: (1..4094)/1	Добавить номер VLAN в качестве Default VLAN для данного интерфейса. Весь нетегированный трафик, поступающий на данный порт, определяется в данный VLAN. - *vlan_id* – идентификационный номер VLAN.
no switchport trunk native vlan		Установить значение по умолчанию.
switchport general allowed vlan add *vlan_list* **[untagged]**	vlan_list: (2..4094)	Добавить список VLAN для интерфейса. - *vlan_list* – список VLAN ID. Диапазон VLAN можно задать перечислением через запятую или указать начальное и конечное значения диапазона через дефис "-".
switchport general allowed vlan remove *vlan_list*		Удалить список VLAN для интерфейса.
switchport general pvid *vlan_id*	vlan_id: (1..4094)/1 – если установлен VLAN по умолчанию	Добавить идентификатор VLAN порта (PVID) для основного интерфейса. - *vlan_id* – идентификационный номер VLAN порта.
no switchport general pvid		Установить значение по умолчанию.
switchport ingress-filter	-/фильтрация включена	Включить фильтрацию входящих пакетов на основе присвоенного им значения VLAN ID. Если фильтрация включена, и пакет не входит в группу VLAN с присвоенным пакету значением VLAN ID, то пакет отбрасывается.
no switchport ingress-filter		Выключить фильтрацию входящих пакетов на основе присвоенного им значения VLAN ID.
switchport acceptable-frame-type {tagged | all |untaggedAndPrioritytagged}	-/all	**- untaggedAndPrioritytagged** – на порту разрешается прием только нетегированных кадров (frame); - **tagged** – только тегированных; - **all** – любых кадров (frame).
switchport forbidden vlan add *vlan_list*	vlan_list: (2..4094, all)/все VLAN разрешены порту	Запретить добавление указанному 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 указанному VLAN-порту.
switchport forbidden default-vlan	По умолчанию членство в дефолтной VLAN разрешено	Запретить добавление дефолтному VLAN-порту.
no switchport forbidden default-vlan		Установить значение по умолчанию.
switchport protected	-	Перевести порт в режим изоляции внутри группы портов.
no switchport protected		Восстановить значение по умолчанию.
port-isolation { gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* | **tengigabitethernet** *te_port* **| port-channel** *group* **}**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); group: (1..24)	Создать или перезаписать существующий список портов на указанный новый.
port-isolation {add | remove} { gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* | **tengigabitethernet** *te_port* **| port-channel** *group***}**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); group: (1..24)	Добавить указанные порты к уже существующему списку или удалить список.
switchport default-vlan tagged	-	Установить порт как тегирующий в дефолтному VLAN.
no switchport default-vlan tagged		Установить значение по умолчанию.
switchport map protocols-group *group-id* **vlan** *vlan-id*	group_id: (1..2147483647); vlan_id: (1..4094)/по умолчанию PBV включен на всех портах	Назначить VLAN ID пакетам, попадающим в указанную Group ID на этом порту. Разные порты одной и той же группы могут соответствовать разным VLAN.
no switchport map protocols-group *group-id*		Выключить PBV на порту.
switchport map macs-group *group-id* **vlan** *vlan-id*	vlan_id: (1..4094)/- group-id: (1..*2147483647*)/-	Осуществитьназначение vlan-id для macs-group.
no switchport map macs-group *group-id*		Отменить назначение vlan-id для macs-group.
gvrp enable	-/выключено	Включить протокол GVRP на интерфейсе.

gvrp disable		Выключить протокол GVRP на интерфейсе.
vlan restricted enable	-/выключено	Включить запрет на изучение vlan-атрибутов, полученных от протокола GVRP, на интерфейсе.
vlan restricted disable		Выключить запрет на изучение vlan-атрибутов, полученных от протокола GVRP, на интерфейсе.
set garp timer {join | leave | leaveall}	join: msec/200 leave: msec/600 leaveall: msec/10000	Установить значения таймеров GVRP на интерфейсе.
switchport unicast-mac learning enable	-/включено	Включить изучение MAC-адресов на интерфейсе.
switchport unicast-mac learning disable		Выключить изучение MAC-адресов на интерфейсе.
switchport egress-filter	-/включено	Включает фильтрацию исходящих кадров (frame) на основе присвоенного им значения VLAN ID. Если фильтрация включена, и пакет не входит в группу разрешенных на интерфейсе VLAN ID, то пакет отбрасывается.
no switchport egress-filter		Выключить фильтрацию исходящих кадров (frame) на основе присвоенного им значения VLAN ID.
switchport egress TPID-type {portbased | vlanbased}	-	Задать TPID для исходящих кадров.
switchport voice vlan *[vlan_id]*	vlan_id: (1..4094)	Включить Voice VLAN для порта. - *vlan_id* – установить идентификатор VLAN для порта.
no switchport voice vlan		Отключить Voice VLAN для порта.
voice vlan authentication bypass	-/выключено	Разрешить трафику Voice VLAN игнорировать аутентификацию 802.1x.
no voice vlan authentication bypass		Запретить трафику Voice VLAN игнорировать аутентификацию 802.1x.

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

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

```
console#configure terminal
console(config)# interface gi 0/1
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 99
console(config-if)# switchport dot1q tunnel
console(config)# interface gi 0/2
console(config-if)# switchport mode trunk
```

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

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 47 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
mac-address-table static unicast *mac_add* **vlan** *vlan_id* **interface [gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **|** **tengigabitethernet** *te_port***] status [deleteOnReset | deleteOnTimeout | permanent | secure]**	vlan_id: (1..4094); gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11)	Добавить исходный MAC-адрес в таблицу. - **Permanent** – данный MAC-адрес остается в таблице адресации после переключения статуса интерфейса; - **Deleteonreset** – данный адрес удалится после перезагрузки устройства; - **Deleteontimeout** – данный адрес удалится по тайм-ауту.
no mac-address-table static unicast *mac_add* **vlan** *vlan_id*		Удалить MAC-адрес из таблицы.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 48 — Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show mac-address-table address *mac_addr* **[interface {gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **}]**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11)	Просмотр всей таблицы MAC-адресов.
show mac-address-table count	-	Показать количество записей в таблице MAC-адресов.
show mac-address-table count summary	-	Показать суммарную статистику по таблице MAC-адресов.
show mac-address-table dynamic unicast [vlan *vlan_id***] [address** *mac_add*] **[interface { gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **}]**	vlan_id: (1..4094); gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11)	Показать таблицу с динамическими MAC-адресами.
clear mac-address-table dynamic [interface { gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **}] [vlan** *vlan_id***]**	vlan_id: (1..4094); gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11)	Удалить динамические записи из таблицы MAC-адресов.
show mac-address-table secure	-	Показать таблицу с защищенными MAC-адресами.
show mac-address-table secure recovery-file	-	Показать таблицу с защищенными MAC-адресами, которые сохраняются при перезагрузке.
show mac-address-table secure [vlan *vlan_id***] [address** *mac_add*] **[interface {gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port}***]**	vlan_id: (1..4094); gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11)	Показать таблицу с защищенными MAC-адресами для указанного интерфейса.

show mac-address-table address *mac_add* **[interface {gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***}]**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11	Показать таблицу MAC-адресов для указанного интерфейса.
clear mac-address-table secure [interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port}* **]**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11)	Удалить защищенные MAC-адреса из таблицы на интерфейсе.
show mac-address-table static unicast [vlan *vlan_id***] [address** *mac_add*] **[interface { gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port}***]**	vlan_id: (1..4094); gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11)	Показать таблицу со статическими MAC-адресами.
show mac-address-table [vlan *vlan_id***] [address** *mac_add*] **[interface {gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port}***]**	vlan_id: (1..4094); gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11)	Показать таблицу MAC-адресов для указанного VLAN.
show garp timer [port { gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group}***]**	vlan_id: (1..4094); gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11) group: (1..24)	Отобразить значения таймеров GVRP на интерфейсах.
show gvrp statistics [port { gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group}***]**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11) group: (1..24)	Отобразить статистику протокола GVRP.
clear garp counters{all |port { gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group}***]**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11) group: (1..24)	Очистить статистику протокола GARP.
show vlan	-	Показать информацию о всех VLAN.
show vlan id *vlan_id*	vlan_id: (1..4094)	Показать информацию по конкретному VLAN.
show vlan protocols-group	-	Показать информацию о настроенных группах и протоколах.
show protocol-vlan	-	Показать информацию о VLAN, соответствующих группам протоколов на разных портах.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 49 — Команды режима EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show interfaces switchport { gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **}**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11)	Показать конфигурацию порта, группы портов.

4.9 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.

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

Вид запроса командной строки режима конфигурации интерфейса конфигурации:

```
console# configure terminal
console(config)# interface{ gigabitethernet gi_port | gitengigabitethernet te_
port| port-channel group|range{…}}
console(config-if)#
```

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

Команда	*Значение/Значение по умолчанию*	*Действие*
selective-qinq list ingress override-vlan *vlan_id* **[ingress-vlan** *ingress_vlan_id***]**	vlan_id: (1..4094) ingress_vlan_id: (1..4094)	Создать правило, на основании которого внешняя метка *ingress_vlan_id* входящего пакета будет заменяться на vlan_id.
no selective-qinq list ingress [ingress-vlan *vlan_id***]**		Удалить указанное правило selective qinq для входящих пакетов.
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***]**		Удалить список правил selective qinq для исходящих пакетов.
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 для трафика с внешней меткой *ingress_vlan_id* будет добавляться метка с vlan_id.
no selective-qinq list ingress [ingress-vlan *vlan_id***]**		Удалить указанное правило selective qinq для входящих пакетов.
selective-qinq list ingress {deny | permit} [ingress-vlan *ingress_vlan_id***]**	vlan_id (1..4094); ingress_vlan_id: (1..4094)	Создать правило, на основании которого трафик с внешней меткой ingress_vlan_id пропускается без изменений или отбрасывается. Если ingress_vlan_id не указан, то пропускаться или отбрасываться будет весь трафик. - **deny** — запрещает прохождение пакетов с указаной внешней меткой; - **permit** — разрешает прохождение пакетов с указанной внешней меткой.
no selective-qinq list ingress [ingress-vlan *ingress_vlan_id***]**		Удалить указанное правило selective qinq для входящих пакетов.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 51 — Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show selective-qinq [gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***]**	-	Отобразить список правил selective sqinq.

4.10 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 глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 52 — Команды режима глобальной конфигурации

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

Команды режима конфигурации интерфейса Ethernet

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

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

Таблица 53 — Команды режима конфигурации интерфейса Ethernet

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

no storm-control broadcast level {*pps* **|** *kbps***}**		Выключить контроль широковещательного трафика.
**storm-control {multicast	dlf	broadcast} action shutdown**	-	Отключить интерфейс при обнаружении многоадресного, неизвестного одноадресного или широковещательного трафика.
**no storm-control {multicast	dlf	broadcast} action**		Отменить отключение интерфейса при обнаружении многоадресного, неизвестного одноадресного или широковещательного трафика.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 54 — Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show interface [gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***] storm-control**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); group: (1..24)	Показать конфигурацию функции контроля широковещательного «шторма» для указанного порта, либо всех портов.
show storm-control	-	Отображает текущую настройку единиц измерения.

4.11 Группы агрегации каналов – Link Aggregation Group (LAG)

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

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

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

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

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

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

Таблица 55 — Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
channel-group *group* **mode {on | active | passive}**	group: (1..24); mode: (on, active, passive)	Добавить Ethernet-интерфейс в группу портов. - On – добавить интерфейс в статическую группу портов; - Active – добавить интерфейс в группу портов, работающих по протоколу LACP, при этом отправка PDU осуществляется всегда; - Passive – добавить интерфейс в группу портов, работающих по протоколу LACP, при этом отправка PDU осуществляется только в том случае, если устройство получает PDU от соседнего устройства. **Если значение MTU для Ethernet и Port-Channel интерфейсов отличаются, то добавить данный Ethernet-интерфейс в группу портов нельзя.**
no channel-group		Удалить Ethernet-интерфейс из группы портов.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

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

Таблица 56 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
shutdown port-channel	-/включено	Отключить работу модуля port-channel на устройстве. **Данная команда отключает работу модуля port-channel с безвозвратным удалением всех настроек блока LAG.**
no shutdown port-channel		Включить работу модуля port-channel на устройстве.
port-channel load-balance {src-dest-mac-ip | src-dest-mac | src-dest-ip | src-dest-mac-ip-port | dest-mac | dest-ip | src-mac | src-ip}	-/src-dest-mac	Задать механизм балансировки нагрузки для стратегии ECMP и для группы агрегированных портов. **- src-dest-mac-ip** – механизм балансировки основывается на MAC-адресе и IP-адресе источника и получателя; - **src-dest-mac** – механизм балансировки основывается на MAC-адресе источника и получателя; - **src-dest-ip** – механизм балансировки основывается на IP-адресе источника и получателя; - **src-dest-mac-ip-port** – механизм балансировки основывается на MAC-адресе, IP-адресе источника и получателя, а также TCP-порте назначения; - **dest-mac** – механизм балансировки основывается на MAC-адресе получателя; - **dest-ip** – механизм балансировки основывается на IP-адресе получателя; - **src-mac** – механизм балансировки основывается на MAC-адресе источника; - **src-ip** – механизм балансировки основывается на IP-адресе источника.
set port-channel enable	-/отключено	Включить работу LAG глобально на коммутаторе.
set port-channel disable		Выключить работу LAG глобально на коммутаторе.
set port-channel independent-mode enable		Включить автономный режим работы LAG.
set port-channel independent-mode disable		Выключить автономный режим работы LAG.

4.11.1 Статические группы агрегации каналов

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

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

4.11.2 Протокол агрегации каналов LACP

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

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 57 — Команды режима глобальной конфигурации

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

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

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

Таблица 58 — Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
lacp timeout {long | short}	-/long	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.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 59 — Команды режима EXEC

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

Пример настройки:

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

4.12 Настройка IPv4-адресации

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

Команды режима конфигурации интерфейса VLAN

Вид запроса командной строки в режиме конфигурации интерфейса VLAN:

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

Таблица 60 — Команды режима конфигурации интерфейса

Команда	*Значение/Значение по умолчанию*	*Действие*
ip address *ip_address {ip_mask |prefix_length}* **[*secondary* {***ip_address {ip_mask |prefix_length}*** }]**	–	Назначение заданному интерфейсу IP-адреса и маски подсети. - **secondary** — позволяет настроить дополнительные IPv4-адреса на текущий interface vlan. Для настройки требуется наличие основного IPv4-адреса на интерфейсе.
no ip address [*ip_address***]**		Удаление IP-адреса интерфейса.
ip management outer-vlan *vlan_id*	vlan_id: (1...4094)	Включение обработки QinQ-трафика управления на CPU. Параметр **vlan-id** назначает внешний тег 802.1Q. **Для корректной работы функции необходимо наличие активного vlan_id на коммутаторе. При этом оперативное состояние interface vlan, на котором настраивается функция, должно быть up.** **Данные настройки выполняются на интерфейсе C-VLAN.**
no ip management outer-vlan		Выключение обработки QinQ-трафика управления на CPU.

ip address dhcp [client-id { gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| vlan** *vlan_id***}] [hostname** *name***]**	vlan_id: (1-4094); gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); name: (1..32) символа	Получение IP-адреса от DHCP-сервера. Установка опций 12 и 61.
no ip address dhcp		Запрет использования протокола DHCP для получения IP-адреса от DHCP-сервера.
ip dhcp client vendor-specific *string*	string:(1..256)/модель коммутатора	Установить значение опции 60.
no ip dhcp client vendor-specific		Установить значение по умолчанию.

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

Пример настройки обработки трафика с S-vlan 10, C-vlan 20 на CPU:

```
console# !
console(config)# interface vlan 20
console(config-vlan)# ip management outer-vlan 10
```

Команды режима Privileged EXEC

Вид запроса командной строки в режиме privileged EXEC:

```
console#
```

Таблица 61 — Команды режима privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
renew dhcp vlan vlan_id	vlan_id: (1..4094)	Отправить запрос к DHCP-серверу на обновление IP-адреса.
show ip interface vlan *vlan_id*	vlan_id: (1..4094)	Показать конфигурацию IP-адресации для указанного интерфейса.

4.13 Настройка IPv6-адресации

4.13.1 Протокол IPv6

Коммутаторы поддерживают работу по протоколу IPv6, что является большим преимуществом, т.к. протокол IPv6 разработан для того, чтобы в будущем полностью заменить адресацию протокола IPv4. По сравнению с IPv4 протокол IPv6 имеет расширенное адресное пространство — 128 бит вместо 32. Адрес IPv6 представляет собой 8 блоков, разделенных двоеточием, в каждом блоке 16 бит, записанных в виде четырех шестнадцатеричных чисел.

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

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

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

4.13.2 Настройки протокола IPv6

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 62 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ipv6 unicast-routing	-/включено	Включить маршрутизацию между ipv6-префиксами.
no ipv6 unicast-routing		Отключить маршрутизацию между ipv6-префиксами.
ipv6 neighbor *ipv6_address* **vlan** *vlan_id MAC-address*	ipv6_address: XXXX::XXXX; vlan_id: (0...4094); MAC-address: XX:XX:XX:XX:XX:XX/-	Создать статическую запись ipv6 neighbor.
no ipv6 neighbor *ipv6_address* **vlan** *vlan_id MAC-address*		Удалить статическую запись ipv6 neighbor.
ipv6 route *ipv6_address prefix-length* {**vlan** *vlan_id* | *next_hop_ipv6_address*} [*administrative_distance*] [{**unicast** | **anycast**}] **/** *next-hop-ipv6-address*}	ipv6_address: XXXX:XXXX; prefix-length: (0-128); vlan_id: (1..4094); next_hop_ipv6_address: XXXX::XXXX: administrative_distance: (1-255)	Настроить статический маршрут до указанного ipv6-префикса.
no ipv6 route *ipv6_address prefix-length* {**vlan** *vlan_id* | *next_hop_ipv6_address*} [*administrative_distance*] [**unicast** | **anycast**]		Удалить статический маршрут до указанного префикса.

Команды режима конфигурации интерфейса VLAN

Вид запроса командной строки в режиме конфигурации интерфейса VLAN:

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

Таблица 63 — Команды режима конфигурации интерфейса

Команда	*Значение/Значение по умолчанию*	*Действие*
ipv6 enable	-/Выключено	Включить работу протокола IPv6 на интерфейсе. Генерирует ipv6 link-local адрес на данном интерфейсе.
no ipv6 enable		Отключить работу протокола IPv6 на интерфейсе.
ipv6 address *ipv6_address prefix-length* **link-local cga**	ipv6_address: XXXX::XXXX; prefix-length: (0-128)	Установить ipv6 link-local адрес на данном интерфейсе.
no ipv6 address *ipv6_address prefix-length* **link-loca**		Удалить ipv6 link-local адрес на данном интерфейсе.
ipv6 address *ipv6_address prefix-length* **[unicast | anycast | eui64]**	ipv6_address: XXXX::XXXX; prefix-length: (0-128)/-	Настроить указанный ipv6-адрес на интерфейсе. - **eui64** – использовать алгоритм EUI-64 для генерации адреса.
no ipv6 address *ipv6_address prefix-length* **[unicast | anycast | eui64]**		Удалить указанный адрес с интерфейса.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 64 — Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ipv6 interface [vlan *vlan***]**	-	Отобразить состояние и настройки IPv6-интерфейсов.
show ipv6 route [connected | static | summary | *ipv6-prefix***]**	-	Отобразить таблицу маршрутизации для IPv6.
show ipv6 traffic [interface vlan {*vlan-id/vfi-id***}] [hc]**	-	Отобразить статистику по принятым и отправленным IPv6-пакетам.

4.14 Настройка протоколов

4.14.1 Настройка протокола ARP

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

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 65 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
arp *ip_addr hw_addr [***vlan** *vlan_id]*	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; vlan_id: (1..4094)	Добавить статическую запись соответствия IP- и MAC-адресов в таблицу ARP для указанной VLAN. - **ip_address —** IP-адрес; - **hw_address** — MAC-адрес.
no arp *ip_addr*		Удалить статическую запись соответствия IP- и MAC-адресов из таблицы ARP для указанного в команде IP-адреса.
arp gratuitous interval *seconds*	seconds: (15..86400)/150 секунд	Установить интервал между отправкой gratuitous arp сообщений.
no arp gratuitous interval		Установить значение по умолчанию.
arp timeout *seconds*	seconds: (30..86400) сек	Настроить время жизни динамических записей в таблице ARP (сек).
no arp timeout		Установить значение по умолчанию.

Команды режима конфигурации интерфейса VLAN

Вид запроса командной строки в режиме конфигурации интерфейса VLAN:

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

Таблица 66 — Команды режима конфигурации интерфейса

Команда	*Значение/Значение по умолчанию*	*Действие*
ip arp gratuitous periodic	-/включено	Включить отправку gratuitous arp-сообщений.
no ip arp gratuitous periodic		Выключить отправку gratuitous arp-сообщений.

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 67 — Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip arp [ip-address *ip_address***] [mac-address** *mac_addres***] [vlan** *vlan_id***]**	формат *ip_address*: A.B.C.D формат *mac_address*: H.H.H или H:H:H:H:H:H или H-H-H-H-H-H; vlan: (1..4094)	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 ip arp statistics	-	Показать текущую статистику протокола arp.
clear ip arp	-	Удалить все динамические записи из ARP-таблицы.

4.14.2 Механизм обнаружения петель (loopback-detection)

Данный механизм позволяет устройству отслеживать закольцованные порты. Петля на порту обнаруживается путём отсылки коммутатором кадра (frame) 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 68 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
shutdown loopback-detection	-/включено	Отключить работу модуля loopback-detection на устройстве. **Данная команда отключает работу модуля loopback-detection с безвозвратным удалением всех настроек блока LBD.**
no shutdown loopback-detection		Включить работу модуля loopback-detection на устройстве.
loopback-detection enable	-/выключено	Включить механизм обнаружения петель для коммутатора.
loopback-detection disable		Восстановить значение по умолчанию.
loopback-detection interval *seconds*	seconds: (1..60)/30 секунд	Установить интервал между loopback-кадрами. - *seconds* — интервал времени между LBD-кадрами.
no loopback-detection interval		Восстановить значение по умолчанию.

loopback-detection destination-address *mac_address*	-/ff:ff:ff:ff:ff:ff	Определить MAC-адрес назначения, указанный в LDB-кадре. **По умолчанию MAC-адрес назначения широковещательный.**

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

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

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

Таблица 69 — Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
loopback-detection enable	-/выключено	Включить механизм обнаружения петель на порту.
loopback-detection disable		Восстановить значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 70 — Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show loopback-detection [gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| statistics]**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11)	Отобразить состояние механизма loopback-detection.
debug loopback-detection [all | buffer-alloc | control | critical | pkt-dump | pkt-flow]	-/отключено	Включить отправку сообщений по событиям loopback-detection.

4.14.3 Семейство протоколов STP (STP, RSTP, MSTP)

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

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

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

Максимально допустимое количество экземпляров MSTP – 64.

4.14.3.1 Настройка протокола STP, RSTP

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 71 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
shutdown spanning-tree	-/включено	Отключить работу модуля STP на устройстве. **Данная команда отключает работу модуля STP с безвозвратным удалением всех настроек блока STP.** **Модуль STP включается командой spanning-tree.**
spanning-tree	-/включено	Разрешить использование коммутатором протокола STP.
no spanning-tree		Запретить использование коммутатором протокола STP.
spanning-tree mode { rst | mst}	-/MSTP	Установить режим работы протокола STP: - **rst** — IEEE 802.1W Rapid Spanning Tree Protocol; - **mst** — IEEE 802.1S Multiple 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..2)/2 сек	Установить интервал времени между передачами широковещательных сообщений «Hello» к взаимодействующим коммутаторам.
no spanning-tree hello-time		Установить значение по умолчанию.
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 устройства в связующем дереве STP. Значение приоритета должно быть кратно 4096.
no spanning-tree priority		Установить значение по умолчанию.
spanning-tree pathcost dynamic [lag-speed]	-/выключено	Включить динамическое определение ценности пути. - **lag-speed** — определение ценности пути будет вычисляться при изменении скорости LAG.
no spanning-tree pathcost		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 compatibility {mst | rst | stp}	-/включено	Версия совместимости STP.
no spanning-tree compatibility		Установить значение по умолчанию.
spanning-tree flush-indication-threshold *value*	value: (0..65535)	Пороговое количество TCN BPDU, при котором запускается таймер, который равен значению flush-interval.
no spanning-tree flush-indication-threshold		Установить значение по умолчанию.
spanning-tree flush-interval *interval*	interval: (0..500)/0	Установить значение интервала, после которого произойдёт очистка MAC-таблицы посде получения TCN BPDU.
no spanning-tree flush-interval		Установить значение по умолчанию.

spanning-tree transmit hold-count *count*	count: (1..10)/6	Это значение указывает максимальное количество пакетов, которые могут быть отправлены в заданный интервал времени hello-time.
no spanning-tree transmit hold-count		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 72 — 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 78	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 78
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	-	Включить режим, в котором порт при поднятии на нем линка сразу становится в состояние передачи, не дожидаясь истечения таймера.
no spanning-tree portfast		Выключить режим моментального перехода в состояние передачи по поднятию «линка».
spanning-tree loop-guard	-/запрещено	Разрешить на интерфейсе дополнительную защиту от петель. В случае, если интерфейс находится в состоянии, отличном от Designated и при этом перестает получать BPDU, интерфейс блокируется.
no spanning-tree loop-guard		Запретить дополнительную защиту от возникновения петель.
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 [admin-down | disable-discarding] | disable | none}	-/выключено	Разрешить защиту, выключающую интерфейс при приёме пакетов BPDU.
no spanning-tree bpduguard		Запретить защиту, выключающую интерфейс при приёме пакетов BPDU.
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	-/выключено	Запретить прием BPDU с флагом TCN.
no spanning-tree restricted-tcn		Разрешить прием BPDU с флагом TCN.
spanning-tree bpdufilter {disable | enable }	-/disabled	Запретить/разрешить приём и передачу STP BDPU на интерфейсе.
no spanning-tree bpdufilter		Установить значение по умолчанию.
spanning-tree auto-edge	-/включено	Включить автоматическое определение клиентских портов.
no spanning-tree auto-edge		Выключить автоматическое определение клиентских портов.
spanning-tree {bpdu-receive | bpdu-transmit} enable	-/включено	Включить режим приёма и/или передачи на интерфейсе.
spanning-tree {bpdu-receive | bpdu-transmit} disable		Выключить режим приёма и/или передачи на интерфейсе.
spanning-tree layer2-gateway-port	-/выключено	Назначить порт как шлюз 2 уровня. **Spanning-tree на данном порту должен быть в состоянии disabled.**
no spanning-tree layer2-gateway-port		Установить значение по умолчанию.
spanning-tree pseudoRootId priority *priority* **mac-address** *mac_add*	priority: (0..61440)	Настроить приоритет для pseudoRoot на интерфейсе.
no spanning-tree pseudoRootId		Установить значение по умолчанию.
spanning-tree {restricted-role | restricted-tcn}	-/	Включить на интерфейсе функцию защиты от атак.
no spanning-tree {restricted-role | restricted-tcn}		Отключить на интерфейсе функцию защиты от атак.

Таблица 73 — Стоимость 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
LAG 10M	1999900	56
LAG 100M	199900	12
LAG 1G	19900	3
LAG 10G	1900	2

Стоимость пути для группы каналов по методу long по умолчанию определяется делением стоимости интерфейса на количество линков в группе -100. Значение cost для LAG приведено с учётом членства в нём 2 физических интерфейсов.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 74 — Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show spanning-tree interface { **gigabitethernet** *gi_port* | **twopointfivegigabitethernet** *two_port*| **tengigabitethernet** *te_port*| **port-channel** *group*} **[bpduguard** | **cost** | **detail** | **inconsistency** | **layer2-gateway-port** | **portfast** | **priority** | **restricted-role** | **restricted-tcn** | **rootcost** | **state** | **stats]**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); group: (1..24)	Показатьсостояние протокола STP на интерфейсе.
show spanning-tree detail	-	Показать подробную информацию о настройках протокола STP.
show spanning-tree active [detail]	-	Показать информацию о состоянии о настройках STP на активных портах.
show spanning-tree bridge [address | detail | forward-time| hello-time | id | max-age | priority | protocol]	-	Отобразить настройки STP на bridge.
show spanning-tree layer2-gateway-port	-	Отобразить настройки шлюза 2 уровня.
show spanning-tree pathcost method	-	Отобразить информацию о методе определения стоимости пути.
show spanning-tree root [address| cost | detail | forward-time | id | max-ege | port | priority]	-	Отобразить информацию о root в топологии STP.
show spanning-tree summary	-	Отобразить состояние протокола STP относительно интерфейсов.

4.14.3.2 Настройка протокола MSTP

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 75 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
spanning-tree mst *instance_id* **priority** *priority*	instance_id: (1..63); priority: (0..61440)/32768	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 *instance_id* **flush-indication-threshold** *threshold*	instance_id: (1..63); threshold: (0..65535)/0	Установить пороговое значение TCN BPDU для экземпляра MST, при котором запускается таймер.
spanning-tree mst max-hops *hop_count*	hop_count: (6..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 configuration	-	Вход в режим конфигурации протокола MSTP.

Команды режима конфигурации протокола MSTP

Вид запроса командной строки в режиме конфигурации протокола MSTP:

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

Таблица 76 — 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*).
exit	-	Выход из режима конфигурации протокола MSTP с сохранением конфигурации.

Команды режима конфигурации интерфейса Ethernet, интерфейса группы портов

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

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

Таблица 77 — 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		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**		Устанавливает 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 78.

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 mst *instance_id* **pseudoRootid priority** *priority* **mac-address** *mac_add*	instance_id: (1..63); priority: (0..240)/128	Установить приоритет pseudoroot в экземпляре MSTP.
no spanning-tree mst *instance_id* **pseudoRootid**		Установить значение по умолчанию.
spanning-tree *mst* **instance_id guard {root/none}**	instance_id: (1..63); -/none	Включить или отключить spanning-tree Root Guard в указанном экземпляре MST.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 78 — Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show spanning-tree interface { gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} [bpduguard** | **cost** | **detail** | **inconsistency** | **layer2-gateway-port** | **portfast** | **priority** | **restricted-role** | **restricted-tcn** | **rootcost** | **state** | **stats]**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); group: (1..24)	Показать конфигурацию протокола STP.
show spanning-tree mst instance_id [detail]	instance_id: (1..63)	Показать подробную информацию о настройке протокола STP.
show spanning-tree mst configuration	-	Показать информацию о сконфигурированных экземплярах MSTP.
clear spanning-tree mst *instance_id* **counters {interface { gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***| port-channel** *group***}}**	Instance_id: (1..63); gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); group: (1..24)	Очистка счетчиков STP.

4.14.4 Настройка функции Layer 2 Protocol Tunneling (L2PT)

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

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 79 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
lacp-tunnel-address *multicast-mac-address*	*multicast-mac-address*/ 01:00:0c:cd:cd:d4	Установить адрес назначения для инкапсулированных кадров (frame) соответствующего протокола.
stp-tunnel-address *multicast-mac-address*	*multicast-mac-address*/ 01:00:0c:cd:cd:d0	Установить адрес назначения для инкапсулированных кадров (frame) соответствующего протокола.
lldp-tunnel-address *multicast-mac-address*	*multicast-mac-address*/ 01:00:0c:cd:cd:d8	Установить адрес назначения для инкапсулированных кадров (frame) соответствующего протокола.
isis-l1-tunnel-address *multicast-mac-address*	*multicast-mac-address*/ 01:00:0c:cd:cd:dc	Установить адрес назначения для инкапсулированных кадров (frame) соответствующего протокола.
isis-l2-tunnel-address *multicast-mac-address*	*multicast-mac-address*/ 01:00:0c:cd:cd:dd	Установить адрес назначения для инкапсулированных кадров (frame) соответствующего протокола.
pvst-tunnel-address *multicast-mac-address*	*multicast-mac-address*/ 01:00:0c:cd:cd:df	Установить адрес назначения для инкапсулированных кадров (frame) соответствующего протокола.
vtp-tunnel-address *multicast-mac-address*	*multicast-mac-address*/ 01:00:0c:cd:cd:e0	Установить адрес назначения для инкапсулированных кадров (frame) соответствующего протокола.
ospf-tunnel-address *multicast-mac-address*	*multicast-mac-address*/ 01:00:0c:cd:cd:e1	Установить адрес назначения для инкапсулированных кадров (frame) соответствующего протокола.
rip-tunnel-address *multicast-mac-address*	*multicast-mac-address*/ 01:00:0c:cd:cd:e2	Установить адрес назначения для инкапсулированных кадров (frame) соответствующего протокола.
fctl-l2-tunnel-address *multicast-mac-address*	*multicast-mac-address*/ 01:00:0c:cd:cd:de	Установить адрес назначения для инкапсулированных кадров (frame) соответствующего протокола.
igmp-tunnel-address *multicast-mac-address*	*multicast-mac-address*/ 01:00:0c:cd:cd:db	Установить адрес назначения для инкапсулированных кадров (frame) соответствующего протокола.
vrrp-tunnel-address *multicast-mac-address*	*multicast-mac-address*/ 01:00:0c:cd:cd:e3	Установить адрес назначения для инкапсулированных кадров (frame) соответствующего протокола.

Команды режима конфигурации интерфейсов Ethernet

Вид запроса командной строки в режиме конфигурации интерфейсов Ethernet:

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

Таблица 80 — Команды режима конфигурации интерфейсов Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
l2protocol-tunnel {stp | lacp | lldp | isis-l1 | isis-l2 | fctl | ospf | rip | vtp | pvst | igmp | vrrp}	-/выключено	Включить режим инкапсуляции PDU.
no l2protocol-tunnel {stp | lacp | lldp | isis-l1 | isis-l2 | fctl | ospf | rip | vtp | pvst | igmp | vrrp}		Выключить режим инкапсуляции PDU.

При включении инкаспуляции для VTP инкапсулироваться будет вся группа протоколов с MAC-адресами назначения 01:00:0C:CC:CC:CC.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 81 — Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show l2protocol-tunnel [interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **port-channel** *group***}] | [summary] | [vlan** *vlan_id***]**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); vlan_id: (1..4094); group: (1..24)	Отобразить конфигурацию L2PT суммарно и по отдельным интерфейсам.
show l2protocol tunnel-mac-address	-	Отобразить адреса назначения для инкапсулированных кадров (frame).

4.14.5 Настройка протокола LLDP

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

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

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 82 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
shutdown lldp	-/включено	Отключить работу модуля LLDP на устройстве. **Данная команда отключает работу модуля LLDP с безвозвратным удалением всех настроек блока LLDP.**
no shutdown lldp		Включить работу модуля LLDP на устройстве.
set lldp enable	-/выключено	Разрешить коммутатору использование протокола LLDP.
set lldp disable		Запретить коммутатору использование протокола LLDP.
set lldp version {v1 | v2}	-/v1	Задать версию протокола LLDP.
lldp *mac_address*	-	Указать MAC-адрес, на который будут отсыдаться lldp-кадры. lldp-кадры так же будут дублироваться на стандартный MAC-адрес.
lldp lldpdu flooding	-/filtering	Установить режим фильтрации пакетов LLDP BPDU.
lldp lldpdu filtering		Установить значение по умолчанию.
lldp chassis-id-subtype {chassis-comp *string* **| if-alias | if-name | local** *string* **| nw-addr | port-comp** *string***}**	string: (1..255) символов; -/mac-address	Задать chassis-id-subtype для lldp-кадра.
lldp chassis-id-subtype mac-addr		Вернуть к значению по умолчанию.
lldp reinitialization-delay *delay*	delay: (1..10)/2	Установить задержку повторной инициализации (время задержки, выполняемое LLDP для повторной инициализации на любом интерфейсе). **Чтобы отменить настройку необходимо выставить значение по умолчанию.**
lldp transmit-interval *interval*	interval: (5-32768)/30	Установить интервал передачи lldp-кадров. **Чтобы отменить настройку необходимо выставить значение по умолчанию.**
lldp notification-interval *seconds*	seconds: (5-3600)/5	Установить максимальную скорость передачи lldp-кадров. Seconds – период времени в течении которого устройство может отправить не более одного кадра (frame). **Чтобы отменить настройку необходимо выставить значение по умолчанию.**
lldp tx-delay *value*	value: (8192)/2	Установить минимальную длительность задержки, между последовательными кадрами LLDP. **Чтобы отменить настройку необходимо выставить значение по умолчанию.**
lldp txCreditMax *value*	value: (1..10)	Установить значение Credit Max (максимальное количество последовательных LLDPDU, которые могут быть переданы в любое время).
lldp txFastInit *value*	value: (1..8)	Установить число пакетов, которое будут отправляться в период fast init.

Команды режима конфигурации интерфейсов Ethernet

Вид запроса командной строки в режиме конфигурации интерфейсов Ethernet:

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

Таблица 83 — Команды режима конфигурации интерфейса Ethernet

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

lldp med-app-type *type* **{none | vlan {untagged| vlan-id** *vlan_id***}} {priority** *priority* **| dscp** *dscp***}**	type: (guestVoice, guestVoiceSignaling, softPhoneVoice, streamingVideo, videoconferencing, voice, voiceSignaling); vlan_id: (1..4094); priority: (0-7); dscp: (0-63)	Назначить правило network-policy данному интерфейсу.
no lldp med-app-type *type*		Удалить правило.
lldp med-location {civic-location | coordinate-location | elin-location} location-id {*coordinate civic_address_data | elin_data***}**	-/выключено	Задать местоположение устройства для протокола LLDP (значение параметра location протокола LLDP MED). - **coordinate** – адрес в системе координат; - **civic_address_data** – административный адрес устройства; - **elin_data** – адрес в формате, определенном ANSI/TIA 1057.
no lldp med-location {civic-location | coordinate-location | elin-location}		Удалить местоположение.
lldp med-tlv-select {ex-power-via-mdi | inventory-management | location-id | med-capability | network-policy}	-/выключено	Сконфигурировать TLV LLDP-MED на данном интерфейсе.
no lldp med-tlv-select {ex-power-via-mdi | inventory-management | location-id | med-capability | network-policy}		Удалить настройку TLV LLDP-MED на интерфейсе.
lldp notification {mis-configuration | remote-table-chg} [mac-address *mac_addr***]**	-	Включить отправку трапов по событиям LLDP.
no lldp notification		Отключить отправку трапов по событиям LLDP.
lldp port-id-subtype {if-alias, if-name, mac-addr, local string}	string: (1..255); -/ if-name	Задать ID Port Subtype для кадра LLDP.
no lldp port-id-subtype		Установить значение по умолчанию.
lldp receive [mac-address *mac_addr***]**	-/включено	Разрешить интерфейсу принимать кадры LLDP.
no lldp receive [mac-address *mac_addr***]**		Запретить интерфейсу принимать кадры LLDP.
lldp tlv-select basic-tlv *tlv_list*	tlv_list: (port-descr, sys-capab, sys-descr, sys-name)	Определить какие базовые опциональные TLV-поля будут включены устройством в передаваемый LLDP-пакет.
no lldp tlv-select basic-tlv		Установить значение по умолчанию.
lldp tlv-select {dot1tlv | dot3tlv} *tlv_list*	tlv_list: (link-aggregation, macphy-config, max-framesize)	Определить какие специальные опциональные TLV-поля будут включены устройством в передаваемый LLDP-пакет.
no lldp tlv-select {dot1tlv | dot3tlv}		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.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 84 — Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show lldp local [gigabitethernet *gi_port* **| tengigabitethernet** *te_port***] [mgmt-addr]**	-	Показать LLDP-информацию, которую анонсируют порты.
show lldp neighbors [detail]	-	Показать информацию о соседних устройствах, на которых работает протокол LLDP.
show lldp statistics	-	Показать статистику LLDP.

Таблица 85 — Описание результатов

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

Таблица 86 — Описание результатов

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

Auto-negotiation status	Определяет, включена ли поддержка автоматического определения режима порта.
Auto-negotiation Advertised Capabilities	Определяет режимы, поддерживаемые функцией автоматического определения порта.
Operational MAU type	Рабочий MAU-тип устройства.

Пример настройки TLV-опций на интерфейсе Gigabitethernet 0/1:

```
console(config)# set lldp enable
console(config)# interface gigabitethernet 0/1
console(config-if)# lldp tlv-select basic-tlv port-descr
console(config-if)# lldp tlv-select basic-tlv sys-name
console(config-if)# lldp tlv-select basic-tlv sys-descr
console(config-if)# lldp tlv-select basic-tlv sys-capab
console(config-if)# lldp tlv-select basic-tlv mgmt-addr ipv4 10.0.0.1
console(config-if)# lldp tlv-select dot1tlv port-vlan-id
console(config-if)# lldp tlv-select dot1tlv protocol-vlan-id all
console(config-if)# lldp tlv-select dot3tlv macphy-config
console(config-if)# lldp tlv-select dot3tlv link-aggregation
console(config-if)# lldp tlv-select dot3tlv max-framesize
```

4.15 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)#
```

Настройка Ethernet OAM требуется для отправки snmp-trap по событию Dying Gasp.

Таблица 87 — Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
shutdown ethernet-oam	-/включено	Отключить работу модуля Ethernet OAM на устройстве. **Данная команда отключает работу модуля Ethernet OAM с безвозвратным удалением всех настроек блока OAM.**
no shutdown ethernet-oam		Включить работу модуля Ethernet OAM на устройстве.
shutdown fault-management	-/включено	Отключить работу модуля Fault-management на устройстве. **Данная команда отключает работу модуля Fault-management с безвозвратным удалением всех настроек блока Fault-management.**
no shutdown fault-management		Включить работу модуля Fault-management на устройстве.
ethernet-oam enable	-/выключено	Разрешить работу OAM.
ethernet-oam disable		Запретить работу OAM.
ethernet oam link-monitor frame threshold *count*	count: (1..900)/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..900)/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: (0xffff../123456..)	Установить временной промежуток для события «frame-period».
no ethernet-oam link-monitor frame-period window		Восстановить значение по умолчанию.
ethernet oam link-monitor frame-sec-summary threshold *count*	count: (1..900)/1	Установить порог для события «frame-sec-summary» (период устанавливается командой **Ethernet-oam link-monitor frame-sec-summary window**), в секундах.
no ethernet-oam link-monitor frame-sec-summary threshold		Восстановить значение по умолчанию.
ethernet-oam link-monitor frame-sec-summary window *window*	window: (100..9000)/100 мс	Установить временной промежуток для события «frame-sec-summary».
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 OAM PDU; - **passive** – коммутатор начинает отправлять OAM PDU только при наличии OAM PDU со встречной стороны.
ethernet oam remote-loopback {deny | disable | enable | permit}	-/выключено	Команда для управления поддержкой функции заворота трафика. - **deny** – игнорирует команды loopback; - **disable** – блокирует loopback; - **enable** – включает контроль для loopback; - **permit** – включает обработку loopback.
ethernet-oam uni-directional detection	-/выключено	Включить функцию обнаружения однонаправленных связей на базе протокола Ethernet OAM.
no ethernet-oam uni-directional detection		Восстанавливает значение по умолчанию.
ethernet-oam uni-directional detection action {log|errdisable}	-/log	Определить реакцию коммутатора на однонаправленную связь: - **log** – запись в журнал; - **errdisable** – 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	-/выключено	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 глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 88 — Команды режима глобальной конфигурации

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

Команды режима Privileged EXEC

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

```
console#
```

Таблица 89 — Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show port ethernet-oam	-	Отобразить информацию о текущем состоянии oam.
show port ethernet-oam { gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port*}	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11).	Отобразить информацию о текущем состоянии oam для конкретного интерфейса.
show port ethernet-oam[gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port*] **neighbor**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11).	Отобразить состояние соседствующей конфигурации.
show port ethernet-oam[gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port*] **statistics**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11).	Отобразить статистику OAM для интерфейсов/конкретного интерфейса.
show port ethernet-oam { gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* } event-notifications	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11).	Отобразить OAM настройки порта.
show ethernet-oam global information	-	Отобразить глобальные настройки блока OAM.

Пример настройки Ethernet OAM:

```
console(config)# set ethernet-oam enable
console(config)# interface gigabitethernet 0/1
console(config-if)# ethernet-oam enable
```

4.16 Групповая адресация

4.16.1 Функция посредника протокола IGMP (IGMP Snooping)

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

Поддерживаются версии протокола IGMP – IGMPv1, IGMPv2, IGMPv3.

Функция групповой фильтрации «bridge multicast filtering» включена по умолчанию.

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

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 90 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
shutdown snooping	-/включено	Отключить работу модуля IGMP/MLD Snooping на устройстве. **Данная команда отключает работу модуля IGMP/MLD Snooping с безвозвратным удалением всех настроек блока IGMP/MLD Snooping.**
no shutdown snooping		Включить работу модуля IGMP/MLD Snooping на устройстве.
ip igmp snooping	-/выключено	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)/выключено	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.
snooping authentication	-/выключено	Включить авторизацию IGMP join глобально.
no snooping authentication		Выключить авторизацию IGMP join глобально.
snooping authentication cache-time *timeout*	timeout: (20-10000) /600	Настроить таймаут для cache-таблицы IGMP-авторизации.
no snooping authentication cache-time		Вернуть значение по умолчанию.
ip igmp snooping vlan *vlan_id* **mrouter {gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **port-channel** *group***}**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); group: (1..24);	Определить порт, к которому подключен маршрутизатор многоадресной рассылки для заданного VLAN. - *vlan_id* – идентификационный номер VLAN.

no ip igmp snooping vlan *vlan_id* **mrouter interface {** **gigabitethernet** *gi_port* **|** **twopointfivegigabitethernet** *two_port* **|** **tengigabitethernet** *te_port* **port-channel** *group***}**		Указать, что к порту не подключен маршрутизатор многоадресной рассылки.
ip igmp snooping vlan *vlan_id* **fast-leave**	vlan_id: (1..4094); -/выключено	Включить процесс IGMP Snooping Immediate-Leave на текущей VLAN. Означает, что порт должен быть немедленно удален из группы IGMP после получения сообщения IGMP leave.
no ip igmp snooping vlan *vlan_id* **fast-leave**		Отключить процесс IGMP Snooping Immediate-Leave на текущей VLAN.
ip igmp snooping vlan *vlan_id* **replace source-ip** *ip_addr*	vlan_id: (1..4094)/выключено	Включить подмену коммутатором адреса источника на заданный IP-адрес в пакетах IGMP-report в указанном VLAN. - *ip_addr* – IP-адрес, который будет использоваться для подмены. **Подмена на заданный адрес для транзитного трафика происходит при включенном ip igmp snooping. Подмена на заданный адрес для трафика, исходящего с CPU коммутатора, – при включенном ip igmp snooping и ip igmp snooping proxy-reporting.**
no ip igmp snooping vlan *vlan_id* **replace source-ip**		Выключить подмену коммутатором адреса источника на заданный IP-адрес в пакетах IGMP-report.
ip igmp snooping group-query-interval *value*	value: (2..5)	Установить интервал времени в секундах, после которого устройство отправляет group-query на mrouter.
ip igmp snooping group-query-interval		Установить значение по умолчанию.
ip igmp snooping port-purge-interval *value*	value: (130..1225)	Установить интервал времени в секундах, по истечении которого mrouter удаляется, если не получает IGMP reports.
no ip igmp snooping port-purge-interval		Отключить настройку.
ip igmp snooping query-forward all-ports	-/non-router	Включить отправку query во все порты.
ip igmp snooping query-forward non-router		Включить отправку query в non-router-порты.
ip igmp snooping report-suppression-interval *value*	value: (1..25)/5	Задать интервал (в секундах), для которого IGMPv2 report для одной и той же группы не будут перенаправлены.
no ip igmp snooping report-suppression-interval		Установить значение по умолчанию.
ip igmp snooping retry-count *value*	value: (1..5)	Максимальное количество query, относящихся к группе, отправленных на mrouter.
no ip igmp snooping retry-count		Отключить настройку.
ip igmp snooping send-query enable	-	Разрешить передачу query-пакетов на устройстве.
ip igmp snooping send-query disable		Запретить передачу query-пакетов на устройстве.
ip igmp snooping source-only learning age-timer *interval*	interval: (130..1225)	Установить интервал (в секундах), после которого порт удаляется, если IGMP reports не получены.
no ip igmp snooping source-only learning age-timer		Отключить таймер.
ip igmp snooping filter	-/выключено	Разрешить использование функций фильтрации IGMP на интерфейсах.
no ip igmp snooping filter		Запретить использование функций фильтрации IGMP на интерфейсах.

Команды режима конфигурации VLAN (диапазон VLAN'ов)

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

Таблица 91 — Команды режима конфигурации VLAN

Команда	*Значение/Значение по умолчанию*	*Действие*
ip igmp snooping replace source-ip *ip_addr*	-	Включить подмену коммутатором адреса источника на заданный IP-адрес в пакетах IGMP-report. -*ip_addr* — IP-адрес, который будет использоваться для подмены **Подмена на заданный адрес для транзитного трафика происходит при включенном ip igmp snooping. Подмена на заданный адрес для трафика, исходящего с CPU коммутатора, — при включенном ip igmp snooping и ip igmp snooping proxy-reporting.**
no ip igmp snooping replace source-ip	-	Выключить подмену коммутатором адреса источника на заданный IP-адрес в пакетах IGMP-report.
ip igmp snooping cos *cos*	cos: (0..7)/-	Установить значение 802.1p для IGMP-пакетов, которые будут использоваться коммутатором на интерфейсе VLAN.
no ip igmp snooping cos		Удаляет значение метки 802.1p для IGMP-пакетов на интерфейсе VLAN.
ip igmp snooping version {v1 | v2 | v3}	-/v3	Установить версию протокола IGMP в VLAN.
ip igmp snooping		Установить значение по умолчанию.
ip igmp snooping fast-leave	-/выключено	Включает функцию fast-leave для VLAN.
no ip igmp snooping fast-leave		Выключает функцию fast-leave для VLAN.
ip igmp snooping max-response-code *value*	value: (0..255)	Установить максимальное время ответа на запрос, задающееся в коде, где одна единица кода равна одной десятой секунды.
no ip igmp snooping max-response-code		Установить значение по умолчанию.
ip igmp snooping mrouter { gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***}** **[time-out** *time***]**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); time: (60..600)	Статически настроить порты маршрутизатора для VLAN. - **time-out** – интервал ожидания до очистки порта маршрутизатора для интерфейса VLAN.
no ip igmp snooping mrouter-port { gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***}**		Удалить указанные порты маршрутизатора для VLAN.
ip igmp snooping mrouter-port {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **} version {v1 | v2 | v3}**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11)	Настроить версию IGMP для порта маршрутизатора для VLAN. -**v1** – IGMP snooping Version 1; -**v2** – IGMP snooping Version 2; -**v3** – IGMP snooping Version 3.
no ip igmp snooping mrouter { gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***} version**		Установить версию по умолчанию.
ip igmp snooping multicast-vlan profile *index*	index: (1..4294967295)	Привязать multicast-профиль с заданным индексом к VLAN.
no ip igmp snooping multicast-vlan profile		Удалить привязку к VLAN.
ip igmp snooping querier	-/выключено	Включить поддержку выдачи запросов igmp-query коммутатором во VLAN.
no ip igmp snooping querier		Выключить поддержку выдачи запросов igmp-query коммутатором во VLAN.
ip igmp snooping query-interval *interval*	interval: (60..600)/выключено	Установить таймаут, по которому система отправляет основные запросы всем участникам группы многоадресной передачи для проверки их активности.

no ip igmp snooping query-interval		Установить значение по умолчанию.
ip igmp snooping sparse-mode enable	-/выключено	Включить режим фильтрации незарегистрированного трафика в VLAN.
ip igmp snooping sparse-mode disable		Отключить режим фильтрации незарегистрированного трафика в VLAN.
ip igmp snooping static-group *ip_addr* **[ports** *ports***]**	-	Создать статическую запись в таблице групповой адресации.
no ip igmp snooping static-group *ip_addr*		Удалить статическую запись из таблицы групповой адресации.
ip igmp snooping blocked-router {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **port-channel group}**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); group: (1..24);	Включить отбрасывание Query на интерфейсе.
no ip igmp snooping blocked-router {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **port-channel group}**		Выключить отбрасывание Query на интерфейсе.

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet

Вид запроса командной строки режима конфигурации интерфейса:

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

Таблица 92 — Команды режима конфигурации интерфейса Ethernet

Команда	***Значение/Значение по умолчанию***	***Действие***
switchport multicast-tv vlan *vlan_id* **[tagged]**	vlan_id: (1..4094)	Включить перенаправление IGMP-запросов из клиентских Vlan в Multicast Vlan и мультикастового трафика в клиентские Vlan в нетегированном виде. - **tagged** – Включить перенаправление IGMP-запросов из клиентских Vlan в Multicast Vlan и мультикастового трафика в клиентские Vlan для интерфейса в тегированном виде.
no switchport multicast-tv vlan		Выключить перенаправление IGMP-запросов с клиентских Vlan в Multicast Vlan и мультикастового трафика в клиентские Vlan для интерфейса в режиме «access».
ip igmp snooping limit groups *limit*	-/выключено	Установить ограничение по количеству групп на интерфейсе. **Для работы требуется команда ip igmp snooping filter.**
no ip igmp snooping limit		Снять ограничение на количество групп.
ip igmp snooping filter-profileId *filter-id*	-/выключено	Включить фильтрацию по *filter-id* на интерфейсе.
no ip igmp snooping filter-profileId		Отключить фильтрацию по *filter-id* на интерфейсе.
ip igmp snooping leavemode {exp-hosttrack | fastleave | normalleave}	-/normalleave	Установить режим leave на интерфейсе. **- exp-hosttrack** – с отслеживаение хостов; **- fastleave** – удаление сразу после получение leave; **- normalleave** – режим по умолчанию. Для работы требуется команда **snooping leave-process config-level port.**
ip igmp snooping trusted	-/выключено	Включить режим доверия IGMP Snooping на интерфейсе. На доверенный интерфейс не распространяется действие команд **ip igmp snooping proxy-reporting** и **ip igmp snooping replace source-ip.**
no ip igmp snooping trusted		Выключить режим доверия на интерфейсе.
ip igmp snooping authentication radius [required]	-/выключено	Включить IGMP-авторизацию на интерфейсе. **- required** – запретить обработку IGMP join при недоступности RADIUS-сервера.

no ip igmp snooping authentication		Вернуть значение по умолчанию.
ip igmp snooping authentication forward-first	-/выключено	Включить опцию forward-first, при которой IGMP join будут обрабатываться перед их авторизацией на сервере.
no ip igmp snooping authentication forward-first		Вернуть значение по умолчанию.
ip igmp sn authentication exception mcast profile *profile*	-	Привязать multicast-профиль для IGMP-авторизации на интерфейс.
no ip igmp sn authentication exception mcast profile		Вернуть значение по умолчанию.

Пример настройки подписки на статические группы

```
console# configure terminal
console(config)# vlan 10
console(config-vlan)#  vlan active
console(config-vlan)# ip igmp snooping static-group 232.0.0.1
console(config)# ip igmp snooping
console(config)# ip igmp snooping proxy-reporting
```

Пример настройки MVR

В примере gigabitethernet 0/1 - mrouter-port, gigabitethernet 0/1 - клиентский порт

```
console(config)# vlan 10,100
console(config-vlan)# vlan active
console(config-vlan)# exit
console(config)# ip mcast profile 1
console(config-profile)# permit
console(config-profile)# range 232.0.0.1 232.0.0.5
console(config-profile)# profile active
console(config-profile)# exit
console(config)# snooping multicast-forwarding-mode ip
console(config)# ip igmp snooping
console(config)# ip igmp snooping vlan 100
console(config)# ip igmp snooping multicast-vlan enable
console(config)# vlan 100
console(config-vlan)# ip igmp snooping multicast-vlan profile 1
console(config)# interface gigabitethernet 0/1
console(config-if)# switchport mode trunk
console(config-if)# exit
console(config)# interface gigabitethernet 0/1
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 10
console(config-if)# switchport multicast-tv vlan 100
console(config-if)# exit
```

Команды режима EXEC

Все команды доступны только для привилегированного пользователя.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 93 — Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip igmp snooping mrouter	-	Показать информацию об изученных многоадресных маршрутизаторах в указанной группе VLAN.

show ip igmp snooping groups	-	Показать информацию об изученных многоадресных группах, участвующих в групповой рассылке.
clear ip igmp snooping groups [vlan *vlan-id***]**	vlan_id: (1..4094)	Очистить таблицу групп полностью или в указанном VLAN.
show ip igmp snooping authentication cache [interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***}]**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); group: (1..24)	Просмотр cache-таблицы IGMP-авторизации.

4.16.2 Правила групповой адресации (multicast addressing)

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 94 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip igmp snooping multicast-vlan enable	-/выключено	Включить функцию групповой фильтрации.
ip igmp snooping multicast-vlan disable		Выключить функцию групповой фильтрации.
snooping multicast-forwarding-mode ip	-/mac	Настраивает режим обработки multicast-трафика по IP-адресу. **В данном режиме часть multicast-трафика перехватывается устройством на CPU.**
snooping multicast-forwarding-mode mac		Настраивает режим обработки multicast-трафика по MAC-адресу.
snooping leave-process config-level port	-/vlan	Определяет уровень конфигурации механизмов обработки отпуска (конфигурации на основе VLAN или на основе порта).
snooping leave-process config-level vlan		Установить значение по умолчанию.
snooping report-process config-level all-ports	-/non-router-ports	Указывает на каких портах обрабатываются полученные IGMP report от хоста. IGMP report могут обрабатываться на всех портах или на портах, которые не являются mrouter-портами.
snooping report-process config-level non-router-ports		Установить значение по умолчанию.

4.16.3 MLD snooping – протокол контроля многоадресного трафика в IPv6

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 95 — Команды глобального режима конфигурации

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

Команды режима конфигурации VLAN (диапазон VLAN'ов)

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

Таблица 96 — Команды режима конфигурации VLAN

Команда	*Значение/Значение по умолчанию*	*Действие*
ipv6 mld snooping mrouter { gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **}**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11)	Привязать порт отслеживающего маршрутизатора MLD к VLAN.
no ipv6 mld snooping mrouter {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **}**		Удалить порт отслеживающего маршрутизатора MLD из VLAN.
ipv6 mld snooping version {v1 | v2}	-/v2	Настроить версию отслеживания MLD в VLAN. - **v1** — MLD snooping Version 1; - **v2** — MLD snooping Version 2.
ipv6 mld snooping version		Установить значение по умолчанию.

Команды режима EXEC

Все команды доступны только для привилегированного пользователя.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 97 — Команды режима EXEC

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

4.16.4 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 98 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip mcast profile *index [description]*	index: (1..4294967295); description: (1..128) символов	Создать multicast-профиль и перейти в режим его конфигурирования.
no ip mcast profile *index*		Удалить multicast-профиль.

Команды режима конфигурации multicast-профиля

Вид запроса командной строки в режиме конфигурации multicast-профиля:

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

Таблица 99 — Команды режима конфигурации multicast-профиля

Команда	*Значение/Значение по умолчанию*	*Описание*
range *first_group_ip last_group_ip*	-	Задать диапазон адресов-источников multicast-трафика. Если задать только один адрес, он станет единственным источником мультикаста.
no range *first_group_ip last_group_ip*		Удалить диапазон адресов-источников multicast-трафика.
permit	-/deny	В случае несоответствия одному из заданных диапазонов, IGMP-report будут пропускаться.
deny		В случае несоответствия одному из заданных диапазонов, IGMP-report будут отбрасываться.
profile active	-	Активировать работу профиля.
no profile active		Деактивировать работу профиля.

Команды режима конфигурации VLAN

Вид запроса командной строки в режиме конфигурации VLAN:

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

Таблица 100 — Команды режима конфигурации VLAN

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

4.16.5 Конфигурация 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.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 101 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
set ip igmp enable	-/выключено	Включить модуль IGMP глобально.
set ip igmp disable		Выключить модуль IGMP глобально.
ip igmp proxy-service	-/выключено	Включить функцию IGMP proxy глобально.
no ip igmp proxy-service		Выключить функцию IGMP proxy глобально.

Команды режима конфигурации интерфейсов VLAN

Вид запроса командной строки в режиме конфигурации интерфейсов VLAN:

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

Таблица 102 — Команды режима конфигурации интерфейсов VLAN

Команда	*Значение/Значение по умолчанию*	*Действие*
set ip igmp enable	-/выключено	Включить модуль IGMP на интерфейсе. Интерфейс получает роль Downstream для функции IGMP proxy.
set ip igmp disable		Выключить модуль IGMP на интерфейсе.
ip igmp-proxy mrouter	-/выключено	Определить роль Upstream для интерфейса IGMP proxy.
no ip igmp-proxy mrouter		Убрать роль Upstream с интерфейса.
ip igmp-proxy mrouter-version *version*	version (1..3)/3	Установить версию IGMP на Upstream-интерфейсе.
ip igmp-proxy mrouter-time-out *timeout*	timeout (60...600)с/125	Установить таймер mrouter purge, после истечения которого версия IGMP на Upstream-интерфейсе сменится на сконфигурированную командой ip igmp-proxy mrouter-version. Таймер перезапускается каждый раз после получения Query на Upstream-интерфейс.
ip igmp immediate-leave	-/выключено	Включить функцию IGMP fast-leave на Downstream-интерфейсе.
no Ip igmp immediate-leave		Выключить функцию IGMP fast-leave на Downstream-интерфейсе.
ip igmp explicit-tracking	-/выключено	Включить функцию отслеживания клиентов для быстрого удаления подписки при получении IGMP leave на Downstream-интерфейсе.
no ip igmp explicit-tracking		Выключить функцию отслеживания клиентов для быстрого удаления подписки при получении IGMP leave на Downstream-интерфейсе.
Ip igmp query-interval *interval*	interval (30...31744)с/125с	Установить интервал отправки IGMP General Query на Downstream-интерфейсе.
no Ip igmp query-interval		Вернуть интервал отправки IGMP General Query на Downstream-интерфейсе по умолчанию.
ip igmp last-member-query-interval *value*	value (1-255)мс/10мс	Установить значение в мс last-member-query-interval в сообщениях IGMP group specific query.
no ip igmp last-member-query-interval		Вернуть значение last-member-query-interval в сообщениях IGMP group specific query по умолчанию.
ip igmp query-max-response-time *value*	value (1-255)мс/100мс	Установить значение max-response-time в сооб0щениях IGMP general query.
no ip igmp query-max-response-time		Вернуть значение max-response-time в сообщениях IGMP general query по умолчанию.
ip igmp robustness *robustness*	robustness (2..7)/2	Установить значение парамета устойчивости IGMP.
no ip igmp robustness		Вернуть значение устойчивости IGMP по умолчанию.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 103 — Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip igmp-proxy mrouter [vlan *vlan-id* **]**	vlan-id: (1..4094)/-	Просмотр информации об Uplink-интерфейсах.
show ip igmp-proxy forwarding-database [vlan*vlan-id* **| group** *group-ip* **| source** *source-ip***]**	vlan-id: (1..4094) group-ip: multicast ip-address source-ip: unicast ip-address/-	Просмотр информации о получаемых группах и наличии подписок для них.
show ip igmp global-config	-/-	Просмотр информации о глобальном состоянии модуля IGMP и функции IGMP proxy.
show ip igmp groups	-/-	Просмотр информации об активных подписках на группы.
show ip igmp interface [vlan *vlan-id***]**	vlan-id: (1..4094)/-	Просмотр информации о состоянии модуля IGMP на интерфейсах.
show ip igmp statistics [vlan *vlan-id***]**	vlan-id: (1..4094)/-	Просмотр статистики модуля IGMP на интерфейсах.

4.17 Функции управления

4.17.1 Механизм AAA

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

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

Для шифрования данных используется *механизм SSH.*

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 104 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
enable password [level *level***]** *password*	level: (1..15)/1; password: (5..20) символов	Установить пароль для контроля изменения привилегий доступа пользователей. - **level** – уровень привилегий; - **password** – пароль. **Включающий в себя спецсимволы пароль требуется указывать в кавычках.**
no enable [level *level***] password**		Удалить пароль для соответствующего уровня привилегий.

username *name* **password** ***password*** **[privilege** ***level*****]**	name: (1..20) символов; password: (5..20) символов; level: (1..15)	Добавить пользователя в локальную базу данных. - **level** – уровень привилегий; - **password** – пароль; **Включающий в себя спецсимволы пароль требуется указывать в кавычках.** - **name** – имя пользователя.
no username *name*		Удалить пользователя из локальной базы данных.
aaa authorization command *level* **tacacs [local]**	level: (1..15)/выключено	Разрешить авторизацию команд пользователей. - **level** – уровень привилегий пользователей. **В текущей версии ПО при локальной авторизации разрешены все команды.**
no aaa authorization command *level*		Установить значение по умолчанию.
aaa authentication mode {chain | break}	-/break	Установить алгоритм действий при невозможности аутентификации на сервере. **- break** – переход к следующему в списке серверу происходит только при недоступности предыдущего сервера. **- chain –** переход к следующему серверу возможен при недоступности сервера или при отказе в аутентификации.
aaa authentication default {[local | radius | tacacs | none]}	-/local	Настроить целевые серверы AAA для списка аутентификации по умолчанию.
aaa authentication user-defined *list* **{[local | radius | default | none]}**	list: (3..32) символов/-	Настроить пользовательский список серверов для аутентификации.
no aaa authentication list *list*		Удалить пользовательский список серверов для аутентификации. Список нельзя удалить, если он привязан к терминалу.
ip http authentication login *list*	list: (3..32) символов/default	Задать список с методами аутентификации при входе через web.
no ip http authentication login		Установить значение по умолчанию.
aaa authentication dot1x default {group radius | local}	-/local	Установить базу данных, к которой нужно обращаться при аутентификации клиента dot1x.
no aaa authentication dot1x default		Установить значение по умолчанию.

Таблица 105 — Атрибуты сообщений ведения учета протокола RADIUS для сессий управления

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

Таблица 106 — Атрибуты сообщений ведения учета протокола RADIUS для сессий 802.1x

Атрибут	*Наличие атрибута в сообщении Start*	*Наличие атрибута в сообщении Stop*	*Описание*
User-Name (1)	Есть	Есть	Идентификация пользователя.
NAS-IP-Address (4)	Есть	Есть	IP-адрес коммутатора, который используется для сессий с Radius-сервером.
NAS-Port (5)	Есть	Есть	Порт коммутатора, на котором подключился пользователь.
Class (25)	Есть	Есть	Произвольное значение, включенное во все сообщения учета сессий.
Called-Station-ID (30)	Есть	Есть	IP-адрес коммутатора.
Calling-Station-ID (31)	Есть	Есть	IP-адрес пользователя.
Acct-Session-ID (44)	Есть	Есть	Уникальный идентификатор учета.
Acct-Authentic (45)	Есть	Есть	Указывает метод, по которому клиент должен быть аутентифицирован.
Acct-Session-Time (46)	Нет	Есть	Показывает, как долго пользователь был подключен к системе.
Acct-Terminate-Cause (49)	Нет	Есть	Причина закрытия сессии.
Nas-Port-Type (61)	Есть	Есть	Показывает тип порта клиента.

Команды режима конфигурации терминала

Вид запроса командной строки в режиме конфигурации терминала:

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

Таблица 107 — Команды режима конфигурации терминала

Команда	*Значение/Значение по умолчанию*	*Действие*
aaa authentication login *list*	list: (3..32) символов/default	Задать список с методами аутентификации при входе для консоли, Telnet, SSH.
no aaa authentication login		Установить значение по умолчанию.
aaa authentication enable *list*	list: (3..32) символов/default	Задать список с методами аутентификации при повышении уровня привилегий для консоли, Telnet, SSH.
no aaa authentication enable		Установить значение по умолчанию.
aaa authorization command {tacacs | local}	-/выключено	Разрешить авторизацию команд для консоли, Telnet, SSH.
no aaa authorization command		Установить значение по умолчанию.

4.17.2 Протокол RADIUS

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

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 108 — Команды режима глобальной конфигурации

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

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 109 — Команды режима Privileged EXEC

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

4.17.3 Протокол TACACS+

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

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

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 110 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
tacacs-server host {*ip_address* **|***hostname***}** **[single-connection] [port** *port***]** **[timeout** *timeout***]** **[key** *secret_key***]**	hostname: (1..63) символов; port: (0..65535)/49; timeout: (1..30) сек; secret_key: (0..128) символов	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; При настройке сервера: «**tacacs-serverhost** *ip_address* **key** *secret_key»* автоматически включается accounting.
no tacacs-server host {*ip_address***|** *hostname***}**		Удалить указанный сервер из списка используемых TACACS-серверов.
tacacs-server retransmit *number*	number: (1..5)/2	Указать количество активных TACACS-серверов, к которым будет поочередно подключиться клиент, в случае неудачной аутентификации.
no tacacs-server retransmit		Удалить настройку.
tacacs use-server address {*ip_address* **|***hostname***}**	-	Выбрать сервер из таблицы серверов для Tacacs-клиента.
no tacacs use-server		Отменить использование заданного сервера.
tacacs authentication type {ascii | pap }	-/pap	Определить метод аутентификации с помощью tacacs.
tacacs attributes port {console | ssh | telnet} *identifer*	identifer (1..255) символов / шаблоны %n %%	Установить атрибута **port** в формате свободной строки определенной пользователем. Возможно использование шаблонов. - %n – номер линии, соответствующий выводу команды show users; -%% – символ %.
no tacacs attributes port {console | ssh | telnet}		Установить значения по умолчанию.

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 111 — Команды режима Privileged EXEC

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

4.17.4 Списки доступа ACL для управления устройством

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 112 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
authorized-manager ip-source {*ipv4_addr* **[***mask* **|** */ ipv4_prefix***] |** ipv6_addr **[**ipv6_prefix**]} [interface** *interface_list***] [vlan** *vlan_list***] [service [snmp] [telnet] [http] [https] [ssh]]**	ipv4_prefix: (0..32); ipv6_prefix: (1..128) vlan_id: (1..4094)	Ограничить управление устройством по заданному фильтру доступа.
no authorized-manager ip-source {*ipv4_addr* **[***mask***] /** *ipv4_prefix***] |** *ipv6_addr* **[***ipv6_prefix***]}**		Отменить ограничение на управление устройством.

На устройстве можно сконфигурировать не больше 100 правил. По умолчанию, если не задано ни одно правило, управление устройством доступно с любого источника.

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

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 113 — Команды режима Privileged EXEC

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

4.17.5 Настройка протоколов управления

4.17.5.1 Telnet, SSH

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 114 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ssh enable	-/включено	Разрешить удаленное конфигурирование устройства через SSH.
ssh disable		Запретить удаленное конфигурирование устройства через SSH.
ssh server-address *ip_addr* **port** *port*	port: (1..65535)	Задать IP-адрес SSH-сервера и TCP-порт, используемый SSH-сервером.
ip ssh mac [hmac-md5 | hmac-sha1]	-/hmac-sha1	Выбрать тип аутентификации по протоколу SSH.
ip ssh cipher [3des-cbc | aes128-cbc | aes128-ctr | aes192-cbc | aes192-ctr | aes256-cbc | aes256-ctr | des-cbc | all]	-/3des-cbc	Выбрать шифр аутентификации по протоколу SSH.
crypto key generate rsa	-	Сгенерировать пару ключей RSA – частный и публичный для SSH-сервиса.
feature telnet	-/включено	Разрешить конфигурирование устройства через Telnet.
no feature telnet		Запретить конфигурирование устройства через Telnet.
ip ssh authorized-key	-	Задать ключ ssh-авторизации, при помощи которого можно установить защищенное соединение.
no ip ssh authorized-key		Удалить ключ ssh-авторизации.
ip ssh auth-type {password | publickey}	- /password	Задать последовательность методов аутентификации по ssh.
no ip ssh auth-type		Установить значение по умолчанию.

Команды режима EXEC

Команды данного раздела доступны только для привилегированных пользователей.

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 115 — Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip ssh	-	Показать конфигурацию SSH-сервера, а также активные входящие SSH-сессии.
show telnet server	-	Отобразить статус сервера Telnet.
sh ip ssh authorized-keys	-	Отобразить сконфигурированные ключи.

4.17.5.2 Настройка параметров протокола SNMP для доступа к устройству

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.

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 116 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
snmp notify *notify_name* **tag** *tag_name* **type {trap | inform}**	notify_name: (1..32) символа; tag_name: (1..32) символа -/выключено	Активировать отправку трапов по событию login/logout.
snmp notify *notify_name*		Отключить отправку трапов по событию login/logout.
snmp-server enable traps dry-contacts	-/выключено	Активировать отправку трапов по событию замыкания/ размыкания сухих контактов.
no snmp-server enable traps dry-contacts		Отключить отправку трапов по событию замыкания/ размыкания сухих контактов.
snmp enable traps coldstart	-/включено	Активировать отправку трапов по событию 'жесткой' перезагрузки.
no snmp enable traps coldstart		Отключить отправку трапов по событию 'жесткой' перезагрузки.
snmp enable traps warmstart	-/включено	Активировать отправку трапов по событию перезагрузки по команде 'reload'.
no snmp enable traps warmstart		Отключить отправку трапов по событию перезагрузки по команде 'reload'.
snmp user *user_name* **[auth {md5 | sha} [encrypted] passwd [priv {DES | AES_CFB128 [encrypted] passwd | None}]] {EngineID** *EngineID***}**	user_name: (1..32) символов	Создать SNMP-пользователя. - **auth** – настройка алгоритма аутентификации; - **priv** – настройка шифрования; - **EngineID** – идентификатор SNMP-устройства **Включающее в себя спецсимволы user_name требуется указывать в кавычках.**
no snmp user *name*		Удалить SNMP-пользователя.
snmp community index *index* **name [encrypted]** *name* **security** *user_name* **[context** *name***] [transporttag** *TransportTagIdentifier* **| none] [contextengineid** *ContextEngineID***]**	index: (1..32) символов; user_name: (1..32) символов ; TransportTagIdentifier: (1..255) символов;	Привязать сообщество с заданным индексом к ранее созданному пользователю. Чтобы разрешить использование любого специального символа в названии и индексе сообщества, укажите его в двойных кавычках. Если название и индекс сообщества содержат только буквы и цифры, тогда двойные кавычки не нужны. **Включающее в себя спецсимволы community требуется указывать в кавычках.**
no snmp community index *index*		Удалить SNMP-сообщество с указанным индексом.
snmp group *group_name* **user** *user_name* **security-model {v1 | v2c |v3}**	user_name: (1..32) символов; group_name: (1..32) символов	Создать SNMP-группу или таблицу соответствий SNMP-пользователей и правил обозрений SNMP.
no snmp group *group_name* **user** *user_name* **security-model {v1 | v2c |v3}**		Удалить SNMP-группу.
snmp access *group_name* **{v1 | v2c |v3} {auth | noauth | priv}} [read** *view* **| none] [write** *view* **| none] [notify** *view* **| none] [context** *context***)]**	group_name: (1..32) символов; view: (1..32) символов; context: (1..32) символов	Разрешить SNMP-группе доступ на чтение, запись и отправку snmp-трапов по объектам, принадлежащим read/write/notify-view.
no snmp access *group_name* **{v1 | v2c |v3 {auth | noauth | priv}}[context <string(32)>]**		Запретить SNMP-группе доступ на чтение, запись и отправку snmp-трапов по объектам, принадлежащим read/write/notify-view.

snmp view *view_nameOID* **{included | excluded}** **snmp view** *view_name OIDTree* **[mask** *OIDMask***] {included | excluded}**	view_name: (1..32) символов	Создать или редактировать правило обозрения для SNMP-разрешающее правило либо ограничивающее серверу-обозревателю доступ к OID. - *OID* – идентификатора обекта MIB, предствленный в виде дерева ASN.1 - **included** – OID включена в правило для обозревания; - **excluded** – OID исключена в правило для обозревания.
snmp view *view_name OID*		Удалить правило обозрения для SNMP.
snmp targetaddr *targetAddr* **param** *targetParamIP_addr* **taglist** *tagList* **snmp targetaddr** *target_address* **param** *param_name* **{***ucast_addr* **|** *IP6Address* **|** *dns_host_name***} [timeout** *seconds***] [retries** *rRetry_Ccount***] [taglist** *tag_Identifier* **| none] [port** *port_number***]**	target_addr: (1..32) символов; param_name: (1..32) символов; tagList: (1..255) символов seconds: (1..1500) символов; retry_count: (1..3) символов; port_number**:** (1..65535) символов; tag_Identifier: (1..255) символов	Создать группу адресов, на которые будут отправляться трапы согласно параметрам тег-листа.
no snmp targetaddr *targetAddr*		Удалить группу адресов, на которые будут отправляться трапы согласно параметрам тег-листа.
snmp targetparams *target_param* **user** *user_name param* **security-model {v1 | v2c | v3 {auth | noauth | priv}} message-processing {v1 | v2c | v3} [filterprofile-name** *profile_name***]**	user_name: (1..32) символов; target_param: (1..32) символов; profile_name: (1..32)	Указать параметры отправки трапов, определяемые пользоваелем.
no snmp targetparams *target_param*		Удалить параметры отправки трапов, определяемые пользоваелем.

4.17.5.3 Команды конфигурации терминала

Команды конфигурации терминала служат для настройки параметров работы терминалов.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 117 — Команды режима глобальной конфигурации

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

Команды режима конфигурации терминала

Вид запроса командной строки в режиме конфигурации терминала:

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

Таблица 118 — Команды режима конфигурации терминала

Команда	*Значение/Значение по умолчанию*	*Действие*
exec-timeout *seconds*	seconds: (1..18000)/1800 сек	Задать интервал, в течение которого система ожидает ввода от пользователя. Если в течение данного интервала пользователь ничего не вводит, то консоль отключается.
no exec-timeout		Установить значение по умолчанию.
speed {4800 | 9600 | 19200 | 38400 | 57600 | 115200}	(4800, 9600, 19200, 38400, 57600, 115200)/ 115200 бит/с	Установить скорость передачи для последовательного интерфейса.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 119 — Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show line exec-timeout	-	Показать значения параметра exec-timeout для всех терминалов.
show line exec-timeout current	-	Показать значения параметра exec-timeout для текущей сессии.

4.18 Журнал аварий, протокол SYSLOG

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

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 120 — 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-server facility {*facility***} severity {***severity***} {ipv4 | ipv6}** *ip_address*	facility:(local0...local7), severity:(0...7), ipv4_address *A.B.C.D,* ipv6_address: X:X:X:X:X:X:X:X/-	Включить передачу аварийных и отладочных сообщений на удаленный SYSLOG-сервер. - *ip_address* – IPv4- или IPv6-адрес SYSLOG-сервера; **Если команда введена без указания facility, то будет использован текущий настроенный facility.** **Если команда введена без указания severity, то будут указаны все severity, кроме debugging.**

no logging-server facility {*facility*} **severity** {*severity*} **{ipv4 | ipv6}** *ip_address*		Удалить выбранный сервер из списка используемых SYSLOG-серверов. **Если команда введена без указания facility, то будет указан текущий facility.** **Если команда введена без указания severity, то будут использованы все severity, включая debugging.**
logging console	-/включено	Включить передачу аварийных или отладочных сообщений на консоль.
no logging console		Выключить передачу аварийных или отладочных сообщений на консоль.
logging buffered *size*	size: (1..200)50	Изменить количество сообщений, запоминаемых во внутреннем буфере. Новое значение размера буфера применится после перезагрузки устройства.
no logging buffered		Установить значение по умолчанию.
syslog file {1 | 2 | 3} *filename*	filename: (1..32)/-	Создать файл записи аварийных и отладочных сообщений.
no logging-file [*facility***] [***severity***] file {1 | 2 | 3}**	facility:(local0...local7), severity:(0...7),	Выключить передачу аварийных или отладочных сообщений в файл журнала. **Если команда введена без указания facility, то будет указан текущий facility.** **Если команда введена без указания severity, то будут использованы все severity, включая debugging.**
logging-file [*facility***] [***severity***] file {1 | 2 | 3}**		Включить передачу аварийных или отладочных сообщений выбранного уровня важности в указанный файл журнала. **Если команда введена без указания facility, то будет указан текущий facility.** **Если команда введена без указания severity, то будут использованы все severity, кроме debugging.**
logging severity *severity*	severity:(0...7)/6	Задать уровень логирования.
no logging severity		Установить значение по умолчанию.
logging facility *facility*	facility:(local0...local7)/local0	Задать категорию логирования.
no logging facility		Установить значение по умолчанию.
syslog localstorage	-/включено	Активировать отправку аварийных или сообщений на сконфигурированные файлы записи.
no syslog localstorage		Установить значение по умолчанию.
logging hostname-format [hostname | ip | ipv6 | string *string* **]**	string: (1..128) -/нет	Задать параметр, который будет использоваться в качестве идентификатора хоста в SYSLOG-сообщениях.
no logging hostname-format		Использовать значение по умолчанию.

Каждое сообщение имеет свой уровень важности. В таблице 133 приведены типы сообщений в порядке убывания их важности.

Таблица 121 — Типы важности сообщений

Важность сообщений	***Тип важности сообщений***	***Описание***
0	Чрезвычайные (emergencies)	В системе произошла критическая ошибка, система может работать неправильно.
1	Сигналы тревоги (alerts)	Необходимо немедленное вмешательство в систему.
2	Критические (critical)	В системе произошла критическая ошибка.
3	Ошибочные (errors)	В системе произошла ошибка.
4	Предупреждения (warnings)	Предупреждение, неаварийное сообщение.
5	Уведомления (notifications)	Уведомление системы, неаварийное сообщение.

6	Информационные (informational)	Информационные сообщения системы.
7	Отладочные (debugging)	Отладочные сообщения, предоставляют пользователю информацию для корректной настройки системы.

Пример настройки logging-file:

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

```
console(config)# syslog filename-one sl1
console(config)# logging-file sl1
```

Пример настройки logging-server:

Укажем адрес syslog-сервера, куда будут отправляться сообщения о событиях с важностью от чрезвычайных до информационных.

```
console(config)# logging-server ipv4 192.168.1.1
```

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 122 — Команда режима Privileged EXEC для просмотра файла журнала

Команда	*Значение/Значение по умолчанию*	*Действие*
clear logs	-	Удалить все сообщения из внутреннего буфера.
show logging-file	-	Отобразить настройки логирования в локальные файлы.
show logging file *file_name*	file_name: (1..3)	Отобразить состояние журнала, аварийные и отладочные сообщения, записанные в файле
show logging-servers	-	Отобразить настройки для удалённых logging-серверов.

4.19 Зеркалирование (мониторинг) портов

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

Возможно зеркалирование любого количества интерфейсов. Отсутствие потерь гарантируется, если пропускная способность интерфейса назначения не превышена. При использовании физических петель на коммутаторе зеркалироваться будет только одна копия кадра (frame), если замкнутые интерфейсы принадлежат одному VLAN.

К контролирующему порту применяются следующие ограничения:

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

К контролируемым портам применяются следующие ограничения:

- Порт не может быть контролирующим и контролируемым портом одновременно.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 123 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
monitor session *session_id* **destination interface [gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port]*	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); session_id: (1..4)	Указать зеркалирующий порт для выбранной сессии мониторинга. **Функция мониторинга может быть настроена на четырёх портах одновременно.**
no monitor session *session_id* **destination**		Выключить функцию мониторинга на настраиваемом интерфейсе.
monitor session *session_id* **destination remote vlan** *vlan_id*	vlan_id: (1..4094); session_id: (1..4)	Указать служебный vlan для зеркалирования трафика с заданного рефлектор-порта для выбранной сессии. remote vlan – служебный vlan для зеркалирования трафика;
no monitor session *session_id* **destination remote vlan** *vlan_id*		Выключить функцию мониторинга на настраиваемом интерфейсе.
monitor session *session_id* **source interface [gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***] [rx | tx | both]**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); session_id: (1..4)	Добавить указанный зеркалируемый порт для выбранной сессии мониторинга. **- rx** – копировать пакеты принятые контролируемым портом; **- tx** – копировать пакеты, переданные контролируемым портом; **- both** – копировать все пакеты с контролируемого порта.
no monitor session *session_id* **source interface [gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***]**		Выключить функцию мониторинга на настраиваемом интерфейсе.
monitor session *session_id* **source remote vlan** *vlan_id*	vlan_id: (1..4094); session_id: (1..4)	Указать vlan, с которого будет зеркалироваться трафик с заданного рефлектор-порта для выбранной сессии. При этом сам vlan будет снят.
no monitor session *session_id* **source remote vlan** *vlan_id*		Выключить функцию мониторинга на настраиваемом интерфейсе.

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 124 — Команды, доступные в режиме EXEC

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

Примеры выполнения команд

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

Вывести информацию по контролирующим и контролируемым портам.

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

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

4.20 Функции диагностики физического уровня

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

Для электрических интерфейсов:

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

Для оптических интерфейсов 1G:

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

4.20.1 Диагностика медного кабеля

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console#
```

Таблица 125 — Команды диагностики медного кабеля

Команда	*Значение/Значение по умолчанию*	*Действие*
test cable-diagnostics [**gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port*/ **tengigabitethernet** *te_port*]	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11)	Выполнить виртуальное тестирование кабеля для указанного интерфейса.

При получении сообщения 'Fail to get cable test result for port Gi0/X. Status: 3' рекомендуется проверить media-type интерфейса и состояние интерфейса на удаленной стороне.

4.20.2 Электропитание по линиям Ethernet (PoE)

Коммутатор MES2318U поддерживает электропитание устройств по линии Ethernet в соответствии с рекомендациями IEEE 802.3af (PoE) и IEEE 802.3at (PoE+). Тип распиновки A.

Команды режима глобальной конфигурации

Вид запроса командной строки в режиме глобальной конфигурации:

```
console(config)#
```

Таблица 126 — Команды режима глобальной конфигурации

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

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet

Вид запроса командной строки режима конфигурации интерфейса:

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

Таблица 127 — Команды режима конфигурации интерфейса Ethernet

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

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console#
```

Таблица 128 — Команды режима EXEC

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

show power inline consumption	-	Отобразить характеристики потребления мощности, тока и напряжения.

4.20.3 Протокол UDLD

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

Команды режима конфигурации интерфейса (диапазона интерфейсов) Ethernet

Вид запроса командной строки режима конфигурации интерфейса:

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

Таблица 129 — Команды режима конфигурации интерфейса Ethernet

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

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console>
```

Таблица 130 — Команды режима EXEC

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

4.20.4 Диагностика оптического трансивера

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

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

Команды режима EXEC

Запрос командной строки в режиме EXEC имеет следующий вид:

```
console#
```

Таблица 131 — Команды диагностики оптического трансивера

Команда	*Значение/Значение по умолчанию*	*Действие*
show fiber-ports optical-transceiver [{ gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port*| **tengigabitethernet** *te_port*}]	-	Отобразить результаты диагностики оптического трансивера.

Таблица 132 — Параметры диагностики оптического трансивера

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

Значения результатов диагностики:

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

4.21 Функции обеспечения безопасности

4.21.1 Функции обеспечения защиты портов

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

Функция безопасности *Locked Port* позволяет сохранить список изученных MAC-адресов в файле конфигурации, таким образом, этот список можно восстановить после перезагрузки устройства.

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

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 133 — Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

Команда	*Значение/Значение по умолчанию*	*Действие*
switchport port-security enable	-/выключено	Включить функцию защиты на интерфейсе. Блокирует функцию изучения новых адресов для интерфейса. Пакеты с неизученными MAC-адресами источника отбрасываются.
no switchport port-security enable		Отключить функцию защиты на интерфейсе.
switchport port-security mac-limit	limit: (0..8192)/1	Задать максимальное количество адресов, которое может изучить порт.
no switchport port-security mac-limit		Установить значение по умолчанию.
switchport port-security mode {max-addresses | lock | secure-delete-on-reset | secure-permanent}	-/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 файл текущие динамически изученные адреса, связанные с интерфейсом и запрещает обучение новым адресам и старение уже изученных адресов. - **secure-delete-on-reset** – удаляет текущие динамически изученные адреса, связанные с интерфейсом. Разрешено изучение максимального количества адресов на порту. Повторное изучение и старение запрещены. Адреса сохраняются до перезагрузки. - **secure-permanent** – удаляет текущие динамически изученные адреса, связанные с интерфейсом. Разрешено изучение максимального количества адресов на порту. Повторное изучение и старение запрещены. Адреса сохраняются при перезагрузке.
no switchport port-security mode		Установить значение по умолчанию.
switchport port-security violation [restrict | protect | discard-shutdown]	-/protect	Задать режим реагирования при нарушении безопасности. - **restrict** – в данном режиме при нарушении безопасности отправляется SYSLOG-сообщение на SYSLOG-сервер. - **protect** – в данном режиме оповещения о нарушении безопасности нет. Включает перехват MAC-адресов, которые должны быть отброшены, на CPU, после чего MAC-адреса помечаются как заблокированные и отбрасываются в течении aging-time; - **discard-shutdown** – в данном режиме кадры с неизученными MAC-адресами источника отбрасываются, порт отключается.

4.21.2 Контроль протокола DHCP и опция 82

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

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

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

Опция 82 протокола DHCP (option 82) используется для того, чтобы проинформировать DHCP-сервер о том, от какого DHCP-ретранслятора (Relay Agent) и через какой его порт был получен запрос. Применяется для установления соответствий IP-адресов и портов коммутатора, а также для защиты от атак с использованием протокола DHCP. Опция 82 представляет собой дополнительную информацию (имя устройства, номер порта), добавляемую коммутатором, который работает в режиме DHCP Relay агента, в виде DHCP-запроса, принятого от клиента. На основании данной опции, DHCP-сервер выделяет IP-адрес (диапазон IP-адресов) и другие параметры порту коммутатора. Получив необходимые данные от сервера, DHCP Relay агент выделяет IP-адрес клиенту, а также передает ему другие необходимые параметры.

Таблица 134 — Формат полей опции 82

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

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 135 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip {dhcp| dhcpv6} snooping	-/выключено	Разрешить коммутатору контролирование протокола DHCP.
no ip {dhcp| dhcpv6} snooping		Запретить коммутатору контролирование протокола DHCP.
ip {dhcp| dhcpv6} snooping vlan *vlan_id*	vlan_id: (1..4094)/выключено	Разрешить контролирование протокола DHCP в пределах указанного VLAN.
no ip {dhcp| dhcpv6} snooping vlan *vlan_id*		Запретить контролирование протокола DHCP в пределах указанного VLAN.

ip dhcp snooping verify mac-address	-/включено	Включить верификацию MAC-адреса клиента и MAC-адреса источника, принятого в DHCP-пакете на «недоверенных» портах.
no ip dhcp snooping verify mac-address		Выключить верификацию MAC-адреса клиента и MAC-адреса источника, принятого в DHCP-пакете на «недоверенных» портах.
ip binding port-down action {clear|retain}	-/retain	Определить реакцию коммутатора на падение интерфейса: **- retain** — сохраняет записи в таблице при падении. **- clear** — удаляет все динамические записи, созданные для упавшего интерфейса.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 136 — Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip {dhcp | dhcpv6} snooping	-	Отобразить соответствия из файла (базы) контроля протокола DHCP.
show ip dhcp snooping global	-	Отобразить глобальную настройку DHCP Snooping.
show {ip | ipv6} binding	-	Показать все соответствия из файла (базы) контроля протокола DHCP.
clear {ipv4 | ipv6} binding [*mac_addr vlan_id***]**	vlan_id: (1..4094)	Очистить соответствия из файла (базы) контроля протокола DHCP.

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

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

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

Таблица 137 — Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

Команда	*Значение/Значение по умолчанию*	*Действие*
ip binding limit *limit*	limit (0..1024)	Включить ограничение количества DHCP-клиентов на порту.
no ip binding limit		Выключить ограничение количества DHCP-клиентов на порту.

Установленное ограничение по количеству DHCP-клиентов будет распространяться только на новые записи. Рекомендуется перед настройкой ограничения очистить таблицу клиентов DHCP snooping.

4.21.3 DSLAM Controller Solution (DCS)

С помощью данной функции настраиваются значения идентификаторов интерфейса и ретранслятора при конфигурировании DHCP snooping, DHCPv6 snooping и PPPoE Intermediate Agent. Circuit-id – идентификатор интерфейса, с которого пришел запрос, remote-id – идентификатор ретранслятора, с которого пришел запрос.

При включении функции на интерфейсе circuit-id и remote-id будут вставляться во всех VLAN, на которых включен DHCPv4/v6 snooping, DHCP Relay, PPPoE-IA. При включении в VLAN circuit-id и remote-id будут вставляться только в данном VLAN на всех интерфейсах.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 138 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
dcs information option [dhcp | dhcpv6 | pppoe-ia | dhcp-relay] enable	-/выключено	Включить добавление circuit-id + remote-id для всех опций (т.е. dhcp | dhcpv6 | pppoe-ia | dhcp-relay) либо задать конкретный протокол для вставки remote-id и circuit-id.
dcs information option [dhcp | dhcpv6 | pppoe-ia] disable		Выключить добавление remote-id и circuit-id.
dcs agent-circuit-id user-defined {dhcp | dhcpv6 | pppoe-ia | dhcp-relay} *identifier*	identifier (1..63) символов/шаблон %h%i%v	Установить circuit-id в формате свободной строки, определенной пользователем. Возможно использование шаблонов.
no dcs agent-circuit-id user-defined {dhcp | dhcpv6 | pppoe-ia | dhcp-relay}		Установить значение по умолчанию.
dcs agent-circuit-id format-type {dhcp | dhcpv6 | pppoe-ia | dhcp-relay} [identifier-string] *identifier* **option** *format* **[delimiter** *delimiter***]**	identifier (1..48) символов/формат *spv*, разделитель *std*, identifier *NULL*	Настроить circuit-id согласно рекомендация TR-101. Идентификатор: - **identifier** – произвольная строка без шаблонов. Формат: - **pv** – номер порта и VLAN; - **sp** – номер слота и порта; - **sv** – номер слота и VLAN; - **spv** – номер слота, порта и VLAN. Разделители: - **comma** – “,”; - **dot** – “.”; - **hash** – “#”; - **semi-colon** – “;”; - **slash** – “/”; - **space** – “ ”; - **std** – “slot:port/vlan”.
no dcs agent-circuit-id format-type {dhcp | dhcpv6 | pppoe-ia | dhcp-relay}		Установить значение по умолчанию.
dcs agent-circuit-id suboption-type {dhcpv4 | dhcpv6 | pppoe-ia | dhcp4-relay} {tr-101 | user-defined} [binary] [add-subtypes]	-/tr-101	Установить формат circuit-id. Форматы: - **tr-101** – добавление circuit-id в формате согласно рекомендациям TR-101 - **user-defined** – добавление circuit-id в формате свободной строки с возможностью использования шаблонов. Дополнительные параметры: **- binary** – данный параметр указывает, что числовые шаблоны будут преобразованы в формат HEX. **- add-subtypes** – данный параметр указывает, что в идентификатор будет добавлен дополнительный подтип (2х-байтовый для DHCPv4 и PPPoE и 4х-байтовый для DHCPv6), в котором определяется формат строки (ASCII-0x01, HEX-0x00) и длина идентификатора.
no dcs agent-circuit-id suboption-type {dhcpv4 | dhcpv6 | pppoe-ia | dhcp4-relay}		Установить значение по умолчанию.
dcs remote-agent-id user-defined {dhcp | dhcpv6 | pppoe-ia | dhcp-relay} *identifer*	identifer (1..63) символов/шаблон %m	Установить remote-id в формате свободной строки, определённой пользователем. Возможно использование шаблонов.

no dcs remote-agent-id user-defined {dhcp | dhcpv6 | pppoe-ia | dhcp-relay}		Установить значение по умолчанию.
dcs remote-agent-id suboption-type {dhcpv4 | dhcpv6 | pppoe-ia | dhcp4-relay} user-defined [binary] [add-subtypes]	-/user-defined	Установить формат remote-id Форматы: - **user-defined** – добавление remote-id в формате свободной строки с возможностью использования шаблонов. Дополнительные параметры: **- binary** – данный параметр указывает, что числовые шаблоны будут преобразованы в формат HEX. **- add-subtypes** – данный параметр указывает, что в идентификатор будет добавлен дополнительный подтип (2х-байтовый для DHCPv4 и PPPoE и 4х-байтовый для DHCPv6), в котором определяется формат строки (ASCII-0x01, HEX-0x00) и длина идентификатора.
no dcs remote-agent-id suboption-type {dhcpv4 | dhcpv6 | pppoe-ia | dhcp4-relay}		Установить значение по умолчанию.

Таблица 139 — Шаблоны, доступные для настройки user-defined идентификаторов

Шаблон	***Описание***
%a	IP-адрес. Данный шаблон может быть преобразован в формат HEX. Есть возможность указать номер VLAN с IP-адресом (например, VLAN 2: %a2).
%h	Имя устройства.
%p	Короткое имя порта, например, gi1/0/1.
%P	Длинное имя порта, например, gigabitethernet 1/0/1.
%t	Тип порта, например, gigabitethernet.
%m	MAC-адрес порта в формате H-H-H-H-H-H-H. Данный шаблон может быть преобразован в формат HEX.
%M	MAC-адрес системы в формате H-H-H-H-H-H-H. Данный шаблон можно преобразовать в формат HEX.
%u	Номер юнита. Данный шаблон может быть преобразован в формат HEX.
%s	Номер слота. Данный шаблон может быть преобразован в формат HEX.
%i	ifIndex порта. Данный шаблон может быть преобразован в формат HEX.
%c	MAC-адрес абонентского устройства в формате H-H-H-H-H-H-H. Данный шаблон может быть преобразован в формат HEX.
%v	Идентификатор VLAN. Данный шаблон может быть преобразован в формат HEX.

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

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

Таблица 140 — Команды режима конфигурации интерфейса Ethernet

Команда	***Значение/Значение по умолчанию***	***Действие***
dcs agent-circuit-identifer *circuit_id*	circuit_id: (1..63) символов/шаблон %h%i%v	Установить circuit-id в формате свободной строки, определённой пользователем. Возможно использование шаблонов. Данная настройка имеет приоритет перед аналогичной глобальной настройкой формата circuit-id.
no dcs agent-circuit-identifer		Установить значения по умолчанию.
dcs remote-agent-identifier *remote_id*	remote_id: (1..63) символов/шаблон %m	Установить remote-id в формате свободной строки, определённой пользователем. Возможно использование шаблонов. Данная настройка имеет приоритет перед аналогичной глобальной настройкой формата remote-id.
no dcs remote-agent-identifier		Установить значение по умолчанию.

dcs information option {dhcp | dhcpv6 | pppoe-ia | dhcp-relay} enable	-/выключено	Включить добавление circuit-id + remote-id для конкретного протокола. **Вставка circuit-id/remote-id должна быть отключена глобально.**
dcs information option {dhcp | dhcpv6 | pppoe-ia} disable		Выключить добавление remote-id и circuit-id для конкретного протокола.

Команды режима конфигурации интерфейса L2Vlan

Вид запроса командной строки:

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

Таблица 141 — Команды режима конфигурации интерфейса L2Vlan

Команда	*Значение/Значение по умолчанию*	*Действие*
dcs information option {dhcp | dhcpv6 | pppoe-ia | dhcp-relay} enable	-/выключено	Включить добавление circuit-id + remote-id для конкретного протокола. **Вставка circuit-id/remote-id должна быть отключена глобально.**
dcs information option {dhcp | dhcpv6 | pppoe-ia} disable		Выключить добавление remote-id и circuit-id для конкретного протокола.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 142 — Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show dcs-port-config [interface gigabitethernet *gi_port* | **twopointfivegigabitethernet** *two_port* | **tengigabitethernet** *te_port***] [vlan** *vlan_id***]**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); vlan_id: (1..4094)	Отобразить текущую конфигурацию идентификаторов remote-id и circuit-id для интерфейсов.
show dcs-global-config	-	Отобразить глобальную конфигурацию идентификатора circuit-id.

Пример настройки DHCP Snooping во VLAN10 с настройкой DCS-опций на интерфейсе Gigabitethernet 0/13.

```
console(config)# interface gigabitethernet 0/10
console(config-if)# port-security-state trusted
console(config-if)# set port-role uplink
console(config-if)# switchport mode trunk
console(config-if)# exit
console(config)# ip dhcp snooping
console(config)# vlan 10
console(config-vlan)# ip dhcp snooping
console(config)# interface gigabitethernet 0/13
console(config-if)# switchport general allowed vlan add 10 untagged
console(config-if)# switchport general pvid 10
console(config-if)# dcs remote-agent-identifier enable
console(config-if)# dcs agent-circuit-identifier "%v %p %h"
console(config-if)# dcs remote-agent-identifier "%M"
```

Пример настройки DHCP Snooping во VLAN10 с настройкой DCS-опций для всех интерфейсов в формате HEX.

```
console(config)# !
console(config)# interface gigabitethernet 0/10
console(config-if)# port-security-state trusted
console(config-if)# set port-role uplink
console(config-if)# switchport mode trunk
console(config-if)# exit
console(config)# ip dhcp snooping
console(config)# dcs remote-agent-id suboption-type dhcpv4 user-defined binary
console(config)# dcs agent-circuit-id suboption-type dhcpv4 user-defined binary
console(config)# dcs agent-circuit-id user-defined "%i%v"
console(config)# dcs remote-agent-id user-defined "%M"
console(config)# !
console(config)# vlan 10
console(config-vlan)# ip dhcp snooping
console(config-vlan)# !
console(config)# interface gigabitethernet 0/13
console(config-if)# switchport general allowed vlan add 10 untagged
console(config-if)# switchport general pvid 10
```

4.21.4 Защита IP-адреса клиента (IP Source Guard)

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

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

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки:

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

Таблица 143 — Команды режима конфигурации интерфейса Ethernet

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

Команды режима конфигурации интерфейса L2Vlan

Вид запроса командной строки:

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

Таблица 144 — Команды режима конфигурации интерфейса L2Vlan

Команда	*Значение/Значение по умолчанию*	*Действие*
{ip | ipv6} verify source port-security	-/Выключено	Включить функцию защиты IP/IPv6-интерфейса для VLAN. После включения на интерфейсе все записи в таблице IP Binding устанавливаются в TCAM в качестве разрешающего правила.
no {ip | ipv6} verify source port-security		Команда удаляет записи из TCAM и отключает отбрасывание IP/IPv6-пакетов во VLAN.

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 145 — Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show { ip | ipv6} verify source [interface {gigabitethernet | tengigabitethernet} *interface* **| vlan [***vlan-id***]]**	-	Отобразить настройки IP/IPv6 source Guard на интерфейсах.
show running-config ip-source-guard	-	Отобразить конфигурацию модуля IP source Guard.

4.21.5 Контроль протокола ARP (ARP Inspection)

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

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

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 146 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip arp inspection enable	-/выключено	Включить контроль протокола ARP (функцию ARP Inspection).
ip arp inspection disable		Выключить контроль протокола ARP (функцию ARP Inspection).
ip arp inspection vlan *vlan_id*	vlan_id: (1..4094)/ выключено	Разрешить проверку протокола ARP, основанную на базе соответствий DHCP snooping, в выбранной группе VLAN.
no ip arp inspection vlan *vlan_id*		Запретить проверку протокола ARP, основанную на базе соответствий DHCP snooping, в выбранной группе VLAN.

ip arp inspection validate {dstmac | dstmac-ipaddr | ipaddr |srcmac | srcmac-dstmac | srcmac-dstmac-ipaddr | srcmac-ipaddr}	-	Предоставить специфичные проверки для контроля протокола ARP. - **srcmac**: Для ARP-запросов и ответов проверяется соответствие MAC-адреса в заголовке Ethernet MAC-адресу источника в содержимом протокола ARP. - **dstmac**: Для ARP-ответов проверяется соответствие MAC-адреса в заголовке Ethernet MAC-адресу назначения в содержимом протокола ARP. - **ipaddr**: Проверяется содержимое ARP-пакета на наличие некорректных IP-адресов.
no ip arp inspection validate		Запретить специфичные проверки для контроля протокола ARP.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 147 — Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip arp inspection globals	-	Отобразить системную конфигурацию функции контроля ARP протокола.
show ip arp inspection vlan [*vlan_id***]**	vlan_id: (1..4094)	Отобразить список VLAN, на которых активен ARP Inspection.
show ip arp inspection statistics [global | interface {gigabitethernet | tengigabitethernet} *interface* **| vlan** *vlan_id***]**	vlan_id: (1..4094)	Показать 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 [global | vlan *vlan_id***]**	vlan_id: (1..4094)	Очистить статистику контроля протокола ARP Inspection.

4.21.6 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 148 — Команды режима глобальной конфигурации

Команда	*Значение/ Значение по умолчанию*	*Действие*
mac-address-table notification change	-/выключено	Команда предназначена для глобального управления функцией MAC notification. Команда разрешает регистрацию событий добавления и удаления MAC-адресов из таблиц коммутатора и отправку уведомления о событиях. Для работы функции необходимо дополнительно разрешать генерацию уведомлений на интерфейсах (см. ниже).

no mac-address-table notification change		Выключить функцию MAC notification глобально и отменить соответствующие настройки на всех интерфейсах.
mac-address-table notification change interval *value*	value: (0..604800)/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		Восстановить 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		Восстановить значение по умолчанию.
logging events mac-address-table change	-/выключено	Включить отправку трапов в syslog о событиях изучения или удаления MAC-адресов.
no logging events mac-address-table change		Выключить отправку трапов в syslog о событиях изучения или удаления MAC-адресов.
mac-address-table notification flapping	-/включено	Включить отслеживание MAC Flapping.
no mac-address-table notification flapping		Выключить отслеживание MAC Flapping.
logging events mac-address-table flapping	-/включено	Включить логирование MAC Flapping.
no logging events mac-address-table flapping		Выключить логирование MAC Flapping.
snmp-server enable traps errdisable {storm-control|loopback-detection| udld}	-/включено	Включить генерацию уведомлений при блокировке порта по событиям: - **loopback-detection** – обнаружение петель; - **udld** – активация защиты UDLD; - **storm-control** – широковещательный шторм.
no snmp-server enable traps errdisable { storm-control|loopback-detection|udld}		Отключить генерацию уведомлений на интерфейсе.

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки:

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

Таблица 149 — Команды режима конфигурации интерфейса Ethernet

Команда	***Значение/Значение по умолчанию***	***Действие***
snmp trap mac-address-table change [learnt | removed]	-/выключено	Включить генерацию уведомлений на каждом интерфейсе о событиях изменения состояния MAC-адресов. - **learnt** – уведомления об изучении MAC-адресов; - **removed** – уведомления об удалении MAC-адресов.
no snmp trap mac-address-table change [learnt | removed]		Отключить генерацию уведомлений на интерфейсе.

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 150 — Команды режима Privileged EXEC

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

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

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 151 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
shutdown dot1x	-/включено	Выключить модуль dot1x.
no shutdown dot1x		Включить модуль dot1x.
dot1x system-auth-control	-/выключено	Включить режим аутентификации 802.1x на коммутаторе.
no dot1x system-auth-control		Выключить режим аутентификации 802.1x на коммутаторе.

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки в режиме конфигурации интерфейса Ethernet:

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

Таблица 152 — Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
dot1x host-mode {multi-host | multi-session}	-/multi-host	Разрешить наличие нескольких клиентов на авторизированном порту dot1x: **- multi-host** – несколько клиентов; **- multi-session** – несколько сессий.
dot1x max-req *number*	number: (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 port-control {auto | force-authorized | force-unauthorized}	-/force-authorized	Настроить аутентификацию 802.1X на интерфейсе. Разрешить ручной контроль за состоянием авторизации порта. - **auto** – использовать 802.1X для изменения состояния клиента между авторизованным и неавторизованным; - **force-authorized** – выключать аутентификацию 802.1X на интерфейсе. Переход порта в авторизованное состояние без аутентификации; - **force-unauthorized** – перевод порта в неавторизованное состояние. Игнорируются все попытки аутентификации клиента, коммутатор не предоставляет сервис аутентификации для этого порта.
no dot1x port-control		Установить значение по умолчанию.
dot1x reauth-max *number*	number: (1..10)/2	Задать максимальное количество попыток авторизации для клиента.
no dot1x reauth-max		Установить значение по умолчанию.
dot1x reauthentication	-/выключено	Включить периодические повторные проверки подлинности (переаутентификацию) клиента.
no dot1x reauthentication		Установить значение по умолчанию.
dot1x timeout quiet-period *sec*	sec: (0..65535)/60	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 reauth-period *sec*	sec: (1..65535)/3600	Указать промежуток времени, по истечении которого коммутатор попробует реаутентифицировать клиента.
no dot1x timeout reauth-period		Установить значение по умолчанию.
dot1x timeout server-timeout *sec*	sec: (1..65535)/30	Установить период, в течение которого коммутатор ожидает ответа от сервера аутентификации.
no dot1x timeout server-timeout		Установить значение по умолчанию.
dot1x timeout supp-timeout *sec*	sec: (1..65535)/30	Установить период между повторными передачами запросов протокола EAP-клиенту.
no dot1x timeout supp-timeout		Установить значение по умолчанию.
dot1x timeout tx-period *sec*	sec: (1..65535)/30	Указать промежуток времени, в течение которого коммутатор ожидает ответа на EAP-запрос/кадр идентификации от клиента.
no dot1x timeout tx-period		Установить значение по умолчанию.
dot1x guest-vlan *vlan_id*	vlan_id: (1..4094)/ выключено	Определить гостевую VLAN. Открывает неавторизованным пользователям интерфейса доступ к гостевой VLAN.
no dot1x guest-vlan		Установить значение по умолчанию.
dot1x unauthenticated-vlan *vlan*	vlan_id: (1..4094)/ выключено	Определить незарегистрированную VLAN. Открывает пользователям интерфейса доступ к VLAN, если сервер аутентификации недоступен.
no dot1x unauthenticated-vlan		Установить значение по умолчанию.
dot1x local-database *username* **password** *password* **permission {allow | deny}** [*auth-timeout*] **[interface** *interface-type*]	username: (1..20) символов; password: (1..20) символов; auth-timeout: (1-7200)	Добавить в локальную базу данных информацию о пользователе.
no dot1x local-database *username*		Удалить информацию о пользователе из локальной базы данных.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 153 — Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
dot1x re-authenticate interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***}**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11)	Осуществить вручную повторную проверку подлинности указанного порта в команде.
show dot1x	-	Показать конфигурацию dot1x.
show dot1x all	-	Показать конфигурацию dot1x для всех интерфейсов.
show dot1x interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***}**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11)	Показать настройки протокола 802.1x на интерфейсе.
show dot1x mac-info [address *mac***]**	mac_address: (aa:aa:aa:aa:aa:aa)	Показать параметры сессии dot1x по всем mac-адресам или по конкретному mac-адресу.
show dot1x mac-statistics [address *mac***]**	mac_address: (aa:aa:aa:aa:aa:aa)	Показать параметры сессии dot1x по портам или по конкретному mac-адресу.
show dot1x statistics interface {gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***}**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11)	Показать статистику обмена пакетами dot1x на интерфейсе.

Пример включения режима 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 terminal
console(config)# dot1x system-auth-control
console(config)# aaa authentication dot1x default group radius
console(config)# interface gigabitethernet 0/8
console(config-if)# dot1x port-control auto
```

4.21.8 Настройка функции IPv6 RA Guard

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

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 154 — Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
shutdown ipv6 snooping	-/включено	Отключить работу модуля IPv6 RA Guard на устройстве. **Данная команда отключает работу модуля IPv6 RA Guard с безвозвратным удалением всех настроек блока IPv6 RA Guard.**
no shutdown ipv6 snooping		Включить работу модуля IPv6 RA Guard на устройстве.
ipv6 nd ra-guard enable	-/выключено	Разрешить коммутатору контролирование посредством функции IPv6 RA Guard.
no ipv6 nd ra-guard enable		Выключение функции IPv6 RA Guard.
ipv6 nd ra-guard policy *policy_id*	policy_id: (1..65535)	Создать и сконфигурировать policy IPv6 RA Guard.
no ipv6 nd ra-guard policy *policy_id*		Удалить policy IPv6 RA Guard.
ipv6 rag-acl-list *access_list_num* **seq** *seqmac_addr*	access_list_num: (1..65535); seq: (1..100)	Создать запись в списке доступа RA Guard на основе link layer адреса.
no ipv6 rag-acl-list *access_list_num* **seq** *seqmac_addr*		Удалить запись в списке доступа RA Guard.
ipv6 rag-prefix-list *list_id* **seq** *seq prefix*	prefix: (2000::1/64)	Создать запись в списке доступа RA Guard на основе IPv6-префикса.
no ipv6 rag-prefix-list *list_id* **seq** *seq [prefix]*		Удалить запись в списке доступа RA Guard.
ipv6 rag-src-ipv6-list *access_list_num* **[seq** *seq***]** *src_ipv6_link-local_address*	access_list_num: (1..65535); seq: (1..100)	Создать запись в списке доступа RA Guard на основе link-local IPv6-адреса.
no ipv6 rag-src-ipv6-list *access_list_num* **[seq** *seq***]** *src_ipv6_link-local_address*		Удалить запись в списке доступа RA Guard.

Команды режима глобального конфигурирования policy IPv6 RA Guard

Вид запроса командной строки режима конфигурирования policy IPv6 RA Guard:

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

Таблица 155 — Команды режима конфигурирования policy IPv6 RA Guard

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

no match rag-src-ipv6-list		Удалить фильтрацию сообщений IPv6 RA Guard по IPv6-префиксу.

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки режима конфигурирования интерфейса:

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

Таблица 156 — Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
ipv6 nd ra-guard	-/выключено	Разрешить коммутатору контролирование функции IPv6 RA Guard на интерфейсе.
no ipv6 nd ra-guard		Выключить функцию IPv6 RA Guard на интерфейсе.
ipv6 nd ra-guard trust-state trusted	По умолчанию все порты являются untrusted	Добавить порт в список доверенных.
ipv6 nd ra-guard trust-state untrusted		Удалить порт из trusted-list.
ipv6 nd ra-guard attach-policy *policy_id* **vlan {add | remove | none}** *vlan_list***]**	policy_id: (1..65535); vlan_list: (1..4094)	Привязать сконфигурированный policy IPv6 RA Guard к интерфейсу.
no ipv6 nd ra-guard attach-policy *policy_id*		Удалить policy IPv6 RA Guard на интерфейсе.

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 157 — Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ipv6 nd ra-guard [interface gigabitethernet *gi_port* | **twopointfivegigabitethernet** *two_port* | **tengigabitethernet** *te_port* | **port-channel** *group***]**	-	Показать настройки IPv6 RA Guard на интрефейсах.
show ipv6 nd ra-guard policy [*policy_id***]**	policy_id: (1..65535)	Показать настройки политик IPv6 RA Guard.
show ipv6 nd ra-guard global	-	Показать глобальные настройки IPv6 RA Guard.

4.21.9 Настройка функции IPv6 ND Inspection

Функция IPv6 ND Inspection предоставляет защиту от атак, основанных на рассылке поддельных Neighbor Advertisement, разрешая отсылку сообщений только с доверенных портов или при соответствии пакета настроенной политике.

Команды режима глобального конфигурирования

Вид запроса командной строки режима глобального конфигурирования:

```
console(config)#
```

Таблица 158 — Команды режима глобального конфигурирования

Команда	*Значение/Значение по умолчанию*	*Действие*
shutdown ipv6 snooping	-/включено	Отключить работу модуля IPv6 ND inspection на устройстве. **Данная команда отключает работу модуля IPv6 RA Guard и IPv6 ND Inspection с безвозвратным удалением всех настроек блока IPv6 RA Guard и IPv6 ND Inspection.**
no shutdown ipv6 snooping		Включить работу модуля IPv6 ND Guard на устройстве.
ipv6 nd inspection	-/выключено	Включить функцию IPv6 ND Inspection.
no ipv6 nd inspection		Выключение функцию IPv6 ND Inspection.
ipv6 nd inspection policy *policy_id*	policy_id: (1..65535)	Создать и сконфигурировать policy IPv6 ND Inspection.
no ipv6 nd inspection policy *policy_id*		Удалить policy IPv6 ND Inspection.
ipv6 nd inspection src-addr-acl *src-addr-acl_num* **[seq** *seq***]** *prefix/prefix-len*	*src-addr-acl_num*: (1..65535); seq: (1..100)	Создать запись в списке доступа ND Inspection на основании src ipv6-prefix в заголовке IPv6.
no ipv6 nd inspection src-addr-acl *src-addr-acl_num* **[seq** *seq***]** *prefix/prefix-len*		Удалить запись в списке доступа ND Inspection на основании src ipv6-prefix в заголовке IPv6.
ipv6 nd inspection tgt-addr-acl *tgt-addr-acl_num* **[seq** *seq***]** *prefix/prefix-len*	*tgt-addr-acl_num*: (1..65535); seq: (1..100)	Создать запись в списке доступа ND Inspection на основании target ipv6-addr в заголовке ICMPv6.
no ipv6 nd inspection tgt-addr-acl *tgt-addr-acl_num* **[seq** *seq***]** *prefix/prefix-len*		Удалить запись в списке доступа ND Inspection на основании target ipv6-addr в заголовке ICMPv6.
ipv6 nd inspection tgt-mac-acl *tgt-mac-acl_num* **[seq** *seq***]** *prefix/prefix-len*	*tgt-mac-acl_num*: (1..65535); seq: (1..100)	Создать запись в списке доступа ND Inspection на основании target mac-addr в заголовке ICMPv6.
no ipv6 nd inspection tgt-mac-acl *tgt-mac-acl_num* **[seq** *seq] prefix/prefix-len*		Удалить запись в списке доступа ND Inspection на основании target mac-addr в заголовке ICMPv6.

Команды режима конфигурирования policy IPv6 ND Inspection

Вид запроса командной строки режима конфигурирования policy IPv6 ND Inspection:

```
console(config-ndi)#
```

Таблица 159 — Команды режима конфигурирования policy IPv6 ND Inspection

Команда	*Значение/Значение по умолчанию*	*Действие*
override-flag {on | off | none}	-/none	Определить значение флага override в NA-сообщениях.
router-flag {on | off | none}	-/none	Определить значение флага router в NA-сообщениях.
solicited-flag {on | off | none}	-/none	Определить значение флага solicited в NA-сообщениях.
match src-addr-acl *src-addr-acl_num*	*src-addr-acl_num*: (1..65535)	Осуществить привязку **src-addr-acl** к policy IPv6 ND Inspection.
no match src-addr-acl *src-addr-acl_num*		Удалить привязку **src-addr-acl** к policy IPv6 ND Inspection.
match tgt-addr-acl *tgt-addr-acl_num*	*tgt-addr-acl_num*: (1..65535)	Осуществить привязку **tgt-addr-acl** к policy IPv6 ND Inspection.
no match tgt-addr-acl *tgt-addr-acl_num*		Удалить привязку **tgt-addr-acl** к policy IPv6 ND Inspection.
match tgt-mac-acl *tgt-mac-acl_num*	*tgt-mac-acl_num*: (1..65535)	Осуществить привязку **tgt-mac-acl** к policy IPv6 ND Inspection.

no match tgt-mac-acl *tgt-mac-list_num*		Удалить привязку **tgt-mac-acl** к policy IPv6 ND Inspection.

Команды режима конфигурирования интерфейса Ethernet

Вид запроса командной строки режима конфигурирования интерфейса:

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

Таблица 160 — Команды режима конфигурирования интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
ipv6 nd inspection	-/выключено	Включить функцию IPv6 ND Inspection на интерфейсе.
no ipv6 nd inspection		Выключить функцию IPv6 ND Inspection на интерфейсе.
ipv6 nd inspection trust-state trusted	По умолчанию все порты являются untrusted	Добавить порт в список доверенных.
ipv6 nd inspection trust-state untrusted		Удалить порт из списка доверенных.
ipv6 nd inspection attach-policy *policy_id*	policy_id: (1..65535)	Привязать сконфигурированный policy IPv6 ND Inspection к интерфейсу. **Политика не может быть привязана к интерфейсу, находящемуся в списке доверенных портов.**
no ipv6 nd inspection attach-policy *policy_id*		Удалить policy IPv6 ND Inspection **с** интерфейса.

Команды режима Privileged EXEC

Вид запроса командной строки в режиме Privileged EXEC:

```
console#
```

Таблица 161 — Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ipv6 nd inspection [interface gigabitethernet *gi_port* | **twopointfivegigabitethernet** *two_port* | **tengigabitethernet** *te_port* | **port-channel** *group* **]**	-	Показать настройки IPv6 ND Inspection на интрефейсах.
show ipv6 nd inspection policy [*policy_id***]**	policy_id: (1..65535)	Показать настройки политик IPv6 ND Inspection.
show ipv6 nd inspection src-addr-acl [*src-addr-acl_num***]**	*src-addr-acl_num*: (1..65535)	Показать настройки IPv6 ND Inspection **src-addr-acl.**
show ipv6 nd inspection tgt-addr-acl [*tgt-addr-acl_num***]**	*tgt-addr-acl_num*: (1..65535)	Показать настройки IPv6 ND Inspection **tgt-addr-acl.**
show ipv6 nd inspection tgt-mac-acl [*tgt-mac-acl_num***]**	*tgt-mac-acl_num*: (1..65535)	Показать настройки IPv6 ND Inspection **tgt-mac-acl.**
show ipv6 nd inspection global	-	Показать глобальные настройки IPv6 ND Inspection.

4.22 Функции DHCP Relay посредника

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

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 162 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip dhcp relay	-/выключено	Включить функцию DHCP Relay агента на коммутаторе. **Если DHCP Relay включен глобально, но не включен на отдельных VLAN, то Relay будет работать на всех активных VLAN.**
no ip dhcp relay		Выключить функцию DHCP Relay агента на коммутаторе.
ip dhcp relay server *ip_add* **[source-port** *src_port***] [destination-port** *dst_port***]**	src_port: (1..65535); dst_port: (1..65535); Может быть задано до пяти серверов	Задать IP-адрес доступного DHCP-сервера для DHCP Relay агента.
no ip dhcp relay server *ip_add*		Удалить IP-адрес из списка DHCP-серверов для DHCP Relay агента.

Команды режима конфигурации VLAN

Вид запроса командной строки в режиме конфигурации VLAN:

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

Таблица 163 — Команды режима конфигурации VLAN

Команда	*Значение/Значение по умолчанию*	*Действие*
ip dhcp relay	-/выключено	Включить функцию DHCP Relay агента для конфигурируемого VLAN.
no ip dhcp relay		Выключить функцию DHCP Relay агента для конфигурируемого VLAN.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 164 — Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip dhcp relay information {gigabitethernet *gi_port* **| two-pointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| vlan** *vlan***}**	gi_port: (0/1..28); two_port: (0/1..8); te_port: (0/1..6); vlan: (1..4094)	Отобразить конфигурацию настроенной функции DHCP Relay агента для коммутатора и отдельно для интерфейсов, а также список доступных серверов.
show dhcp server	-	Отобразить список доступных серверов.

4.23 Конфигурация DHCP-сервера

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

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

Конфигурирование опций DHCP-сервера возможно как из режима глобальной конфигурации, так и из режима конфигурирования DHCP-пула адресов. В режиме конфигурирования DHCP-пула адресов есть возможность настраивать статические записи.

При одновременной настройке значений опций DHCP-сервера в режиме глобальной конфигурации, режиме конфигурирования DHCP-пула адресов и настройке host-записей выдача опций будет осуществляться в соответствии со следующим приоритетом:
1. Настройка статической записи.
2. Настройка для pool.
3. Глобальная настройка.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 165 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
ip dhcp server	-/выключено	Включение функции DHCP-сервера на коммутаторе.
no ip dhcp server		Выключение функции DHCP-сервера на коммутаторе.
ip dhcp pool {number**}** **[***name***]**	number: (1..2147483647) name: (1..64) символов	Войти в режим конфигурации DHCP-пула адресов DHCP-сервера. - *number* – номер DHCP-пула адресов; - *name* – имя DHCP-пула адресов. **Максимально допустимое количество DHCP pool указано в таблице 9.**
no ip dhcp pool {number**}**		Удалить DHCP-пул с заданным именем.
ip dhcp server 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 server excluded-address *low_address* **[***high_address***]**		Удалить IP-адрес из списка исключений для назначения его DHCP-клиентам.
ip dhcp server bootfile *name*	filename: (1..64) символов	Указать имя файла, используемого для начальной загрузки DHCP-клиента.
no ip dhcp server bootfile		Установить значение по умолчанию.
ip dhcp server 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 ip dhcp server default-router		Установить значение по умолчанию.
ip dhcp server 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 ip dhcp server dns-server		Установить значение по умолчанию.
ip dhcp server domain-name *domain*	domain: (1..128) символов	Определить доменное имя для DHCP-клиентов.
no ip dhcp server domain-name		Установить значение по умолчанию.
ip dhcp server 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 ip dhcp server netbios-name-server		Установить значение по умолчанию.
ip dhcp server 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 ip dhcp server netbios-node-type		Установить значение по умолчанию.
ip dhcp server next-server *ip_address*	-	Использовать для указания DHCP-клиенту адреса сервера (как правило, TFTP-сервера), с которого должен быть получен загрузочный файл.
no ip dhcp server next-server		Установить значение по умолчанию.
ip dhcp server ntp-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 ip dhcp server ntp-server		Установить значение по умолчанию.
ip dhcp server sip-server {domain *domain_name_list* **| ip** *ip_address_list***}**	По умолчанию список SIP-серверов не определен	Определить список SIP-серверов, доступных для клиентов DHCP. - *domain_name_list* – список доменных имен SIP-серверов, может содержать до 2 записей, разделенных пробелом. Максимальная длина строки – 125 символов. - *ip_address_list* – список IP-адресов SIP-серверов, может содержать до 8 записей, разделенных пробелом.
no ip dhcp server sip-server		Установить значение по умолчанию.
ip dhcp server vendor-specific *ascii_string*	ascii_string: (1..128) символов	Определить соответствие между опредленными опциями DHCP с конкретным вендором.
no ip dhcp server vendor-specific		Установить значение по умолчанию.

ip dhcp server option *code* **{boolean** *bool_val* **| ascii** *ascii_string* **| ip** *ip_address_list* **| hex** *hex_string* **| none}**	code: (0..255); bool_val: (true, false); ascii_string: (1..160) символов	Настроить опции DHCP-сервера. - *code* – код опции DHCP-сервера; - *bool_val* – логическое значение; - *ascii_string* – строка в формате ASCII; - *ip_address_list* – список IP-адресов (в некоторых случаях может содержать до 8 записей); - *hex_string* – строка в 16-ом формате.
no ip dhcp server option *code*		Удалить опции для DHCP-сервера.
ip dhcp server offer-reuse *time*	time: (1..120) секунд	Задать время, в течение которого DHCP-сервер ожидает DHCP REQUEST от клиента, прежде чем повторно отправить OFFER.
no ip dhcp server offer-reuse		Установить значение по умолчанию.
ip dhcp server ping-packets	-/выключена	Включить передачу ICMP-запросов на назначаемый IP-адрес, чтобы проверить занятость адреса, прежде чем он будет назначен DHCP-клиенту.
no ip dhcp server ping-packets		Установить значение по умолчанию.

Команды режима конфигурации пула DHCP-сервера

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

```
console# configure
console(config)# ip dhcp pool 1 test
console(config-dhcp)#
```

Таблица 166 — Команды режима конфигурации

Команда	***Значение/Значение по умолчанию***	***Действие***
network *low_address {ip_mask |prefix_length} high_address* **|** *network_number*	-	Задать диапазон выдаваемых адресов для указанного DHCP-пула. - *network_number* – IP-адрес номера подсети; - *low_address* – начальный IP-адрес диапазона адресов; - *high_address* – конечный IP-адрес диапазона адресов; - *mask* – маска подсети.
no network		Удалить диапазон адресов DHCP-пула.
lease {*days* **[***hours* **[***minutes***]] | infinite}**	-/1 день	Время аренды IP-адреса, которое назначено от DHCP. - **infinite** – время аренды не ограничено; - *days* – количество дней; - *hours* – количество часов; - *minutes* – количество минут.
no lease		Установить значение по умолчанию.
excluded-address *low_address high_address*	-	Указать IP-адреса, которые DHCP-сервер не будет назначать для DHCP-клиентов. - *low-address* – начальный IP-адрес диапазона; - *high-address* – конечный IP-адрес диапазона.
no excluded-address *low_address high_address*		Удалить IP-адреса из списка исключений для назначения его DHCP-клиентам.
bootfile *filename*	filename: (1..64) символов	Указать имя файла, используемого для начальной загрузки DHCP-клиента.
no bootfile		Установить значение по умолчанию.
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..128) 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*	-	Использовать для указания DHCP-клиенту адреса сервера (как правило, TFTP-сервера), с которого должен быть получен загрузочный файл.
no next-server		Установить значение по умолчанию.
ntp-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 ntp-server		Установить значение по умолчанию.
sip-server {domain *domain_name_list* **| ip** *ip_address_list***}**	По умолчанию список SIP-серверов не определен	Определить списов SIP-серверов, доступных для клиентов DHCP. - *domain_name_list* – список доменных имен SIP-серве-ров, может содержать до 2 записей, разделенных пробелом. Максимальная длина строки – 125 символов. - *ip_address_list* – список IP-адресов SIP-серверов, может содержать до 8 записей, разделенных пробелом.
no sip-server		Установить значение по умолчанию.
vendor-specific *ascii_string*	ascii_string: (1..128) символов	Определить соответствие между определенными опциями DHCP с конкретным вендором. - *ascii_string* – строка в формате ASCII.
vendor-specific		Установить значение по умолчанию.
option *code* **{boolean** *bool_val* **| ascii** *ascii_string* **| ip** *ip_address_list* **| hex** *hex_string* **| none}**	code: (0..255); bool_val: (true, false); ascii_string: (1..160) символов	Настроить опции DHCP-сервера. - *code* – код опции DHCP-сервера; - *bool_val* – логическое значение; - *ascii_string* – строка в формате ASCII; - *ip_address_list* – список IP-адресов (в некоторых случаях может содержать до 8 записей); - *hex_string* – строка в 16-ом формате.
no option *code*		Удалить опции для DHCP-сервера.
utilization threshold *percentage*	percentage: (0..100); -/75 процентов	Задать значение в процентах, при котором будет сгенерировано сообщение о заполнении пула до указанных границ.
no utilization threshold		Установить значение по умолчанию.

Примеры использования 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 terminal
console(config)# interface vlan 1
console(config-if)# ip address 192.168.45.1 255.255.255.0
console(config-if)# exit
console(config)# ip dhcp server
console(config)# ip dhcp pool 1 test
console(dhcp-config)# network 192.168.45.0 255.255.255.0
```

```
console(dhcp-config)# domain-name test.ru
console(dhcp-config)# dns-server 192.168.45.112
console(dhcp-config)# default-router 192.168.45.1
console(dhcp-config)# host hardware-address aa:bb:cc:dd:ee:ff ip
192.168.45.250
console(dhcp-config)# host hardware-address aa:bb:cc:dd:ee:ff ntp-server
192.168.45.254
console(dhcp-config)# host hardware-address aa:bb:cc:dd:ee:ff dns-server
192.168.45.113
```

Примеры настройки опций

Настроить DHCP-пул с именем test и указать для DHCP-клиентов следующие опции: option 3 - 192.168.45.1, option 12 - hostname_test, option 15 - test.ru, option 19 - True.

```
console#
console# configure terminal
console(config)# interface vlan 1
console(config-if)# ip address 192.168.45.1 255.255.255.0
console(config-if)# exit
console(config)# ip dhcp server
console(config)# ip dhcp pool 1 test
console(dhcp-config)# network 192.168.45.0 255.255.255.0
console(dhcp-config)# option 3 ip 192.168.45.1
console(dhcp-config)# option 12 hex 686f73746e616d655f74657374
console(dhcp-config)# option 15 ascii test.ru
console(dhcp-config)# option 19 boolean
```

В примере значение опции 12 переведено из ascii в hex.

Команды режима конфигурации статических записей DHCP-сервера

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

```
console# configure
console(config)# ip dhcp pool 1 test
console(config-dhcp)#
```

Таблица 167 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
host client-identifier hex *hex_string* **ip** *ip_address*	hex_string: (1..156) символов	Задать ip-адрес для устройства с указанным идентификатором. - *hex_string* – идентификатор клиента, представляющий собой hex-строку; - *ip_address* – IP-адрес, назначаемый клиенту DHCP-сервера.
no host client-identifier hex *hex_string* **ip**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host client-identifier hex *hex_string* **bootfile** *filename*	hex_string: (1..156) символов; filename: (1..64)	Создать статическую запись для клиента с указанным идентификатором. - *hex_string* – идентификатор клиента, представляющий собой hex-строку; - *filename* – наименование загрузочного файла.
no host client-identifier hex *hex_string* **bootfile**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.

host client-identifier hex *hex_string* **default-router** *ip_address_list*	hex_string: (1..156) символов	Определить список маршрутизаторов по умолчанию для указанного клиента DHCP-сервера: - *hex_string* – идентификатор клиента, представляющий собой hex-строку; - *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 host client-identifier hex *hex_string* **default-router**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host client-identifier hex *hex_string* **dns-server** *ip_address_list*	hex_string: (1..156) символов	Определить список DNS-серверов, доступных для статической записи с указанным идентификатором. - *hex_string* – идентификатор клиента, представляющий собой hex-строку; - *ip_address_list* – список IP-адресов маршрутизаторов, может содержать до 8 записей, разделенных пробелом.
no host client-identifier hex *hex_string* **dns-server**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host client-identifier hex *hex_string* **domain-name** *domain*	hex_string: (1..156) символов; domain: (1..128) символов	Определить доменное имя для статической запсиси с указанным идентификатором. - *hex_string* – идентификатор клиента, представляющий собой hex-строку.
no host client-identifier hex *hex_string* **domain-name**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host client-identifier hex *hex_string* **netbios-name-server** *ip_address_list*	hex_string: (1..156) символов	Определить список WINS-серверов, для статической записи с указанным идентификатором. - *hex_string* – идентификатор клиента, представляющий собой hex-строку; - *ip_address_list* – список IP-адресов WINS-серверов, может содержать до 8 записей, разделенных пробелом.
no host client-identifier hex *hex_string* **netbios-name-server**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host client-identifier hex *hex_string* **netbios-node-type {b-node | p-node | m-node | h-node}**	hex_string: (1..156) символов	Определить тип узла NetBIOS Microsoft для татической записи с указанным идентификатором: - *b-node* – широковещательный; - *p-node* – точка-точка; - *m-node* – комбинированный; - *h-node* – гибридный. - *hex_string* – идентификатор клиента, представляющий собой hex-строку.
no host client-identifier hex *hex_string* **netbios-node-type**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host client-identifier hex *hex_string* **next-server** *ip_address*	hex_string: (1..156) символов	Определить для статической записи с указанным идентификатоорм адреса сервера (как правило, TFTP-сервера), с которого должен быть получен загрузочный файл. - *hex_string* – идентификатор клиента, представляющий собой hex-строку.
no host client-identifier hex *hex_string* **next-server**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host client-identifier hex *hex_string* **ntp-server** *ip_address_list*	hex_string: (1..156) символов	Определяет список серверов времени, для статической записи с указанным идентификатором. - *ip_address_list* – список IP-адресов серверов времени, может содержать до 8 записей, разделенных пробелом; - *hex_string* – идентификатор клиента, представляющий собой hex-строку.
no host client-identifier hex *hex_string* **ntp-server**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.

host client-identifier hex *hex_string* **sip-server {domain** *domain_name_list* **| ip** *ip_address_list***}**	hex_string: (1..156) символов	Определить списов SIP-серверов, доступных для статической записи с указанным идентификатором. - *hex_string* – идентификатор клиента, представляющий собой hex-строку; - *domain_name_list* – список доменных имен SIP-серверов, может содержать до 2 записей, разделенных проблом. Максимальная длина строки 125 символов. - *ip_address_list* – список IP-адресов SIP-серверов, может содержать до 8 записей, разделенных пробелом.
no host client-identifier hex *hex_string* **sip-server**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host client-identifier hex *hex_string* **option** *code* **{boolean** *bool_val* **| ascii** *ascii_string* **| ip** *ip_address_list* **| hex** *option_hex_string* **| none}**	code: (0..255); bool_val: (true, false); ascii_string: (1..160) символов; option_hex_string: (1..128) символов; hex_string: (1..156) символов	Определить указанные опции для статической записи с заданным идентификатором. - *hex_string* – идентификатор клиента, представляющий собой hex-строку; - *code* – код опции DHCP-сервера; - *bool_val* – логическое значение; - *ascii_string* – строка в формате ASCII; - *ip_address_list* – список IP-адресов (в некоторых случаях может содержать до 8 записей); - *option_hex_string* – строка в 16-ом формате.
no host client-identifier hex *hex_string* **option** *code*		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
no host client-identifier hex *hex_string*	hex_string: (1..156) символов	Удалить все опции назначенные для статической записи с указанным идентификатором.
host client-identifier ascii *ascii_string* **ip** *ip_address*	ascii_string: (1..128) символов	Создать статическую запись для клиента с указанным идентификатором. - *ascii_string* – идентификатор клиента, представляющий собой ascii-строку; - *ip_address* – IP-адрес, назначаемый клиенту DHCP-сервера.
no host client-identifier ascii *ascii_string* **ip**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host client-identifier ascii *ascii_string* **bootfile** *filename*	ascii_string: (1..128) символов; filename: (1..64)	Создать статическую запись для клиента с указанным идентификатором. - *ascii_string* – идентификатор клиента, представляющий собой ascii-строку; - *filename* – наименование загрузочного файла.
no host client-identifier ascii *ascii_string* **bootfile**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host client-identifier ascii *ascii_string* **default-router** *ip_address_list*	ascii_string: (1..128) символов	Определить список маршрутизаторов для статической записи с указанным удентификатором. - *ascii_string* – идентификатор клиента, представляющий собой ascii-строку; - *ip_address_list* – список IP-адресов маршрутизаторов, доступных клиенту DHCP-сервера. Может содержать до 8 записей. **IP-адрес маршрутизатора должен быть в той же подсети, что и клиент.**
no host client-identifier ascii *ascii_string* **default-router**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host client-identifier ascii *ascii_string* **dns-server** *ip_address_list*	ascii_string: (1..128) символов	Определить список DNS-серверов, доступных для статической записи с указанным идентификатором. - *ip_address_list* – список IP-адресов DNS-серверов, может содержать до 8 записей, разделенных пробелом; - *ascii_string* – идентификатор клиента, представляющий собой ascii-строку.
no host client-identifier hex *ascii_string* **dns-server**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host client-identifier ascii *ascii_string* **domain-name** *domain*	ascii_string: (1..128) символов; domain: (1..128) символов	Определить доменное имя для статической запсиси с указанным идентификатором. - *ascii_string* – идентификатор клиента, представляющий собой ascii-строку.

no host client-identifier ascii *ascii_string* **domain-name**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host client-identifier ascii *ascii_string* **netbios-name-server** *ip_address_list*	ascii_string: (1..128) символов	Определить список WINS-серверов, для статической записи с указанным идентификатором. - *ascii_string* – идентификатор клиента, представляющий собой ascii-строку; - *ip_address_list* – список IP-адресов WINS-серверов, может содержать до 8 записей, разделенных пробелом.
no host client-identifier ascii *ascii_string* **netbios-name-server**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host client-identifier ascii *ascii_string* **netbios-node-type {b-node | p-node | m-node | h-node}**	ascii_string: (1..128) символов	Определить тип узла NetBIOS Microsoft для татической записи с указанным идентификатором: - *b-node* – широковещательный; - *p-node* – точка-точка; - *m-node* – комбинированный; - *h-node* – гибридный. - *ascii_string* – идентификатор клиента, представляющий собой ascii-строку.
no host client-identifier ascii *ascii_string* **netbios-node-type**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host client-identifier ascii *ascii_string* **next-server** *ip_address*	ascii_string: (1..128) символов	Определить для статичской записи с указанным идентификатоорм адреса сервера (как правило, TFTP-сервера), с которого должен быть получен загрузочный файл. - *ascii_string* – идентификатор клиента, представляющий собой ascii-строку.
no host client-identifier ascii *ascii_string* **next-server**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host client-identifier ascii *ascii_string* **ntp-server** *ip_address_list*	ascii_string: (1..128) символов	Определить список серверов времени, для статической записи с указанным идентификатором. - *ip_address_list* – список IP-адресов серверов времени, может содержать до 8 записей, разделенных пробелом; - *ascii_string* – идентификатор клиента, представляющий собой ascii-строку.
no host client-identifier ascii *ascii_string* **ntp-server**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host client-identifier ascii *ascii_string* **sip-server {domain** *domain_name_list* **| ip** *ip_address_list***}**	ascii_string: (1..128) символов	Определить списов SIP-серверов, доступных для статической записи с указанным идентификатором. - *asccii_string* – идентификатор клиента, представляющий собой ascii-строку; - *domain_name_list* – список доменных имен SIP-серверов, может содержать до 2 записей, разделенных пробелом. Максимальная длина строки – 125 символов. - *ip_address_list* – список IP-адресов SIP-серверов, может содержать до 8 записей, разделенных пробелом.
no host client-identifier ascii *ascii_string* **sip-server**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host client-identifier ascii *asccii_string* **option** *code* **{boolean** *bool_val* **| ascii** *option_ascii_string* **| ip** *ip_address_list* **| hex** *hex_string* **| none}**	code: (0..255); bool_val: (true, false); option_ascii_string: (1..160) символов; hex_string: (1..128) символов; ascii_string: (1..128) символов	Определить указанные опции для статической записи с заданным идентификатором. - *ascii_string* – идентификатор клиента, представляющий собой ascii-строку; - *code* – код опции DHCP-сервера; - *bool_val* – логическое значение; - *option_ascii_string* – строка в формате ASCII; - *ip_address_list* – список IP-адресов (в некоторых случаях может содержать до 8 записей); - *hex_string* – строка в 16-ом формате.
no host client-identifier ascii *ascii_string* **option** *code*		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
no host client-identifier ascii *ascii_string*	ascii_string: (1..128) символов	Удалить все опции, назначенные для статической записи с указанным идентификатором.

host hardware-address *mac_address* **ip** *ip_address*	-	Создать статическую запись для клиента с указанным идентификатором. - *mac_address* – идентификатор клиента, представляющий собой MAC-адрес устройства; - *ip_address* – IP-адрес, назначаемый клиенту DHCP-сервера.
no host hardware-address *mac_address* **ip**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host hardware-address *mac_address* **bootfile** *filename*	filename: (1..64)	Создать статическую запись для клиента с указанным идентификатором. - *mac_address* – идентификатор клиента, представляющий собой MAC-адрес устройства; - *filename* – наименование загрузочного файла.
no host hardware-address *mac_address* **bootfile**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host hardware-address *mac_address* **default-router** *ip_address_list*	-	Определить список маршрутизаторов для статической записи с указанным удентификатором. - *mac_address* – идентификатор клиента, представляющий собой MAC-адрес устройства; - *ip_address_list* – список IP-адресов маршрутизаторов, доступных клиенту DHCP-сервера. Может содержать до 8 записей. **IP-адрес маршрутизатора должен быть в той же подсети, что и клиент.**
no host hardware-address *mac_address* **default-router**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host hardware-address *mac_address* **dns-server** *ip_address_list*	-	Определить список DNS-серверов, доступных для статической записи с указанным идентификатором. - *ip_address_list* – список IP-адресов DNS-серверов, может содержать до 8 записей, разделенных пробелом; - *mac_address* – идентификатор клиента, представляющий собой MAC-адрес устройства.
no host hardware-address *mac_address* **dns-server**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host hardware-address *mac_address* **domain-name** *domain*	domain: (1..128) символов	Определить доменное имя для статической записи с указанным идентификатором. - *mac_address* – идентификатор клиента, представляющий собой MAC-адрес устройства.
no host hardware-address *mac_address* **domain-name**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host hardware-address *mac_address* **netbios-name-server** *ip_address_list*	-	Определить список WINS-серверов, для статической записи с указанным идентификатором. - *mac_address* – идентификатор клиента, представляющий собой MAC-адрес устройства; - *ip_address_list* – список IP-адресов WINS-серверов, может содержать до 8 записей, разделенных пробелом.
no host hardware-address *mac_address* **netbios-name-server**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host hardware-address *mac_address* **netbios-node-type {b-node | p-node | m-node | h-node}**	-	Определить тип узла NetBIOS Microsoft для статической записи с указанным идентификатором: - *b-node* – широковещательный; - *p-node* – точка-точка; - *m-node* – комбинированный; - *h-node* – гибридный. - *mac_address* – идентификатор клиента, представляющий собой MAC-адрес устройства.
no host hardware-address *mac_address* **netbios-node-type**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.

host hardware-address *mac_address* **next-server** *ip_address*	-	Определить для статической записи с указанным идентификатором адреса сервера (как правило, TFTP-сервера), с которого должен быть получен загрузочный файл. - *mac_address* – идентификатор клиента, представляющий собой MAC-адрес устройства.
no host hardware-address *mac_address* **next-server**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host hardware-address *mac_address* **ntp-server** *ip_address_list*	-	Определить список серверов времени для статической записи с указанным идентификатором. - *ip_address_list* – список IP-адресов серверов времени, может содержать до 8 записей, разделенных пробелом; - *mac_address* – идентификатор клиента, представляющий собой MAC-адрес устройства.
no hardware-address *mac_address* **ntp-server**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host hardware-address *mac_address* **sip-server {domain** *domain_name_list* **| ip** *ip_address_list***}**	-	Определить список SIP-серверов, доступных для статической записи с указанным идентификатором. - *mac_address* – идентификатор клиента, представляющий собой MAC-адрес устройства; - *domain_name_list* – список доменных имен SIP-серверов, может содержать до 2 записей, разделенных пробелом. Максимальная длина строки – 125 символов; - *ip_address_list* – список IP-адресов SIP-серверов, может содержать до 8 записей, разделенных пробелом.
no host hardware-address *mac_address* **sip-server**		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
host hardware-address *mac_address* **option** *code* **{boolean** *bool_val* **| ascii** *ascii_string* **| ip** *ip_address_list* **| hex** *hex_string* **| none}**	code: (0..255); bool_val: (true, false); ascii_string: (1..160) символов; hex_string: (1..128) символов.	Определить указанные опции для статической записи с заданным идентификатором. - *mac_address* – идентификатор клиента, представляющий собой MAC-адрес устройства; - *code* – код опции DHCP-сервера; - *bool_val* – логическое значение; - *ascii_string* – строка в формате ASCII; - *ip_address_list* – список IP-адресов (в некоторых случаях может содержать до 8 записей); - *option_hex_string* – строка в 16-ом формате.
no host hardware-address *mac_address* **option** *code*		Удалить статическую запись, соответствующую клиенту с указанным идентификатором.
no host hardware-address *mac_address*	-	Удалить все опции, назначенные для статической записи с указанным идентификатором.

При задании Client ID в формате ASCII убедитесь, что DHCP-клиент отправляет Client ID с Hardware Type в первом байте, соответствующий заданному формату.

Пример настройки статической записи

Назначить устройству с MAC-адресом aa:bb:cc:dd:ee:ff ip-адрес – 192.168.45.250, сервер времени – 192.168.45.254 и DNS-сервер – 192.168.45.113

```
console#
console# configure terminal
console(config)# interface vlan 1
console(config-if)# ip address 192.168.45.1 255.255.255.0
console(config-if)# exit
console(config)# ip dhcp server
console(config)# ip dhcp pool 1 test
console(dhcp-config)# network 192.168.45.0 255.255.255.0
console(dhcp-config)# host hardware-ad-
dress aa:bb:cc:dd:ee:ff ip 192.168.45.250
console(dhcp-config)# host hardware-address aa:bb:cc:dd:ee:ff ntp-
server 192.168.45.254
```

```
console(dhcp-config)# host hardware-address aa:bb:cc:dd:ee:ff dns-
server 192.168.45.113
```

Команды режима Privileged EXEC

Вид запроса командной строки режима Privileged EXEC:

```
console#
```

Таблица 168 – Команды режима Privileged EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
clear ip dhcp server binding [*ip_address***]**	-	Удалить записи из таблицы соответствия физических адресов и адресов, выданных с пула DHCP-сервером: - *ip_address* – IP-адрес, назначенный DHCP-сервером.
clear ip dhcp server statistics	-	Удалить статистистики работы DHCP-сервера.
show ip dhcp server binding	-	Просмотреть IP-адреса, которые сопоставлены с физическими адресами клиентов, а также время аренды, способ назначения и состояние IP-адресов.
show ip dhcp server information	-	Просмотреть информацию о конфигурации DHCP-сервера.
show ip dhcp server pools	-	Просмотреть информацию о глобальных настройка DHCP-сервера, а также о созданных пулах и существующих host-записях.
show ip dhcp server statistics	-	Просмотреть статистику DHCP-сервера.

4.24 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 169 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
shutdown pppoe intermediate-agent	-/включено	Отключить работу модуля pppoe intermediate-agent на устройстве. **Данная команда отключает работу модуля pppoe intermediate-agent с безвозвратным удалением всех настроек блока PPPoE IA.**
no shutdown pppoe intermediate-agent		Включить работу модуля pppoe intermediate-agent на устройстве.
pppoe-ia snooping	-/выключено	Глобально включить контроль функции PPPoE IA.
no pppoe-ia snooping		Выключить контроль функции PPPoE IA.

pppoe-ia snooping session timeout *range*	range: (0..600)/300	Задать таймаут для работы функции PPPoE IA.
pppoe-ia snooping session timeout 0		Отключить таймаут для работы функции PPPoE IA.
pppoe pass-through	-/выключено	Включение команды заставляет PPPoE-пакеты проходить через коммутатор как неизвестный L2-трафик, и делает их "невидимыми" для IP ACL.
no pppoe pass-through		Включить парсинг инкапсулированных в PPPoE-пакетах L3-заголовков, правила IP ACL начинают работать для инкапсулированных пакетов.

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

Команды режима конфигурации VLAN (диапазон VLAN'ов)

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

Таблица 170 — Команды режима конфигурации интерфейса L2Vlan

Команда	*Значение/Значение по умолчанию*	*Действие*
pppoe-ia snooping	-/выключено	Включить контроль функции PPPoE IA в пределах указанного VLAN.
no pppoe-ia snooping		Выключить контроль функции PPPoE IA в пределах указанного VLAN.

Пример настройки PPPoE IA в VLAN10 с настройкой DCS-опций на интерфейсе Gigabitethernet0/13.

```
console(config)#pppoe-ia snooping
console(config)#pppoe passthrough
console(config)#dcs information option enable
console(config)#vlan 10
console(config-vlan)#pppoe-ia snooping
console(config-vlan)#exit
console(config)#interface gigabitethernet 0/13
console(config-if)#switchport general allowed vlan add 10 untagged
console(config-if)#switchport general pvid 10
console(config-if)#dcs agent-circuit-identifier "%v %p %h"
console(config-if)#dcs remote-agent-identifier "%M"
console(config-if)#exit
console(config)#interface gigabitethernet 0/24
console(config-if)#switchport general allowed vlan add 10
console(config-if)#port-security-state trusted
console(config-if)#set port-role uplink
console(config-if)#exit
```

4.25 Конфигурация ACL (списки контроля доступа)

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

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

ACL автоматически снимается с интерфейса при изменении в нем правила.

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 171 — Команды для создания и конфигурации списков ACL

Команда	***Значение/Значение по умолчанию***	***Действие***
ip access-list standart *access_list_num* [**description** *description*]	access_list_num: (1..1000); description: (1..128) символов	Создать стандартный список ACL.
no ip access-list standart *access_list_num*		Удалить стандартный список ACL.
ip access-list extended *access_list_num* [**description** *description*]	access_list_num: (1001..65535); description: (1..128) символов	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_num*		Удалить расширенный список ACL для адресации IPv4.
ipv6 access-list extended *access_list_num* [**description** *description*]		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_num*		Удалить расширенный список ACL для адресации IPv6.
mac access-list extended *access_list_num* [**description** *description*]	mac_ access_list_num: (1..65535); description: (1..128) символов	Создать новый список ACL 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 *mac_access_list_num*		Удалить список ACL на базе MAC-адресации.
user-defined offset *offset_id* **{ l2 | ethtype | l3 | l4 }** *value*	offset_id: (1..4); value: (0..255)	Настроить смещение в байтах относительно выбранной стартовой позиции. Значение и маска, используемые для фильтрации, задаются через параметры ACL-правил. - **l2** – начало пакета (Destination MAC address); - **ethtype** – Ethertype (самый внутренний, при наличии VLAN-тегов); - **l3** – L3-заголовок; - **l4** – L4-заголовок.
no user-defined offset *offset_id*		Удалить смещение относительно выбранной стартовой позиции.

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

Команды режима конфигурации интерфейса Ethernet, VLAN

Командная строка в режиме конфигурации интерфейса Ethernet имеет вид:

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

Командная строка в режиме конфигурации интерфейса VLAN имеет вид:

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

Таблица 172 — Команда назначения списка ACL-интерфейсу

Команда	*Значение/Значение по умолчанию*	*Действие*
ip access-group *access_list_num* **in**	access_list_num: (1..65535)	В настройках определённого физического интерфейса команда привязывает указанный список к данному интерфейсу.
no ip access-group *access_list_num* **in**		Удалить список с интерфейса.
mac access-group *access_list_num* **in**	access_list_num: (1..65535)	В настройках определённого физического интерфейса команда привязывает указанный mac-список к данному интерфейсу.
no mac access-group *access_list_num* **in**		Удалить список с интерфейса.
ipv6 access-group *access_list_num* **in**	access_list_num: (1001..65535)	В настройках определённого физического интерфейса команда привязывает указанный список к данному интерфейсу.
no ipv6 access-group *access_list_num* **in**		Удалить список с интерфейса.

Команды режима Privileged EXEC

Командная строка в режиме Privileged EXEC имеет вид:

```
console#
```

Таблица 173 — Команды для просмотра списков ACL

Команда	*Значение/Значение по умолчанию*	*Действие*
show access-lists [*access_list_num***]**	access_list_num: (1-65535) символа	Показать списки ACL, созданные на коммутаторе.
show running-config acl	-	Показать блок команд ACL в конфигурации устройства.
show access-group [interface {gigabitethernet | tengiga-bitethernet} *interface* **| vlan [***vlan-id***]]**	-	Показать списки ACL, привязанные к интерфейсу.

4.25.1 Конфигурация ACL на базе IPv4

В данном разделе приведены значения и описания основных параметров, используемых в составе команд настройки списков ACL, основанных на адресации IPv4. Создание и вход в режим редактирования списков ACL, основанных на адресации IPv4, осуществляется по команде:

ip access-list {extended | standart} *access-list_num*.

Таблица 174 — Команды, используемые для настройки ACL-списков на основе IP-адресации

Команда	*Действие*
permit *protocol* **{any |** *source* **host} {any |** *destination***} [parametr]**	Добавить разрешающую запись фильтрации для протокола. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.
permit ip {any | *source* **host} {any |** *destination***} [parametr]**	Добавить разрешающую запись фильтрации для протокола IP. Пакеты, отвечающие условиям записи, будут обрабатываться коммутатором.

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

Таблица 175 — Основные параметры, используемые в командах

Параметр	***Значение***	***Действие***
permit	Действие ‘разрешить’	Создать разрешающее правило фильтрации в списке ACL.
deny	Действие ‘запретить’	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, ip, tcp, udp, ipv6, ipv6:icmp, ospf, pim,либо числовое значение протокола, в диапазоне (0 – 255). Для соответствия любому протоколу используется значение IP.
source	Адрес источника	Определяет IP-адрес источника пакета.
source_mask	Маска адреса источника	Маска, применяемая к IP-адресу источника пакета. Маска определяет биты IP-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Например, используя маску, можно определить для правила фильтрации IP-сеть. Чтобы добавить в правило фильтрации IP-сеть 195.165.0.0, необходимо задать значение маски 255.255.0.0, то есть, согласно данной маске, первые 16 бит IP-адреса будут игнорироваться.
destination	Адрес назначения	Определяет IP-адрес назначения пакета.
destination_mask	Маска адреса назначения	Битовая маска, применяемая к IP-адресу назначения пакета. Маска определяет биты IP-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Маска используется аналогично маске *source_mask.*
vlan	Идентификатор VLAN	Определяет VLAN, для которого будет применяться правило.
dscp	Поле DSCP в заголовке L3	Определяет значение DSCP-поля diffserv. Возможные коды сообщений поля **dscp:** (0 – 63).
	Приоритет IP	Определяет приоритет IP-трафика: (0-7).
icmp_type	-	Тип сообщений протокола ICMP, используемый для фильтрации ICMP-пакетов. Числовое значение типа сообщения, в диапазоне (0 – 255).
icmp_code	Код сообщения протокола ICMP	Код сообщений протокола ICMP, используемый для фильтрации ICMP-пакетов. Возможные коды сообщений поля *icmp_code***:** (0 – 255).

destination_port	UDP/TCP-порт назначения	Возможные значения поля TCP/UDP-порта: eq, gt, host, lt,range.
source_port	UDP/TCP-порт источника	
priority	Приоритет записи	Индекс задает положение правила в списке и его приоритет. Чем меньше индекс – тем приоритетнее правило. Диапазон допустимых значений (1..255).
optional parametr	Опциональный параметр	Опциональные параметры при конфигурировании списка доступа: **- tos —** фильтрация по байту ToS; - **user-defined** — фильтрация по User-defined bytes; **- sub-action** — дополнительное действие над трафиком. Доступные дополнительные действия — modify-vlan (изменение VLAN) и nested-vlan (добавление дополнительного тега VLAN).

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

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

4.25.2 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 extended *apv6_access-list*.

Таблица 176 — Команды, используемые для настройки ACL-списков на основе IP-адресации

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

deny tcp {any|*source* **host} {any|***destination***} [parametr]**	Добавить запрещающую запись фильтрации для протокола TCP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором.
deny udp {any|*source* **host} {any|***destination***} [parametr]**	Добавить запрещающую запись фильтрации для протокола UDP. Пакеты, отвечающие условиям записи, будут блокироваться коммутатором.

Таблица 177 — Основные параметры, используемые в командах

Параметр	*Значение*	*Действие*
permit	Действие ‘разрешить’	Создать разрешающее правило фильтрации в списке ACL.
deny	Действие ‘запретить’	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, ipv6.
source	Адрес источника	Определяет IP-адрес источника пакета.
destination	Адрес назначения	Определяет IP-адрес назначения пакета.
vlan	Идентификатор VLAN	Определяет VLAN, для которого будет применяться правило.
dscp	Поле DSCP в заголовке L3	Определяет значение DSCP-поля diffserv. Возможные коды сообщений поля **dscp:** (0 – 63).
icmp_type	-	Тип сообщений протокола ICMP, используемый для фильтрации ICMP-пакетов. Числовоезначениетипасообщения, вдиапазоне (0 – 255).
icmp_code	Код сообщения протокола ICMP	Код сообщений протокола ICMP, используемый для фильтрации ICMP-пакетов. Возможные коды сообщений поля *icmp_code***:** (0 – 255).
destination_port	UDP/TCP-порт назначения	Возможные значения поля TCP/UDP-порта: eq, gt, host, lt,range.
source_port	UDP/TCP-порт источника	
priority	Приоритет записи	Индекс задает положение правила в списке и его приоритет. Чем меньше индекс – тем приоритетнее правило. Диапазон допустимых значений(1..255).

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

4.25.3 Конфигурация ACL на базе MAC

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

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

Таблица 178 — Команды, используемые для настройки ACL-списков на основе MAC-адресации

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

Таблица 179 — Основные параметры, используемые в командах

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

source_mask	Битовая маска, применяемая к MAC-адресу источника пакета	Маска определяет биты MAC-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Например, используя маску, можно определить для правила фильтрации диапазона MAC-адресов. Чтобы добавить в правило фильтрации все MAC-адреса, начинающиеся на 00:00:02:AA.xx.xx, необходимо задать значение маски FF:FF:FF:FF:00:00, то есть, согласно данной маске, первые 16 бит MAC-адреса будут не важны для анализа.
destination	Адрес назначения	Определяет MAC-адрес назначения пакета.
destination_ mask	Битовая маска, применяемая к MAC-адресу назначения пакета	Маска определяет биты MAC-адреса, которые необходимо игнорировать. В значения игнорируемых битов должны быть записаны единицы. Маска используется аналогично маске source_ mask.
vlan_id	vlan_id: (0..4095)	Подсеть VLAN фильтруемых пакетов.
cvlan-priority	cvlan_priority: (0..7)	Класс обслуживания фильтруемых пакетов.
ethertype	eth_type: (0..0xFFFF)	Ethernet тип фильтруемых пакетов в шестнадцатеричной записи.
encaptype value	Value: (1..65535)	Тип ethertype для фильтруемых пакетов.
etype_list	*etype_list: (1..65535)*	Список стандартных ethertype.
priority	Индекс правила	Индекс правила в таблице, чем меньше индекс — тем приоритетнее правило 1-255.
Optional parameter	Опциональный параметр	Опциональные параметры при конфигурировании списка доступа: - **user-defined** — фильтрация по User-defined bytes; **- sub-action** — дополнительное действие над трафиком. Доступные дополнительные действия — modify-vlan (изменение VLAN), nested-vlan (добавление дополнительного тегаи VLAN) и modify-cvlan (добавление внутреннего тега VLAN).

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

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

Для прохождения остальных пакетов на интерфейсе требуется добавить второй ACL, разрешающий прохождение пакетов, не попадающих под правило фильтрации padi/pado:

```
console(config)# mac access-list extended 2
console(config-ext-macl)# permit any any
console(config-ext-macl)# ex
console(config)# interface gigabitethernet 0/1
console(config-if)# mac access-group 2 in
```

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

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

Для прохождения остальных пакетов на интерфейсе требуется добавить второй ACL, разрешающий прохождение пакетов, не попадающих под правило фильтрации padi/pado:

```
console(config)# mac access-list extended 2
console(config-ext-macl)# permit any any
console(config-ext-macl)# ex
console(config)# interface gigabitethernet 0/1
console(config-if)# mac access-group 2 in
```

4.26 Конфигурация защиты от DOS-атак

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

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 180 — Команды режима глобальной конфигурации

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

Вид запроса командной строки:

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

Таблица 181 — Команды режима конфигурации функционала firewall

Команда	*Значение/Значение по умолчанию*	*Действие*
enable	-/включено	Включить поддержку защиты от DOS-атак.
disable		Выключить поддержку защиты от DOS-атак.
ip tcp inspection syn-fin enable	-/включено	Включить обнаружение syn-fin-пакетов.
no ip tcp inspection syn-fin		Выключить обнаружение syn-fin-пакетов.
ip tcp inspection timeout *<sec>*	sec: (1..65535)/1	Установить таймер блокировки syn-fin-пакетов.
ip tcp limit syn-flag enable	-/выключено	Включить ограничение скорости для входящего TCP-трафика с флагом SYN.
ip tcp limit syn-flag disable		Выключить ограничение скорости для входящего TCP-трафика с флагом SYN.
notification interval *<sec>*	sec: (1..3600)/1	Установить временной интервал между SYSLOG-сообщениями о превышении ограничения входящего TCP-трафика с флагом SYN.
no notification interval		Установить значение по умолчанию.

Команды режима конфигурации интерфейса

Вид запроса командной строки режима конфигурации интерфейса:

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

Таблица 182 — Команды режима конфигурации интерфейса

Команда	*Значение/значение по умолчанию*	*Действие*
ip tcp limit syn-flag <*value*>	value: (1-262143) pps/ 100	Установить значение скорости для входящего TCP-трафика с флагом SYN на интерфейсе.
no ip tcp limit syn-flag		Выключить ограничение скорости для входящего TCP-трафика с флагом SYN на интерфейсе.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 183 — Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
Show running-config firewall	-	Отобразить настройку модуля firewall.
show firewall stats	-	Отобразить статистику по пакетам, обработанными модулем firewall.
show firewall tcp-syn-limit	-	Отобразить текущие настройки ограничения скорости для входящего TCP-трафика с флагом SYN.

4.27 Качество обслуживания – QoS

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

4.27.1 Настройка QoS

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 184 — Команды режима глобальной конфигурации

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

scheduler ***sched_num*** **interface {gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} sched-algo {strict-priority | wrr}**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); group: (1..24); sched_num: (1..65535)	Определить алгоритм работы планировщика на интерфейсе. - **strict-priority** – строгая очередь, имеет наивысший приоритет; - **strict-wrr** – очередь по механизму wrr, имеющая приоритет выше очереди wrr; - **wrr** – очередь, обрабатывающаяся по механизму wrr; - *fa/gi/two/te_port* – исходящий интерфейс.
no scheduler *sched_num* **interface {gigabitethernet** *gi_port* **| port-channel** *group***}**		Удалить настройки планировщика.
queue *queue_num* **interface {gigabitethernet** *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} [scheduler** *sched_num***] weight** *weight*	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); group: (1..24); queue_num: (1..8); weight: (1..127); sched_num: (1..65535)	Задать номер и вес очереди для исходящего интерфейса.
queue-map regn-priority {ipDscp *dscp_map* **| vlanPri** *cos_map***} queue-id** *queue_id*	dscp_map: (0..63); cas_map: (0..7); queue_id: (1..8)	Определить трафик с меткой CoS/DSCP в очередь.
no queue-map regn-priority {ipDscp *dscp_map* **| vlanPri** *cos_map***}**		Отменить определение трафика в очередь.
qos interface { gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***} def-user-priority** *priority*	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); Priority: (0..7)/0	Указать очередь для интерфейса, при условии отсутствия меток CoS/DSCP у входящих пакетов.
logging service cpu rate-limit [queue]	-/выключено	Включить отправку трапов о превышении порога cpu-rate-limit в syslog.
no logging service cpu rate-limit [queue]		Установить значение по умолчанию.
snmp-server enable traps cpu rate-limit [queue]	-/выключено	Включить генерацию уведомлений при превышении значения cpu-rate-limit.
no snmp-server enable traps cpu rate-limit [queue]		Отключить генерацию уведомления на устройстве.

Команды режима конфигурации VLAN

Вид запроса командной строки в режиме конфигурации VLAN:

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

Таблица 185 — Команды режима конфигурации VLAN

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

Команды режима конфигурации интерфейса Ethernet

Вид запроса командной строки:

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

Таблица 186 — Команды режима конфигурации интерфейса Ethernet

Команда	*Значение/Значение по умолчанию*	*Действие*
qos trust {cos | dscp | cos-dscp | none}	-/выключено	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.
no qos trust		Установить значения по умолчанию.
qos map regen-priority {vlanPri | ipDscp} enable	-/выключено	**- VlanPri** – разрешить установить на исходящем интерфейсе значение CoS в пакетах согласно настроенному внутреннему приоритету. **- ipDscp** – разрешить измерителю перемаркировывать трафик согласно настроенному алгоритму.
no qos map regen-priority {vlanPri | ipDscp} enable		Отменить настройки перемаркировки трафика на исходящем интерфейсе.
qos def-vlanPri source {inner-vlanPri/none/user-pri}	-/none	Устанавливает источник svlan-priority при использовании Dot1Q tunnel для входящего трафика на интерфейсе. **- inner-vlanPri** – копирует cvlan-priority в svlan-priority; **- user-pri** – значение svlan-priority берется из **qos interface {gigabitethenet/tengigabitethernet/port-channel** *port***} def-user-priority** *priority;* **- none** – значение по умолчанию, svlan-priority = 0.
no qos def-vlanPri source		Возвращается значение по умолчанию.

Команды режима редактирования списка критериев классификации трафика

Вид запроса командной строки режима редактирования списка критериев классификации трафика:

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

Таблица 187 — Команды режима редактирования списка критериев классификации трафика

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

Команды режима редактирования стратегии классификации трафика

Вид запроса командной строки режима редактирования стратегии классификации трафика:

```
console# configure terminal
console(config)# policy-map policy-map-name
console(config-ply-map)#
```

Таблица 188 — Команды режима редактирования стратегии классификации трафика

Команда	*Значение/Значение по умолчанию*	*Действие*
set policy class *class_num* **default-priority-type {vlanPri** *new_cos_map* **| ipDscp** *new_dscp_map***}**	class_num: (0..65535); new_cos_map: (0..7); new_dscp_map: (0..63)	Установить новое значение метки для пакета.
set meter *meter*	-	Установить ограничение для скорости потока согласно настроенному алгоритму.
no set meter		Удалить ограничение для скорости потока согласно настроенному алгоритму.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 189 — Команды режима глобальной конфигурации

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

Команды режима конфигурации измерителя ограничения скорости для входящего трафика

Вид запроса командной строки в режиме конфигурации:

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

Таблица 190 — Команды режима конфигурации измерителя ограничения скорости

Команда	*Значение/Значение по умолчанию*	*Действие*
meter-type avgRate cir {*cir_value***} mode {bytes | packets}**	-	Установить ограничение скорости для исходящего трафика согласно алгоритму avgRate (leaky bucket).
meter-type srTCM cir {*cir_value***} cbs {***cbs_value***} ebs {***ebs_value***} mode {bytes | packets} [color-aware]**	-	Установить ограничение скорости для исходящего трафика согласно алгоритму single rate — Three Color Marker (rfc2697). **Color-aware** – включает анализ DSCP при анализе объема трафика.
meter-type trTCM cir {*cir_value***} cbs {***cbs_value***} eir {***eir_value***} ebs {***ebs_value***} mode {bytes | packets} [color-aware]**	-	Установить ограничение скорости для исходящего трафика согласно алгоритму two rate – Three Color Marker (rfc2698). **Color-aware** – включает анализ DSCP при анализе объема трафика.

Для корректной работы измерителя с алгоритмами sr-TCM и tr-TCM требуется установить на исходящем интерфейсе команду qos map regen-priority ipDscp enable.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 191 — Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
show qos global info	-	Отобразить глобальные настройки qos.
show qos def-user-priority [gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **|port-channel** *group***]**	-	Показать в какую очередь определены интерфейсы.
show queue-map [gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **|port-channel** *group***]**	-	Отобразить маппинг CoS и DSCP по умолчанию.
show qos trust	-	Просмотр текущих настроек доверия меткам cos и dscp.
show qos queue-stats [interface gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port***]**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11)	Отобразить статистику QoS.

Пример применения сервисной политики:

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

```
console(config)# ip access-list extended 1008
console(config-ext-nacl)# permit ip any any traffic-class 8 sub-action modify-vlan 100
console(config-ext-nacl)# !
console(config)# interface gigabitethernet 0/6
console(config-if)# qos trust cos
console(config-if)# switchport mode trunk
console(config-if)# ip access-group 1008 in
console(config-if)# !
console(config)# interface gigabitethernet 0/7
console(config-if)# switchport mode trunk
console(config-if)# qos map regen-priority-type vlanPri enable
console(config-if)# !
console(config)# class-map 1008
console(config-cls-map)# match access-group ip-access-list 1008
console(config-cls-map)# set class 1008 regen-priority 7 group-name QOS
console(config-cls-map)# !
console(config)# meter 10
console(config-meter)# meter-type avgRate cir 512 kbps
console(config-meter)# !
console(config)# policy-map 1008
console(config-ply-map)# set policy class 1008 default-priority-type ipDscp 63
```

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 192 — Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

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

Пример настройки ограничении скорости портаGigabitEthernet 0/4:

```
console# configure terminal
console(config)# vlan 10
console(config-vlan)# vlan active
console(config-vlan)# !
console(config)# interface gigabitethernet 0/4
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 10
console(config-if)# rate-limit input 512
console(config-if)# rate-limit output 512
```

Пример настройки QoS:

Настроить планировщик по алгоритму wrr для исходящего интерфейса gi0/1. Распределить трафик согласно полю CoS в очереди 1-4. Назначить вес wrr для очередей согласно номеру очереди. Очередь 5 объявить приоритетной.

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

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

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

4.28 Конфигурация протоколов маршрутизации

4.28.1 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 193 — Команды режима конфигурации интерфейса Ethernet, группы интерфейсов

Команда	*Значение/Значение по умолчанию*	*Действие*
ip route *prefix* **{ip_mask |prefix_length}** ***{gateway***	prefix_length: (0..32); distance (1..255)/1 vlan_id: (1..4094)	Создать статическое правило маршрутизации. - *prefix* – сеть назначения (например, 172.7.0.0); - *mask* – маска сети (в формате десятичной системы счисления); - *gateway* – шлюз для доступа к сети назначения; - *distance* – вес маршрута; - *vlan_id* – задаётся в том случае, если сеть назначения напрямую (directly) подключена к интерфейсу, соответствующему *vlan_id.*
no ip route [all | *prefix {ip_mask |prefix_length**}** [gateway]]*		Удалить правило из таблицы статической маршрутизации. - *all* – удалить все правила из таблицы статической маршрутизации.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 194 — Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip route [*prefix [mask]***| connected | details | failed | static | summary]**	-	Показать таблицу маршрутизации, удовлетворяющую заданным критериям. - *prefix* – сеть назначения; - *mask* – маска сети (в формате десятичной системы счисления); - **connected** – подключенный маршрут, то есть маршрут,взятый с непосредственно подключенного и функционирующего интерфейса; - **details** – детализированная информация; - **failed** – маршруты, установленные с ошибками; - **static** – статический маршрут, прописанный в таблице маршрутизации; - **summary** – общее количество маршрутов.

4.28.2 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 — 32.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 195 — Команды режима глобальной конфигурации

Команда	*Значение/Значение по умолчанию*	*Действие*
vrrp enable	-/выключено	Включить VRRP глобально. **Для того чтобы VRRP заработал на интерфейсах, нужно включить VRRP глобально.**
no vrrp enable		Удалить правило из таблицы статической маршрутизации.
vrrp version {v2 | v3}	-/v2	Задать версию VRRP.

Команды режима конфигурации интерфейсов VLAN

Вид запроса командной строки в режиме конфигурации интерфейсов VLAN:

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

Таблица 196 — Команды режима конфигурации интерфейс VLAN

Команда	*Значение/Значение по умолчанию*	*Действие*
vrrp *vrid* **ipv4** *ip_address*	vrid: (1..255)/-	Определить IPv4-адрес VRRP-маршрутизатора.
no vrrp *vrid* **ipv4** [*ip_address*]		Удалить виртуальный маршрутизатор *vrid* на данном устройстве.
vrrp *vrid* **accept-mode {enable | disable}**	vrid: (1..255)/ выключено	**enable** – включить режим, в котором VR-адрес будет отвечать на ICMP-запросы и принимать запросы на подключение по Telnet и SSH; **disable** – выключить данный режим.
vrrp *vrid* **preempt**	vrid: (1..255)/ 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**		Выключить режим преемственности.

vrrp *vrid* **priority** *priority*	vrid: (1..255); priority: (1..254)/ 255 для владельца IP-адреса, 100 для остальных	Назначить приоритет VRRP-маршрутизатора.
no vrrp *vrid* **priority**		Установить значение по умолчанию.
vrrp *vrid* **timer {***seconds***| msec** *milliseconds***}**	seconds: (1..255); milliseconds: (10..255000)/ 1 сек	Определить интервал между анонсами master-маршрутизатора.
no vrrp *vrid* **timer**		Установить значение по умолчанию.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 197 — Команды режима EXEC

Команда	*Значение/Значение по умолчанию*	*Действие*
show vrrp [detail | statistics | interface vlan *vlan_id* **|** *vrid* **[detail | statistics]]**	vrid: (1..255)/-	Просмотреть краткую или детальную информацию для всех или одного настроенного виртуального маршрутизатора VRRP. - **detail** – просмотр детальной информации; - **statistics** – просмотр общей статистики.

4.28.3 Настройка протокола OSPFv2

OSPF (Open Shortest Path First) — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующийся для нахождения кратчайшего пути алгоритм Дейкстры. Протокол OSPF представляет собой протокол внутреннего шлюза (IGP). Протокол OSPF распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы.

Команды режима глобальной конфигурации для OSPFv2

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 198 — Команды режима глобальной конфигурации OSPFv2

Команда	*Значение/Значение по умолчанию*	*Действие*
router ospf	-/-	Зайти в режим конфигурации процесса OSPFv2.

Команды режима процесса OSPFv2

Вид запроса командной строки в режиме конфигурации процесса OSPFv2:

```
console(config-router)#
```

Таблица 199 — Команды режима конфигурации процесса OSPFv2

Команда	*Значение/Значение по умолчанию*	*Действие*
shutdown	-/выключен	Выключить OSPF-процесс. **По умолчанию OSPF-процесс выключен**.

no shutdown		Включить OSPF-процесс.
distance *dist*	dist: (1..255)/110	Установить административную дистанцию для OSPF.
no distance		Установить значение по умолчанию.
default-information originate always [metric *metric***] [metric-type {1 | 2}]**	metric: (1..16777214)/20	Включить анонсирование шлюза по умолчанию, вне зависимости от того задан ли он статическим маршрутом или не задан.
no default-information originate always [metric *metric***] [metric-type {1 |2}]**		Установить значение по умолчанию. В случае указания параметра вернуть его значение по умолчанию.
set nssa asbr-default-route translator {enable | disable}	-/выключено	Включить или выключить трансляцию маршрута по умолчанию (установить P-бит) в NSSA на ASBR, который не является ABR. **Должно быть включено анонсирование маршрута по умолчанию (default-information originate always).**
redistribute connected [metric *metric***] [metric-type {1 | 2}]**	metric: (1..16777214)/20	Разрешить анонсирование connected-маршрутов: - **metric-type 1** — установить тип импортируемых маршрутов как external-1; - **metric-type 2** — установить тип импортируемых маршрутов как external-2; - *metric* — значение метрики для импортируемых маршрутов.
no redistribute connected [metric]		Запретить анонсирование connected-маршрутов. В случае указания параметра вернуть его значение по умолчанию.
redistribute static [metric *metric***] [metric-type {1 | 2}]**	metric: (1..16777214)/20	Разрешить анонсирование статических маршрутов: - **metric-type 1** — установить тип импортируемых маршрутов как external-1; - **metric-type 2** — установить тип импортируемых маршрутов как external-2; - *metric* — значение метрики для импортируемых маршрутов.
no redistribute static [metric]		Запретить анонсирование статических маршрутов. В случае указания параметра вернуть его значение по умолчанию.
redistribute rip [metric *metric***] [metric-type {1 | 2}]**	metric: (1..16777214)/20	Разрешить анонсирование маршрутов, полученных по протоколу RIP: - **metric-type 1** — установить тип импортируемых маршрутов как external-1; - **metric-type 2** — установить тип импортируемых маршрутов как external-2; - *metric* — значение метрики для импортируемых маршрутов.
no redistribute rip [metric]		Запретить анонсирование маршрутов, полученных по протоколу RIP. В случае указания параметра вернуть его значение по умолчанию.
redistribute bgp [metric *metric***] [metric-type {1 | 2}]**	metric: (1..16777214)/20	Разрешить анонсирование маршрутов, полученных по протоколу BGP: - **metric-type 1** — установить тип импортируемых маршрутов как external-1; - **metric-type 2** — установить тип импортируемых маршрутов как external-2; - *metric* — значение метрики для импортируемых маршрутов.
no redistribute bgp [metric]		Запретить анонсирование маршрутов, полученных по протоколу BGP. В случае указания параметра вернуть его значение по умолчанию.
redistribute all [metric *metric***] [metric-type {1 | 2}]**	metric: (1..16777214)/20	Разрешить анонсирование маршрутов, полученных по всем поддерживаемым протоколам маршрутизации: - **metric-type 1** — установить тип импортируемых маршрутов как external-1; - **metric-type 2** — установить тип импортируемых маршрутов как external-2; - *metric* — значение метрики для импортируемых маршрутов.

no redistribute all [metric]		Запретить анонсирование маршрутов, полученных по всем поддерживаемым протоколам маршрутизации. В случае указания параметра вернуть его значение по умолчанию.
compatible rfc1583	-/включено	Включить совместимость с RFC 1583.
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		Установить значение по умолчанию.
network *ip_addr* **area** *A.B.C.D*	A.B.C.D: идентификатор зоны в формате IPv4-адреса	Включить OSPF на IP-интерфейсе.
no network *ip_addr*		Удалить IP-адрес интерфейса.
area *A.B.C.D* **stub [no-summary]**	A.B.C.D: идентификатор зоны 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 [no-summary]**		Установить значение по умолчанию.
area *A.B.C.D* **nssa [no-summary] [default-information-originate [metric** *metric*] **[metric-type {1 | 2}]]**	A.B.C.D: идентификатор зоны в формате IPv4-адреса; metric: (1..16777214)/20	Установить для указанной зоны тип NSSA. - **no-summary** — не отправлять информацию о суммированных внешних маршрутах внутрь NSSA-зоны; - **default-information-originate** — включить анонсирование шлюза по умолчанию, вне зависимости от того задан ли он статическим маршрутом или не задан; - **metric-type 1** — установить тип маршрута по умолчанию как external-1; - **metric-type 2** — установить тип маршрута по умолчанию как external-2; - *metric* — значение метрики для анонсируемого маршрута.
no area *A.B.C.D* **nssa [no-summary] [default-information-originate]**		Установить значение по умолчанию. В случае указания параметра вернуть его значение по умолчанию.
area *A.B.C.D* **default-cost** *metric*	A.B.C.D: идентификатор зоны в формате IPv4-адреса; metric: (1..16777215)/20	Установить метрику для шлюза по умолчанию в анонсах для зон stub и NSSA.
no area *A.B.C.D* **default-cost**		Установить значение по умолчанию.
area *A.B.C.D* **range** *ip_addr prefix_length* **{summary | Type7} [advertise | not-advertise]**	A.B.C.D: идентификатор зоны в формате IPv4-адреса;	Выполнить суммирование маршрутов, попадающих под указанный диапазон. - **summary** — для межзональных маршрутов (LSA тип-3); - **Type7** — для внешних маршрутов из NSSA в магистральную зону; - **advertise** — объявить указанный маршрут; - **not-advertise** — не объявлять указанный маршрут.
no area *A.B.C.D* **range** *ip_addr prefix_length*		Удалить суммирование маршрутов для данной OSPF-зоны.
area *A.B.C.D* **translation-role {always | candidate}**	A.B.C.D: идентификатор зоны в формате IPv4-адреса	Установить роль транслятора в NSSA-зоне. - **always** — транслировать всегда LSA тип-7 в LSA тип-5; - **candidate** — участвовать в процессе выбора транслятора.
no area *A.B.C.D* **translation-role**		Установить значение по умолчанию.
area *A.B.C.D* **stability-interval** *sec*	sec: (0..2147483647)/40 секунд	Период стабилизации в секундах, для транслятора в NSSA.
no area *A.B.C.D* **stability-interval**		Установить значение по умолчанию.
area *A.B.C.D* **virtual-link** *E.F.G.H* **[dead-interval** *dead*]	A.B.C.D: идентификатор зоны в формате IPv4-адреса;	Создать виртуальное соединение между магистральной и немагистральной зонами, между которыми присутствует другая немагистральная зона.

[hello-interval *hello***] [retransmit-interval** *ret***]**	E.F.G.H: идентификатор маршрутизатора назначения в формате IPv4-адреса; dead:(1..65535)/40 секунд; hello: (1..65535)/10 секунд ret: (1..3600)/5 секунд	- **dead-interval** — указать dead-интервал; - **hello-interval** — указать hello-интервал; - **retransmit-interval** — указать интервал меду повторными передачами.
no area *A.B.C.D* **virtual-link** *E.F.G.H*		Удалить виртуальное соединение.
passive-interface {default | loopback *loopback* **| vlan** *vlan_id***}**	loopback: (0..100); vlan_id: (1..4094)/disabled	Запретить IP-интерфейсу обмениваться протокольными сообщениями с соседями через указанные интерфейсы. - **default** — запретить для всех интерфейсов.
no passive-interface {default | loopback *loopback* **| vlan** *vlan_id***}**		Разрешить IP-интерфейсу обмениваться протокольными сообщениями с соседями через указанные интерфейсы.
neighbor *ip_addr*	ip_addr: A.B.C.D	Задать вручную OSPF-соседа.
no neighbor *ip_addr*		Удалить OSPF-соседа.
redist-config *ip_addr prefix_length* **[metric-type {asExttype1 | asExttype2}] [metric-value** *metric***]**	metric: (1..16777215)/20	Установить параметры редистрибуции для внешних маршрутов. - *ip_addr* — IP-адрес сети назначения; - *prefix_length* — IP-маска сети; - **metric-type asExttype1** — установить тип маршрута external-1; - **metric-type asExttype2** — установить тип маршрута external-2; - *metric-value* – установить значение метрики.
no redist-config *ip_addr prefix_length*		Удалить установленные параметры редистрибуции для заданного маршрута.
summary-external *ip_addr prefix_length* **[advertise | allowAll | denyAll | not-advertise] [translation {disabled | enabled}]**	-/отключено	Выполнить суммирование внешних маршрутов. - *ip_addr* — IP-адрес сети; - *prefix_length* — IP-маска сети; - **advertise** – суммированный маршрут объявляется в LSA тип-5; если тип зоны NSSA, то маршрут не объявляется; - **allowAll** — суммированный маршрут объявляется в LSA тип-5; если тип зоны NSSA, то маршрут объявляется в LSA тип-7; - **denyAll** - суммированный маршрут не объявляется; - **not-advertise** — суммированный маршрут не объявляется в LSA тип-5; если тип зоны NSSA, то маршрут объявляется в LSA тип-7; - **translation disabled** — не устанавливать P-бит в генерируемых LSA тип-7; - **translation enabled** — установить P-бит в генерируемых LSA тип-7.
no summary-external *ip_addr prefix_length*		Выключить суммирование внешних маршрутов.
capability opaque	-/отключено	Включить поддержку opaque LSA.
no capability opaque		Выключить поддержку opaque LSA.

Команды режима конфигурации интерфейса VLAN для OSPFv2

Вид запроса командной строки:

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

Таблица 200 — Команды режима конфигурации интерфейса VLAN для OSPFv2

Команда	***Значение/Значение по умолчанию***	***Действие***
ip ospf network {broadcast | non-broadcast | point-to-multipoint | point-to-point}	-/broadcast	Выбрать тип сети: - **broadcast** — широковещательная сеть с множественным доступом; - **non-broadcast** — нешироковещательная сеть, в данном случае адреса соседних маршрутизаторов настраиваются вручную;

		- **point-to-multipoint** – многоточечная сеть; - **point-to-point** — сеть «точка-точка».
no ip ospf network		Установить значение по умолчанию.
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 dead-interval *sec*	sec: (1..65535)/40 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 ip ospf dead-interval		Установить значение по умолчанию.
ip ospf hello-interval *sec*	sec: (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	-/выключено	Отключить проверку MTU при установлении соседства.
no ip ospf mtu-ignore		Установить значение по умолчанию.
ip ospf priority *prior*	prior: (0..255)/1	Установить приоритет маршрутизатора, который используется для выбора DR и BDR.
no ip ospf priority		Установить значение по умолчанию.
ip ospf poll-interval *sec*	sec: (1..2147483647)/120 секунд	Установить период между посылкой hello-пакетов для неактивного non-broadcast соседа.
no ip ospf poll-interval		Установить значение по умолчанию.
ip ospf retransmit-interval *sec*	sec: (1..3600)/5 секунд	Установить интервал времени в секундах, по истечении которого маршрутизатор повторно отправит пакет, на который не получил подтверждения о получении (например, DatabaseDescription- или LinkStateRequest-пакеты).
no ip ospf retransmit-interval		Установить значение по умолчанию.
ip ospf transmit-delay *sec*	sec: (1..3600)/1 секунд	Установить примерное время в секундах, необходимое для передачи пакета состояния канала.
no ip ospf transmit-delay		Установить значение по умолчанию.
ip ospf demand-circuit	-/выключено	Включить подавление отправки hello-сообщений (для интерфейсов типа point-to-point и point-to-multipoint и периодических обновлений LSA).
no ip ospf demand-circuit		Установить значение по умолчанию.
ip ospf authentication {message-digest | null | sha-1 | sha-224 | sha-256 | sha-384 | sha-512 | simple}	-/выключено	Включить OSPF-аутентификацию и задать её тип. - **message-digest** — использовать шифрование MD5; - **null** — не использовать аутентификацию; - **sha-1** — использовать шифрование SHA-1; - **sha-224** — использовать шифрование SHA-1; - **sha-256** — использовать шифрование SHA-256; - **sha-384** — использовать шифрование SHA-384; - **sha-512** — использовать шифрование SHA-512; - **simple** — не использовать шифрование (пароль передается в открытом виде).
no ip ospf authentication		Выключить OSPF-аутентификацию.
ip ospf authentication-key *simple_password*	simple_password: (1..64) символов	Установить пароль, который предназначен для простого типа аутентификации (передача пароля в открытом виде).
no ip ospf authentication-key		Удалить пароль.
ip ospf message-digest-key *key_id* **{md5 | sha-1 | sha-224 | sha-**	key_id (0..255) string (1..64)	Добавить ключ аутентификации. - *key_id* — идентификатор ключа; - **md5** — шифровать ключ алгоритмом MD5;

256 | sha-384 | sha-512} *string*		- **sha-1** — шифровать ключ алгоритмом SHA-1; - **sha-224** — шифровать ключ алгоритмом SHA-224; - **sha-256** — шифровать ключ алгоритмом SHA-256; - **sha-384** — шифровать ключ алгоритмом SHA-384; - **sha-512** — шифровать ключ алгоритмом SHA-512; - *string* — пароль.
no ip ospf message-digest-key *key_id*		Удалить ключ аутентификации.
ip ospf key *key_id* **{start-accept | start-generate | stop-accept | stop-generate}** *dd-mon-year,hh:mm*	key_id (0..255); dd (01..31); mon: (Jan..Dec); year: (2000..2100); hh: (00..23); mm: (00..59)	Установить параметры для ключа аутентификации. - **start-accept** — задать время, начиная с которого действует ключ на приём; - **start-generate** — задать время, начиная с которого действует ключ на передачу; - **stop-accept** — задать время, до которого действует ключ на приём; - **stop-generate** — задать время, до которого действует ключ на передачу.
no ip ospf key *key_id* **[start-accept | start-generate | stop-accept | stop-generate]**		Сбросить параметры для ключа аутентификации.

Команды режима privileged EXEC

Вид запроса командной строки в режиме privileged EXEC:

```
console#
```

Таблица 201 — Команды режима privileged EXEC для OSPFv2

Команда	*Значение/Значение по умолчанию*	*Действие*
show ip ospf	-	Отобразить конфигурацию OSPF.
show ip ospf neighbor	-	Отобразить информацию об OSPF-соседях.
show ip ospf route	-	Отобразить таблицу маршрутизации OSPF.
show ip ospf interface [vlan *vlan_id***]**	vlan_id: (1..4094)	Отобразить конфигурацию OSPF-интерфейсов. - vlan — для конкретного интерфейса VLAN.
show ip ospf virtual-links	-	Отобразить параметры и текущее состояние виртуальных линков.
show ip ospf database [adv-router *A.B.C.D* **| self-originate]**	A.B.C.D: IP-адрес	Отобразить состояние базы данных протокола OSPF. - **adv-router** — для конкретного маршрутизатора; - **self-originate** — для локального маршрутизатора.
show ip ospf database {asbr-summary | external | network | nssa-external | summary | opaque-area | opaque-as | opaque-link | router} [*A.B.C.D* **| adv-router** *A.B.C.D* **| self-originate]**	A.B.C.D: IP-адрес	Отобразить состояние базы данных протокола OSPF, только, для определённых типов LSA: - **asbr-summary** — для LSA тип-4; - **external** — для LSA тип-5 и тип-7; - **network** — для LSA тип-2; - **nssa-external** — для LSA тип-7; - **summary** — для LSA тип-3; - **opaque-area** — для LSA тип-10; - **opaque-as** — для LSA тип-11; - **opaque-link** — для LSA тип-9; - **router** — для LSA тип-1.
show ip ospf database database-summary	-	Отобразить общую статистику для базы данных OSPF.
show ip ospf *area_id* **database**	area_id: идентификатор зоны	Отобразить состояние базы данных протокола OSPF для определённой зоны.
show ip ospf border-routers	-	Отобразить список пограничных маршрутизаторов.
show ip ospf {summary-address | area-range}	-	Отобразить суммированные маршруты: - summary-address — для LSA тип-5 и тип-7; - area-range — для LSA тип-3.

4.28.4 Настройка протокола OSPFv3

Команды режима глобальной конфигурации для OSPFv3

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 202 — Команды режима глобальной конфигурации OSPFv3

Команда	*Значение/Значение по умолчанию*	*Действие*
router ospf	-/-	Зайти в режим конфигурации процесса OSPFv3.

Команды режима процесса OSPFv3

Вид запроса командной строки в режиме конфигурации процесса OSPFv3:

```
console(config-router)#
```

Таблица 203 — Команды режима конфигурации процесса OSPFv3

Команда	*Значение/Значение по умолчанию*	*Действие*
shutdown	-/выключен	Выключить OSPF-процесс. **По умолчанию OSPF-процесс выключен**.
no shutdown		Включить OSPF-процесс.
nssa asbr default-route-translator	-/выключено	Включить трансляцию маршрута по умолчанию (установить P-бит) в NSSA на ASBR, который не является ABR.
no nssa asbr default-route-translator		Установить значение по умолчанию.
redistribute connected	-/выключено	Разрешить анонсирование connected-маршрутов.
no redistribute connected		Запретить анонсирование connected-маршрутов.
redistribute static	-/выключено	Разрешить анонсирование статических маршрутов.
no redistribute static		Запретить анонсирование статических маршрутов.
redistribute bgp	-/выключено	Разрешить анонсирование маршрутов, полученных по протоколу BGP.
no redistribute bgp		Запретить анонсирование маршрутов, полученных по протоколу BGP.
router-id {*A.B.C.D* **| auto}**	A.B.C.D: идентификатор маршрутизатора в формате IPv4-адреса/auto	Установить идентификатор маршрутизатора, который уникально идентифицирует маршрутизатор в пределах одной автономной системы: - *A.B.C.D* — задать идентификатор вручную; - **auto** — в качестве router-id будут использованы последние четыре байта базового MAC-адреса коммутатора.
area *A.B.C.D* **stub [no-summary]**	A.B.C.D: идентификатор зоны 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]**	A.B.C.D: идентификатор зоны в формате IPv4-адреса	Установить для указанной зоны тип NSSA. - **no-summary** — не отправлять информацию о суммированных внешних маршрутах.
no area *A.B.C.D* **nssa**		Установить значение по умолчанию. В случае указания параметра вернуть его значение по умолчанию.
area *A.B.C.D* **default-metric** *cost*	A.B.C.D: идентификатор зоны в формате IPv4-адреса;	Установить цену для шлюза по умолчанию в анонсах для зон stub и NSSA.
no area *A.B.C.D* **default-**		Установить значение по умолчанию.

metric	cost: (1..16777215)/20	
area *A.B.C.D* **default-metric type {1 | 2}**	A.B.C.D: идентификатор зоны в формате IPv4-адреса	Установить тип для маршрута по умолчанию в NSSA: - **type 1** — тип external-1; - **type 2** — тип external-2.
no area *A.B.C.D* **default-metric type**		Установить тип для маршрута по умолчанию как external-1.
area *A.B.C.D* **range** *ip_addr prefix_length* **[advertise | not-advertise] {summary | Type7}**	A.B.C.D: идентификатор зоны в формате IPv4-адреса	Выполнить суммирование маршрутов, попадающих под указанный диапазон. - **summary** — для межзональных маршрутов (LSA тип-3); - **Type7** — для внешних маршрутов из NSSA в магистральную зону; - **advertise** — объявить указанный маршрут; - **not-advertise** — не объявлять указанный маршрут.
no area *A.B.C.D* **range** *ip_addr prefix_length* **{summary | Type7}**		Удалить суммирование маршрутов для данной OSPF-зоны.
area *A.B.C.D* **summary-prefix** *ip_addr prefix_length* **[advertise | allowAll | denyAll | not-advertise] [translation {disabled | enabled}]**	-/отключено	Выполнить суммирование внешних маршрутов. - *ip_addr* — IP-адрес сети; - *prefix_length* — IP-маска сети; - **advertise** — суммированный маршрут объявляется в LSA тип-7 для NSSA; не объявляется если трансляция происходит из магистральной зоны в NSSA; - **allowAll** — правило применяется, только, со стороны магистральной зоны; суммированный маршрут объявляется в LSA тип-7, если трансляция происходит из магистральной зоны в NSSA; - **denyAll** — правило применяется только со стороны магистральной зоны; суммированный маршрут не объявляется; - **not-advertise** — суммированный маршрут не объявляется в NSSA; объявляется в LSA тип-7 если трансляция происходит из магистральной зоны в NSSA; - **translation disabled** — не устанавливать P-бит в генерируемых LSA тип-7; - **translation enabled** — установить P-бит в генерируемых LSA тип-7.
no area *A.B.C.D* **summary-prefix** *ip_addr prefix_length*		Выключить суммирование внешних маршутов.
area *A.B.C.D* **translation-role {always | candidate}**	A.B.C.D: идентификатор зоны в формате IPv4-адрес	Установить роль транслятора в NSSA зоне. - **always** — транслировать всегда LSA тип-7 в LSA тип-5; - **candidate** — участвовать в процессе выбора транслятора.
no area *A.B.C.D* **translation-role**		Установить значение по умолчанию.
area *A.B.C.D* **stability-interval** *sec*	sec: (1..65535)/40 секунд	Период стабилизации в секундах, для транслятора в NSSA.
no area *A.B.C.D* **stability-interval**		Установить значение по умолчанию.
area *A.B.C.D* **virtual-link** *E.F.G.H index* **[dead-interval** *dead***] [hello-interval** *hello***] [retransmit-interval** *ret***] [transmit-delay** *delay***]**	A.B.C.D: идентификатор зоны в формате IPv4-адреса; E.F.G.H: идентификатор маршрутизатора назначения в формате IPv4-адреса; index: (1..2147483647); dead:(1..65535)/40 секунд; hello: (1..65535)/10 секунд ret: (1..1800)/5 секунд; delay: (1..1800)/1 секунда	Создать виртуальное соединение между магистральной и немагистральной зонами, между которыми присутствует другая немагистральная зона. - *index* — указать индекс, который будет идентифицировать данный виртуальный канал; - **dead-interval** — указать dead-интервал; - **hello-interval** — указать hello-интервал; - **retransmit-interval** — указать интервал между повторными передачами; - **transmit-delay** — указать примерное время передачи пакета в сети.
no area *A.B.C.D* **virtual-link** *E.F.G.H*		Удалить виртуальное соединение.
passive-interface	-/выключено	Запретить для всех IP-интерфейсов, созданных после

		ввода данной команды, обмениваться протокольными сообщениями с соседями.
no passive-interface		Установить значение по умолчанию.
redist-config *ip_addr prefix_length* **[metric-value** *metric***] [metric-type {asExttype1 | asExttype2}]**	metric: (1..16777215)/20	Установить параметры редистрибуции для внешних маршрутов. - *ip_addr* — IP-адрес сети назначения; - *prefix_length* — IP-маска сети; - *metric-value* — установить значение метрики; - **metric-type asExttype1** — установить тип маршрута external-1; - **metric-type asExttype2** — установить тип маршрута external-2.
no redist-config *ip_addr prefix_length*		Удалить установленные параметры редистрибуции для заданного маршрута.

*Команды режима конфигурации интерфейса VLAN для OSPFv*3

Вид запроса командной строки:

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

Таблица 204 — Команды режима конфигурации интерфейса VLAN для OSPFv3

Команда	***Значение/Значение по умолчанию***	***Действие***
ipv6 ospf area *A.B.C.D*	A.B.C.D: идентификатор зоны в формате IPv4-адреса	Включить OSPFv3 на интерфейсе.
no ipv6 ospf		Выключить OSPFv3 на интерфейсе.
ipv6 ospf network {broadcast | non-broadcast | point-to-multipoint | point-to-point}	-/broadcast	Выбрать тип сети: - **broadcast** — широковещательная сеть с множественным доступом; - **non-broadcast** — нешироковещательная сеть, в данном случае адреса соседних маршрутизаторов настраиваются вручную; - **point-to-multipoint** — многоточечная сеть; - **point-to-point** — сеть «точка-точка».
no ipv6 ospf network		Установить значение по умолчанию.
ipv6 ospf neighbor *link_local_addr*	-/не задан	Добавить статического соседа: - *link_local_addr* — указать IPv6 link-local адрес соседа.
no ipv6 ospf neighbor *link_local_addr*		Удалить статического соседа.
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 *sec*	sec: (1..65535)/40 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 *sec*	sec: (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 при установлении соседства.
no ipv6 ospf mtu-ignore		Установить значение по умолчанию.
ipv6 ospf passive-interface	-/выключено	Запретить IP-интерфейсу обмениваться протокольными сообщениями с соседями через данный интерфейс.
no ipv6 ospf passive-		Установить значение по умолчанию.

interface		
ipv6 ospf priority *prior*	prior: (1..255)/1	Установить приоритет маршрутизатора, который используется для выбора DR и BDR.
no ipv6 ospf priority		Установить значение по умолчанию.
ipv6 ospf poll-interval *sec*	sec: (1..65535)/120 секунд	Установить период между посылкой hello-пакетов для неактивного non-broadcast соседа.
no ipv6 ospf poll-interval		Установить значение по умолчанию.
ipv6 ospf retransmit-interval *sec*	sec: (1..1800)/5 секунд	Установить интервал времени в секундах, по истечении которого маршрутизатор повторно отправит пакет, на который не получил подтверждения о получении.
no ipv6 ospf retransmit-interval		Установить значение по умолчанию.
ipv6 ospf transmit-delay *sec*	sec: (1..1800)/1 секунд	Установить примерное время в секундах, необходимое для передачи пакета состояния канала.
no ipv6 ospf transmit-delay		Установить значение по умолчанию.
ipv6 ospf demand-circuit	-/выключено	Включить подавление отправки hello-сообщений (для интерфейсов типа point-to-point и point-to-multipoint) и периодических обновлений LSA.
no ipv6 ospf demand-circuit		Установить значение по умолчанию.

Команды режима privileged EXEC

Вид запроса командной строки в режиме privileged EXEC:

```
console#
```

Таблица 205 — Команды режима privileged EXEC для OSPFv3

Команда	***Значение/Значение по умолчанию***	***Действие***
show ipv6 ospf	-	Отобразить конфигурацию OSPF.
show ipv6 ospf area *A.B.C.D* **database**	A.B.C.D: идентификатор зоны в формате IPv4-адреса;	Отобразить состояние базы данных конкретной зоны.
show ipv6 ospf border-routers	-	Отобразить список пограничных маршрутизаторов.
show ipv6 ospf database [as-external | inter-prefix | inter-router | intra-prefix | link | network | nssa | router] [HEX] [detail]	-	Отобразить состояние базы данных протокола OSPF: - **as-external** — для LSA тип-5 и тип-7; - **inter-prefix** — для LSA тип-3; - **inter-router** — для LSA тип-4; - **intra-prefix** — для LSA тип-9; - **link** — для LSA тип-8; - **network** — для LSA тип-2; - **nssa** — для LSA тип-7; - **router** — для LSA тип-1; - **HEX** — отобразить информацию в 16-ом виде; - **detail** — отобразить детальную информацию об LSA.
show ipv6 ospf interface [vlan *vlan_id***]**	vlan_id: (1..4094)	Отобразить конфигурацию OSPF-интерфейсов. - vlan — для конкретного интерфейса VLAN.
show ipv6 ospf neighbor	-	Отобразить информацию об OSPF-соседях.
show ipv6 ospf packet-stats vlan *vlan_id*	vlan_id: (1..4094)	Отобразить статистику по пакетам.
show ipv6 ospf redist-config	-	Отобразить конфигурацию редистрибуции.
show ipv6 ospf route	-	Отобразить таблицу маршрутизации OSPF.
show ipv6 ospf virtual-links	-	Отобразить параметры и текущее состояние виртуальных линков.

4.28.5 Настройка протокола RIP

RIP — (Routing Information Protocol) протокол маршрутной информации, относящийся к внутренним протоколам маршрутизации дистанционно-векторного типа.

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*
router rip	-/-	Зайти в режим конфигурации процесса RIP.

Команды режима процесса RIP

Вид запроса командной строки в режиме конфигурации процесса RIP:

```
console(config-router)#
```

Таблица 207 — Команды режима конфигурации процесса RIP

Команда	*Значение/Значение по умолчанию*	*Действие*
auto-summary {disable | enable}	-/выключено	Установить автоматическое суммирование по классу сети: - **enable** — включить; - **disable** — выключить.
default-metric	metric: (1..16)/3	Установить значение метрики по умолчанию для маршрутов, полученных из других протоколов.
no default-metric		Установить значение по умолчанию.
distance *distance*	distance: (1..255)/121	Установить административную дистанцию для маршрутов RIP.
no distance		Установить значение по умолчанию.
network *ip_addr* **[unnum vlan** *vlan_id***]**	ip_addr:A.B.C.D vlan_id: (1..4094)	Включить RIP на IP-интерфейсе. - **unnum** — RIP будет включен на интерфейсе, на котором не задан IP-адрес, и RIP-сообщения будут отправляться от адреса *ip_addr*.
no network *ip_addr* **[unnum vlan** *vlan_id***]**		Выключить RIP на IP-интерфейсе.
output-delay	-/выключено	Включить задержку между пакетами RIP-сообщений.
no output-delay		Выключить задержку между пакетами RIP-сообщений.
passive-interface {Gigabitethernet *gi_port* **| Twopointfivegigabitethernet** *two_port* **| Tengigabitethernet** *te_port* **| vlan** *vlan_id***}**	gi_port: (0/1..48); two_port: (0/1..8); te_port: (0/1..11); vlan_id: (1..4094)/disabled	Запретить IP-интерфейсу посылать и принимать RIP-сообщения.
no passive-interface {Gigabitethernet *gi_port* **| Twopointfivegigabitethernet** *two_port* **| Tengigabitethernet** *te_port* **| vlan** *vlan_id***}**		Разрешить IP-интерфейсу посылать и принимать RIP-сообщения.
redistribute connected	-/выключено	Разрешить анонсирование connected-маршрутов.
no redistribute connected		Запретить анонсирование connected-маршрутов.
redistribute static	-/выключено	Разрешить анонсирование статических маршрутов.
no redistribute static		Запретить анонсирование статических маршрутов.
redistribute ospf	-/выключено	Разрешить анонсирование маршрутов, полученных

		по протоколу OSPF.
no redistribute ospf		Запретить анонсирование маршрутов, полученных по протоколу OSPF.
redistribute bgp	-/выключено	Разрешить анонсирование маршрутов, полученных по протоколу BGP.
no redistribute bgp		Запретить анонсирование маршрутов, полученных по протоколу BGP.
redistribute all	-/выключено	Разрешить анонсирование маршрутов из всех поддерживаемых протоколов.
no redistribute all		Запретить анонсирование маршрутов из всех поддерживаемых протоколов.
security {maximum | minimum}	-/maximum	Установить уровень безопасности: - **maximum** — RIPv1-пакеты будут игнорироваться, когда включена аутентификация; - **minimum** — RIPv1-пакеты будут приниматься, даже если аутентификация включена.
no security		Установить значение по умолчанию.
version {1 [2] | 2 [1] | none}	-/по умолчанию установлены и 1 и 2 версии	Установить версию RIP: - **1** — RIPv1; - **2** — RIPv2; - **none** — не посылать RIP-сообщения.
no version		Установить значение по умолчанию.

Команды режима конфигурации интерфейса VLAN

Вид запроса командной строки:

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

Таблица 208 — Команды режима конфигурации интерфейса VLAN

Команда	***Значение/Значение по умолчанию***	***Действие***
ip rip default route install	-/выключено	Установить шлюз по умолчанию в таблицу маршрутизации, если он присутствует в RIP-сообщениях.
no ip rip default route install		Установить значение по умолчанию.
ip rip default route originate *metric*	metric (1..15)	Включить объявление шлюза по умолчанию: - *metric* — метрика для маршрута по умолчанию.
no ip rip default route originate		Выключить объявление шлюза по умолчанию.
ip rip receive version {1 [2] | 2 [1] | none}	-/по умолчанию установлены и 1, и 2 версии	Установить версию RIP для принимаемых пакетов: - **1** — RIPv1; - **2** — RIPv2; - **none** — не посылать RIP-сообщения.
no ip rip receive version		Установить значение по умолчанию.
ip rip send version {1 [2] | 2 [1] | none}	-/по умолчанию установлены и 1, и 2 версии	Установить версию RIP для отправляемых пакетов: - **1** — RIPv1; - **2** — RIPv2; - **none** — не посылать RIP-сообщения.
no ip rip send version		Установить значение по умолчанию.
ip rip split-horizon [poisson]	-/включено	Включить расщепление горизонта. - **poisson** — реверсивно объявлять сети, принятые на текущем интерфейсе как недостижимые.
no ip rip split-horizon		Выключить расщепление горизонта.
ip rip summary-address *ip_addr prefix_length*	-/-	Выполнить суммирование маршрутов. - *ip_addr* — IP-адрес сети назначения; - *prefix_length* — IP-маска сети.
no ip rip summary-ad-		Выключить суммирование маршрутов.

dress *ip_addr prefix_length*		
ip rip timers basic *update invalid garbage*	update (10..3600)/30 секунд; invalid (30..500)/180 секунд; garbage (120..180)/120 секунд	Установить значения таймеров. - *update* — интервал между отправлением обновлений; - *invalid* — интервал, после которого маршруты будут помечены как недостижимые, если они не обновлялись; - *garbage* — интервал, после которого маршруты будут удалены, если они не обновлялись.
no ip rip timers basic		Установить значения по умолчанию.
ip rip auth-type {md5 | sha-1 | sha-256 | sha-384 | sha-512 | text key *string***}**	-/выключено	Включить RIP-аутентификацию и задать её тип. - **md5** — использовать шифрование MD5; - **sha-1** — использовать шифрование SHA-1; - **sha-256** — использовать шифрование SHA-256; - **sha-384** — использовать шифрование SHA-384; - **sha-512** — использовать шифрование SHA-512; - **text key** — не использовать шифрование (пароль передаётся в открытом виде); - *string* — пароль.
no ip rip authentication		Выключить RIP-аутентификацию.
ip rip authentication key-id *key_id* **key** *string*	key_id (0..255); string (1..16) символов	Добавить ключ аутентификации. - *key_id* — идентификатор ключа; - *string* — пароль.
no ip rip authentication key-id *key_id*		Удалить ключ.
ip rip key-id *key_id* **{start-accept | start-generate | stop-accept | stop-generate}** *year-mon-dd,hh:mm:ss*	key_id (0..255); year: (2000..2100); mon: (01..12); dd (01..31); hh: (00..23); mm: (00..59); ss: (00..59)	Установить параметры для ключа аутентификации. - **start-accept** — задать время, начиная с которого действует ключ на приём; - **start-generate** — задать время, начиная с которого действует ключ на передачу; - **stop-accept** — задать время, до которого действует ключ на приём; - **stop-generate** — задать время, до которого действует ключ на передачу; - *year-mon-dd,hh:mm:ss* — дата и время, значение по умолчанию для **start-accept** и **start-generate**: 2000-01-01,00:00:00.

Команды режима privileged EXEC

Вид запроса командной строки в режиме privileged EXEC:

```
console#
```

Таблица 209 — Команды режима privileged EXEC

Команда	***Значение/Значение по умолчанию***	***Действие***
show ip rip authentication	-	Отобразить информацию о аутентификации.
show ip rip database [*ip_addr prefix_length***]**	-	Отобразить базу данных. - *ip_addr* — IP-адрес сети; - *prefix_length* — IP-маска сети.
show ip rip peerinfo	-	Отобразить информацию о соседях.
show ip rip statistics	-	Отобразить общую статистику и статистику по интерфейсам.

4.29 Обновление программного обеспечения с сервера TFTP

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

Обновление программного обеспечения может осуществляться только привилегированным пользователем.

4.29.1 Обновление системного программного обеспечения

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

Процедура обновления ПО:

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

```
console# copy tftp://tftp_ip_address/[directory]/filename image
```

Или командой

```
console# firmware upgrade tftp://tftp_ip_address/[directory]/filename
```

Пример команды для загрузки ПО через sftp:

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

Новая версия программного обеспечения станет активной после перезагрузки коммутатора.

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

```
console# show bootvar
```

4.30 Режим отладки

Режим отладки позволяет снимать дополнительную диагностическую информацию с устройства.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 210 — Команды режима глобальной конфигурации

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 211 — Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
no debug all	-	Отключить вывод всех отладочных сообщений.
dump sockets	-	Просмотр всех сокетов в системе.
dump mem *location* **[len** *byte***]**	location: (1..0xffffffff); byte: (1..256)	Отобразить содержимого памяти из заданной области памяти.
dump {task | sem | que} name [*name***]**	-	Показать детали задачи, очереди или семафора при присвоении имени таска. - *name* – название таска.
debug test mem alloc *bytes*	bytes: (1..4294967295)	Выделить блок памяти с заданным в байтах размером.
debug test mem free	-	Освободить выделенный блок памяти.
debug show sensor temprerature *index*	index: (0..3)	Отобразить значения датчика температуры.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 212 — Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
debug np module { all | aps | cfa | eth | fwl | igs | ip | iss | isspi | l2app | la | mau | mlds | mstp | pnac | qosx | rstp | tcam | vct | vlan } [level {all | errors | general | polling}]	-	Включить генерацию отладочных сообщений для NPAPI для указанного модуля.
no debug np module { all | aps | cfa | eth | fwl | igs | ip | iss | isspi | l2app | la | mau | mlds | mstp | pnac | qosx | rstp | tcam | vct | vlan }		Выключить генерацию отладочных сообщений для NPAPI для указанного модуля.
debug show vlan np port [gigabitethernet *gi_port* **| twopointfivegigabitethernet** *two_port* **| tengigabitethernet** *te_port* **| port-channel** *group***]**	gi_port:(0/1..48); two_port: (0/1..8); te_port: (0/1..11); group: (1..24)	Отобразить конфигурацию порта NPAPI.

debug show ip arp np interfaces	-	Отобразить дерево интерфейсов ARP в NPAPI.

4.30.1 Команды отладки для интерфейсов

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 213 — Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
debug interface all *severity*	severity: (0..7)/-	Включить генерацию отладочных сообщений для всех видов трассировок.
no debug interface all		Выключить генерацию отладочных сообщений для интерфейсов.
debug interface arp-pkt-dump *severity*	severity: (0..7)/-	Включить трассировки дампа пакетов ARP.
no debug interface arp-pkt-dump		Выключить трассировки дампа пакетов ARP.
debug interface buffer *severity*	severity: (0..7)/-	Включить генерацию отладочных сообщений для пакетного буфера.
no debug interface buffer		Выключить генерацию отладочных сообщений для пакетного буфера.
debug interface enet-pkt-dump *severity*	severity: (0..7)/-	Включить трассировки дампа пакетов Ethernet.
no debug interface enet-pkt-dump		Выключить трассировки дампа пакетов Ethernet.
debug interface fail-all *severity*	severity: (0..7)/-	Включить генерацию отладочных сообщений при возникновении всех видов сбоев, включая валидацию пакетов.
no debug interface fail-all		Выключить генерацию отладочных сообщений при возникновении сбоев.
debug interface ip-pkt-dump *severity*	severity: (0..7)/-	Включить трассировки дампа пакетов IP.
no debug interface ip-pkt-dump		Выключить трассировки дампа пакетов IP.
debug interface os *severity*	severity: (0..7)/-	Генерировать отладочные сообщения для ресурсов ОС.
no debug interface os		Выключить генерацию отладочных сообщений для ресурсов ОС.
debug interface track *severity*	severity: (0..7)/-	Включить генерацию отладочных сообщений слежения интерфейса.
no debug interface track		Выключить генерацию отладочных сообщений слежения интерфейса.
debug interface trc-error *severity*	severity: (0..7)/-	Включить генерацию отладочных сообщений ошибок интерфейсов.
no debug interface trc-error		Выключить генерацию отладочных сообщений ошибок интерфейсов.

4.30.2 Отладка VLAN

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 214 — Команды режима EXEC

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

no debug vlan priority		Выключить генерацию отладочных сообщений приоритетов vlan.
debug vlan redundancy	-	Включить генерацию отладочных сообщений избыточности vlan.
no debug vlan redundancy		Выключить генерацию отладочных сообщений избыточности vlan.
debug garp	-/выключено	Включить отладку протокола GARP.
no debug garp		Выключить отладку протокола GARP.

4.30.3 Отладка Ethernet-oam

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 215 — Команды режима EXEC

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

debug ethernet-oam redundancy	-	Включить генерацию сообщений избыточности eoam.
no debug ethernet-oam redundancy		Выключить генерацию сообщений избыточности eoam.
debug ethernet-oam resource	-	Включить генерацию сообщений для ресурсов eoam, кроме буферов.
no debug ethernet-oam resource		Выключить генерацию сообщений для ресурсов eoam, кроме буферов.
debug ethernet-oam rfi	-	Включить генерацию сообщений удаленного обнаружения аварий eoam.
no debug ethernet-oam rfi		Выключить генерацию сообщений удаленного обнаружения аварий eoam.
debug ethernet-oam var-reqresp	-	Включить генерацию сообщений для значений запросов-ответов eoam.
no debug ethernet-oam var-reqresp		Выключить генерацию сообщений для значений запросов-ответов eoam.

4.30.4 Журналирование отладочных сообщений

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

Название журнала содержит в себе дату его создания на flash.

Команды режима глобальной конфигурации

Вид запроса командной строки режима глобальной конфигурации:

```
console(config)#
```

Таблица 216 — Команды режима

Команда	*Значение/Значение по умолчанию*	*Действие*
debug-logging { console | file | buffered-file}	-	Перенаправить вывод отладочных сообщений в конкретное расположение. **console** – в терминал консоли; **file** – в отдельный файл на flash; **buffered-file** – в отдельный буфер, при исчерпании ресурса буфера – в файл на flash.
no debug-logging		Установить значение по умолчанию.
debug-logging log-path {*flash_url***}**	flash:/LogDir/Debug/	Установить расположение файла, в который записываются debug-сообщения.
no debug-logging log-path		Установить значение по умолчанию.

Информация о debug-logging log-path хранится в файле nvram. Для возврата директории по умолчанию требуется использовать команду no debug-logging log-path или delete startup.

При использовании команды clear logs debug file стирается все содержимое директории, в которой находятся файлы журналов. Рекомендуется использовать отдельную директорию или директорию по умолчанию для хранения журналов во избежание потери конфигурацонных файлов.

Возможна совместная работа команд debug-logging console и debug-logging {file | buffered-file}

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 217 — Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
clear logs debug file	-	Очистить содержимое директории с debug-файлами.

4.30.5 Команды для отладки функций управления

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 218 — Команды режима EXEC

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

4.30.6 Команды для отладки протокола DHCP

Команды данного блока включают отслеживание модуля DHCP.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 219 — Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
debug ip dhcp snooping {all | critical | entry | exit | debug | fail}	-/выключено	Включить генерацию сообщений отладки функции DHCP Snooping.
no debug ip dhcp snooping {all | critical | entry | exit | debug | fail}		Выключить генерацию сообщений отладки функции DHCP Snooping.
debug ip dhcp client all	-/выключено	Включить генерацию всех сообщений отладки функции DHCP client.
no debug ip dhcp client all		Выключить генерацию всех сообщений отладки функции DHCP client.
debug ip dhcp client {bind | errors | event | packets}	-/выключено	Включить генерацию выборочных сообщений отладки функции DHCP client.
no debug ip dhcp client {bind | errors | event | packets}		Выключить генерацию выборочных сообщений отладки функции DHCP client.
debug ip dhcp relay {all | errors}	-/выключено	Включить генерацию сообщений отладки функции DHCP relay: - **all** – все отладочные сообщения; - **errors** – отладочные сообщения при ошибках.
no debug ip dhcp relay {all | errors}		Выключить генерацию сообщений отладки функции DHCP relay.
debug ip dhcp server {all | bind | arrors | events | linkage | packets}	-/выключено	Включить генерацию выборочных сообщений отладки функции DHCP server.
no debug ip dhcp server {all | bind | arrors | events | linkage | packets}		Выключить генерацию выборочных сообщений отладки функции DHCP server.
debug show ip dhcp np interfaces	-	Показать конфигурацию функции контроля протокола DHCP.

4.30.7 Отладка функции PPPoE-IA

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 220 — Команды режима EXEC

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

debug pppoe intermediate-agent pkt	-	Включить генерацию отладочных сообщений о пакетах PPPoE-IA.
no debug pppoe intermediate-agent		Выключить генерацию всех отладочных сообщений PPPoE-IA.

4.30.8 Отладка функции DCS

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 221 — Команды режима EXEC

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

4.30.9 Отладка функций QoS

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 222 — Команды режима EXEC

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

debug qos mgmt	-	Включить генерацию отладочных сообщений для управления QoS.
no debug qos mgmt		Выключить генерацию отладочных сообщений для управления QoS.
debug qos os	-	Включить генерацию отладочных сообщений для ресурсов QoS, кроме буферов.
no debug qos os		Выключить генерацию отладочных сообщений для ресурсов QoS, кроме буферов.
debug show qos meters	-	Отобразить информацию о количестве выделенных и свободных QoS Meters.

4.30.10 Команды для отладки протокола SNTP

Команды данного блока позволяют снимать дополнительную диагностическую информациюдля протокола SNTP.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 223 — Команды режима EXEC

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

4.30.11 Команды для отладки протокола STP

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 224 — Команды режима EXEC

Команда	*Значение/значение по умолчанию*	*Действие*
debug spanning-tree global	-/выключено	Включить генерацию отладочных сообщений для протокола STP глобально.
no debug spanning-tree global		Установить значение по умолчанию.
debug spanning-tree all	-/выключено	Включить генерацию всех отладочных сообщений для протокола STP.
no debug spanning-tree all		Установить значение по умолчанию.
debug spanning-tree errors	-/выключено	Включить генерацию сообщений отладки для протокола STP для диагностики ошибок.
no debug spanning-tree errors		Установить значение по умолчанию.

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

4.30.12 Команды для отладки протокола LLDP

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 225 — Команды режима EXEC

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

4.30.13 Команды для отладки функции IGMP Snooping

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

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 226 — Команды режима EXEC

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

4.30.14 Отладка для port-channel

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 227 — Команды режима EXEC

Команда	Значение/значение по умолчанию	Действие
debug lacp all	-	Включить генерацию всех отладочных сообщенийя для LACP.
no debug lacp all		Выключить генерацию всех отладочных сообщенийя для LACP.
debug lacp buffer	-	Включить генерацию отладочных сообщений по буферам LACP.
no debug lacp buffer		Выключить генерацию отладочных сообщений по буферам LACP.
debug lacp data	-	Включить генерацию отладочных сообщений обмена данными LACP.
no debug lacp data		Выключить генерацию отладочных сообщений обмена данными LACP.
debug lacp events	-	Включить генерацию отладочных сообщений по событиям LACP.
no debug lacp events		Выключить генерацию отладочных сообщений по событиям LACP.
debug lacp failall	-	Включить генерацию отладочных сообщений по ошибкам LACP.
no debug lacp failall		Выключить генерацию отладочных сообщений по ошибкам LACP.
debug lacp init-shutdown	-	Включить генерацию отладочных сообщений изменения состояния LACP.
no debug lacp init-shutdown		Выключить генерацию отладочных сообщений изменения состояния LACP.
debug lacp mgmt	-	Включить генерацию отладочных сообщений по управляющим сообщениям LACP.
no debug lacp mgmt		Выключить генерацию отладочных сообщений по управляющим сообщениям LACP.
debug lacp os	-	Включить генерацию отладочных сообщений по ресурсам LACP, исключая буферы.
no debug lacp os		Выключить генерацию отладочных сообщений по ресурсам LACP, исключая буферы.
debug lacp packet	-	Включить генерацию отладочных сообщений по пакетам LACP.
no debug lacp packet		Выключить генерацию отладочных сообщений по пакетам LACP.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 228 — Команды режима EXEC

Команда	Значение/значение по умолчанию	Действие
debug etherchannel all	-	Включить генерацию всех отладочных сообщений для LAG.
no debug etherchannel all		Выключить генерацию всех отладочных сообщений для LAG.
debug etherchannel detail	-	Включить генерацию подробных отладочных сообщений для LAG.
no debug etherchannel detail		Выключить генерацию подробных отладочных сообщений для LAG.

debug etherchannel error	-	Включить генерацию отладочных сообщений об ошибках LAG.
no debug etherchannel error		Выключить генерацию отладочных сообщений об ошибках LAG.
debug etherchannel event	-	Включить генерацию отладочных сообщений по событиям LAG.
no debug etherchannel event		Выключить генерацию отладочных сообщений по событиям LAG.
debug etherchannel idb	-	Включить генерацию отладочных сообщений по дескрипторам интерфейсов LAG.
no debug etherchannel idb		Выключить генерацию отладочных сообщений по дескрипторам интерфейсов LAG.

4.30.15 Отладка loopback-detection

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 229 — Команды режима EXEC

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

4.30.16 Отладка для протокола SNMP

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 230 — Команды режима EXEC

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

4.30.17 Команды для диагностики параметров TCAM

Команды данного блока позволяют снимать дополнительную диагностическую информацию для TCAM.

Команды режима EXEC

Вид запроса командной строки режима EXEC:

```
console#
```

Таблица 231 — Команды режима EXEC

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

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

ПРИЛОЖЕНИЕ А. КОНСОЛЬНЫЙ КАБЕЛЬ

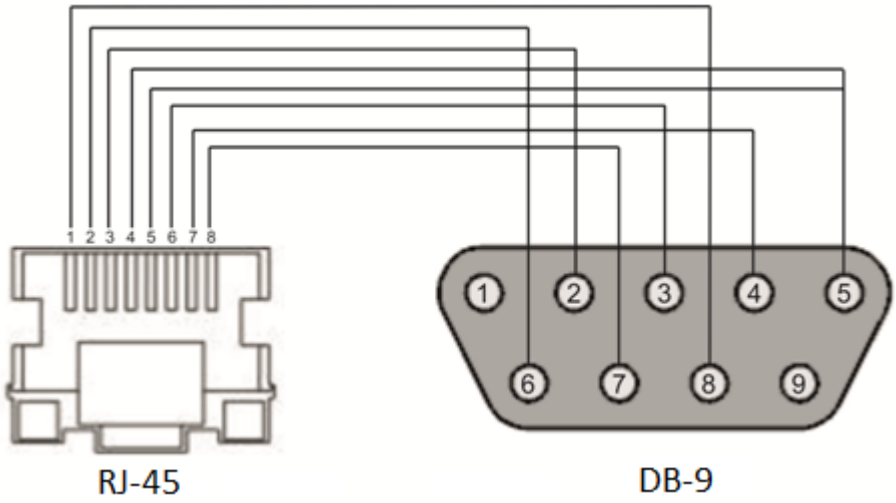

Рисунок А.1 – Подключение консольного кабеля

ПРИЛОЖЕНИЕ Б. ПОДДЕРЖИВАЕМЫЕ ЗНАЧЕНИЯ ETHERTYPE

Таблица Б.1 – Поддерживаемые значения EtherType

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

ПРИЛОЖЕНИЕ В. ОЧЕРЕДИ ДЛЯ ПРИНИМАЕМОГО НА CPU ТРАФИКА

Таблица В.1 — Распределение очередей для принимаемого на CPU трафика

Сервис	***Номер очереди***
Прочий трафик	1
Firewall (уведомление о начале атаки)	2
Незарегистрированный мультикаст (в режиме IP based IGMP/MLD)	7
Port Security (уведомление о превышении ограничения)	8
DHCP Client/Snooping	12
PPPoE IA Snooping	12
DHCP Server/Relay	15
EAPOL	16
L2 Protocol Tunneling	16
LLDP	18
OAM	20
IPv6 ND Inspection	21
ARP Inspection	22
IGMP/MLD Snooping	24
Пакеты с MAC DA коммутатора	25
Slow protocols (LACP)	30
BPDU	31
Loopback detection	31
Stacking	32

ПРИЛОЖЕНИЕ Г. РАСШИФРОВКА СПИСКА ПРОЦЕССОВ

Название	Описание
TMR#	Управление таймерами
PKTT	Периодическая отправка пакетов (сейчас не используется, поддерживает только Heart Beat)
VcmT	Обработка событий стека (сейчас не используется)
SMT	SYSLOG
CFA	Первоначальная обработка пакетов, мониторинг состояния портов
IPDB	Управление базой IP Binding (для ARP Inspection и IP Source Guard)
L2DS	DHCP Snooping
BOXF	Мониторинг состояния SFP
ERRD	Errdisable
ELMT	Мониторинг портов для Ethernet OAM
EOAT	Основной поток Ethernet OAM
FMGT	Ethernet OAM Fault Management, обработка событий в аппаратном окружении
AST	STP
PIf	IEEE 802.1x
LaTT	LAG, LACP
CNMT	MAC Notification
VLAN	Основной поток модуля VLAN
FDBP	Синхронизация с аппаратной MAC-таблицей
SnpT	IGMP/MLD Snooping
QoS	Основной поток модуля QoS
SMGT	Мониторинг аппаратного окружения (RAM, FLASH, вентиляторы, источники питания и прочее)
CPUU	Мониторинг утилизации CPU
BAKP	Автосохранение конфигурации
RT6	Маршрутизация IPv6
IP6	Обработка IPv6-пакетов
PNG6	Ping v6
RTM	Маршрутизация IPv4
IPFW	Обработка IPv4-пакетов
UDP	Обработка UDP-пакетов
ARP	Обработка ARP-пакетов
PNG	Ping v4
SLT	Управление сокетами
SAT	Сервер SNMP
TCP	Обработка TCP-пакетов
RAD	Клиент RADIUS
TACT	Клиент TACACS
DHRL	DHCP Relay
DHC	Протокол клиента DHCP
DCS	Прослушивание сокета для клиента DHCP
PIA	PPPoE Intermediate Agent
L2SN	IPv6 RA Guard
CLIC	CLI
CTS	Сервер TELNET

SSH	Сервер SSH
LLDP	LLDP
LBD	Loopback Detection
LOGF	Логирование отладочных сообщений
SNT	SNTP
STOC	Storm Control
HWPK	Измерение утилизации портов
MSR	Управление файлами конфигурации, загрузка/выгрузка файлов, обновление прошивки
C[200-999]	Временный поток для обработки отдельного подключения по TELNET/SSH

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения технической консультации по вопросам эксплуатации оборудования ООО «Предприятие «ЭЛТЕКС» Вы можете обратиться в Сервисный центр компании:

Форма обратной связи на сайте: **https://eltex-co.ru/support/**
Servicedesk: **https://servicedesk.eltex-co.ru**

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

Официальный сайт компании: **https://eltex-co.ru/**
База знаний: **https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base**
Центр загрузок: **https://eltex-co.ru/support/downloads**